Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Проєкт підсистеми виявлення вразливостей IT-інфраструктури на основі сканера безпеки OpenVAS»

Виконав: студент 4-го курсу групи КБ-22-2
спеціальності 125 «Кібербезпека»
_____ Денис ПРИХОДЬКО
Керівник: старший викладач кафедри КІ та КБ
_____ Ольга ДЯЧУК
Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент
_____ Юрій РОССІНСЬКИЙ

Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
_____ Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студент: Приходько Денис Сергійович

Тема роботи: «Проєкт підсистеми виявлення вразливостей IT-інфраструктури на основі сканера безпеки OpenVAS»

затверджена Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 17 червня 2026 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єкт дослідження: процес аудиту інформаційної безпеки IT-інфраструктури підприємства.

Предмет дослідження: методи та засоби автоматизованого аналізу вразливостей корпоративної мережі з використанням платформи Greenbone OpenVAS.

Вихідні дані для роботи: нормативні документи та стандарти у сфері інформаційної безпеки (ISO/IEC 27001, NIST SP 800-115, OWASP Testing Guide); технічна документація платформи Greenbone OpenVAS; науково-технічна література з питань аудиту безпеки та аналізу вразливостей; база даних Common Vulnerabilities and Exposures.

Обладнання та програмне забезпечення:

1. Персональний комп'ютер (процесор AMD, оперативна пам'ять 16 ГБ, накопичувач SSD);
2. Oracle VirtualBox 7.x – платформа віртуалізації для розгортання гостьових операційних систем;
3. GNS3 2.x – програмний емулятор мережевого обладнання для побудови тестової топології;
4. Cisco IOS 15.x – образ операційної системи маршрутизаторів Cisco для емуляції в GNS3;
5. Kali Linux 2026.x – спеціалізована операційна система для проведення тестування безпеки;
6. Greenbone OpenVAS (GVM 24.10) (Greenbone Vulnerability Manager) – платформа автоматизованого сканування вразливостей;
7. Ubuntu Server 22.04 LTS – серверна операційна система (цільовий вузол сканування);
8. Microsoft Windows 10 – клієнтська операційна система (цільовий вузол сканування);
9. Metasploitable 2 – навчальна операційна система з навмисно вразливою конфігурацією (цільовий вузол сканування).

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Артем ЛАЙЧУК	02.02.2026	02.02.2026
2	Артем ЛАЙЧУК	02.02.2026	02.02.2026
3	Артем ЛАЙЧУК	02.02.2026	02.02.2026

Студент _____ Денис ПРИХОДЬКО

Керівник _____ Ольга ДЯЧУК

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання, визначення мети та завдань дослідження	02.02 – 08.02	Виконано
2	Огляд літературних джерел та нормативно-правової бази з питань аудиту інформаційної безпеки	09.02 – 28.02	Виконано
3	Аналіз теоретичних засад аудиту безпеки та класифікація методів сканування. Написання розділу 1	01.03 – 21.03	Виконано
4	Порівняльний аналіз сучасних платформ сканування вразливостей та обґрунтування вибору OpenVAS	22.03 – 04.04	Виконано
5	Проєктування топології тестового мережевого середовища. Написання розділу 2	05.04 – 18.04	Виконано
6	Побудова тестового середовища у GNS3, розгортання віртуальних машин та налаштування мережевих служб	19.04 – 09.05	Виконано
7	Проведення трьох етапів сканування (Black Box, White Box, Full Network Audit)	10.05 – 23.05	Виконано
8	Аналіз результатів сканування, класифікація вразливостей та формування рекомендацій. Написання розділу 3	24.05 – 01.06	Виконано
9	Оформлення пояснювальної записки відповідно до вимог	02.06 – 05.06	Виконано
10	Підготовка презентації та доповіді до захисту	06.06 – 08.06	Виконано
11	Захист випускної кваліфікаційної роботи	17.06	

Студент _____ Денис ПРИХОДЬКО

Керівник _____ Ольга ДЯЧУК

АНОТАЦІЯ

Кваліфікаційна робота бакалавра: 172 сторінки, 79 рисунків, 6 таблиць, 34 джерела на 4 сторінках.

Мета кваліфікаційної роботи – дослідження та практична апробація методики комплексного аудиту інформаційної безпеки IT-інфраструктури підприємства з використанням автоматизованої платформи аналізу вразливостей Greenbone OpenVAS.

Проаналізовано теоретичні засади аудиту інформаційної безпеки, класифікацію типів аудиту та нормативно-правову базу у сфері захисту інформації. Розглянуто сучасні інструменти автоматизованого сканування вразливостей та обґрунтовано вибір платформи OpenVAS. Описано процес проєктування та побудови тестового мережевого середовища у програмному емуляторі GNS3, що включає маршрутизатори з протоколом резервування GLBP, серверні та клієнтські операційні системи. Показано налаштування та проведення трьох етапів сканування: зовнішнього неавтентифікованого (Black Box), внутрішнього автентифікованого (White Box) та повного мережевого аудиту підмережі підприємства. Наведено результати аналізу виявлених вразливостей, їхню класифікацію за шкалою CVSS та практичні рекомендації щодо усунення. Визначено, що комплексне застосування трьох методів аудиту є оптимальною стратегією оцінки захищеності корпоративної мережі.

Ключові слова: АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, OPENVAS, GREENBONE, СКАНУВАННЯ МЕРЕЖІ, КІБЕРБЕЗПЕКА, GNS3, METASPLOITABLE, CVSS, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, КОРПОРАТИВНА МЕРЕЖА, BLACK BOX, WHITE BOX.

ANNOTATION

Bachelor's Thesis: 172 pages, 79 figures, 6 tables, 34 references on 4 pages

The purpose of this thesis is to investigate and practically test a methodology for a comprehensive information security audit of an enterprise's IT infrastructure using the Greenbone OpenVAS automated vulnerability analysis platform.

The theoretical foundations of information security auditing, the classification of audit types, and the regulatory framework in the field of information protection are analyzed. Modern tools for automated vulnerability scanning are reviewed, and the choice of the OpenVAS platform is justified. The process of designing and building a test network environment in the GNS3 software emulator is described, which includes routers with the GLBP backup protocol, as well as server and client operating systems. The configuration and execution of three scanning stages are demonstrated: external unauthenticated (Black Box), internal authenticated (White Box), and a full network audit of the enterprise subnet. The results of the analysis of the identified vulnerabilities, their classification on the CVSS scale, and practical recommendations for remediation are presented. It is determined that the comprehensive application of the three audit methods is the optimal strategy for assessing the security of a corporate network.

Keywords: INFORMATION SECURITY AUDIT, VULNERABILITY ANALYSIS, OPENVAS, GREENBONE, NETWORK SCANNING, CYBERSECURITY, GNS3, METASPLOITABLE, CVSS, PENETRATION TESTING, CORPORATE NETWORK, BLACK BOX, WHITE BOX.

ЗМІСТ

ВСТУП 10
РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІТ-ІНФРАСТРУКТУРИ 12
1.1. Поняття та класифікація вразливостей інформаційних систем 12
1.2. Основні загрози безпеці ІТ-інфраструктури 14
1.3. Методи виявлення вразливостей 17
1.4. Огляд сучасних систем сканування вразливостей 25
1.5. Порівняльний аналіз систем сканування вразливостей 29
1.6. Обґрунтування вибору OpenVAS 36
Висновки до першого розділу 40
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІТ-ІНФРАСТРУКТУРИ 42
2.1. Архітектура підсистеми виявлення вразливостей 42
2.2. Функціональна структура системи 46
2.3. Модель взаємодії компонентів системи 51
2.4. Розробка топології тестової мережі 53
2.5. Модель загроз для досліджуваної ІТ-інфраструктури 58
Висновки до другого розділу 61
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НА БАЗІ OPENVAS 63
3.1. Встановлення та налаштування OpenVAS 63
3.2. Створення тестового середовища 73
3.3. Налаштування та проведення сканування ІТ-інфраструктури 91
3.4. Аналіз результатів сканування та оцінка вразливостей 105
Висновки до третього розділу 115
ВИСНОВКИ 117
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 119
ДОДАТКИ 123

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AJP (Apache JServ Protocol) – протокол взаємодії між вебсервером та контейнером сервлетів

ARP (Address Resolution Protocol) – протокол визначення MAC-адреси за IP-адресою

CBC (Cipher Block Chaining) – режим зчеплення блоків шифрування

CVE (Common Vulnerabilities and Exposures) – єдиний реєстр ідентифікаторів вразливостей

CVSS (Common Vulnerability Scoring System) – система оцінювання критичності вразливостей

DCE/RPC (Distributed Computing Environment / Remote Procedure Call) – протокол віддаленого виклику процедур

DH (Diffie-Hellman) – алгоритм обміну криптографічними ключами

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного призначення мережевих адрес

DNS (Domain Name System) – система доменних імен

EOL (End of Life) – завершення терміну підтримки програмного продукту

FTP (File Transfer Protocol) – протокол передачі файлів

GLBP (Gateway Load Balancing Protocol) – протокол балансування навантаження шлюзів

GNS3 (Graphical Network Simulator 3) – програмний емулятор мережевого обладнання

HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту

IANA (Internet Assigned Numbers Authority) – організація з призначення номерів портів та протоколів

ICMP (Internet Control Message Protocol) – протокол міжмережевих керуючих повідомлень

IEC (International Electrotechnical Commission) – Міжнародна електротехнічна комісія

IP (Internet Protocol) – міжмережевий протокол

ISO (International Organization for Standardization) – Міжнародна організація зі стандартизації

IT – інформаційні технології

KEX (Key Exchange) – обмін криптографічними ключами

MAC (Message Authentication Code) – код автентифікації повідомлення

NAT (Network Address Translation) – трансляція мережевих адрес

NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технологій США

NVT (Network Vulnerability Tests) – тести мережевих вразливостей

ОС – операційна система

OWASP (Open Web Application Security Project) – відкритий проєкт із забезпечення безпеки вебзастосунків

ПЗ – програмне забезпечення

QoD (Quality of Detection) – якість виявлення вразливості

RCE (Remote Code Execution) – віддалене виконання коду

RMI (Remote Method Invocation) – віддалений виклик методів

SMB (Server Message Block) – протокол спільного доступу до ресурсів у мережах Windows

SSH (Secure Shell) – протокол захищеного віддаленого доступу

TCP (Transmission Control Protocol) – протокол управління передачею даних

UDP (User Datagram Protocol) – протокол передачі датаграм

VNC (Virtual Network Computing) – протокол віддаленого доступу до графічного робочого столу

VPN (Virtual Private Network) – віртуальна приватна мережа

XSS (Cross-Site Scripting) – міжсайтове виконання скриптів

ВСТУП

В умовах стрімкої цифровізації бізнес-процесів та зростання кількості кіберзагроз питання захисту IT-інфраструктури підприємств набуває стратегічного значення. За даними міжнародних аналітичних звітів, кількість кібератак на організації малого та середнього бізнесу щорічно зростає, при цьому значна частина інцидентів обумовлена наявністю відомих, але вчасно не усунених вразливостей у програмному забезпеченні та мережевому обладнанні. Аудит інформаційної безпеки є одним із ключових механізмів виявлення таких вразливостей до того, як ними скористається зловмисник. Проте на практиці більшість вітчизняних підприємств не проводять регулярного аудиту через високу вартість комерційних рішень та відсутність кваліфікованих спеціалістів. Використання вільно розповсюджуваних платформ з відкритим вихідним кодом, таких як Greenbone OpenVAS, дозволяє суттєво знизити фінансовий бар'єр та зробити аудит безпеки доступним для організацій з обмеженим бюджетом. Актуальність роботи також підсилюється тим, що для ефективного аудиту необхідне коректне поєднання різних методів сканування, проте практичні рекомендації щодо їхнього комплексного застосування у корпоративних мережах залишаються недостатньо систематизованими в україномовній літературі.

Метою кваліфікаційної роботи є дослідження та практична апробація методики комплексного аудиту інформаційної безпеки IT-інфраструктури підприємства з використанням автоматизованої платформи аналізу вразливостей Greenbone OpenVAS.

Визначена мета обумовлює наступні завдання:

1. Проаналізувати теоретичні засади аудиту інформаційної безпеки, класифікацію типів аудиту та чинну нормативно-правову базу;
2. Провести порівняльний аналіз сучасних платформ автоматизованого сканування вразливостей та обґрунтувати вибір інструменту для проведення аудиту;
3. Спроєктувати та побудувати тестове мережеве середовище, що відтворює типову архітектуру корпоративної мережі підприємства;

4. Провести комплексне сканування тестової інфраструктури з використанням трьох методів аудиту (зовнішній, внутрішній та мережевий) та проаналізувати отримані результати;

5. Розробити практичні рекомендації щодо усунення виявлених вразливостей та підвищення рівня захищеності інфраструктури.

Об'єктом дослідження є процес аудиту інформаційної безпеки IT-інфраструктури підприємства.

Предметом дослідження є методи та засоби автоматизованого аналізу вразливостей корпоративної мережі з використанням платформи Greenbone OpenVAS.

У процесі виконання кваліфікаційної роботи було розроблено проєкт тестового мережевого середовища у програмному емуляторі GNS3, яке відтворює типову інфраструктуру малого підприємства, та проведено його комплексний аудит безпеки з використанням трьох різних методів сканування засобами платформи OpenVAS.

Практичне значення отриманих результатів полягає в тому, що розроблена методика комплексного триетапного аудиту може бути безпосередньо використана системними адміністраторами та спеціалістами з кібербезпеки організацій малого та середнього бізнесу для проведення регулярної оцінки захищеності власної IT-інфраструктури. Побудоване тестове мережеве середовище у GNS3 є повністю відтворюваним і може слугувати лабораторною базою для навчальних курсів з аудиту інформаційної безпеки у закладах вищої освіти. Сформульовані за результатами сканування рекомендації щодо усунення вразливостей мають прикладний характер та можуть бути адаптовані до реальних корпоративних мереж.

Апробація результатів дослідження. Основні положення та результати кваліфікаційної роботи були представлені на XVI Міжнародній науково-технічній конференції «Інформаційно-комп'ютерні технології — 2026» (м. Житомир, 2–3 квітня 2026 р.) та опубліковані у збірнику матеріалів конференції [15].

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІТ-ІНФРАСТРУКТУРИ

1.1. Поняття та класифікація вразливостей інформаційних систем

Фундаментальною основою комплексної кібербезпеки є чітке розуміння терміну “вразливість”. Еволюція ІТ-інфраструктур змістила концепцію сприйняття цього поняття від суто технічних програмних помилок до комплексного ризик-орієнтованого підходу, що охоплює архітектурні, організаційні, апаратні та процесні аспекти.

У світовому консенсусі ключову роль відіграють стандарти ISO/IEC 27000. Відповідно до базових документів ISO/IEC 27001 та 27002, вразливість – це “слабкість активу або засобу контролю, яка може бути використана загрозами”. Це цілеспрямовано виводить поняття за межі ІТ-систем, адже активом є будь-що цінне для організації: бази даних, інтелектуальна власність, персонал та фізичні приміщення [1].

Альтернативний підхід NIST є більш інфраструктурно-орієнтованим. Вразливість тут концептуалізується як специфічний недолік у системі, процедурах безпеки чи внутрішньому контролі. Методологія NIST передбачає ітеративну оцінку ризиків від базової підготовки до безперервного моніторингу [2]. Інші фреймворки доповнюють картину власною специфікою: FAIR розглядає вразливість як математичну ймовірність фінансових втрат, PCI DSS фокусується на загрозі компрометації платіжних даних, а CIS RAM - на безпеці інформаційних активів [3].

В Україні термінологія у сфері ТЗІ визначається документом НД ТЗІ 1.1-003-99, де “уразливість системи” трактується як її нездатність протистояти загрозам. Експлуатація вразливості призводить до порушення ключових властивостей інформації: конфіденційності, цілісності та доступності (тріада CIA). Крім того, в Україні діє гармонізований стандарт ДСТУ ISO/IEC 27000:2015, який повністю імплементує міжнародний концепт оцінки слабкостей активу [4].

Для проектування систем безпеки критично важливо розмежовувати ці два концепти, що інституціоналізовано в екосистемі MITRE (бази CWE, CVE та NVD від NIST).

CWE (Common Weakness Enumeration) каталогізує типи фундаментальних архітектурних чи синтаксичних помилок. Це першопричина, яка виникає на етапі написання коду і вимагає превентивних дій від розробників.

Натомість CVE (Common Vulnerabilities and Exposures) документує конкретні інциденти у вже розгорнутому ПЗ. Вразливість за класифікацією CVE - це специфічний екземпляр слабкості у реальному продукті. Ці дані використовуються командами SOC для оперативного реагування та управління патчами.

Історичні моделі розподіляли дефекти за генезисом (навмисні/ненавмисні), часом виникнення та місцем локалізації. Сучасна практика відмовляється від однопараметричних класифікацій через їхню епістемологічну обмеженість. Натомість використовується багатопараметричний підхід, який дозволяє виділити три магістральні групи вразливостей: програмні дефекти коду, мережеві/інфраструктурні вразливості та організаційно-процесні прогалини [5].

Для ефективної пріоритезації загроз індустрія використовує Загальну систему оцінки вразливостей - CVSS. Перехід на версію CVSS v4.0 був зумовлений системною проблемою “інфляції балів” попередньої версії 3.1, коли невиправдано велика кількість вразливостей отримувала максимальний статус критичності [6].

Нова архітектура CVSS v4.0 забезпечує точнішу гранулярність і складається з 4 груп метрик:

1. Базові: Відображають незмінні якості вразливості. Введено нову метрику “Вимоги до атаки” (AT) та деталізовано “Взаємодію з користувачем” (UI).
2. Загрози: Замінили “Часові” метрики, змістивши фокус на реальне існування робочого експлойту в дикій природі.
3. Середовища: Дозволяють скоригувати базовий бал залежно від бізнес-цінності конкретного IT-активу компанії.
4. Додаткові: Нова група контекстних даних, що не впливає на математичний бал, але вказує на супутні ризики.

Важливою зміною стала ліквідація неоднозначної метрики “Область дії” та її заміна на чітке розмежування впливу: окремо на вразливу систему та на пов'язані з нею вузли. Впровадження метрик загрози у CVSS v4.0 дозволяє знизити кількість хибних спрацювань і вразливостей, що потребують термінового реагування, на 65–76%. Це забезпечує надійну аналітичну базу для сучасних систем автоматичного сканування і процесів управління вразливостями [6].

1.2. Основні загрози безпеці IT-інфраструктури

Поняття “загроза” є концептуально невіддільним від поняття “вразливість”. Якщо вразливість виступає пасивною умовою або слабкістю активу, то загроза є активним каталізатором, який здатний цю слабкість експлуатувати для нанесення шкоди IT-інфраструктурі.

У національному нормативно-правовому полі України базовим документом у сфері захисту інформації є НД ТЗІ 1.1-003-99. Відповідно до нього, загроза визначається як будь-які обставини або події, що можуть бути причиною порушення політики безпеки та призвести до втрати конфіденційності, цілісності або доступності інформації. Спроба практичної реалізації такої загрози кваліфікується як атака. З розвитком технологій на законодавчому рівні (Закон України “Про основні засади забезпечення кібербезпеки України”) було закріплено поняття “кіберзагроза” – наявні та потенційно можливі явища у кіберпросторі, які створюють небезпеку національним інтересам, причому пріоритетного захисту потребують об'єкти критичної інфраструктури.

У міжнародній моделі управління ризиками (стандарт NIST SP 800-30 Rev. 1) загрози аналізуються через дві складові: джерела загроз (об'єкти з потенціалом ініціювання атаки) та події загроз. Оцінка ризиків за NIST вимагає вимірювання ймовірності того, що джерело успішно ініціює подію загрози й подолає існуючі засоби контролю. У теорії технічного захисту інформації загрози традиційно класифікують за декількома ключовими ознаками. За результатом впливу на систему виокремлюють загрози порушення конфіденційності, порушення цілісності та порушення доступності [7].

За джерелом виникнення загрози поділяються на три класи. Перший - людський чинник, який включає як зовнішні атаки хакерських угруповань, так і внутрішні інциденти, такі як умисний інсайдерський виток даних чи помилки персоналу. Другий - технічний чинник, що охоплює апаратні збої, фізичне зношення обладнання та програмні баги. Третій - стихійний чинник. Сьогодні саме зовнішній людський чинник формує найнебезпечніший глобальний ландшафт кіберзагроз.

Згідно зі звітом Європейського агентства з кібербезпеки (ENISA) “Threat Landscape 2025”, кіберзлочинність продовжує індустріалізуватися. До ключових глобальних загроз 2024-2025 років належать (Рис. 1.1.):

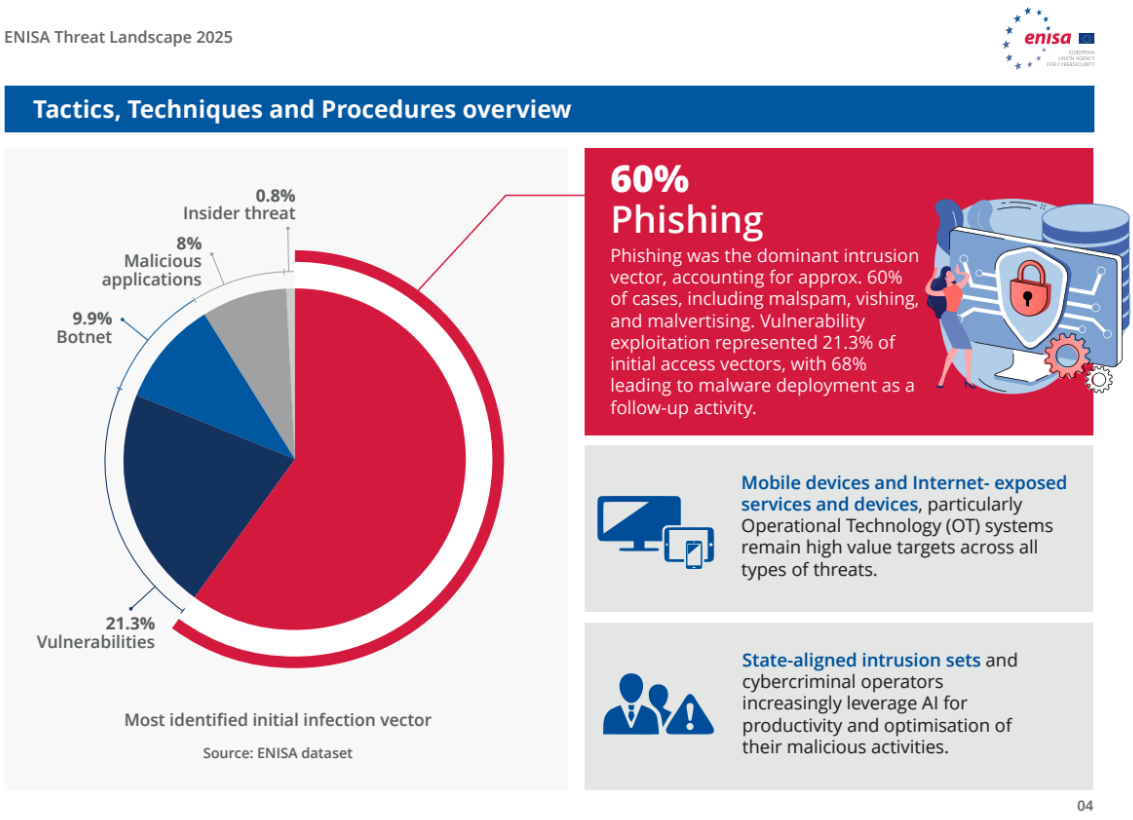


Рисунок 1.1 – Глобальні вектори кібератак (ENISA, 2025)

1. Програми-вимагачі та Фішинг: Фішинг залишається домінуючим вектором початкового доступу, на який припадає близько 60% усіх спроб вторгнення, що часто слугує “вхідними дверима” для розгортання Ransomware. Зловмисники децентралізують інфраструктуру та активно використовують модель RaaS.

2. Соціальна інженерія з використанням ШІ: Зловмисники змінюють тактику. Майже 1 з 4 атак (~25%) у корпоративних додатках для спільної роботи (Teams,

Zoom тощо) вже включає використання згенерованих ШІ дипфейків або автоматизованих експлойтів для крадіжки сесій.

3. Шкідливе програмне забезпечення та BEC-атаки: Програми-крадії інформації продовжують збирати облікові дані, а кількість атак типу BEC (спрямованих на підміну платіжних доручень) зросла на 33% лише за один квартал.

4. Експлуатація вразливостей: Знаходиться на другому місці з показником 21,3% успішних початкових вторгнень.

Головними цілями для атак у глобальному вимірі залишається сектор державного управління (≈38% інцидентів в ЄС), а також транспорт, цифрова інфраструктура та фінанси. Важливо зазначити, що 53,7% усіх інцидентів припадає саме на критично важливі організації [8].

В Україні ландшафт кіберзагроз має яскраво виражену специфіку, зумовлену збройною агресією рф, де кібератаки синхронізуються з кінетичними ударами та інформаційними операціями. За даними CERT-UA, у 2025 році кількість опрацьованих кіберінцидентів зросла на 37,4% і досягла 5927 випадків. Домінуючими векторами початкового проникнення стали соціальна інженерія (зокрема глибоко персоналізований фішинг), експлуатація програмних вразливостей, використання скомпрометованих облікових записів та атаки на ланцюги постачання. Найбільшу кількість кібератак було спрямовано на державні органи, сектор безпеки і оборони, енергетичний сектор та оборонно-промисловий комплекс. Водночас спостерігається стала тенденція до розширення географії атак - мішенями дедалі частіше стають місцеві органи влади, комунальні підприємства та провайдери прифронтових областей [9].

Російські кібероперації у 2025 році зазнали концептуальних змін: фокус змістився з масованих деструктивних атак на стратегічне кібершпигунство. Пріоритетним завданням для ворога стало отримання доступу та довготривале приховане закріплення в IT-інфраструктурах. Окремою небезпечною тенденцією є масштабування атак на ланцюги постачання: оскільки рівень захисту основних цілей зріс, атакуючі компрометують постачальників спеціалізованого ПЗ та IT-послуг, щоб непомітно закріпитися в системах критичної інфраструктури. Крім

того, ландшафт загроз ускладнюється злиттям різних груп: державні APT-групи все частіше співпрацюють із фінансово-вмотивованими кіберзлочинцями та псевдохактивістами, надаючи їм сучасний інструментарій в обмін на розширення масштабів атак та доступ до розвідувальних даних [9].

1.3. Методи виявлення вразливостей

Сучасний ландшафт кіберзагроз характеризується активізацією передових постійних загроз класу APT, які використовують масштабне сканування Інтернету для пошуку вразливих активів. За таких умов фундаментальна проблема багатьох корпоративних програм кібербезпеки полягає у проведенні так званих "щорічних ритуалів" тестування. Це створює хибне відчуття захищеності та залишає величезний розрив між задокументованою політикою безпеки та реальною ефективністю технічних засобів. Для подолання цієї моделі галузеві регулятори вимагають переходу до безперервного управління експозицією інфраструктури. Цей підхід гармонійно поєднує пасивний аудит, автоматизоване активне сканування та тестування на проникнення як синергетичні компоненти єдиної архітектури безпеки.

Мережевий пентест у цій системі - це процес практичної оцінки безпеки комп’ютерних мереж шляхом моделювання реальних кібератак. Зазвичай таке тестування проводять команди фахівців із кібербезпеки, які намагаються знайти та використати слабкі місця в інфраструктурі. Основна мета пентесту полягає у виявленні та усуненні вразливостей до того, як їх зможуть експлуатувати зловмисники для несанкціонованого доступу до систем або конфіденційних даних (Рис. 1.2.). Це дозволяє організації об'єктивно оцінити рівень безпеки мережі, перевірити ефективність впроваджених засобів захисту, розробити стратегії ремедіації та підвищити практичну обізнаність співробітників [10].



Рисунок 1.2 – Переваги мережевого пентесту (Datami)

Проведення мережевого пентесту є критично необхідним перед впровадженням нових систем, після суттєвих змін в IT-інфраструктурі та для підтвердження відповідності галузевим нормативним стандартам. Регулярне тестування забезпечує виявлення слабких місць у конфігураціях, логічно обґрунтовує необхідність інвестицій у посилення захисту та надійно оберігає репутацію компанії від можливих інцидентів. Крім того, такий підхід значно підвищує готовність внутрішніх команд своєчасно та правильно реагувати на реальні загрози, роблячи пентест невід'ємним інструментом захисту на всіх рівнях [10].

Для перетворення пошуку вразливостей на формалізований та повторюваний процес індустрія використовує міжнародні стандарти. Документ NIST SP 800-115 є абсолютним галузевим орієнтиром, який переводить оцінку безпеки у площину суворої практичної технічної валідації. Цей стандарт визначає структурований життєвий цикл тестування: від планування області перевірки до експлуатації вразливостей та розробки стратегій їх усунення [11]. Комплексний огляд методів та інструментів оцінки мережевої безпеки, включаючи сканування портів, ідентифікацію сервісів та аналіз вразливостей на різних рівнях мережевої моделі, систематизований у спеціалізованій літературі з мережевого аудиту [34].

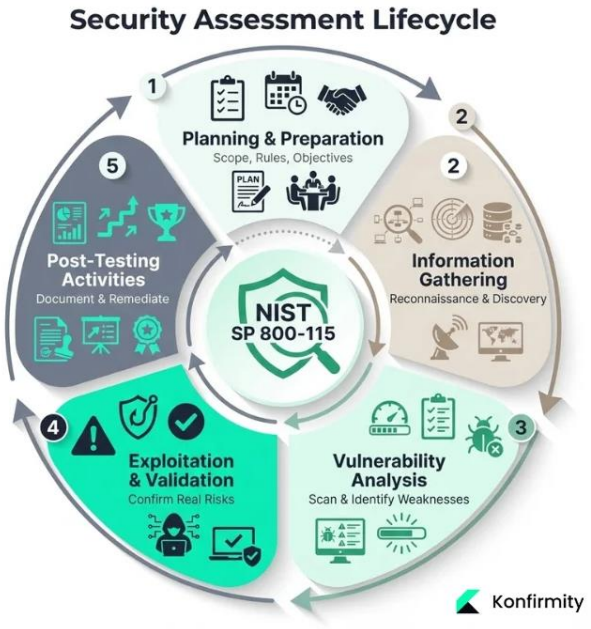


Рисунок 1.3 – Життєвий цикл оцінки безпеки (Konfirmity)

Існують також вузькоспеціалізовані методології. OSSTMM пропонує науково-обґрунтований підхід до тестування мережевих середовищ із глибоким аналізом довіри та автентифікації. З іншого боку, проєкт OWASP виступає глобальним еталоном для оцінки захищеності програмного забезпечення на прикладному рівні [12].

Пасивний аудит є першим ешелоном виявлення вразливостей, що базується на принципі абсолютного невтручання в операційну діяльність. Інструменти збирають інформацію шляхом тихого спостереження: аналізують існуючі потоки мережевих даних, конфігураційні файли та журнали подій [13].

На рівні інфраструктури використовуються пасивні сканери вразливостей. Вони безперервно перехоплюють трафік, ідентифікують підключені пристрої, відкриті порти та запущені додатки, не надсилаючи тестових пакетів. Головна перевага пасивного сканування - абсолютна безпечність для критичних та нестабільних середовищ. Проте цей метод має "сліпі зони": він ідентифікує лише ті загрози, які проявляються під час передачі даних мережею, і не виявляє приховані некоректні конфігурації всередині системи [13].

Активне сканування передбачає пряму взаємодію з інформаційними системами шляхом відправлення згенерованих пакетів даних та аналізу відповідей.

Цей процес дозволяє виявляти активні хости, відкриті порти та порівнювати отримані параметри з глобальними базами відомих вразливостей [13].

Критичним аспектом цього методу є наявність або відсутність у сканера легітимних облікових даних.

1. Неавтентифіковане сканування виконується без системних привілеїв, імітуючи розвідку зовнішнього хакера. Воно виявляє вразливості, доступні ззовні, які зазвичай мають найвищий пріоритет критичності.

2. Автентифіковане сканування передбачає надання сканеру адміністративних прав, що дозволяє проводити глибоку інспекцію внутрішньої архітектури, перевіряти реєстри та контролювати наявність локальних оновлень ОС [13].

Професійна стратегія безпеки вимагає комбінації обох методів. Проте активне сканування генерує значне мережеве навантаження і може спричинити збої в роботі застарілого обладнання, тому його частіше планують у спеціальні технологічні вікна. Для комплексного розуміння концептуальних відмінностей між цими двома підходами, доцільно розглянути їх порівняльну характеристику (табл. 1.1).

Таблиця 1.1

Порівняння активного та пасивного підходів до виявлення вразливостей

Характеристика	**Активний моніторинг (сканування)**	**Пасивний моніторинг (аудит)**
Природа використовуваних даних	Використовує синтетичні (штучно згенеровані) дані.	Використовує реальні мережеві дані.
Обсяг даних	Використовується менший обсяг даних.	Використовується значно більший обсяг даних.
Сценарії використання	Тестування якості обслуговування (QoS), виявлення проблем, оцінка нового обладнання, вимірювання продуктивності.	Моніторинг стану та працездатності інфраструктури, виявлення патернів використання, системи виявлення вторгнень (IDS).

Продовження таблиці 1.1

Контроль над даними	Повний контроль (параметри кількості пакетів, їх розміру, періодичності тощо).	Обмежений контроль, оскільки дані генеруються реальними процесами.
Виявлення проблем	Проактивне (на випередження).	Реактивне (за фактом події).
Вимоги до зберігання	Менші вимоги завдяки невеликому обсягу даних.	Вимагає більш ємних та масштабованих систем зберігання.
Вимоги до обчислювальних ресурсів	Менш ресурсоємне через менший обсяг та низьку складність даних.	Висока ресурсоємність через необхідність обробки та аналізу великих масивів складних даних.
Питання конфіденційності	Відсутні, оскільки використовуються синтетичні дані.	Існує необхідність вирішення питань конфіденційності, пов'язаних із перехопленням реальних даних користувачів.
Складність даних	Синтетично згенеровані дані є менш складними та прогнозованими.	Вища складність через захоплення різноманітних та гетерогенних типів реальних даних.
Характер виявлених проблем	Не здатен виявляти періодичні (плаваючі) проблеми, оскільки тести проводяться лише у визначені проміжки часу.	Дозволяє ідентифікувати складні періодичні проблеми завдяки безперервному аналізу.

Якщо сканери надають перелік потенційних проблем, то тестування на проникнення є глибоким процесом їх практичної валідації. Етичний хакер цілеспрямовано імітує логіку зловмисника: використовує соціальну інженерію, підбирає паролі та безпосередньо експлуатує програмні недоліки для отримання несанкціонованого контролю. Саме фази експлуатації та постексплуатації наочно доводять керівництву, що конкретна вразливість може призвести до реальних збитків.

Залежно від наданої інформації, пентестинг поділяють на метод чорного ящика (повна імітація зовнішньої атаки без знань про систему), білого ящика (повний доступ до архітектури та коду) та сірого ящика (частковий доступ, що імітує компрометацію інсайдера). Для забезпечення всебічного аналізу та уникнення хаотичного підходу процес тестування суворо регламентується Стандартом проведення тестування на проникнення - PTES. Ця методологія діє як

комплексний посібник, що гарантує послідовність, структурність та ретельність перевірок.



Рисунок 1.4 – Переваги використання PTES (Datami)

Впровадження PTES надає організаціям значні стратегічні переваги. Стандарт забезпечує повноту процесу кіберзахисту, гнучке управління ризиками та сприяє ефективній комунікації між технічним персоналом і керівництвом завдяки зрозумілому звітуванню. Окрім цього, методологія дозволяє компаніям порівнювати свої практики з визнаними світовими еталонами та постійно вдосконалювати захист [14].



Рисунок 1.5 – 7 основних етапів PTES (Datami)

Для досягнення цих результатів методологія PTES визначає сім нерозривних етапів тестування:

1. Починається все з попереднього планування, де визначаються цілі, межі аналізу та правила взаємодії.

2. Далі йде збір інформації за допомогою методів відкритої розвідки OSINT та сканування.

3. На етапі моделювання загроз фахівці класифікують активи та створюють профілі потенційних зловмисників.

4. Після цього проводиться детальний аналіз вразливостей із поєднанням автоматизованих інструментів та ручної перевірки.

5. Кульмінацією є безпосередня експлуатація вразливостей - контрольована імітація хакерської атаки з урахуванням непомітності та глибини проникнення.

6. Фаза постексплуатації дозволяє оцінити реальну цінність скомпрометованих ресурсів і стратегію утримання доступу.

7. Завершується процес звітуванням, яке включає резюме для керівництва та детальний технічний звіт [14].



Рисунок 1.6 – Ризики і наслідки недотримання вимог PTES (Datami)

Недотримання цих суворих вимог несе серйозні ризики для компанії. Відсутність стандартизованого підходу неминуче призводить до неповного виявлення критичних недоліків, хибної оцінки ризиків та марнотратного використання ресурсів. До того ж це створює юридичні загрози, оскільки відповідність стандартам є обов'язковою вимогою багатьох регуляторів, зокрема стандарту безпеки платіжних карток PCI DSS [14].

Підсумовуючи комплексний аналіз, можна стверджувати, що покладання виключно на один технічний підхід є критичною архітектурною помилкою. Максимальний рівень стійкості досягається лише через об'єднання всіх методів у єдину систему захисту, архітектуру якої доцільно вибудовувати за принципом аналітичної лійки:

1. Фундаментальний рівень: Забезпечує безперервний макрорівневий нагляд. Інструменти пасивного аудиту тихо фіксують появу нових IT-активів та відхилення від конфігурацій у режимі реального часу без ризику системних збоїв.

2. Операційний рівень: Деталізує картину за допомогою регулярних автоматизованих перевірок. Активне сканування контролює наявність відомих експлойтів та актуальність патчів як на периметрі, так і всередині мережі.

3. Експертний рівень: Періодична ручна валідація критичних точок відмови етичними хакерами за стандартом PTES. Дозволяє перевірити стійкість бізнес-логіки додатків та швидкість реакції внутрішніх команд безпеки на складні цілеспрямовані атаки [14].

1.4. Огляд сучасних систем сканування вразливостей

Сучасні підходи до класифікації загроз тісно пов'язані з міжнародними стандартами. Наприклад, бази даних CWE та OWASP створюють єдину структуру для визначення типових програмних помилок, звертаючи увагу на головні причини їх виникнення. Ускладнення корпоративних мереж, використання хмарних технологій та Інтернету речей створюють потребу в надійних інструментах для пошуку загроз. Сьогодні якісна платформа управління вразливостями має не лише знаходити застарілі програми, але й оцінювати реальну ймовірність успішної атаки, враховуючи специфіку бізнес-процесів компанії [15].

Наявність або відсутність у сканера прав доступу суттєво впливає на результати перевірки. Сканування без авторизації імітує дії зовнішнього порушника, шукаючи відкриті порти та загальні помилки в налаштуваннях. Цей процес швидкий, але дає лише поверхневу картину. Сканування з авторизацією надає програмі легальний доступ до операційної системи. Це дає змогу перевірити системний реєстр, точні версії встановлених програм та локальні правила безпеки. Цей метод виявляє значно більше недоліків і менше навантажує мережу, але потребує надійного зберігання паролів для сканування.

Раніше мережеве сканування мало проблеми з переносними робочими комп'ютерами, які рідко перебувають у корпоративній мережі достатньо довго для повної перевірки. Тому розробники почали використовувати програмних агентів. Це невеликі програми, які встановлюються безпосередньо на комп'ютери працівників і локально аналізують файли від імені адміністратора. Оскільки агент

сам встановлює зв'язок із центральним сервером, відпадає потреба змінювати правила мережевих екранів для вхідного трафіку. Це дозволяє безперервно контролювати стан безпеки: щойно налаштування пристрою змінюються, агент одразу передає оновлені дані [15].



Рисунок 1.7 – Логотип Nessus vulnerability scaner

Сканер Nessus був створений у 1998 році та згодом перетворився на комплексну платформу управління вразливостями від компанії Tenable. Гнучкість та точність цього рішення забезпечується модульною будовою, яка спирається на власну мову сценаріїв NASL. Вона була розроблена спеціально для безпечного створення алгоритмів перевірок [16]. Принцип роботи сканера базується на кількох компонентах. Модуль політик встановлює загальні правила та керує паролями, а планувальник розподіляє навантаження. Після підключення до пристрою система автоматично запускає лише ті перевірки, які підходять для знайденої операційної системи. Платформа Nessus розроблена так, щоб мінімально впливати на швидкість роботи мережі. Для цього існують суворі обмеження на кількість одночасних мережевих з'єднань. Також система вміє повторно використовувати вже відкриті сесії зв'язку, що значно знижує навантаження на сервери та допомагає уникнути блокувань [17].



Рисунок 1.8 – Логотип Greenbone OpenVAS

Платформа Greenbone виникла на базі відкритого проєкту OpenVAS та відрізняється високим рівнем модульності. Головним елементом є менеджер логіки, який керує базою даних та правами доступу користувачів. Окремі фонові програми відповідають за роботу веб-інтерфейсу, передачу команд та безпосереднє виконання перевірок на цільових комп'ютерах [16]. Важливим оновленням

останніх версій стала зміна алгоритму локальних перевірок. Замість почергового запуску тисяч окремих команд, сучасний сканер лише раз підключається до системи, збирає повний список встановлених програм і швидко порівнює його з єдиною базою відомих вразливостей. Це дозволило значно скоротити час перевірки та зменшити використання оперативної пам'яті. Загальна ефективність платформи залежить від обраної бази оновлень. Безкоштовна версія орієнтована переважно на масове програмне забезпечення, тоді як платна підписка містить перевірки для складного корпоративного обладнання [17].



Рисунок 1.9 – Логотип Qualys

Компанія Qualys однією з перших перевела процеси сканування у хмарне середовище. Структура цього рішення спирається на використання невеликих програмних агентів, які встановлюються на комп'ютерах і передають дані до захищеного хмарного сервера. Оскільки основний обсяг обчислень відбувається у хмарі, навантаження на процесори робочих станцій залишається мінімальним. Для обладнання, на яке неможливо встановити таку програму, передбачено використання віртуальних або фізичних сканерів всередині локальної мережі компанії [16]. Щоб уникнути перевантаження фахівців зайвою інформацією, розробники створили спеціальний алгоритм оцінки ризику TruRisk. Він вимірює рівень небезпеки за шкалою до тисячі балів, автоматично враховуючи наявність готових кодів для злому та активність хакерів. Важливою особливістю платформи є можливість не тільки виявляти ризики, але й одразу їх усувати. Вбудований модуль оновлень дозволяє системним адміністраторам встановлювати критично важливі виправлення операційної системи в автоматизованому режимі [17].



Рисунок 1.10 – Логотип Rapid7

Система Rapid7 розроблена з фокусом на тісну взаємодію з IT-відділами та оптимізацію мережевих перевірок. Архітектура рішення чітко розділяє головний сервер управління, який генерує звіти, та окремі модулі сканування, які розміщуються у різних сегментах мережі. Правильне розташування цих модулів є дуже важливим, адже це допомагає уникнути перевантаження захисного обладнання під час активного тестування. Впровадження цієї системи потребує ретельного планування обчислювальних потужностей, оскільки бази даних накопичують значні обсяги інформації. Для визначення пріоритетності загроз компанія використовує динамічний підхід до оцінки ризиків. Цей алгоритм тісно пов'язаний з аналітичними базами даних і автоматично підвищує рівень загрози для того обладнання, програмне забезпечення якого вже не підтримується розробником і не отримує нових оновлень безпеки [16].

Аналіз архітектурних особливостей сучасних платформ показує помітний розвиток підходів до управління вразливостями в інформаційних системах. Успішне впровадження системи безпеки вимагає точного розуміння побудови мережі та її взаємозв'язку з бізнес-процесами підприємства. На основі вивчення технічних характеристик можна виділити три ключові тенденції у сфері кібербезпеки:

1. Перехід до використання програмних агентів. Практика показала, що звичайне сканування мережі без авторизації виявляє лише незначну частину реальних загроз. Сучасний корпоративний стандарт вимагає встановлення спеціальних агентів на всіх робочих станціях. Це вирішує проблему переносних пристроїв та забезпечує безперервний збір інформації без перевантаження мережі.

2. Ретельне планування інфраструктури. Розгортання корпоративної системи сканування потребує точного розрахунку апаратних ресурсів. Фахівці мають враховувати обсяги баз даних, затримки в передачі сигналів та потребу в локальному збереженні мережевого трафіку. Неправильне розміщення активних сканерів може призвести до системних помилок і уповільнення роботи всієї мережі.

3. Зміна алгоритмів оцінки ризиків. Стандартні базові показники втрачають свою ефективність при визначенні пріоритетів. Сучасні системи змінюють логіку

роботи команд безпеки, застосовуючи комплексні шкали оцінювання. Вони враховують реальне використання шкідливих кодів зловмисниками на даний момент. Це дає змогу зосередити зусилля фахівців виключно на тих загрозах, які становлять найвищу небезпеку.

Результати роботи апробовано шляхом публікації тез доповіді на XVI Міжнародній науково-технічній конференції «Інформаційно-комп'ютерні технології – 2026» (м. Житомир, 2–3 квітня 2026 р.).

1.5. Порівняльний аналіз систем сканування вразливостей

Проведення об'єктивного порівняльного аналізу систем сканування вразливостей вимагає застосування стандартизованої, багатовимірної системи оцінювання, яка враховує як суто технічні характеристики платформ, так і операційні, фінансові та організаційні фактори, що визначають ефективність їх практичного впровадження. У рамках даного розділу аналізуються чотири провідні рішення ринку: Tenable Nessus (у складі екосистеми Tenable Vulnerability Management), Greenbone OpenVAS (Greenbone Community/Enterprise Edition), Qualys VMDR та Rapid7 InsightVM (Nexpose).

Для забезпечення репрезентативності та об'єктивності порівняння застосовувалися наступні джерела даних:

1. Незалежний бенчмарк Pentest-Tools.com (2024) - тестування семи провідних сканерів на 167 вразливих середовищах [18];
2. Технічна документація виробників та незалежні аналітичні огляди TuxCare (2024) [16];
3. Порівняльний аналіз SenseLearner (2025) щодо технічних характеристик OpenVAS, Nessus та Qualys [17];
4. Дані аналітичних агентств Gartner (Magic Quadrant for Exposure Assessment Platforms) та Mordor Intelligence (Vulnerability Management Market, 2024).

Таблиця 1.2

Порівняння баз даних вразливостей досліджуваних платформ

Параметр	Tenable Nessus	OpenVAS (GVM)	Qualys VMDR	Rapid7 InsightVM
Обсяг бази плагінів/NVT	>107 000 плагінів NASL	>90 000 NVT (Community) / >150 000 (Enterprise)	>145 000 сигнатур	>170 000 перевірок
Частота оновлень	Щоденно (< 24 год для нових CVE)	Щоденно (Community); Щогодинно (Enterprise)	В режимі реального часу (хмара)	Щоденно
Час реакції на нові CVE	< 24 год (зазвичай 12–16 год)	24–72 год (Community); < 24 год (Enterprise)	< 12 год (хмарна синхронізація)	24–48 год
Підтримка IoT/OT/SCADA	Часткова (через Tenable OT)	Обмежена (Community)	Часткова	Часткова
Підтримка контейнерів	Так (Tenable Container Security)	Обмежена	Так (Qualys Container Security)	Так (InsightVM)

Порівняння здійснюється за наступними ключовими критеріями: охоплення вразливостей та база плагінів, методологія виявлення та точність, архітектура розгортання, система пріоритезації ризиків, інтеграційний потенціал та автоматизація, а також модель ліцензування та сукупна вартість впровадження (TCO). Критичним показником ефективності будь-якої платформи управління вразливостями є обсяг та актуальність бази даних перевірок. Станом на 2024–2025 роки ситуація на ринку виглядає наступним чином (таблиця 1.2).

Tenable традиційно позиціонується як “золотий стандарт” галузі за обсягом та якістю плагінної бази. Компанія підтримує понад 107 000 активних перевірок, написаних мовою NASL, що охоплюють вразливості у операційних системах Windows, Linux, Unix, macOS, мережевому обладнанні Cisco, Juniper, сервісах хмарних провайдерів AWS, Azure та Google Cloud [16]. База Qualys є порівнянною за обсягом, однак ключовою перевагою хмарної архітектури є миттєве розповсюдження оновлень без необхідності ручного оновлення сканерів. OpenVAS у безкоштовному варіанті (Community Feed) суттєво відстає від комерційних конкурентів за охопленням специфічного корпоративного програмного забезпечення - зокрема, перевірки для SAP, Oracle Database, Cisco IOS (розширені) та VMware доступні виключно у комерційній редакції Enterprise Feed [17].

Незалежний бенчмарк мережевих сканерів вразливостей, проведений компанією Pentest-Tools.com у 2024 році, є найбільш репрезентативним актуальним дослідженням, що дозволяє об'єктивно порівняти реальну ефективність платформ [18]. Методологія тестування передбачала перевірку сканерів на 167 спеціально підготовлених вразливих середовищах, з яких 128 були доступні для виявлення дистанційно (без аутентифікації). Для кожної платформи вимірювалися два ключових показники:

1. Detection Availability (заявлена доступність) - відсоток CVE з тестового набору, для яких у базі сканера теоретично існують перевірки;
2. Detection Accuracy (фактична точність) - відсоток CVE, фактично виявлених під час реального сканування без аутентифікації.

Результати бенчмарку наведені у таблиці 1.3.

Таблиця 1.3

Результати незалежного бенчмарку Pentest-Tools.com (2024): Detection Availability vs. Detection Accuracy

Платформа	Detection Availability (%)	Detection Accuracy (%)	Розрив між заявленим та фактичним (%)	Тип ліцензії
Nessus Professional	55,09	18,56	−36,53	Комерційна
Qualys	~45	~35	-10	Комерційна (SaaS)
Nuclei (FOSS)	~40	~30	-10	Безкоштовна
OpenVAS (GVM Community)	~30	~22	-8	Безкоштовна
Rapid7 Nexpose	н/д*	н/д*	-	Комерційна
Pentest-Tools.com Scanner	Висока	Висока (консистентна)	~0	Комерційна (хмарна)

**Примітка: У методології бенчмарку відзначається складність диференціації між локальними та дистанційними перевірками у базі Nexpose, що унеможливлює пряме порівняння за цим показником при тестуванні виключно в режимі black-box.*

Наведені дані потребують ретельного контекстуального трактування. Значний розрив між заявленою доступністю та фактичною точністю Nessus (36,53 процентних пункти) відображає принципову архітектурну відмінність у підході до формування звітів. Tenable свідомо налаштовує Nessus на стратегію “мовчання при невпевненості” (conservative reporting): сканер не генерує сповіщення, якщо не може з достатньою мірою достовірності підтвердити наявність вразливості через приховані банери версій або нетипову поведінку сервісу при неавтентифікованому скануванні [18]. Такий підхід мінімізує кількість хибнопозитивних результатів (false positives) ціною зниження повноти виявлення (recall) при зовнішньому тестуванні. Qualys та Nuclei демонструють більш збалансований підхід, тоді як OpenVAS показує найменший розрив між заявленою та фактичною точністю, що свідчить про більш консервативну формалізацію бази перевірок.

Аналогічне порівняння ефективності сканерів Nessus, OpenVAS та Nmap Scripting Engine у контексті мереж малих і середніх підприємств було проведено Chalvatzis та ін. Автори підтвердили, що OpenVAS є потужною безкоштовною альтернативою комерційним рішенням, хоча й потребує більш глибокої технічної компетенції оператора [33].

Критично важливо підкреслити, що усі описані показники відносяться виключно до неавтентифікованого (black-box) режиму сканування. При переході до автентифікованих перевірок ситуація кардинально змінюється - Nessus, за даними самого вендора, демонструє точність на рівні “Шести сигм” (менше 0,32 дефекти на мільйон перевірок), виявляючи в середньому 307 вразливостей на вузол (проти 18 при неавтентифікованому скануванні) [16].

Архітектурний підхід до розгортання є одним із найбільш значущих факторів при виборі платформи, оскільки він визначає масштабованість рішення, вимоги до інфраструктури та операційне навантаження на IT-персонал (таблиця 1.4).

Таблиця 1.4

Порівняння архітектур розгортання

Параметр	Tenable Nessus / Tenable VM	OpenVAS (GVM)	Qualys VMDR	Rapid7 InsightVM
Модель розгортання	On-premise / Hybrid / SaaS	Self-hosted (on-premise)	Cloud-native SaaS	Hybrid (Cloud + On-prem)
Резидентні агенти	Так (Tenable Agent)	Ні	Так (Qualys Cloud Agent)	Так (Insight Agent)
Пасивне сканування	Так (Tenable PVS)	Ні	Ні (обмежено)	Так (PAS module)
Агентне сканування (без мережі)	Так	Ні	Так	Так
Підтримка air-gapped мереж	Так (Security Center)	Так (self-hosted)	Так (QGS)	Частково
Мультисенсорна архітектура	Так (Nessus Scanners + PVS + Agents)	Так (ospd, openvasd, agenti)	Так (Appliances + CA)	Так (Security Console + Engines)
Підтримка хмарних середовищ	AWS, Azure, GCP	Обмежено	AWS, Azure, GCP	AWS, Azure, GCP

Qualys VMDR є єдиною з розглянутих платформ, яка спочатку проектувалася як хмарна нативна архітектура (Cloud-First), що дає їй принципові переваги у сценаріях управління глобально розподіленими підприємствами. Tenable та Rapid7 пропонують гнучкі гібридні моделі. OpenVAS, у свою чергу, є виключно on-premise рішенням, що є суттєвим обмеженням для організацій, що мігрують до хмарних інфраструктур.

Важливим диференціатором є також підтримка пасивного сканування. Лише Tenable (через компонент Passive Vulnerability Scanner, PVS) та Rapid7 (через Passive Assessment Sensor) пропонують можливість безперервного моніторингу трафіку без активного зондування - функція критично важлива для фінансових установ та промислових середовищ, де активні сканування категорично заборонені через ризик дестабілізації критичних систем.

Таблиця 1.5

Порівняння інтеграційних можливостей

Параметр	Tenable Nessus / VM	OpenVAS (GVM)	Qualys VMDR	Rapid7 InsightVM
REST API	Так (Tenable.io API)	Так (GMP/OSP Protocol)	Так (Qualys API v2/v3)	Так (InsightVM API)
Інтеграція з SIEM	Splunk, QRadar, Sentinel	Обмежено (syslog)	Splunk, QRadar	Splunk, QRadar, Sentinel
Інтеграція з ITSM	Jira, ServiceNow	Ні (нативно)	ServiceNow, Jira	Jira, ServiceNow
Patch Management (нативний)	Ні (окремий модуль)	Ні	Так (Qualys Patch Mgmt)	Частково (через Insight)
CI/CD інтеграція	Обмежено	Ні	Так	Так (DevOps native)
SOAR інтеграція	Так (через Splunk SOAR)	Ні	Так	Так
Управління відповідністю	Так (CIS, NIST, PCI DSS)	Обмежено	Так (CIS, SOX, HIPAA)	Так (CIS, PCI DSS)

Найбільш комплексний інтеграційний стек у 2024–2025 роках демонструє Qualys VMDR. Нативний модуль патч-менеджменту дозволяє, виявивши вразливість, одразу ж засобами того самого Cloud Agent розгорнути відповідне виправлення або автоматично сформувати тікет у ServiceNow, скорочуючи середній час усунення на заявлені 60% порівняно із розрізненими рішеннями [17].

Rapid7 InsightVM традиційно позиціонується як найбільш DevOps-орієнтоване рішення, забезпечуючи нативну інтеграцію з CI/CD пайплайнами, що дозволяє впровадити перевірки вразливостей безпосередньо у процес розробки програмного забезпечення. OpenVAS, попри наявність GMP-протоколу та набору командних утиліт gvm-tools, потребує суттєвих зусиль для інтеграції в корпоративні екосистеми, оскільки не підтримує більшість “out-of-the-box” конекторів для популярних SIEM, ITSM та SOAR платформ.

Фінансова модель є одним із визначальних факторів при виборі платформи для малих і середніх підприємств. Порівняння актуальних цінових категорій наведено у таблиці 1.6.

Таблиця 1.6

Порівняльний аналіз моделей ліцензування та ціноутворення (2024)

Параметр	Tenable Nessus	OpenVAS (GVM)	Qualys VMDR	Rapid7 InsightVM
Базова ліцензія	Комерційна (підписка)	GNU GPL v2 (відкрита)	Комерційна SaaS	Комерційна (підписка)
Безкоштовна версія	Nessus Essentials (≤16 IP)	Community Edition (повна функціональність)	Community Edition (обмежена)	Ні
Ціна стартового рівня	~4790/рік (*NessusPro*) 6 790/рік (Nessus Expert)	$0 (Community) ~€2 524/рік (Enterprise)	Договірна (~$199–250/актив/рік)	Договірна (~$19–23/актив/рік)
Модель тарифікації	Фіксована (за кількістю сканерів)	Безкоштовно або за обладнання	За кількістю активів	За кількістю активів
Підтримка	24/7 (для Pro/Expert)	Спільнота (Community); SLA (Enterprise)	24/7 (включена в підписку)	24/7 (включена)
Сертифікати відповідності	SOC 2, FedRAMP (Tenable.io)	Ні	SOC 2, ISO 27001, FedRAMP	SOC 2

Важливо враховувати концепцію сукупної вартості впровадження (Total Cost of Ownership, TCO). Попри формальну відсутність ліцензійних виплат, впровадження OpenVAS Community Edition у корпоративному середовищі несе приховані операційні витрати: необхідність виділення кваліфікованого персоналу Linux/security-адміністраторів для обслуговування системи, ручна робота з управління конфігураціями та регулярні оновлення бази NVT, а також потреба у самостійній розробці інтеграцій з існуючою IT-екосистемою. За різними оцінками, реальні витрати на підтримку OpenVAS у корпоративному середовищі можуть перевищувати вартість комерційної ліцензії Nessus Professional у разі, якщо організація не має досвідченої внутрішньої команди безпеки.

Відповідно до аналітичних даних ринку управління вразливостями за 2024 рік, Tenable, Qualys та Rapid7 стабільно займають лідируючі позиції у сегменті великих підприємств, формуючи понад 70% доходів ринку у своїй категорії [16]. Ринок управління вразливостями демонструє стійку тенденцію до трансформації у напрямку ширшої концепції “управління поверхнею атаки” (Exposure

Management), при цьому спостерігається закономірний перехід від on-premise до SaaS та гібридних моделей розгортання.

OpenVAS/GVM продовжує займати вагоме місце в академічному та дослідницькому секторі, а також у середньому бізнесі з обмеженими бюджетами на кібербезпеку. Водночас Greenbone активно розвиває комерційну лінійку Enterprise Appliances як повноцінну альтернативу для ринку, конкуруючи за ціновою перевагою з початковими рівнями Nessus та Rapid7.

1.6. Обґрунтування вибору OpenVAS

За результатами порівняльного аналізу, проведеного у розділі 1.5, встановлено, що жодна з розглянутих комерційних платформ - Tenable Nessus, Qualys VMDR та Rapid7 InsightVM – не відповідає повною мірою специфічним вимогам академічного дослідження в галузі кібербезпеки. Системна аргументація на користь Greenbone OpenVAS формується на основі п'яти взаємодоповнюючих критеріїв: відповідності принципам відкритої науки, технічної прозорості й розширюваності, правової та фінансової доступності, зрілості й активної підтримки спільноти, а також функціональної достатності для вирішення поставлених завдань.

Першим і методологічно найважливішим аргументом на користь OpenVAS є його повна відповідність принципу відтворюваності результатів - фундаментальної вимоги до будь-якого академічного дослідження в галузі інформаційних технологій. Результати сканування вразливостей безпосередньо залежать від конкретної версії бази даних плагінів, алгоритмів аналізу мережевих відповідей та внутрішньої логіки класифікації знахідок. Комерційні платформи - Nessus, Qualys та Rapid7 InsightVM - реалізовані як “чорні скриньки”: їх плагіни поширюються у скомпільованому вигляді або виконуються виключно на сервері вендора, тоді як внутрішня логіка алгоритмів VPR, TruRisk та Real Risk Score є захищеною комерційною таємницею. Це принципово унеможливлює верифікацію алгоритму оцінки ризиків на рівні вихідного коду та цілеспрямовану модифікацію перевірок для специфічних умов тестового стенду. OpenVAS/GVM, навпаки, є повністю

відкритою системою: усі компоненти стеку - openvas-scanner на мові C, gvmd на мові C, gsad на Python та React, ospd-openvas на Python, openvasd на Rust, а також gvm-tools на Python - розповсюджуються під ліцензіями GNU GPL v2/v3 та GNU AGPL v3, а вихідний код цілком відкрито розміщено у публічному репозиторії на GitHub. Кожен NVT-скрипт написаний мовою NASL і може бути прочитаний, модифікований та детально задокументований дослідником.

Другим суттєвим аргументом є технічна прозорість і розширюваність платформи. Центральним інструментом дослідника в OpenVAS є мова NASL - спеціалізована скриптова мова, синтаксично подібна до C та Perl, розроблена виключно для написання безпечних і портативних перевірок мережевих вразливостей. Дослідник може відкрити будь-який з понад 90 000 наявних NVT-скриптів і точно зрозуміти, яким чином система встановлює наявність конкретної вразливості - аналізуючи банер відповіді, порівнюючи версію встановленого пакунку або перевіряючи конфігураційний файл. Офіційна бібліотека python-gvm дозволяє у рамках єдиного Python-скрипту програмно запускати серії сканувань, отримувати результати, реалізовувати власну логіку бробки результатів сканування, а також програмно отримувати звіти у різних форматах. Модульна мікросервісна архітектура GVM, де компонент openvas-scanner взаємодіє з ospd-openvas через UNIX-сокет, ospd-openvas - з gvmd через протокол OSP, а gvmd - з веб-інтерфейсом gsad через GMP/TLS, забезпечує принципову можливість підключення власної зовнішньої системи або аналітичного модуля безпосередньо до gvmd.

Третім визначальним критерієм є правова та фінансова доступність. Tenable Nessus Professional розповсюджується за EULA-ліцензією, яка категорично забороняє тестування мереж, якими не володіє ліцензіат; безкоштовна версія Nessus Essentials обмежена 16 IP-адресами й позбавлена повноцінних функцій звітності. Qualys VMDR є суто SaaS-рішенням без можливості локального розгортання зі строго обмеженим пробним доступом. Rapid7 InsightVM не має безкоштовної версії для академічного використання, а trial-ліцензія надається лише на 30 днів. Мінімальна річна вартість Nessus Professional становить близько 4 790

доларів США, тоді як Qualys VMDR тарифікується від 199 доларів на актив на рік. OpenVAS/GVM розповсюджується за ліцензіями GNU General Public License v2 та v3 - класичними “копілефт”-ліцензіями вільного програмного забезпечення, відповідно до яких програма може бути вільно встановлена, запущена, вивчена, модифікована та розповсюджена без будь-яких фінансових зобов'язань та часових обмежень. Повне розгортання GVM Community Edition на навчальному стенді є абсолютно безкоштовним і вимагає лише наявності відповідних апаратних або хмарних ресурсів із рекомендованим мінімумом у 4 ядра CPU, 8 ГБ RAM та 60 ГБ дискового простору.

Четвертим аргументом слугує технологічна зрілість платформи та наявність активної підтримки. Greenbone OpenVAS є одним із найстаріших і найстабільніших проектів у сфері відкритого програмного забезпечення для кібербезпеки. Початком його історії став 1998 рік, коли Рено Деразоном було розроблено відкритий сканер Nessus, а після переходу Nessus на пропрієтарну ліцензію у 2005 році спільнота вільного програмного забезпечення утворила форк OpenVAS. З 2008 року підтримку й розвиток проекту взяла на себе німецька компанія Greenbone Networks. У 2019 році система отримала нову назву Greenbone Vulnerability Management з чіткою специфікацією всіх компонентів, а у 2022 році впровадження компонентів Notus Scanner та openvasd на мові Rust стало революційною зміною архітектури, що кардинально підвищила продуктивність локальних перевірок. Актуальна версія GVM 24.10 містить розширену підтримку CVSSv4 та вдосконалені механізми Security Intelligence Export. Нині проект підтримується командою Greenbone Networks, що налічує понад 60 штатних фахівців в Оснабрюку (Німеччина), та активною глобальною спільнотою. База Community NVT оновлюється щоденно і містить понад 90 000 перевірок, що охоплюють понад 70 000 унікальних CVE-ідентифікаторів. Важливим підтвердженням академічної зрілості платформи є її широке використання у рецензованих публікаціях журналів IEEE та ACM, а також у дисертаційних роботах провідних університетів Європи та Північної Америки.

П'ятий критерій - функціональна достатність - безпосередньо пов'язаний із конкретними завданнями практичної частини роботи. Попри констатовані у розділі

1.5 обмеження OpenVAS Community Edition, зокрема відсутність власних алгоритмів машинного навчання для пріоритезації ризиків та дещо вужчу базу NVT для специфічного корпоративного програмного забезпечення, платформа є повністю функціонально достатньою для вирішення завдань дослідження. Автоматизоване та автентифіковане сканування мережевих вузлів, ідентифікація й класифікація вразливостей за стандартами CVE/CVSSv3/CPE, генерація структурованих звітів у форматах XML, PDF та TXT, а також гнучке налаштування параметрів сканування через вебінтерфейс GSA – усі ці функції підтримуються у повному обсязі і є достатніми для побудови комплексної методики триетапного аудиту безпеки IT-інфраструктури. Базова відсутність алгоритму пріоритезації типу VPR або TruRisk компенсується експертною інтерпретацією результатів сканування на основі метрик CVSS v3 та аналізу контексту виявлених вразливостей.

Для наочного підсумування порівняльних аргументів наведена зважена матриця вибору, де кожному критерію присвоєно ваговий коефіцієнт відповідно до його значущості для академічного дослідження, підтверджує значну перевагу OpenVAS із результатом 9,30 балів над комерційними альтернативами: Nessus - 4,14 балів, Qualys та Rapid7 - по 3,40 балів. Визначальним є те, що за критеріями відкритості вихідного коду та можливості розробки власних NVT - ключовими з точки зору академічної методології - комерційні платформи отримують нульову оцінку, оскільки їх закрита архітектура є принципово несумісною з фундаментальними вимогами академічної відтворюваності та науково-дослідницького розширення.

На підставі проведеного п'ятикритеріального аналізу встановлено, що Greenbone OpenVAS у редакції Community Edition є найбільш обґрунтованим та технічно відповідним вибором для практичної реалізації завдань даного дипломного дослідження. Відкритість вихідного коду є науковою необхідністю, а не другорядним параметром, оскільки лише за цієї умови забезпечується можливість верифікації кожної перевірки вразливостей та відтворення всього дослідницького процесу незалежним спостерігачем. Ліцензія GNU GPL усуває

будь-які юридичні ризики та фінансові перешкоди для дослідження і публікації результатів. Таким чином, у практичній частині даної дипломної роботи OpenVAS використовується як відкрита дослідницька платформа, на базі якої розробляється методика комплексного триетапного аудиту безпеки, що поєднує зовнішнє неавтентифіковане, внутрішнє автентифіковане та повне мережеве сканування. Такий підхід відповідає принципам відкритої науки, забезпечує повну відтворюваність результатів та створює методологічну основу для подальших досліджень у галузі автоматизованого управління вразливостями.

Висновки до першого розділу:

У першому розділі проведено комплексний аналіз теоретичних засад та практичного інструментарію виявлення вразливостей IT-інфраструктури. Досліджено еволюцію поняття “вразливість” від суто технічних програмних помилок до багатовимірного ризик-орієнтованого концепту, закріпленого у міжнародних стандартах ISO/IEC 27000, NIST SP 800-30 та національному НД ТЗІ 1.1-003-99. Встановлено, що перехід на систему оцінювання CVSS v4.0 з її чотирма групами метрик дозволяє знизити кількість хибно пріоритизованих вразливостей на 65–76% порівняно з попередньою версією, що є критично важливим для автоматизованих систем сканування. Аналіз сучасного ландшафту загроз на основі звітів ENISA Threat Landscape 2025 та CERT-UA за 2025 рік підтвердив, що експлуатація вразливостей залишається другим вектором початкового проникнення (21,3% інцидентів), а в українських реаліях кількість кіберінцидентів зросла на 37,4% і досягла 5927 випадків, що обґрунтовує актуальність теми дослідження.

Проведено системний огляд методів виявлення вразливостей (пасивного аудиту, активного сканування та тестування на проникнення за PTES) та обґрунтовано їх комбінування за принципом аналітичної лійки. Аналіз архітектури систем Nessus, OpenVAS, Qualys та Rapid7 виявив ключові тенденції: перехід до агентного сканування, ретельне планування інфраструктури та впровадження контекстної пріоритезації ризиків замість сортування за базовим балом CVSS.

Порівняльний аналіз платформ за критеріями охоплення, точності, архітектури, інтеграції та ліцензування, підкріплений даними бенчмарку Pentest-Tools.com (2024), завершився вибором Greenbone OpenVAS Community Edition як основного інструменту практичної частини роботи. Вибір зумовлений відкритою архітектурою платформи, підтримкою протоколу GMP для автоматизації сканування, можливістю локального розгортання та вільною ліцензією GNU GPL.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІТ-ІНФРАСТРУКТУРИ

2.1. Архітектура підсистеми виявлення вразливостей

За результатами аналізу, проведеного у першому розділі, обґрунтовано вибір платформи Greenbone OpenVAS як базового інструменту для побудови підсистеми виявлення вразливостей ІТ-інфраструктури. Перехід до проєктування потребує формалізації архітектурних рішень, які визначатимуть структуру, поведінку та взаємодію всіх програмних компонентів підсистеми.

Підсистема виявлення вразливостей проєктується як розподілений програмний комплекс, побудований за принципом багаторівневої архітектури. Такий підхід, широко обґрунтований у літературі з проєктування інформаційних систем, забезпечує розділення відповідальностей між компонентами, спрощує масштабування та дозволяє замінювати або модифікувати окремі модулі без впливу на решту системи. Архітектура підсистеми організована у три логічних ешелони: рівень збору даних, рівень управління та зберігання, а також рівень подання та інтеграції (Рис. 2.1).

Рівень збору даних є операційним ядром підсистеми, що безпосередньо взаємодіє з досліджуваною ІТ-інфраструктурою. Центральним елементом цього рівня виступає компонент openvas-scanner – високопродуктивний мережевий сканер, реалізований мовою програмування C. Його основним завданням є виконання тестів мережевих вразливостей, кожен з яких представляє собою окремий скрипт, написаний спеціалізованою мовою NASL. Під час сканування openvas-scanner послідовно виконує NVT-скрипти проти цільових вузлів: здійснює виявлення портів, ідентифікацію сервісів, визначення версій програмного забезпечення та безпосередню перевірку наявності відомих вразливостей шляхом порівняння отриманих параметрів з базою знань CVE [19].

Важливим архітектурним рішенням, впровадженим у версії GVM 22.x, стала поява компонента Notus Scanner, який кардинально оптимізував процедуру локальних перевірок безпеки. Традиційний підхід передбачав запуск окремого

NASL-скрипту для кожної перевірки оновлень – за наявності десятків тисяч таких перевірок це створювало значне обчислювальне навантаження. Notus Scanner вирішує цю проблему принципово інакше: він одноразово збирає список встановлених пакунків на цільовому хості, а потім виконує офлайн-порівняння з JSON-базою рекомендацій безпеки без повторних мережевих звернень. У найновішій версії архітектури GVM 24.x функціональність Notus інтегрована безпосередньо в компонент openvasd – нову службу сканування, реалізовану мовою програмування Rust. Перехід з Python-обгортки ospd-openvas на нативну Rust-реалізацію openvasd є стратегічною модернізацією, що забезпечує суттєве підвищення продуктивності та зменшення кількості компонентів у стеку [19].

Для забезпечення обміну проміжними результатами між NVT-скриптами під час активного сканування використовується сховище Redis – високошвидкісна база даних у оперативній пам'яті. Redis виконує функцію тимчасової бази знань, де кожному цільовому хосту виділяється окрема логічна база даних. NVT-скрипти записують виявлену інформацію (відкриті порти, банери сервісів, версії програмного забезпечення) до KB, а наступні скрипти зчитують ці дані для прийняття рішень про подальші перевірки. Взаємодія openvas-scanner з Redis здійснюється виключно через UNIX-сокет, що забезпечує мінімальну латентність та виключає можливість зовнішнього перехоплення даних [20].

Рівень управління та зберігання представлений центральним компонентом gvmd – демоном управління, реалізованим мовою C. Саме gvmd виконує роль оркестратора всієї підсистеми: він відповідає за створення та планування завдань сканування, управління обліковими записами та правами доступу, обробку результатів, генерацію звітів та координацію роботи сканерів. Для зберігання усіх персистентних даних – результатів сканувань, конфігурацій завдань, метаданих NVT-скриптів, інформації SCAP/CERT та облікових записів користувачів – gvmd використовує реляційну базу даних PostgreSQL [20].

Взаємодія gvmd зі сканером здійснюється через протокол OSP – XML-базований протокол, розроблений Greenbone для стандартизації комунікації між менеджером та різними типами сканерів. У поточній архітектурі проміжним

компонентом виступає ospd-openvas – Python-сервер, який приймає OSP-команди від gvmd через UNIX-сокет і транслює їх у виклики openvas-scanner. У перспективній архітектурі GVM 24.x протокол OSP замінюється на RESTful HTTP API, реалізований безпосередньо в openvasd, що спрощує інтеграцію та зменшує кількість проміжних ланок [21].

Для зовнішнього управління підсистемою gvmd надає повнофункціональний програмний інтерфейс – протокол GMP. GMP є XML-базованим протоколом типу "запит-відповідь", що забезпечує повний набір операцій управління: створення та конфігурування цілей сканування, визначення політик перевірок, запуск та зупинка завдань, отримання звітів у різних форматах (XML, PDF, HTML, CSV), налаштування розкладів та сповіщень, а також адміністрування користувачів. При з'єднанні через мережу GMP використовує шифрування TLS з інфраструктурою відкритих ключів, що забезпечує конфіденційність та автентифікацію комунікації. Порт за замовчуванням для GMP-з'єднань – TCP/9390 [21].

Рівень подання та інтеграції забезпечує взаємодію підсистеми з кінцевими користувачами та зовнішніми системами. Основним інструментом візуалізації є Greenbone Security Assistant – сучасний веб-інтерфейс, реалізований як односторінковий додаток (SPA) на базі фреймворку React. GSA надає інтуїтивно зрозумілий графічний інтерфейс для управління усіма аспектами підсистеми: від налаштування параметрів сканування до аналізу результатів з можливістю фільтрації, сортування та експорту звітів. Серверна частина веб-інтерфейсу – демон gsad – виконує роль HTTP-проксі, який приймає запити від браузера користувача та транслює їх у GMP-команди до gvmd через UNIX-сокет [22].

Для програмної інтеграції та автоматизації у підсистемі передбачено два ключових інструменти. Бібліотека python-gvm є офіційною Python-бібліотекою, що абстрагує XML-комунікацію GMP-протоколу та підтримує три типи з'єднань: через UNIX-сокет, TLS та SSH. Утиліта gvm-tools надає набір командних інструментів – gvm-cli для відправки XML-команд, gvm-script для запуску Python-скриптів та gvm-pyshell для інтерактивної роботи. Наявність таких інструментів робить обрану

платформу максимально гнучкою для проведення комплексного триетапного аудиту безпеки IT-інфраструктури та аналізу виявлених вразливостей [22].

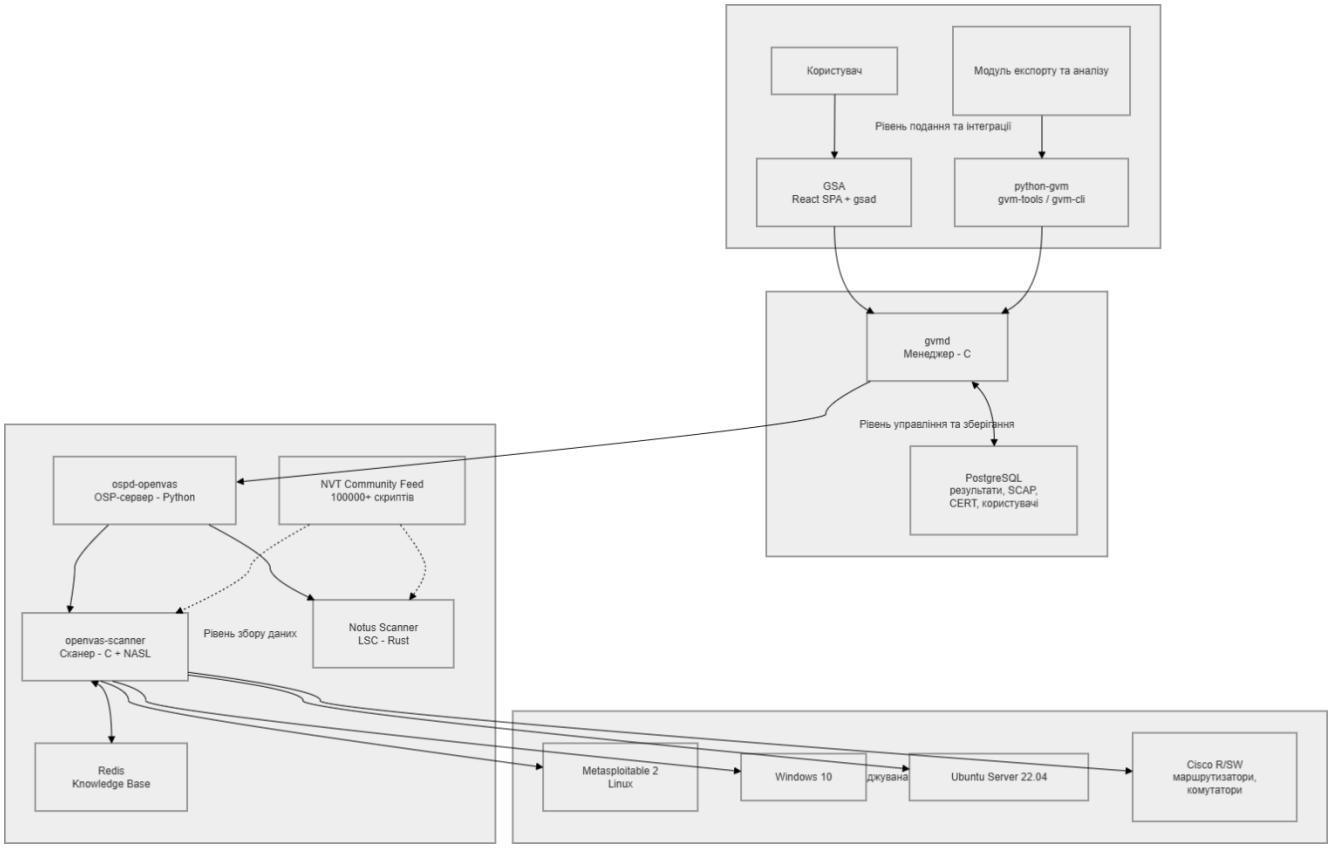


Рисунок 2.1 – Триешелонна архітектура підсистеми виявлення вразливостей на базі GVM

Потік даних у підсистемі під час типового циклу сканування може бути описаний як послідовність семи етапів. Користувач або автоматизований скрипт формує запит на сканування через веб-інтерфейс GSA або GMP API. Запит потрапляє до gvmd, який валідує параметри, створює завдання у PostgreSQL та передає команду запуску сканування до ospd-openvas через OSP-протокол. Компонент ospd-openvas ініціює процес openvas-scanner, передаючи йому перелік цілей та вибрані NVT-скрипти. Сканер починає взаємодію з цільовими вузлами, записуючи проміжні результати до Redis KB. Одночасно Notus Scanner виконує офлайн-перевірку пакунків для автентифікованих сканувань. Після завершення сканування результати повертаються через ospd-openvas до gvmd, який здійснює їх обробку – присвоює рівні критичності за CVSS, пов'язує знахідки з ідентифікаторами CVE та CPE, зберігає структуровані дані у PostgreSQL. Кінцевий

звіт стає доступним користувачеві через GSA або може бути програмно отриманий через GMP API для подальшого аналізу.

Обрана триешелонна архітектура забезпечує ряд принципових переваг для дослідження. Наявність відкритого GMP API створює надійне підґрунтя для автоматизації процесів аудиту та масштабування системи без необхідності модифікації її ядра.

2.2. Функціональна структура системи

У підрозділі 2.1 визначено триешелонну архітектуру підсистеми виявлення вразливостей та окреслено ролі основних компонентів. Проте архітектурне представлення описує лише структурні зв'язки між програмними елементами і не розкриває їхнього внутрішнього функціонального наповнення. Для забезпечення повноти проєктування необхідно деталізувати кожен компонент як функціональний модуль із чітко визначеними задачами, вхідними та вихідними даними. Функціональна декомпозиція підсистеми дозволяє виділити п'ять логічних модулів, кожен з яких відповідає за окремий аспект процесу виявлення та управління вразливостями (Рис. 2.2).

Модуль сканування є виконавчим елементом підсистеми, який безпосередньо реалізує технічну процедуру виявлення вразливостей на цільових вузлах мережі. Функціонально він об'єднує три компоненти, кожен з яких спеціалізується на певному типі перевірок. Компонент openvas-scanner виконує активне мережеве сканування – послідовно запускає NVT-скрипти, що здійснюють виявлення хостів, сканування портів методами TCP SYN, TCP Connect та UDP, ідентифікацію сервісів за банерами відповідей, визначення версій програмного забезпечення та безпосередню перевірку наявності відомих вразливостей. Кожен NVT-скрипт є автономною одиницею перевірки, яка отримує вхідні дані з бази знань Redis, виконує мережеву взаємодію з ціллю та повертає результат у структурованому вигляді: ідентифікатор вразливості, рівень критичності, опис та рекомендації щодо усунення [23].

Компонент Notus Scanner відповідає за локальні перевірки безпеки, які потребують автентифікованого доступу до цільового хоста. На відміну від класичного підходу, де для кожного оновлення запускається окремий NVT-скрипт, Notus працює за принципом пакетного аналізу: він одноразово збирає повний перелік встановлених програмних пакунків через SSH або WMI, після чого виконує офлайн-порівняння з локальною базою рекомендацій безпеки у форматі JSON. Такий підхід дозволяє перевірити тисячі потенційних вразливостей за час, порівнянний з виконанням одного мережевого запиту. Для операційних систем сімейства Linux Notus аналізує пакунки форматів DEB та RPM, а для Windows – перевіряє встановлені оновлення через системний реєстр [23].

Компонент ospd-openvas виконує функцію уніфікованого інтерфейсу між рівнем управління та виконавчими компонентами сканування. Він приймає команди від gvmd у форматі протоколу OSP, розподіляє завдання між openvas-scanner та Notus Scanner, агрегує проміжні результати та повертає консолідований потік даних назад до менеджера. Для забезпечення паралельного виконання кількох сканувань ospd-openvas підтримує механізм черг завдань та контролює споживання системних ресурсів, обмежуючи кількість одночасних потоків сканування відповідно до параметрів конфігурації [24].

Модуль управління реалізований компонентом gvmd і є центральним координаційним вузлом підсистеми. Функціонально цей модуль охоплює шість взаємопов'язаних підсистем. Підсистема управління завданнями відповідає за повний життєвий цикл сканування: від створення завдання з визначенням цілей, політики перевірок та облікових даних – до запуску, моніторингу прогресу та збереження результатів. Підсистема планування забезпечує автоматизоване виконання сканувань за розкладом із підтримкою рекурентних інтервалів у форматі iCalendar, що дозволяє організувати регулярний моніторинг інфраструктури без участі оператора [24].

Підсистема політик визначає набори NVT-скриптів, які застосовуватимуться під час конкретного сканування. GVM надає кілька стандартних політик різного рівня глибини: “Discovery” обмежується виявленням хостів і портів, “Host

Discovery” визначає активні вузли, “Full and Fast” виконує комплексне сканування з оптимізацією швидкості, а “Full and Very Deep” здійснює максимально ретельну перевірку, включаючи потенційно небезпечні тести. Адміністратор може створювати власні політики, вибираючи конкретні сімейства NVT або окремі скрипти для специфічних задач [24].

Підсистема управління доступом реалізує рольову модель авторизації з підтримкою кількох рівнів привілеїв. Адміністратор має повний доступ до всіх функцій системи, оператор може створювати та запускати завдання, а спостерігач – лише переглядати звіти. Додатково реалізовано механізм груп та дозволів, що дозволяє обмежити видимість результатів сканування відповідно до організаційної структури. Підсистема сповіщень дозволяє налаштувати автоматичне реагування на завершення сканування або виявлення критичних вразливостей – через відправку електронних листів, HTTP-запитів до зовнішніх систем або виконання довільних команд [24].

Підсистема звітування здійснює формування підсумкових документів у кількох форматах: XML для програмної обробки, PDF та HTML для представлення керівництву, CSV для імпорту в аналітичні системи. Звіти містять структуровану інформацію про кожну виявлену вразливість: ідентифікатор CVE, оцінку CVSS, опис проблеми, вектор атаки та рекомендації щодо усунення. Підтримується механізм фільтрації результатів за рівнем критичності, хостом, сімейством NVT та іншими параметрами [25].

Модуль бази знань забезпечує підсистему актуальною інформацією про відомі вразливості та методи їх виявлення. Основним джерелом даних є Greenbone Community Feed – відкрита колекція, яка налічує понад сто тисяч NVT-скриптів мовою NASL. Скрипти організовані за сімействами відповідно до типу перевірки або цільової платформи: “Debian Local Security Checks”, “Windows: Microsoft Bulletins”, “Web application abuses”, “SNMP”, “General” та інші. Кожен NVT-скрипт містить метадані, що описують його призначення, пов'язані CVE та CPE, рівень критичності за CVSS та умови застосування [23].

Окрім NVT-скриптів, база знань включає дані SCAP – стандартизовані визначення CVE та словники CPE, які використовуються для кореляції результатів сканування з глобальними базами вразливостей. Також завантажуються рекомендації CERT-Bund та DFN-CERT, що надають контекстну інформацію про загрози та доступні виправлення. Оновлення всіх компонентів бази знань здійснюється утилітою greenbone-feed-sync, яка використовує протокол rsync для синхронізації з серверами Greenbone. Важливо зазначити, що Community Feed має затримку оновлень приблизно 14 днів порівняно з комерційним Enterprise Feed, що слід враховувати при плануванні критичних сканувань [25].

Модуль зберігання реалізує двокомпонентну стратегію збереження даних, оптимізовану для різних типів навантаження. PostgreSQL виступає основним персистентним сховищем, де зберігаються результати всіх сканувань, конфігурації завдань, політики, дані користувачів, метадані NVT-скриптів та інформація SCAP/CERT. Структура бази даних забезпечує ефективне виконання аналітичних запитів: пошук вразливостей за CVE-ідентифікатором, агрегацію статистики за рівнями критичності, порівняння результатів послідовних сканувань для виявлення динаміки стану безпеки [20].

Redis виконує принципово іншу функцію – забезпечує тимчасове високошвидкісне сховище для бази знань під час активного сканування. Формула розрахунку необхідної кількості логічних баз даних Redis визначається виразом: databases = 2 + n × m, де n – кількість одночасних сканувань, m – кількість хостів у кожному скануванні, а дві додаткових бази зарезервовані для основних даних та кешу NVT. Після завершення сканування тимчасові бази знань у Redis видаляються, а релевантні результати мігрують до PostgreSQL через gvmd. Така стратегія розділення забезпечує, з одного боку, максимальну швидкість обміну даними між NVT-скриптами під час сканування і, з іншого – надійне довготривале зберігання результатів з підтримкою складних запитів [20].

Модуль подання та інтеграції надає інтерфейси для взаємодії як з людиною-оператором, так і з зовнішніми програмними системами. Веб-інтерфейс GSA є основним інструментом повсякденної роботи оператора безпеки. Він надає

візуальну панель моніторингу з графіками розподілу вразливостей за рівнями критичності, інтерактивні таблиці результатів з підтримкою сортування та фільтрації, візуальний конструктор завдань та цілей сканування, а також засоби управління користувачами та правами доступу. GSA побудований як односторінковий додаток на базі фреймворку React, що забезпечує динамічне оновлення інтерфейсу без перезавантаження сторінки [22].

Для програмної інтеграції модуль надає доступ через протокол GMP. Бібліотека python-gvm абстрагує XML-комунікацію протоколу та надає об'єктно-орієнтований інтерфейс для створення скриптів автоматизації. Типовий сценарій використання включає програмне створення цілей та завдань, запуск сканування, очікування завершення та автоматичне отримання звіту для подальшої обробки. Набір утиліт gvm-tools доповнює бібліотеку командними інструментами для інтерактивної роботи: gvm-cli дозволяє надсилати довільні GMP-команди безпосередньо з терміналу, gvm-script виконує Python-скрипти в контексті автентифікованої GMP-сесії, а gvm-pyshell надає інтерактивну оболонку для дослідницьких задач [26].

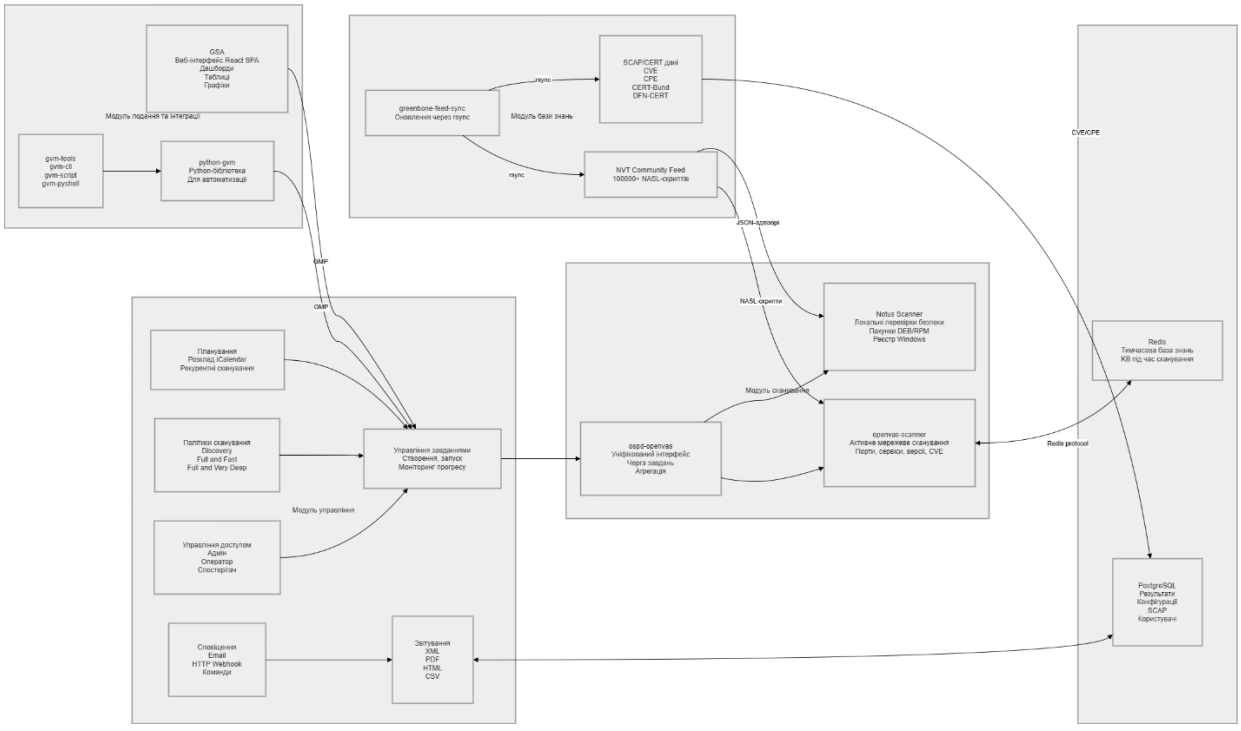


Рисунок 2.2 – Функціональна структура підсистеми виявлення вразливостей

Описана функціональна структура визначає п'ять чітко розмежованих модулів, кожен з яких може бути налаштований та масштабований незалежно від

інших. Модуль сканування забезпечує технічну реалізацію перевірок, модуль управління координує процес та формує звіти, модуль бази знань підтримує актуальність інформації про загрози, модуль зберігання гарантує надійність та швидкість роботи з даними, а модуль подання забезпечує доступність результатів для всіх категорій користувачів та інтеграцію з зовнішніми системами.

2.3. Модель взаємодії компонентів системи

Визначена у попередніх підрозділах функціональна структура підсистеми вимагає деталізації інформаційних потоків між її модулями. Згідно з офіційною архітектурною документацією GVM, взаємодія організована навколо центрального вузла – демона управління gvmd [19]. Цей компонент виконує роль координатора, який консолідує базове сканування у повноцінне рішення для управління вразливостями. Загальну модель взаємодії можна умовно розділити на три вектори: внутрішня комунікація компонентів, взаємодія з цільовим середовищем та зовнішня інтеграція.

Взаємодія користувача з підсистемою ініціюється через рівень подання. Головною точкою доступу є GSA – веб-інтерфейс, який через службу gsad взаємодіє з gvmd. Комунікація на цьому рівні здійснюється виключно за допомогою протоколу GMP [19]. Відповідно до офіційної специфікації API, GMP є XML-базованим протоколом, який забезпечує передачу всього спектру команд управління: від створення завдань і цілей до запуску перевірок та отримання готових звітів [21].

Після отримання команди на запуск сканування через GMP, компонент gvmd ініціює взаємодію з виконавчим рівнем. Для цього використовується інший комунікаційний стандарт – OSP [19]. З боку сканера ці запити приймає служба ospd-openvas. Вона функціонує як інтерфейс між менеджером та безпосереднім ядром перевірок: через неї синхронізуються дані тестів, передаються сигнали управління станами сканування та повертаються результати перевірок назад до gvmd. Послідовність цих викликів відображена на діаграмі взаємодії (Рис. 2.3).

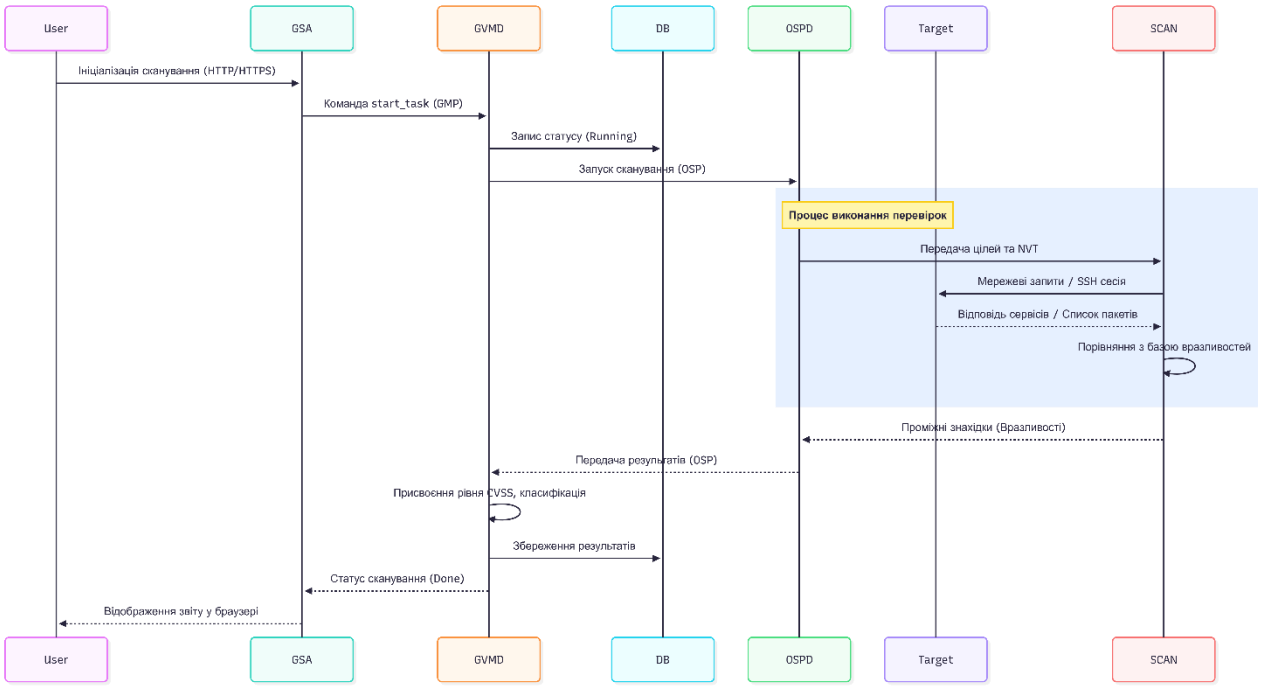


Рисунок 2.3 – Діаграма послідовності взаємодії компонентів під час виконання сканування

Усі консолідовані дані – конфігураційні налаштування, права користувачів, політики та результати сканувань – передаються демоном gvmd до реляційної бази даних PostgreSQL [19]. Така транзакційна модель гарантує, що менеджер є єдиним компонентом з прямим доступом до сховища, забезпечуючи ізоляцію бази від безпосередніх процесів сканування.

Процес комунікації сканера з досліджуваними вузлами реалізується у двох різних моделях. Традиційна активна модель передбачає, що для кожної перевірки індивідуально завантажується та виконується окремий мережевий скрипт, який ініціює з'єднання з портом або сервісом цілі для підтвердження вразливості [19].

Альтернативною схемою є локальні перевірки безпеки за допомогою Notus Scanner. Цей компонент кардинально змінює потік даних: замість багаторазового виконання скриптів, підсистема здійснює єдину автентифіковану сесію (через SSH або WMI), збирає повний перелік встановленого програмного забезпечення на цільовому хості, після чого це зведення локально порівнюється з переліком відомих вразливих програм [19]. Такий алгоритм усуває мережеву надмірність та мінімізує вплив на продуктивність цільових серверів під час моніторингу.

Архітектура GVM спроєктована не лише як інструмент з графічним інтерфейсом, але й як підсистема, здатна до глибокої програмної інтеграції в існуючі процеси інформаційної безпеки підприємства. Використання відкритого протоколу GMP дозволяє перетворити систему на повноцінний “headless” сервіс (сервіс без графічного інтерфейсу), яким керують зовнішні системи управління.

Як зазначається в офіційній документації до бібліотеки python-gvm [22], ця абстракція над GMP-протоколом активно використовується для автоматизації рутинних задач. Зокрема, така архітектура дозволяє вбудовувати запуск сканувань безпосередньо у конвеєри безперервної інтеграції та доставки. У такій моделі тригером для взаємодії виступає не людина-оператор, а програмна подія (наприклад, розгортання нового сервера).

Крім того, використання мережевого протоколу OSP створює передумови для розподіленої архітектури розгортання. Один центральний екземпляр gvmd здатен комунікувати через зашифровані канали з віддаленими сенсорами ospd-openvas. Така модель взаємодії вирішує проблеми маршрутизації та доступу через міжмережеві екрани, оскільки сканування ініціюється локально у цільовому сегменті мережі, а центральному серверу повертаються лише оброблені результати перевірок [19].

2.4. Розробка топології тестової мережі

Для перевірки ефективності роботи розробленої підсистеми виявлення вразливостей необхідне реалістичне тестове середовище. Як базову інфраструктуру було обрано корпоративну мережу, спроєктовану в рамках попередніх етапів дослідження. Її архітектура базується на класичній трирівневій ієрархічній моделі Cisco (рівні ядра, розподілу та доступу) з використанням протоколу GLBP для резервування шлюзів та балансування навантаження (Рис. 2.4.). Такий підхід дозволяє імітувати типову сучасну корпоративну мережу з притаманною їй складністю, сегментацією та маршрутизацією.

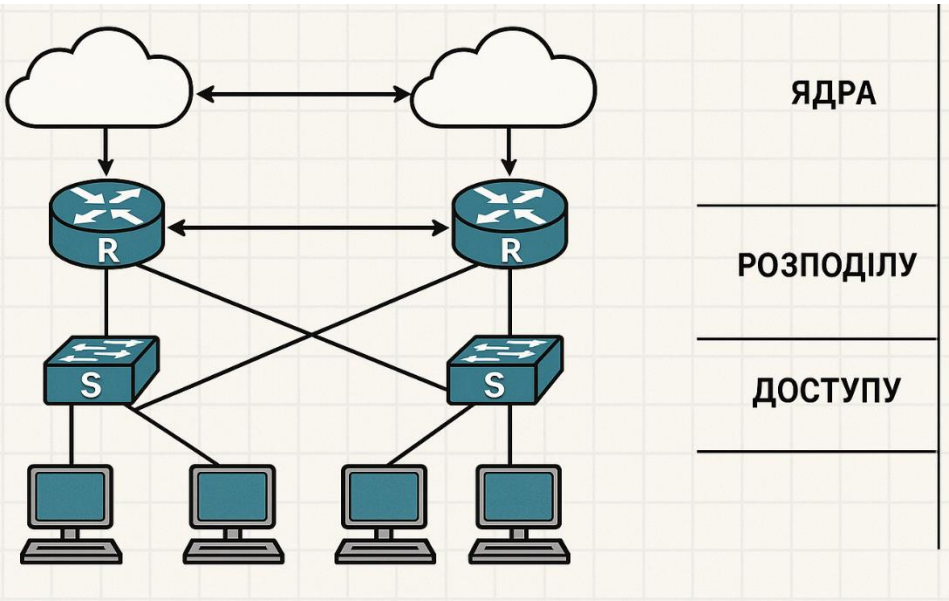


Рисунок 2.4 – Схематичне предствлення трирівневої ієрархічної архітектури

Для рівня ядра обрано потужне обладнання, розраховане на швидкісну передачу даних (магістральну комутацію) між основними логічними сегментами мережі. Головна вимога до нього – мінімізація затримок та забезпечення гранично високої пропускної здатності, адже саме тут обробляється весь транзитний трафік. Критична важливість надійності вимагає впровадження дублювання каналів зв'язку та механізмів миттєвого перемикання трафіку при збоях.

На рівні розподілу, який слугує ланкою між ядром та доступом, реалізовано протокол GLBP. Для цього буде задіяно групу маршрутизаторів, які діятимуть як єдиний віртуальний шлюз за замовчуванням. Використання GLBP дасть змогу цим пристроям одночасно обробляти ARP-запити від клієнтів, що дозволить ефективно балансувати трафік та гарантувати безперебійність мережевих сервісів. Реалізація цього протоколу також сприятиме гнучкому керуванню потоками даних, враховуючи пріоритетність сервісів та стан резервних лінків у різних штатах мережі.

Для безпосереднього підключення кінцевих користувачів та пристроїв призначений рівень доступу. Тут буде використано кероване комутаційне обладнання з широким набором функцій: VLAN-сегментація, політики безпеки, захист портів та контроль доступу. Трафік з цього рівня буде перенаправлятися на маршрутизатори рівня розподілу для обробки за протоколом GLBP та подальшої маршрутизації до зовнішніх або внутрішніх сервісів. Додаткові заходи безпеки

передбачають перевірку ARP-пакетів, використання ACL для обмеження GLBP-трафіку та виділення окремих VLAN для взаємодії між самими маршрутизаторами.

Впровадження протоколу GLBP як ключового елемента архітектури дозволяє уникнути перевантаження каналів при підключенні до зовнішніх мереж та Інтернету. При цьому зберігається оптимальний баланс між складністю реалізації та ефективністю обраного технічного рішення для конкретного середовища.

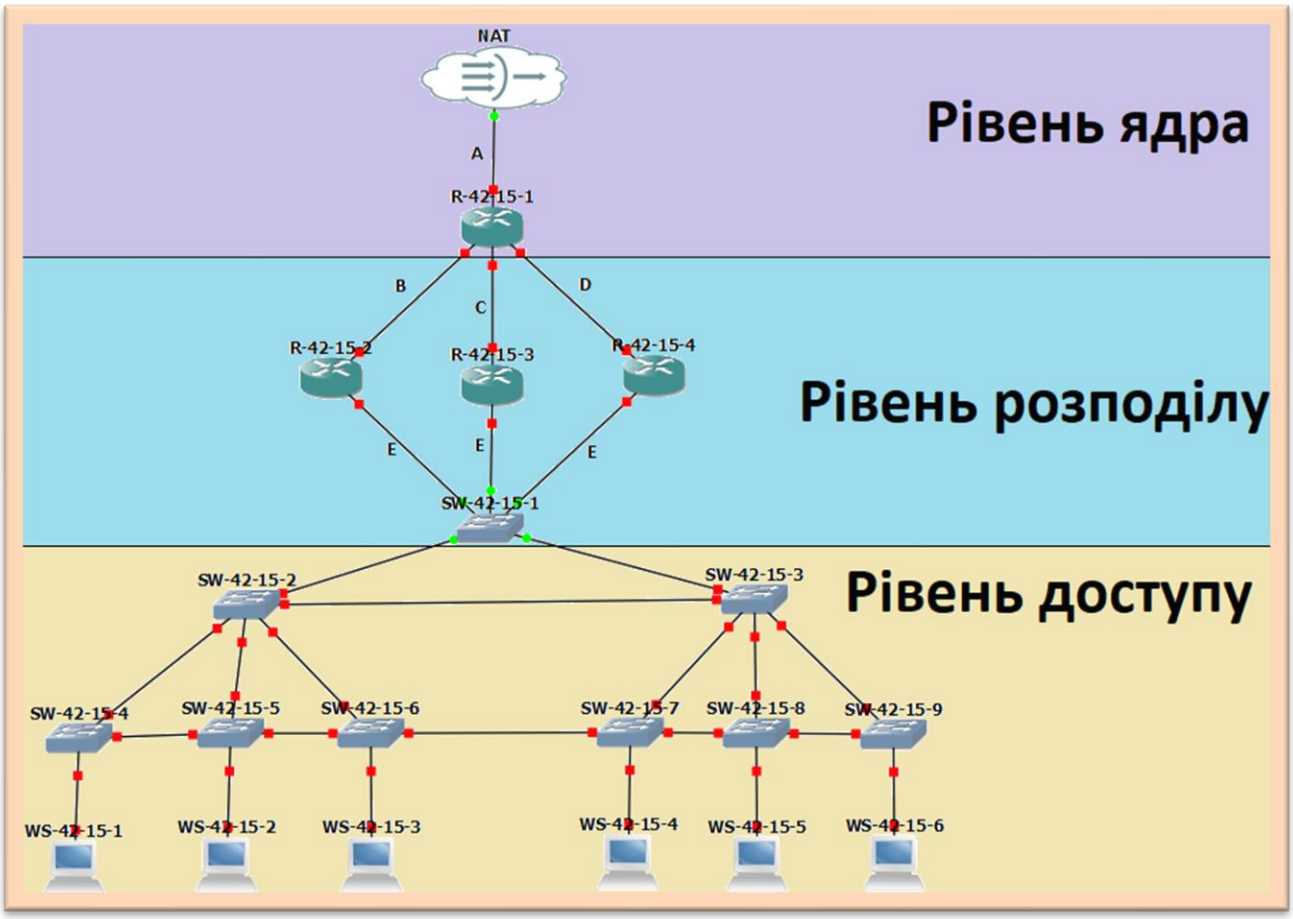


Рисунок 2.5 – Загальна топологія мережі

Загальна розроблена мережа складається з 4 маршрутизаторів та 9 комутаторів, що забезпечують підключення користувачів, серверів і систем моніторингу. Для зручності адміністрування та підвищення рівня безпеки, мережу логічно розділено на п'ять ключових підмереж (A, B, C, D, E), кожна з яких виконує свою специфічну функцію в загальній архітектурі.

Підмережа A (Зовнішній шлюз та NAT) Ця підмережа виконує роль демілітаризованої зони або зовнішнього інтерфейсу між ядром мережі та глобальною мережею Інтернет. Центральним елементом тут виступає

маршрутизатор R-42-15-1, який виконує функції магістрального ядра. Він забезпечує доступ до зовнішніх ресурсів за допомогою механізму трансляції мережевих адрес (NAT Overload/PAT). З'єднання реалізується через інтерфейс Gigabit Ethernet, де маршрутизатор отримує динамічні або статичні налаштування від провайдера. Цей сегмент є критично важливим для отримання оновлень баз вразливостей сервером OpenVAS із зовнішніх джерел.

Підмережі B, C, D (Транзитні лінки точка-точка) Внутрішня маршрутизація між рівнем ядра (R-42-15-1) та рівнем розподілу (R-42-15-2, R-42-15-3, R-42-15-4) реалізована через ізольовані транзитні підмережі B (10.10.10.0/30), C (20.20.20.0/30) та D (30.30.30.0/30). Використання маски /30 дозволяє виділити рівно дві корисні IP-адреси для кожного каналу зв'язку, що мінімізує марнотратство адресного простору та унеможливлює підключення несанкціонованих пристроїв у магістральні канали. Ці підмережі забезпечують створення трикутної відмовостійкої топології: якщо один із маршрутизаторів розподілу виходить з ладу, трафік автоматично перенаправляється через інші вузли завдяки протоколу динамічної маршрутизації EIGRP.

Підмережа E (Мережа доступу та інфраструктури) Найбільший сегмент мережі (193.42.15.0/24), який охоплює весь рівень доступу. Саме тут розгорнуто пул керованих комутаторів від SW-42-15-1 до SW-42-15-9. Маршрутизатори розподілу виступають для цієї мережі єдиним віртуальним шлюзом за замовчуванням (IP: 193.42.15.254) завдяки налаштованій групі GLBP. Розподіл IP-адрес для клієнтських станцій здійснюється централізовано через DHCP-сервер на базі ядра R-42-15-1 (з використанням функції DHCP relay на рівні розподілу).

Для реалізації завдань дипломного проєкту базова підмережа E була суттєво модифікована шляхом впровадження компонентів підсистеми сканування та інтеграції вразливих цілей (Target Systems).

Центральним елементом оновленої топології став сервер сканування OpenVAS (розгорнутий на базі ОС Kali Linux). Його підключено до комутатора SW-42-15-8. Серверу призначено IP-адресу 193.42.15.25 за протоколом DHCP.

Для перевірки ефективності сканера та відпрацювання різних сценаріїв атак, замість стандартних робочих станцій (WS-42-15-1, WS-42-15-2 та WS-42-15-3) у мережу доступу (підмережа E) було інтегровано три спеціалізовані вразливі цілі:

1. Metasploitable 2 – навмисно вразлива операційна система на базі Linux, спеціально створена для тестування засобів безпеки. Вона містить велику кількість відкритих портів та застарілих сервісів (FTP, Telnet, SSH, вразливі веб-сервери, бази даних). Цей вузол дозволить перевірити здатність OpenVAS виявляти класичні мережеві вразливості та помилки відкритого доступу.

2. Windows 10 – клієнтська операційна система розгорнута без останніх оновлень безпеки. Вона слугуватиме мішенню для тестування механізмів автентифікованого сканування через протоколи WMI та SMB, що дозволить системі GVM проаналізувати реєстр і файлову систему на наявність пропущених патчів від Microsoft.

3. Ubuntu Server 22.04 LTS – серверна ОС з навмисно некоректно налаштованими сервісами. Цей вузол спрямований на перевірку якості виявлення логічних вразливостей конфігурації (наприклад, слабкі алгоритми шифрування SSH, надмірні права доступу до директорій).

Детальна таблиця адресації усієї мережі, включно з виділеними діапазонами для комутаторів (193.42.15.5 - 193.42.15.14) та пулами DHCP для кінцевих станцій і вразливих цілей, винесена в Додатки до дипломної роботи.

Спроєктована таким чином топологія є масштабованою та технічно обґрунтованою. Вона дозволяє не лише перевірити працездатність алгоритмів резервування GLBP, але й забезпечує ідеальне середовище для повноцінного тестування підсистеми виявлення вразливостей. Наявність різних операційних систем та типів загроз в одному сегменті гарантує комплексне випробування сканера OpenVAS в умовах, максимально наближених до реальної інфраструктури підприємства.

2.5. Модель загроз для досліджуваної IT-інфраструктури

Для забезпечення ефективного функціонування підсистеми виявлення вразливостей необхідно чітко формалізувати перелік загроз, які є релевантними для спроєктованої тестової інфраструктури. Розробка моделі загроз є критичним етапом, що дозволяє обґрунтувати вибір політик сканування та налаштування параметрів OpenVAS таким чином, щоб охопити максимально широкий спектр потенційних векторів атак на різних рівнях еталонної моделі OSI. При формуванні даної моделі враховуються базові принципи класифікації загроз (наприклад, елементи методології STRIDE – підміна, втручання, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв), адаптовані під специфіку розгорнутої топології.

Оскільки основою інфраструктури є обладнання Cisco, організоване за трирівневою ієрархічною моделлю, значна частина загроз лежить у площині канального (L2) та мережевого (L3) рівнів. На рівні доступу (комутатори серії SW-42-15) критичними загрозами є:

1. ARP Spoofing – підміна MAC-адрес з метою перехоплення трафіку між робочими станціями та шлюзом за замовчуванням [27].
2. DHCP Starvation – зловмисне вичерпання пулу IP-адрес на DHCP-сервері, що призводить до відмови в обслуговуванні для нових легітимних клієнтів мережі [28].
3. VLAN Hopping – несанкціонований перехід між віртуальними локальними мережами через експлуатацію протоколу DTP або подвійне тегування кадрів, що дозволяє зловмиснику отримати доступ до ізольованих сегментів [29].

На рівні розподілу та ядра, де функціонують протоколи динамічної маршрутизації та резервування, існують специфічні вектори атак високого рівня критичності. До них належать маніпуляції з протоколом балансування навантаження GLBP. Оскільки протокол покладається на обмін мультикаст-повідомленнями, зловмисник може здійснити GLBP Spoofing – ініціювати несанкціоноване захоплення ролі Active Virtual Gateway або Active Virtual Forwarder, що дозволить повністю перехопити або заблокувати вихідний трафік

підмережі E [30]. Іншою загрозою є EIGRP Poisoning – ін'єкція хибних маршрутів у автономну систему, що може призвести до утворення петель маршрутизації або перенаправлення магістрального трафіку [31]. Крім того, зберігається ризик експлуатації адміністративних протоколів: використання стандартних community string для SNMP, атаки повного перебору (brute-force) на сервіси управління Telnet/SSH, а також розкриття топології мережі через неконтрольоване розсилання пакетів протоколу CDP.

Загрози для цільових операційних систем та сервісів Другий масив загроз стосується безпосередньо кінцевих вузлів мережі (серверного та клієнтського сегментів), які у тестовій топології представлені трьома спеціалізованими цільовими операційними системами. Кожна з них імітує окремий клас проблем інформаційної безпеки.

Для вузла на базі Metasploitable 2 ключовими загрозами є наявність вбудованих бекдорів та експлуатація застарілих мережевих протоколів. Цей вектор охоплює перехоплення автентифікаційних даних через незашифровані канали (наприклад, FTP та Telnet), наявність вразливих версій баз даних (MySQL без пароля root, PostgreSQL), а також критичні вразливості у веб-серверах (Apache, Tomcat) та сервісах віддаленого виклику процедур. Ці загрози класифікуються як проблеми розкриття інформації та віддаленого виконання коду. Вони вимагають від сканера використання інтенсивних активних мережевих тестів [32].

Для клієнтської ОС Windows 10 головним вектором загроз є організаційні недоліки – відсутність своєчасного встановлення оновлень безпеки. Це створює високі ризики експлуатації відомих критичних вразливостей у мережевих службах Server Message Block, Remote Procedure Call та підсистемах ядра ОС. Відсутність патчів дозволяє реалізувати атаки типу Pass-the-Hash, NTLM Relaying, а також експлуатувати вразливості нульового або N-го дня, що неминуче призводить до повного компрометування машини або локального підвищення привілеїв.

Серверна ОС Ubuntu Server 22.04 LTS формує вектор загроз, безпосередньо пов'язаний з помилками адміністрування та конфігурації. До таких загроз належать використання застарілих і слабких криптографічних алгоритмів (наприклад, CBC-

шифрів або старих версій TLS) для SSH та HTTPS-з'єднань. Також сюди входять залишені стандартні облікові записи доступу, надмірно ліберальні права доступу до критичних файлів і директорій, а також невірно налаштовані політики міжмережевого екрану на рівні хоста, що залишають відкритими службові порти баз даних чи систем моніторингу для загального доступу.

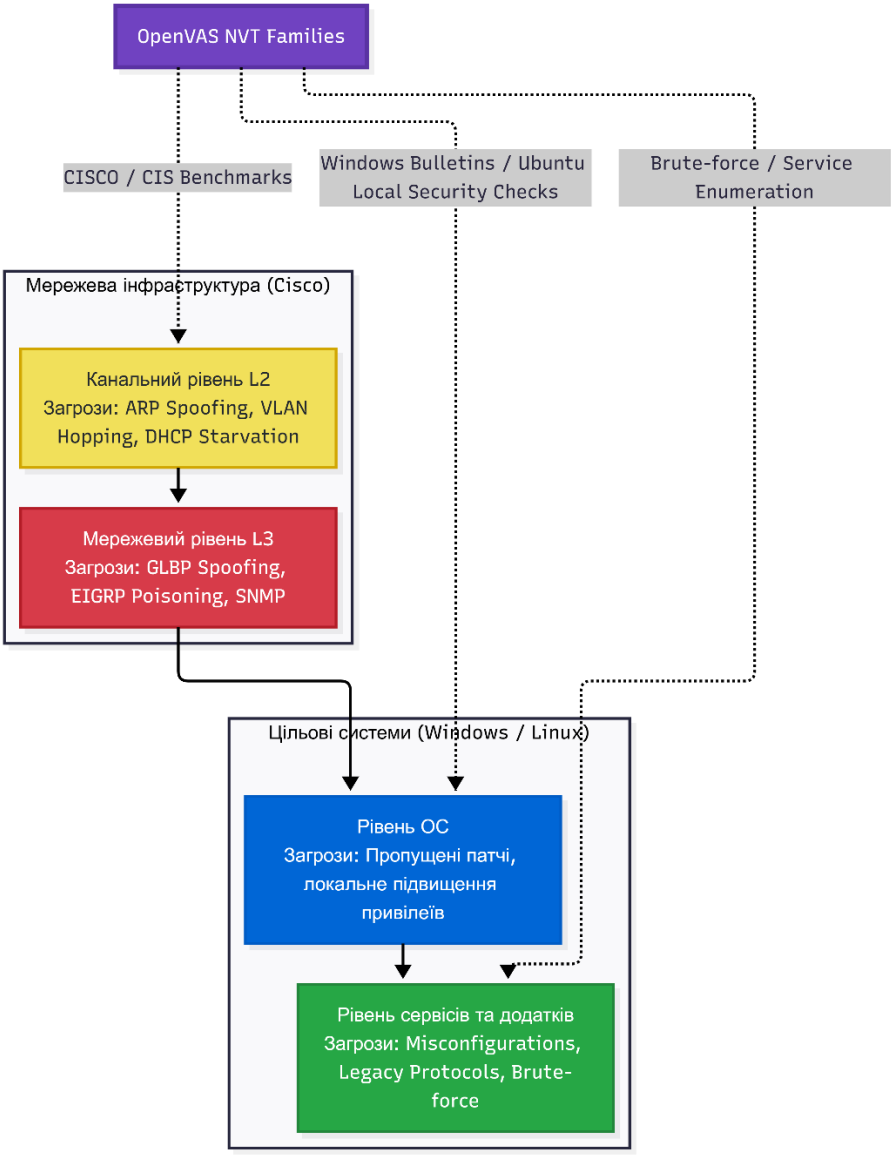


Рисунок 2.6 – Матриця загроз по рівнях IT-інфраструктури

Кореляція моделі загроз із функціоналом сканера OpenVAS Для проактивного виявлення описаних загроз до моменту їх експлуатації, підсистема GVM використовує базу спеціалізованих сімейств тестів, які безперервно оновлюються через Greenbone Community Feed.

Перевірка мережевого обладнання Cisco забезпечується сімейством скриптів CIS-Benchmarks та CISCO, які аналізують конфігураційні файли на

відповідність галузевим стандартам безпеки, виявляючи вразливості CDP чи слабкі SNMP-ком'юніті. Загрози слабкої автентифікації на всіх вузлах виявляються модулями сімейства Brute-Force. Відсутність необхідних патчів на Windows-машині ідентифікується за допомогою сімейств Windows та Windows: Microsoft Bulletins, які базуються безпосередньо на базах даних CVE.

На основі розробленої багатовекторної моделі загроз, для комплексного тестування інфраструктури буде використано дві паралельні стратегії сканування в OpenVAS:

1. Неавтентифіковане мережеве сканування з використанням політики “Full and fast”. Вона дозволить швидко виявити відкриті порти, ідентифікувати запущені сервіси та знайти очевидні мережеві вразливості (зокрема на вузлі Metasploitable 2 та магістральних маршрутизаторах).

2. Автентифіковане сканування через протоколи SSH (для Ubuntu) та WMI/SMB (для Windows 10). Цей метод дозволить сканеру авторизуватися в системі, зібрати списки встановлених пакетів, перевірити ключі реєстру та проаналізувати локальні конфігурації, забезпечуючи виявлення загроз типу “Missing Patches” та “Misconfigurations” з нульовим рівнем хибних спрацьовувань.

Висновки до другого розділу:

У другому розділі було здійснено комплексне проєктування підсистеми виявлення вразливостей на базі технологічного стеку OpenVAS/GVM, а також розроблено тестове середовище для її практичної апробації.

Зокрема, було обґрунтовано вибір трирівневої модульної архітектури системи безпеки, яка логічно розділяє процеси збору даних (через компоненти сканування), централізованого управління (за допомогою gvmd та баз даних PostgreSQL/Redis) та рівня подання інформації (через веб-інтерфейс GSA та API). Такий підхід забезпечує високу масштабованість підсистеми та дозволяє інтегрувати її в корпоративні конвеєри автоматизації з використанням протоколу GMP.

Функціональна структура підсистеми була деталізована з акцентом на сучасні методи сканування. Розглянуто модель взаємодії компонентів, що підтвердила переваги використання протоколу OSP для побудови розподілених архітектур сканування, здатних працювати в ізольованих сегментах мережі без порушення політик міжмережевих екранів.

Для перевірки ефективності спроєктованої підсистеми було розроблено топологію досліджуваної мережі. За основу взято класичну трирівневу ієрархічну модель Cisco з реалізацією протоколу балансування навантаження GLBP. Базову інфраструктуру було модифіковано: до мережі доступу інтегровано сервер OpenVAS та три типи спеціалізованих вразливих цілей (Metasploitable 2, Windows 10 без оновлень та некоректно налаштований Ubuntu Server). Це дозволило створити середовище, максимально наближене до реальних корпоративних умов.

На основі розробленої топології було сформовано комплексну модель загроз. Модель класифікує вектори атак на мережеве обладнання (ARP Spoofing, GLBP Spoofing) та цільові операційні системи. Кожну загрозу було успішно зіставлено з відповідними сімействами тестів NVT та політиками сканування OpenVAS.

Отже, результати проєктування, отримані у другому розділі, формують повноцінне теоретичне та архітектурне підґрунтя для переходу до етапу практичної реалізації, розгортання віртуального стенда в середовищі GNS3 та безпосереднього проведення сканувань, що буде розглянуто в наступному розділі.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НА БАЗІ OPENVAS

3.1. Встановлення та налаштування OpenVAS

Практична реалізація підсистеми виявлення вразливостей розпочинається з розгортання центрального елемента – сканера OpenVAS (Greenbone Vulnerability Management). Для забезпечення максимальної сумісності та стабільності роботи, як базову операційну систему було обрано спеціалізований дистрибутив Kali Linux, який містить необхідні компоненти GVM у своїх офіційних репозиторіях.

Першим етапом розгортання стало завантаження та імпортування офіційного образу Kali Linux до середовища віртуалізації VirtualBox. Під час базового налаштування віртуальної машини було виділено оптимальні апаратні ресурси (зокрема об'єм оперативної пам'яті), необхідні для стабільної роботи ресурсоємних баз даних PostgreSQL та Redis, що використовуються сканером під час обробки тисяч вразливостей.

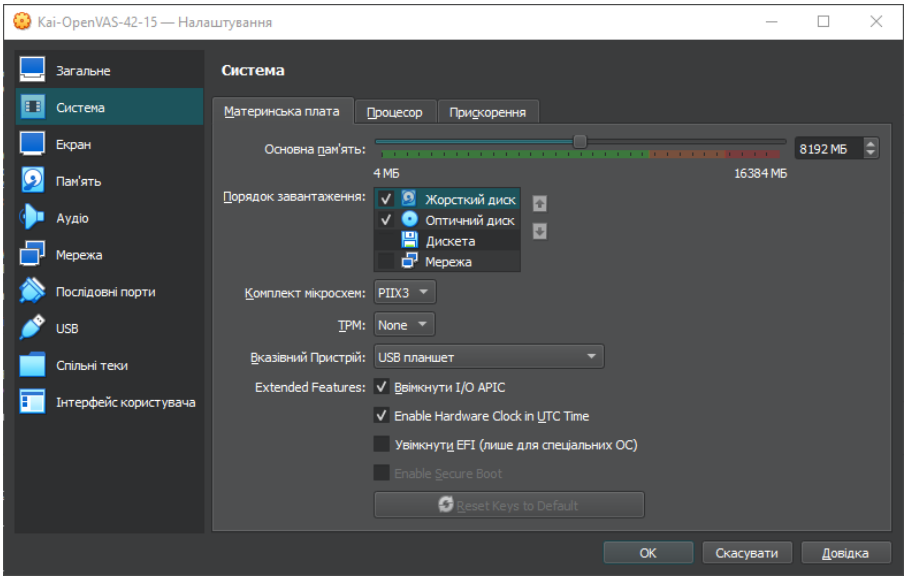


Рисунок 3.1 – Імпортування та налаштування віртуальної машини

Перед безпосереднім встановленням програмного комплексу OpenVAS, було проведено обов'язкову процедуру актуалізації списків пакетів операційної системи. Це критично важливо для уникнення конфліктів залежностей під час інсталяції специфічних служб. Синхронізація з офіційними репозиторіями Kali Linux здійснювалася за допомогою системного менеджера пакетів (команда sudo apt update).

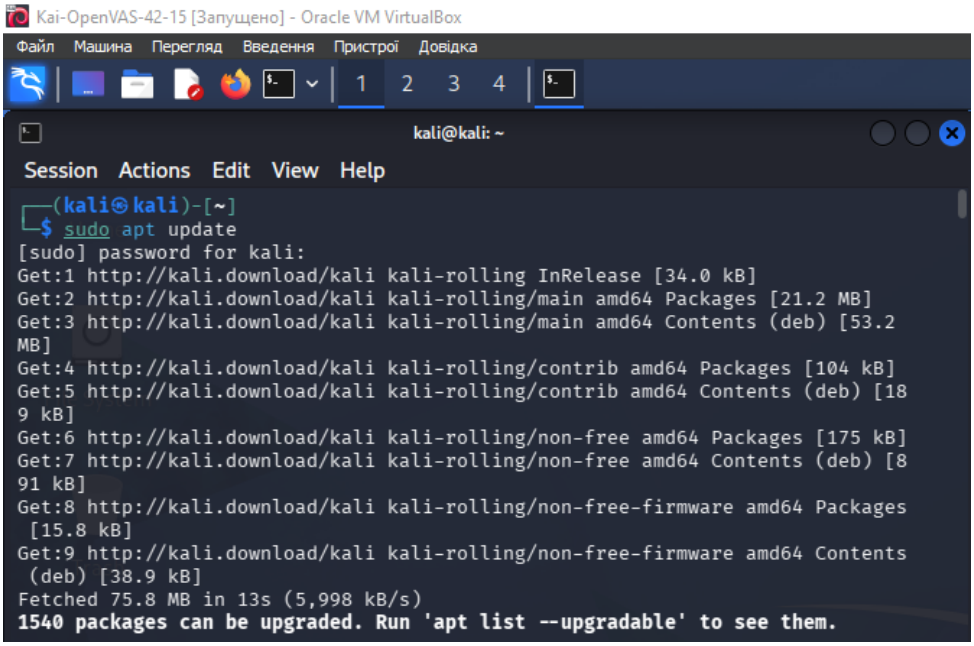


Рисунок 3.2 – Актуалізація списків пакетів sudo apt update

Після отримання актуальних індексів пакетів, було виконано глобальне оновлення всіх встановлених компонентів операційної системи до останніх стабільних версій (команда sudo apt upgrade -y). Це гарантує усунення наявних локальних вразливостей в самій системі сканування та забезпечує абсолютну сумісність ядра з останніми модулями GVM.

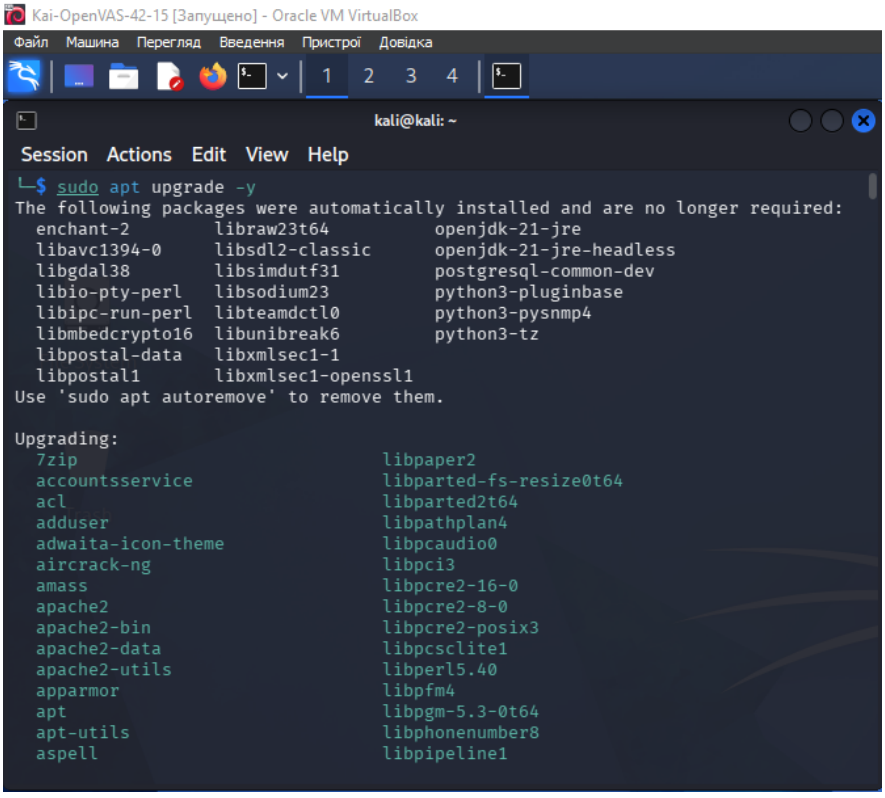


Рисунок 3.3 – Оновлення системи sudo apt upgrade -y

Безпосередній процес встановлення сканера включає розгортання ключових служб: gvmd (менеджер управління), ospd-openvas (демон сканера), gsad (веб-інтерфейс) та бази даних PostgreSQL. Після базового розгортання компонентів системи критично важливим етапом є первинна синхронізація баз даних вразливостей. Система використовує кілька джерел даних: NVT для активних перевірок мережевих служб, SCAP-дані для перевірки відповідності стандартам безпеки, та CERT-дані для отримання актуальної інформації про загрози. Цей процес ініціюється автоматичним скриптом gvm-setup, який завантажує найсвіжіші підписи безпосередньо з репозиторіїв Greenbone Community Feed.



Рисунок 3.4 – Процес встановлення ядра сканера OpenVAS



Рисунок 3.5 – Запуск автоматичного налаштування

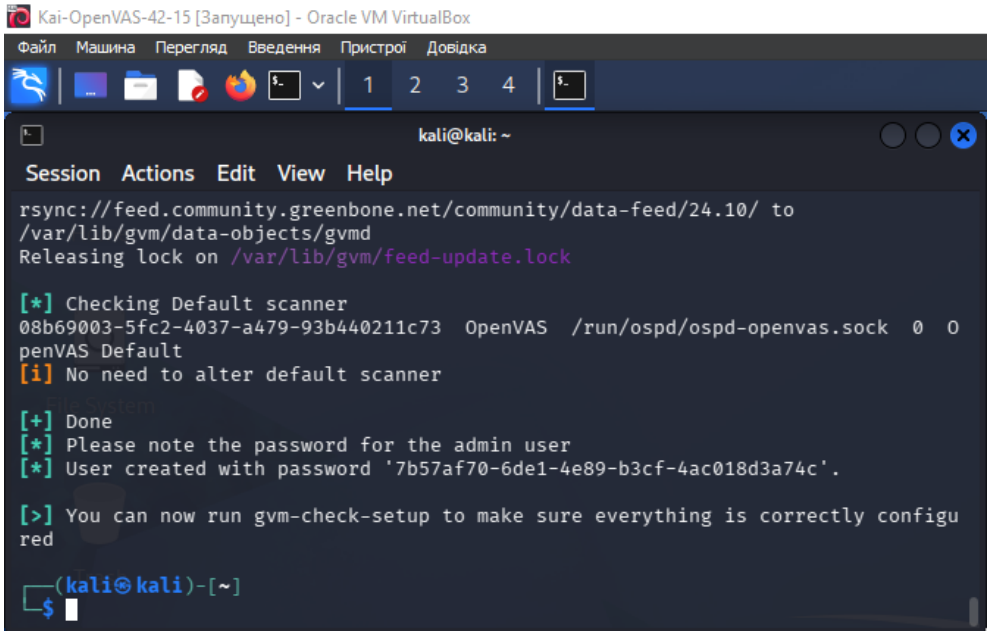


Рисунок 3.6 – Результат успішного автоматичного налаштування

Після завершення синхронізації фідів, підсистема перевіряє цілісність баз даних і перебудовує кеш. На цьому етапі важливо переконатися, що всі системні демони працюють у штатному режимі і коректно взаємодіють між собою. Служба ospd-openvas встановлює з'єднання через Unix-сокет з gvmd, який, у свою чергу, відповідає на запити від веб-сервера gsad. Успішність конфігурації перевіряється спеціальною утилітою.



Рисунок 3.7 – Перевірка коректності розгортання компонентів GVM

Управління системою, налаштування завдань та аналіз результатів здійснюється через графічний веб-інтерфейс GSA. Веб-інтерфейс працює на порту

9392 і вимагає авторизації за допомогою облікового запису адміністратора, створеного на етапі встановлення.

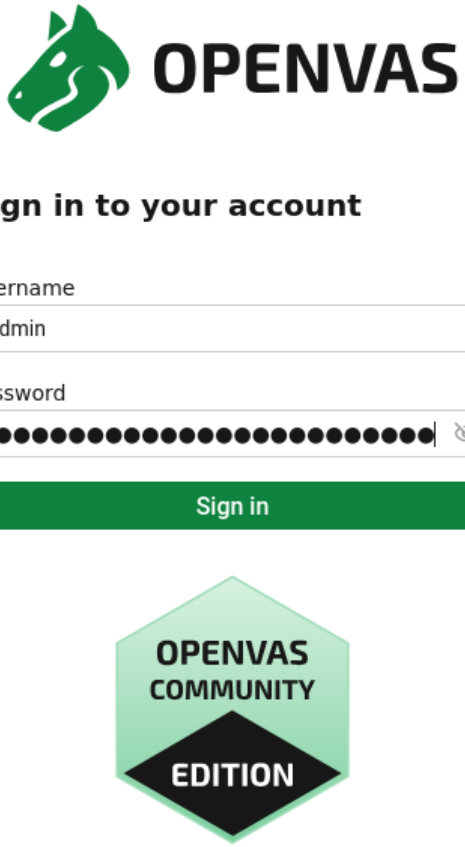


Рисунок 3.8 – Форма авторизації веб-інтерфейсу OpenVAS

Після успішного розгортання та авторизації в системі, відкривається доступ до головного робочого простору OpenVAS. Графічний веб-інтерфейс платформи побудований за зручним модульним принципом, що логічно розділяє інструментарій на кілька ключових розділів, забезпечуючи адміністратору ефективне управління процесами аудиту кібербезпеки. Головне навігаційне меню включає наступні основні категорії:

1. Розділ Dashboards (Панелі інструментів) Це стартова сторінка платформи, яка слугує аналітичним центром для візуалізації загального стану безпеки інфраструктури. Інформація подається у вигляді кругових діаграм та інтерактивних графіків, що відображають статистику за кількістю виявлених вразливостей, їх рівнем критичності (High, Medium, Low) та статусом виконання поточних завдань. Цей модуль дозволяє швидко оцінити загальну ситуацію в мережі без глибокого занурення у звіти.

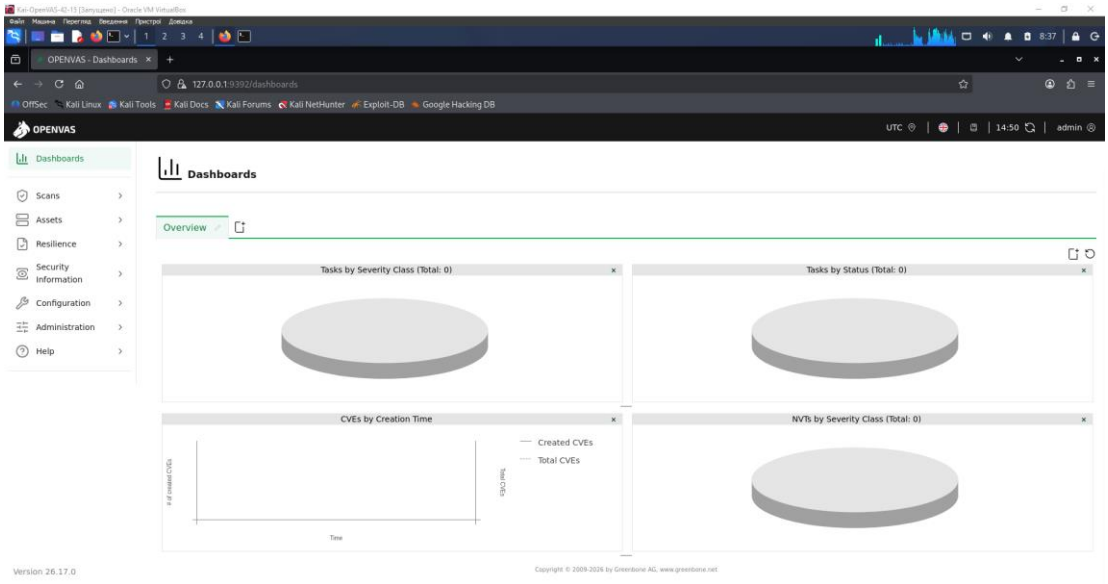


Рисунок 3.9 – Розділ Dashboards

2. Розділ Scans (Сканування) Цей розділ є основним робочим простором для проведення безпосереднього аудиту. Він логічно поділяється на три підкатегорії:

- *Tasks*: меню для конфігурації, запуску та відстеження прогресу завдань на сканування.
- *Reports*: архів усіх завершених перевірок, який надає можливість детального перегляду або експорту результатів аудиту у форматах PDF, XML чи CSV.
- *Results*: зведений реєстр усіх конкретних вразливостей, ідентифікованих під час сканувань, із зазначенням рівня загрози за шкалою CVSS та IP-адреси вразливого хоста.

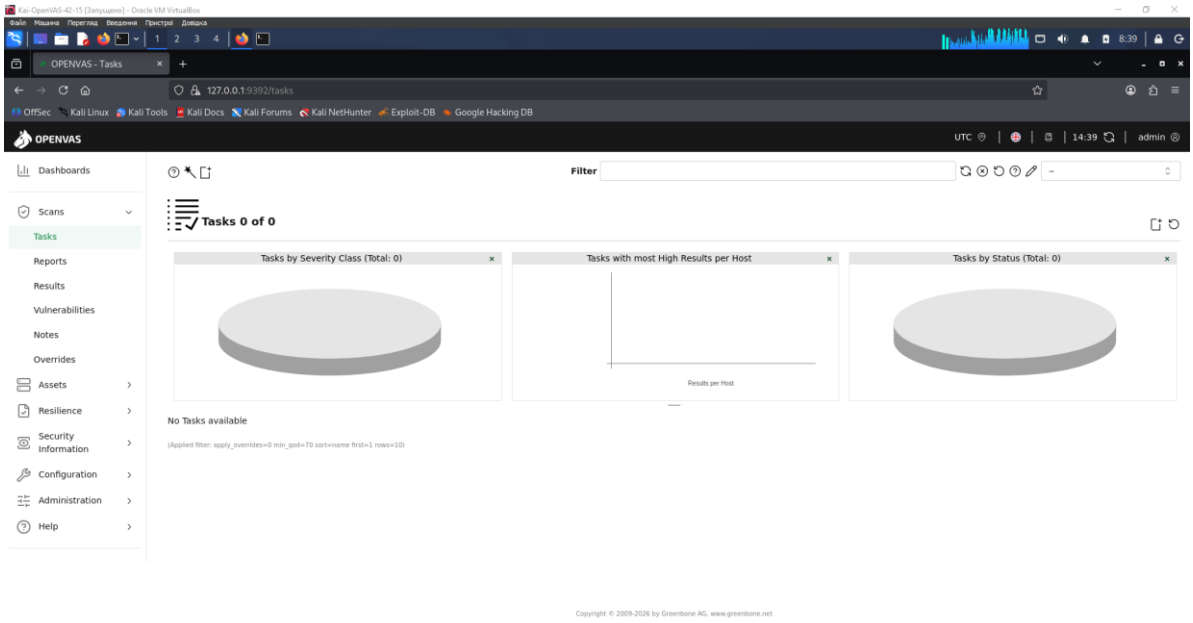


Рисунок 3.10 – Розділ Scans (Tasks)

3. Розділ Assets (Активи) Модуль відповідає за автоматизовану інвентаризацію досліджуваної мережі. Платформа накопичує та структурує інформацію про всі просканові вузли. У вкладці *Hosts* формується список виявлених IP-адрес із прив'язкою до знайдених загроз, а у вкладці *Operating Systems* акумулюються дані про ідентифіковані операційні системи цільових машин. Це суттєво полегшує подальший контроль над інфраструктурою та виявлення несанкціонованих пристроїв.

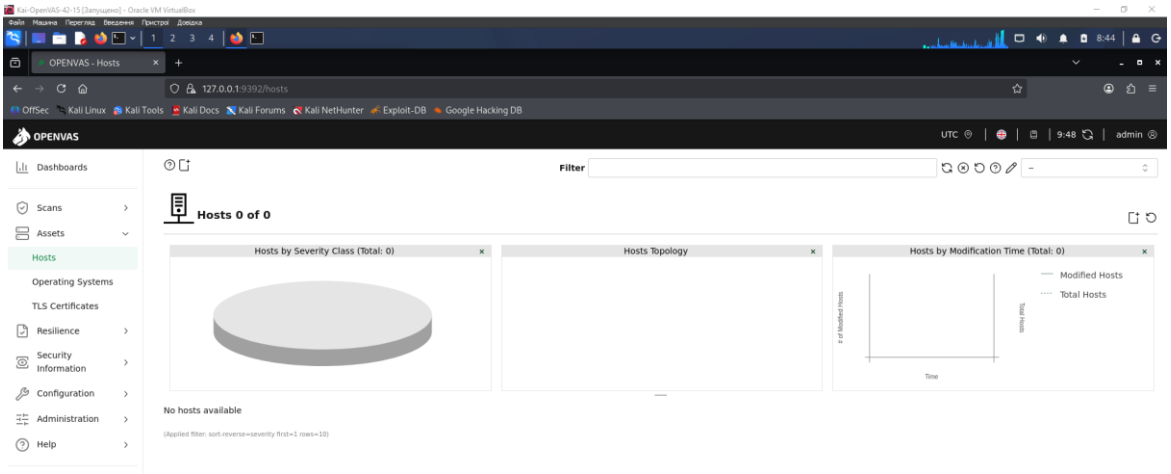


Рисунок 3.11 – Розділ Assets (Hosts)

4. Розділ Security Information (Інформація про безпеку) Один із найважливіших розділів системи, що містить її глобальну базу знань. Тут зібрані всі алгоритми тестів на вразливості (NVT), реєстр загальновідомих вразливостей (CVE), ідентифікатори конфігурацій (CPE) та сертифікати безпеки. Цей розділ регулярно синхронізується з серверами Greenbone Community Feed, що гарантує максимальну актуальність та точність перевірок.

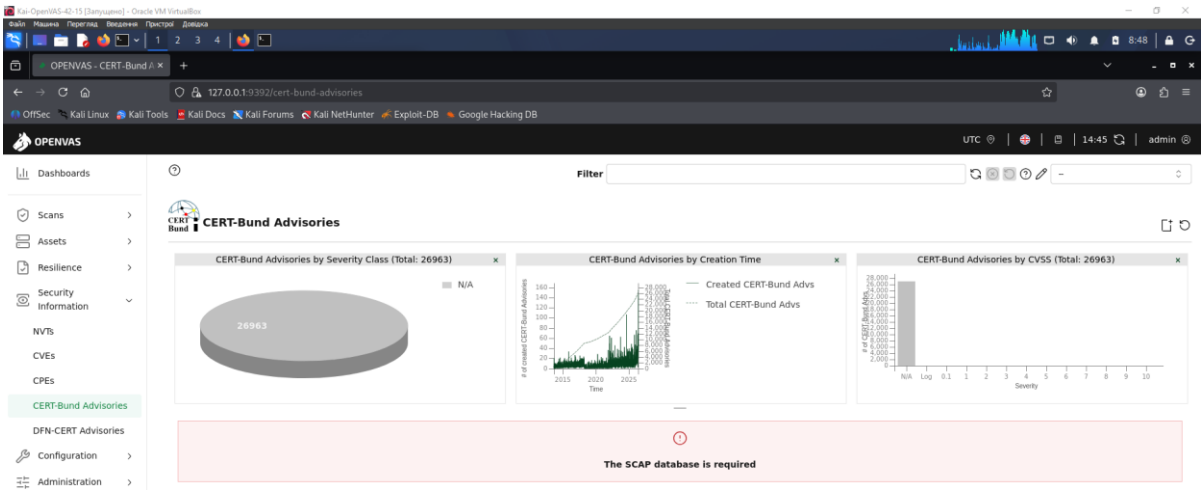


Рисунок 3.12 – Розділ SecInfo (CERT-Bund Advisories)

5. Розділ Configuration (Налаштування) Цей модуль є ключовим інструментом для глибокої кастомізації параметрів аудиту та логіки роботи системи.

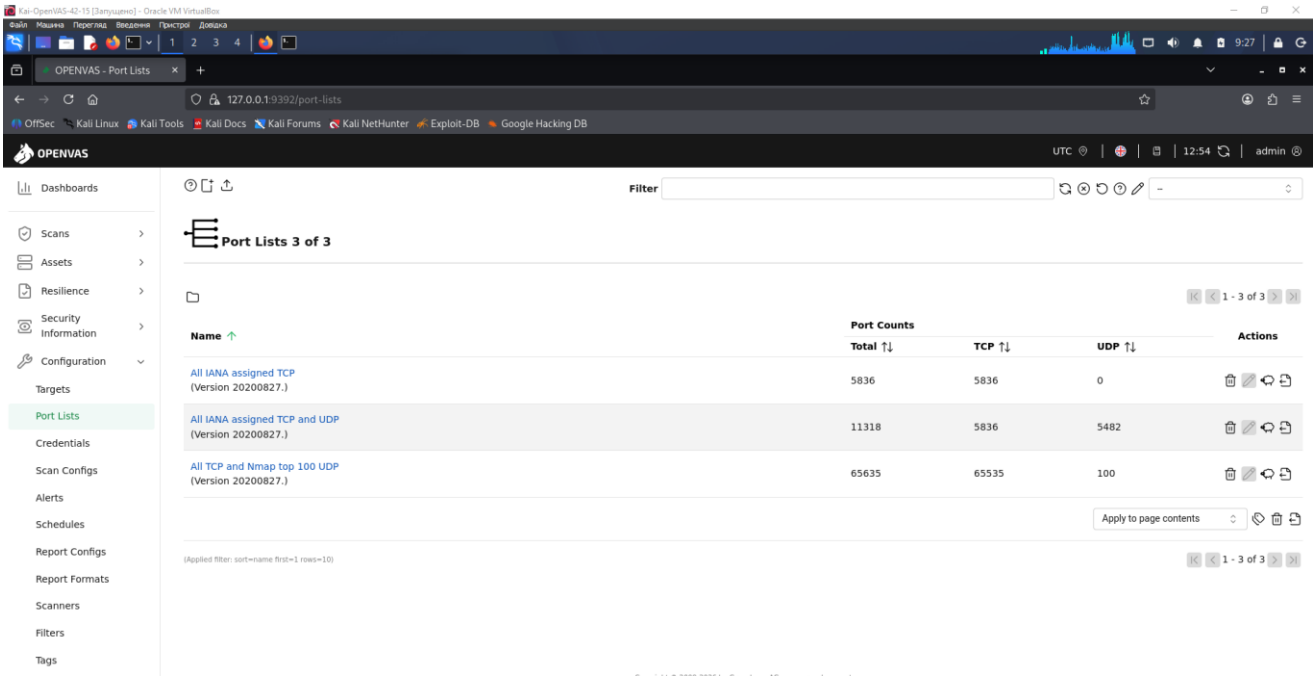


Рисунок 3.13 – Розділ Configuration (Port Lists)

Він пропонує розширений набір підкатегорій:

- *Targets*: створення та групування цілей аудиту, списків IP-адрес, підмереж або доменних імен.
- *Port Lists*: управління діапазонами мережевих портів, які підлягають перевірці: наприклад, сканування всіх доступних TCP/UDP портів або лише стандартних за IANA.
- *Credentials*: безпечне централізоване управління обліковими даними, паролями, SSH-ключами, SMB-токенами, які використовуються для проведення глибокого автентифікованого сканування (“білого ящика”).
- *Scan Configs*: вибір профілів інтенсивності та глибини перевірки (зокрема, базові політики “Full and fast” або “Discovery”).
- *Alerts* та *Schedules*: налаштування автоматизованих сповіщень про критичні знахідки: наприклад, відправка звітів на електронну пошту та планування регулярних перевірок за розкладом.

- *Report Configs* та *Report Formats*: налаштування структури підсумкових звітів та управління форматами їх експорту (PDF, XML, CSV тощо).
- *Scanners*: управління підключеними рушіями сканування, за замовчуванням використовується стандартний OpenVAS Scanner через протокол OSP.
- *Filters* та *Tags*: створення складних правил сортування інформації та маркування цілей чи вразливостей для зручної класифікації великих масивів даних.

6. Розділ Administration (Адміністрування) Це глобальний модуль для управління самою системою Greenbone Vulnerability Management та її інтеграцією в інфраструктуру підприємства. Меню містить наступні підрозділи:

- *Users*, *Groups*, *Roles* та *Permissions*: забезпечують реалізацію моделі управління доступом на основі ролей (RBAC). Вони дозволяють адміністратору створювати облікові записи для аудиторів, об'єднувати їх у групи та гнучко налаштовувати рівні привілеїв щодо перегляду звітів чи запуску завдань.
- *Performance*: інструмент для моніторингу завантаженості підсистеми GVM, що дозволяє оптимізувати використання апаратних ресурсів під час масового сканування.
- *Trashcan*: спеціалізований кошик для тимчасового зберігання видалених конфігурацій, завдань або звітів із можливістю їх відновлення.
- *Feed Status*: критично важлива сторінка для моніторингу статусу та дати останньої синхронізації баз даних вразливостей (NVT, SCAP, CERT) з серверами Greenbone.
- *LDAP* та *RADIUS*: модулі, що дозволяють інтегрувати підсистему аутентифікації OpenVAS із корпоративними службами каталогів (наприклад, Active Directory), забезпечуючи централізований та безпечний вхід для співробітників компанії.

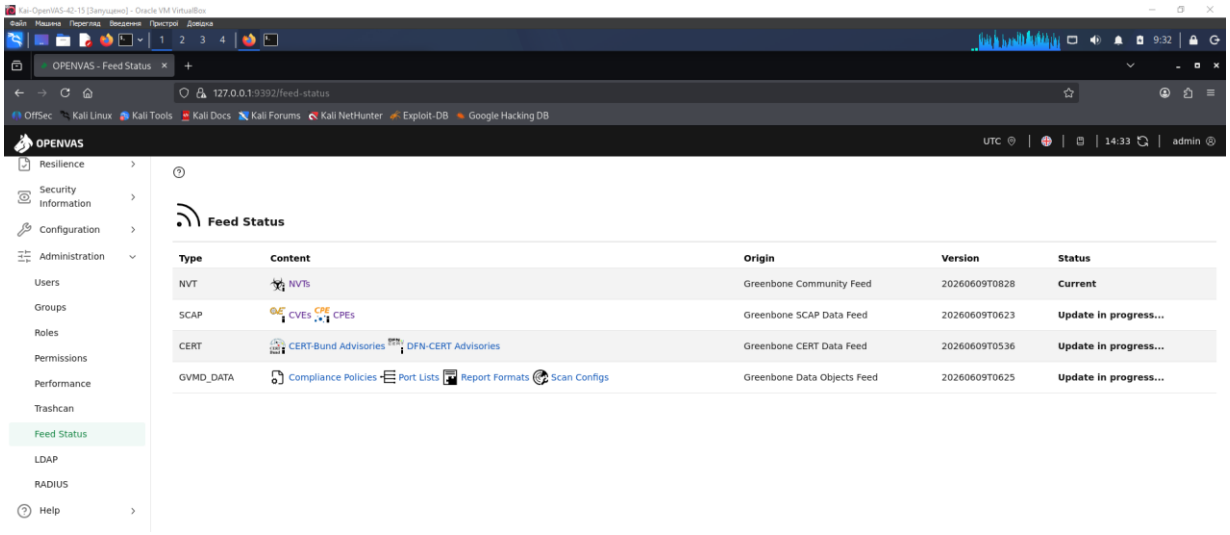


Рисунок 3.14 – Розділ Administration (Feed Status)

3.2. Створення тестового середовища

На поточному етапі виконано початкове налаштування маршрутизаторів корпоративної мережі. Зокрема, реалізовано адресацію мережевих інтерфейсів відповідно до розробленого плану IP-адресації та налаштовано динамічну маршрутизацію з використанням протоколу EIGRP. Це забезпечило коректний обмін маршрутною інформацією між маршрутизаторами та можливість передачі пакетів між усіма підмережами корпоративної інфраструктури.

Налаштування IP-адресації

На першому етапі було призначено IP-адреси інтерфейсам маршрутизаторів R-42-15-1, R-42-15-2, R-42-15-3 та R-42-15-4. Для організації з'єднань між маршрутизаторами використано мережі типу “точка-точка” з маскою підмережі /30 (255.255.255.252), що дозволяє раціонально використовувати доступний адресний простір. Крім того, на маршрутизаторі R-42-15-1 налаштовано інтерфейс, підключений до NAT-сегмента з адресним простором 192.42.15.0/24, який забезпечує доступ внутрішньої мережі до зовнішніх ресурсів.

Налаштування адресації на R-42-15-1:

```
R-42-15-1#conf t
R-42-15-1(config)#int gig0/0
R-42-15-1(config-if)#ip address 10.10.10.1 255.255.255.252
R-42-15-1(config-if)#no sh
R-42-15-1(config-if)#exit
R-42-15-1(config)#
```

```
R-42-15-1(config)#int gig1/0
R-42-15-1(config-if)#ip address 20.20.20.1 255.255.255.252
R-42-15-1(config-if)#no sh
R-42-15-1(config-if)#exit
R-42-15-1(config)#int gig2/0
R-42-15-1(config-if)#ip address 30.30.30.1 255.255.255.252
R-42-15-1(config-if)#no sh
R-42-15-1(config-if)#exit
R-42-15-1(config)#int gig4/0
R-42-15-1(config-if)#ip address 192.42.15.1 255.255.255.0
R-42-15-1(config-if)#no sh
R-42-15-1(config-if)#exit
```

Аналогічним чином виконано налаштування інтерфейсів на інших маршрутизаторах. Наприклад, R-42-15-2 підключений до R-42-15-1 через мережу 10.10.10.0/30, а також має доступ до підмережі 193.42.15.0/24, яка реалізує функції користувацького або серверного сегменту.

Налаштування динамічної маршрутизації

Для забезпечення маршрутизації між усіма сегментами мережі використано протокол EIGRP, що є оптимальним вибором для Cisco-інфраструктури завдяки швидкій конвергенції, масштабованості та підтримці VLSM.

На всіх маршрутизаторах активовано процес маршрутизації EIGRP з ідентифікатором автономної системи *4215*. У конфігурації перераховано всі локальні мережі, які повинні брати участь у маршрутизації. Для зменшення трафіку маршрутизаторів у користувацьких сегментах використано команду passive-interface, яка забороняє надсилання Hello-повідомлень EIGRP на певних інтерфейсах.

Налаштування протоколу маршрутизації EIGRP на R-42-15-1:

```
R-42-15-1#conf t
R-42-15-1(config)#router eigrp 4215
R-42-15-1(config-router)#network 192.42.15.0 255.255.255.0
R-42-15-1(config-router)#network 10.10.10.0 255.255.255.252
R-42-15-1(config-router)#network 20.20.20.0 255.255.255.252
R-42-15-1(config-router)#network 30.30.30.0 255.255.255.252
R-42-15-1(config-router)#network 193.42.15.0 255.255.255.0
R-42-15-1(config-router)#no auto-summary
R-42-15-1(config-router)#exit
```

```
R-42-15-1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         10.10.10.1      YES NVRAM  up                    up
GigabitEthernet1/0         20.20.20.1      YES NVRAM  up                    up
GigabitEthernet2/0         30.30.30.1      YES NVRAM  up                    up
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         192.42.15.1     YES NVRAM  up                    up
FastEthernet5/0            unassigned      YES NVRAM  administratively down down
FastEthernet5/1            unassigned      YES NVRAM  administratively down down
FastEthernet6/0            unassigned      YES NVRAM  administratively down down
FastEthernet6/1            unassigned      YES NVRAM  administratively down down
R-42-15-1#
```

Рисунок 3.15 – Перевірка стану інтерфейсів на R-42-15-1

```
R-42-15-2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         10.10.10.2      YES NVRAM  up                    up
GigabitEthernet1/0         193.42.15.1     YES NVRAM  up                    up
GigabitEthernet2/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
FastEthernet5/0            unassigned      YES NVRAM  administratively down down
FastEthernet5/1            unassigned      YES NVRAM  administratively down down
FastEthernet6/0            unassigned      YES NVRAM  administratively down down
FastEthernet6/1            unassigned      YES NVRAM  administratively down down
R-42-15-2#
```

Рисунок 3.16 – Перевірка стану інтерфейсів на R-42-15-2

```
R-42-15-3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         20.20.20.2      YES NVRAM  up                    up
GigabitEthernet1/0         193.42.15.2     YES NVRAM  up                    up
GigabitEthernet2/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
FastEthernet5/0            unassigned      YES NVRAM  administratively down down
FastEthernet5/1            unassigned      YES NVRAM  administratively down down
FastEthernet6/0            unassigned      YES NVRAM  administratively down down
FastEthernet6/1            unassigned      YES NVRAM  administratively down down
R-42-15-3#
```

Рисунок 3.17 – Перевірка стану інтерфейсів на R-42-15-3

```
R-42-15-4#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         30.30.30.2      YES NVRAM  up                    up
GigabitEthernet1/0         193.42.15.3     YES NVRAM  up                    up
GigabitEthernet2/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
FastEthernet5/0            unassigned      YES NVRAM  administratively down down
FastEthernet5/1            unassigned      YES NVRAM  administratively down down
FastEthernet6/0            unassigned      YES NVRAM  administratively down down
FastEthernet6/1            unassigned      YES NVRAM  administratively down down
R-42-15-4#
```

Рисунок 3.18 – Перевірка стану інтерфейсів на R-42-15-4

На маршрутизаторах R-42-15-2, R-42-15-3 та R-42-15-4 також налаштовано участь у протоколі EIGRP лише на необхідних інтерфейсах, а інтерфейси, що підключені до користувацької мережі, переведені в пасивний режим.

```
R-42-15-1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(4215)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
2   10.10.10.2              Gi0/0                    12 02:02:58   32   192  0
3
1   20.20.20.2              Gi1/0                    11 02:03:00   24   144  0
3
0   30.30.30.2              Gi2/0                    14 02:03:03   19   114  0
3
R-42-15-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/30 is directly connected, GigabitEthernet0/0
L        10.10.10.1/32 is directly connected, GigabitEthernet0/0
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.20.20.0/30 is directly connected, GigabitEthernet1/0
L        20.20.20.1/32 is directly connected, GigabitEthernet1/0
      30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        30.30.30.0/30 is directly connected, GigabitEthernet2/0
L        30.30.30.1/32 is directly connected, GigabitEthernet2/0
      192.42.15.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.42.15.0/24 is directly connected, GigabitEthernet4/0
L        192.42.15.1/32 is directly connected, GigabitEthernet4/0
D     193.42.15.0/24 [90/3072] via 30.30.30.2, 02:03:02, GigabitEthernet2/0
                     [90/3072] via 20.20.20.2, 02:03:02, GigabitEthernet1/0
                     [90/3072] via 10.10.10.2, 02:03:02, GigabitEthernet0/0
```

Рисунок 3.19 – Перевірка налаштування EIGRP на R-42-15-1

```
R-42-15-1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(4215)/ID(192.42.15.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 193.42.15.0/24, 3 successors, FD is 3072
        via 10.10.10.2 (3072/2816), GigabitEthernet0/0
        via 20.20.20.2 (3072/2816), GigabitEthernet1/0
        via 30.30.30.2 (3072/2816), GigabitEthernet2/0
P 30.30.30.0/30, 1 successors, FD is 2816
        via Connected, GigabitEthernet2/0
P 20.20.20.0/30, 1 successors, FD is 2816
        via Connected, GigabitEthernet1/0
P 192.42.15.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet4/0
P 10.10.10.0/30, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0

R-42-15-1#show running-config | section router eigrp
router eigrp 4215
 network 10.10.10.0 0.0.0.3
 network 20.20.20.0 0.0.0.3
 network 30.30.30.0 0.0.0.3
 network 192.42.15.0
 network 193.42.15.0
```

Рисунок 3.20 – Перевірка налаштування EIGRP на R-42-15-1 (Продовження)

```
R-42-15-2#ping 193.42.15.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.42.15.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/40 ms
R-42-15-2#ping 193.42.15.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.42.15.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/20 ms
R-42-15-2#
```

Рисунок 3.21– Перевірка зв’язку між віддаленими підмережами

Після завершення налаштування маршрутизації та механізмів резервування шлюзу було реалізовано службу автоматичної видачі мережевих параметрів за допомогою протоколу DHCP. Використання DHCP дозволяє централізовано керувати процесом призначення IP-адрес клієнтським пристроям, що значно спрощує адміністрування мережі та зменшує ймовірність помилок під час ручного налаштування.

Для цього на маршрутизаторі R-42-15-1 було налаштовано DHCP-сервер. У конфігурації визначено діапазон адрес мережі 193.42.15.0/24, з якого клієнтам автоматично видаються IP-адреси. При цьому адреси від 193.42.15.1 до 193.42.15.20 були виключені з процесу автоматичного розподілу за допомогою команди ip dhcp excluded-address, оскільки вони зарезервовані для мережевого обладнання та інших пристроїв зі статичною адресацією. Також у параметрах DHCP-пулу вказано адресу шлюзу за замовчуванням 193.42.15.1 та DNS-сервер 8.8.8.8, що дозволяє клієнтам отримувати всі необхідні мережеві налаштування автоматично.

Оскільки частина клієнтів розташована в інших сегментах мережі, на маршрутизаторах R-42-15-2, R-42-15-3 та R-42-15-4 було налаштовано механізм DHCP Relay Agent. Для цього на інтерфейсах GigabitEthernet1/0 використано команду ip helper-address, яка забезпечує пересилання широкомовних DHCP-запитів до відповідного DHCP-сервера. Завдяки цьому клієнтські пристрої можуть отримувати IP-адреси навіть тоді, коли DHCP-сервер знаходиться в іншій підмережі.

Після завершення налаштування було підтверджено коректну роботу механізму DHCP. Клієнтські пристрої успішно отримують IP-адреси, адресу шлюзу за замовчуванням та параметри DNS-сервера автоматично, незалежно від сегмента мережі, до якого вони підключені. Використання DHCP Relay Agent забезпечує централізоване керування адресним простором і дозволяє уникнути необхідності розгортання окремого DHCP-сервера в кожній підмережі.

Налаштування протоколу DHCP на R-42-15-1:

R-42-15-1(config)#ip dhcp excluded-address 193.42.15.1 193.42.15.20

R-42-15-1(config)#ip dhcp pool LAN_E

R-42-15-1(dhcp-config)#network 193.42.15.0 255.255.255.0

R-42-15-1(dhcp-config)#default-router 193.42.15.1

R-42-15-1(dhcp-config)#dns-server 8.8.8.8

R-42-15-1(dhcp-config)#exit

Налаштування DHCP Relay Agent на R-42-15-2:

R-42-15-2#conf t

R-42-15-2(config)#int gig1/0

R-42-15-2(config-if)#ip helper-address 10.10.10.1

R-42-15-2(config-if)#exit

Аналогічним чином виконано налаштування інтерфейсів на інших маршрутизаторах.

```
WS-42-15-1> ip dhcp
DDORA IP 193.42.15.24/24 GW 193.42.15.1
```

Рисунок 3.22 – Перевірка роботи DHCP на WS-42-15-1

```
R-42-15-1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
193.42.15.22        0100.5079.6668.06       May 31 2025 01:04 PM    Automatic
193.42.15.23        0100.5079.6668.07       May 31 2025 01:06 PM    Automatic
193.42.15.24        0100.5079.6668.00       May 31 2025 01:11 PM    Automatic
R-42-15-1#show ip dhcp pool

Pool LAN_E :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 193.42.15.25         193.42.15.1      - 193.42.15.254     3
R-42-15-1#show running-config | include excluded-address
ip dhcp excluded-address 193.42.15.1 193.42.15.20
```

Рисунок 3.23 – Перевірка налаштувань DHCP

У цьому етапі було реалізовано налаштування GLBP на трьох маршрутизаторах: R-42-15-2, R-42-15-3 та R-42-15-4. Метою є створення

віртуального шлюзу з IP-адресою 193.42.15.254, яка буде використовуватись як шлюз за замовчуванням для хостів мережі LAN.

GLBP забезпечує балансування навантаження між трьома шлюзами, а також автоматичне відновлення доступності віртуального шлюзу у випадку відмови активного маршрутизатора.

Налаштування GLBP на R-42-15-2:

```
R-42-15-2#conf t
R-42-15-2(config)#interface GigabitEthernet1/0
R-42-15-2(config-if)#glbp 1 ip 193.42.15.254
R-42-15-2(config-if)#glbp 1 priority 110
R-42-15-2(config-if)#glbp 1 preempt delay minimum 30
R-42-15-2(config-if)#glbp 1 timers 5 15
R-42-15-2(config-if)#glbp 1 timers redirect 1200 14400
R-42-15-2(config-if)#glbp 1 load-balancing round-robin
R-42-15-2(config-if)#exit
```

Аналогічним чином виконано налаштування інтерфейсів на R-42-15-3 та R-42-15-4. Таким чином, активним шлюзом буде R-42-15-2, а R-42-15-3 і R-42-15-4 забезпечують резервування.

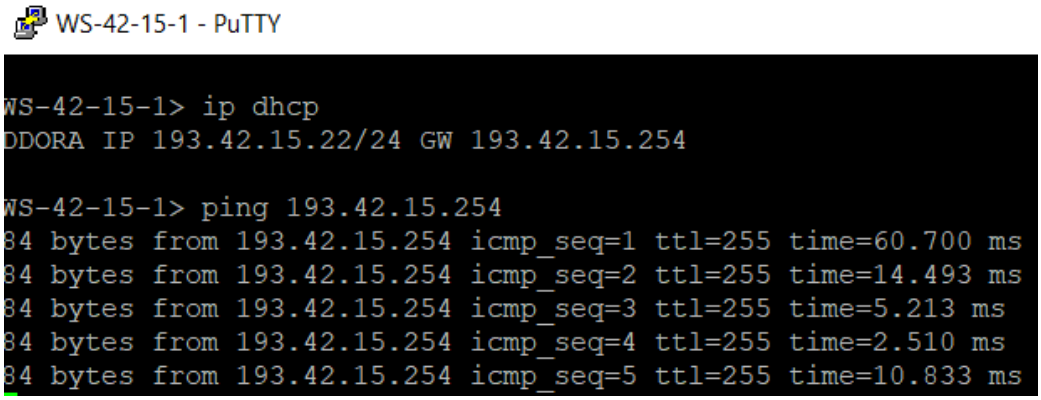


Рисунок 3.24 – Перевірка роботи DHCP та GLBP

```
R-42-15-2#show glbp
GigabitEthernet1/0 - Group 1
  State is Active
    1 state change, last state change 00:07:55
  Virtual IP address is 193.42.15.254
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 0.768 secs
  Redirect time 1200 sec, forwarder timeout 14400 sec
  Preemption enabled, min delay 30 sec
  Active is local
  Standby is 193.42.15.2, priority 105 (expires in 10.400 sec)
  Priority 110 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ca02.68a8.001c (193.42.15.1) local
    ca03.0a80.001c (193.42.15.2)
    ca04.5fcc.001c (193.42.15.3)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:07:06
    MAC address is 0007.b400.0101 (default)
    Owner ID is ca02.68a8.001c
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is ca03.0a80.001c
    Redirection enabled, 1195.424 sec remaining (maximum 1200 sec)
    Time to live: 14395.424 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.2 (primary), weighting 100 (expires in 11.104 sec)
  Forwarder 3
    State is Listen
    MAC address is 0007.b400.0103 (learnt)
    Owner ID is ca04.5fcc.001c
    Redirection enabled, 1197.952 sec remaining (maximum 1200 sec)
    Time to live: 14397.952 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.3 (primary), weighting 100 (expires in 15.328 sec)
R-42-15-2#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
Gi1/0       1    -   110 Active   193.42.15.254   local           193.42.15.2
Gi1/0       1    1   -   Active   0007.b400.0101  local           -
Gi1/0       1    2   -   Listen   0007.b400.0102  193.42.15.2     -
Gi1/0       1    3   -   Listen   0007.b400.0103  193.42.15.3     -
R-42-15-2#
```

Рисунок 3.25 – Перевірка роботи GLBP на R-42-15-2

```
R-42-15-3#show glbp
GigabitEthernet1/0 - Group 1
  State is Standby
    1 state change, last state change 00:11:07
  Virtual IP address is 193.42.15.254
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 0.864 secs
  Redirect time 1200 sec, forwarder timeout 14400 sec
  Preemption enabled, min delay 30 sec
  Active is 193.42.15.1, priority 110 (expires in 14.560 sec)
  Standby is local
  Priority 105 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ca02.68a8.001c (193.42.15.1)
    ca03.0a80.001c (193.42.15.2) local
    ca04.5fcc.001c (193.42.15.3)
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Listen
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is ca02.68a8.001c
    Time to live: 14399.552 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.1 (primary), weighting 100 (expires in 15.424 sec)
  Forwarder 2
    State is Active
      1 state change, last state change 00:11:13
    MAC address is 0007.b400.0102 (default)
    Owner ID is ca03.0a80.001c
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 3
    State is Listen
    MAC address is 0007.b400.0103 (learnt)
    Owner ID is ca04.5fcc.001c
    Time to live: 14398.528 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.3 (primary), weighting 100 (expires in 16.288 sec)
R-42-15-3#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
r
Gi1/0       1    -   105 Standby  193.42.15.254   193.42.15.1     local
Gi1/0       1    1   -   Listen   0007.b400.0101  193.42.15.1     -
Gi1/0       1    2   -   Active   0007.b400.0102  local           -
Gi1/0       1    3   -   Listen   0007.b400.0103  193.42.15.3     -
R-42-15-3#
```

Рисунок 3.26 – Перевірка роботи GLBP на R-42-15-3

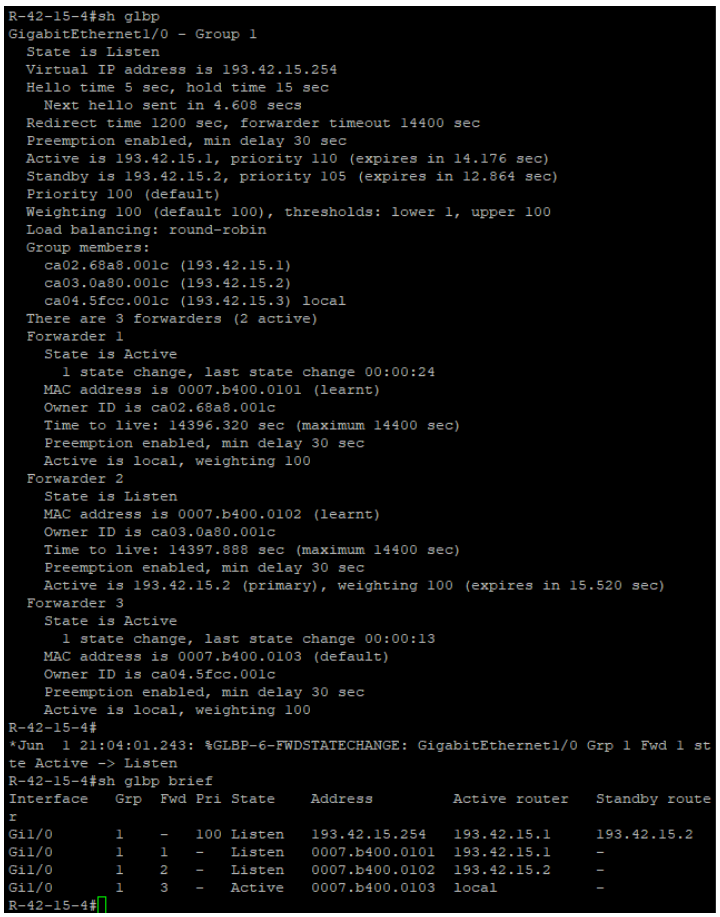


Рисунок 3.27 – Перевірка роботи GLBP на R-42-15-4

Після завершення налаштування протоколу GLBP та перевірки його функціонування за допомогою команд show glbp і show glbp brief було підтверджено коректну роботу механізму резервування шлюзу та балансування навантаження. Аналіз отриманих результатів показав, що маршрутизатори R-42-15-2, R-42-15-3 та R-42-15-4 об'єднані в одну GLBP-групу з номером 1, яка використовує спільну віртуальну IP-адресу 193.42.15.254. Саме ця адреса виступає шлюзом за замовчуванням для клієнтів мережі, забезпечуючи безперервний доступ до мережевих ресурсів навіть у разі відмови одного з маршрутизаторів.

Відповідно до налаштованих значень пріоритету, маршрутизатор R-42-15-2 з пріоритетом 110 був обраний активним віртуальним шлюзом. Його основним завданням є керування групою та розподіл віртуальних MAC-адрес між учасниками GLBP. Кожен маршрутизатор групи виконує роль AVF, маючи власну віртуальну MAC-адресу для обробки мережевого трафіку. Результати виконання команди show glbp підтверджують створення трьох активних forwarder'ів, готових до передачі пакетів.

Для розподілу навантаження використовується алгоритм round-robin. У цьому режимі кожен новий ARP-запит до віртуальної IP-адреси отримує відповідь від іншого forwarder'a групи. Внаслідок цього мережеві вузли послідовно отримують різні віртуальні MAC-адреси, що належать маршрутизаторам R-42-15-2, R-42-15-3 та R-42-15-4. Такий механізм дозволяє рівномірно розподіляти мережевий трафік між усіма шлюзами групи та ефективніше використовувати доступні ресурси мережевої інфраструктури.

Додатково для забезпечення швидкого виявлення змін у топології були налаштовані таймери Hello та Hold зі значеннями 5 і 15 секунд відповідно. Це дозволяє маршрутизаторам оперативно визначати втрату зв'язку з іншими учасниками групи та своєчасно реагувати на відмови. Також активовано механізм preemption із затримкою 30 секунд, завдяки якому маршрутизатор із вищим пріоритетом автоматично відновлює свою роль після повернення до роботи. Використання зазначених механізмів підвищує відмовостійкість, надійність і стабільність функціонування мережі.

Налаштування NAT на R-42-15-1:

```
R-42-15-1#conf t
R-42-15-1(config)#int gig4/0
R-42-15-1(config-if)#ip nat outside
R-42-15-1(config-if)#ip address dhcp
R-42-15-1(config-if)#exit
R-42-15-1(config)#int range gig0/0, gig1/0, gig2/0
R-42-15-1(config-if-range)#ip nat inside
R-42-15-1(config-if-range)#exit
R-42-15-1(config)#access-list 1 permit any
R-42-15-1(config)#ip nat inside source list 1 interface gig4/0 overload
R-42-15-1(config)#exit
```

```
R-42-15-1#show ip nat statistics
*Jun  3 22:23:15.979: %SYS-5-CONFIG_I: Configured from console by console
R-42-15-1#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  GigabitEthernet4/0
Inside interfaces:
  GigabitEthernet0/0, GigabitEthernet1/0, GigabitEthernet2/0
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface GigabitEthernet4/0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Рисунок 3.28 – Перевірка роботи GLBP на R-42-15-1

```
R-42-15-1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/60 ms
```

Рисунок 3.29 – Перевірка зв’язку з www.google.com

Для забезпечення доступу вузлів внутрішньої мережі до зовнішніх ресурсів на маршрутизаторі R-42-15-1 було реалізовано механізм трансляції мережевих адрес NAT. Як зовнішній інтерфейс використовується GigabitEthernet4/0, який позначений як ip nat outside та отримує IP-адресу автоматично від провайдера за допомогою DHCP. Інтерфейси GigabitEthernet0/0, GigabitEthernet1/0 і GigabitEthernet2/0 налаштовані як внутрішні (ip nat inside), що дозволяє виконувати трансляцію адрес для всіх підключених сегментів корпоративної мережі.

Для економії адресного простору та забезпечення одночасного доступу багатьох користувачів до мережі Інтернет було використано технологію PAT. Налаштування виконано за допомогою команди ip nat inside source list 1 interface gig4/0 overload, яка дозволяє всім внутрішнім вузлам використовувати одну зовнішню IP-адресу з розрізненням сеансів за номерами портів. Застосування списку доступу ACL 1 забезпечує включення до трансляції всього внутрішнього трафіку, що сприяє ефективному використанню доступних мережевих ресурсів.

З метою підвищення рівня захисту шлюзової інфраструктури було налаштовано механізм автентифікації протоколу GLBP. Усі маршрутизатори, які входять до складу GLBP-групи (R-42-15-2, R-42-15-3 та R-42-15-4), використовують MD5-автентифікацію з єдиним ключем безпеки. Завдяки перевірці достовірності службових повідомлень GLBP значно знижується ймовірність успішного виконання атак, пов'язаних із підміною мережевих повідомлень або навмисним порушенням роботи протоколу.

Додатково було реалізовано механізм контролю працездатності маршрутизаторів на основі вагових коефіцієнтів. Початкове значення ваги встановлено на рівні 110, верхній поріг відновлення становить 105, а нижній поріг спрацювання – 95. Таке налаштування дозволяє автоматично визначати здатність маршрутизатора виконувати функції AVF та своєчасно виключати його з процесу балансування навантаження у випадку деградації мережевих ресурсів.

Для моніторингу стану критичних каналів зв'язку використовується механізм track, який відстежує працездатність інтерфейсу GigabitEthernet0/0. У разі втрати з'єднання вага маршрутизатора автоматично зменшується на задану величину. Якщо значення ваги опускається нижче встановленого порогу, маршрутизатор припиняє виконувати функції AVF, а обробка трафіку передається іншому учаснику групи. Після відновлення працездатності інтерфейсу значення ваги повертається до початкового рівня, і маршрутизатор автоматично повертається до процесу балансування навантаження.

Для додаткового захисту службових повідомлень GLBP було застосовано розширений список контролю доступу ACL 100. Його правила дозволяють приймати повідомлення протоколу лише від довірених маршрутизаторів групи, пропускають необхідний мультикаст-трафік GLBP, блокують усі сторонні UDP-пакети, адресовані на порт 3222, із веденням журналу подій, а також дозволяють передачу решти IP-трафіку без обмежень.

Реалізація автентифікації, контролю стану інтерфейсів та фільтрації службового трафіку у поєднанні з можливостями GLBP забезпечує високий рівень відмовостійкості та безпеки мережевої інфраструктури. Завдяки цьому мережа

зберігає працездатність навіть у разі відмови окремих пристроїв або спроб несанкціонованого втручання в роботу шлюзового протоколу.

Налаштування механізмів захисту на R-42-15-2:

```
R-42-15-2#conf t
R-42-15-2(config)#int gig1/0
R-42-15-2(config-if)#glbp 1 authentication md5 key-string glbpSECUREkey!
R-42-15-2(config-if)#glbp 1 weighting 110 lower 95 upper 105
R-42-15-2(config-if)#glbp 1 weighting track 1 decrement 10
R-42-15-2(config-if)#exit
R-42-15-2(config)#track 1 interface gig0/0 line-protocol
R-42-15-2(config-track)#exit
R-42-15-2(config)#access-list 100 permit udp host 193.42.15.3 host 193.42.15.2 eq 3222
R-42-15-2(config)#access-list 100 permit udp host 193.42.15.4 host 193.42.15.2 eq 3222
R-42-15-2(config)#access-list 100 permit udp any eq 3222 host 224.0.0.102 eq 3222
R-42-15-2(config)#access-list 100 deny   udp any any eq 3222 log
R-42-15-2(config)#access-list 100 permit ip any any
R-42-15-2(config)#exit
R-42-15-2(config)#int gig1/0
R-42-15-2(config-if)#ip access-group 100 in
R-42-15-2(config-if)#exit
```

Аналогічним чином виконано налаштування на R-42-15-3 та R-42-15-4.

```
R-42-15-2#show glbp
GigabitEthernet1/0 - Group 1
  State is Active
    1 state change, last state change 01:28:38
  Virtual IP address is 193.42.15.254
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 4.480 secs
  Redirect time 1200 sec, forwarder timeout 14400 sec
  Authentication MD5, key-string
  Preemption enabled, min delay 30 sec
  Active is local
  Standby is 193.42.15.2, priority 105 (expires in 11.488 sec)
  Priority 110 (configured)
  Weighting 110 (configured 110), thresholds: lower 95, upper 105
    Track object 1 state Up decrement 10
  Load balancing: round-robin
  Group members:
    ca02.68a8.001c (193.42.15.1) local
    ca03.0a80.001c (193.42.15.2) authenticated
    ca04.5fcc.001c (193.42.15.3) authenticated
  There are 3 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 01:27:50
    MAC address is 0007.b400.0101 (default)
    Owner ID is ca02.68a8.001c
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 110
    Client selection count: 2
  Forwarder 2
    State is Listen
      6 state changes, last state change 00:17:23
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is ca04.5fcc.001c
    Redirection enabled, 1199.328 sec remaining (maximum 1200 sec)
    Time to live: 14399.328 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.3 (primary), weighting 110 (expires in 15.648 sec)
    Client selection count: 2
  Forwarder 3
    State is Listen
      4 state changes, last state change 00:17:23
    MAC address is 0007.b400.0103 (learnt)
    Owner ID is ca03.0a80.001c
    Redirection enabled, 1196.512 sec remaining (maximum 1200 sec)
    Time to live: 14396.512 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 193.42.15.2 (primary), weighting 110 (expires in 12.576 sec)
    Client selection count: 2
R-42-15-2#
```

Рисунок 3.30 – Перевірка налаштувань автентифікації та вагових значенн на R-42-15-2

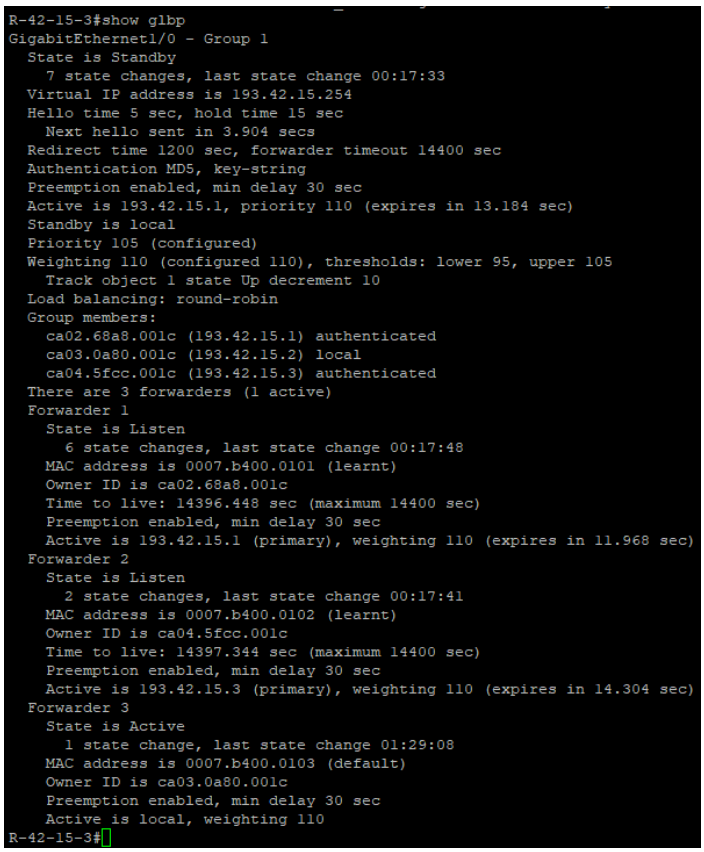


Рисунок 3.31 – Перевірка налаштувань автентифікації та вагових значенн на R-42-15-3

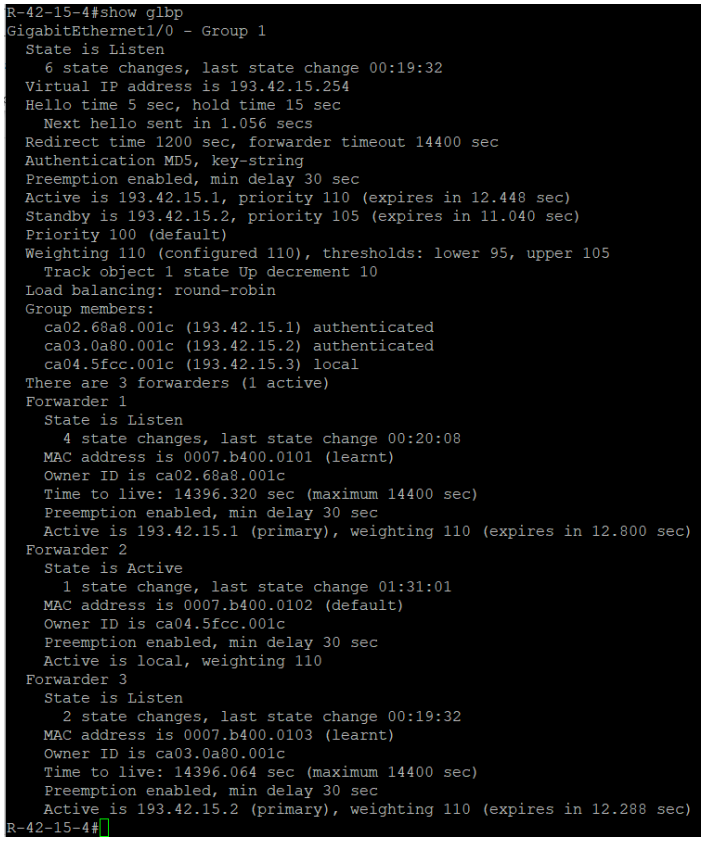


Рисунок 3.32 – Перевірка налаштувань автентифікації та вагових значенн на R-42-15-4

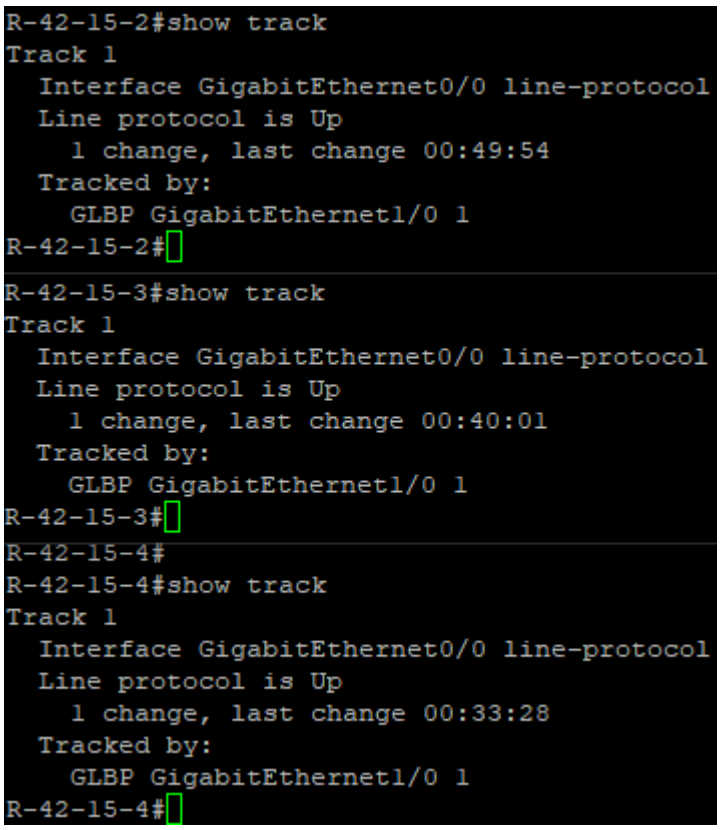


Рисунок 3.33 – Відображення поточного стану об'єктів, за якими здійснюється стеження

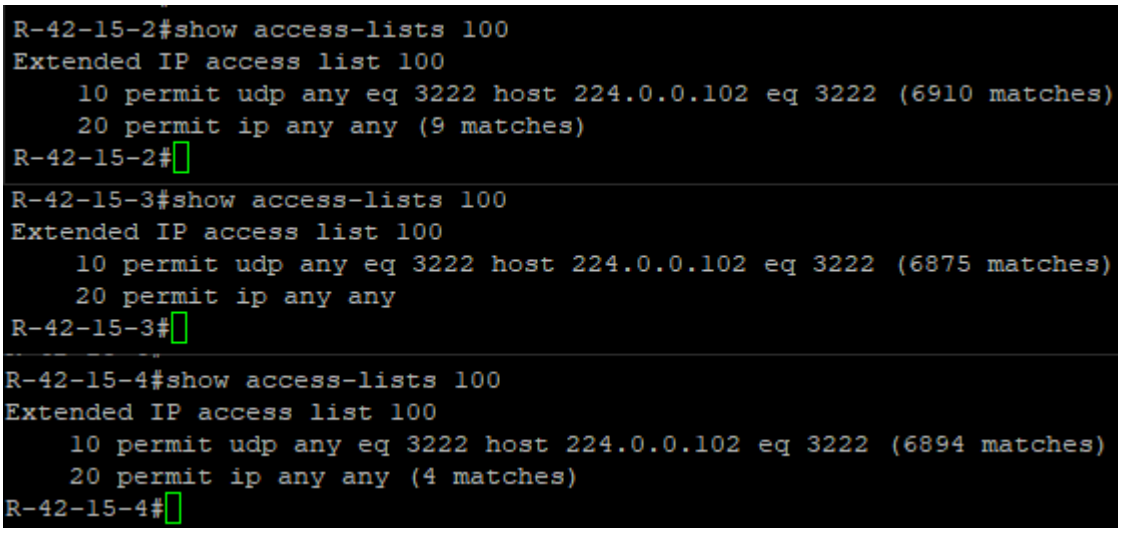


Рисунок 3.34– Перегляд вмісту налаштованих списків контролю доступу

У межах підвищення рівня безпеки мережевої інфраструктури була реалізована конфігурація безпечного віддаленого доступу до маршрутизаторів за допомогою протоколу SSH. Цей протокол забезпечує захищене шифрування переданої інформації, що суттєво знижує ризики перехоплення облікових даних або інших чутливих даних під час адміністрування пристроїв.

Для кожного маршрутизатора спочатку було задано доменне ім’я prikhodko.net, яке використовується під час генерації криптографічних ключів. Після цього створювалася пара RSA-ключів довжиною 1024 біти. Ці ключі необхідні для встановлення захищеного SSH-з'єднання. У результаті кожен маршрутизатор отримав унікальне ім’я ключа, сформоване на основі його імені та вказаного домену.

Далі було створено обліковий запис користувача з іменем admin і паролем, зашифрованим за допомогою механізму secret, що забезпечує вищий рівень захисту порівняно зі звичайним password. Для шифрування всіх паролів у конфігураціях було активовано сервіс service password-encryption.

Для віртуальних термінальних ліній (vty 0–4) було вказано, що доступ до маршрутизатора дозволений лише через SSH-протокол, а також налаштовано автентифікацію за локальними обліковими даними. Це виключає можливість підключення через незахищені протоколи, як-от Telnet, і гарантує, що всі сеанси адміністрування виконуються у зашифрованому вигляді.

Налаштування механізму віддаленого підключення на R-42-15-1:

```
R-42-15-1#conf t
R-42-15-1(config)#ip domain-name prikhodko.net
R-42-15-1(config)#crypto key generate rsa
The name for the keys will be: R-42-15-1.prikhodko.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
R-42-15-1(config)#username admin secret adminpass
R-42-15-1(config)#ip ssh version 2
R-42-15-1(config)#line vty 0 4
R-42-15-1(config-line)#login local
R-42-15-1(config-line)#transport input ssh
R-42-15-1(config-line)#exit
R-42-15-1(config)#service password-encryption
*Jun  4 17:00:30.755: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-42-15-1(config)#service password-encryption
R-42-15-1(config)#exit
```

Для маршрутизаторів R-42-15-2, R-42-15-3 та R-42-15-4 налаштування механізму віддаленого підключення за допомогою SSH виконувалося аналогічним чином.

Фінальним етапом створення тестового середовища стала підготовка та інтеграція цільових операційних систем у мережеву топологію. Для імітації реальної IT-інфраструктури компанії було використано гіпервізор VirtualBox, де створено чотири унікальні віртуальні машини з відповідними апаратними налаштуваннями. Мережеві адаптери кожної машини були переведені у режим непідключеного кабелю для подальшого програмного об'єднання їх безпосередньо через інтерфейс платформи GNS3.

В якості типової клієнтської системи використано операційну систему Windows 10 Pro. Вона імітує звичайне робоче місце співробітника корпоративної мережі. Для стабільної роботи графічного інтерфейсу системі виділено 4 гігабайти оперативної пам'яті та створено динамічний жорсткий диск. З метою демонстрації ефективності роботи сканера безпеки систему було свідомо встановлено у базовій комплектації, а службу автоматичного завантаження оновлень повністю деактивовано.

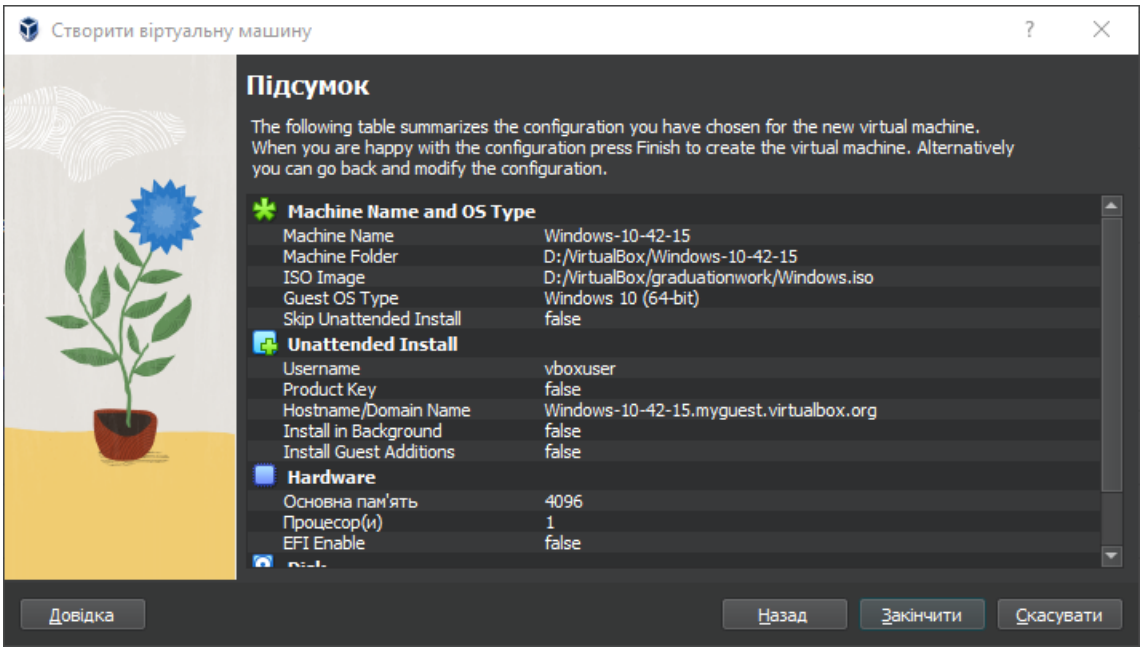


Рисунок 3.35 – Підсумкові апаратні налаштування віртуальної машини Windows 10 Pro

Серверну частину інфраструктури представляє Ubuntu Server актуальної версії. Ця операційна система функціонує без графічної оболонки та виконує роль корпоративного вебсервера, що дозволило оптимізувати споживання апаратних ресурсів і виділити для її роботи 2 гігабайти оперативної пам'яті.

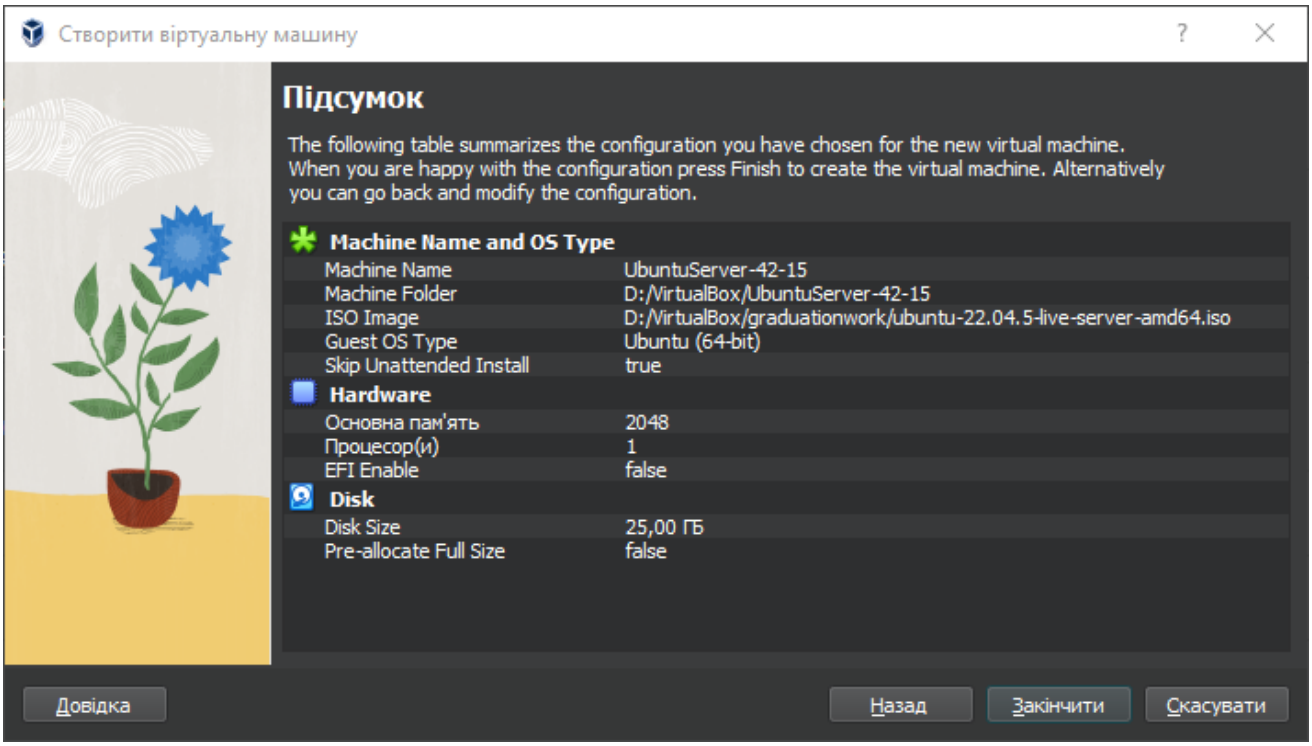


Рисунок 3.36 – Підсумкові апаратні налаштування віртуальної машини Ubuntu Server

Останнім компонентом є спеціалізована система Metasploitable 2. Це навмисно вразлива операційна система на базі ядра Linux, яка використовується як еталонна ціль для перевірки повноти виявлення критичних недоліків мережевого захисту. Оскільки система базується на дуже легкій архітектурі, для її повноцінного функціонування виявилося достатньо 1 гігабайта оперативної пам'яті.

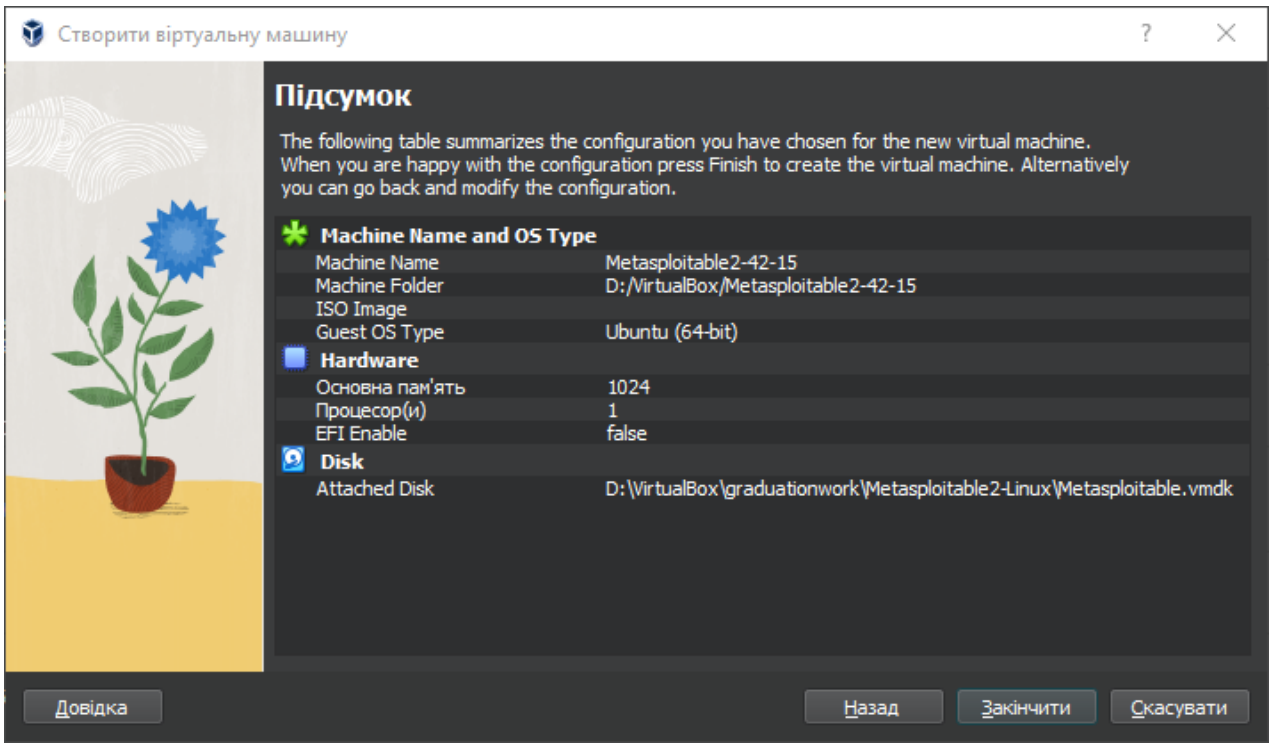


Рисунок 3.37 – Підсумкові апаратні налаштування віртуальної машини Metasploitable 2

3.3. Налаштування та проведення сканування ІТ-інфраструктури

Після розгортання тестового середовища, описаного у попередньому підрозділі, усі вузли мережі автоматично отримали мережеві адреси від DHCP-сервера, налаштованого на маршрутизаторі корпоративної мережі. Було зафіксовано наступний розподіл адрес у підмережі 193.42.15.0/24: сканер безпеки Kali Linux (OpenVAS) – 193.42.15.25, цільовий сервер Ubuntu Server – 193.42.15.21, вразлива система Metasploitable 2 – 193.42.15.22, робоча станція Windows 10 – 193.42.15.27, віртуальний шлюз GLBP – 193.42.15.254. Коректність отриманих адрес було підтверджено за допомогою стандартних системних утиліт: команди ip a на Linux-системах та ipconfig на робочій станції Windows.

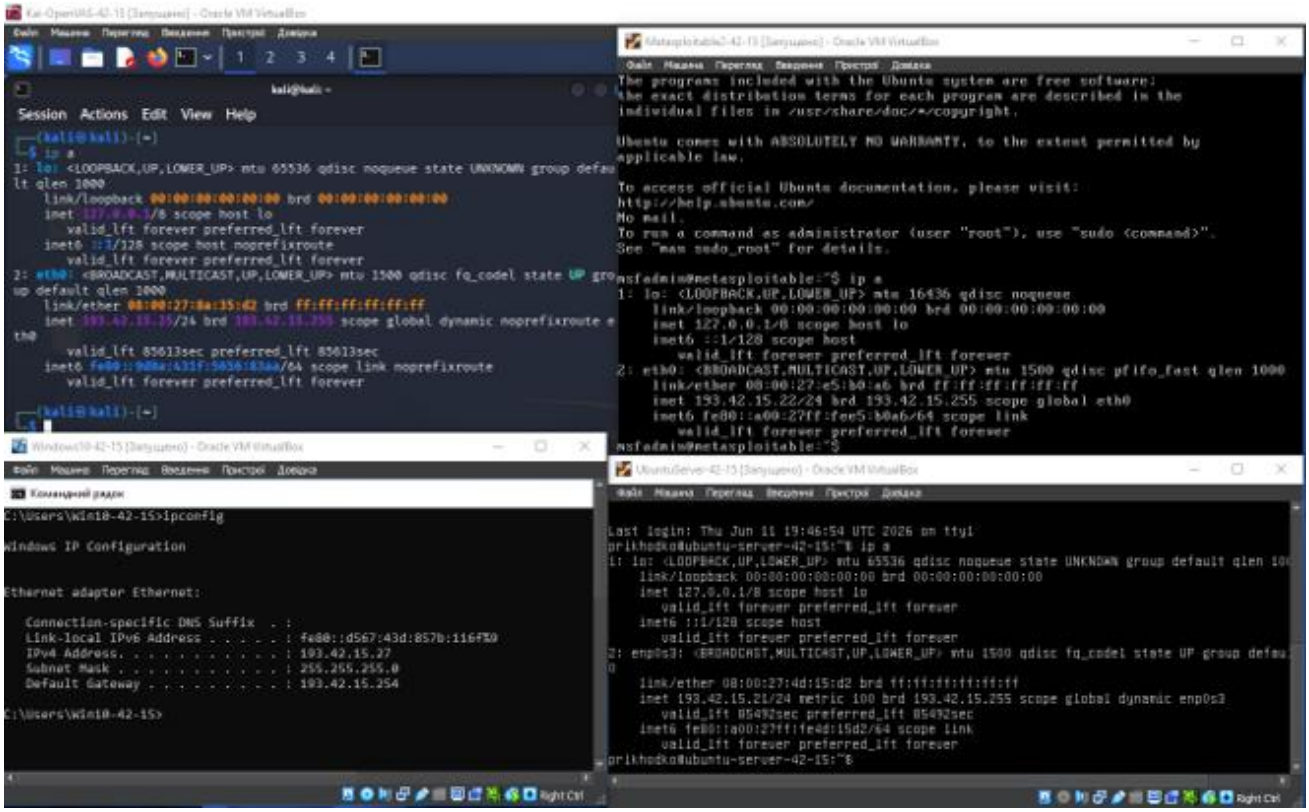


Рисунок 3.38 – Мережеві адреси вузлів тестового середовища, отримані за протоколом DHCP

Перед початком сканування було виконано верифікацію мережевої зв'язності між сканером безпеки та кожним із цільових вузлів за допомогою ICMP-запитів. Результати тестування підтвердили повну доступність усіх вузлів тестового середовища зі сканера: шлюз 193.42.15.254, Metasploitable 2 (193.42.15.22), Ubuntu Server (193.42.15.21) та Windows 10 (193.42.15.27) – усі відповіли без втрат пакетів (0% packet loss). Додатково було перевірено наявність зовнішнього з'єднання шляхом надсилання ICMP-запитів до публічного DNS-сервера Google (8.8.8.8), що підтвердило коректну роботу механізму NAT на прикордонному маршрутизаторі та доступність зовнішніх ресурсів мережі Інтернет із тестового середовища. Таким чином, було встановлено повну працездатність мережевої інфраструктури та готовність середовища до проведення аудиту безпеки.

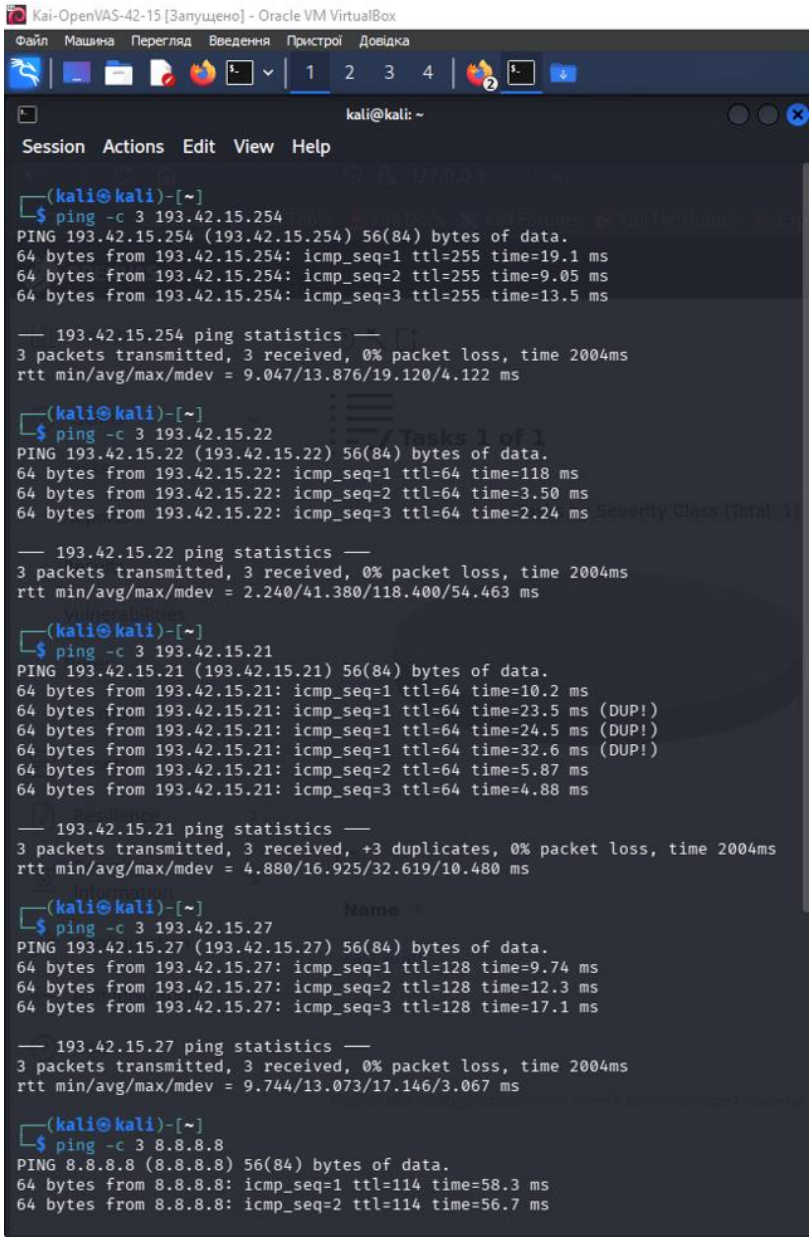


Рисунок 3.39 – Перевірка мережевої зв'язності між сканером та цільовими вузлами за допомогою ICMP-запитів

Для всебічного аналізу захищеності модельованої корпоративної мережі було проведено три послідовних етапи сканування, кожен з яких мав чітко визначену мету, власний набір параметрів та імітував конкретний сценарій реального аудиту безпеки. Усі сканування виконувалися за допомогою сканера OpenVAS Default, який є ядром платформи Greenbone і забезпечує автоматичну перевірку вузлів мережі на відповідність понад 60 000 тестів мережевих вразливостей NVT.

Для всіх трьох етапів було обрано конфігурацію сканування “Full and fast” – стандартний і рекомендований розробниками профіль, який виконує повний набір

перевірок безпеки з оптимізацією швидкості. Цей профіль включає всі доступні NVT-модулі, але виключає потенційно деструктивні тести (DoS), що могли б порушити стабільність роботи вузлів тестового середовища. Вибір саме цього профілю обумовлений тим, що він забезпечує максимальне покриття вразливостей при мінімальному ризику для інфраструктури, що є критично важливим при проведенні аудиту в корпоративних мережах, де безперервність роботи сервісів є пріоритетом.

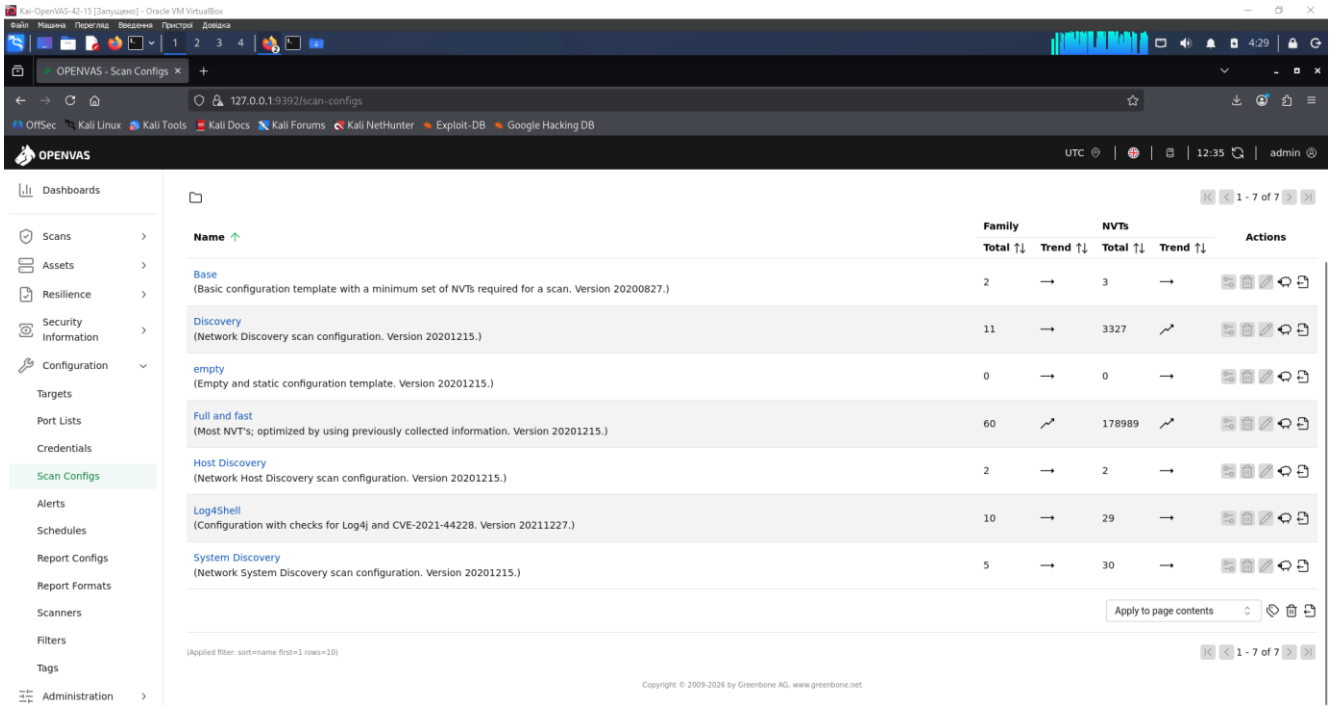


Рисунок 3.40 –Профіль конфігурації сканування “Full and fast”

Як список портів для всіх сканувань було обрано “All IANA assigned TCP” – перелік, що включає всі TCP-порти, офіційно зареєстровані в реєстрі Internet Assigned Numbers Authority. Цей список охоплює приблизно 5000 найбільш поширених портів, що використовуються відомими мережевими сервісами та протоколами (HTTP, SSH, FTP, SMB, RDP, DNS тощо), і є оптимальним компромісом між повнотою сканування та часом його виконання.

Перший етап сканування імітував дії зовнішнього зловмисника або аудитора, який не має жодних облікових даних для доступу до систем і здійснює розвідку виключно “ззовні”, аналізуючи лише ті сервіси та порти, що доступні через мережу. Такий підхід відповідає методології тестування на проникнення за принципом

“чорної скриньки” згідно з рекомендаціями стандарту OWASP Testing Guide та NIST SP 800-115 [11].

У модулі Configuration → Targets було створено ціль під назвою “Fast Target” з наступними параметрами:

1. Hosts (Цільові вузли): 193.42.15.22, 193.42.15.21, 193.42.15.27 – IP-адреси трьох цільових вузлів тестового середовища (Metasploitable 2, Ubuntu Server та Windows 10 відповідно). Адреси було вказано вручну через кому, щоб сканер перевіряв лише конкретні машини, а не витрачав час на порожні адреси у підмережі.
2. Port List (Список портів): All IANA assigned TCP.
3. Alive Test (Метод визначення доступності): було обрано значення “Consider Alive” (вважати вузол доступним). Цей параметр є ключовим для віртуальних середовищ: він інструктує сканер пропустити попередню фазу виявлення вузлів (Host Discovery) і одразу перейти до сканування портів та перевірки вразливостей. У середовищі GNS3, де віртуальні комутатори можуть непередбачувано обробляти масові ICMP- або ARP-запити, такий підхід гарантує, що жоден із цільових вузлів не буде помилково визнаний “недоступним” і пропущений сканером.
4. Credentials (Облікові дані): не використовувались.

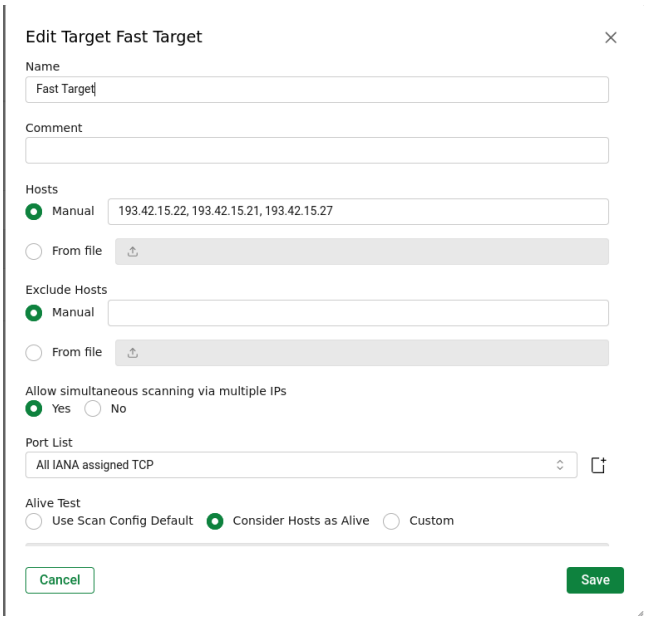


Рисунок 3.41 – Налаштування цілі “Fast Target” для неавтентифікованого сканування

У модулі Scans → Tasks було створено завдання під назвою “Fast Audit” з наступними параметрами:

1. Scan Targets: Fast Target.
2. Scan Config: Full and fast.
3. Scanner: OpenVAS Default.
4. Maximum concurrently executed NVTs per host: 4 – кількість тестів вразливостей, що одночасно виконуються на одному вузлі. Значення 4 забезпечує помірне навантаження на кожну цільову машину.
5. Maximum concurrently scanned hosts: 20 – оскільки цілей лише три, це значення дозволяє сканеру перевіряти всі вузли одночасно, що суттєво скорочує загальний час аудиту.

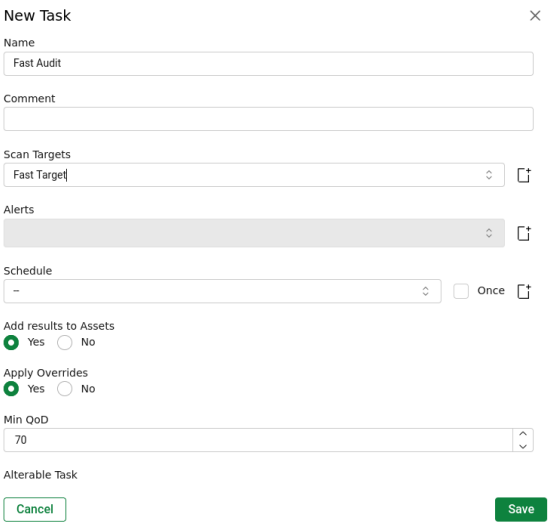


Рисунок 3.42 – Налаштування завдання “Fast Audit”

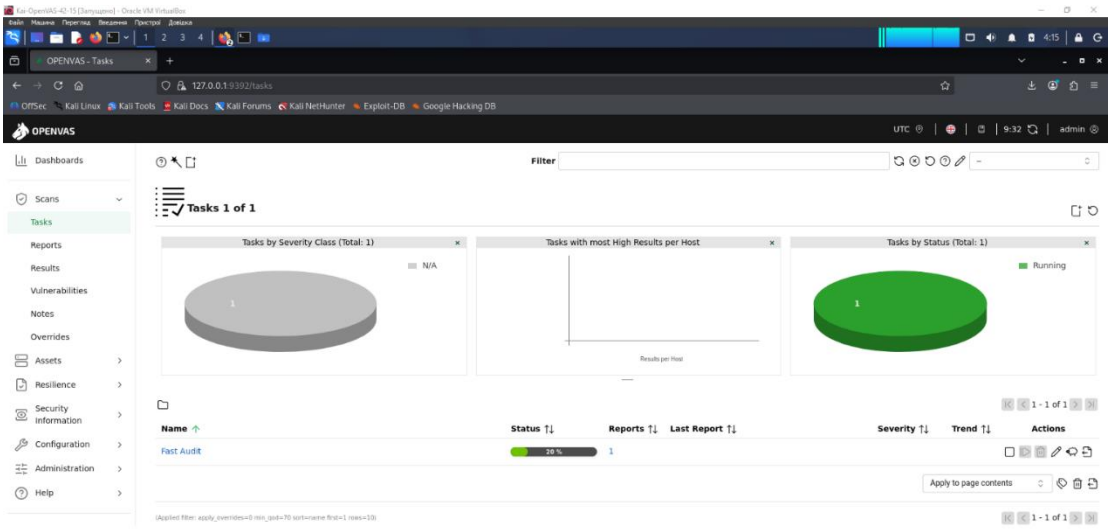


Рисунок 3.43 – Запуск завдання “Fast Audit”

Сканування було розпочато 12 червня 2026 року о 08:12 UTC та успішно завершено о 09:06 UTC (загальна тривалість – приблизно 54 хвилини). За результатами було виявлено 648 записів (до фільтрації, 69 після), з яких: 13 критичних (Critical), 10 високих (High), 39 середніх (Medium) та 7 низьких (Low) вразливостей. Переважна більшість критичних та високих вразливостей була ідентифікована на вузлі Metasploitable 2, що підтверджує його штучно вразливу конфігурацію.

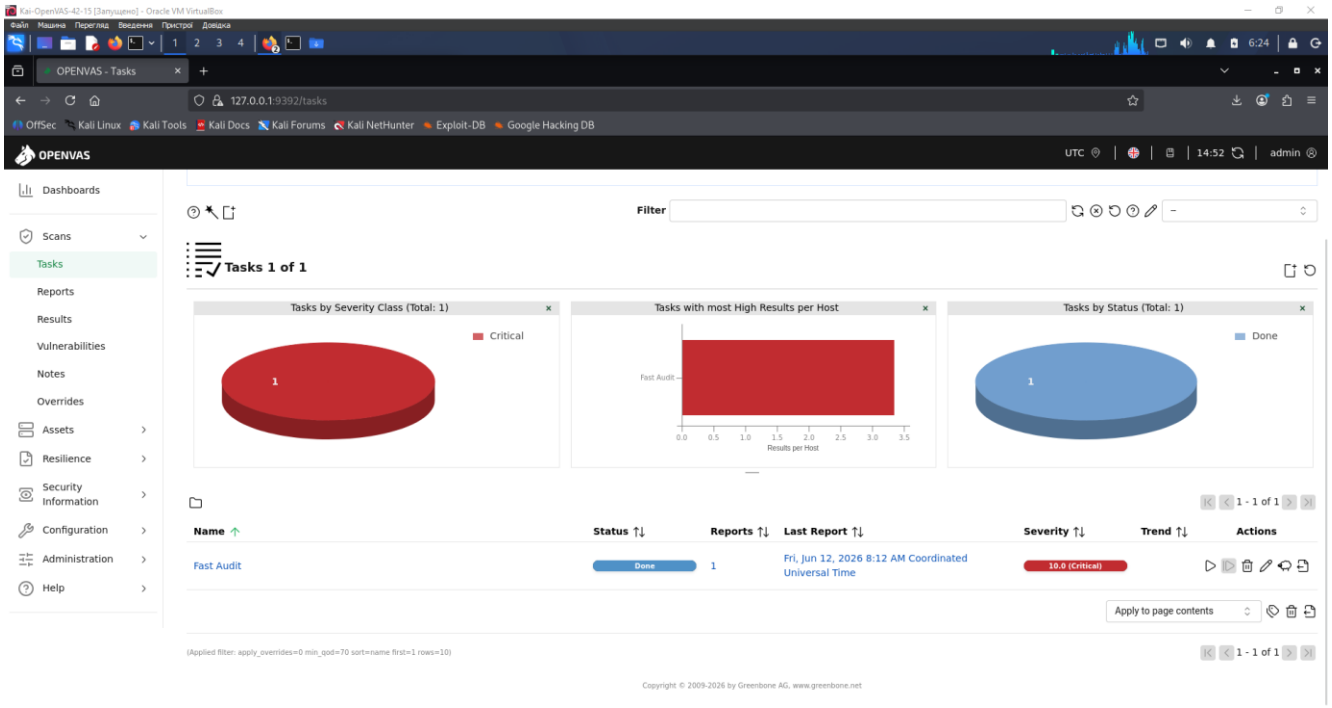


Рисунок 3.44 – Результат завершення сканування “Fast Audit” зі статусом Done

Другий етап сканування імітував сценарій внутрішнього аудиту, при якому аудитор має легітимний доступ до систем із відповідними обліковими даними. Такий підхід відповідає методології “білої скриньки” і дозволяє сканеру не лише аналізувати зовнішні мережеві сервіси, а й увійти всередину операційної системи для перевірки внутрішніх конфігурацій, встановлених пакетів програмного забезпечення, стану оновлень, параметрів реєстру Windows та локальних політик безпеки.

На цьому етапі зі списку цілей було свідомо виключено вузол Metasploitable 2 (193.42.15.22). Причина полягає в тому, що ця система є навчальною платформою зі штучно створеними вразливостями, і проведення автентифікованого сканування для неї не має практичного сенсу – її незахищеність уже була повністю виявлена на

першому етапі. Натомість увага була зосереджена на Ubuntu Server та Windows 10 – типових представниках корпоративної інфраструктури.

Перед налаштуванням цілі було створено два набори облікових даних у модулі Configuration → Credentials:

1. “Linux SSH Access” – тип: Username + Password; логін: prikhodko; протокол: SSH (порт 22). Ці облікові дані призначені для автентифікації на серверах під управлінням Linux за допомогою протоколу SSH, що дозволяє сканеру виконувати команди на віддаленій машині та аналізувати її внутрішній стан.

2. “Windows SMB Password” – тип: Username + Password; логін: Win10-42-15; протокол: SMB (порт 445). Ці облікові дані призначені для автентифікації на робочих станціях під управлінням Windows за допомогою протоколу SMB, що надає сканеру доступ до реєстру Windows, списку встановлених оновлень та конфігурації системних служб.

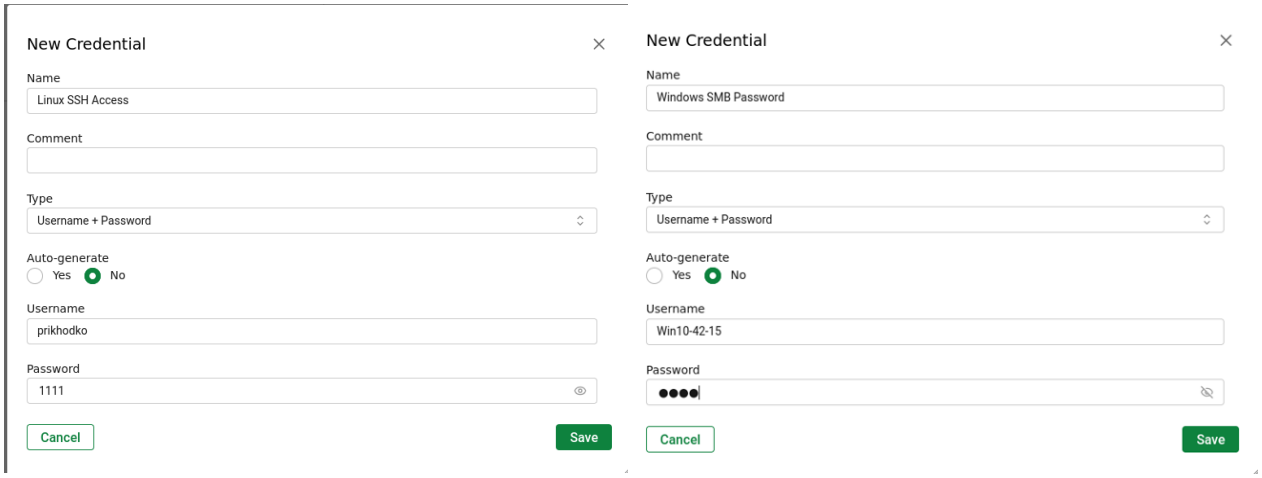


Рисунок 3.45 – Створення облікових даних для автентифікованого доступу

Було створено нову ціль під назвою “Authenticated Target” з наступними параметрами:

1. Hosts: 193.42.15.21, 193.42.15.27 – лише Ubuntu Server та Windows 10.
2. Port List: All IANA assigned TCP.
3. Alive Test: Consider Alive – аналогічно до першого етапу, для уникнення хибних спрацьовувань у віртуальному середовищі.
4. Credentials for Authenticated Checks:
   - SSH: Linux SSH Access – для автентифікації на Ubuntu Server.
   - SMB: Windows SMB Password – для автентифікації на Windows 10.

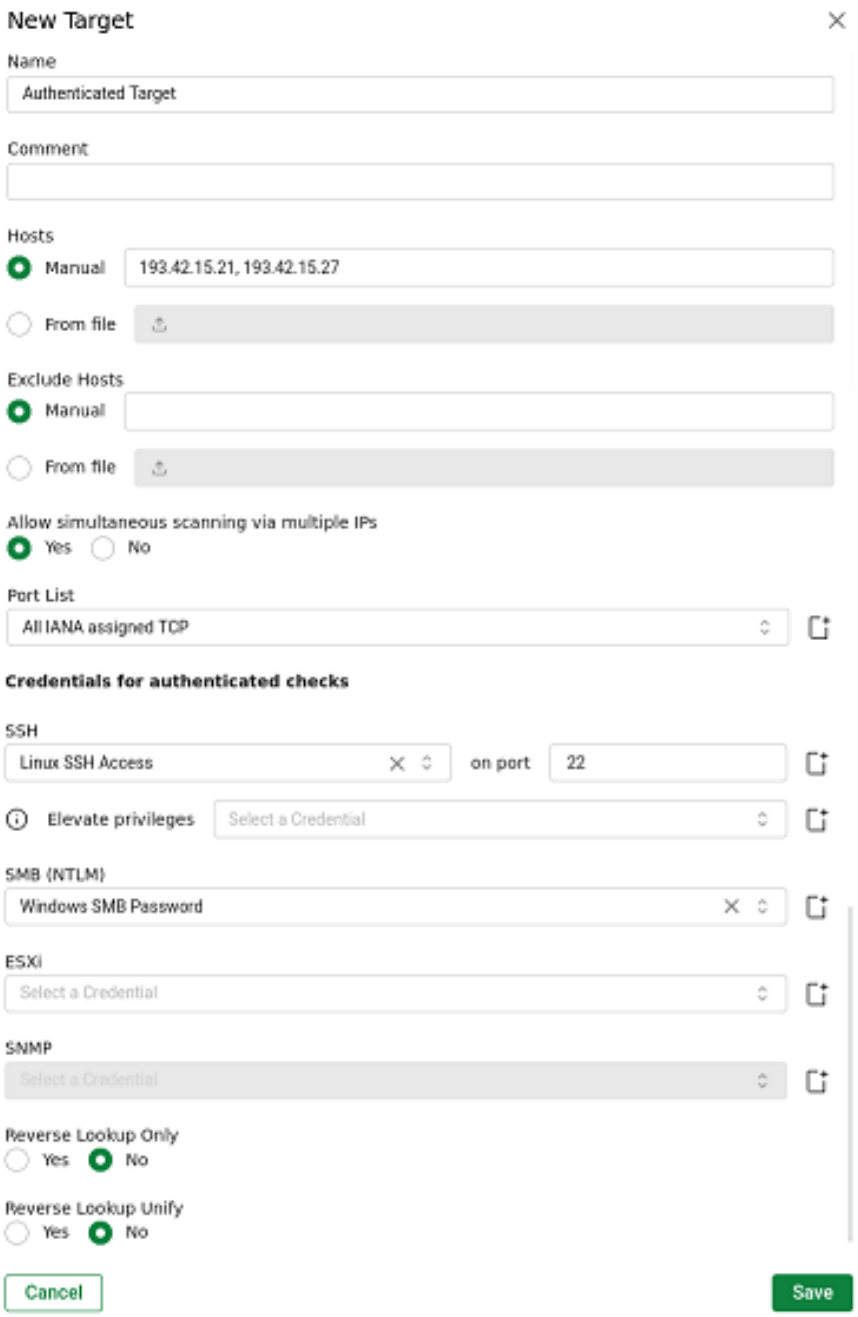


Рисунок 3.46 – Налаштування цілі “Authenticated Target” із прикріпленими обліковими даними

Було створено завдання під назвою “White Box Audit:

1. Scan Targets: Authenticated Target.
2. Scan Config: Full and fast.
3. Scanner: OpenVAS Default.
4. Maximum concurrently executed NVTs per host: 4.
5. Maximum concurrently scanned hosts: 10.

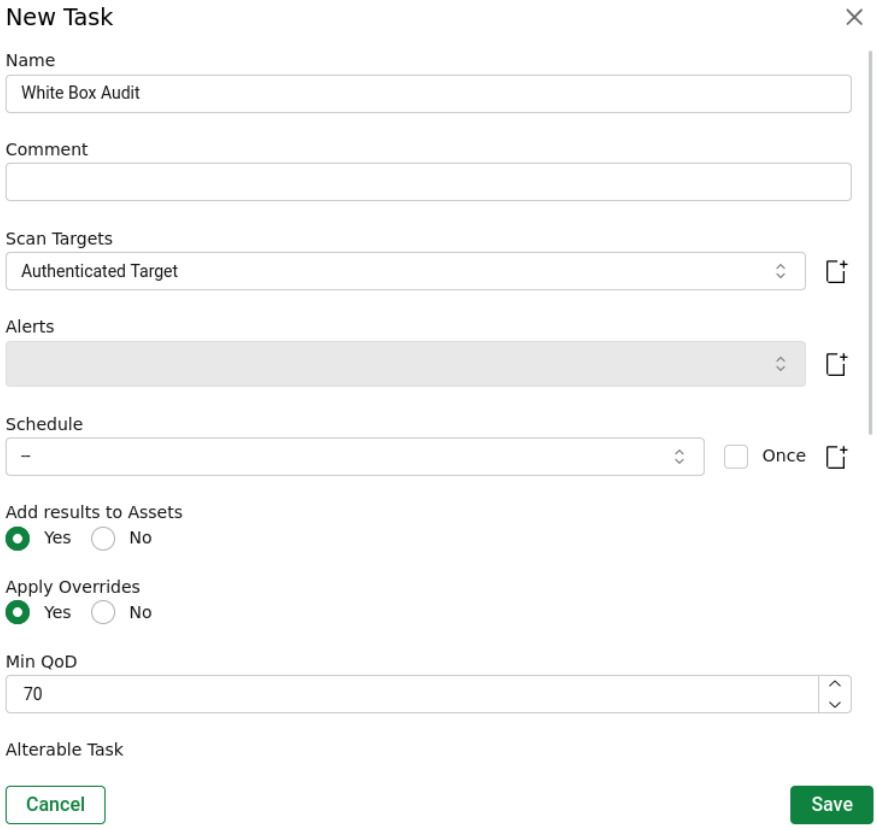


Рисунок 3.47 – Налаштування завдання “White Box Audit”

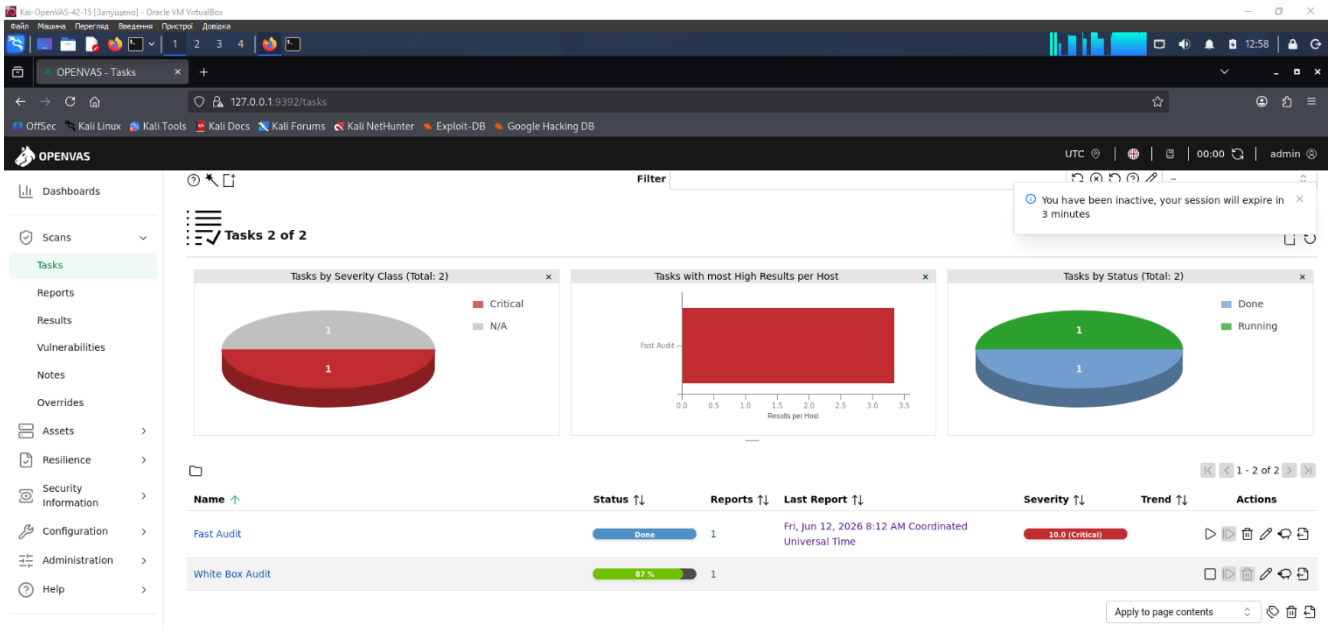


Рисунок 3.48 – Запуск завдання “White Box Audit”

Сканування було розпочато о 17:41 UTC та завершено о 18:31 UTC (загальна тривалість – приблизно 50 хвилин). За результатами було виявлено 214 запис (до фільтрації, 6 після), з яких: 0 критичних, 0 високих, 1 середня (Medium) та 5 низьких (Low) вразливостей. У розділі Host Authentications звіту було зафіксовано успішну

автентифікацію по протоколу SMB на вузлі Windows 10 (SMB: Success), що підтвердило коректність наданих облікових даних та дозволило сканеру виконати глибокий аналіз внутрішнього стану операційної системи. Значно менша кількість виявлених вразливостей порівняно з першим етапом пояснюється тим, що Ubuntu Server та Windows 10, на відміну від Metasploitable 2, є сучасними операційними системами з базовим рівнем захисту, що вже включає вбудований брандмауер та механізми автоматичного оновлення.

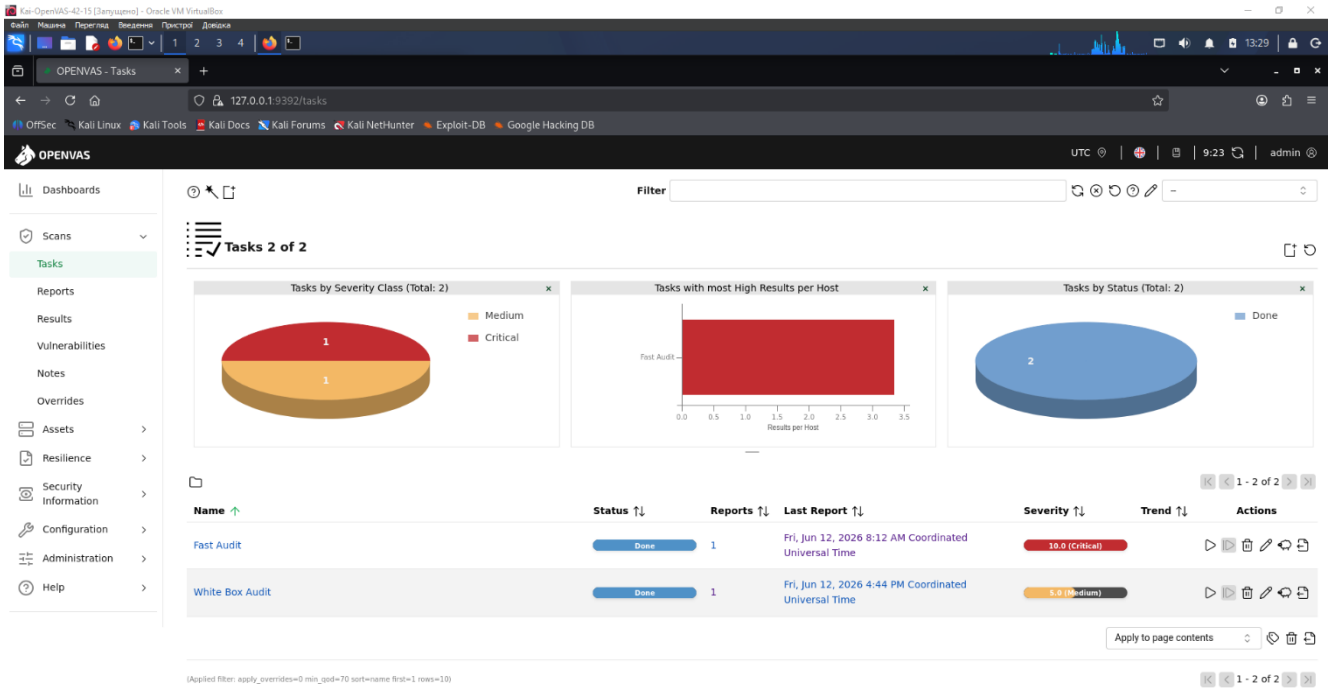


Рисунок 3.49 – Результат завершення сканування “White Box Audit” зі статусом Done

Третій, фінальний етап сканування імітував комплексний аудит усієї корпоративної підмережі, який проводиться при первинному обстеженні IT-інфраструктури підприємства. На відміну від попередніх етапів, де адреси цілей вказувалися вручну, тут сканеру було надано повний діапазон адрес підмережі, щоб він самостійно здійснив виявлення (Discovery) усіх активних вузлів і провів їх повний аудит. Цей сценарій є найбільш реалістичним з точки зору практики корпоративної кібербезпеки, оскільки аудитор часто не має попередньої інформації про повний перелік пристроїв у мережі.

Було створено ціль під назвою “Full Network Scan” з наступними параметрами:

1. Hosts: 193.42.15.0/24 – уся підмережа класу C, що охоплює 254 потенційні адреси вузлів (від 193.42.15.1 до 193.42.15.254).

2. Port List: All IANA assigned TCP.

3. Alive Test: було обрано комбінований метод “ICMP, TCP-ACK Service & ARP Ping”, який є найбільш надійним підходом для виявлення активних вузлів у гетерогенній мережі. Цей метод послідовно застосовує три різні механізми виявлення:

- ARP Ping – надсилає ARP-запити на канальному рівні (L2) моделі OSI, що дозволяє виявити будь-який пристрій у локальному сегменті мережі, навіть якщо він блокує ICMP-пакети або має увімкнений брандмауер;
- ICMP Ping – використовує стандартні ICMP Echo Request пакети (аналог команди ping) для виявлення вузлів на мережевому рівні (L3);
- TCP-ACK Service Ping – відправляє TCP-пакети з прапорцем ACK на стандартні порти сервісів, що дозволяє виявити вузли, які фільтрують ICMP, але мають відкриті TCP-порти.

Використання саме комбінованого методу замість простого ICMP Ping або Consider Alive є критично важливим при скануванні повної підмережі: параметр Consider Alive змусив би сканер виконувати повний аудит усіх 254 адрес, що призвело б до багатогодинного марного очікування таймаутів.

4. Credentials for Authenticated Checks:

- SSH: Linux SSH Access – для автоматичної автентифікації на виявлених Linux-системах.
- SMB (NTLM): Windows SMB Password – для автоматичної автентифікації на виявлених Windows-системах.

Таким чином, третє сканування поєднало в собі можливості обох попередніх етапів: автоматичне виявлення вузлів, зовнішній аналіз портів і сервісів, а також внутрішній автентифікований аудит тих вузлів, до яких сканер зміг отримати доступ за допомогою наданих облікових даних.

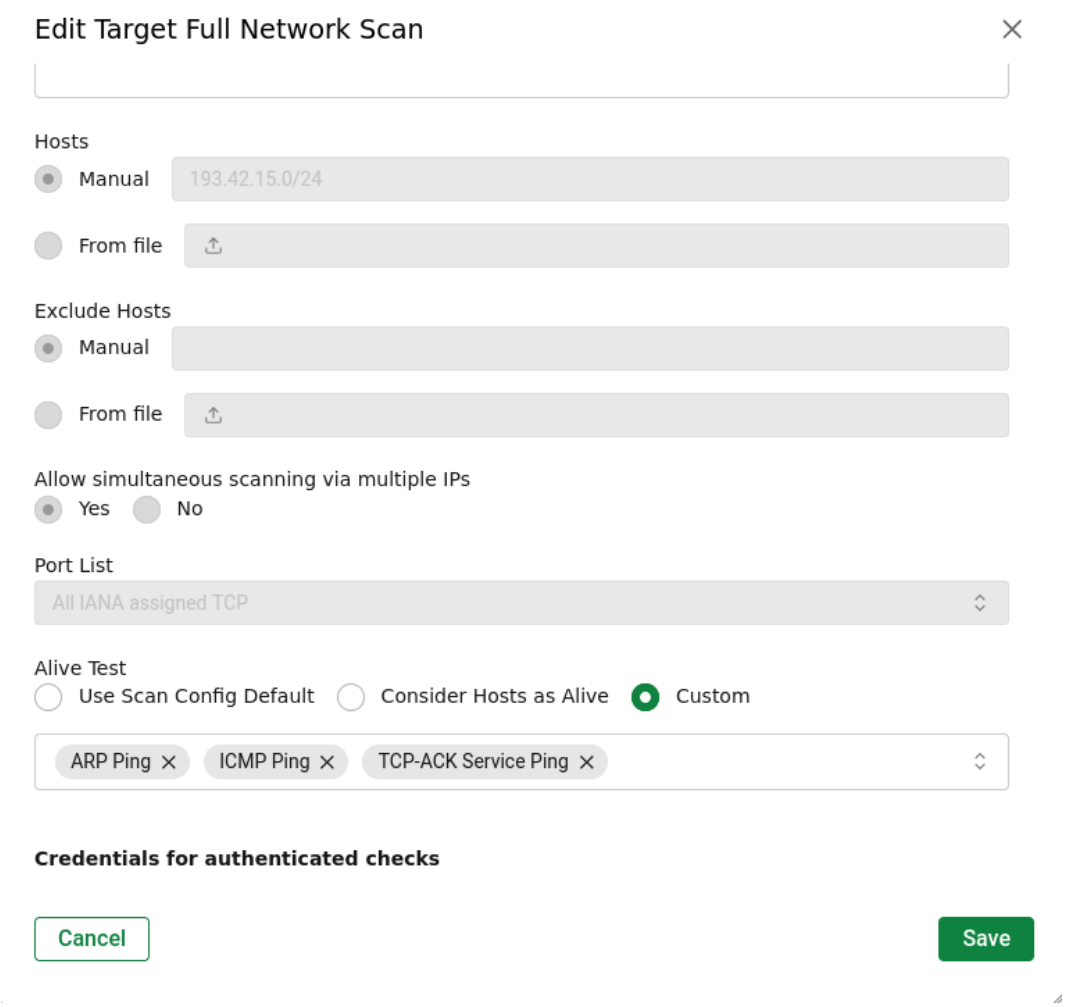


Рисунок 3.50 – Налаштування цілі “Full Network Scan” із зазначенням підмережі та облікових даних

Було створено завдання під назвою “Full Network Audit” зі спеціально оптимізованими параметрами для стабільної роботи у віртуальному середовищі:

1. Scan Targets: Full Network Scan.
2. Scan Config: Full and fast.
3. Scanner: OpenVAS Default.
4. Maximum concurrently executed NVTs per host: 10 – збільшене значення порівняно з попередніми етапами, що дозволяє прискорити аудит кожного окремого вузла за рахунок паралельного виконання більшої кількості перевірок.
5. Maximum concurrently scanned hosts: 2 – це значення було свідомо зменшено з метою обмеження загального обсягу мережевого трафіку, що генерується сканером. У віртуальному середовищі GNS3, де віртуальні комутатори мають обмежений розмір буферів пакетів, надмірне одночасне сканування багатьох

вузлів може призводити до переповнення черг (queue overflow) та втрати пакетів, що, у свою чергу, спричиняє хибні результати або таймаути сканування.

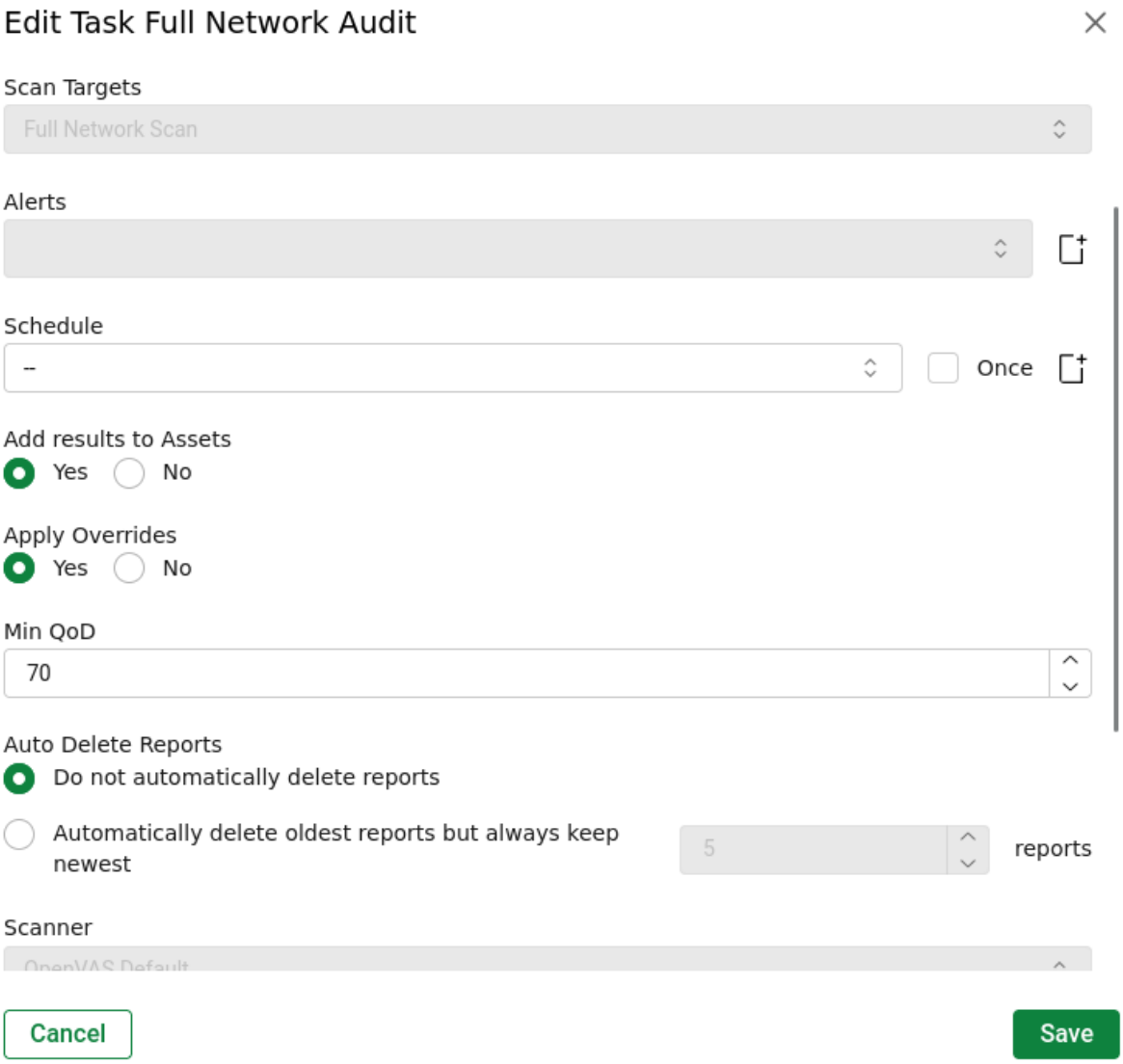


Рисунок 3.51 – Налаштування завдання “Full Network Audit”

Перед запуском сканування на сканері також було виконано оптимізацію мережевого стеку за допомогою команди:

sudo ethtool -K eth0 tx off rx off

Ця команда вимикає апаратне обчислення контрольних сум на мережевому інтерфейсі. У віртуальних середовищах, де мережеві адаптери є програмними емуляціями, функція Checksum Offloading може призводити до генерації пакетів з некоректними контрольними сумами, які будуть відкинуті цільовими вузлами, що негативно впливає на повноту та точність результатів сканування.

Результати виконання. Сканування було розпочато о 19:40 UTC та успішно завершено о 21:00 UTC (загальна тривалість – приблизно 80 хвилин). Збільшена тривалість порівняно з попередніми етапами пояснюється необхідністю попереднього виявлення активних вузлів серед 254 адрес підмережі та обмеженням у 2 одночасно скановані вузли. За результатами було виявлено 919 записів (до фільтрації, 92 після), з яких: 13 критичних (Critical), 10 високих (High), 50 середніх (Medium) та 19 низьких (Low) вразливостей. Сканер успішно виявив усі активні вузли тестового середовища, включаючи мережеве обладнання (маршрутизатор 193.42.15.1), та провів їх повний аудит.

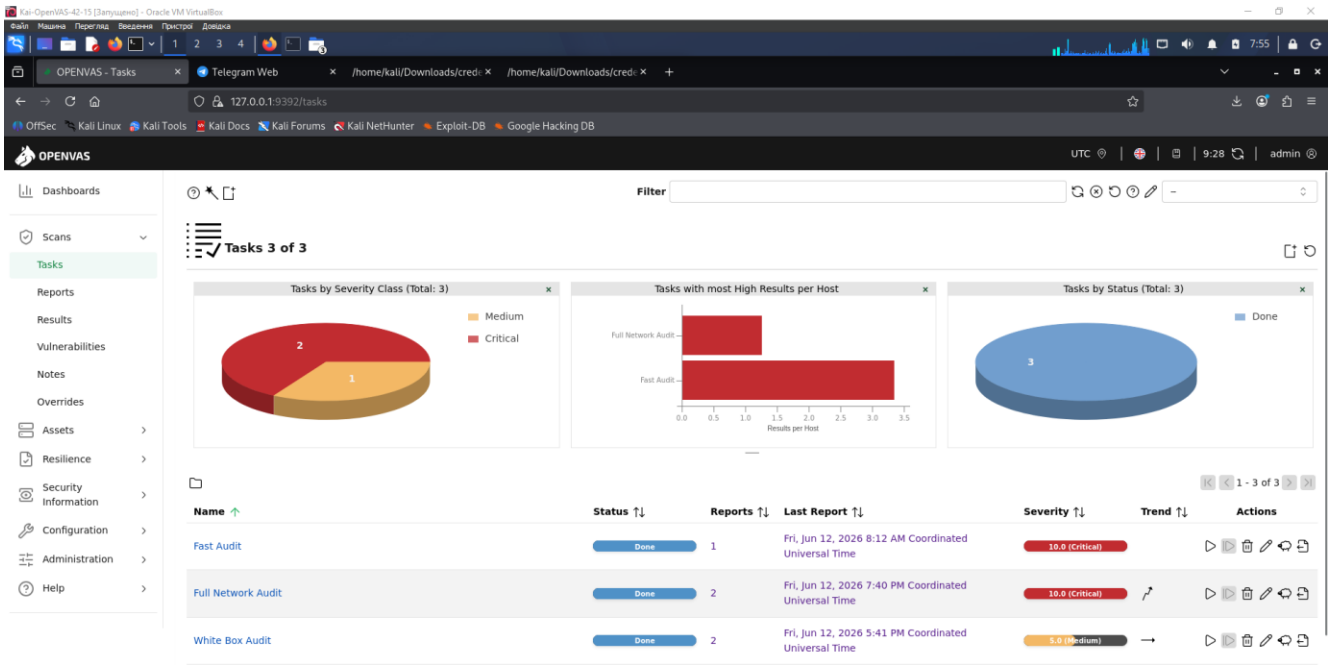


Рисунок 3.52 – Результат завершення сканування “Full Network Audit” зі статусом Done

3.4. Аналіз результатів сканування та оцінка вразливостей

Після успішного завершення всіх трьох етапів сканування за допомогою OpenVAS було отримано масив даних щодо стану захищеності цільової інфраструктури. Аналіз згенерованих звітів дозволив класифікувати виявлені вразливості за рівнем критичності відповідно до шкали CVSS та визначити їхній потенційний вплив на безпеку корпоративної мережі. Кожен із застосованих підходів продемонстрував унікальні результати, що підтверджує необхідність комплексного багаторівневого аудиту інформаційної безпеки.

Цільовими вузлами для сканування виступили три віртуальні машини, інтегровані в мережу доступу для імітації різних типів інфраструктурних елементів та сервісів:

1. Ubuntu Server 22.04 LTS (IP-адреса: 193.42.15.21) – серверна ОС;
2. Metasploitable 2 (IP-адреса: 193.42.15.22) – навмисно вразлива ОС на базі Linux, орієнтована на тестування безпеки;
3. Windows 10 (IP-адреса: 193.42.15.27) – клієнтська ОС без останніх оновлень.
4. Сам сканер Kali OpenVAS був розгорнутий за адресою 193.42.15.25.

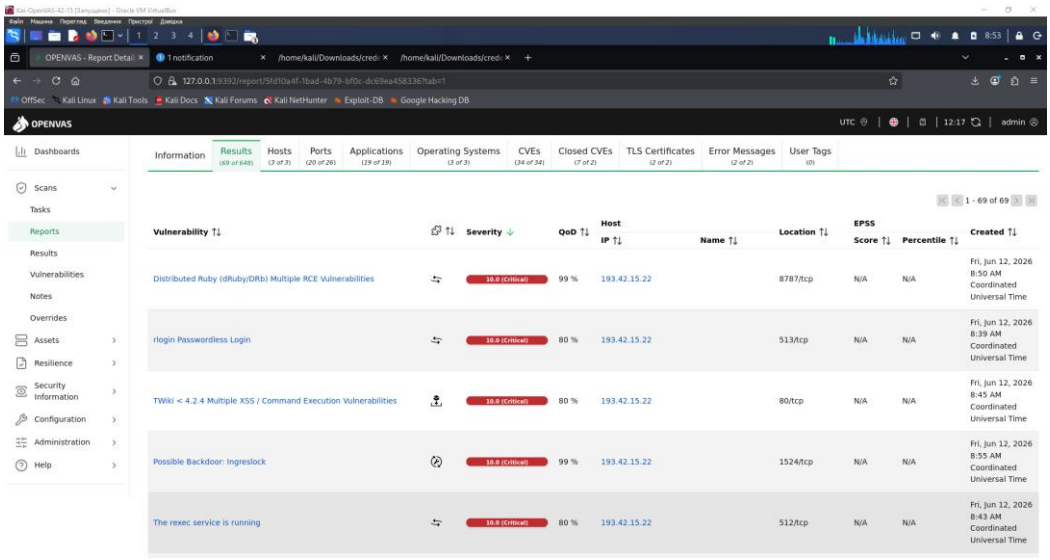


Рисунок 3.53 – Загальний перелік виявлених вразливостей за результатами сканування "Fast Audit"

Сканування тривало близько 54 хвилин (розпочато о 08:12:18 UTC і завершено о 09:06:07 UTC 12 червня 2026 року). Загалом під час аудиту було виявлено 648 результатів, з яких 69 релевантних вразливостей (після фільтрації результатів зі статусами "Log", "Debug", "False Positive" та рівнем точності виявлення QoD нижче 70%).

Результати першого етапу виявилися найбільш показовими для практичної частини дослідження. Зі 69 зафіксованих записів (після застосування фільтру мінімального рівня довіри QoD ≥ 70) на трьох цільових вузлах було знайдено 13 критичних та 10 високих вразливостей.

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	Critical	High	Medium	Low	Log	False Pos.	Tota
193.42.15.22			19	19			Fri, Jun 12, 2026 8:13 AM Coordinated Universal Time	Fri, Jun 12, 2026 9:05 AM Coordinated Universal Time	13	10	38	5	0	0	66
193.42.15.27			1	0			Fri, Jun 12, 2026 8:13 AM Coordinated Universal Time	Fri, Jun 12, 2026 9:03 AM Coordinated Universal Time	0	0	1	1	0	0	2
193.42.15.21			0	0			Fri, Jun 12, 2026 8:13 AM Coordinated Universal Time	Fri, Jun 12, 2026 8:19 AM Coordinated Universal Time	0	0	0	1	0	0	1

Рисунок 3.54 – Розподіл виявлених вразливостей за рівнями критичності для кожного цільового вузла

Абсолютна більшість критичних знахідок зосереджена на вузлі Metasploitable 2 (193.42.15.22), що є прямим наслідком його цільового призначення як навчальної системи з навмисно вразливою конфігурацією. Критичною знахідкою з методологічної точки зору є те, що сканер не просто виявив теоретичні вразливості, а в переважній більшості випадків виконав їхнє активне підтвердження.

Зокрема, на порту 3632/tcp сканер успішно експлуатував вразливість DistCC Remote Code Execution (CVE-2004-2687, CVSS 9.3) і отримав реальний результат виконання системної команди: uid=1(daemon) gid=1(daemon). На порту 5900/tcp сервіс VNC прийняв підключення з паролем password, що є прикладом найгіршої можливої практики – використання тривіальних облікових даних. Служба PostgreSQL на порту 5432/tcp дозволила автентифікацію від імені привілейованого користувача postgres з однойменним паролем postgres. Аналогічно, через FTP-сервер на портах 21/tcp та 2121/tcp сканер підібрав кілька пар стандартних облікових даних: msfadmin:msfadmin, service:service, user:user.

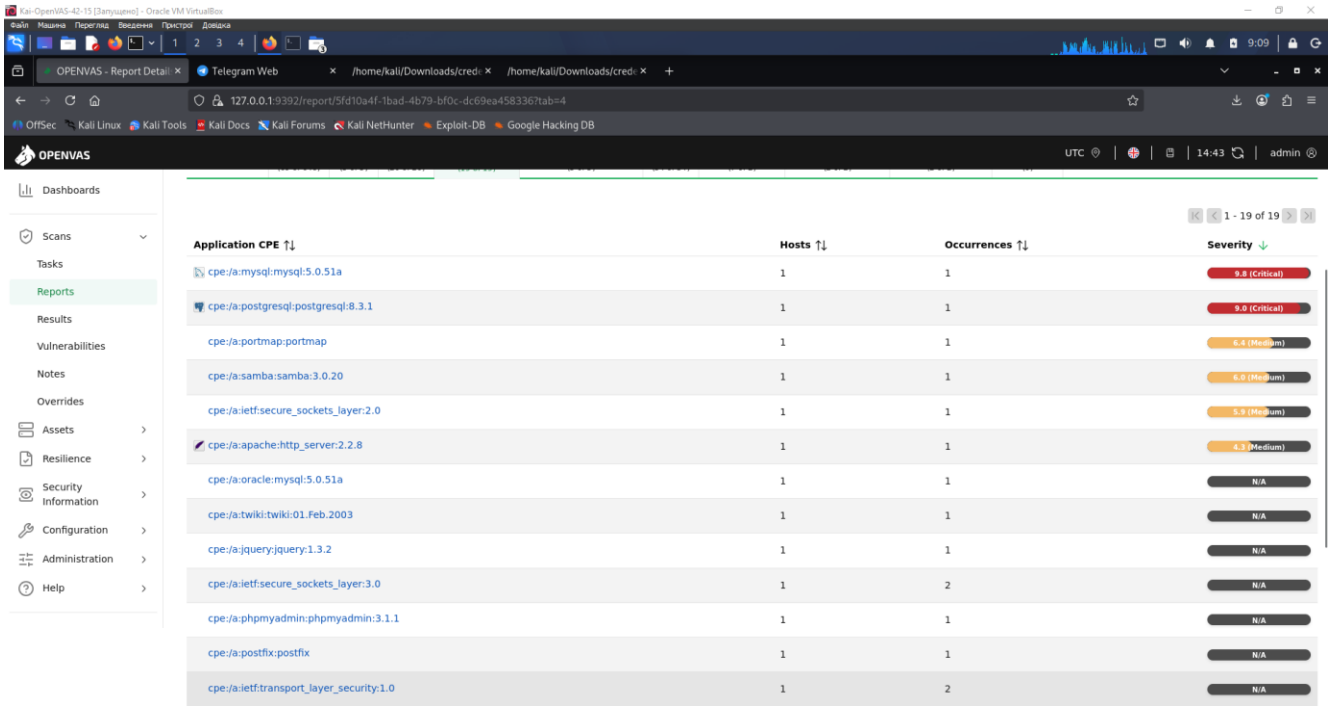


Рисунок 3.55 – Перелік ідентифікованого програмного забезпечення (CPE) та відповідний рівень загроз

Особливої уваги заслуговує вразливість Apache Tomcat Ghostcat (CVE-2020-1938, CVSS 9.8) на порту 8009/tcp. Сканер здійснив активний запит через AJP-конектор та отримав вміст конфігураційного файлу /WEB-INF/web.xml, що є беззаперечним доказом можливості несанкціонованого читання довільних файлів у контексті вебзастосунку. Також було підтверджено наявність відомого бекдора vsftpd 2.3.4 (CVE-2011-2523, CVSS 9.8), який відкриває командну оболонку на порту 6200/tcp, та можливість несанкціонованого root-доступу через службу rlogin без введення будь-якого пароля.

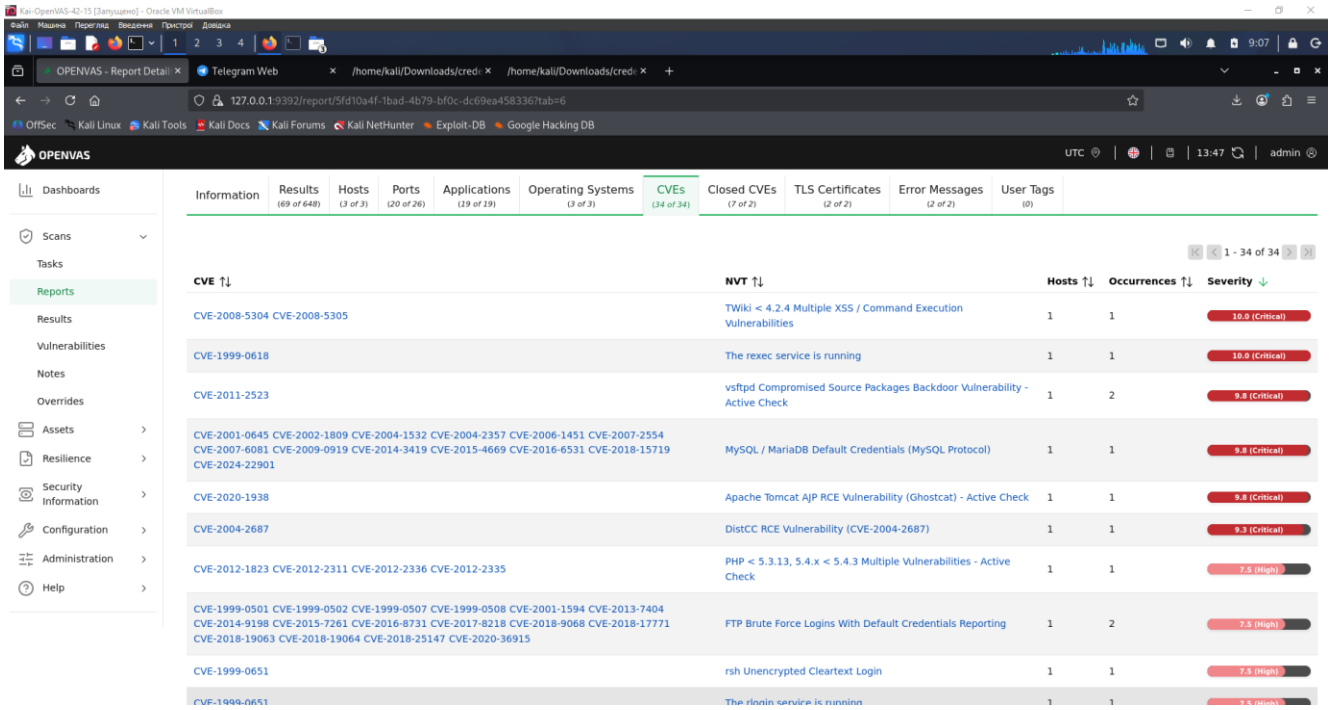


Рисунок 3.56 – Зведений перелік виявлених вразливостей за міжнародним стандартом CVE

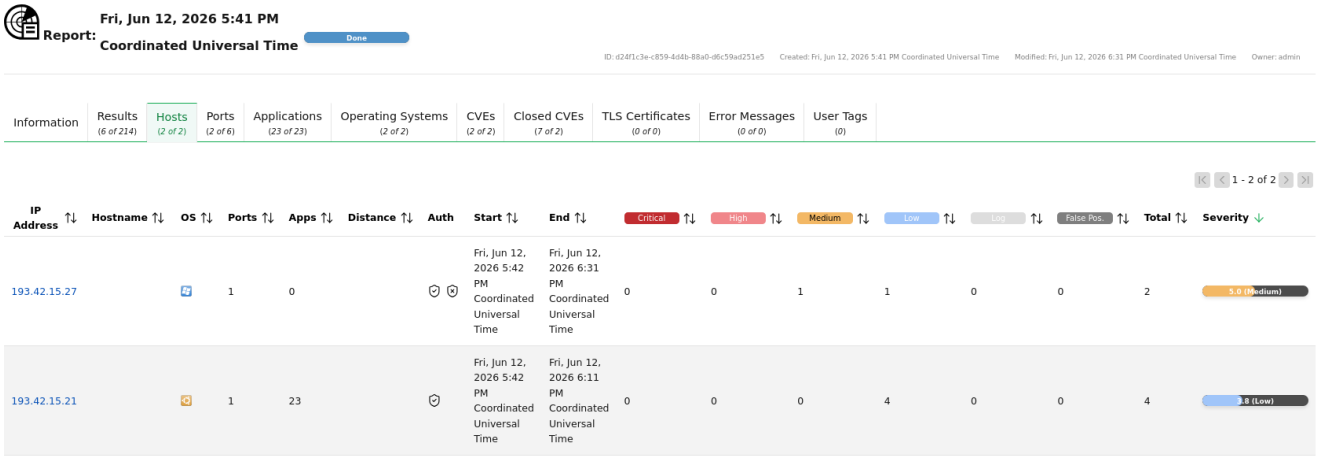
На вебсервері Metasploitable (порт 80/tcp) сканер виявив одразу кілька критичних проблем: застарілий вебзастосунок TWiki з вразливостями виконання довільних команд (CVE-2008-5304, CVE-2008-5305, CVSS 10.0), можливість виконання PHP-коду через некоректно налаштований PHP-CGI (CVE-2012-1823, CVSS 7.5), а також активовані небезпечні HTTP-методи PUT і DELETE, за допомогою яких сканер успішно завантажив та видалив тестовий файл на сервері. Додатково виявлено вразливість OpenSSL CCS Injection (CVE-2014-0224, CVSS 7.4) та Java RMI Insecure Default Configuration (CVE-2011-3556, CVSS 7.5), за якої цільова машина самостійно ініціювала зворотне TCP-з'єднання до сканера.

Особливо важливою з практичної точки зору є знахідка, яку OpenVAS класифікує як критичну: операційна система Metasploitable 2 базується на Ubuntu 8.04, термін підтримки якої завершився ще 2013-05-09. Відсутність будь-яких оновлень безпеки протягом понад десяти років означає, що всі відомі вразливості, опубліковані за цей час, залишаються без виправлень.

На відміну від Metasploitable 2, сучасні системи Ubuntu Server (193.42.15.21) та Windows 10 (193.42.15.27) при зовнішньому скануванні без автентифікації не виявили критичних проблем. На Windows 10 сканер ідентифікував лише

доступність переліку внутрішніх RPC-служб через порт 135/tcp (DCE/RPC Services Enumeration, CVSS 5.0), що є типовою конфігурацією для Windows-систем у внутрішніх мережах.

Другий етап сканування був зосереджений на Ubuntu Server та Windows 10 із наданням легітимних облікових даних (протоколи SSH та SMB відповідно). Ключовою передумовою для отримання достовірних результатів була успішна автентифікація сканера на обох цільових вузлах, що підтверджується розділом Host Authentications у звіті.



Report: Fri, Jun 12, 2026 5:41 PM Coordinated Universal Time — Done

ID: d24f1c3e-c859-4d4b-88a0-d6c59ad251e5 Created: Fri, Jun 12, 2026 5:41 PM Coordinated Universal Time Modified: Fri, Jun 12, 2026 6:31 PM Coordinated Universal Time Owner: admin

Information | Results (6 of 214) | Hosts (2 of 2) | Ports (2 of 6) | Applications (23 of 23) | Operating Systems (2 of 2) | CVEs (2 of 2) | Closed CVEs (7 of 2) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 2 of 2

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	Critical	High	Medium	Low	Log	False Pos.	Total	Severity
193.42.15.27			1	0			Fri, Jun 12, 2026 5:42 PM Coordinated Universal Time	Fri, Jun 12, 2026 6:31 PM Coordinated Universal Time	0	0	1	1	0	0	2	5.0 (Medium)
193.42.15.21			1	23			Fri, Jun 12, 2026 5:42 PM Coordinated Universal Time	Fri, Jun 12, 2026 6:11 PM Coordinated Universal Time	0	0	0	4	0	0	4	1.8 (Low)

Рисунок 3.57 – Загальна статистика автентифікованого сканування (White Box Audit) за цільовими вузлами

Результати цього етапу кардинально відрізняються від попереднього як за кількістю, так і за характером знахідок. Жодної критичної або високої вразливості виявлено не було, що підтверджує належний базовий рівень безпеки цих систем. Проте автентифікований доступ дозволив виявити приховані недоліки, принципово недосяжні для зовнішнього сканера.

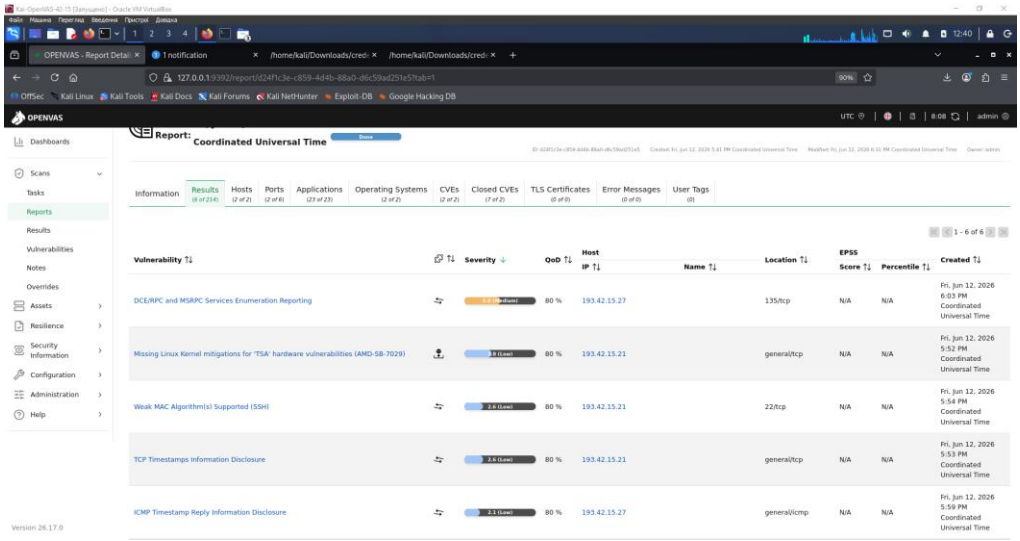


Рисунок 3.58 – Відображення деталей виявлених вразливостей під час автентифікованого доступу до цільових систем

На Ubuntu Server (193.42.15.21) завдяки доступу по SSH сканер отримав можливість читати системний інтерфейс ядра операційної системи. Він встановив, що ядро Linux на цьому вузлі не має мікрокодових патчів проти апаратних вразливостей процесора AMD, відомих як Transient Scheduler Attacks (CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357). Статус захисту, зчитаний безпосередньо з ядра, містив рядок Vulnerable: Clear CPU buffers attempted, no microcode, що свідчить про відсутність необхідного мікрокодового оновлення від виробника процесора. Ця вразливість є виключно знахідкою White Box підходу: жоден зовнішній сканер не здатен прочитати подібну інформацію без автентифікованого доступу до системи. Крім того, конфігурація служби OpenSSH підтримує слабкі 64-бітні алгоритми автентифікації повідомлень (Weak MAC Algorithms), зокрема umac-64, відмова від яких є стандартною рекомендацією безпеки.

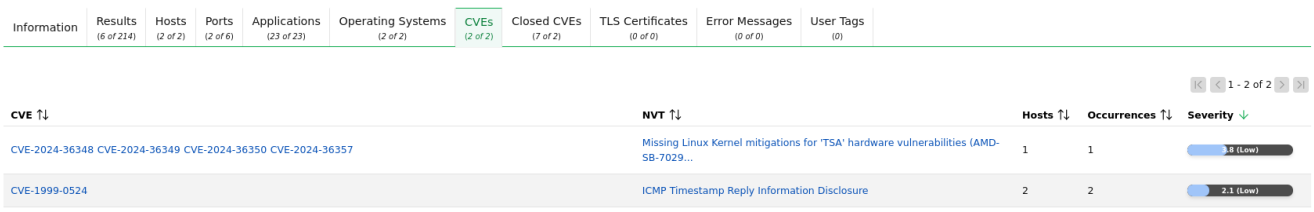


Рисунок 3.59 – Ідентифікація апаратних вразливостей ядра (CVE) за допомогою локальних перевірок

На робочій станції Windows 10 (193.42.15.27) автентифікація по протоколу SMB дозволила отримати детальний перелік усіх внутрішніх RPC-служб системи. Сканер ідентифікував конкретні процеси, що обслуговують кожен порт: зокрема, lsass.exe (підсистема автентифікації та авторизації) на порту 49664/tcp та spoolsv.exe (диспетчер черги друку) на порту 49668/tcp. Ця інформація є критично цінною для зловмисника, оскільки дозволяє точно визначити цілі для подальших атак на конкретні привілейовані процеси.

Зведений результат White Box Audit підтверджує загальний принцип сучасної кібербезпеки: оновлені операційні системи є стійкими до поширених мережевих атак, однак навіть вони можуть містити приховані апаратні та конфігураційні вразливості, виявлення яких вимагає автентифікованого внутрішнього аудиту.

Третій етап – “Full Network Audit” – дав найбільш комплексну картину стану інфраструктури. Сканер, отримавши для дослідження цілу підмережу 193.42.15.0/24, самостійно виявив 8 активних вузлів з 254 можливих адрес. Серед них, на додаток до відомих цільових систем, було ідентифіковано мережеве обладнання: маршрутизатори та шлюзи за адресами 193.42.15.1, 193.42.15.2, 193.42.15.3 та 193.42.15.254.

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	Critical	High	Medium	Low	Log	False Pos.	Total	Severity
193.42.15.22			20	19			Fri, Jun 12, 2026 8:19 PM Coordinated Universal Time	Fri, Jun 12, 2026 9:00 PM Coordinated Universal Time	13	10	41	6	0	0	70	10.0 (Critical)
193.42.15.1			1	1			Fri, Jun 12, 2026 7:45 PM Coordinated Universal Time	Fri, Jun 12, 2026 7:52 PM Coordinated Universal Time	0	0	2	2	0	0	4	5.3 (Medium)
193.42.15.2			1	1			Fri, Jun 12, 2026 7:57 PM Coordinated Universal Time	Fri, Jun 12, 2026 8:01 PM Coordinated Universal Time	0	0	2	2	0	0	4	5.3 (Medium)
193.42.15.3			1	1			Fri, Jun 12, 2026 7:52 PM Coordinated Universal Time	Fri, Jun 12, 2026 7:57 PM Coordinated Universal Time	0	0	2	2	0	0	4	5.3 (Medium)
193.42.15.254			1	1			Fri, Jun 12, 2026 8:11 PM Coordinated Universal Time	Fri, Jun 12, 2026 8:19 PM Coordinated Universal Time	0	0	2	2	0	0	4	5.3 (Medium)
193.42.15.27			1	0			Fri, Jun 12, 2026 8:01 PM Coordinated Universal Time	Fri, Jun 12, 2026 8:34 PM Coordinated Universal Time	0	0	1	1	0	0	2	5.0 (Medium)
193.42.15.21			1	23			Fri, Jun 12, 2026 7:43 PM Coordinated Universal Time	Fri, Jun 12, 2026 8:10 PM Coordinated Universal Time	0	0	0	4	0	0	4	2.6 (Low)
193.42.15.25			0	0			Fri, Jun 12, 2026 7:41 PM Coordinated Universal Time	Fri, Jun 12, 2026 7:45 PM Coordinated Universal Time	0	0	0	0	0	0	0	N/A

Рисунок 3.60 – Результати автоматичної ідентифікації операційних систем в інфраструктурі

Аналіз мережевого обладнання виявив однотипні вразливості середнього рівня на всіх маршрутизаторах і шлюзах, пов'язані з конфігурацією SSH. На кожному з них підтримуються застарілі алгоритми обміну ключами, що використовують SHA-1 та 1024-бітні групи Діффі-Гелмана, а також слабкі алгоритми симетричного шифрування, зокрема 3DES-CBC та AES-CBC. Зазначені алгоритми вважаються вразливими до атак типу SWEET32 та BEAST і потенційно

дозволяють зловмиснику з достатніми обчислювальними ресурсами розшифрувати адміністративний трафік мережевого обладнання.

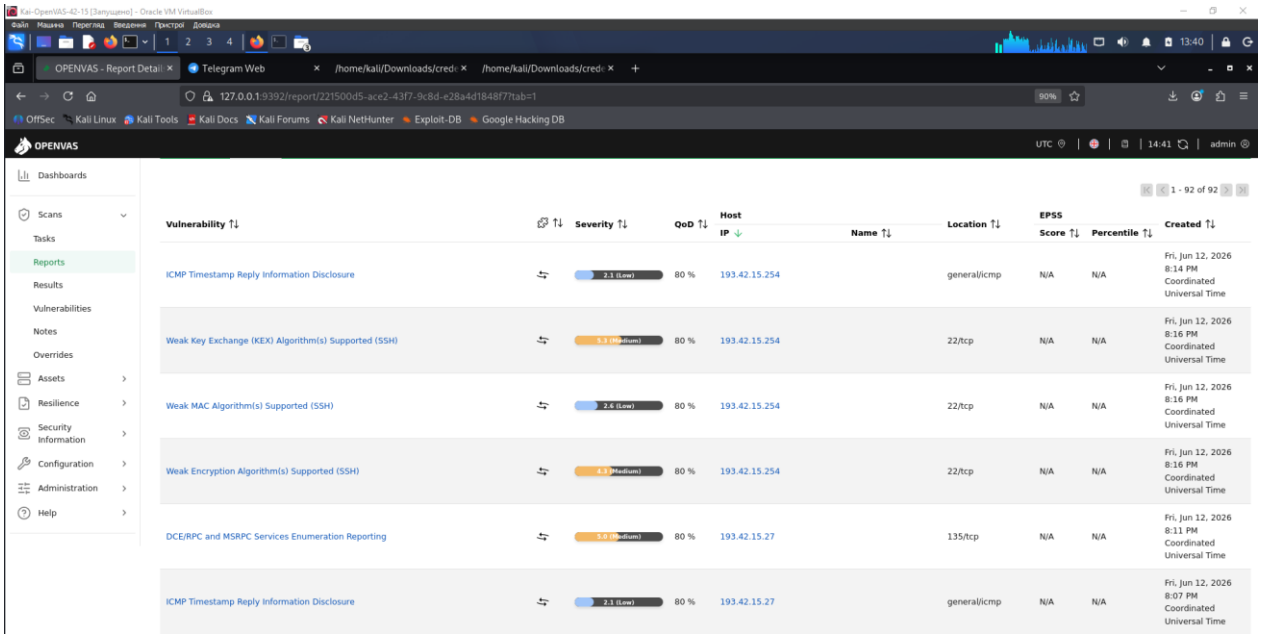
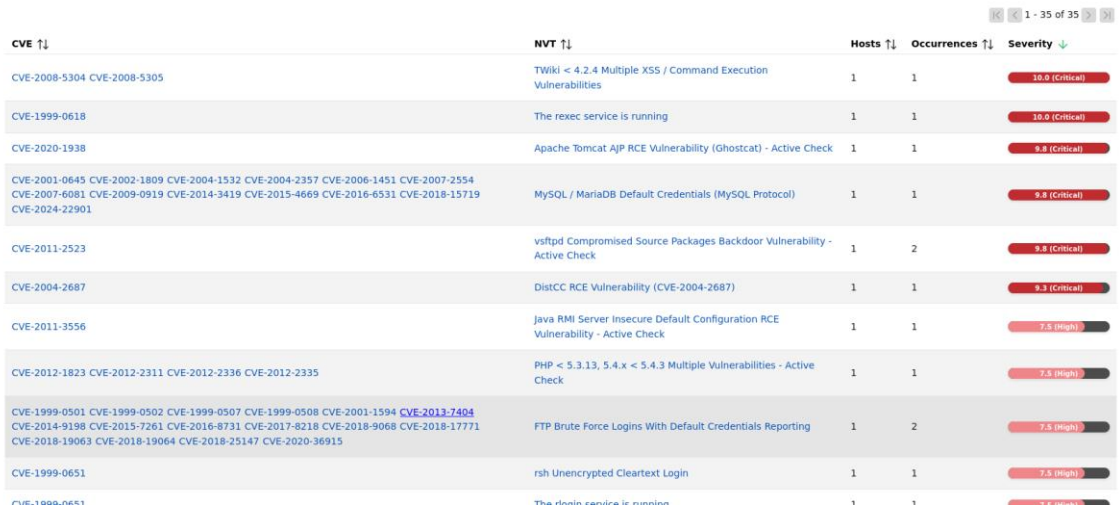


Рисунок 3.61 – Деталізований перелік вразливостей конфігурації протоколу SSH на мережевому шлюзі (хост 193.42.15.254)

Порівняння результатів усіх трьох етапів демонструє чітку закономірність. Метод Black Box є найшвидшим для виявлення критичних, експлуатованих вразливостей у публічно доступних сервісах. Метод White Box забезпечує глибину, необхідну для виявлення апаратних, ядерних та конфігураційних недоліків, які не мають зовнішніх проявів. Повне мережеве сканування дозволяє скласти вичерпну карту інфраструктури і виявити вузли, існування яких аудитор міг і не знати. Комплексне застосування всіх трьох підходів, реалізоване в рамках цієї роботи, є оптимальною стратегією проведення аудиту безпеки IT-інфраструктури підприємства.



CVE	NVT	Hosts	Occurrences	Severity
CVE-2008-5304 CVE-2008-5305	TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	1	1	10.0 (Critical)
CVE-1999-0618	The rexec service is running	1	1	10.0 (Critical)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check	1	1	9.8 (Critical)
CVE-2001-0645 CVE-2002-1809 CVE-2004-1532 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719 CVE-2024-22901	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (Critical)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check	1	2	9.8 (Critical)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (Critical)
CVE-2011-3556	Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	1	1	7.5 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	1	1	7.5 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2014-9198 CVE-2015-7261 CVE-2016-8731 CVE-2017-8218 CVE-2018-9068 CVE-2018-17771 CVE-2018-19063 CVE-2018-19064 CVE-2018-25147 CVE-2020-36915	FTP Brute Force Logins With Default Credentials Reporting	1	2	7.5 (High)
CVE-1999-0651	rsh Unencrypted Cleartext Login	1	1	7.5 (High)

Рисунок 3.62 – Класифікація виявлених загроз IT-інфраструктури за міжнародними ідентифікаторами CVE

Комплексне сканування продемонструвало ефективність застосування підсистеми OpenVAS для моніторингу не лише кінцевих станцій і серверів, але й базової мережевої інфраструктури. Виявлені недоліки конфігурації протоколу SSH на маршрутизаторах Cisco підкреслюють критичну важливість імплементації сучасних криптографічних стандартів (використання RSA-ключів довжиною не менше 2048 біт або еліптичних кривих ECDHE) для захисту внутрішнього адміністративного трафіку від атак типу Man-in-the-Middle.

Operating System	CPE	Hosts	Severity
Ubuntu 8.04	cpe:/o:canonical:ubuntu_linux:8.04	1	10.0 (Critical)
Cisco IOS	cpe:/o:cisco:ios	4	5.3 (Medium)
Microsoft Windows	cpe:/o:microsoft:windows	1	5.0 (Medium)
Ubuntu 22.04 LTS	cpe:/o:canonical:ubuntu_linux:22.04:-:lts	1	2.8 (Low)
Linux Kernel	cpe:/o:linux:kernel	1	N/A

Рисунок 3.63 – Зведена статистика виявлених активних вузлів та розподіл вразливостей за результатами комплексного сканування мережі

Загальна оцінка захищеності демонструє, що головним вектором атаки в дослідженій інфраструктурі є застарілі та невідповідно налаштовані сервіси (імітовані вузлом Metasploitable 2), у той час як оновлені операційні системи за умови правильного мережевого екранування залишаються стійкими до віддаленого злому. Водночас виявлені внутрішні та апаратні недоліки вимагають впровадження організаційно-технічних заходів, таких як регулярне оновлення мікрокоду процесорів, відмова від використання застарілих криптографічних примітивів

(SHA-1, 3DES, RC4) на мережевому обладнанні та суворе розмежування доступу до протоколів управління (SSH, SMB, RPC) на рівні міжмережевих екранів.

Висновки до третього розділу:

У третьому розділі було реалізовано практичну частину дослідження – проведення комплексного аудиту безпеки модельованої корпоративної IT-інфраструктури за допомогою платформи Greenbone OpenVAS.

На першому етапі було побудовано тестове середовище у програмному емуляторі GNS3, яке відтворює типову архітектуру мережі малого підприємства. Топологія включала маршрутизатори з протоколом резервування шлюзу GLBP, DHCP-сервер для автоматичного призначення адрес, механізм трансляції адрес NAT для забезпечення доступу до зовнішніх ресурсів, а також чотири кінцеві вузли різних типів: сервер під управлінням Ubuntu Server, робочу станцію Windows 10, навмисно вразливу систему Metasploitable 2 та сканер безпеки на базі Kali Linux з розгорнутим OpenVAS. Працездатність інфраструктури було підтверджено перевіркою мережевої зв'язності між усіма вузлами.

Сканування було проведено у три послідовних етапи, кожен з яких імітував окремий сценарій реального аудиту. Неавтентифіковане сканування (Black Box) виявило 13 критичних та 10 високих вразливостей, переважна більшість яких зосереджена на вузлі Metasploitable 2. Сканер не лише ідентифікував вразливості, а й активно підтвердив можливість їхньої експлуатації: було виконано віддалений запуск команд через DistCC та PHP-CGI, прочитано конфігураційний файл Apache Tomcat через вразливість Ghostcat, підібрано стандартні паролі до служб FTP, VNC, PostgreSQL та MySQL. Автентифіковане сканування (White Box) дозволило виявити приховані недоліки сучасних операційних систем – відсутність мікрокодових патчів для апаратних вразливостей процесорів AMD та використання слабких криптографічних алгоритмів, – що є принципово недосяжним для зовнішнього спостерігача. Повний аудит підмережі (Full Network Audit) забезпечив виявлення 8 активних вузлів, включаючи мережеве обладнання, та показав наявність конфігураційних вразливостей SSH-протоколу на маршрутизаторах.

Результати трьох етапів сканування переконливо підтвердили, що комплексний підхід, який поєднує зовнішній, внутрішній та мережевий аудит, є оптимальною стратегією оцінки захищеності ІТ-інфраструктури підприємства. Жоден окремий метод не забезпечує повноти картини: Black Box не бачить внутрішніх конфігурацій, White Box не охоплює мережеве обладнання, а повне сканування мережі без облікових даних пропускає глибинні вразливості операційних систем.

ВИСНОВКИ

У дипломній роботі було досліджено процес аудиту інформаційної безпеки IT-інфраструктури підприємства з використанням сучасних засобів автоматизованого аналізу вразливостей. Поставлена мета – розробка та практична апробація методики комплексного аудиту безпеки корпоративної мережі – була досягнута в повному обсязі.

У першому розділі було проаналізовано теоретичні засади аудиту інформаційної безпеки, розглянуто нормативно-правову базу (стандарти ISO/IEC 27001, NIST SP 800-115, методологію OWASP), класифіковано типи аудиту та визначено роль автоматизованих сканерів вразливостей у сучасній системі забезпечення кібербезпеки підприємств. Встановлено, що використання спеціалізованих інструментів є необхідною, але не достатньою умовою ефективного аудиту – результати потребують кваліфікованої інтерпретації фахівцем.

У другому розділі було проведено порівняльний аналіз сучасних платформ для сканування вразливостей та обґрунтовано вибір Greenbone OpenVAS як основного інструменту дослідження. Платформа відповідає вимогам відкритості, регулярного оновлення бази вразливостей та підтримки множини протоколів автентифікації, що робить її придатною для проведення аудиту в гетерогенних мережевих середовищах. Також було описано процес проєктування та побудови тестової інфраструктури у середовищі GNS3, що включає маршрутизатори Cisco з протоколом GLBP, серверні та клієнтські операційні системи.

У третьому розділі було реалізовано практичну частину дослідження. Неавтентифіковане сканування (Black Box) зафіксувало 69 результатів після фільтрації, серед яких 13 критичних та 10 високих вразливостей. Автентифіковане сканування (White Box) виявило 6 результатів, жодного з критичним або високим рівнем. Повний аудит підмережі (Full Network Audit) зафіксував 92 результати, серед яких 13 критичних, 10 високих, 50 середніх та 19 низьких вразливостей. Збіг кількості критичних та високих знахідок між першим та третім етапами пояснюється тим, що повний аудит повторно охоплює ті самі вузли, зокрема Metasploitable 2, який є домінуючим джерелом критичних вразливостей. Практична

цінність отриманих результатів полягає у демонстрації наступних ключових висновків:

Перше. Системи з простроченим терміном підтримки (на прикладі Metasploitable 2 / Ubuntu 8.04) становлять найбільшу загрозу для безпеки корпоративної мережі. Наявність у мережі хоча б одного такого вузла з відкритим мережевим доступом дозволяє зловмиснику отримати повний контроль без жодних спеціальних навичок чи інструментів.

Друге. Сучасні операційні системи (Ubuntu Server 22.04 LTS, Windows 10) за умови базової конфігурації демонструють високу стійкість до зовнішніх атак. Однак внутрішній автентифікований аудит здатен виявити приховані вразливості апаратного рівня та конфігураційні недоліки криптографічних протоколів, що потребують цілеспрямованого усунення.

Третє. Мережеве обладнання (маршрутизатори, комутатори) часто залишається поза увагою при проведенні аудиту, хоча може містити вразливості в налаштуваннях протоколів адміністративного доступу. Повне сканування підмережі є єдиним методом, що гарантує виявлення всіх активних пристроїв та оцінку їхнього стану захищеності.

Четверте. Комплексний підхід до аудиту, що поєднує зовнішній (Black Box), внутрішній (White Box) та мережевий (Network Audit) методи, є обов'язковою умовою для формування повної та достовірної картини стану інформаційної безпеки підприємства. Застосування лише одного з методів неминуче призводить до пропуску суттєвих категорій вразливостей.

Розроблена у дипломній роботі методика може бути застосована підприємствами малого та середнього бізнесу для проведення регулярного внутрішнього аудиту безпеки без залучення зовнішніх комерційних сервісів, оскільки всі використані інструменти (GNS3, OpenVAS, Kali Linux) є вільно розповсюджуваним програмним забезпеченням з відкритим вихідним кодом.

Результати роботи апробовано шляхом публікації тез доповіді на XVI Міжнародній науково-технічній конференції «Інформаційно-комп'ютерні технології – 2026» (м. Житомир, 2–3 квітня 2026 р.).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Vulnerability Management Under ISO 27001? [Електронний ресурс] // ZenGRC. – Режим доступу: https://www.zengrc.com/blog/what-is-vulnerability-management-under-iso-27001/

2. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments / Joint Task Force Transformation Initiative. Gaithersburg : National Institute of Standards and Technology, 2012. 95 p. [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/pubs/sp/800/30/r1/final

3. Vulnerability [Електронний ресурс] // ctcarlsoncom. – Режим доступу: https://ctcarlsoncom.wordpress.com/2024/11/01/vulnerability/

4. Нормативні документи системи ТЗІ 2024 [Електронний ресурс] // Держспецзв'язку. – Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024

5. Vulnerabilities and Software Weaknesses: Acronym Breakdown [Електронний ресурс] // Automox. – Режим доступу: https://www.automox.com/blog/vulnerabilities-software-weaknesses-acronym-breakdown

6. Common Vulnerability Scoring System version 4.0 [Електронний ресурс] // FIRST. – Режим доступу: https://www.first.org/cvss/v4.0/

7. Phishing 2025: Why It Still Fuels 60% of Cyber Attacks [Електронний ресурс] // Revel8. – Режим доступу: https://www.revel8.ai/blog/phishing-2025-why-it-still-fuels-60-of-cyber-attacks

8. ENISA Threat Landscape 2025. – European Union Agency for Cybersecurity (ENISA), 2025. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

9. Огляд національної системи кібербезпеки України 2025 [Електронний ресурс] // РНБО України. – С. [16, 19, 24, 25, 32]. – Режим доступу: https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf

10. Network Penetration Testing: What is a Network Pentest? [Електронний ресурс] // Datami. – Режим доступу: https://datami.ee/ua/blog/network-penetration-testing-what-is-a-network-pentest/

11. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment: NIST Special Publication 800-115. Gaithersburg : National Institute of Standards and Technology, 2008. 80 p. DOI: Електронний ресурс] – Режим доступу: https://csrc.nist.gov/pubs/sp/800-115/final

12. Penetration Testing Methodology [Електронний ресурс] // DigitalXRAID. – Режим доступу: https://www.digitalxraid.com/blog/penetration-testing-methodology/

13. Active vs. Passive Monitoring [Електронний ресурс] // Splunk. – Режим доступу: https://www.splunk.com/en_us/blog/learn/active-vs-passive-monitoring.html

14. Penetration Testing Execution Standard: 7 PTES Stages [Електронний ресурс] // Datami. – Режим доступу: https://datami.ee/ua/blog/penetration-testing-execution-standard-7-ptes-stages/

15. Приходько Д. С., Дячук О. Ю. Аналіз методів та засобів виявлення вразливостей іт-інфраструктури на основі openvas. Інформаційно-комп'ютерні технології – 2026: матеріали XVI Міжнародної науково-технічної конференції, м. Житомир, 2–3 квіт. 2026 р. Житомир: Державний університет «Житомирська політехніка», 2026. С. 131–132.

16. Vulnerability Scanning Tools [Електронний ресурс] // TuxCare. – Режим доступу: https://tuxcare.com/blog/vulnerability-scanning-tools/

17. Best Vulnerability Scanners: OpenVAS, Nessus & Qualys [Електронний ресурс] // SenseLearner. – Режим доступу: https://senselearner.com/best-vulnerability-scanners-openvas-nessus-qualys/

18. A comprehensive benchmark of network vulnerability scanners 2024 [Електронний ресурс] // Pentest-Tools. – Режим доступу: https://pentest-tools.com/benchmarks/network-vulnerability-scanners-benchmark-2024.pdf

19. Greenbone Community Documentation: Architecture [Електронний ресурс] // Greenbone. – Режим доступу: https://greenbone.github.io/docs/latest/background.html

20. OpenVAS Scanner [Електронний ресурс] // GitHub – Greenbone. – Режим доступу: https://github.com/greenbone/openvas-scanner

21. Greenbone Management Protocol (GMP) [Електронний ресурс] // Greenbone AG. – Режим доступу: https://docs.greenbone.net/API/GMP/gmp-22.4.html

22. python-gvm: Greenbone Vulnerability Management Python Library [Електронний ресурс] // GitHub – Greenbone. – Режим доступу: https://github.com/greenbone/python-gvm

23. OpenVAS – Open Vulnerability Assessment Scanner [Електронний ресурс] // Greenbone AG. – Режим доступу: https://www.openvas.org/

24. Greenbone Community Edition Documentation: Administration [Електронний ресурс] // Greenbone AG. – Режим доступу: https://greenbone.github.io/docs/latest/22.4/container/index.html

25. Greenbone Feed Sync [Електронний ресурс] // GitHub – Greenbone. – Режим доступу: https://github.com/greenbone/greenbone-feed-sync

26. gvm-tools: Remote Control for Greenbone Vulnerability Management [Електронний ресурс] // GitHub – Greenbone. – Режим доступу: https://github.com/greenbone/gvm-tools

27. ARP Spoofing: Перехоплення Даних Мережі [Електронний ресурс] // CyberSet. – Режим доступу: https://cyberset.com.ua/beginners/network/arp-spoofing-percept-data-mergesecurity/

28. What is DHCP Starvation [Електронний ресурс] // Deepstrike. – Режим доступу: https://deepstrike.io/blog/what-is-dhcp-starvation

29. What is VLAN Hopping [Електронний ресурс] // JumpCloud. – Режим доступу: https://jumpcloud.com/it-index/what-is-vlan-hopping

30. GLBP and HSRP Attacks [Електронний ресурс] // HackTricks. – Режим доступу: https://hacktricks.wiki/uk/generic-methodologies-and-resources/pentesting-network/glbp-and-hsrp-attacks.html

31. EIGRP Poisoned Floating Summarization [Електронний ресурс] // Journey2theCCIE. – Режим доступу:

https://journey2theccie.wordpress.com/2020/02/05/eigrp-poisoned-floating-summarization/

32. Metasploitable 2 Exploitability Guide [Електронний ресурс] // Rapid7. – Режим доступу: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

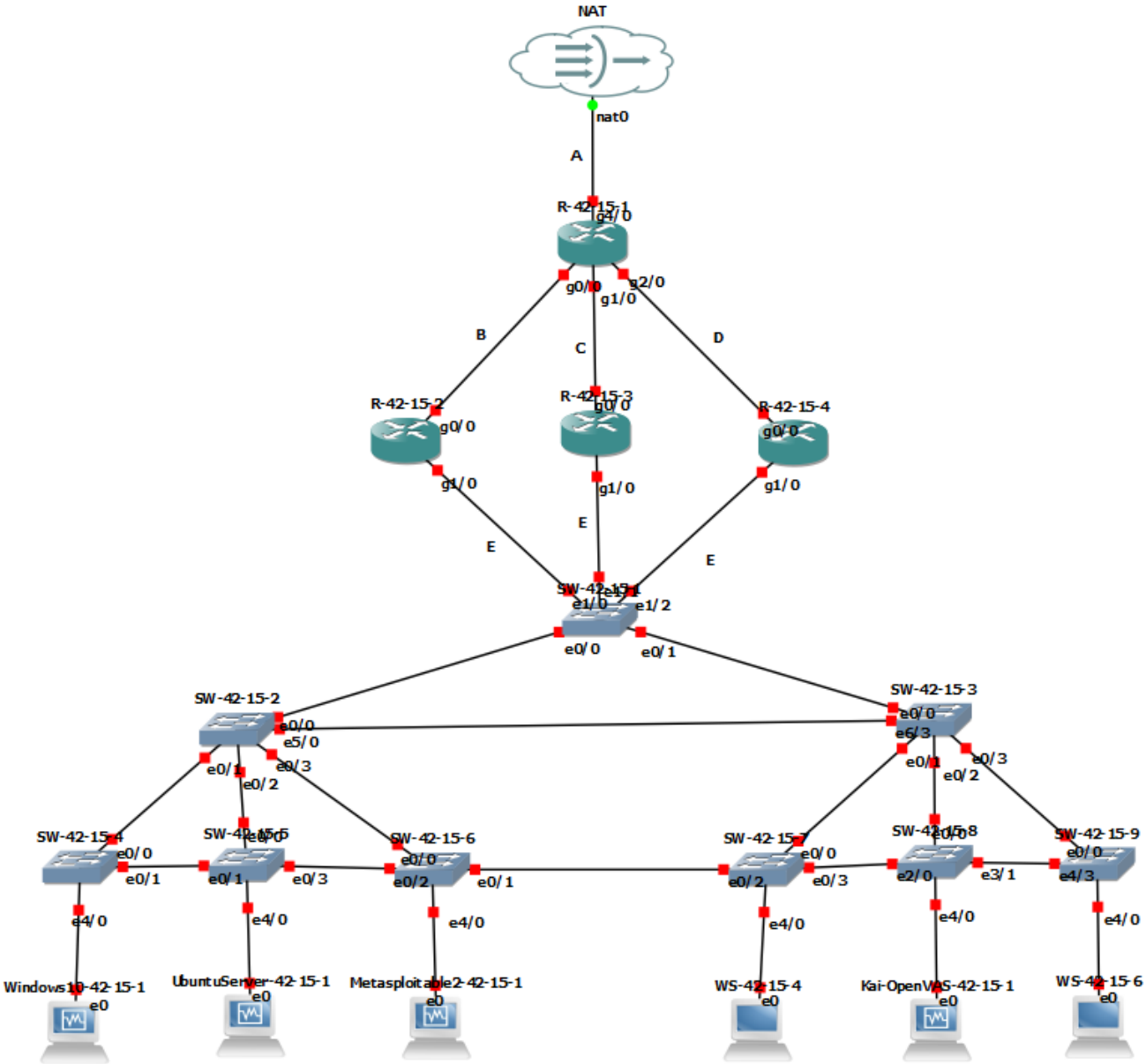
33. Chalvatzis I., Karras D. A., Papademetriou R. C. Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment. 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). Dalian, 2019. P. 52–58. [Електронний ресурс] 10.1109/ICAICA.2019.8873438 – Режим доступу: https://doi.org/10.1109/ICAICA.2019.88734381

34. McNab C. Network Security Assessment: Know Your Network. 3rd ed. Sebastopol : O'Reilly Media, 2016. 504 p. [Електронний ресурс] 978-1-491-91095-5. – Режим доступу: https://www.oreilly.com/library/view/network-security-assessment/9781491911044/

ДОДАТКИ

Додаток А*

Проект мережі



Додаток Б*

Адресація пристроїв мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	---	DHCP		
Підмережа B	---	10.10.10.0	255.255.255.252	/30
Підмережа C	---	20.20.20.0	255.255.255.252	/30
Підмережа D	---	30.30.30.0	255.255.255.252	/30
Підмережа E	---	193.42.15.0	255.255.255.0	/24
R-42-15-1	gig0/0	10.10.10.1	255.255.255.252	/30
	gig1/0	20.20.20.1	255.255.255.252	/30
	gig2/0	30.30.30.1	255.255.255.252	/30
	gig4/0	DHCP		
R-42-15-2	gig0/0	10.10.10.2	255.255.255.252	/30
	gig1/0	193.42.15.1	255.255.255.0	/24
	gig1/0 (virtual)	193.42.15.254	255.255.255.0	/24
R-42-15-3	gig0/0	20.20.20.2	255.255.255.252	/30
	gig1/0	193.42.15.2	255.255.255.0	/24
	gig1/0 (virtual)	193.42.15.254	255.255.255.0	/24
R-42-15-4	gig0/0	30.30.30.2	255.255.255.252	/30
	gig1/0	193.42.15.3	255.255.255.0	/24
	gig1/0 (virtual)	193.42.15.254	255.255.255.0	/24
SW-42-15-(1-9)	vlan1	193.42.15.5-193.42.15.14	255.255.255.0	/24
WS-42-15-(1-6)	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			

Додаток В*

Конфігураційні файли мережевих пристроїв

```
R-42-15-1#sh run
Building configuration...

Current configuration : 2482
bytes
!
upgrade fpd auto
version 15.2
service timestamps debug
datetime msec
service timestamps log datetime
msec
service password-encryption
!
hostname R-42-15-1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit
unreachable
!
ip dhcp excluded-address
193.42.15.1 193.42.15.20
!
ip dhcp pool LAN_E
 network 193.42.15.0
255.255.255.0
 default-router 193.42.15.254
 dns-server 8.8.8.8
!
no ip domain lookup
ip domain name prikhodko.net
ip cef
no ipv6 cef
!
multilink bundle-name
authenticated
!
username admin secret 5
$1$vJe2$34QlDuJDmGLzLAJ5MHndI0
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 10.10.10.1
255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 20.20.20.1
255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 30.30.30.1
255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 4215
 network 10.10.10.0 0.0.0.3
 network 20.20.20.0 0.0.0.3
 network 30.30.30.0 0.0.0.3
 network 192.42.15.0
 network 193.42.15.0
 redistribute static
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 1
interface GigabitEthernet4/0
overload
ip nat inside source list
NAT_ACL interface
GigabitEthernet4/0 overload
!
ip access-list extended NAT_ACL
 deny   ip any 192.168.122.0
0.0.0.255
 permit ip any any
!
access-list 1 permit any
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
End
```

```
R-42-15-2#sh run
Building configuration...

Current configuration : 2327
bytes
!
upgrade fpd auto
version 15.2
service timestamps debug
datetime msec
service timestamps log datetime
msec
service password-encryption
!
hostname R-42-15-2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit
unreachable
!
no ip domain lookup
ip domain name prikhodko.net
ip cef
no ipv6 cef
!
multilink bundle-name
authenticated
!
username admin secret 5
$1$hWkM$PwFJkh68VkUXUfi8c5fAY1
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
track 1 interface
GigabitEthernet0/0 line-protocol
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 10.10.10.2
255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
```

```
 ip address 193.42.15.1
255.255.255.0
 ip access-group 100 in
 ip helper-address 10.10.10.1
 glbp 1 ip 193.42.15.254
 glbp 1 timers 5 15
 glbp 1 timers redirect 1200
14400
 glbp 1 priority 110
 glbp 1 preempt delay minimum 30
 glbp 1 weighting 110 lower 95
upper 105
 glbp 1 authentication md5 key-
string 7
094B420B093632313E3E21212E3D69
 glbp 1 weighting track 1
decrement 10
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 4215
 network 10.10.10.0 0.0.0.3
 network 193.42.15.0
 passive-interface
GigabitEthernet1/0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
access-list 100 permit udp any
eq 3222 host 224.0.0.102 eq 3222
access-list 100 permit ip any
any
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
End
```

R-42-15-3#sh run

```
Building configuration...

Current configuration : 2327
bytes
!
upgrade fpd auto
version 15.2
service timestamps debug
datetime msec
service timestamps log datetime
msec
service password-encryption
!
hostname R-42-15-3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit
unreachable
!
no ip domain lookup
ip domain name prikhodko.net
ip cef
no ipv6 cef
!
multilink bundle-name
authenticated
!
username admin secret 5
$1$OTN1$7BO4NpZmb.vIiETmL0zWK1
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
track 1 interface
GigabitEthernet0/0 line-protocol
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 20.20.20.2
255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 193.42.15.2
255.255.255.0
 ip access-group 100 in
 ip helper-address 20.20.20.1
 glbp 1 ip 193.42.15.254
 glbp 1 timers 5 15
 glbp 1 timers redirect 1200
14400
 glbp 1 priority 105
 glbp 1 preempt delay minimum 30
 glbp 1 weighting 110 lower 95
upper 105
 glbp 1 authentication md5 key-
string 7
03035709163C046F7B3B3C0E120B4A
 glbp 1 weighting track 1
decrement 10
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
!
router eigrp 4215
 network 20.20.20.0 0.0.0.3
 network 193.42.15.0
 passive-interface
GigabitEthernet1/0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
access-list 100 permit udp any
eq 3222 host 224.0.0.102 eq 3222
access-list 100 permit ip any
any
no cdp log mismatch duplex
!
control-plane
!
```

```
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
End
```

R-42-15-4#sh run

```
Building configuration...

Current configuration : 2306
bytes
!
upgrade fpd auto
version 15.2
service timestamps debug
datetime msec
service timestamps log datetime
msec
service password-encryption
!
hostname R-42-15-4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit
unreachable
!
no ip domain lookup
ip domain name prikhodko.net
ip cef
no ipv6 cef
!
multilink bundle-name
authenticated
!
username admin secret 5
$1$YBj0$o8QlKQ029u1R2kxNOersE1
!
redundancy
!
ip tcp synwait-time 5
ip ssh version 2
!
track 1 interface
GigabitEthernet0/0 line-protocol
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 30.30.30.2
255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 193.42.15.3
255.255.255.0
 ip access-group 100 in
 ip helper-address 30.30.30.1
 glbp 1 ip 193.42.15.254
 glbp 1 timers 5 15
 glbp 1 timers redirect 1200
14400
 glbp 1 preempt delay minimum 30
 glbp 1 weighting 110 lower 95
upper 105
 glbp 1 authentication md5 key-
string 7
03035709163C046F7B3B3C0E120B4A
 glbp 1 weighting track 1
decrement 10
 negotiation auto
!
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet5/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet6/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 4215
 network 30.30.30.0 0.0.0.3
 network 193.42.15.0
 passive-interface
GigabitEthernet1/0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
access-list 100 permit udp any
eq 3222 host 224.0.0.102 eq 3222
access-list 100 permit ip any
any
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
End
```

Конфігураційні файли Targets (Цілі)

Authenticated Target:

```
<get_targets_response status="200" s
tatus_text="OK">
<target id="4b0818d7-e23d-4f9e-995c-
1cdd24fb5bd1">
<owner>
<name>admin</name>
</owner>
<name>Authenticated Target</name>
<comment/>
<creation_time>2026-06-
12T11:41:18Z</creation_time>
<modification_time>2026-06-
12T11:41:18Z</modification_time>
<writable>1</writable>
<in_use>1</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<hosts>193.42.15.21,
193.42.15.27</hosts>
<exclude_hosts/>
<max_hosts>2</max_hosts>
<port_list id="33d0cd82-57c6-11e1-
8ed1-406186ea4fc5">
<name>All IANA assigned TCP</name>
<trash>0</trash>
</port_list>
<ssh_credential id="82b31ce6-8e93-
4937-9fc4-dc594dfd53ce">
<name>Linux SSH Access</name>
<port>22</port>
<trash>0</trash>
</ssh_credential>
<smb_credential id="8ed45000-ae08-
4bda-a1ac-33cc9e75da5c">
<name>Windows SMB Password</name>
<trash>0</trash>
</smb_credential>
<esxi_credential id="">
<name/>
<trash>0</trash>
</esxi_credential>
<snmp_credential id="">
<name/>
<trash>0</trash>
</snmp_credential>
<ssh_elevate_credential id="">
<name/>
<trash>0</trash>
</ssh_elevate_credential>
<krb5_credential id="">
<name/>
<trash>0</trash>
</krb5_credential>
<reverse_lookup_only>0</reverse_look
up_only>
<reverse_lookup_unify>0</reverse_loo
kup_unify>
<allow_simultaneous_ips>1</allow_sim
ultaneous_ips>
<alive_tests>
Consider Alive
<alive_test>Consider
Alive</alive_test>
</alive_tests>
<port_range>T:1-3,5,7,9,11,13,17-
25,27,29,31,33,35,37-39,41-46,48-
50,52-59,62-80,82-99,101-113,115-
224,242-248,256-257,259-269,271,280-
284,286-287,308-324,333,344-584,586-
658,660-702,704-707,709-715,729-
731,741-742,744,747-754,758-
765,767,769-777,780,800-802,810,828-
833,847-848,853-854,860-862,873,886-
888,900-903,910-913,953,989-993,995-
1001,1010,1021-1022,1025-
1026,1029,1033-1108,1110-1275,1277-
1300,1303-1490,1492-1527,1529-
1782,1784-2193,2197-2199,2201-
2258,2260-2368,2370-2377,2379-
2681,2683-2692,2694-2793,2795-
2824,2826-2872,2874-2924,2926-
3091,3093-3096,3098-3125,3127-
3300,3302-3321,3326-3366,3372-
3402,3405-3545,3547-3693,3695-
3993,3995-4047,4049-4076,4078-
4083,4085,4087-4143,4145-4172,4174-
4190,4192-4193,4197,4199,4300-
4314,4316,4320-4323,4325-
4336,4340,4343-4360,4368-4379,4389-
4393,4395-4396,4400-4411,4413-
4417,4419-4423,4425-4433,4442-
4458,4484-4488,4500,4535-4538,4545-
4556,4559,4563,4566-4570,4573,4590-
4591,4593-4605,4646,4658-4692,4700-
4704,4711,4725,4727-4728,4730-
4731,4733,4737-4745,4749-
4753,4756,4774,4784,4786-4788,4800-
4803,4827,4837-4851,4867-4871,4876-
4877,4879-4880,4883-4885,4888-
4889,4894,4899-4902,4912-4915,4940-
4942,4949-4953,4969-4971,4984-
4991,4999-5013,5015,5020-5030,5032-
5034,5042-5045,5048-5057,5059-
5075,5080-5087,5093-5094,5099-
5103,5106-5107,5111-5112,5114-
5115,5117,5120,5133-5135,5137,5145-
5146,5150-5152,5154-5157,5161-
5168,5172,5190-5197,5200-
5203,5209,5215,5221-5237,5245,5248-
5254,5264-5265,5269-5272,5280-
5282,5298-5310,5312-5318,5320-
5321,5343-5344,5349,5352-5363,5397-
5435,5443,5445,5450,5453-5456,5461-
5465,5470-5473,5475,5500-
5507,5550,5553-5557,5565-5569,5573-
5575,5579-5586,5597-5605,5618,5627-
5639,5646,5666,5670-5681,5683-
5684,5688-
5689,5693,5696,5700,5705,5713-
5730,5741-5748,5750,5755,5757,5766-
5771,5777,5780-5783,5785,5793,5813-
5814,5841-
5842,5859,5863,5868,5883,5900,5910-
5913,5963,5968-5969,5984-
5993,5999,6064-6066,6068-6077,6084-
6088,6099-6117,6121-
6124,6130,6133,6140-6149,6159-
6163,6200,6209,6222,6241-6244,6251-
6253,6267-6269,6300-6301,6306,6315-
6317,6320-6322,6324-6326,6343-
6344,6346-
6347,6350,6355,6360,6370,6379,6382,6
389-6390,6417-6421,6432,6440,6442-
6446,6455-6456,6464,6471,6480-
6489,6500-6503,6505-6510,6513-
6515,6543-6544,6547-
6551,6558,6566,6568,6579-6583,6600-
6602,6619-6629,6632,6640,6653,6655-
6656,6670-6673,6678-6679,6687-
6690,6697,6701-6703,6714-6716,6767-
6771,6777-6778,6785-
6791,6801,6817,6831,6841-
6842,6850,6868,6888,6900-
6901,6924,6935-6936,6946,6951,6961-
6966,6969-6970,6997-7026,7030-
7031,7070-7073,7080,7099-
7101,7117,7121,7128-7129,7161-
7174,7200-7202,7215-7216,7227-
7229,7236-7237,7244,7262,7272-
7283,7365,7391-7395,7397,7400-
7402,7410-7411,7421,7426-
7431,7437,7443,7471,7473-
7474,7478,7491,7500-7501,7508-
7511,7542-
7549,7551,7560,7563,7566,7569-
7570,7574,7588,7606,7624,7626-
7631,7633,7648,7663,7672-
7677,7680,7683,7687,7689,7697,7700,7
707-7708,7720,7724-
7728,7734,7738,7741-
7744,7747,7775,7777-7779,7781,7786-
7787,7789,7794,7797-7801,7810,7845-
7847,7869-7871,7878,7880,7887,7900-
7903,7913,7932-7933,7962,7967,7979-
7982,7997,7999-8009,8015-8016,8019-
8023,8025-8026,8032-8034,8040-
8044,8051-8059,8066-
8067,8070,8074,8077,8080-8084,8086-
8088,8090-8091,8097,8100-8102,8115-
8118,8121-8122,8128-
8132,8140,8148,8153,8160-8162,8181-
8184,8190-8192,8194-8195,8199-
8201,8204-
8208,8230,8243,8270,8276,8280,8282,8
292-8294,8300-8301,8313,8320-
8322,8351,8376-8380,8383,8400-
8405,8415-8417,8423,8442-
8445,8450,8457,8470-8474,8500-
8502,8554-8555,8567,8600,8610-
8615,8665-
8666,8675,8686,8688,8699,8710-
8711,8733,8750,8763-8770,8778,8786-
8787,8793,8800,8804,8873,8880-
8881,8883,8888-8894,8899-8901,8910-
8913,8937,8953-8954,8980,8989-
8991,8997-9002,9005,9008-9010,9020-
9026,9050-9051,9060,9080,9083-
9093,9100-9107,9111,9119,9122-
9123,9131,9160-9164,9191,9200-
9217,9222,9255,9278-9285,9287,9292-
9295,9300,9306,9310,9312,9318,9321,9
339,9343-9346,9374,9380,9387-
9390,9396-9397,9400-9402,9418,9443-
9445,9450,9500,9535-9536,9555,9592-
9600,9612,9614,9616-9618,9628-
9631,9640,9666-9668,9694-
9695,9700,9747,9750,9753,9762,9800-
9802,9875-9877,9888-
9889,9898,9900,9909,9911,9925,9950-
9955,9966,9978-9979,9981,9987-
9988,9990-10010,10020,10050-
10051,10055,10080-10081,10100-
10104,10107,10110,10113-
10117,10125,10128-10129,10160-
10162,10200-10201,10252,10260-
10261,10288,10321,10443,10540-
10544,10548,10631,10800,10805,10809,
10860,10880,10933,10990,11000-
11001,11095,11103-11106,11109-
11112,11161-11165,11172-11175,11201-
11202,11208,11211,11319-
11321,11367,11371,11489,11600,11623,
11720,11723,11751,11796,11876,11967,
11971,12000-12008,12010,12012-
12013,12109,12121,12168,12172,12300,
12302,12321-
12322,12345,12753,12865,13160,13216-
13218,13223-13224,13400,13720-
13722,13724,13782-13783,13785-
13786,13818-13823,13894,13929-
13930,14000-14001,14033-14034,14141-
14143,14145,14149-
14150,14154,14250,14414,14500,14936-
14937,15000,15002,15345,15363,15555,
15660,15740,15999-16002,16020-
16021,16161-16162,16309-16311,16360-
16361,16367-16368,16384-
16385,16619,16665,16789,16900,16950,
16991-16995,17007,17184-17185,17219-
17221,17223,17225,17234-
17235,17500,17555,17729,17754-
17756,17777,18000,18104,18136,18181-
18187,18241-18243,18262,18463,18634-
18635,18668,18769,18881,18888,19000,
19007,19020,19191,19194,19220,19283,
19315,19398,19410-19412,19539-
19541,19998-20003,20005,20013-
20014,20034,20046,20048-
20049,20057,20167,20202,20222,20480,
20670,20999-21000,21010,21212-
21213,21221,21553-
21554,21590,21800,21845-21849,22000-
```

22005,22125,22128,22222,22273,22305,
22335,22343,22347,22350-
22351,22537,22555,22763,22800,22951,
23000-23005,23053,23294,23333,23400-
23402,23456-23457,23546,24000-
24006,24242,24249,24321,24323,24386,
24465,24554,24577,24666,24676-
24678,24680,24754,24922,25000-
25009,25576,25604,25793,25900-
25903,26000,26133,26208,26257,26260-
26263,26486-
26487,26489,27010,27017,27345,27442,
27504,27782,27876,27999-
28001,28010,28200,28240,28589,29167,
29999-
30003,30100,30260,30400,30999,31016,
31020,31400,31416,31457,31620,31685,
31765,31948-
31949,32034,32249,32400,32483,32635-
32636,32767-
32777,32801,32811,32896,33000,33060,
33123,33331,33333-
33334,33434,33656,34249,34378-
34379,34567,34962-34964,34980,35000-
35006,35100,35354-
35357,36001,36524,36602,36700,36865,
37475,37483,37601,37654,38000-
38002,38201-
38203,38800,38865,39681,40000,40404,
40841-40843,41111,41121,41230,41794-
41797,42508-42510,43000,43188-
43191,43210,43439-43441,44123,44321-
44323,44444-
44445,44553,44818,44900,45000-
45002,45045,45054,45514,45678,45824-
45825,45966,46336,46998-
47001,47557,47624,47806,47808,48000-
48005,48048-48050,48128-
48129,48556,48619,48653,49000-
49001,49150</port_range>
</target>
<filters id="">
<term>first=1 rows=1000 uuid=
uuid=4b0818d7-e23d-4f9e-995c-
1cdd24fb5bd1 sort=name</term>
<keywords>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>4b0818d7-e23d-4f9e-995c-
1cdd24fb5bd1</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<targets start="1" max="1000"/>
<target_count>
3
<filtered>1</filtered>
<page>1</page>
</target_count>
</get_targets_response>

Fast Target:
This XML file does not appear to have
any style information associated with
it. The document tree is shown below.
<get_targets_response status="200" s
tatus_text="OK">
<target id="b9e0ee69-3e99-4339-a37d-
21b6bbb50607">
<owner>
<name>admin</name>
</owner>
<name>Fast Target</name>
<comment/>
<creation_time>2026-06-
11T12:53:03Z</creation_time>
<modification_time>2026-06-
12T08:08:22Z</modification_time>
<writable>1</writable>
<in_use>1</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<hosts>193.42.15.22, 193.42.15.21,
193.42.15.27</hosts>
<exclude_hosts/>
<max_hosts>3</max_hosts>
<port_list id="33d0cd82-57c6-11e1-
8ed1-406186ea4fc5">
<name>All IANA assigned TCP</name>
<trash>0</trash>
</port_list>
<ssh_credential id="">
<name/>
<port/>
<trash>0</trash>
</ssh_credential>
<smb_credential id="">
<name/>
<trash>0</trash>
</smb_credential>
<esxi_credential id="">
<name/>
<trash>0</trash>
</esxi_credential>
<snmp_credential id="">
<name/>
<trash>0</trash>
</snmp_credential>
<ssh_elevate_credential id="">
<name/>
<trash>0</trash>
</ssh_elevate_credential>
<krb5_credential id="">
<name/>
<trash>0</trash>
</krb5_credential>
<reverse_lookup_only>0</reverse_look
up_only>
<reverse_lookup_unify>0</reverse_loo
kup_unify>
<allow_simultaneous_ips>1</allow_sim
ultaneous_ips>
<alive_tests>
Consider Alive
<alive_test>Consider
Alive</alive_test>
</alive_tests>
<port_range>T:1-3,5,7,9,11,13,17-
25,27,29,31,33,35,37-39,41-46,48-
50,52-59,62-80,82-99,101-113,115-
224,242-248,256-257,259-269,271,280-
284,286-287,308-324,333,344-584,586-
658,660-702,704-707,709-715,729-
731,741-742,744,747-754,758-
765,767,769-777,780,800-802,810,828-
833,847-848,853-854,860-862,873,886-
888,900-903,910-913,953,989-993,995-
1001,1010,1021-1022,1025-
1026,1029,1033-1108,1110-1275,1277-
1300,1303-1490,1492-1527,1529-
1782,1784-2193,2197-2199,2201-
2258,2260-2368,2370-2377,2379-
2681,2683-2692,2694-2793,2795-
2824,2826-2872,2874-2924,2926-
3091,3093-3096,3098-3125,3127-
3300,3302-3321,3326-3366,3372-
3402,3405-3545,3547-3693,3695-
3993,3995-4047,4049-4076,4078-
4083,4085,4087-4143,4145-4172,4174-
4190,4192-4193,4197,4199,4300-
4314,4316,4320-4323,4325-
4336,4340,4343-4360,4368-4379,4389-
4393,4395-4396,4400-4411,4413-
4417,4419-4423,4425-4433,4442-
4458,4484-4488,4500,4535-4538,4545-
4556,4559,4563,4566-4570,4573,4590-
4591,4593-4605,4646,4658-4692,4700-
4704,4711,4725,4727-4728,4730-
4731,4733,4737-4745,4749-
4753,4756,4774,4784,4786-4788,4800-
4803,4827,4837-4851,4867-4871,4876-
4877,4879-4880,4883-4885,4888-
4889,4894,4899-4902,4912-4915,4940-
4942,4949-4953,4969-4971,4984-
4991,4999-5013,5015,5020-5030,5032-
5034,5042-5045,5048-5057,5059-
5075,5080-5087,5093-5094,5099-
5103,5106-5107,5111-5112,5114-
5115,5117,5120,5133-5135,5137,5145-
5146,5150-5152,5154-5157,5161-
5168,5172,5190-5197,5200-
5203,5209,5215,5221-5237,5245,5248-
5254,5264-5265,5269-5272,5280-
5282,5298-5310,5312-5318,5320-
5321,5343-5344,5349,5352-5363,5397-
5435,5443,5445,5450,5453-5456,5461-
5465,5470-5473,5475,5500-
5507,5550,5553-5557,5565-5569,5573-
5575,5579-5586,5597-5605,5618,5627-
5639,5646,5666,5670-5681,5683-
5684,5688-
5689,5693,5696,5700,5705,5713-
5730,5741-5748,5750,5755,5757,5766-
5771,5777,5780-5783,5785,5793,5813-
5814,5841-
5842,5859,5863,5868,5883,5900,5910-
5913,5963,5968-5969,5984-
5993,5999,6064-6066,6068-6077,6084-
6088,6099-6117,6121-
6124,6130,6133,6140-6149,6159-
6163,6200,6209,6222,6241-6244,6251-
6253,6267-6269,6300-6301,6306,6315-
6317,6320-6322,6324-6326,6343-
6344,6346-
6347,6350,6355,6360,6370,6379,6382,6
389-6390,6417-6421,6432,6440,6442-
6446,6455-6456,6464,6471,6480-
6489,6500-6503,6505-6510,6513-
6515,6543-6544,6547-
6551,6558,6566,6568,6579-6583,6600-
6602,6619-6629,6632,6640,6653,6655-
6656,6670-6673,6678-6679,6687-
6690,6697,6701-6703,6714-6716,6767-
6771,6777-6778,6785-
6791,6801,6817,6831,6841-
6842,6850,6868,6888,6900-
6901,6924,6935-6936,6946,6951,6961-
6966,6969-6970,6997-7026,7030-
7031,7070-7073,7080,7099-
7101,7117,7121,7128-7129,7161-
7174,7200-7202,7215-7216,7227-
7229,7236-7237,7244,7262,7272-
7283,7365,7391-7395,7397,7400-
7402,7410-7411,7421,7426-
7431,7437,7443,7471,7473-
7474,7478,7491,7500-7501,7508-
7511,7542-
7549,7551,7560,7563,7566,7569-
7570,7574,7588,7606,7624,7626-
7631,7633,7648,7663,7672-
7677,7680,7683,7687,7689,7697,7700,7
707-7708,7720,7724-
7728,7734,7738,7741-
7744,7747,7775,7777-7779,7781,7786-
7787,7789,7794,7797-7801,7810,7845-
7847,7869-7871,7878,7880,7887,7900-
7903,7913,7932-7933,7962,7967,7979-
7982,7997,7999-8009,8015-8016,8019-
8023,8025-8026,8032-8034,8040-
8044,8051-8059,8066-
8067,8070,8074,8077,8080-8084,8086-
8088,8090-8091,8097,8100-8102,8115-
8118,8121-8122,8128-
8132,8140,8148,8153,8160-8162,8181-
8184,8190-8192,8194-8195,8199-
8201,8204-

8208,8230,8243,8270,8276,8280,8282,8
292-8294,8300-8301,8313,8320-
8322,8351,8376-8380,8383,8400-
8405,8415-8417,8423,8442-
8445,8450,8457,8470-8474,8500-
8502,8554-8555,8567,8600,8610-
8615,8665-
8666,8675,8686,8688,8699,8710-
8711,8733,8750,8763-8770,8778,8786-
8787,8793,8800,8804,8873,8880-
8881,8883,8888-8894,8899-8901,8910-
8913,8937,8953-8954,8980,8989-
8991,8997-9002,9005,9008-9010,9020-
9026,9050-9051,9060,9080,9083-
9093,9100-9107,9111,9119,9122-
9123,9131,9160-9164,9191,9200-
9217,9222,9255,9278-9285,9287,9292-
9295,9300,9306,9310,9312,9318,9321,9
339,9343-9346,9374,9380,9387-
9390,9396-9397,9400-9402,9418,9443-
9445,9450,9500,9535-9536,9555,9592-
9600,9612,9614,9616-9618,9628-
9631,9640,9666-9668,9694-
9695,9700,9747,9750,9753,9762,9800-
9802,9875-9877,9888-
9889,9898,9900,9909,9911,9925,9950-
9955,9966,9978-9979,9981,9987-
9988,9990-10010,10020,10050-
10051,10055,10080-10081,10100-
10104,10107,10110,10113-
10117,10125,10128-10129,10160-
10162,10200-10201,10252,10260-
10261,10288,10321,10443,10540-
10544,10548,10631,10800,10805,10809,
10860,10880,10933,10990,11000-
11001,11095,11103-11106,11109-
11112,11161-11165,11172-11175,11201-
11202,11208,11211,11319-
11321,11367,11371,11489,11600,11623,
11720,11723,11751,11796,11876,11967,
11971,12000-12008,12010,12012-
12013,12109,12121,12168,12172,12300,
12302,12321-
12322,12345,12753,12865,13160,13216-
13218,13223-13224,13400,13720-
13722,13724,13782-13783,13785-
13786,13818-13823,13894,13929-
13930,14000-14001,14033-14034,14141-
14143,14145,14149-
14150,14154,14250,14414,14500,14936-
14937,15000,15002,15345,15363,15555,
15660,15740,15999-16002,16020-
16021,16161-16162,16309-16311,16360-
16361,16367-16368,16384-
16385,16619,16665,16789,16900,16950,
16991-16995,17007,17184-17185,17219-
17221,17223,17225,17234-
17235,17500,17555,17729,17754-
17756,17777,18000,18104,18136,18181-
18187,18241-18243,18262,18463,18634-
18635,18668,18769,18881,18888,19000,
19007,19020,19191,19194,19220,19283,
19315,19398,19410-19412,19539-
19541,19998-20003,20005,20013-
20014,20034,20046,20048-
20049,20057,20167,20202,20222,20480,
20670,20999-21000,21010,21212-
21213,21221,21553-
21554,21590,21800,21845-21849,22000-
22005,22125,22128,22222,22273,22305,
22335,22343,22347,22350-
22351,22537,22555,22763,22800,22951,
23000-23005,23053,23294,23333,23400-
23402,23456-23457,23546,24000-
24006,24242,24249,24321,24323,24386,
24465,24554,24577,24666,24676-
24678,24680,24754,24922,25000-
25009,25576,25604,25793,25900-
25903,26000,26133,26208,26257,26260-
26263,26486-
26487,26489,27010,27017,27345,27442,
27504,27782,27876,27999-
28001,28010,28200,28240,28589,29167,
29999-
30003,30100,30260,30400,30999,31016,
31020,31400,31416,31457,31620,31685,
31765,31948-
31949,32034,32249,32400,32483,32635-
32636,32767-
32777,32801,32811,32896,33000,33060,
33123,33331,33333-
33334,33434,33656,34249,34378-
34379,34567,34962-34964,34980,35000-
35006,35100,35354-
35357,36001,36524,36602,36700,36865,
37475,37483,37601,37654,38000-
38002,38201-
38203,38800,38865,39681,40000,40404,
40841-40843,41111,41121,41230,41794-
41797,42508-42510,43000,43188-
43191,43210,43439-43441,44123,44321-
44323,44444-
44445,44553,44818,44900,45000-
45002,45045,45054,45514,45678,45824-
45825,45966,46336,46998-
47001,47557,47624,47806,47808,48000-
48005,48048-48050,48128-
48129,48556,48619,48653,49000-
49001,49150</port_range>
</target>
<filters id="">
<term>first=1 rows=1000 uuid=
uuid=b9e0ee69-3e99-4339-a37d-
21b6bbb50607 sort=name</term>
<keywords>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>b9e0ee69-3e99-4339-a37d-
21b6bbb50607</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<targets start="1" max="1000"/>
<target_count>
3
<filtered>1</filtered>
<page>1</page>
</target_count>
</get_targets_response>

Full Network Scan:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<get_targets_response status="200" s
tatus_text="OK">
<target id="8f397eee-58b4-48c3-94a5-
5376a44dfce1">
<owner>
<name>admin</name>
</owner>
<name>Full Network Scan</name>
<comment/>
<creation_time>2026-06-
11T11:34:41Z</creation_time>
<modification_time>2026-06-
12T19:39:58Z</modification_time>
<writable>1</writable>
<in_use>1</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<hosts>193.42.15.0/24</hosts>
<exclude_hosts/>
<max_hosts>254</max_hosts>
<port_list id="33d0cd82-57c6-11e1-
8ed1-406186ea4fc5">
<name>All IANA assigned TCP</name>
<trash>0</trash>
</port_list>
<ssh_credential id="82b31ce6-8e93-
4937-9fc4-dc594dfd53ce">
<name>Linux SSH Access</name>
<port>22</port>
<trash>0</trash>
</ssh_credential>
<smb_credential id="8ed45000-ae08-
4bda-a1ac-33cc9e75da5c">
<name>Windows SMB Password</name>
<trash>0</trash>
</smb_credential>
<esxi_credential id="">
<name/>
<trash>0</trash>
</esxi_credential>
<snmp_credential id="">
<name/>
<trash>0</trash>
</snmp_credential>
<ssh_elevate_credential id="">
<name/>
<trash>0</trash>
</ssh_elevate_credential>
<krb5_credential id="">
<name/>
<trash>0</trash>
</krb5_credential>
<reverse_lookup_only>0</reverse_look
up_only>
<reverse_lookup_unify>0</reverse_loo
kup_unify>
<allow_simultaneous_ips>1</allow_sim
ultaneous_ips>
<alive_tests>
ICMP, TCP-ACK Service & ARP Ping
<alive_test>ARP Ping</alive_test>
<alive_test>ICMP Ping</alive_test>
<alive_test>TCP-ACK Service
Ping</alive_test>
</alive_tests>
<port_range>T:1-3,5,7,9,11,13,17-
25,27,29,31,33,35,37-39,41-46,48-
50,52-59,62-80,82-99,101-113,115-
224,242-248,256-257,259-269,271,280-
284,286-287,308-324,333,344-584,586-
658,660-702,704-707,709-715,729-
731,741-742,744,747-754,758-
765,767,769-777,780,800-802,810,828-
833,847-848,853-854,860-862,873,886-
888,900-903,910-913,953,989-993,995-
1001,1010,1021-1022,1025-
1026,1029,1033-1108,1110-1275,1277-
1300,1303-1490,1492-1527,1529-
1782,1784-2193,2197-2199,2201-
2258,2260-2368,2370-2377,2379-
2681,2683-2692,2694-2793,2795-
2824,2826-2872,2874-2924,2926-
3091,3093-3096,3098-3125,3127-
3300,3302-3321,3326-3366,3372-
3402,3405-3545,3547-3693,3695-
3993,3995-4047,4049-4076,4078-
4083,4085,4087-4143,4145-4172,4174-
4190,4192-4193,4197,4199,4300-
4314,4316,4320-4323,4325-
4336,4340,4343-4360,4368-4379,4389-
4393,4395-4396,4400-4411,4413-
4417,4419-4423,4425-4433,4442-
4458,4484-4488,4500,4535-4538,4545-
4556,4559,4563,4566-4570,4573,4590-
4591,4593-4605,4646,4658-4692,4700-
4704,4711,4725,4727-4728,4730-
4731,4733,4737-4745,4749-
4753,4756,4774,4784,4786-4788,4800-
4803,4827,4837-4851,4867-4871,4876-
4877,4879-4880,4883-4885,4888-
4889,4894,4899-4902,4912-4915,4940-
4942,4949-4953,4969-4971,4984-

4991,4999-5013,5015,5020-5030,5032-
5034,5042-5045,5048-5057,5059-
5075,5080-5087,5093-5094,5099-
5103,5106-5107,5111-5112,5114-
5115,5117,5120,5133-5135,5137,5145-
5146,5150-5152,5154-5157,5161-
5168,5172,5190-5197,5200-
5203,5209,5215,5221-5237,5245,5248-
5254,5264-5265,5269-5272,5280-
5282,5298-5310,5312-5318,5320-
5321,5343-5344,5349,5352-5363,5397-
5435,5443,5445,5450,5453-5456,5461-
5465,5470-5473,5475,5500-
5507,5550,5553-5557,5565-5569,5573-
5575,5579-5586,5597-5605,5618,5627-
5639,5646,5666,5670-5681,5683-
5684,5688-
5689,5693,5696,5700,5705,5713-
5730,5741-5748,5750,5755,5757,5766-
5771,5777,5780-5783,5785,5793,5813-
5814,5841-
5842,5859,5863,5868,5883,5900,5910-
5913,5963,5968-5969,5984-
5993,5999,6064-6066,6068-6077,6084-
6088,6099-6117,6121-
6124,6130,6133,6140-6149,6159-
6163,6200,6209,6222,6241-6244,6251-
6253,6267-6269,6300-6301,6306,6315-
6317,6320-6322,6324-6326,6343-
6344,6346-
6347,6350,6355,6360,6370,6379,6382,6
389-6390,6417-6421,6432,6440,6442-
6446,6455-6456,6464,6471,6480-
6489,6500-6503,6505-6510,6513-
6515,6543-6544,6547-
6551,6558,6566,6568,6579-6583,6600-
6602,6619-6629,6632,6640,6653,6655-
6656,6670-6673,6678-6679,6687-
6690,6697,6701-6703,6714-6716,6767-
6771,6777-6778,6785-
6791,6801,6817,6831,6841-
6842,6850,6868,6888,6900-
6901,6924,6935-6936,6946,6951,6961-
6966,6969-6970,6997-7026,7030-
7031,7070-7073,7080,7099-
7101,7117,7121,7128-7129,7161-
7174,7200-7202,7215-7216,7227-
7229,7236-7237,7244,7262,7272-
7283,7365,7391-7395,7397,7400-
7402,7410-7411,7421,7426-
7431,7437,7443,7471,7473-
7474,7478,7491,7500-7501,7508-
7511,7542-
7549,7551,7560,7563,7566,7569-
7570,7574,7588,7606,7624,7626-
7631,7633,7648,7663,7672-
7677,7680,7683,7687,7689,7697,7700,7
707-7708,7720,7724-
7728,7734,7738,7741-
7744,7747,7775,7777-7779,7781,7786-
7787,7789,7794,7797-7801,7810,7845-
7847,7869-7871,7878,7880,7887,7900-
7903,7913,7932-7933,7962,7967,7979-
7982,7997,7999-8009,8015-8016,8019-
8023,8025-8026,8032-8034,8040-
8044,8051-8059,8066-
8067,8070,8074,8077,8080-8084,8086-
8088,8090-8091,8097,8100-8102,8115-
8118,8121-8122,8128-
8132,8140,8148,8153,8160-8162,8181-
8184,8190-8192,8194-8195,8199-
8201,8204-
8208,8230,8243,8270,8276,8280,8282,8
292-8294,8300-8301,8313,8320-
8322,8351,8376-8380,8383,8400-
8405,8415-8417,8423,8442-
8445,8450,8457,8470-8474,8500-
8502,8554-8555,8567,8600,8610-
8615,8665-
8666,8675,8686,8688,8699,8710-
8711,8733,8750,8763-8770,8778,8786-
8787,8793,8800,8804,8873,8880-
8881,8883,8888-8894,8899-8901,8910-
8913,8937,8953-8954,8980,8989-
8991,8997-9002,9005,9008-9010,9020-
9026,9050-9051,9060,9080,9083-
9093,9100-9107,9111,9119,9122-
9123,9131,9160-9164,9191,9200-
9217,9222,9255,9278-9285,9287,9292-
9295,9300,9306,9310,9312,9318,9321,9
339,9343-9346,9374,9380,9387-
9390,9396-9397,9400-9402,9418,9443-
9445,9450,9500,9535-9536,9555,9592-
9600,9612,9614,9616-9618,9628-
9631,9640,9666-9668,9694-
9695,9700,9747,9750,9753,9762,9800-
9802,9875-9877,9888-
9889,9898,9900,9909,9911,9925,9950-
9955,9966,9978-9979,9981,9987-
9988,9990-10010,10020,10050-
10051,10055,10080-10081,10100-
10104,10107,10110,10113-
10117,10125,10128-10129,10160-
10162,10200-10201,10252,10260-
10261,10288,10321,10443,10540-
10544,10548,10631,10800,10805,10809,
10860,10880,10933,10990,11000-
11001,11095,11103-11106,11109-
11112,11161-11165,11172-11175,11201-
11202,11208,11211,11319-
11321,11367,11371,11489,11600,11623,
11720,11723,11751,11796,11876,11967,
11971,12000-12008,12010,12012-
12013,12109,12121,12168,12172,12300,
12302,12321-
12322,12345,12753,12865,13160,13216-
13218,13223-13224,13400,13720-
13722,13724,13782-13783,13785-
13786,13818-13823,13894,13929-
13930,14000-14001,14033-14034,14141-
14143,14145,14149-
14150,14154,14250,14414,14500,14936-
14937,15000,15002,15345,15363,15555,
15660,15740,15999-16002,16020-
16021,16161-16162,16309-16311,16360-
16361,16367-16368,16384-
16385,16619,16665,16789,16900,16950,
16991-16995,17007,17184-17185,17219-
17221,17223,17225,17234-
17235,17500,17555,17729,17754-
17756,17777,18000,18104,18136,18181-
18187,18241-18243,18262,18463,18634-
18635,18668,18769,18881,18888,19000,
19007,19020,19191,19194,19220,19283,
19315,19398,19410-19412,19539-
19541,19998-20003,20005,20013-
20014,20034,20046,20048-
20049,20057,20167,20202,20222,20480,
20670,20999-21000,21010,21212-
21213,21221,21553-
21554,21590,21800,21845-21849,22000-
22005,22125,22128,22222,22273,22305,
22335,22343,22347,22350-
22351,22537,22555,22763,22800,22951,
23000-23005,23053,23294,23333,23400-
23402,23456-23457,23546,24000-
24006,24242,24249,24321,24323,24386,
24465,24554,24577,24666,24676-
24678,24680,24754,24922,25000-
25009,25576,25604,25793,25900-
25903,26000,26133,26208,26257,26260-
26263,26486-
26487,26489,27010,27017,27345,27442,
27504,27782,27876,27999-
28001,28010,28200,28240,28589,29167,
29999-
30003,30100,30260,30400,30999,31016,
31020,31400,31416,31457,31620,31685,
31765,31948-
31949,32034,32249,32400,32483,32635-
32636,32767-
32777,32801,32811,32896,33000,33060,
33123,33331,33333-
33334,33434,33656,34249,34378-
34379,34567,34962-34964,34980,35000-
35006,35100,35354-
35357,36001,36524,36602,36700,36865,
37475,37483,37601,37654,38000-
38002,38201-
38203,38800,38865,39681,40000,40404,
40841-40843,41111,41121,41230,41794-
41797,42508-42510,43000,43188-
43191,43210,43439-43441,44123,44321-
44323,44444-
44445,44553,44818,44900,45000-
45002,45045,45054,45514,45678,45824-
45825,45966,46336,46998-
47001,47557,47624,47806,47808,48000-
48005,48048-48050,48128-
48129,48556,48619,48653,49000-
49001,49150</port_range>
</target>
<filters id="">
<term>first=1 rows=1000 uuid=
uuid=8f397eee-58b4-48c3-94a5-
5376a44dfce1 sort=name</term>
<keywords>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>8f397eee-58b4-48c3-94a5-
5376a44dfce1</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<targets start="1" max="1000"/>
<target_count>
3
<filtered>1</filtered>
<page>1</page>
</target_count>
</get_targets_response>

Fast Audit:

```
<get_tasks_response status="200" sta
tus_text="OK">
<apply_overrides>0</apply_overrides>
<task id="8171af3c-16c4-4cc1-8ccd-
0a987ce1dd12">
<owner>
<name>admin</name>
</owner>
<name>Fast Audit</name>
<comment/>
<creation_time>2026-06-
12T08:09:58Z</creation_time>
<modification_time>2026-06-
12T08:09:58Z</modification_time>
<writable>1</writable>
<in_use>0</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<alterable>0</alterable>
<usage_type>scan</usage_type>
<config id="daba56c8-73ec-11df-a475-
002264764cea">
<name>Full and fast</name>
<trash>0</trash>
</config>
<target id="b9e0ee69-3e99-4339-a37d-
21b6bbb50607">
<name>Fast Target</name>
<trash>0</trash>
</target>
<scanner id="08b69003-5fc2-4037-
a479-93b440211c73">
<name>OpenVAS Default</name>
<type>2</type>
<trash>0</trash>
</scanner>
<status>Done</status>
<progress>-1</progress>
<report_count>
1
<finished>1</finished>
</report_count>
<trend/>
<schedule id="">
<name/>
<trash>0</trash>
</schedule>
<schedule_periods>0</schedule_period
s>
<last_report>
<report id="5fd10a4f-1bad-4b79-bf0c-
dc69ea458336">
<timestamp>2026-06-
12T08:12:00Z</timestamp>
<scan_start>2026-06-
12T08:12:18Z</scan_start>
<scan_end>2026-06-
12T09:06:07Z</scan_end>
<result_count>
<critical>13</critical>
<hole deprecated="1">10</hole>
<high>10</high>
<info deprecated="1">7</info>
<low>7</low>
<log>104</log>
<warning deprecated="1">39</warning>
<medium>39</medium>
<false_positive>0</false_positive>
</result_count>
<severity>10.0</severity>
</report>
</last_report>
<observers/>
<average_duration>3229</average_dura
tion>
<result_count>166</result_count>
<preferences>
<preference>
<name>Maximum concurrently executed
NVTs per host</name>
<scanner_name>max_checks</scanner_na
me>
<value>4</value>
</preference>
<preference>
<name>Maximum concurrently scanned
hosts</name>
<scanner_name>max_hosts</scanner_nam
e>
<value>20</value>
</preference>
<preference>
<name>Add results to Asset
Management</name>
<scanner_name>in_assets</scanner_nam
e>
<value>yes</value>
</preference>
<preference>
<name>Apply Overrides when adding
Assets</name>
<scanner_name>assets_apply_overrides
</scanner_name>
<value>yes</value>
</preference>
<preference>
<name>Min QOD when adding
Assets</name>
<scanner_name>assets_min_qod</scanne
r_name>
<value>70</value>
</preference>
<preference>
<name>Auto Delete Reports</name>
<scanner_name>auto_delete</scanner_n
ame>
<value>no</value>
</preference>
<preference>
<name>Auto Delete Reports
Data</name>
<scanner_name>auto_delete_data</scan
ner_name>
<value>5</value>
</preference>
</preferences>
</task>
<filters id="">
<term>apply_overrides=0 min_qod=70
first=1 rows=1000 uuid=
uuid=8171af3c-16c4-4cc1-8ccd-
0a987ce1dd12 sort=name</term>
<keywords>
<keyword>
<column>apply_overrides</column>
<relation>=</relation>
<value>0</value>
</keyword>
<keyword>
<column>min_qod</column>
<relation>=</relation>
<value>70</value>
</keyword>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>8171af3c-16c4-4cc1-8ccd-
0a987ce1dd12</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<tasks start="1" max="1000"/>
<task_count>
3
<filtered>1</filtered>
<page>1</page>
</task_count>
</get_tasks_response>
```

White Box Audit:

```
<get_tasks_response status="200" sta
tus_text="OK">
<apply_overrides>0</apply_overrides>
<task id="57fc01d8-e2bc-475f-9051-
3f38e54858a5">
<owner>
<name>admin</name>
</owner>
<name>White Box Audit</name>
<comment/>
<creation_time>2026-06-
12T11:46:02Z</creation_time>
<modification_time>2026-06-
12T11:46:02Z</modification_time>
<writable>1</writable>
<in_use>0</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<alterable>0</alterable>
<usage_type>scan</usage_type>
<config id="daba56c8-73ec-11df-a475-
002264764cea">
<name>Full and fast</name>
<trash>0</trash>
</config>
<target id="4b0818d7-e23d-4f9e-995c-
1cdd24fb5bd1">
<name>Authenticated Target</name>
<trash>0</trash>
</target>
<scanner id="08b69003-5fc2-4037-
a479-93b440211c73">
<name>OpenVAS Default</name>
<type>2</type>
<trash>0</trash>
</scanner>
<status>Done</status>
<progress>-1</progress>
<report_count>
2
<finished>2</finished>
</report_count>
<trend>same</trend>
<schedule id="">
<name/>
<trash>0</trash>
</schedule>
<schedule_periods>0</schedule_period
s>
<last_report>
<report id="d24f1c3e-c859-4d4b-88a0-
d6c59ad251e5">
<timestamp>2026-06-
12T17:41:20Z</timestamp>
<scan_start>2026-06-
12T17:41:36Z</scan_start>
<scan_end>2026-06-
12T18:31:57Z</scan_end>
<result_count>
<critical>0</critical>
<hole deprecated="1">0</hole>
<high>0</high>
<info deprecated="1">5</info>
<low>5</low>
```

<log>54</log>
<warning deprecated="1">1</warning>
<medium>1</medium>
<false_positive>0</false_positive>
</result_count>
<severity>5.0</severity>
</report>
</last_report>
<observers/>
<average_duration>2779</average_dura
tion>
<result_count>91</result_count>
<preferences>
<preference>
<name>Maximum concurrently executed
NVTs per host</name>
<scanner_name>max_checks</scanner_na
me>
<value>4</value>
</preference>
<preference>
<name>Maximum concurrently scanned
hosts</name>
<scanner_name>max_hosts</scanner_nam
e>
<value>10</value>
</preference>
<preference>
<name>Add results to Asset
Management</name>
<scanner_name>in_assets</scanner_nam
e>
<value>yes</value>
</preference>
<preference>
<name>Apply Overrides when adding
Assets</name>
<scanner_name>assets_apply_overrides
</scanner_name>
<value>yes</value>
</preference>
<preference>
<name>Min QOD when adding
Assets</name>
<scanner_name>assets_min_qod</scanne
r_name>
<value>70</value>
</preference>
<preference>
<name>Auto Delete Reports</name>
<scanner_name>auto_delete</scanner_n
ame>
<value>no</value>
</preference>
<preference>
<name>Auto Delete Reports
Data</name>
<scanner_name>auto_delete_data</scan
ner_name>
<value>5</value>
</preference>
</preferences>
</task>
<filters id="">
<term>apply_overrides=0 min_qod=70
first=1 rows=1000 uuid=
uuid=57fc01d8-e2bc-475f-9051-
3f38e54858a5 sort=name</term>
<keywords>
<keyword>
<column>apply_overrides</column>
<relation>=</relation>
<value>0</value>
</keyword>
<keyword>
<column>min_qod</column>
<relation>=</relation>
<value>70</value>
</keyword>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>57fc01d8-e2bc-475f-9051-
3f38e54858a5</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<tasks start="1" max="1000"/>
<task_count>
3
<filtered>1</filtered>
<page>1</page>
</task_count>
</get_tasks_response>

Full Network Audit:

<get_tasks_response status="200" sta
tus_text="OK">
<apply_overrides>0</apply_overrides>
<task id="56138b44-418f-4fd3-a26f-
6048bbaca62e">
<owner>
<name>admin</name>
</owner>
<name>Full Network Audit</name>
<comment/>
<creation_time>2026-06-
12T19:22:06Z</creation_time>
<modification_time>2026-06-
12T19:22:06Z</modification_time>
<writable>1</writable>
<in_use>0</in_use>
<permissions>
<permission>
<name>Everything</name>
</permission>
</permissions>
<alterable>0</alterable>
<usage_type>scan</usage_type>
<config id="daba56c8-73ec-11df-a475-
002264764cea">
<name>Full and fast</name>
<trash>0</trash>
</config>
<target id="8f397eee-58b4-48c3-94a5-
5376a44dfce1">
<name>Full Network Scan</name>
<trash>0</trash>
</target>
<scanner id="08b69003-5fc2-4037-
a479-93b440211c73">
<name>OpenVAS Default</name>
<type>2</type>
<trash>0</trash>
</scanner>
<status>Done</status>
<progress>-1</progress>
<report_count>
2
<finished>2</finished>
</report_count>
<trend>up</trend>
<schedule id="">
<name/>
<trash>0</trash>
</schedule>
<schedule_periods>0</schedule_period
s>
<last_report>
<report id="221500d5-ace2-43f7-9c8d-
e28a4d1848f7">
<timestamp>2026-06-
12T19:40:06Z</timestamp>
<scan_start>2026-06-
12T19:40:32Z</scan_start>
<scan_end>2026-06-
12T21:00:37Z</scan_end>
<result_count>
<critical>13</critical>
<hole deprecated="1">10</hole>
<high>10</high>
<info deprecated="1">19</info>
<low>19</low>
<log>195</log>
<warning deprecated="1">50</warning>
<medium>50</medium>
<false_positive>0</false_positive>
</result_count>
<severity>10.0</severity>
</report>
</last_report>
<observers/>
<average_duration>2681</average_dura
tion>
<result_count>298</result_count>
<preferences>
<preference>
<name>Maximum concurrently executed
NVTs per host</name>
<scanner_name>max_checks</scanner_na
me>
<value>10</value>
</preference>
<preference>
<name>Maximum concurrently scanned
hosts</name>
<scanner_name>max_hosts</scanner_nam
e>
<value>2</value>
</preference>
<preference>
<name>Add results to Asset
Management</name>
<scanner_name>in_assets</scanner_nam
e>
<value>yes</value>
</preference>
<preference>
<name>Apply Overrides when adding
Assets</name>
<scanner_name>assets_apply_overrides
</scanner_name>
<value>yes</value>
</preference>
<preference>
<name>Min QOD when adding
Assets</name>
<scanner_name>assets_min_qod</scanne
r_name>
<value>70</value>
</preference>
<preference>
<name>Auto Delete Reports</name>
<scanner_name>auto_delete</scanner_n
ame>
<value>no</value>
</preference>
<preference>
<name>Auto Delete Reports
Data</name>
<scanner_name>auto_delete_data</scan
ner_name>
<value>5</value>
</preference>
</preferences>
</task>
<filters id="">
<term>apply_overrides=0 min_qod=70
first=1 rows=1000 uuid=
uuid=56138b44-418f-4fd3-a26f-
6048bbaca62e sort=name</term>
<keywords>
<keyword>
<column>apply_overrides</column>
<relation>=</relation>
<value>0</value>
</keyword>
<keyword>
<column>min_qod</column>
<relation>=</relation>

```
<value>70</value>
</keyword>
<keyword>
<column>first</column>
<relation>=</relation>
<value>1</value>
</keyword>
<keyword>
<column>rows</column>
<relation>=</relation>
<value>1000</value>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value/>
</keyword>
<keyword>
<column>uuid</column>
<relation>=</relation>
<value>56138b44-418f-4fd3-a26f-
6048bbaca62e</value>
</keyword>
<keyword>
<column>sort</column>
<relation>=</relation>
<value>name</value>
</keyword>
</keywords>
</filters>
<sort>
<field>
name
<order>ascending</order>
</field>
</sort>
<tasks start="1" max="1000"/>
<task_count>
3
<filtered>1</filtered>
<page>1</page>
</task_count>
</get_tasks_response>
```

Конфігураційні файли Targets (Цілі)

```
I Summary
=========

This document reports on the results
of an automatic security scan.
The report first summarises the
results found.
Then, for each host, the report
describes every issue found.
Please consider the advice given in
each description, in order to
rectify
the issue.

All dates are displayed using the
timezone "Coordinated Universal
Time",
which is abbreviated "UTC".

Vendor security updates are not
trusted.

Overrides are off.  Even when a
result has an override, this report
uses
the actual threat of the result.

Notes are included in the
report.Information on overrides is
included in the report.

This report might not show details
of all issues that were found.
Issues with the threat level "Log"
are not shown.
Issues with the threat level "Debug"
are not shown.
Issues with the threat level "False
Positive" are not shown.
Only results with a minimum QoD of
70 are shown.

This report contains all 92 results
selected by the
filtering described above.  Before
filtering there were 919 results.

Scan started: Fri Jun 12 19:40:32
2026 UTC
Scan ended:   Fri Jun 12 21:00:37
2026 UTC
Task:         Full Network Audit

Host Summary
************

Host            Critical  High
Medium  Low  Log  False Positive
193.42.15.1            0     0
2    2    0              0
193.42.15.2            0     0
2    2    0              0
193.42.15.3            0     0
2    2    0              0
193.42.15.21           0     0
0    4    0              0
193.42.15.22          13    10
41    6    0             0
193.42.15.25           0     0
0    0    0              0
193.42.15.27           0     0
1    1    0              0
193.42.15.254          0     0
2    2    0              0
Total: 8              13    10
50   19    0             0


II Results per Host
===================

Host 193.42.15.1
****************

Scanning of this host started at:
Fri Jun 12 19:45:57 2026 UTC
Number of results: 4

Port Summary for Host 193.42.15.1
---------------------------------

Service (Port)          Threat Level
22/tcp                  Medium
(CVSS: 5.3)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host 193.42.15.1
------------------------------------

Issue
-----
NVT:    Weak Key Exchange (KEX)
Algorithm(s) Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.150713
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak key
  exchange (KEX) algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak KEX algorithm(s):
KEX algorithm                      |
Reason
-----------------------------------
-----------------------------------
--------!
-----------
diffie-hellman-group-exchange-sha1 |
Using SHA-1
diffie-hellman-group1-sha1         |
Using Oakley Group 2 (a 1024-bit
MODP group!
) and SHA-1

Impact:
An attacker can quickly break
individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX
algorithm(s)
  - 1024-bit MODP group / prime KEX
algorithms:
  Alternatively use elliptic-curve
Diffie-Hellmann in general, e.g.
Curve 25519.

Vulnerability Insight:
- 1024-bit MODP group / prime KEX
algorithms:
  Millions of HTTPS, SSH, and VPN
servers all use the same prime
numbers for Dif!
fie-Hellman key
  exchange. Practitioners believed
this was safe as long as new key
exchange mes!
sages were generated
  for every connection. However, the
first step in the number field
sieve-the mo!
st efficient
  algorithm for breaking a Diffie-
Hellman connection-is dependent only
on this p!
rime.
  A nation-state can break a 1024-
bit prime.

Vulnerability Detection Method:
Checks the supported KEX algorithms
of the remote SSH server.
  Currently weak KEX algorithms are
defined as the following:
  - non-elliptic-curve Diffie-
Hellmann (DH) KEX algorithms with
1024-bit MODP gr!
oup / prime
  - ephemerally generated key
exchange groups uses SHA-1
  - using RSA 1024-bit modulus key
Details:
Weak Key Exchange (KEX) Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.150713)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url:
https://weakdh.org/sysadmin.html
 url: https://www.rfc-
editor.org/rfc/rfc9142
 url: https://www.rfc-
editor.org/rfc/rfc9142#name-summary-
guidance-for-implem
 url: https://www.rfc-
editor.org/rfc/rfc6194
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.5


Issue
-----
NVT:    Weak Encryption Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105611
Threat: Medium (CVSS: 4.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak
  encryption algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

```
The remote SSH server supports the
following weak server-to-client
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption
algorithm(s).

Vulnerability Insight:
- The 'arcfour' cipher is the
Arcfour stream cipher with 128-bit
  keys. The Arcfour cipher is
believed to be compatible with the
RC4 cipher [SCH!
NEIER]. Arcfour
  (and RC4) has problems with weak
keys, and should not be used
anymore.
  - The 'none' algorithm specifies
that no encryption is to be done.
Note that t!
his method provides
  no confidentiality protection, and
it is NOT RECOMMENDED to use it.
  - A vulnerability exists in SSH
messages that employ CBC mode that
may allow a!
n attacker to
  recover plaintext from a block of
ciphertext.

Vulnerability Detection Method:
Checks the supported encryption
algorithms (client-to-server
  and server-to-client) of the
remote SSH server.
  Currently weak encryption
algorithms are defined as the
following:
  - Arcfour (RC4) cipher based
algorithms
  - 'none' algorithm
  - CBC mode cipher based algorithms
Details:
Weak Encryption Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8758
 url:
https://www.kb.cert.org/vuls/id/9585
63
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.3


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.2
****************

Scanning of this host started at:
Fri Jun 12 19:57:41 2026 UTC
Number of results: 4

Port Summary for Host 193.42.15.2
---------------------------------

Service (Port)          Threat Level
22/tcp                  Medium
(CVSS: 5.3)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host 193.42.15.2
------------------------------------

Issue
-----
NVT:    Weak Key Exchange (KEX)
Algorithm(s) Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.150713
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak key
  exchange (KEX) algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak KEX algorithm(s):
KEX algorithm                      |
Reason
-----------------------------------
-----------------------------------
--------!
-----------
```

```
diffie-hellman-group-exchange-sha1 |
Using SHA-1
diffie-hellman-group1-sha1         |
Using Oakley Group 2 (a 1024-bit
MODP group!
) and SHA-1

Impact:
An attacker can quickly break
individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX
algorithm(s)
  - 1024-bit MODP group / prime KEX
algorithms:
  Alternatively use elliptic-curve
Diffie-Hellmann in general, e.g.
Curve 25519.

Vulnerability Insight:
- 1024-bit MODP group / prime KEX
algorithms:
  Millions of HTTPS, SSH, and VPN
servers all use the same prime
numbers for Dif!
fie-Hellman key
  exchange. Practitioners believed
this was safe as long as new key
exchange mes!
sages were generated
  for every connection. However, the
first step in the number field
sieve-the mo!
st efficient
  algorithm for breaking a Diffie-
Hellman connection-is dependent only
on this p!
rime.
  A nation-state can break a 1024-
bit prime.

Vulnerability Detection Method:
Checks the supported KEX algorithms
of the remote SSH server.
  Currently weak KEX algorithms are
defined as the following:
  - non-elliptic-curve Diffie-
Hellmann (DH) KEX algorithms with
1024-bit MODP gr!
oup / prime
  - ephemerally generated key
exchange groups uses SHA-1
  - using RSA 1024-bit modulus key
Details:
Weak Key Exchange (KEX) Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.150713)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url:
https://weakdh.org/sysadmin.html
 url: https://www.rfc-
editor.org/rfc/rfc9142
 url: https://www.rfc-
editor.org/rfc/rfc9142#name-summary-
guidance-for-implem
 url: https://www.rfc-
editor.org/rfc/rfc6194
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.5


Issue
-----
NVT:    Weak Encryption Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105611
Threat: Medium (CVSS: 4.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak
  encryption algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The remote SSH server supports the
following weak server-to-client
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption
algorithm(s).

Vulnerability Insight:
- The 'arcfour' cipher is the
Arcfour stream cipher with 128-bit
  keys. The Arcfour cipher is
believed to be compatible with the
RC4 cipher [SCH!
NEIER]. Arcfour
  (and RC4) has problems with weak
keys, and should not be used
anymore.
  - The 'none' algorithm specifies
that no encryption is to be done.
Note that t!
his method provides
  no confidentiality protection, and
it is NOT RECOMMENDED to use it.
  - A vulnerability exists in SSH
messages that employ CBC mode that
may allow a!
n attacker to
  recover plaintext from a block of
ciphertext.

Vulnerability Detection Method:
Checks the supported encryption
algorithms (client-to-server
  and server-to-client) of the
remote SSH server.
  Currently weak encryption
algorithms are defined as the
following:
  - Arcfour (RC4) cipher based
algorithms
  - 'none' algorithm
  - CBC mode cipher based algorithms
Details:
Weak Encryption Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8758
 url:
https://www.kb.cert.org/vuls/id/9585
63
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.3


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
```

```
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.3
****************

Scanning of this host started at:
Fri Jun 12 19:52:50 2026 UTC
Number of results: 4

Port Summary for Host 193.42.15.3
---------------------------------

Service (Port)          Threat Level
22/tcp                  Medium
(CVSS: 5.3)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host 193.42.15.3
------------------------------------

Issue
-----
NVT:    Weak Key Exchange (KEX)
Algorithm(s) Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.150713
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak key
  exchange (KEX) algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak KEX algorithm(s):
KEX algorithm                     |
Reason
----------------------------------
----------------------------------
--------!
-----------
diffie-hellman-group-exchange-sha1 |
Using SHA-1
diffie-hellman-group1-sha1        |
Using Oakley Group 2 (a 1024-bit
MODP group!
) and SHA-1

Impact:
An attacker can quickly break
individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX
algorithm(s)
  - 1024-bit MODP group / prime KEX
algorithms:
  Alternatively use elliptic-curve
Diffie-Hellmann in general, e.g.
Curve 25519.

Vulnerability Insight:
- 1024-bit MODP group / prime KEX
algorithms:
  Millions of HTTPS, SSH, and VPN
servers all use the same prime
numbers for Dif!
fie-Hellman key
  exchange. Practitioners believed
this was safe as long as new key
exchange mes!
sages were generated
  for every connection. However, the
first step in the number field
sieve-the mo!
st efficient
  algorithm for breaking a Diffie-
Hellman connection-is dependent only
on this p!
rime.
  A nation-state can break a 1024-
bit prime.

Vulnerability Detection Method:
Checks the supported KEX algorithms
of the remote SSH server.
  Currently weak KEX algorithms are
defined as the following:
  - non-elliptic-curve Diffie-
Hellmann (DH) KEX algorithms with
1024-bit MODP gr!
oup / prime
  - ephemerally generated key
exchange groups uses SHA-1
  - using RSA 1024-bit modulus key
Details:
Weak Key Exchange (KEX) Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.150713)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url:
https://weakdh.org/sysadmin.html
 url: https://www.rfc-
editor.org/rfc/rfc9142
 url: https://www.rfc-
editor.org/rfc/rfc9142#name-summary-
guidance-for-implem
 url: https://www.rfc-
editor.org/rfc/rfc6194
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.5


Issue
-----
NVT:    Weak Encryption Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105611
Threat: Medium (CVSS: 4.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak
  encryption algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The remote SSH server supports the
following weak server-to-client
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption
algorithm(s).

Vulnerability Insight:
- The 'arcfour' cipher is the
Arcfour stream cipher with 128-bit
  keys. The Arcfour cipher is
believed to be compatible with the
RC4 cipher [SCH!
NEIER]. Arcfour
  (and RC4) has problems with weak
keys, and should not be used
anymore.
  - The 'none' algorithm specifies
that no encryption is to be done.
Note that t!
his method provides
  no confidentiality protection, and
it is NOT RECOMMENDED to use it.
  - A vulnerability exists in SSH
messages that employ CBC mode that
may allow a!
n attacker to
  recover plaintext from a block of
ciphertext.

Vulnerability Detection Method:
Checks the supported encryption
algorithms (client-to-server
  and server-to-client) of the
remote SSH server.
  Currently weak encryption
algorithms are defined as the
following:
```

```
  - Arcfour (RC4) cipher based
algorithms
  - 'none' algorithm
  - CBC mode cipher based algorithms
Details:
Weak Encryption Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8758
 url:
https://www.kb.cert.org/vuls/id/9585
63
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.3


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.21
**********

Scanning of this host started at:
Fri Jun 12 19:43:34 2026 UTC
Number of results: 4

Port Summary for Host 193.42.15.21
----------------------------------

Service (Port)          Threat Level
general/tcp             Low (CVSS:
3.8)
22/tcp                  Low (CVSS:
2.6)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host
193.42.15.21
------------------------------------
-

Issue
-----
NVT:    Missing Linux Kernel
mitigations for 'TSA' hardware
vulnerabilities (AMD-SB-7029)
OID:    1.3.6.1.4.1.25623.1.0.119211
Threat: Low (CVSS: 3.8)
Port:   general/tcp

Product detection result:
cpe:/a:linux:kernel
Detected by: Detection of Linux
Kernel mitigation status for
hardware vulnerabilities (OID:
1.3.6.1.4.1.25623.1.0.108765)

Summary:
The remote host is missing one or
more known mitigation(s) on
  Linux Kernel side for the
referenced 'AMD Transient Scheduler
Attacks' (TSA) h!
ardware
  vulnerabilities.

Vulnerability Detection Result:
The Linux Kernel on the remote host
is missing the mitigation for the
"tsa" hard!
ware vulnerability as reported by
the sysfs interface:
sysfs file checked
| Linux Kernel status (SSH response)
------------------------------------
------------------------------------
--------!
-------------------
/sys/devices/system/cpu/vulnerabilit
ies/tsa | Vulnerable: Clear CPU
buffers atte!
mpted, no microcode
Notes on the "Linux Kernel status
(SSH response)" column:
- sysfs file missing: The sysfs
interface is available but the sysfs
file for th!
is specific vulnerability is
missing. This means the current
Linux Kernel doesn'!
t know this vulnerability yet. Based
on this it is assumed that it
doesn't provi!
de any mitigation and that the
target system is vulnerable.
- Strings including "Mitigation:",
"Not affected" or "Vulnerable" are
reported d!
irectly by the Linux Kernel.
- All other strings are responses to
various SSH commands.

Solution:
Solution type: VendorFix
The following solutions exist:
  - Update to a more recent Linux
Kernel to receive mitigations on
Kernel level !
and info about
  the mitigation status from it
  - Enable the mitigation(s) in the
Linux Kernel (might be disabled
depending on!
```

```
 the configuration)
  Additional possible mitigations
(if provided by the vendor) are to:
  - install a Microcode update
  - update the BIOS of the Mainboard
  Note: Please create an override
for this result if one of the
following applie!
s:
  - the sysfs file is not available
but other mitigations like a
Microcode updat!
e is already in
  place
  - the sysfs file is not available
but the CPU of the host is not
affected
  - the reporting of the Linux
Kernel is not correct (this is out
of the control!
 of this VT)

Affected Software/OS:
Various AMD CPUs. Please see the
references for the full list
  of affected CPUs.

Vulnerability Insight:
The following flaws exist:
  - CVE-2024-36348: A transient
execution vulnerability may allow a
user process!
 to infer the
  control registers speculatively
even if UMIP[3] feature is enabled,
potentiall!
y resulting in
  information leakage.
  - CVE-2024-36349: A transient
execution vulnerability may allow a
user process!
 to infer TSC_AUX
  even when such a read is disabled,
potentially resulting in information
leakag!
e.
  - CVE-2024-36350: A transient
execution vulnerability may allow an
attacker to!
 infer data from
  previous stores, potentially
resulting in the leakage of
privileged informatio!
n.
  - CVE-2024-36357: A transient
execution vulnerability may allow an
attacker to!
 infer data in the
  L1D cache, potentially resulting
in the leakage of sensitive
information acros!
s privileged
  boundaries.

Vulnerability Detection Method:
Checks previous gathered information
on the mitigation status
  reported by the Linux Kernel.
Details:
Missing Linux Kernel mitigations for
'TSA' hardware vulnerabilities (AMD-
SB-...
(OID: 1.3.6.1.4.1.25623.1.0.119211)
Version used: 2026-01-14T05:47:41Z

Product Detection Result:
Product:cpe:/a:linux:kernel

Method:Detection of Linux Kernel
mitigation status for hardware
vulnerabilities
(OID: 1.3.6.1.4.1.25623.1.0.108765)

References:
 cve: CVE-2024-36348
 cve: CVE-2024-36349
 cve: CVE-2024-36350
 cve: CVE-2024-36357
 url: https://docs.kernel.org/admin-
guide/hw-vuln/index.html
 url:
https://www.amd.com/en/resources/pro
duct-security/bulletin/amd-sb-
7029.html
 cert-bund: WID-SEC-2025-1850
 cert-bund: WID-SEC-2025-1502
 dfn-cert: DFN-CERT-2026-1712
 dfn-cert: DFN-CERT-2025-3377
 dfn-cert: DFN-CERT-2025-3133
 dfn-cert: DFN-CERT-2025-2173
 dfn-cert: DFN-CERT-2025-1912
 dfn-cert: DFN-CERT-2025-1908
 dfn-cert: DFN-CERT-2025-1839
 dfn-cert: DFN-CERT-2025-1835
 dfn-cert: DFN-CERT-2025-1833
 dfn-cert: DFN-CERT-2025-1825
 dfn-cert: DFN-CERT-2025-1811


Issue
-----
NVT:    TCP Timestamps Information
Disclosure
OID:    1.3.6.1.4.1.25623.1.0.80091
Threat: Low (CVSS: 2.6)
Port:   general/tcp

Summary:
The remote host implements TCP
timestamps and therefore allows
  to compute the uptime.

Vulnerability Detection Result:
It was detected that the host
implements RFC1323/RFC7323.
The following timestamps were
retrieved with a delay of 1 seconds
in-between:
Packet 1: 2849880309
Packet 2: 2849881370

Impact:
A side effect of this feature is
that the uptime of the remote
  host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux
add the line
  'net.ipv4.tcp_timestamps = 0' to
/etc/sysctl.conf. Execute 'sysctl -
p' to appl!
y the settings at
  runtime.
  To disable TCP timestamps on
Windows execute 'netsh int tcp set
global timesta!
mps=disabled'
  Starting with Windows Server 2008
and Vista, the timestamp can not be
complete!
ly disabled.
  The default behavior of the TCP/IP
stack on this Systems is to not use
the Tim!
estamp options when
  initiating TCP connections, but
use them if the TCP peer that is
initiating co!
mmunication includes
  them in their synchronize (SYN)
segment.
  See the references for more
information.

Affected Software/OS:
TCP implementations that implement
RFC1323/RFC7323.

Vulnerability Insight:
The remote host implements TCP
timestamps, as defined by
  RFC1323/RFC7323.

Vulnerability Detection Method:
Special IP packets are forged and
sent with a little delay in
  between to the target IP. The
responses are searched for a
timestamps. If foun!
d, the timestamps
  are reported.
Details:
TCP Timestamps Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.80091)
Version used: 2023-12-15T16:10:08Z

References:
 url:
https://datatracker.ietf.org/doc/htm
l/rfc1323
 url:
https://datatracker.ietf.org/doc/htm
l/rfc7323
 url:
https://web.archive.org/web/20151213
072445/http://www.microsoft.com/en-
us/download/details.aspx?id=9152
 url:
https://www.fortiguard.com/psirt/FG-
IR-16-090


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol
```

```
Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.22
**********

Scanning of this host started at:
Fri Jun 12 20:19:09 2026 UTC
Number of results: 70

Port Summary for Host 193.42.15.22
----------------------------------

Service (Port)          Threat Level
1524/tcp                Critical
(CVSS: 10.0)
512/tcp                 Critical
(CVSS: 10.0)
513/tcp                 Critical
(CVSS: 10.0)
80/tcp                  Critical
(CVSS: 10.0)
8787/tcp                Critical
(CVSS: 10.0)
general/tcp             Critical
(CVSS: 10.0)
21/tcp                  Critical
(CVSS: 9.8)
3306/tcp                Critical
(CVSS: 9.8)
6200/tcp                Critical
(CVSS: 9.8)
8009/tcp                Critical
(CVSS: 9.8)
3632/tcp                Critical
(CVSS: 9.3)
5432/tcp                Critical
(CVSS: 9.0)
5900/tcp                Critical
(CVSS: 9.0)
1099/tcp                High (CVSS:
7.5)
2121/tcp                High (CVSS:
7.5)
514/tcp                 High (CVSS:
7.5)
25/tcp                  Medium
(CVSS: 6.8)
111/tcp                 Medium
(CVSS: 6.4)
445/tcp                 Medium
(CVSS: 6.0)
22/tcp                  Medium
(CVSS: 5.3)
23/tcp                  Medium
(CVSS: 4.8)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host
193.42.15.22
------------------------------------
-

Issue
-----
NVT:    rlogin Passwordless Login
OID:    1.3.6.1.4.1.25623.1.0.113766
Threat: Critical (CVSS: 10.0)
Port:   513/tcp

Summary:
The rlogin service allows root
access without a password.

Vulnerability Detection Result:
It was possible to gain root access
without a password.

Impact:
This vulnerability allows an
attacker to gain
  complete control over the target
system.

Solution:
Solution type: Mitigation
Disable the rlogin service and use
alternatives like SSH instead.

Vulnerability Detection Method:
Checks if a vulnerable version is
present on the target host.
Details:
rlogin Passwordless Login
(OID: 1.3.6.1.4.1.25623.1.0.113766)
Version used: 2020-09-30T09:30:12Z

Issue
-----
NVT:    Operating System (OS) End of
Life (EOL) Detection
OID:    1.3.6.1.4.1.25623.1.0.103674
Threat: Critical (CVSS: 10.0)
Port:   general/tcp

Product detection result:
cpe:/o:canonical:ubuntu_linux:8.04
Detected by: OS Detection
Consolidation and Reporting (OID:
1.3.6.1.4.1.25623.1.0.105937)

Summary:
The Operating System (OS) on the
remote host has reached the end
  of life (EOL) and should not be
used anymore.

Vulnerability Detection Result:
The "Ubuntu" Operating System on the
remote host has reached the end of
life.
CPE:
cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:       8.04
EOL date:          2013-05-09
EOL info:
https://documentation.ubuntu.com/pro
ject/release-team/list-of!
-releases/

Impact:
An EOL version of an OS is not
receiving any security updates
  from the vendor. Unfixed security
vulnerabilities might be leveraged
by an att!
acker to compromise
  the security of this host.

Solution:
Solution type: Mitigation
Update the OS on the remote host to
a version which is still
  supported and receiving security
updates by the vendor.
  Note / Important: Please create an
override for this result if the
target host!
 is a:
  - Windows system with Extended
Security Updates (ESU)
  - System with additional 3rd-party
/ non-vendor security updates like
e.g. fro!
m 'TuxCare',
  'Freexian Extended LTS' or similar

Vulnerability Detection Method:
Checks if an EOL version of an OS is
present on the target
  host.
Details:
Operating System (OS) End of Life
(EOL) Detection
(OID: 1.3.6.1.4.1.25623.1.0.103674)
Version used: 2025-05-21T05:40:19Z

Product Detection Result:
Product:cpe:/o:canonical:ubuntu_linu
x:8.04

Method:OS Detection Consolidation
and Reporting
(OID: 1.3.6.1.4.1.25623.1.0.105937)


Issue
-----
NVT:    TWiki < 4.2.4 Multiple XSS /
Command Execution Vulnerabilities
OID:    1.3.6.1.4.1.25623.1.0.800320
Threat: Critical (CVSS: 10.0)
Port:   80/tcp
```

```
Summary:
TWiki is prone to multiple cross-
site scripting (XSS) and
  command execution vulnerabilities.

Vulnerability Detection Result:
Installed version: 01.Feb.2003
Fixed version:     4.2.4

Impact:
Successful exploitation could allow
execution of arbitrary script code
or
  commands. This could let attackers
steal cookie-based authentication
credentia!
ls or compromise the affected
  application.

Solution:
Solution type: VendorFix
Update to version 4.2.4 or later.

Affected Software/OS:
TWiki versions prior to 4.2.4.

Vulnerability Insight:
The flaws are due to:
  - %URLPARAM{}% variable is not
properly sanitized which lets
attackers
    conduct cross-site scripting
attack.
  - %SEARCH{}% variable is not
properly sanitised before being used
in an
    eval() call which lets the
attackers execute perl code through
eval
    injection attack.

Vulnerability Detection Method:
Details:
TWiki < 4.2.4 Multiple XSS / Command
Execution Vulnerabilities
(OID: 1.3.6.1.4.1.25623.1.0.800320)
Version used: 2025-12-11T05:46:19Z

References:
 cve: CVE-2008-5304
 cve: CVE-2008-5305
 url: http://twiki.org/cgi-
bin/view/Codev.SecurityAlert-CVE-
2008-5304
 url:
http://www.securityfocus.com/bid/326
68
 url:
http://www.securityfocus.com/bid/326
69
 url: http://twiki.org/cgi-
bin/view/Codev/SecurityAlert-CVE-
2008-5305



Issue
-----
NVT:    The rexec service is running
OID:    1.3.6.1.4.1.25623.1.0.100111
Threat: Critical (CVSS: 10.0)
Port:   512/tcp

Summary:
This remote host is running a rexec
service.

Vulnerability Detection Result:
The rexec service was detected on
the target system.

Solution:
Solution type: Mitigation
Disable the rexec service and use
alternatives like SSH
  instead.

Vulnerability Insight:
rexec (remote execution client for
an exec server) has the same
  kind of functionality that rsh
has: you can execute shell commands
on a remote!
 computer.
  The main difference is that rexec
authenticate by reading the username
and pas!
sword *unencrypted*
  from the socket.

Vulnerability Detection Method:
Checks whether an rexec service is
exposed on the target
  host.
Details:
The rexec service is running
(OID: 1.3.6.1.4.1.25623.1.0.100111)
Version used: 2023-09-12T05:05:19Z

References:
 cve: CVE-1999-0618



Issue
-----
NVT:    Possible Backdoor:
Ingreslock
OID:    1.3.6.1.4.1.25623.1.0.103549
Threat: Critical (CVSS: 10.0)
Port:   1524/tcp

Summary:
A backdoor is installed on the
remote host.

Vulnerability Detection Result:
The service is answering to an 'id;'
command with the following response:
uid=0(!
root) gid=0(root)

Impact:
Attackers can exploit this issue to
execute arbitrary commands in the
  context of the application.
Successful attacks will compromise
the affected is!
ystem.

Solution:
Solution type: Workaround
A whole cleanup of the infected
system is recommended.

Vulnerability Detection Method:
Details:
Possible Backdoor: Ingreslock
(OID: 1.3.6.1.4.1.25623.1.0.103549)
Version used: 2023-07-25T05:05:58Z



Issue
-----
NVT:    Distributed Ruby (dRuby/DRb)
Multiple RCE Vulnerabilities
OID:    1.3.6.1.4.1.25623.1.0.108010
Threat: Critical (CVSS: 10.0)
Port:   8787/tcp

Summary:
Systems using Distributed Ruby
(dRuby/DRb), which is available in
Ruby versions !
1.6
  and later, may permit unauthorized
systems to execute distributed
commands.

Vulnerability Detection Result:
The service is running in $SAFE >= 1
mode. However it is still possible
to run a!
rbitrary syscall commands on the
remote host. Sending an invalid
syscall the ser!
vice returned the following
response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby
/1.8/drb/drb.rb:1555:in
`syscall'"0/usr/lib/!
ruby/1.8/drb/drb.rb:1555:in
`send'"4/usr/lib/ruby/1.8/drb/drb.rb
:1555:in `__send!
__'"A/usr/lib/ruby/1.8/drb/drb.rb:15
55:in
`perform_without_block'"3/usr/lib/ru
by!
/1.8/drb/drb.rb:1515:in
`perform'"5/usr/lib/ruby/1.8/drb/drb
.rb:1589:in `main_lo!
op'"0/usr/lib/ruby/1.8/drb/drb.rb:15
85:in
`loop'"5/usr/lib/ruby/1.8/drb/drb.rb
:1!
585:in
`main_loop'"1/usr/lib/ruby/1.8/drb/d
rb.rb:1581:in
`start'"5/usr/lib/ruby/!
1.8/drb/drb.rb:1581:in
`main_loop'"//usr/lib/ruby/1.8/drb/d
rb.rb:1430:in `run'"1!
/usr/lib/ruby/1.8/drb/drb.rb:1427:in
`start'"//usr/lib/ruby/1.8/drb/drb.r
b:1427:!
in
`run'"6/usr/lib/ruby/1.8/drb/drb.rb:
1347:in
`initialize'"//usr/lib/ruby/1.8/d!
rb/drb.rb:1627:in
`new'"9/usr/lib/ruby/1.8/drb/drb.rb:
1627:in `start_service'"%/!
usr/sbin/druby_timeserver.rb:12:errn
oi+:mesg"Function not implemented

Impact:
By default, Distributed Ruby does
not impose restrictions on allowed
hosts or se!
t the
  $SAFE environment variable to
prevent privileged activities. If
other controls!
 are not in place, especially if the
  Distributed Ruby process runs with
elevated privileges, an attacker
could exec!
ute arbitrary system commands or
Ruby
  scripts on the Distributed Ruby
server. An attacker may need to know
only the !
URI of the listening Distributed
Ruby
  server to submit Ruby commands.

Solution:
Solution type: Mitigation
Administrators of environments that
rely on Distributed Ruby should
ensure that
  appropriate controls are in place.
Code-level controls may include:
  - Implementing taint on untrusted
input
  - Setting $SAFE levels
appropriately (>=2 is recommended if
untrusted hosts ar!
e allowed to submit Ruby commands,
and >=3 may be appropriate)
  - Including drb/acl.rb to set
ACLEntry to restrict access to
trusted hosts

Vulnerability Detection Method:
Send a crafted command to the
service and check for a remote
command execution
  via the instance_eval or syscall
requests.
Details:
Distributed Ruby (dRuby/DRb)
Multiple RCE Vulnerabilities
(OID: 1.3.6.1.4.1.25623.1.0.108010)
Version used: 2024-06-28T05:05:33Z

References:
```

```
 url:
https://tools.cisco.com/security/cen
ter/viewAlert.x?alertId=22750
 url:
http://www.securityfocus.com/bid/470
71
 url: http://blog.recurity-
labs.com/archives/2011/05/12/druby_f
or_penetration_testers/
 url: http://www.ruby-
doc.org/stdlib-
1.9.3/libdoc/drb/rdoc/DRb.html


Issue
-----
NVT:    Apache Tomcat AJP RCE
Vulnerability (Ghostcat) - Active
Check
OID:    1.3.6.1.4.1.25623.1.0.143545
Threat: Critical (CVSS: 9.8)
Port:   8009/tcp

Summary:
Apache Tomcat is prone to a remote
code execution (RCE)
  vulnerability in the AJP connector
dubbed 'Ghostcat'.

Vulnerability Detection Result:
It was possible to read the file
"/WEB-INF/web.xml" through the AJP
connector.
Result:
AB 8\x0004 Ã\x0088 \x0002OK  \x0001
\x000CContent-Type
\x001Ctext/html;charset=!
ISO-8859-1
AB\x001FÃ¾\x0003\x001FÃ¸<!--
  Licensed to the Apache Software
Foundation (ASF) under one or more
  contributor license agreements.
See the NOTICE file distributed with
  this work for additional
information regarding copyright
ownership.
  The ASF licenses this file to You
under the Apache License, Version
2.0
  (the "License"); you may not use
this file except in compliance with
  the License.  You may obtain a
copy of the License at

http://www.apache.org/licenses/LICEN
SE-2.0
  Unless required by applicable law
or agreed to in writing, software
  distributed under the License is
distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS
OF ANY KIND, either express or
implied.
  See the License for the specific
language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-
8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Strict//EN"

"http://www.w3.org/TR/xhtml1/DTD/xht
ml1-strict.dtd">
<html
xmlns="http://www.w3.org/1999/xhtml"
xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
           font-family: Arial,
"Times New Roman", Times, serif;
          margin: 10px 0px;
      }
    img {
        border: none;
    }

    a:link, a:visited {
        color: blue
    }
    th {
        font-family: Verdana, "Times
New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }
    td {
        color: #000000;
         font-family: Arial,
Helvetica, sans-serif;
    }

    td.menu {
        background: #FFDC75;
    }
    .center {
        text-align: center;
    }
    .code {
        color: #000000;
        font-family: "Courier New",
Courier, monospace;
        font-size: 110%;
        margin-left: 2.5em;
    }

     #banner {
        margin-bottom: 12px;
     }
     p#congrats {
         margin-top: 0;
         font-weight: bold;
         text-align: center;
     }
     p#footer {
         text-align: right;
         font-size: 80%;
     }
     /*]]>*/
   </style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
      <td align="left"
style="width:130px">
        <a
href="http://tomcat.apache.org/">
          <img src="tomcat.gif"
height="92" width="130" alt="The
Mighty Tomcat - MEOW!"!
/>
         </a>
      </td>
      <td align="left"
valign="top"><b>Apache
Tomcat/5.5</b></td>
      <td align="right">
        <a
href="http://www.apache.org/">
          <img src="asf-logo-
wide.gif" height="51" width="537"
alt="The Apache Software!
 Foundation"/>
         </a>
       </td>
     </tr>
</table>
<table>
    <tr>
        <!-- Table of Contents -->
        <td valign="top">
            <table width="100%"
border="1" cellspacing="0"
cellpadding="3">
                <tr>

<th>Administration</th>
                </tr>
                <tr>
                    <td
class="menu">
                      <a
href="manager/status">Status</a><br/
>
                    <a
href="admin">Tomcat Administrat
ion</a><br/>
                    <a
href="manager/html">Tomcat Manag
er</a><br/>
                     
                  </td>
                </tr>
            </table>
             <br />
            <table width="100%"
border="1" cellspacing="0"
cellpadding="3">
                <tr>

<th>Documentation</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a
href="RELEASE-
NOTES.txt">Release Notes</a><br
/>
                    <a href="tomcat-
docs/changelog.html">Change Log
</a><br/!
>
                    <a href="tomcat-
docs">Tomcat Documentation</a><
br/>    !
                     
                     
                      </td>
                </tr>
            </table>

            <br/>
            <table width="100%"
border="1" cellspacing="0"
cellpadding="3">
                <tr>
                  <th>Tomcat
Online</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a
href="http://tomcat.apache.org/">Hom
e Page</a><br/>
                      <a
href="http://tomcat.apache.org/faq/"
>FAQ</a><br/>
                    <a
href="http://tomcat.apache.org/bugre
port.html">Bug D!
atabase</a><br/>
                    <a
href="http://issues.apache.org/bugzi
lla/buglist.cgi?bug_s!
tatus=UNCONFIRMED&amp;bug_status=NEW
&amp;bug_status=ASSIGNED&amp;bug_sta
tus=REOP!
ENED&amp;bug_status=RESOLVED&amp;res
olution=LATER&amp;resolution=REMIND&
amp;reso!
lution=---
&amp;bugidtype=include&amp;product=T
omcat+5&amp;cmdtype=doit&amp;order!
=Importance">Open Bugs</a><br/>
                    <a
href="http://mail-
archives.apache.org/mod_mbox/tomcat-
use!
rs/">Users Mailing List</a
><br/>
                    <a
href="http://mail-
archives.apache.org/mod_mbox/tomcat-
dev!
/">Developers Mailing List
</a><br/>
```

```
                  <a
href="irc://irc.freenode.net/#tomcat
">IRC</a><br/>
                     
                </td>
              </tr>
            </table>

            <br/>
            <table width="100%"
border="1" cellspacing="0"
cellpadding="3">
              <tr>
                <th>Examples</th>
              </tr>
              <tr>
                <td class="menu">
                  <a href="jsp-
examples/">JSP Examples</a><br/
>
                  <a
href="servlets-
examples/">Servlet Examples</a>
<br/>
                  <a
href="webdav/">WebDAV capabilit
ies</a><br/>
                     
                </td>
              </tr>
            </table>

            <br/>
            <table width="100%"
border="1" cellspacing="0"
cellpadding="3">
              <tr>

<th>Miscellaneous</th>
              </tr>
              <tr>
                <td class="menu">
                  <a
href="http://java.sun.com/products/j
sp">Sun's Java&n!
bsp;Server Pages Site</a><
br/>
                  <a
href="http://java.sun.com/products/s
ervlet">Sun's Se!
rvlet Site</a><br/>
                     
                </td>
              </tr>
            </table>
        </td>
        <td
style="width:20px"> </td>

        <!-- Body -->
        <td align="left"
valign="top">
          <p id="congrats">If you're
seeing this page via a web browser,
it mean!
s you've setup Tomcat successfully.
Congratulations!</p>

          <p>As you may have guessed
by now, this is the default Tomcat
home pag!
e. It can be found on the local
filesystem at:</p>
          <p
class="code">$CATALINA_HOME/webapps/
ROOT/index.jsp</p>

          <p>where "$CATALINA_HOME"
is the root of the Tomcat
installation direc!
tory. If you're seeing this page,
and you don't think you should be,
then either!
 you're either a user who has
arrived at new installation of
Tomcat, or you're a!
n administrator who hasn't got
his/her setup quite right. Providing
the latter i!
s the case, please refer to the <a
href="tomcat-docs">Tomcat
Documentation</a> f!
or more detailed setup and
administration information than is
found in the INSTA!
LL file.</p>
            <p><b>NOTE:</b> This
page is precompiled. If you change
it, this pag!
e will not change since
                it was compiled
into a servlet at build time.
                (See
<tt>$CATALINA_HOME/webapps/ROOT/WEB-
INF/web.xml</tt> as t!
o how it was mapped.)
            </p>
            <p><b>NOTE: For security
reasons, using the administration
webapp
            is restricted to users
with role "admin". The manager
webapp
            is restricted to users
with role "manager".</b>
            Users are defined in
<code>$CATALINA_HOME/conf/tomcat-
users.xml</cod!
e>.</p>
            <p>Included with this
release are a host of sample
Servlets and JSPs!
 (with associated source code),
extensive documentation (including
the Servlet 2!
.4 and JSP 2.0 API JavaDoc), and an
introductory guide to developing web
applica!
tions.</p>
            <p>Tomcat mailing lists
are available at the Tomcat project
web site!
:</p>
            <ul>
                <li><b><a
href="mailto:users@tomcat.apache.org
">users@tomc

Solution:
Solution type: VendorFix
- Update Apache Tomcat to version
7.0.100, 8.5.51, 9.0.31 or
  later
  - For other products using Tomcat
please contact the vendor for more
informati!
on on fixed
  versions

Affected Software/OS:
Apache Tomcat versions prior
7.0.100, 8.5.51 or 9.0.31 when the
  AJP connector is enabled.
  Other products like JBoss or
Wildfly which are using Tomcat might
be affected !
as well.

Vulnerability Insight:
Apache Tomcat server has a file
containing vulnerability, which
  can be used by an attacker to read
or include any files in all webapp
director!
ies on Tomcat, such
  as webapp configuration files or
source code.

Vulnerability Detection Method:
Sends a crafted AJP request and
checks the response.
Details:
Apache Tomcat AJP RCE Vulnerability
(Ghostcat) - Active Check
(OID: 1.3.6.1.4.1.25623.1.0.143545)
Version used: 2026-03-18T05:59:10Z

References:
 cve: CVE-2020-1938
 url:
https://lists.apache.org/thread/bnys
5lvg1875dsslkkx2vmwxv833l35x
 url:
https://tomcat.apache.org/security-
9.html#Fixed_in_Apache_Tomcat_9.0.31
 url:
https://tomcat.apache.org/security-
8.html#Fixed_in_Apache_Tomcat_8.5.51
 url:
https://tomcat.apache.org/security-
7.html#Fixed_in_Apache_Tomcat_7.0.10
0
 url:
https://web.archive.org/web/20250114
042903/https://www.chaitin.cn/en/gho
stcat
 url:
https://www.cnvd.org.cn/flaw/show/CN
VD-2020-10487
 url:
https://github.com/YDHCUI/CNVD-2020-
10487-Tomcat-Ajp-lfi
 url:
https://securityboulevard.com/2020/0
2/patch-your-tomcat-and-jboss-
instances-to-protect-from-ghostcat-
vulnerability-cve-2020-1938-and/
 url: https://www.cisa.gov/known-
exploited-vulnerabilities-catalog
 cisa: Known Exploited Vulnerability
(KEV) catalog
 cert-bund: WID-SEC-2024-0528
 cert-bund: WID-SEC-2023-2480
 cert-bund: CB-K20/0711
 cert-bund: CB-K20/0705
 cert-bund: CB-K20/0693
 cert-bund: CB-K20/0555
 cert-bund: CB-K20/0543
 cert-bund: CB-K20/0154
 dfn-cert: DFN-CERT-2021-1736
 dfn-cert: DFN-CERT-2020-1508
 dfn-cert: DFN-CERT-2020-1413
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2020-1134
 dfn-cert: DFN-CERT-2020-0850
 dfn-cert: DFN-CERT-2020-0835
 dfn-cert: DFN-CERT-2020-0821
 dfn-cert: DFN-CERT-2020-0569
 dfn-cert: DFN-CERT-2020-0557
 dfn-cert: DFN-CERT-2020-0501
 dfn-cert: DFN-CERT-2020-0381


Issue
-----
NVT:    MySQL / MariaDB Default
Credentials (MySQL Protocol)
OID:    1.3.6.1.4.1.25623.1.0.103551
Threat: Critical (CVSS: 9.8)
Port:   3306/tcp

Product detection result:
cpe:/a:mysql:mysql:5.0.51a
Detected by: MariaDB / Oracle MySQL
Detection (MySQL Protocol) (OID:
1.3.6.1.4.1.25623.1.0.100152)

Summary:
It was possible to login into the
remote MySQL using default
  credentials.

Vulnerability Detection Result:
It was possible to login as user
"root" with an empty password.

Solution:
Solution type: Mitigation
- Change the password as soon as
possible
  - Contact the vendor for other
possible fixes / updates

Affected Software/OS:
The following products are know to
use such weak credentials:
```

```
  - CVE-2001-0645: Symantec/AXENT
NetProwler 3.5.x
  - CVE-2002-1809: Windows binary
release of MySQL 3.23.2 through
3.23.52
  - CVE-2004-1532: AppServ 2.5.x and
earlier
  - CVE-2004-2357: Proofpoint
Protection Server
  - CVE-2006-1451: MySQL Manager in
Apple Mac OS X 10.3.9 and 10.4.6
  - CVE-2007-2554: Associated Press
(AP) Newspower 4.0.1 and earlier
  - CVE-2007-6081: AdventNet
EventLog Analyzer build 4030
  - CVE-2009-0919: XAMPP
  - CVE-2014-3419: Infoblox NetMRI
before 6.8.5
  - CVE-2015-4669: Xsuite 2.x
  - CVE-2016-6531, CVE-2018-15719:
Open Dental before version 18.4
  - CVE-2024-22901: Vinchin Backup &
Recovery 7.2 and prior
  - No CVE / GHSA-g38h-mr9p-fjmf:
Vvveb CMS 1.0.8 and prior
  Other products might be affected
as well.

Vulnerability Detection Method:
Details:
MySQL / MariaDB Default Credentials
(MySQL Protocol)
(OID: 1.3.6.1.4.1.25623.1.0.103551)
Version used: 2026-05-27T08:10:51Z

Product Detection Result:
Product:cpe:/a:mysql:mysql:5.0.51a

Method:MariaDB / Oracle MySQL
Detection (MySQL Protocol)
(OID: 1.3.6.1.4.1.25623.1.0.100152)

References:
 cve: CVE-2001-0645
 cve: CVE-2002-1809
 cve: CVE-2004-1532
 cve: CVE-2004-2357
 cve: CVE-2006-1451
 cve: CVE-2007-2554
 cve: CVE-2007-6081
 cve: CVE-2009-0919
 cve: CVE-2014-3419
 cve: CVE-2015-4669
 cve: CVE-2016-6531
 cve: CVE-2018-15719
 cve: CVE-2024-22901


Issue
-----
NVT:    vsftpd Compromised Source
Packages Backdoor Vulnerability -
Active Check
OID:    1.3.6.1.4.1.25623.1.0.103185
Threat: Critical (CVSS: 9.8)
Port:   6200/tcp

Summary:
vsftpd is prone to a backdoor
vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Impact:
Attackers can exploit this issue to
execute arbitrary commands
  in the context of the application.
Successful attacks will compromise
the affe!
cted
  application.

Solution:
Solution type: VendorFix
The repaired package can be
downloaded from the referenced
  vendor homepage. Please validate
the package with its signature.

Affected Software/OS:
vsftpd 2.3.4 source packages
downloaded between 20110630
  and 20110703 are affected.

Vulnerability Insight:
The tainted source package contains
a backdoor which opens a
  shell on port 6200/tcp.

Vulnerability Detection Method:
Details:
vsftpd Compromised Source Packages
Backdoor Vulnerability - Active
Check
(OID: 1.3.6.1.4.1.25623.1.0.103185)
Version used: 2026-02-18T05:57:21Z

References:
 cve: CVE-2011-2523
 url:
https://scarybeastsecurity.blogspot.
com/2011/07/alert-vsftpd-download-
backdoored.html
 url:
https://web.archive.org/web/20210127
090551/https://www.securityfocus.com
/bid/48539/


Issue
-----
NVT:    vsftpd Compromised Source
Packages Backdoor Vulnerability -
Active Check
OID:    1.3.6.1.4.1.25623.1.0.103185
Threat: Critical (CVSS: 9.8)
Port:   21/tcp

Summary:
vsftpd is prone to a backdoor
vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Impact:
Attackers can exploit this issue to
execute arbitrary commands
  in the context of the application.
Successful attacks will compromise
the affe!
cted
  application.

Solution:
Solution type: VendorFix
The repaired package can be
downloaded from the referenced
  vendor homepage. Please validate
the package with its signature.

Affected Software/OS:
vsftpd 2.3.4 source packages
downloaded between 20110630
  and 20110703 are affected.

Vulnerability Insight:
The tainted source package contains
a backdoor which opens a
  shell on port 6200/tcp.

Vulnerability Detection Method:
Details:
vsftpd Compromised Source Packages
Backdoor Vulnerability - Active
Check
(OID: 1.3.6.1.4.1.25623.1.0.103185)
Version used: 2026-02-18T05:57:21Z

References:
 cve: CVE-2011-2523
 url:
https://scarybeastsecurity.blogspot.
com/2011/07/alert-vsftpd-download-
backdoored.html
 url:
https://web.archive.org/web/20210127
090551/https://www.securityfocus.com
/bid/48539/


Issue
-----
NVT:    DistCC RCE Vulnerability
(CVE-2004-2687)
OID:    1.3.6.1.4.1.25623.1.0.103553
Threat: Critical (CVSS: 9.3)
Port:   3632/tcp

Summary:
DistCC is prone to a remote code
execution (RCE)
  vulnerability.

Vulnerability Detection Result:
It was possible to execute the "id"
command.
Result: uid=1(daemon) gid=1(daemon)

Impact:
DistCC by default trusts its clients
completely that in turn
  could allow a malicious client to
execute arbitrary commands on the
server.

Solution:
Solution type: VendorFix
Vendor updates are available. Please
see the references for
  more information.
  For more information about
DistCC's security see the
references.

Vulnerability Insight:
DistCC 2.x, as used in XCode 1.5 and
others, when not configured
  to restrict access to the server
port, allows remote attackers to
execute arbi!
trary commands via
  compilation jobs, which are
executed by the server without
authorization check!
s.

Vulnerability Detection Method:
Details:
DistCC RCE Vulnerability (CVE-2004-
2687)
(OID: 1.3.6.1.4.1.25623.1.0.103553)
Version used: 2022-07-07T10:16:06Z

References:
 cve: CVE-2004-2687
 url:
https://distcc.github.io/security.ht
ml
 url:
https://web.archive.org/web/20150511
045306/http://archives.neohapsis.com
:80/archives/bugtraq/2005-
03/0183.html
 dfn-cert: DFN-CERT-2019-0381


Issue
-----
NVT:    PostgreSQL Default
Credentials (PostgreSQL Protocol)
OID:    1.3.6.1.4.1.25623.1.0.103552
Threat: Critical (CVSS: 9.0)
Port:   5432/tcp

Product detection result:
cpe:/a:postgresql:postgresql:8.3.1
Detected by: PostgreSQL Detection
Consolidation (OID:
1.3.6.1.4.1.25623.1.0.128025)

Summary:
```

It was possible to login into the
remote PostgreSQL as user
  postgres using weak credentials.

Vulnerability Detection Result:
It was possible to login as user
postgres with password "postgres".

Solution:
Solution type: Mitigation
Change the password as soon as
possible.

Vulnerability Detection Method:
Details:
PostgreSQL Default Credentials
(PostgreSQL Protocol)
(OID: 1.3.6.1.4.1.25623.1.0.103552)
Version used: 2024-07-19T15:39:06Z

Product Detection Result:
Product:cpe:/a:postgresql:postgresql
:8.3.1

Method:PostgreSQL Detection
Consolidation
(OID: 1.3.6.1.4.1.25623.1.0.128025)

Issue

NVT: VNC Brute Force Login
OID: 1.3.6.1.4.1.25623.1.0.106056
Threat: Critical (CVSS: 9.0)
Port: 5900/tcp

Summary:
Try to log in with given passwords
via VNC protocol.

Vulnerability Detection Result:
It was possible to connect to the
VNC server with the password:
password

Solution:
Solution type: Mitigation
Change the password to something
hard to guess or enable
  password protection at all.

Vulnerability Insight:
This script tries to authenticate to
a VNC server with the
  passwords set in the password
preference. It will also test and
report if no a!
uthentication /
  password is required at all.
  Note: Some VNC servers have a
blacklisting scheme that blocks IP
addresses aft!
er five unsuccessful
  connection attempts for a period
of time. The script will abort the
brute forc!
e attack if it
  encounters that it gets blocked.
  Note as well that passwords can be
max. 8 characters long.

Vulnerability Detection Method:
Details:
VNC Brute Force Login
(OID: 1.3.6.1.4.1.25623.1.0.106056)
Version used: 2021-07-23T07:56:26Z

Issue

NVT: Java RMI Server Insecure
Default Configuration RCE
Vulnerability - Active Check
OID: 1.3.6.1.4.1.25623.1.0.140051
Threat: High (CVSS: 7.5)
Port: 1099/tcp

Summary:
Multiple Java products that
implement the RMI Server contain a
  vulnerability that could allow an
unauthenticated, remote attacker to
execute !
arbitrary code
  (remote code execution/RCE) on a
targeted system with elevated
privileges.

Vulnerability Detection Result:
By doing an RMI request it was
possible to trigger the
vulnerability and make th!
e remote host send a request back to
the scanner host (Details on the
received p!
acket follows).
Destination IP: 193.42.15.25
(receiving IP on scanner host side)
Destination port: 13921/tcp
(receiving port on scanner host
side)
Originating IP: 193.42.15.22
(originating IP from target host
side)

Impact:
An unauthenticated, remote attacker
could exploit the
  vulnerability by transmitting
crafted packets to the affected
software. When t!
he packets are
  processed, the attacker could
execute arbitrary code on the system
with elevat!
ed privileges.

Solution:
Solution type: Workaround
Disable class-loading. Please
contact the vendor of the
  affected system for additional
guidance.

Vulnerability Insight:
The vulnerability exists because of
an incorrect default
  configuration of the Remote Method
Invocation (RMI) Server in the
affected sof!
tware.

Vulnerability Detection Method:
Sends a crafted JRMI request and
checks if the target is
  connecting back to the scanner
host.
  Note: For a successful detection
of this flaw the target host needs
to be able!
 to reach the
  scanner host on a TCP port
randomly generated during the
runtime of the VT (cu!
rrently in the
  range of 10000-32000).
Details:
Java RMI Server Insecure Default
Configuration RCE Vulnerability -
Active Ch...
(OID: 1.3.6.1.4.1.25623.1.0.140051)
Version used: 2026-04-17T15:51:27Z

References:
 cve: CVE-2011-3556
 url:
https://web.archive.org/web/20211208
040855/http://www.securitytracker.co
m/id?1026215
 url:
https://web.archive.org/web/20110824
060234/http://download.oracle.com/ja
vase/1.3/docs/guide/rmi/spec/rmi-
protocol.html
 url:
https://tools.cisco.com/security/cen
ter/viewAlert.x?alertId=23665
 dfn-cert: DFN-CERT-2012-1829
 dfn-cert: DFN-CERT-2012-1380
 dfn-cert: DFN-CERT-2012-1377
 dfn-cert: DFN-CERT-2012-1156
 dfn-cert: DFN-CERT-2012-1155
 dfn-cert: DFN-CERT-2012-0956
 dfn-cert: DFN-CERT-2012-0828
 dfn-cert: DFN-CERT-2012-0815
 dfn-cert: DFN-CERT-2012-0638
 dfn-cert: DFN-CERT-2012-0451
 dfn-cert: DFN-CERT-2012-0418
 dfn-cert: DFN-CERT-2012-0354
 dfn-cert: DFN-CERT-2012-0146
 dfn-cert: DFN-CERT-2012-0142
 dfn-cert: DFN-CERT-2012-0126
 dfn-cert: DFN-CERT-2012-0095
 dfn-cert: DFN-CERT-2012-0047
 dfn-cert: DFN-CERT-2011-1844
 dfn-cert: DFN-CERT-2011-1826
 dfn-cert: DFN-CERT-2011-1804
 dfn-cert: DFN-CERT-2011-1743
 dfn-cert: DFN-CERT-2011-1738
 dfn-cert: DFN-CERT-2011-1706
 dfn-cert: DFN-CERT-2011-1628
 dfn-cert: DFN-CERT-2011-1627
 dfn-cert: DFN-CERT-2011-1619

Issue

NVT: PHP < 5.3.13, 5.4.x < 5.4.3
Multiple Vulnerabilities - Active
Check
OID: 1.3.6.1.4.1.25623.1.0.103482
Threat: High (CVSS: 7.5)
Port: 80/tcp

Summary:
PHP is prone to multiple
vulnerabilities.

Vulnerability Detection Result:
By doing the following HTTP POST
request:
"HTTP POST" body : <?php
phpinfo();?>
URL   :
http://193.42.15.22/cgi-
bin/php?%2D%64+%61%6C%6C%6F%77%5F%75
%!
72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%
6E+%2D%64+%73%61%66%65%5F%6D%6F%64%6
5%3D%6F%!
66%66+%2D%64+%73%75%68%6F%73%69%6E%2
E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6
F%6E+%2D!
%64+%64%69%73%61%62%6C%65%5F%66%75%6
E%63%74%69%6F%6E%73%3D%22%22+%2D%64+
%6F%70%6!
5%6E%5F%62%61%73%65%64%69%72%3D%6E%6
F%6E%65+%2D%64+%61%75%74%6F%5F%70%72
%65%70%6!
5%6E%64%5F%66%69%6C%65%3D%70%68%70%3
A%2F%2F%69%6E%70%75%74+%2D%64+%63%67
%69%2E%6!
6%6F%72%63%65%5F%72%65%64%69%72%65%6
3%74%3D%30+%2D%64+%63%67%69%2E%72%65
%64%69%7!
2%65%63%74%5F%73%74%61%74%75%73%5F%6
5%6E%76%3D%30+%2D%6E
it was possible to execute the
"<?php phpinfo();?>" command.
Result:
  <title>phpinfo()</title><meta
name="ROBOTS"
content="NOINDEX,NOFOLLOW,NOARCHIV!
E" /></head>
  <tr><td class="e">Configuration
File (php.ini) Path </td><td
class="v">/etc/ph!
p5/cgi </td></tr>
  <h2>PHP Core</h2>
  <h2>PHP Variables</h2>

Impact:
Exploiting this issue allows remote
attackers to view the source

code of files in the context of the server process. This may allow the attacke!
r to obtain
sensitive information and to run arbitrary PHP code on the affected computer. !
Other attacks are
also possible.

Solution:
Solution type: VendorFix
PHP: Update to version 5.3.13, 5.4.3 or later
- Other products / applications: Please contact the vendor for a solution

Affected Software/OS:
PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.
Other products / applications might be affected by the tested CVE-2012-1823 as!
well.

Vulnerability Insight:
When PHP is used in a CGI-based setup (such as Apache's
mod_cgid), the php-cgi receives a processed query string parameter as command !
line arguments which
allows command-line switches, such as -s, -d or -c to be passed to the php-cgi!
binary, which can
be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of !
index.php is below:
http://example.com/index.php?-s

Vulnerability Detection Method:
Send multiple a crafted HTTP POST requests and checks the
responses.
Notes:
- This script checks for the presence of CVE-2012-1823 which indicates that th!
e system is also
affected by the other included CVEs.
- It is currently expected that a result of this VT is reported if the system !
is generally
exposing a phpinfo() output on the relevant URL / endpoint (independent from t!
he running product).
Exposing such sensitive information is generally seen as a security misconfigu!
ration and should be
avoided.
Details:
PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check (OID: 1.3.6.1.4.1.25623.1.0.103482)
Version used: 2026-04-23T06:21:05Z

References:
cve: CVE-2012-1823
cve: CVE-2012-2311
cve: CVE-2012-2336
cve: CVE-2012-2335
url: https://web.archive.org/web/20190212080415/http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
url: https://www.kb.cert.org/vuls/id/520827
url: https://bugs.php.net/bug.php?id=61910
url: https://www.php.net/manual/en/security.cgi-bin.php
url: https://web.archive.org/web/20210121223743/http://www.securityfocus.com/bid/53388
url: https://web.archive.org/web/20120709064615/http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-2-1567532.html
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
cisa: Known Exploited Vulnerability (KEV) catalog
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1316
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-1101
dfn-cert: DFN-CERT-2012-0994
dfn-cert: DFN-CERT-2012-0993
dfn-cert: DFN-CERT-2012-0992
dfn-cert: DFN-CERT-2012-0920
dfn-cert: DFN-CERT-2012-0915
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878

Issue

NVT: EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check
OID: 1.3.6.1.4.1.25623.1.0.803189
Threat: High (CVSS: 7.5)
Port: 80/tcp

Summary:
EasyPHP Webserver is prone to multiple vulnerabilities.

Vulnerability Detection Result:
Vulnerable URL:
http://193.42.15.22/phpinfo.php
Concluded from:
<title>phpinfo()</title><meta name="ROBOTS"
content="NOINDEX,NOFOLLOW,NOARCHIV!
E" /></head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph!
p5/cgi </td></tr>
<h2>PHP Core</h2>
<h2>PHP Variables</h2>

Impact:
Successful exploitation will allow attackers to gain
administrative access, disclose the information, inject PHP code/shell and exe!
cute a remote PHP
Code.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year
since the disclosure of this vulnerability. Likely none will be provided anymo!
re. General solution
options are to upgrade to a newer release, disable respective features, remove!
the product or
replace the product by another one.

Affected Software/OS:
EasyPHP version 12.1 and prior.

Vulnerability Insight:
The bug in EasyPHP WebServer Manager, its skipping
authentication for certain requests. Which allows to bypass the authentication!
, disclose the
information or execute a remote PHP code.

Vulnerability Detection Method:
Sends a crafted HTTP GET request and checks the response.
Note: It is currently expected that a result of this VT is reported if the sys!
tem is generally
exposing a phpinfo() output on the relevant URL / endpoint (independent from t!
he running product).
Exposing such sensitive information is generally seen as a security misconfigu!
ration and should be
avoided.
Details:
EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check (OID: 1.3.6.1.4.1.25623.1.0.803189)
Version used: 2025-11-11T05:40:18Z

References:
url: https://cxsecurity.com/issue/WLB-2013040069

Issue

NVT: FTP Brute Force Logins With Default Credentials Reporting
OID: 1.3.6.1.4.1.25623.1.0.108718
Threat: High (CVSS: 7.5)
Port: 2121/tcp

Summary:
It was possible to login into the remote FTP server using
weak/known credentials.

Vulnerability Detection Result:
It was possible to login with the following credentials
<User>:<Password>
msfadmin:msfadmin
postgres:postgres
service:service
user:user

Impact:
This issue may be exploited by a remote attacker to e.g. gain
access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight:
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA!
P&R

```
  - CVE-2013-7404: GE Healthcare
Discovery NM 750b
  - CVE-2014-9198: Schneider
Electric ETG3000 FactoryCast HMI
gateways
  - CVE-2015-7261: QNAP iArtist Lite
distributed with QNAP Signage
Station
  - CVE-2016-8731: Foscam C1 devices
  - CVE-2017-8218: vsftpd on TP-Link
C2 and C20i devices
  - CVE-2018-9068: IMM2 for IBM and
Lenovo System x
  - CVE-2018-17771: Ingenico Telium
2 PoS terminals
  - CVE-2018-19063, CVE-2018-19064:
Foscam C2 and Opticam i5 devices
  - CVE-2018-25147: Microhard
Systems IPn4G
  - CVE-2020-36915: Adtec Digital
SignEdje Digital Signage Player
  Note: As the VT 'FTP Brute Force
Logins With Default Credentials'
(OID:
  1.3.6.1.4.1.25623.1.0.108717)
might run into a timeout the actual
reporting of!
 this vulnerability
  takes place in this VT instead.

Vulnerability Detection Method:
Reports weak/known credentials
detected by the VT
  'FTP Brute Force Logins With
Default Credentials' (OID:
1.3.6.1.4.1.25623.1.0.!
108717).
Details:
FTP Brute Force Logins With Default
Credentials Reporting
(OID: 1.3.6.1.4.1.25623.1.0.108718)
Version used: 2026-01-16T15:42:49Z

References:
 cve: CVE-1999-0501
 cve: CVE-1999-0502
 cve: CVE-1999-0507
 cve: CVE-1999-0508
 cve: CVE-2001-1594
 cve: CVE-2013-7404
 cve: CVE-2014-9198
 cve: CVE-2015-7261
 cve: CVE-2016-8731
 cve: CVE-2017-8218
 cve: CVE-2018-9068
 cve: CVE-2018-17771
 cve: CVE-2018-19063
 cve: CVE-2018-19064
 cve: CVE-2018-25147
 cve: CVE-2020-36915


Issue
-----
NVT:    Apache JServ Protocol (AJP)
Public WAN (Internet) / Public LAN
Accessible (TCP)
OID:    1.3.6.1.4.1.25623.1.0.108716
Threat: High (CVSS: 7.5)
Port:   8009/tcp

Summary:
The script checks if the target host
is running a service
  supporting the Apache JServ
Protocol (AJP) accessible from a
public WAN (Inter!
net) / public
  LAN.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Solution:
Solution type: Mitigation
Only allow access to the AJP service
from trusted sources /
  networks.

Vulnerability Insight:
When using the Apache JServ Protocol
(AJP), care must be taken
  when trusting incoming connections
to Apache Tomcat. Tomcat treats AJP
connect!
ions as having
  higher trust than, for example, a
similar HTTP connection. If such
connections!
 are available to an
  attacker, they can be exploited in
ways that may be surprising (e.g.
bypassing!
 security checks,
  bypassing user authentication
among others).

Vulnerability Detection Method:
Evaluate if the target host is
running a service supporting
  the Apache JServ Protocol (AJP)
accessible from a public WAN
(Internet) / publ!
ic LAN.
  Note: A configuration option
'Network type' to define if a
scanned network sho!
uld be seen as a
  public LAN can be found in the
preferences of the following VT:
  Global variable settings (OID:
1.3.6.1.4.1.25623.1.0.12288)
Details:
Apache JServ Protocol (AJP) Public
WAN (Internet) / Public LAN
Accessible (T...
(OID: 1.3.6.1.4.1.25623.1.0.108716)
Version used: 2025-07-11T05:42:17Z

References:
 url:
https://lists.apache.org/thread/bnys
5lvg1875dsslkkx2vmwxv833l35x


Issue
-----
NVT:    rsh Unencrypted Cleartext
Login
OID:    1.3.6.1.4.1.25623.1.0.100080
Threat: High (CVSS: 7.5)
Port:   514/tcp

Summary:
This remote host is running a rsh
service.

Vulnerability Detection Result:
The rsh service is misconfigured so
it is allowing connections without a
passwor!
d or with default root:root
credentials.

Solution:
Solution type: Mitigation
Disable the rsh service and use
alternatives like SSH
  instead.

Vulnerability Insight:
rsh (remote shell) is a command line
computer program which can
  execute shell commands as another
user, and on another computer across
a compu!
ter network.
  Remark: NIST don't see
'configuration issues' as software
flaws so the referen!
ced CVE has a
  severity of 0.0. The severity of
this VT has been raised by Greenbone
to still!
 report a
  configuration issue on the target.

Vulnerability Detection Method:
Details:
rsh Unencrypted Cleartext Login
(OID: 1.3.6.1.4.1.25623.1.0.100080)
Version used: 2021-10-20T09:03:29Z

References:
 cve: CVE-1999-0651


Issue
-----
NVT:    FTP Brute Force Logins With
Default Credentials Reporting
OID:    1.3.6.1.4.1.25623.1.0.108718
Threat: High (CVSS: 7.5)
Port:   21/tcp

Summary:
It was possible to login into the
remote FTP server using
  weak/known credentials.

Vulnerability Detection Result:
It was possible to login with the
following credentials
<User>:<Password>
msfadmin:msfadmin
postgres:postgres
service:service
user:user

Impact:
This issue may be exploited by a
remote attacker to e.g. gain
  access to sensitive information or
modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as
possible.

Vulnerability Insight:
The following devices are / software
is known to be affected:
  - CVE-2001-1594: Codonics printer
FTP service as used in GE Healthcare
eNTEGRA!
 P&R
  - CVE-2013-7404: GE Healthcare
Discovery NM 750b
  - CVE-2014-9198: Schneider
Electric ETG3000 FactoryCast HMI
gateways
  - CVE-2015-7261: QNAP iArtist Lite
distributed with QNAP Signage
Station
  - CVE-2016-8731: Foscam C1 devices
  - CVE-2017-8218: vsftpd on TP-Link
C2 and C20i devices
  - CVE-2018-9068: IMM2 for IBM and
Lenovo System x
  - CVE-2018-17771: Ingenico Telium
2 PoS terminals
  - CVE-2018-19063, CVE-2018-19064:
Foscam C2 and Opticam i5 devices
  - CVE-2018-25147: Microhard
Systems IPn4G
  - CVE-2020-36915: Adtec Digital
SignEdje Digital Signage Player
  Note: As the VT 'FTP Brute Force
Logins With Default Credentials'
(OID:
  1.3.6.1.4.1.25623.1.0.108717)
might run into a timeout the actual
reporting of!
 this vulnerability
  takes place in this VT instead.

Vulnerability Detection Method:
Reports weak/known credentials
detected by the VT
  'FTP Brute Force Logins With
Default Credentials' (OID:
1.3.6.1.4.1.25623.1.0.!
108717).
Details:
```

FTP Brute Force Logins With Default Credentials Reporting
(OID: 1.3.6.1.4.1.25623.1.0.108718)
Version used: 2026-01-16T15:42:49Z

References:
 cve: CVE-1999-0501
 cve: CVE-1999-0502
 cve: CVE-1999-0507
 cve: CVE-1999-0508
 cve: CVE-2001-1594
 cve: CVE-2013-7404
 cve: CVE-2014-9198
 cve: CVE-2015-7261
 cve: CVE-2016-8731
 cve: CVE-2017-8218
 cve: CVE-2018-9068
 cve: CVE-2018-17771
 cve: CVE-2018-19063
 cve: CVE-2018-19064
 cve: CVE-2018-25147
 cve: CVE-2020-36915

Issue

NVT: Test HTTP dangerous methods
OID: 1.3.6.1.4.1.25623.1.0.10498
Threat: High (CVSS: 7.5)
Port: 80/tcp

Summary:
Misconfigured web servers allows remote clients to perform
  dangerous HTTP methods such as PUT and DELETE.

Vulnerability Detection Result:
We could upload the following files via the PUT method at this web server:
http://193.42.15.22/dav/puttest1082812230.html
We could delete the following files via the DELETE method at this web server:
http://193.42.15.22/dav/puttest1082812230.html

Impact:
- Enabled PUT method: This might allow an attacker to upload
  and run arbitrary code on this web server.
  - Enabled DELETE method: This might allow an attacker to delete additional fil!
es on this web
  server.

Solution:
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods
  or disable them completely.

Affected Software/OS:
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method:
Checks if dangerous HTTP methods such as PUT and DELETE are
  enabled and can be misused to upload or delete files.
Details:
Test HTTP dangerous methods
(OID: 1.3.6.1.4.1.25623.1.0.10498)
Version used: 2023-08-01T13:29:10Z

References:
 url:
http://www.securityfocus.com/bid/12141
 owasp: OWASP-CM-001

Issue

NVT: The rlogin service is running
OID: 1.3.6.1.4.1.25623.1.0.901202
Threat: High (CVSS: 7.5)
Port: 513/tcp

Summary:
This remote host is running a rlogin service.

Vulnerability Detection Result:
The rlogin service is running on the target system.

Solution:
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight:
rlogin has several serious security problems,
  - all information, including passwords, is transmitted unencrypted.
  - .rlogin (or .rhosts) file is easy to misuse (potentially allowing
  anyone to login without a password)

Vulnerability Detection Method:
Details:
The rlogin service is running
(OID: 1.3.6.1.4.1.25623.1.0.901202)
Version used: 2025-03-05T05:38:53Z

References:
 cve: CVE-1999-0651

Issue

NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.105042
Threat: High (CVSS: 7.4)
Port: 5432/tcp

Summary:
OpenSSL is prone to a security bypass vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according to the Vulnerability Detection Method.

Impact:
Successfully exploiting this issue may allow attackers to obtain
  sensitive information by conducting a man-in-the-middle attack. This may lead !
to other attacks.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS:
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight:
OpenSSL does not properly restrict processing of ChangeCipherSpec
  messages, which allows man-in-the-middle attackers to trigger use of a zero-le!
ngth master key in
  certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or!
 obtain sensitive
  information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerabilit!
y.

Vulnerability Detection Method:
Send two SSL ChangeCipherSpec request and check the response.
Details:
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.105042)
Version used: 2025-01-17T15:39:18Z

References:
 cve: CVE-2014-0224
 url:
https://www.openssl.org/news/secadv/20140605.txt
 url:
http://www.securityfocus.com/bid/67899
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2023-0500
 cert-bund: CB-K15/0567
 cert-bund: CB-K15/0415
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0080
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0074
 cert-bund: CB-K14/1617
 cert-bund: CB-K14/1537
 cert-bund: CB-K14/1299
 cert-bund: CB-K14/1297
 cert-bund: CB-K14/1294
 cert-bund: CB-K14/1202
 cert-bund: CB-K14/1174
 cert-bund: CB-K14/1153
 cert-bund: CB-K14/0876
 cert-bund: CB-K14/0756
 cert-bund: CB-K14/0746
 cert-bund: CB-K14/0736
 cert-bund: CB-K14/0722
 cert-bund: CB-K14/0716
 cert-bund: CB-K14/0708
 cert-bund: CB-K14/0684
 cert-bund: CB-K14/0683
 cert-bund: CB-K14/0680
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2015-0593
 dfn-cert: DFN-CERT-2015-0427
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0082
 dfn-cert: DFN-CERT-2015-0079
 dfn-cert: DFN-CERT-2015-0078
 dfn-cert: DFN-CERT-2014-1717
 dfn-cert: DFN-CERT-2014-1632
 dfn-cert: DFN-CERT-2014-1364
 dfn-cert: DFN-CERT-2014-1357
 dfn-cert: DFN-CERT-2014-1350
 dfn-cert: DFN-CERT-2014-1265
 dfn-cert: DFN-CERT-2014-1209
 dfn-cert: DFN-CERT-2014-0917
 dfn-cert: DFN-CERT-2014-0789
 dfn-cert: DFN-CERT-2014-0778
 dfn-cert: DFN-CERT-2014-0768
 dfn-cert: DFN-CERT-2014-0752
 dfn-cert: DFN-CERT-2014-0747
 dfn-cert: DFN-CERT-2014-0738
 dfn-cert: DFN-CERT-2014-0715
 dfn-cert: DFN-CERT-2014-0714
 dfn-cert: DFN-CERT-2014-0709

Issue

NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.103935
Threat: Medium (CVSS: 6.8)
Port: 25/tcp

Summary:
Multiple vendors' implementations of 'STARTTLS' are prone to a
  vulnerability that lets attackers inject arbitrary commands.

Vulnerability Detection Result:

Vulnerability was detected according to the Vulnerability Detection Method.

Impact:
An attacker can exploit this issue to execute arbitrary commands
  in the context of the user running the application. Successful exploits can al!
low attackers to
  obtain email usernames and passwords.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for more
  information.

Affected Software/OS:
The following vendors are known to be affected:
  Ipswitch
  Kerio
  Postfix
  Qmail-TLS
  Oracle
  SCO Group
  spamdyke
  ISC

Vulnerability Detection Method:
Send a special crafted 'STARTTLS' request and check the
  response.
Details:
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injecti...
(OID: 1.3.6.1.4.1.25623.1.0.103935)
Version used: 2023-10-31T05:06:37Z

References:
 cve: CVE-2011-0411
 cve: CVE-2011-1430
 cve: CVE-2011-1431
 cve: CVE-2011-1432
 cve: CVE-2011-1506
 cve: CVE-2011-1575
 cve: CVE-2011-1926
 cve: CVE-2011-2165
 url: http://www.securityfocus.com/bid/46767
 url: http://kolab.org/pipermail/kolab-announce/2011/000101.html
 url: http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
 url: http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
 url: http://www.kb.cert.org/vuls/id/MAPG-8D9M4P
 url: http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt
 url: http://www.postfix.org/CVE-2011-0411.html
 url: http://www.pureftpd.org/project/pure-ftpd/news
 url: http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
 url: http://www.spamdyke.org/documentation/Changelog.txt
 url: http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1
 url: http://www.securityfocus.com/archive/1/516901
 url: http://support.avaya.com/css/P8/documents/100134676
 url: http://support.avaya.com/css/P8/documents/100141041
 url: http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
 url: http://inoa.net/qmail-tls/vu555316.patch
 url: http://www.kb.cert.org/vuls/id/555316
 cert-bund: CB-K15/1514
 dfn-cert: DFN-CERT-2011-0917
 dfn-cert: DFN-CERT-2011-0912
 dfn-cert: DFN-CERT-2011-0897
 dfn-cert: DFN-CERT-2011-0844
 dfn-cert: DFN-CERT-2011-0818
 dfn-cert: DFN-CERT-2011-0808
 dfn-cert: DFN-CERT-2011-0771
 dfn-cert: DFN-CERT-2011-0741
 dfn-cert: DFN-CERT-2011-0712
 dfn-cert: DFN-CERT-2011-0673
 dfn-cert: DFN-CERT-2011-0597
 dfn-cert: DFN-CERT-2011-0596
 dfn-cert: DFN-CERT-2011-0519
 dfn-cert: DFN-CERT-2011-0516
 dfn-cert: DFN-CERT-2011-0483
 dfn-cert: DFN-CERT-2011-0434
 dfn-cert: DFN-CERT-2011-0393
 dfn-cert: DFN-CERT-2011-0381

Issue

NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)
OID: 1.3.6.1.4.1.25623.1.0.801281
Threat: Medium (CVSS: 6.8)
Port: 80/tcp

Summary:
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result:
Installed version: 01.Feb.2003
Fixed version: 4.3.2

Impact:
Successful exploitation will allow attacker to gain administrative
  privileges on the target application and can cause CSRF attack.

Solution:
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS:
TWiki version prior to 4.3.2

Vulnerability Insight:
Attack can be done by tricking an authenticated TWiki user into visiting
  a static HTML page on another side, where a Javascript enabled browser will se!
nd an HTTP POST request
  to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method:
Details:
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)
(OID: 1.3.6.1.4.1.25623.1.0.801281)
Version used: 2024-03-01T14:37:10Z

References:
 cve: CVE-2009-4898
 url: http://www.openwall.com/lists/oss-security/2010/08/03/8
 url: http://www.openwall.com/lists/oss-security/2010/08/02/17
 url: http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
 url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Issue

NVT: RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible
OID: 1.3.6.1.4.1.25623.1.0.104901
Threat: Medium (CVSS: 6.4)
Port: 111/tcp

Product detection result:
cpe:/a:portmap:portmap
Detected by: RPC Portmapper Service Detection (TCP) (OID: 1.3.6.1.4.1.25623.1.0.108090)

Summary:
The script checks if the target host is running a RPC Portmapper
  service accessible from a public WAN (Internet) / public LAN.

Vulnerability Detection Result:
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:
Solution type: Mitigation
- Only allow access to the RPC Portmapper service from trusted
  sources
  - Disable the service if unused / not required

Vulnerability Insight:
A public accessible RPC Portmapper service is generally seen as
  / assumed to be a security misconfiguration.
  In addition openly accessible RPC Portmapper services can be abused for distri!
buted denial of
  service (DDoS) reflection attacks against third parties.
  Please see the references for more information.

Vulnerability Detection Method:
Evaluate if the target host is running a RPC Portmapper
  service accessible from a public WAN (Internet) / public LAN.
  Note: A configuration option 'Network type' to define if a scanned network sho!
uld be seen as a
  public LAN can be found in the preferences of the following VT:
  Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
Details:
RPC Portmapper Service Public WAN (Internet) / Public LAN Accessible
(OID: 1.3.6.1.4.1.25623.1.0.104901)
Version used: 2023-09-13T05:05:22Z

Product Detection Result:
Product:cpe:/a:portmap:portmap

Method:RPC Portmapper Service Detection (TCP)
(OID: 1.3.6.1.4.1.25623.1.0.108090)

References:
 url:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/Offene-Portmapper-Dienste/Offene-Portmapper-Dienste.html
 url:
https://www.debian.org/doc/manuals/securing-debian-manual/rpc.en.html
 url: https://blog.lumen.com/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

Issue

NVT: Anonymous FTP Login Reporting
OID: 1.3.6.1.4.1.25623.1.0.900600
Threat: Medium (CVSS: 6.4)
Port: 21/tcp

Summary:
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result:
It was possible to login to the remote FTP service with the following anonymous !
account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com

Impact:
Based on the files accessible via this anonymous FTP login and
  the permissions of this account an attacker might be able to:
  - gain access to sensitive files
  - upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous
  logins.

Vulnerability Insight:
A host that provides an FTP service may additionally provide
  Anonymous FTP access as well. Under this arrangement, users do not strictly ne!
ed an account on the
  host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for!
 username. Although
  users are commonly asked to send their email address as their password, little!
 to no verification
  is actually performed on the supplied data.
  Remark: NIST don't see 'configuration issues' as software flaws so the referen!
ced CVE has a
  severity of 0.0. The severity of this VT has been raised by Greenbone to still!
 report a
  configuration issue on the target.

Vulnerability Detection Method:
Details:
Anonymous FTP Login Reporting
(OID: 1.3.6.1.4.1.25623.1.0.900600)
Version used: 2021-10-20T09:03:29Z

References:
 cve: CVE-1999-0497

Issue

NVT: TWiki < 6.1.0 XSS Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.141830
Threat: Medium (CVSS: 6.1)
Port: 80/tcp

Summary:
bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result:
Installed version: 01.Feb.2003
Fixed version: 6.1.0

Solution:
Solution type: VendorFix
Update to version 6.1.0 or later.

Affected Software/OS:
TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Details:
TWiki < 6.1.0 XSS Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.141830)
Version used: 2023-07-14T16:09:27Z

References:
 cve: CVE-2018-20212
 url:
https://seclists.org/fulldisclosure/2019/Jan/7
 url: http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Issue

NVT: jQuery < 1.9.0 XSS Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.141636
Threat: Medium (CVSS: 6.1)
Port: 80/tcp

Summary:
jQuery is prone to a cross-site scripting (XSS)
  vulnerability.

Vulnerability Detection Result:
Installed version: 1.3.2
Fixed version: 1.9.0
Installation
path / port:
/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID:
1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file:
http://193.42.15.22/mutillidae/javascript/ddsmoothmenu/jquery!
.min.js
- Referenced at:
http://193.42.15.22/mutillidae/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS:
jQuery prior to version 1.9.0.

Vulnerability Insight:
The jQuery(strInput) function does not differentiate selectors
  from HTML in a reliable fashion. In vulnerable versions, jQuery determined whe!
ther the input was
  HTML by looking for the '<' character anywhere in the string, giving attackers!
 more flexibility
  when attempting to construct a malicious payload. In fixed versions, jQuery on!
ly deems the input
  to be HTML if it explicitly starts with the '<' character, limiting exploitabi!
lity only to
  attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Details:
jQuery < 1.9.0 XSS Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.141636)
Version used: 2023-07-14T05:06:08Z

References:
 cve: CVE-2012-6708
 url:
https://bugs.jquery.com/ticket/11290
 cert-bund: WID-SEC-2026-1752
 cert-bund: WID-SEC-2022-0673
 cert-bund: CB-K22/0045
 cert-bund: CB-K18/1131
 dfn-cert: DFN-CERT-2025-1803
 dfn-cert: DFN-CERT-2023-1197
 dfn-cert: DFN-CERT-2020-0590

Issue

NVT: Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Active Check
OID: 1.3.6.1.4.1.25623.1.0.108011
Threat: Medium (CVSS: 6.0)
Port: 445/tcp

Product detection result:
cpe:/a:samba:samba:3.0.20
Detected by: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary:
Samba is prone to a vulnerability that allows attackers to
  execute arbitrary shell commands because the software fails to sanitize user-s!
upplied input.

Vulnerability Detection Result:
By sending a special crafted SMB request it was possible to execute ``ping -p 5f!
4f70656e564153565431393039335f -c50 193.42.15.25`` on the remote host.
Received answer (ICMP "Data" field):
0x00: 6B 70 2C 6A 1B F3 04 00 56 54 31 39 30 39 33 5F
kp,j....VT19093_
0x10: 5F 4F 70 65 6E 56 41 53 56 54 31 39 30 39 33 5F
OpenVASVT19093
0x20: 5F 4F 70 65 6E 56 41 53 56 54 31 39 30 39 33 5F
OpenVASVT19093
0x30: 5F 4F 70 65 6E 56 41 53
_OpenVAS

Impact:
An attacker may leverage this issue to execute arbitrary shell
  commands on an affected system with the privileges of the application.

Solution:
Solution type: VendorFix
Updates are available. Please see the referenced vendor
  advisory.

Affected Software/OS:

```
Samba versions 3.0.0 through
3.0.25rc3.

Vulnerability Detection Method:
Sends a crafted SMB request and
checks if the target is
  sending an ICMP Echo Request back
to the scanner host.
  Note: For a successful detection
of this flaw the scanner host needs
to be abl!
e to directly
  receive ICMP Echo Requests (Type
8) from the target.
Details:
Samba 3.0.0 <= 3.0.25rc3 MS-RPC
Remote Shell Command Execution
Vulnerability...
(OID: 1.3.6.1.4.1.25623.1.0.108011)
Version used: 2026-03-12T05:56:11Z

Product Detection Result:
Product:cpe:/a:samba:samba:3.0.20

Method:SMB NativeLanMan
(OID: 1.3.6.1.4.1.25623.1.0.102011)

References:
 cve: CVE-2007-2447
 url:
https://www.samba.org/samba/security
/CVE-2007-2447.html
 url:
https://web.archive.org/web/20210121
173708/http://www.securityfocus.com/
bid/23972


Issue
-----
NVT:    TWiki CSRF Vulnerability
OID:    1.3.6.1.4.1.25623.1.0.800400
Threat: Medium (CVSS: 6.0)
Port:   80/tcp

Summary:
TWiki is prone to a cross-site
request forgery (CSRF)
vulnerability.

Vulnerability Detection Result:
Installed version: 01.Feb.2003
Fixed version:     4.3.1

Impact:
Successful exploitation will allow
attacker to gain administrative
  privileges on the target
application and can cause CSRF
attack.

Solution:
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS:
TWiki version prior to 4.3.1

Vulnerability Insight:
Remote authenticated user can create
a specially crafted image tag that,
  when viewed by the target user,
will update pages on the target
system with th!
e privileges of the target user
  via HTTP requests.

Vulnerability Detection Method:
Details:
TWiki CSRF Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.800400)
Version used: 2024-06-28T05:05:33Z

References:
 cve: CVE-2009-1339
 url:
http://secunia.com/advisories/34880
 url: http://bugs.debian.org/cgi-
bin/bugreport.cgi?bug=526258
 url:
http://twiki.org/p/pub/Codev/Securit
yAlert-CVE-2009-1339/TWiki-4.3.0-c-
diff-cve-2009-1339.txt


Issue
-----
NVT:    SSL/TLS: Deprecated SSLv2
and SSLv3 Protocol Detection
OID:    1.3.6.1.4.1.25623.1.0.111012
Threat: Medium (CVSS: 5.9)
Port:   5432/tcp

Product detection result:
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by: SSL/TLS: Version
Detection (OID:
1.3.6.1.4.1.25623.1.0.105782)

Summary:
It was possible to detect the usage
of the deprecated SSLv2
  and/or SSLv3 protocol on this
system.

Vulnerability Detection Result:
In addition to TLSv1.0+ the service
is also providing the deprecated
SSLv3 proto!
col and supports one or more
ciphers. Those supported ciphers can
be found in th!
e 'SSL/TLS: Report Supported Cipher
Suites' (OID:
1.3.6.1.4.1.25623.1.0.802067) !
VT.

Impact:
An attacker might be able to use the
known cryptographic flaws to
  eavesdrop the connection between
clients and the service to get
access to sens!
itive data
  transferred within the secured
connection.
  Furthermore newly uncovered
vulnerabilities in this protocols
won't receive se!
curity updates
  anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the
deprecated SSLv2 and/or SSLv3
  protocols in favor of the TLSv1.2+
protocols.
  Please see the references for more
resources supporting you with this
task.

Affected Software/OS:
All services providing an encrypted
communication using the
  SSLv2 and/or SSLv3 protocols.

Vulnerability Insight:
The SSLv2 and SSLv3 protocols
contain known cryptographic flaws
  like:
  - CVE-2014-3566: Padding Oracle On
Downgraded Legacy Encryption
(POODLE)
  - CVE-2016-0800: Decrypting RSA
with Obsolete and Weakened
eNcryption (DROWN)

Vulnerability Detection Method:
Checks the used SSL protocols of the
services provided by this
  system.
Details:
SSL/TLS: Deprecated SSLv2 and SSLv3
Protocol Detection
(OID: 1.3.6.1.4.1.25623.1.0.111012)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:secure_sockets_l
ayer:3.0

Method:SSL/TLS: Version Detection
(OID: 1.3.6.1.4.1.25623.1.0.105782)

References:
 cve: CVE-2016-0800
 cve: CVE-2014-3566
 url:
https://configurator.tlsref.org/
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
 url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
 url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
 url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
 url: https://drownattack.com
 url:
https://www.imperialviolet.org/2014/
10/14/poodle.html
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2025-1658
 cert-bund: WID-SEC-2023-0431
 cert-bund: WID-SEC-2023-0427
 cert-bund: CB-K18/0094
 cert-bund: CB-K17/1198
 cert-bund: CB-K17/1196
 cert-bund: CB-K16/1828
 cert-bund: CB-K16/1438
 cert-bund: CB-K16/1384
 cert-bund: CB-K16/1141
 cert-bund: CB-K16/1107
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0792
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0597
 cert-bund: CB-K16/0459
 cert-bund: CB-K16/0456
 cert-bund: CB-K16/0433
 cert-bund: CB-K16/0424
 cert-bund: CB-K16/0415
 cert-bund: CB-K16/0413
 cert-bund: CB-K16/0374
 cert-bund: CB-K16/0367
 cert-bund: CB-K16/0331
 cert-bund: CB-K16/0329
 cert-bund: CB-K16/0328
 cert-bund: CB-K16/0156
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1358
 cert-bund: CB-K15/1021
 cert-bund: CB-K15/0972
 cert-bund: CB-K15/0637
 cert-bund: CB-K15/0590
 cert-bund: CB-K15/0525
 cert-bund: CB-K15/0393
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0287
 cert-bund: CB-K15/0252
 cert-bund: CB-K15/0246
 cert-bund: CB-K15/0237
 cert-bund: CB-K15/0118
 cert-bund: CB-K15/0110
 cert-bund: CB-K15/0108
 cert-bund: CB-K15/0080
 cert-bund: CB-K15/0078
 cert-bund: CB-K15/0077
```

cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Issue

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID: 1.3.6.1.4.1.25623.1.0.111012
Threat: Medium (CVSS: 5.9)
Port: 25/tcp

Product detection result:
cpe:/a:ietf:secure_sockets_layer:2.0
Detected by: SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

Summary:
It was possible to detect the usage of the deprecated SSLv2
and/or SSLv3 protocol on this system.

Vulnerability Detection Result:
In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S!
SLv3 protocols and supports one or more ciphers. Those supported ciphers can be !
found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1!
.0.802067) VT.

Impact:
An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sens!
itive data
transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive se!
curity updates
anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3
protocols in favor of the TLSv1.2+ protocols.
Please see the references for more resources supporting you with this task.

Affected Software/OS:
All services providing an encrypted communication using the
SSLv2 and/or SSLv3 protocols.

Vulnerability Insight:
The SSLv2 and SSLv3 protocols contain known cryptographic flaws
like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method:
Checks the used SSL protocols of the services provided by this
system.
Details:
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
(OID: 1.3.6.1.4.1.25623.1.0.111012)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:secure_sockets_layer:2.0

Method:SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

References:
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://configurator.tlsref.org/
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
url: https://drownattack.com
url: https://www.imperialviolet.org/2014/10/14/poodle.html
cert-bund: WID-SEC-2026-0180
cert-bund: WID-SEC-2025-1658
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459

```
 dfn-cert: DFN-CERT-2016-0453
 dfn-cert: DFN-CERT-2016-0451
 dfn-cert: DFN-CERT-2016-0415
 dfn-cert: DFN-CERT-2016-0403
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2016-0360
 dfn-cert: DFN-CERT-2016-0359
 dfn-cert: DFN-CERT-2016-0357
 dfn-cert: DFN-CERT-2016-0171
 dfn-cert: DFN-CERT-2015-1431
 dfn-cert: DFN-CERT-2015-1075
 dfn-cert: DFN-CERT-2015-1026
 dfn-cert: DFN-CERT-2015-0664
 dfn-cert: DFN-CERT-2015-0548
 dfn-cert: DFN-CERT-2015-0404
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0259
 dfn-cert: DFN-CERT-2015-0254
 dfn-cert: DFN-CERT-2015-0245
 dfn-cert: DFN-CERT-2015-0118
 dfn-cert: DFN-CERT-2015-0114
 dfn-cert: DFN-CERT-2015-0083
 dfn-cert: DFN-CERT-2015-0082
 dfn-cert: DFN-CERT-2015-0081
 dfn-cert: DFN-CERT-2015-0076
 dfn-cert: DFN-CERT-2014-1717
 dfn-cert: DFN-CERT-2014-1680
 dfn-cert: DFN-CERT-2014-1632
 dfn-cert: DFN-CERT-2014-1564
 dfn-cert: DFN-CERT-2014-1542
 dfn-cert: DFN-CERT-2014-1414
 dfn-cert: DFN-CERT-2014-1366
 dfn-cert: DFN-CERT-2014-1354


Issue
-----
NVT:    SSL/TLS: Report Weak Cipher
Suites
OID:    1.3.6.1.4.1.25623.1.0.103440
Threat: Medium (CVSS: 5.9)
Port:   5432/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Report
Supported Cipher Suites (OID:
1.3.6.1.4.1.25623.1.0.802067)

Summary:
This routine reports all weak
SSL/TLS cipher suites accepted by
  a service.

Vulnerability Detection Result:
'Weak' cipher suites accepted by
this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by
this service via the TLSv1.0
protocol:
TLS_RSA_WITH_RC4_128_SHA

Impact:
This could allow remote attackers to
obtain sensitive information
  or have other, unspecified
impacts.

Solution:
Solution type: Mitigation
The configuration of this services
should be changed so that it
  does not accept the listed weak
cipher suites anymore.
  Please see the references for more
resources supporting you with this
task.

Affected Software/OS:
All services providing an encrypted
communication using weak
  SSL/TLS cipher suites.

Vulnerability Insight:
These rules are applied for the
evaluation of the cryptographic
  strength:
  - RC4 is considered to be weak
(CVE-2013-2566, CVE-2015-2808)
  - Ciphers using 64 bit or less are
considered to be vulnerable to brute
force !
methods and
  therefore considered as weak (CVE-
2015-4000)
  - 1024 bit RSA authentication is
considered to be insecure and
therefore as we!
ak
  - Any cipher considered to be
secure for only the next 10 years is
considered !
as medium
  - Any other cipher is considered
as strong

Vulnerability Detection Method:
Checks previous collected cipher
suites.
  NOTE: No severity for SMTP
services with 'Opportunistic TLS'
and weak cipher s!
uites on port 25/tcp
  is reported. If too strong cipher
suites are configured for this
service the a!
lternative would be
  to fall back to an even more
insecure cleartext communication.
Details:
SSL/TLS: Report Weak Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.103440)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_
security

Method:SSL/TLS: Report Supported
Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.802067)

References:
 cve: CVE-2013-2566
 cve: CVE-2015-2808
 cve: CVE-2015-4000
 url:
https://configurator.tlsref.org/
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
 url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
 url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
 url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
 cert-bund: WID-SEC-2026-0180
 cert-bund: CB-K21/0067
 cert-bund: CB-K19/0812
 cert-bund: CB-K17/1750
 cert-bund: CB-K16/1593
 cert-bund: CB-K16/1552
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0617
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0168
 cert-bund: CB-K16/0121
 cert-bund: CB-K16/0090
 cert-bund: CB-K16/0030
 cert-bund: CB-K15/1751
 cert-bund: CB-K15/1591
 cert-bund: CB-K15/1550
 cert-bund: CB-K15/1517
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1464
 cert-bund: CB-K15/1442
 cert-bund: CB-K15/1334
 cert-bund: CB-K15/1269
 cert-bund: CB-K15/1136
 cert-bund: CB-K15/1090
 cert-bund: CB-K15/1059
 cert-bund: CB-K15/1022
 cert-bund: CB-K15/1015
 cert-bund: CB-K15/0986
 cert-bund: CB-K15/0964
 cert-bund: CB-K15/0962
 cert-bund: CB-K15/0932
 cert-bund: CB-K15/0927
 cert-bund: CB-K15/0926
 cert-bund: CB-K15/0907
 cert-bund: CB-K15/0901
 cert-bund: CB-K15/0896
 cert-bund: CB-K15/0889
 cert-bund: CB-K15/0877
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0849
 cert-bund: CB-K15/0834
 cert-bund: CB-K15/0827
 cert-bund: CB-K15/0802
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0733
 cert-bund: CB-K15/0667
 cert-bund: CB-K14/0935
 cert-bund: CB-K13/0942
 dfn-cert: DFN-CERT-2023-2939
 dfn-cert: DFN-CERT-2021-0775
 dfn-cert: DFN-CERT-2020-1561
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2017-1821
 dfn-cert: DFN-CERT-2016-1692
 dfn-cert: DFN-CERT-2016-1648
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0665
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0184
 dfn-cert: DFN-CERT-2016-0135
 dfn-cert: DFN-CERT-2016-0101
 dfn-cert: DFN-CERT-2016-0035
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1679
 dfn-cert: DFN-CERT-2015-1632
 dfn-cert: DFN-CERT-2015-1608
 dfn-cert: DFN-CERT-2015-1542
 dfn-cert: DFN-CERT-2015-1518
 dfn-cert: DFN-CERT-2015-1406
 dfn-cert: DFN-CERT-2015-1341
 dfn-cert: DFN-CERT-2015-1194
 dfn-cert: DFN-CERT-2015-1144
 dfn-cert: DFN-CERT-2015-1113
 dfn-cert: DFN-CERT-2015-1078
 dfn-cert: DFN-CERT-2015-1067
 dfn-cert: DFN-CERT-2015-1038
 dfn-cert: DFN-CERT-2015-1016
 dfn-cert: DFN-CERT-2015-1012
 dfn-cert: DFN-CERT-2015-0980
 dfn-cert: DFN-CERT-2015-0977
 dfn-cert: DFN-CERT-2015-0976
 dfn-cert: DFN-CERT-2015-0960
 dfn-cert: DFN-CERT-2015-0956
 dfn-cert: DFN-CERT-2015-0944
 dfn-cert: DFN-CERT-2015-0937
 dfn-cert: DFN-CERT-2015-0925
 dfn-cert: DFN-CERT-2015-0884
 dfn-cert: DFN-CERT-2015-0881
 dfn-cert: DFN-CERT-2015-0879
 dfn-cert: DFN-CERT-2015-0866
 dfn-cert: DFN-CERT-2015-0844
 dfn-cert: DFN-CERT-2015-0800
 dfn-cert: DFN-CERT-2015-0737
 dfn-cert: DFN-CERT-2015-0696
 dfn-cert: DFN-CERT-2014-0977


Issue
-----
NVT:    HTTP Debugging Methods
(TRACE/TRACK) Enabled
```

OID: 1.3.6.1.4.1.25623.1.0.11213
Threat: Medium (CVSS: 5.8)
Port: 80/tcp

Summary:
The remote web server supports the TRACE and/or TRACK
  methods. TRACE and TRACK are HTTP methods which are used to debug web server c!
onnections.

Vulnerability Detection Result:
The web server has the following HTTP methods enabled: TRACE

Impact:
An attacker may use this flaw to trick your legitimate web
  users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server
  configuration.
  Please see the manual of your web server or the references for more informatio!
n.

Affected Software/OS:
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight:
It has been shown that web servers supporting this methods
  are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing!
, when used in
  conjunction with various weaknesses in browsers.

Vulnerability Detection Method:
Checks if HTTP methods such as TRACE and TRACK are
  enabled and can be used.
Details:
HTTP Debugging Methods (TRACE/TRACK) Enabled
(OID: 1.3.6.1.4.1.25623.1.0.11213)
Version used: 2023-08-01T13:29:10Z

References:
 cve: CVE-2003-1567
 cve: CVE-2004-2320
 cve: CVE-2004-2763
 cve: CVE-2005-3398
 cve: CVE-2006-4683
 cve: CVE-2007-3008
 cve: CVE-2008-7253
 cve: CVE-2009-2823
 cve: CVE-2010-0386
 cve: CVE-2012-2223
 cve: CVE-2014-7883
 url: http://www.kb.cert.org/vuls/id/288308
 url: http://www.securityfocus.com/bid/11604
 url: http://www.securityfocus.com/bid/15222
 url: http://www.securityfocus.com/bid/19915
 url: http://www.securityfocus.com/bid/24456
 url: http://www.securityfocus.com/bid/33374
 url: http://www.securityfocus.com/bid/36956
 url: http://www.securityfocus.com/bid/36990
 url: http://www.securityfocus.com/bid/37995
 url: http://www.securityfocus.com/bid/9506
 url: http://www.securityfocus.com/bid/9561
 url: http://www.kb.cert.org/vuls/id/867593
 url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
 url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trace-verbs/ba-p/784482
 url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
 cert-bund: CB-K14/0981
 dfn-cert: DFN-CERT-2021-1825
 dfn-cert: DFN-CERT-2014-1018
 dfn-cert: DFN-CERT-2010-0020

Issue

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits
OID: 1.3.6.1.4.1.25623.1.0.150710
Threat: Medium (CVSS: 5.3)
Port: 25/tcp

Summary:
The remote SSL/TLS server certificate and/or any of the
  certificates in the certificate chain is using a RSA key with less than 2048 b!
its.

Vulnerability Detection Result:
The remote SSL/TLS server is using the following certificate(s) with a RSA key w!
ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D!
626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Com!
plication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such t!
hing outside US,C=XX (Server certificate)

Impact:
Using certificates with weak RSA key size can lead to
  unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the
  certificates it signed.

Vulnerability Insight:
SSL/TLS certificates using RSA keys with less than 2048 bits are
  considered unsafe.

Vulnerability Detection Method:
Checks the RSA keys size of the server certificate and all
  certificates in chain for a size < 2048 bit.
Details:
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2...
(OID: 1.3.6.1.4.1.25623.1.0.150710)
Version used: 2021-12-10T12:48:00Z

References:
 url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Issue

NVT: phpinfo() Output Reporting (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.11229
Threat: Medium (CVSS: 5.3)
Port: 80/tcp

Summary:
Reporting of files containing the output of the phpinfo() PHP
  function previously detected via HTTP.

Vulnerability Detection Result:
The following files are calling the function phpinfo() which disclose potentiall!
y sensitive information:
http://193.42.15.22/mutillidae/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV!
E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph!
p5/cgi </td></tr>
  <h2>PHP Core</h2>
  <h2>PHP Variables</h2>
http://193.42.15.22/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV!
E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph!
p5/cgi </td></tr>
  <h2>PHP Core</h2>
  <h2>PHP Variables</h2>

Impact:
Some of the information that can be gathered from this file
  includes:
  The username of the user running the PHP process, if it is a sudo user, the IP!
 address of the
  host, the web server version, the system version (Unix, Linux, Windows, ...), !
and the root
  directory of the web server.

Solution:
Solution type: Workaround
Delete the listed files or restrict access to them.

Affected Software/OS:
All systems exposing a file containing the output of the
  phpinfo() PHP function.
  This VT is also reporting if an affected endpoint for the following products h!
ave been identified:
  - CVE-2008-0149: TUTOS
  - CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK
  - CVE-2024-10486: Google for WooCommerce plugin for WordPress

```
Vulnerability Insight:
Many PHP installation tutorials
instruct the user to create a
  file called phpinfo.php or similar
containing the phpinfo() statement.
Such a !
file is often left
  back in the webserver directory.

Vulnerability Detection Method:
This script reports files identified
by the following separate
  VT: 'phpinfo() Output Detection
(HTTP)' (OID:
1.3.6.1.4.1.25623.1.0.108474).
Details:
phpinfo() Output Reporting (HTTP)
(OID: 1.3.6.1.4.1.25623.1.0.11229)
Version used: 2025-07-09T05:43:50Z

References:
 cve: CVE-2008-0149
 cve: CVE-2023-49282
 cve: CVE-2023-49283
 cve: CVE-2024-10486
 url:
https://www.php.net/manual/en/functi
on.phpinfo.php
 url:
https://beaglesecurity.com/blog/vuln
erability/revealing-phpinfo.html


Issue
-----
NVT:    Weak Key Exchange (KEX)
Algorithm(s) Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.150713
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak key
  exchange (KEX) algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak KEX algorithm(s):
KEX algorithm                      |
Reason
-----------------------------------
-----------------------------------
--------!
-----------
diffie-hellman-group-exchange-sha1 |
Using SHA-1
diffie-hellman-group1-sha1         |
Using Oakley Group 2 (a 1024-bit
MODP group!
) and SHA-1

Impact:
An attacker can quickly break
individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX
algorithm(s)
  - 1024-bit MODP group / prime KEX
algorithms:
  Alternatively use elliptic-curve
Diffie-Hellmann in general, e.g.
Curve 25519.

Vulnerability Insight:
- 1024-bit MODP group / prime KEX
algorithms:
  Millions of HTTPS, SSH, and VPN
servers all use the same prime
numbers for Dif!
fie-Hellman key
  exchange. Practitioners believed
this was safe as long as new key
exchange mes!
sages were generated
  for every connection. However, the
first step in the number field
sieve-the mo!
st efficient
  algorithm for breaking a Diffie-
Hellman connection-is dependent only
on this p!
rime.
  A nation-state can break a 1024-
bit prime.

Vulnerability Detection Method:
Checks the supported KEX algorithms
of the remote SSH server.
  Currently weak KEX algorithms are
defined as the following:
  - non-elliptic-curve Diffie-
Hellmann (DH) KEX algorithms with
1024-bit MODP gr!
oup / prime
  - ephemerally generated key
exchange groups uses SHA-1
  - using RSA 1024-bit modulus key
Details:
Weak Key Exchange (KEX) Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.150713)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url:
https://weakdh.org/sysadmin.html
 url: https://www.rfc-
editor.org/rfc/rfc9142
 url: https://www.rfc-
editor.org/rfc/rfc9142#name-summary-
guidance-for-implem
 url: https://www.rfc-
editor.org/rfc/rfc6194
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.5


Issue
-----
NVT:    Weak Host Key Algorithm(s)
(SSH)
OID:    1.3.6.1.4.1.25623.1.0.117687
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak host
  key algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak host key
algorithm(s):
host key algorithm | Description
-----------------------------------
-----------------------------------
--------!
---------
ssh-dss            | Digital
Signature Algorithm (DSA) / Digital
Signature Stand!
ard (DSS)

Solution:
Solution type: Mitigation
Disable the reported weak host key
algorithm(s).

Vulnerability Detection Method:
Checks the supported host key
algorithms of the remote SSH
  server.
  Currently weak host key algorithms
are defined as the following:
  - ssh-dss: Digital Signature
Algorithm (DSA) / Digital Signature
Standard (DSS!
)
Details:
Weak Host Key Algorithm(s) (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.117687)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8332
 url: https://www.rfc-
editor.org/rfc/rfc8709
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.6


Issue
-----
NVT:    SSL/TLS: Server Certificate
/ Certificate in Chain with RSA keys
less than 2048 bits
OID:    1.3.6.1.4.1.25623.1.0.150710
Threat: Medium (CVSS: 5.3)
Port:   5432/tcp

Summary:
The remote SSL/TLS server
certificate and/or any of the
  certificates in the certificate
chain is using a RSA key with less
than 2048 b!
its.

Vulnerability Detection Result:
The remote SSL/TLS server is using
the following certificate(s) with a
RSA key w!
ith less than 2048 bits (public-key-
size:public-key-
algorithm:serial:issuer):
1024:RSA:00FAF93A4C7FB6B9CC:1.2.840.
113549.1.9.1=#726F6F74407562756E7475
3830342D!
626173652E6C6F63616C646F6D61696E,CN=
ubuntu804-base.localdomain,OU=Office
for Com!
plication of Otherwise Simple
Affairs,O=OCOSA,L=Everywhere,ST=Ther
e is no such t!
hing outside US,C=XX (Server
certificate)

Impact:
Using certificates with weak RSA key
size can lead to
  unauthorized exposure of sensitive
information.

Solution:
Solution type: Mitigation
Replace the certificate with a
stronger key and reissue the
  certificates it signed.

Vulnerability Insight:
SSL/TLS certificates using RSA keys
with less than 2048 bits are
  considered unsafe.
```

Vulnerability Detection Method:
Checks the RSA keys size of the server certificate and all
  certificates in chain for a size < 2048 bit.
Details:
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2...
(OID: 1.3.6.1.4.1.25623.1.0.150710)
Version used: 2021-12-10T12:48:00Z

References:
 url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Issue

NVT: SSL/TLS: Certificate Expired
OID: 1.3.6.1.4.1.25623.1.0.103955
Threat: Medium (CVSS: 5.0)
Port: 25/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)

Summary:
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result:
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
fingerprint (SHA-1) | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256) | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A!
F1E32DEE436DE813CC
issued by | 1.2.840.113549.1.9.1=#726F6F74407562756E747538!
30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office f!
or Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no !
such thing outside US,C=XX
public key algorithm | RSA
public key size (bits) | 1024
serial | 00FAF93A4C7FB6B9CC
signature algorithm | sha1WithRSAEncryption
subject | 1.2.840.113549.1.9.1=#726F6F74407562756E747538!
30342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office f!
or Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no !
such thing outside US,C=XX
subject alternative names (SAN) | None
valid from | 2010-03-17 14:07:45 UTC
valid until | 2010-04-16 14:07:45 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight:
This script checks expiry dates of certificates associated with
  SSL/TLS-enabled services on the target and reports whether any have already ex!
pired.

Vulnerability Detection Method:
Details:
SSL/TLS: Certificate Expired
(OID: 1.3.6.1.4.1.25623.1.0.103955)
Version used: 2026-03-13T05:54:58Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_security

Method:SSL/TLS: Collect and Report Certificate Details
(OID: 1.3.6.1.4.1.25623.1.0.103692)

Issue

NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
OID: 1.3.6.1.4.1.25623.1.0.117761
Threat: Medium (CVSS: 5.0)
Port: 5432/tcp

Summary:
The remote SSL/TLS service is prone to a denial of service (DoS)
  vulnerability.

Vulnerability Detection Result:
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an!
 existing / already established SSL/TLS connection
---!

--------!

TLSv1.0 | 10

Impact:
The flaw might make it easier for remote attackers to cause a
  DoS (CPU consumption) by performing many renegotiations within a single connec!
tion.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch
  information.
  A general solution is to remove/disable renegotiation capabilities altogether !
from/in the affected
  SSL/TLS service.

Affected Software/OS:
Every SSL/TLS service which does not properly restrict
  client-initiated renegotiation.

Vulnerability Insight:
The flaw exists because the remote SSL/TLS service does not
  properly restrict client-initiated renegotiation within the SSL and TLS protoc!
ols.
  Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security S!
ervices (NSS) but
  both are in a DISPUTED state with the following rationale:
  > It can also be argued that it is the responsibility of server deployments, n!
ot a security
  library, to prevent or limit renegotiation when it is inappropriate within a s!
pecific environment.
  Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method:
Checks if the remote service allows to re-do the same SSL/TLS
  handshake (Renegotiation) over an existing / already established SSL/TLS conne!
ction.
Details:
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
(OID: 1.3.6.1.4.1.25623.1.0.117761)
Version used: 2026-03-13T05:54:58Z

References:
 cve: CVE-2011-1473
 cve: CVE-2011-5094
 url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/
 url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
 url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
 url: https://www.openwall.com/lists/oss-security/2011/07/08/2
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2024-1591
 cert-bund: WID-SEC-2024-0796
 cert-bund: WID-SEC-2023-1435
 cert-bund: CB-K17/0980
 cert-bund: CB-K17/0979
 cert-bund: CB-K14/0772
 cert-bund: CB-K13/0915
 cert-bund: CB-K13/0462
 dfn-cert: DFN-CERT-2025-0933
 dfn-cert: DFN-CERT-2017-1013
 dfn-cert: DFN-CERT-2017-1012
 dfn-cert: DFN-CERT-2014-0809
 dfn-cert: DFN-CERT-2013-1928
 dfn-cert: DFN-CERT-2012-1112

Issue

NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check
OID: 1.3.6.1.4.1.25623.1.0.103210
Threat: Medium (CVSS: 5.0)
Port: 80/tcp

Summary:
awiki is prone to multiple local file include (LFI)
  vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result:
Vulnerable URL: http://193.42.15.22/mutillidae/index.php?page=/etc/passwd

Impact:
An attacker can exploit this vulnerability to obtain potentially
  sensitive information and execute arbitrary local scripts in the context of th!
e webserver
  process. This may allow the attacker to compromise the application and the hos!

```
t.

Solution:
Solution type: WillNotFix
No known solution was made available
for at least one year
  since the disclosure of this
vulnerability. Likely none will be
provided anymo!
re. General
  solution options are to upgrade to
a newer release, disable respective
feature!
s, remove the
  product or replace the product by
another one.

Affected Software/OS:
awiki version 20100125 and prior.

Vulnerability Detection Method:
Sends a crafted HTTP GET request and
checks the response.
Details:
awiki <= 20100125 Multiple LFI
Vulnerabilities - Active Check
(OID: 1.3.6.1.4.1.25623.1.0.103210)
Version used: 2025-04-15T05:54:49Z

References:
 url: https://www.exploit-
db.com/exploits/36047/
 url:
http://www.securityfocus.com/bid/491
87


Issue
-----
NVT:    Check if Mailserver answer
to VRFY and EXPN requests
OID:    1.3.6.1.4.1.25623.1.0.100072
Threat: Medium (CVSS: 5.0)
Port:   25/tcp

Summary:
The Mailserver on this host answers
to VRFY and/or EXPN requests.

Vulnerability Detection Result:
'VRFY root' produces the following
answer: 252 2.0.0 root

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your
Mailserver.
  For postfix add
'disable_vrfy_command=yes' in
'main.cf'.
  For Sendmail add the option 'O
PrivacyOptions=goaway'.
  It is suggested that, if you
really want to publish this type of
information, !
you use a mechanism
  that legitimate users actually
know about, such as Finger or HTTP.

Vulnerability Insight:
VRFY and EXPN ask the server for
information about an address. They
are
  inherently unusable through
firewalls, gateways, mail exchangers
for part-time!
 hosts, etc.

Vulnerability Detection Method:
Details:
Check if Mailserver answer to VRFY
and EXPN requests
(OID: 1.3.6.1.4.1.25623.1.0.100072)
Version used: 2023-10-31T05:06:37Z

References:
 url: http://cr.yp.to/smtp/vrfy.html

Issue
-----
NVT:    SSL/TLS: Certificate Expired
OID:    1.3.6.1.4.1.25623.1.0.103955
Threat: Medium (CVSS: 5.0)
Port:   5432/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Collect and
Report Certificate Details (OID:
1.3.6.1.4.1.25623.1.0.103692)

Summary:
The remote server's SSL/TLS
certificate has already expired.

Vulnerability Detection Result:
The certificate of the remote
service expired on 2010-04-16
14:07:45.
Certificate details:
fingerprint (SHA-1)             |
ED093088706603BFD5DC237399B498DA2D4D
31C6
fingerprint (SHA-256)           |
E7A7FA0D63E457C7C4A59B38B70849C6A70B
DA6F830C7A!
F1E32DEE436DE813CC
issued by                       |
1.2.840.113549.1.9.1=#726F6F74407562
756E747538!
30342D626173652E6C6F63616C646F6D6169
6E,CN=ubuntu804-
base.localdomain,OU=Office f!
or Complication of Otherwise Simple
Affairs,O=OCOSA,L=Everywhere,ST=Ther
e is no !
such thing outside US,C=XX
public key algorithm            |
RSA
public key size (bits)          |
1024
serial                          |
00FAF93A4C7FB6B9CC
signature algorithm             |
sha1WithRSAEncryption
subject                         |
1.2.840.113549.1.9.1=#726F6F74407562
756E747538!
30342D626173652E6C6F63616C646F6D6169
6E,CN=ubuntu804-
base.localdomain,OU=Office f!
or Complication of Otherwise Simple
Affairs,O=OCOSA,L=Everywhere,ST=Ther
e is no !
such thing outside US,C=XX
subject alternative names (SAN) |
None
valid from                      |
2010-03-17 14:07:45 UTC
valid until                     |
2010-04-16 14:07:45 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a
new one.

Vulnerability Insight:
This script checks expiry dates of
certificates associated with
  SSL/TLS-enabled services on the
target and reports whether any have
already ex!
pired.

Vulnerability Detection Method:
Details:
SSL/TLS: Certificate Expired
(OID: 1.3.6.1.4.1.25623.1.0.103955)
Version used: 2026-03-13T05:54:58Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_
security

Method:SSL/TLS: Collect and Report
Certificate Details
(OID: 1.3.6.1.4.1.25623.1.0.103692)


Issue
-----
NVT:    SSL/TLS: Renegotiation DoS
Vulnerability (CVE-2011-1473, CVE-
2011-5094)
OID:    1.3.6.1.4.1.25623.1.0.117761
Threat: Medium (CVSS: 5.0)
Port:   25/tcp

Summary:
The remote SSL/TLS service is prone
to a denial of service (DoS)
  vulnerability.

Vulnerability Detection Result:
The following indicates that the
remote SSL/TLS service is affected:
Protocol Version | Successful re-
done SSL/TLS handshakes
(Renegotiation) over an!
 existing / already established
SSL/TLS connection
-----------------------------------
-----------------------------------
--------!
-----------------------------------
--------------
TLSv1.0          | 10

Impact:
The flaw might make it easier for
remote attackers to cause a
  DoS (CPU consumption) by
performing many renegotiations
within a single connec!
tion.

Solution:
Solution type: VendorFix
Users should contact their vendors
for specific patch
  information.
  A general solution is to
remove/disable renegotiation
capabilities altogether !
from/in the affected
  SSL/TLS service.

Affected Software/OS:
Every SSL/TLS service which does not
properly restrict
  client-initiated renegotiation.

Vulnerability Insight:
The flaw exists because the remote
SSL/TLS service does not
  properly restrict client-initiated
renegotiation within the SSL and TLS
protoc!
ols.
  Note: The referenced CVEs are
affecting OpenSSL and Mozilla
Network Security S!
ervices (NSS) but
  both are in a DISPUTED state with
the following rationale:
  > It can also be argued that it is
the responsibility of server
deployments, n!
ot a security
  library, to prevent or limit
renegotiation when it is
inappropriate within a s!
pecific environment.
  Both CVEs are still kept in this
VT as a reference to the origin of
this flaw.

Vulnerability Detection Method:
Checks if the remote service allows
to re-do the same SSL/TLS
  handshake (Renegotiation) over an
existing / already established
SSL/TLS conne!
ction.
Details:
```

SSL/TLS: Renegotiation DoS
Vulnerability (CVE-2011-1473, CVE-
2011-5094)
(OID: 1.3.6.1.4.1.25623.1.0.117761)
Version used: 2026-03-13T05:54:58Z

References:
 cve: CVE-2011-1473
 cve: CVE-2011-5094
 url:
https://web.archive.org/web/20211201
133213/https://orchilles.com/ssl-
renegotiation-dos/
 url:
https://mailarchive.ietf.org/arch/ms
g/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
 url:
https://vincent.bernat.ch/en/blog/20
11-ssl-dos-mitigation
 url:
https://www.openwall.com/lists/oss-
security/2011/07/08/2
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2024-1591
 cert-bund: WID-SEC-2024-0796
 cert-bund: WID-SEC-2023-1435
 cert-bund: CB-K17/0980
 cert-bund: CB-K17/0979
 cert-bund: CB-K14/0772
 cert-bund: CB-K13/0915
 cert-bund: CB-K13/0462
 dfn-cert: DFN-CERT-2025-0933
 dfn-cert: DFN-CERT-2017-1013
 dfn-cert: DFN-CERT-2017-1012
 dfn-cert: DFN-CERT-2014-0809
 dfn-cert: DFN-CERT-2013-1928
 dfn-cert: DFN-CERT-2012-1112

Issue

NVT: QWikiwiki directory
traversal vulnerability
OID: 1.3.6.1.4.1.25623.1.0.16100
Threat: Medium (CVSS: 5.0)
Port: 80/tcp

Summary:
The remote host is running
QWikiwiki, a Wiki application
written in PHP.
  The remote version of this
software contains a validation input
flaw which may!
 allow an attacker
  to use it to read arbitrary files
on the remote host with the
privileges of th!
e web server.

Vulnerability Detection Result:
Vulnerable URL:
http://193.42.15.22/mutillidae/index
.php?page=../../../../../../!
../../../../../etc/passwd%00

Solution:
Solution type: WillNotFix
No known solution was made available
for at least one year since the
disclosure
  of this vulnerability. Likely none
will be provided anymore. General
solution !
options are to upgrade to a newer
  release, disable respective
features, remove the product or
replace the produc!
t by another one.

Vulnerability Detection Method:
Details:
QWikiwiki directory traversal
vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.16100)
Version used: 2025-04-15T05:54:49Z

References:
 cve: CVE-2005-0283
 url:
http://www.securityfocus.com/bid/121
63

Issue

NVT: /doc directory browsable
OID: 1.3.6.1.4.1.25623.1.0.10056
Threat: Medium (CVSS: 5.0)
Port: 80/tcp

Summary:
The /doc directory is browsable.
  /doc shows the content of the
/usr/doc directory and therefore it
shows which !
programs and - important! - the
version of the installed programs.

Vulnerability Detection Result:
Vulnerable URL:
http://193.42.15.22/doc/

Solution:
Solution type: Mitigation
Use access restrictions for the /doc
directory.
  If you use Apache you might use
this in your access.conf:
  <Directory /usr/doc>
  AllowOverride None
  order deny, allow
  deny from all
  allow from localhost
  </Directory>

Vulnerability Detection Method:
Details:
/doc directory browsable
(OID: 1.3.6.1.4.1.25623.1.0.10056)
Version used: 2023-08-01T13:29:10Z

References:
 cve: CVE-1999-0678
 url:
http://www.securityfocus.com/bid/318

Issue

NVT: FTP Unencrypted Cleartext
Login
OID: 1.3.6.1.4.1.25623.1.0.108528
Threat: Medium (CVSS: 4.8)
Port: 21/tcp

Summary:
The remote host is running a FTP
service that allows cleartext logins
over
  unencrypted connections.

Vulnerability Detection Result:
The remote FTP service accepts
logins without a previous sent 'AUTH
TLS' command!
. Response(s):
Non-anonymous sessions: 331 Please
specify the password.
Anonymous sessions: 331 Please
specify the password.

Impact:
An attacker can uncover login names
and passwords by sniffing traffic to
the
  FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the
connection via the 'AUTH TLS'
command. Please see
  the manual of the FTP service for
more information.

Vulnerability Detection Method:
Tries to login to a non FTPS enabled
FTP service without sending a
  'AUTH TLS' command first and
checks if the service is accepting
the login with!
out enforcing the use of
  the 'AUTH TLS' command.
Details:
FTP Unencrypted Cleartext Login
(OID: 1.3.6.1.4.1.25623.1.0.108528)
Version used: 2023-12-20T05:05:58Z

Issue

NVT: FTP Unencrypted Cleartext
Login
OID: 1.3.6.1.4.1.25623.1.0.108528
Threat: Medium (CVSS: 4.8)
Port: 2121/tcp

Summary:
The remote host is running a FTP
service that allows cleartext logins
over
  unencrypted connections.

Vulnerability Detection Result:
The remote FTP service accepts
logins without a previous sent 'AUTH
TLS' command!
. Response(s):
Non-anonymous sessions: 331 Password
required for openvasvt
Anonymous sessions: 331 Password
required for anonymous

Impact:
An attacker can uncover login names
and passwords by sniffing traffic to
the
  FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the
connection via the 'AUTH TLS'
command. Please see
  the manual of the FTP service for
more information.

Vulnerability Detection Method:
Tries to login to a non FTPS enabled
FTP service without sending a
  'AUTH TLS' command first and
checks if the service is accepting
the login with!
out enforcing the use of
  the 'AUTH TLS' command.
Details:
FTP Unencrypted Cleartext Login
(OID: 1.3.6.1.4.1.25623.1.0.108528)
Version used: 2023-12-20T05:05:58Z

Issue

NVT: Telnet Unencrypted Cleartext
Login
OID: 1.3.6.1.4.1.25623.1.0.108522
Threat: Medium (CVSS: 4.8)
Port: 23/tcp

Summary:
The remote host is running a Telnet
service that allows cleartext logins
over
  unencrypted connections.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Impact:
An attacker can uncover login names
and passwords by sniffing traffic to
the
  Telnet service.

Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method:
Details:
Telnet Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108522)
Version used: 2023-10-13T05:06:09Z

Issue

NVT: VNC Server Unencrypted Data Transmission
OID: 1.3.6.1.4.1.25623.1.0.108529
Threat: Medium (CVSS: 4.8)
Port: 5900/tcp

Summary:
The remote host is running a VNC server providing one or more insecure or
cryptographically weak Security Type(s) not intended for use on untrusted netw!
orks.

Vulnerability Detection Result:
The VNC server provides the following insecure or cryptographically weak Securit!
y Type(s):
2 (VNC authentication)

Impact:
An attacker can uncover sensitive data by sniffing traffic to the
VNC server.

Solution:
Solution type: Mitigation
Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RF!
C4254].
Some VNC server vendors are also providing more secure Security Types within t!
heir products.

Vulnerability Detection Method:
Details:
VNC Server Unencrypted Data Transmission
(OID: 1.3.6.1.4.1.25623.1.0.108529)
Version used: 2023-07-12T05:05:04Z

References:
url:
https://tools.ietf.org/html/rfc6143#page-10

Issue

NVT: Cleartext Transmission of Sensitive Information via HTTP
OID: 1.3.6.1.4.1.25623.1.0.108440
Threat: Medium (CVSS: 4.8)
Port: 80/tcp

Summary:
The host / application transmits sensitive information (username, passwords) in
cleartext via HTTP.

Vulnerability Detection Result:
The following input fields were identified (URL:input name):
http://193.42.15.22/dvwa/login.php:password
http://193.42.15.22/phpMyAdmin/:pma_password
http://193.42.15.22/phpMyAdmin/?D=A:pma_password
http://193.42.15.22/tikiwiki/tiki-install.php:pass
http://193.42.15.22/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword

Impact:
An attacker could use this situation to compromise or eavesdrop on the
HTTP communication between the client and the server using a man-in-the-middle!
attack to get access to
sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
Additionally make sure the host / application is redirecting all users to the !
secured SSL/TLS connection before
allowing to input sensitive data into the mentioned functions.

Affected Software/OS:
Hosts / applications which doesn't enforce the transmission of sensitive data vi!
a an
encrypted SSL/TLS connection.

Vulnerability Detection Method:
Evaluate previous collected information and check if the host / application is n!
ot
enforcing the transmission of sensitive data via an encrypted SSL/TLS connecti!
on.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details:
Cleartext Transmission of Sensitive Information via HTTP
(OID: 1.3.6.1.4.1.25623.1.0.108440)
Version used: 2023-09-07T05:05:21Z

References:
url:
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
url:
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url:
https://cwe.mitre.org/data/definitions/319.html

Issue

NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.801660
Threat: Medium (CVSS: 4.3)
Port: 80/tcp

Summary:
phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according to the Vulnerability Detection Method.

Impact:
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure
of this vulnerability. Likely none will be provided anymore. General solution !
options are to upgrade to a newer
release, disable respective features, remove the product or replace the produc!
t by another one.

Affected Software/OS:
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight:
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which
could allow attackers to inject arbitrary HTML code within the error page
and conduct phishing attacks.

Vulnerability Detection Method:
Details:
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.801660)
Version used: 2023-10-17T05:05:34Z

References:
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url:
http://www.vupen.com/english/advisories/2010/3133
dfn-cert: DFN-CERT-2011-0467
dfn-cert: DFN-CERT-2011-0451
dfn-cert: DFN-CERT-2011-0016
dfn-cert: DFN-CERT-2011-0002

Issue

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.902830
Threat: Medium (CVSS: 4.3)
Port: 80/tcp

Product detection result:
cpe:/a:apache:http_server:2.2.8
Detected by: Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)

Summary:
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according to the Vulnerability Detection Method.

Impact:
Successful exploitation will allow attackers to obtain sensitive information
that may aid in further attacks.

Solution:
Solution type: VendorFix

```
Update to Apache HTTP Server version
2.2.22 or later.

Affected Software/OS:
Apache HTTP Server versions 2.2.0
through 2.2.21.

Vulnerability Insight:
The flaw is due to an error within
the default error response for
  status code 400 when no custom
ErrorDocument is configured, which
can be
  exploited to expose 'httpOnly'
cookies.

Vulnerability Detection Method:
Details:
Apache HTTP Server 'httpOnly' Cookie
Information Disclosure Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.902830)
Version used: 2026-02-24T05:57:09Z

Product Detection Result:
Product:cpe:/a:apache:http_server:2.
2.8

Method:Apache HTTP Server Detection
Consolidation
(OID: 1.3.6.1.4.1.25623.1.0.117232)

References:
 cve: CVE-2012-0053
 url:
http://secunia.com/advisories/47779
 url:
http://www.securityfocus.com/bid/517
06
 url: http://www.exploit-
db.com/exploits/18442
 url:
http://rhn.redhat.com/errata/RHSA-
2012-0128.html
 url:
http://httpd.apache.org/security/vul
nerabilities_22.html
 url:
http://svn.apache.org/viewvc?view=re
vision&revision=1235454
 url:
http://lists.opensuse.org/opensuse-
security-announce/2012-
02/msg00026.html
 cert-bund: CB-K15/0080
 cert-bund: CB-K14/1505
 cert-bund: CB-K14/0608
 dfn-cert: DFN-CERT-2015-0082
 dfn-cert: DFN-CERT-2014-1592
 dfn-cert: DFN-CERT-2014-0635
 dfn-cert: DFN-CERT-2013-1307
 dfn-cert: DFN-CERT-2012-1276
 dfn-cert: DFN-CERT-2012-1112
 dfn-cert: DFN-CERT-2012-0928
 dfn-cert: DFN-CERT-2012-0758
 dfn-cert: DFN-CERT-2012-0744
 dfn-cert: DFN-CERT-2012-0568
 dfn-cert: DFN-CERT-2012-0425
 dfn-cert: DFN-CERT-2012-0424
 dfn-cert: DFN-CERT-2012-0387
 dfn-cert: DFN-CERT-2012-0343
 dfn-cert: DFN-CERT-2012-0332
 dfn-cert: DFN-CERT-2012-0306
 dfn-cert: DFN-CERT-2012-0264
 dfn-cert: DFN-CERT-2012-0203
 dfn-cert: DFN-CERT-2012-0188


Issue
-----
NVT:    SSL/TLS: Deprecated TLSv1.0
and TLSv1.1 Protocol Detection
OID:    1.3.6.1.4.1.25623.1.0.117274
Threat: Medium (CVSS: 4.3)
Port:   5432/tcp

Product detection result:
cpe:/a:ietf:secure_sockets_layer:3.0
Detected by: SSL/TLS: Version
Detection (OID:
1.3.6.1.4.1.25623.1.0.105782)

Summary:
It was possible to detect the usage
of the deprecated TLSv1.0
  and/or TLSv1.1 protocol on this
system.

Vulnerability Detection Result:
The service is only providing the
deprecated TLSv1.0 protocol and
supports one o!
r more ciphers. Those supported
ciphers can be found in the
'SSL/TLS: Report Sup!
ported Cipher Suites' (OID:
1.3.6.1.4.1.25623.1.0.802067) VT.

Impact:
An attacker might be able to use the
known cryptographic flaws to
  eavesdrop the connection between
clients and the service to get
access to sens!
itive data
  transferred within the secured
connection.
  Furthermore newly uncovered
vulnerabilities in this protocols
won't receive se!
curity updates
  anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the
deprecated TLSv1.0 and/or
  TLSv1.1 protocols in favor of the
TLSv1.2+ protocols.
  Please see the references for more
resources supporting you with this
task.

Affected Software/OS:
- All services providing an
encrypted communication using the
  TLSv1.0 and/or TLSv1.1 protocols
  - CVE-2023-41928: Kiloview P1 4G
and P2 4G Video Encoder
  - CVE-2024-41270: Gorush v1.18.4
  - CVE-2025-3200: Multiple products
from Wiesemann & Theis

Vulnerability Insight:
The TLSv1.0 and TLSv1.1 protocols
contain known cryptographic
  flaws like:
  - CVE-2011-3389: Browser Exploit
Against SSL/TLS (BEAST)
  - CVE-2015-0204: Factoring Attack
on RSA-EXPORT Keys Padding Oracle On
Downgra!
ded Legacy
  Encryption (FREAK)

Vulnerability Detection Method:
Checks the used TLS protocols of the
services provided by this
  system.
Details:
SSL/TLS: Deprecated TLSv1.0 and
TLSv1.1 Protocol Detection
(OID: 1.3.6.1.4.1.25623.1.0.117274)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:secure_sockets_l
ayer:3.0

Method:SSL/TLS: Version Detection
(OID: 1.3.6.1.4.1.25623.1.0.105782)

References:
 cve: CVE-2011-3389
 cve: CVE-2015-0204
 cve: CVE-2023-41928
 cve: CVE-2024-41270
 cve: CVE-2025-3200
 url:
https://configurator.tlsref.org/
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
 url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
 url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
 url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
 url:
https://datatracker.ietf.org/doc/rfc
8996/
 url:
https://vnhacker.blogspot.com/2011/0
9/beast.html
 url:
https://web.archive.org/web/20201108
095603/https://censys.io/blog/freak
 url:
https://certvde.com/en/advisories/VD
E-2025-031/
 url:
https://gist.github.com/nyxfqq/cfae3
8fada582a0f576d154be1aeb1fc
 url:
https://advisories.ncsc.nl/advisory?
id=NCSC-2024-0273
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2023-1435
 cert-bund: CB-K18/0799
 cert-bund: CB-K16/1289
 cert-bund: CB-K16/1096
 cert-bund: CB-K15/1751
 cert-bund: CB-K15/1266
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0720
 cert-bund: CB-K15/0548
 cert-bund: CB-K15/0526
 cert-bund: CB-K15/0509
 cert-bund: CB-K15/0493
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0365
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0016
 cert-bund: CB-K14/1342
 cert-bund: CB-K14/0231
 cert-bund: CB-K13/0845
 cert-bund: CB-K13/0796
 cert-bund: CB-K13/0790
 dfn-cert: DFN-CERT-2020-0177
 dfn-cert: DFN-CERT-2020-0111
 dfn-cert: DFN-CERT-2019-0068
 dfn-cert: DFN-CERT-2018-1441
 dfn-cert: DFN-CERT-2018-1408
 dfn-cert: DFN-CERT-2016-1372
 dfn-cert: DFN-CERT-2016-1164
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1332
 dfn-cert: DFN-CERT-2015-0884
 dfn-cert: DFN-CERT-2015-0800
 dfn-cert: DFN-CERT-2015-0758
 dfn-cert: DFN-CERT-2015-0567
 dfn-cert: DFN-CERT-2015-0544
 dfn-cert: DFN-CERT-2015-0530
```

```
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482


Issue
-----
NVT:    SSL/TLS: Deprecated TLSv1.0
and TLSv1.1 Protocol Detection
OID:    1.3.6.1.4.1.25623.1.0.117274
Threat: Medium (CVSS: 4.3)
Port:   25/tcp

Product detection result:
cpe:/a:ietf:secure_sockets_layer:2.0
Detected by: SSL/TLS: Version
Detection (OID:
1.3.6.1.4.1.25623.1.0.105782)

Summary:
It was possible to detect the usage
of the deprecated TLSv1.0
  and/or TLSv1.1 protocol on this
system.

Vulnerability Detection Result:
The service is only providing the
deprecated TLSv1.0 protocol and
supports one o!
r more ciphers. Those supported
ciphers can be found in the
'SSL/TLS: Report Sup!
ported Cipher Suites' (OID:
1.3.6.1.4.1.25623.1.0.802067) VT.

Impact:
An attacker might be able to use the
known cryptographic flaws to
  eavesdrop the connection between
clients and the service to get
access to sens!
itive data
  transferred within the secured
connection.
  Furthermore newly uncovered
vulnerabilities in this protocols
won't receive se!
curity updates
  anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the
deprecated TLSv1.0 and/or
  TLSv1.1 protocols in favor of the
TLSv1.2+ protocols.
  Please see the references for more
resources supporting you with this
task.

Affected Software/OS:
- All services providing an
encrypted communication using the
  TLSv1.0 and/or TLSv1.1 protocols
  - CVE-2023-41928: Kiloview P1 4G
and P2 4G Video Encoder
  - CVE-2024-41270: Gorush v1.18.4
  - CVE-2025-3200: Multiple products
from Wiesemann & Theis

Vulnerability Insight:
The TLSv1.0 and TLSv1.1 protocols
contain known cryptographic
  flaws like:
  - CVE-2011-3389: Browser Exploit
Against SSL/TLS (BEAST)
  - CVE-2015-0204: Factoring Attack
on RSA-EXPORT Keys Padding Oracle On
Downgra!
ded Legacy
  Encryption (FREAK)

Vulnerability Detection Method:
Checks the used TLS protocols of the
services provided by this
  system.
Details:
SSL/TLS: Deprecated TLSv1.0 and
TLSv1.1 Protocol Detection
(OID: 1.3.6.1.4.1.25623.1.0.117274)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:secure_sockets_l
ayer:2.0

Method:SSL/TLS: Version Detection
(OID: 1.3.6.1.4.1.25623.1.0.105782)

References:
 cve: CVE-2011-3389
 cve: CVE-2015-0204
 cve: CVE-2023-41928
 cve: CVE-2024-41270
 cve: CVE-2025-3200
 url:
https://configurator.tlsref.org/
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
 url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
 url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
 url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
 url:
https://datatracker.ietf.org/doc/rfc
8996/
 url:
https://vnhacker.blogspot.com/2011/0
9/beast.html
 url:
https://web.archive.org/web/20201108
095603/https://censys.io/blog/freak
 url:
https://certvde.com/en/advisories/VD
E-2025-031/
 url:
https://gist.github.com/nyxfqq/cfae3
8fada582a0f576d154be1aeb1fc
 url:
https://advisories.ncsc.nl/advisory?
id=NCSC-2024-0273
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2023-1435
 cert-bund: CB-K18/0799
 cert-bund: CB-K16/1289
 cert-bund: CB-K16/1096
 cert-bund: CB-K15/1751
 cert-bund: CB-K15/1266
 cert-bund: CB-K15/0850
 cert-bund: CB-K15/0764
 cert-bund: CB-K15/0720
 cert-bund: CB-K15/0548
 cert-bund: CB-K15/0526
 cert-bund: CB-K15/0509
 cert-bund: CB-K15/0493
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0365
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0079
 cert-bund: CB-K15/0016
 cert-bund: CB-K14/1342
 cert-bund: CB-K14/0231
 cert-bund: CB-K13/0845
 cert-bund: CB-K13/0796
 cert-bund: CB-K13/0790
 dfn-cert: DFN-CERT-2020-0177
 dfn-cert: DFN-CERT-2020-0111
 dfn-cert: DFN-CERT-2019-0068
 dfn-cert: DFN-CERT-2018-1441
 dfn-cert: DFN-CERT-2018-1408
 dfn-cert: DFN-CERT-2016-1372
 dfn-cert: DFN-CERT-2016-1164
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1332
 dfn-cert: DFN-CERT-2015-0884
 dfn-cert: DFN-CERT-2015-0800
 dfn-cert: DFN-CERT-2015-0758
 dfn-cert: DFN-CERT-2015-0567
 dfn-cert: DFN-CERT-2015-0544
 dfn-cert: DFN-CERT-2015-0530
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0375
 dfn-cert: DFN-CERT-2015-0374
 dfn-cert: DFN-CERT-2015-0305
 dfn-cert: DFN-CERT-2015-0199
 dfn-cert: DFN-CERT-2015-0079
 dfn-cert: DFN-CERT-2015-0021
 dfn-cert: DFN-CERT-2014-1414
 dfn-cert: DFN-CERT-2013-1847
 dfn-cert: DFN-CERT-2013-1792
 dfn-cert: DFN-CERT-2012-1979
 dfn-cert: DFN-CERT-2012-1829
 dfn-cert: DFN-CERT-2012-1530
 dfn-cert: DFN-CERT-2012-1380
 dfn-cert: DFN-CERT-2012-1377
 dfn-cert: DFN-CERT-2012-1292
 dfn-cert: DFN-CERT-2012-1214
```

dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

Issue

NVT: jQuery < 1.6.3 XSS Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.141637
Threat: Medium (CVSS: 4.3)
Port: 80/tcp

Summary:
jQuery is prone to a cross-site scripting (XSS)
vulnerability.

Vulnerability Detection Result:
Installed version: 1.3.2
Fixed version: 1.6.3
Installation
path / port:
/mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID:
1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file:
http://193.42.15.22/mutillidae/javascript/ddsmoothmenu/jquery!
.min.js
- Referenced at:
http://193.42.15.22/mutillidae/

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS:
jQuery prior to version 1.6.3.

Vulnerability Insight:
Cross-site scripting (XSS)
vulnerability in jQuery before 1.6.3,
when using location.hash to select elements, allows remote attackers to inject!
arbitrary web
script or HTML via a crafted tag.

Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Details:
jQuery < 1.6.3 XSS Vulnerability
(OID: 1.3.6.1.4.1.25623.1.0.141637)
Version used: 2023-07-14T05:06:08Z

References:
cve: CVE-2011-4969
url:
https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: WID-SEC-2026-1752
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890

Issue

NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID: 1.3.6.1.4.1.25623.1.0.805142
Threat: Medium (CVSS: 4.3)
Port: 25/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Report Supported Cipher Suites (OID:
1.3.6.1.4.1.25623.1.0.802067)

Summary:
This host is accepting 'RSA_EXPORT' cipher suites and is prone
to a man-in-the-middle (MITM) vulnerability.

Vulnerability Detection Result:
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact:
Successful exploitation will allow remote attacker to downgrade
the security of a session to use 'RSA_EXPORT' cipher suites, which are signifi!
cantly weaker than
non-export cipher suites. This may allow a man-in-the-middle attacker to more !
easily break the
encryption and monitor or tamper with the encrypted stream.

Solution:
Solution type: VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the
service. Please see the references for more resources supporting you with this!
task.
- If the service is using OpenSSL: Update to version 0.9.8zd, 1.0.0p, 1.0.1k o!
r later.

Affected Software/OS:
- Hosts accepting 'RSA_EXPORT' cipher suites.
- OpenSSL versions prior to 0.9.8zd, 1.0.0 prior to 1.0.0p and 1.0.1 prior to !
1.0.1k.

Vulnerability Insight:
Flaw is due to improper handling RSA temporary keys in a
non-export RSA key exchange cipher suite.

Vulnerability Detection Method:
Checks previous collected cipher suites.
Details:
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
(OID: 1.3.6.1.4.1.25623.1.0.805142)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_security

Method:SSL/TLS: Report Supported Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.802067)

References:
cve: CVE-2015-0204
url: https://freakattack.com
url: https://openssl-library.org/news/secadv/20150108.txt
url:
https://web.archive.org/web/20210122095002/http://www.securityfocus.com/bid/71936
url:
https://www.secpod.com/blog/freak-attack
url:
https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa
url:
https://configurator.tlsref.org/
url:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html
url:
https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html
url:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html
url:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html
url:
https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url:
https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
cert-bund: WID-SEC-2026-0180
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365

```
 cert-bund: CB-K15/0364
 cert-bund: CB-K15/0302
 cert-bund: CB-K15/0192
 cert-bund: CB-K15/0016
 dfn-cert: DFN-CERT-2018-1408
 dfn-cert: DFN-CERT-2016-1372
 dfn-cert: DFN-CERT-2016-1164
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2015-1853
 dfn-cert: DFN-CERT-2015-1332
 dfn-cert: DFN-CERT-2015-0884
 dfn-cert: DFN-CERT-2015-0800
 dfn-cert: DFN-CERT-2015-0758
 dfn-cert: DFN-CERT-2015-0567
 dfn-cert: DFN-CERT-2015-0544
 dfn-cert: DFN-CERT-2015-0530
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0375
 dfn-cert: DFN-CERT-2015-0374
 dfn-cert: DFN-CERT-2015-0305
 dfn-cert: DFN-CERT-2015-0199
 dfn-cert: DFN-CERT-2015-0021


Issue
-----
NVT:    Weak Encryption Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105611
Threat: Medium (CVSS: 4.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak
  encryption algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the
following weak server-to-client
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution:
Solution type: Mitigation
Disable the reported weak encryption
algorithm(s).

Vulnerability Insight:
- The 'arcfour' cipher is the
Arcfour stream cipher with 128-bit
  keys. The Arcfour cipher is
believed to be compatible with the
RC4 cipher [SCH!
NEIER]. Arcfour
  (and RC4) has problems with weak
keys, and should not be used
anymore.
  - The 'none' algorithm specifies
that no encryption is to be done.
Note that t!
his method provides
  no confidentiality protection, and
it is NOT RECOMMENDED to use it.
  - A vulnerability exists in SSH
messages that employ CBC mode that
may allow a!
n attacker to
  recover plaintext from a block of
ciphertext.

Vulnerability Detection Method:
Checks the supported encryption
algorithms (client-to-server
  and server-to-client) of the
remote SSH server.
  Currently weak encryption
algorithms are defined as the
following:
  - Arcfour (RC4) cipher based
algorithms
  - 'none' algorithm
  - CBC mode cipher based algorithms
Details:
Weak Encryption Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8758
 url:
https://www.kb.cert.org/vuls/id/9585
63
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.3


Issue
-----
NVT:    SSL/TLS: Certificate Signed
Using A Weak Signature Algorithm
OID:    1.3.6.1.4.1.25623.1.0.105880
Threat: Medium (CVSS: 4.0)
Port:   25/tcp

Summary:
The remote service is using a
SSL/TLS certificate in the
certificate chain that !
has been signed using a
  cryptographically weak hashing
algorithm.

Vulnerability Detection Result:
The following certificates are part
of the certificate chain but using
insecure !
signature algorithms:
Subject:
1.2.840.113549.1.9.1=#726F6F74407562
756E74753830342D626173!
652E6C6F63616C646F6D61696E,CN=ubuntu
804-base.localdomain,OU=Office for
Complicat!
ion of Otherwise Simple
Affairs,O=OCOSA,L=Everywhere,ST=Ther
e is no such thing o!
utside US,C=XX
Signature Algorithm:
sha1WithRSAEncryption

Solution:
Solution type: Mitigation
Servers that use SSL/TLS
certificates signed with a weak SHA-
1, MD5, MD4 or MD2 !
hashing algorithm will need to
obtain new
  SHA-2 signed SSL/TLS certificates
to avoid web browser SSL/TLS
certificate war!
nings.

Vulnerability Insight:
The following hashing algorithms
used for signing SSL/TLS
certificates are consi!
dered cryptographically weak
  and not secure enough for ongoing
use:
  - Secure Hash Algorithm 1 (SHA-1)
  - Message Digest 5 (MD5)
  - Message Digest 4 (MD4)
  - Message Digest 2 (MD2)
  Beginning as late as January 2017
and as early as June 2016, browser
developer!
s such as Microsoft and Google will
begin warning users when visiting
  web sites that use SHA-1 signed
Secure Socket Layer (SSL)
certificates.
  NOTE: The script preference allows
to set one or more custom SHA-1
fingerprint!
s of CA certificates which are
trusted by this routine. The
fingerprints
  needs to be passed comma-separated
and case-insensitive:
  Fingerprint1
  or
  fingerprint1, Fingerprint2

Vulnerability Detection Method:
Check which hashing algorithm was
used to sign the remote SSL/TLS
certificate.
Details:
SSL/TLS: Certificate Signed Using A
Weak Signature Algorithm
(OID: 1.3.6.1.4.1.25623.1.0.105880)
Version used: 2021-10-15T11:13:32Z

References:
 url:
https://blog.mozilla.org/security/20
14/09/23/phasing-out-certificates-
with-sha-1-based-signature-
algorithms/


Issue
-----
NVT:    SSL/TLS: Diffie-Hellman Key
Exchange Insufficient DH Group
Strength Vulnerability
OID:    1.3.6.1.4.1.25623.1.0.106223
Threat: Medium (CVSS: 4.0)
Port:   5432/tcp

Summary:
The SSL/TLS service uses Diffie-
Hellman groups with insufficient
  strength (key size < 2048).

Vulnerability Detection Result:
Server Temporary Key Size: 1024 bits

Impact:
An attacker might be able to decrypt
the SSL/TLS communication
  offline.

Solution:
Solution type: Workaround
- Deploy (Ephemeral) Elliptic-Curve
Diffie-Hellman (ECDHE) or use
  a 2048-bit or stronger Diffie-
Hellman group. Please see the
references for mor!
e resources
  supporting you with this task.
```

- For Apache Web Servers:
Beginning with version 2.4.7,
mod_ssl will use DH pa!
rameters which
include primes with lengths of
more than 1024 bits.

Affected Software/OS:
All services providing an encrypted
communication using
Diffie-Hellman groups with
insufficient strength.

Vulnerability Insight:
The Diffie-Hellman group are some
big numbers that are used as
base for the DH computations. They
can be, and often are, fixed. The
security !
of the final secret
depends on the size of these
parameters. It was found that 512
and 768 bits to!
be weak, 1024 bits
to be breakable by really powerful
attackers like governments.

Vulnerability Detection Method:
Checks the DHE temporary public key
size.
Details:
SSL/TLS: Diffie-Hellman Key Exchange
Insufficient DH Group Strength
Vulnerab...
(OID: 1.3.6.1.4.1.25623.1.0.106223)
Version used: 2026-06-03T07:18:10Z

References:
url: https://weakdh.org
url:
https://weakdh.org/sysadmin.html
url:
https://configurator.tlsref.org/
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
url:
https://httpd.apache.org/docs/2.4/mo
d/mod_ssl.html#sslcertificatefile

Issue

NVT: SSL/TLS: Diffie-Hellman Key
Exchange Insufficient DH Group
Strength Vulnerability
OID: 1.3.6.1.4.1.25623.1.0.106223
Threat: Medium (CVSS: 4.0)
Port: 25/tcp

Summary:
The SSL/TLS service uses Diffie-
Hellman groups with insufficient
strength (key size < 2048).

Vulnerability Detection Result:
Server Temporary Key Size: 1024 bits

Impact:
An attacker might be able to decrypt
the SSL/TLS communication
offline.

Solution:
Solution type: Workaround
- Deploy (Ephemeral) Elliptic-Curve
Diffie-Hellman (ECDHE) or use
a 2048-bit or stronger Diffie-
Hellman group. Please see the
references for mor!
e resources
supporting you with this task.
- For Apache Web Servers:
Beginning with version 2.4.7,
mod_ssl will use DH pa!
rameters which
include primes with lengths of
more than 1024 bits.

Affected Software/OS:
All services providing an encrypted
communication using
Diffie-Hellman groups with
insufficient strength.

Vulnerability Insight:
The Diffie-Hellman group are some
big numbers that are used as
base for the DH computations. They
can be, and often are, fixed. The
security !
of the final secret
depends on the size of these
parameters. It was found that 512
and 768 bits to!
be weak, 1024 bits
to be breakable by really powerful
attackers like governments.

Vulnerability Detection Method:
Checks the DHE temporary public key
size.
Details:
SSL/TLS: Diffie-Hellman Key Exchange
Insufficient DH Group Strength
Vulnerab...
(OID: 1.3.6.1.4.1.25623.1.0.106223)
Version used: 2026-06-03T07:18:10Z

References:
url: https://weakdh.org
url:
https://weakdh.org/sysadmin.html
url:
https://configurator.tlsref.org/
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
url:
https://httpd.apache.org/docs/2.4/mo
d/mod_ssl.html#sslcertificatefile

Issue

NVT: SSL/TLS: Certificate Signed
Using A Weak Signature Algorithm
OID: 1.3.6.1.4.1.25623.1.0.105880
Threat: Medium (CVSS: 4.0)
Port: 5432/tcp

Summary:
The remote service is using a
SSL/TLS certificate in the
certificate chain that !
has been signed using a
cryptographically weak hashing
algorithm.

Vulnerability Detection Result:
The following certificates are part
of the certificate chain but using
insecure !
signature algorithms:
Subject:
1.2.840.113549.1.9.1=#726F6F74407562
756E74753830342D626173!
652E6C6F63616C646F6D61696E,CN=ubuntu
804-base.localdomain,OU=Office for
Complicat!
ion of Otherwise Simple
Affairs,O=OCOSA,L=Everywhere,ST=Ther
e is no such thing o!
utside US,C=XX
Signature Algorithm:
sha1WithRSAEncryption

Solution:
Solution type: Mitigation
Servers that use SSL/TLS
certificates signed with a weak SHA-
1, MD5, MD4 or MD2 !
hashing algorithm will need to
obtain new
SHA-2 signed SSL/TLS certificates
to avoid web browser SSL/TLS
certificate war!
nings.

Vulnerability Insight:
The following hashing algorithms
used for signing SSL/TLS
certificates are consi!
dered cryptographically weak
and not secure enough for ongoing
use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017
and as early as June 2016, browser
developer!
s such as Microsoft and Google will
begin warning users when visiting
web sites that use SHA-1 signed
Secure Socket Layer (SSL)
certificates.
NOTE: The script preference allows
to set one or more custom SHA-1
fingerprint!
s of CA certificates which are
trusted by this routine. The
fingerprints
needs to be passed comma-separated
and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method:
Check which hashing algorithm was
used to sign the remote SSL/TLS
certificate.
Details:
SSL/TLS: Certificate Signed Using A
Weak Signature Algorithm
(OID: 1.3.6.1.4.1.25623.1.0.105880)
Version used: 2021-10-15T11:13:32Z

References:

```
 url:
https://blog.mozilla.org/security/20
14/09/23/phasing-out-certificates-
with-sha-1-based-signature-
algorithms/


Issue
-----
NVT:    SSL/TLS: 'DHE_EXPORT' MITM
Security Bypass Vulnerability
(LogJam)
OID:    1.3.6.1.4.1.25623.1.0.805188
Threat: Low (CVSS: 3.7)
Port:   25/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Report
Supported Cipher Suites (OID:
1.3.6.1.4.1.25623.1.0.802067)

Summary:
This host is accepting 'DHE_EXPORT'
cipher suites and is prone
  to a man-in-the-middle (MITM)
vulnerability.

Vulnerability Detection Result:
'DHE_EXPORT' cipher suites accepted
by this service via the SSLv3
protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SH
A
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SH
A
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted
by this service via the TLSv1.0
protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SH
A
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SH
A
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact:
Successful exploitation will allow a
man-in-the-middle attacker
  to downgrade the security of a TLS
session to 512-bit export-grade
cryptograph!
y, which is
  significantly weaker, allowing the
attacker to more easily break the
encryptio!
n and monitor or
  tamper with the encrypted stream.

Solution:
Solution type: VendorFix
- Remove support for 'DHE_EXPORT'
cipher
  suites from the service. Please
see the references for more
resources supporti!
ng you with this
  task.
  - If the service is using OpenSSL:
Update to version 1.0.1n, 1.0.2b or
later.

Affected Software/OS:
- Hosts accepting 'DHE_EXPORT'
cipher suites.
  - OpenSSL versions prior to 1.0.1n
and 1.0.2 prior to 1.0.2b.

Vulnerability Insight:
Flaw is triggered when handling
Diffie-Hellman key exchanges
  defined in the 'DHE_EXPORT' cipher
suites.

Vulnerability Detection Method:
Checks previous collected cipher
suites.
Details:
SSL/TLS: 'DHE_EXPORT' MITM Security
Bypass Vulnerability (LogJam)
(OID: 1.3.6.1.4.1.25623.1.0.805188)
Version used: 2026-06-03T07:18:10Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_
security

Method:SSL/TLS: Report Supported
Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.802067)

References:
 cve: CVE-2015-4000
 url: https://weakdh.org
 url:
https://weakdh.org/sysadmin.html
 url:
https://web.archive.org/web/20210122
160144/http://www.securityfocus.com/
bid/74733
 url: https://weakdh.org/imperfect-
forward-secrecy.pdf
 url:
https://openwall.com/lists/oss-
security/2015/05/20/8
 url:
https://blog.cloudflare.com/logjam-
the-latest-tls-vulnerability-
explained
 url: https://openssl-
library.org/post/2015-05-20-logjam-
freak-upcoming-changes/index.html
 url:
https://configurator.tlsref.org/
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/EN/BSI/Publications/TechGui
delines/TG02102/BSI-TR-02102-1.html
 url:
https://www.bsi.bund.de/EN/Themen/Oe
ffentliche-
Verwaltung/Mindeststandards/TLS-
Protokoll/TLS-Protokoll_node.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Publikationen/Techni
scheRichtlinien/TR03116/BSI-TR-
03116-4.html
 url:
https://www.bsi.bund.de/SharedDocs/D
ownloads/DE/BSI/Mindeststandards/Min
deststandard_BSI_TLS_Version_2_4.htm
l
 url:
https://web.archive.org/web/20240113
175943/https://www.bettercrypto.org
 url:
https://www.enisa.europa.eu/publicat
ions/algorithms-key-size-and-
parameters-report-2014
 cert-bund: WID-SEC-2026-0180
 cert-bund: CB-K21/0067
 cert-bund: CB-K19/0812
 cert-bund: CB-K16/1593
 cert-bund: CB-K16/1552
 cert-bund: CB-K16/0617
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0168
 cert-bund: CB-K16/0121
 cert-bund: CB-K16/0090
 cert-bund: CB-K16/0030
 cert-bund: CB-K15/1591
 cert-bund: CB-K15/1550
 cert-bund: CB-K15/1517
 cert-bund: CB-K15/1464
 cert-bund: CB-K15/1442
 cert-bund: CB-K15/1334
 cert-bund: CB-K15/1269
 cert-bund: CB-K15/1136
 cert-bund: CB-K15/1090
 cert-bund: CB-K15/1059
 cert-bund: CB-K15/1022
 cert-bund: CB-K15/1015
 cert-bund: CB-K15/0964
 cert-bund: CB-K15/0932
 cert-bund: CB-K15/0927
 cert-bund: CB-K15/0926
 cert-bund: CB-K15/0907
 cert-bund: CB-K15/0901
 cert-bund: CB-K15/0896
 cert-bund: CB-K15/0877
 cert-bund: CB-K15/0834
 cert-bund: CB-K15/0802
 cert-bund: CB-K15/0733
 dfn-cert: DFN-CERT-2023-2939
 dfn-cert: DFN-CERT-2021-0775
 dfn-cert: DFN-CERT-2020-1561
 dfn-cert: DFN-CERT-2020-1276
 dfn-cert: DFN-CERT-2016-1692
 dfn-cert: DFN-CERT-2016-1648
 dfn-cert: DFN-CERT-2016-0665
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0184
 dfn-cert: DFN-CERT-2016-0135
 dfn-cert: DFN-CERT-2016-0101
 dfn-cert: DFN-CERT-2016-0035
 dfn-cert: DFN-CERT-2015-1679
 dfn-cert: DFN-CERT-2015-1632
 dfn-cert: DFN-CERT-2015-1608
 dfn-cert: DFN-CERT-2015-1542
 dfn-cert: DFN-CERT-2015-1518
 dfn-cert: DFN-CERT-2015-1406
 dfn-cert: DFN-CERT-2015-1341
 dfn-cert: DFN-CERT-2015-1194
 dfn-cert: DFN-CERT-2015-1144
 dfn-cert: DFN-CERT-2015-1113
 dfn-cert: DFN-CERT-2015-1078
 dfn-cert: DFN-CERT-2015-1067
 dfn-cert: DFN-CERT-2015-1016
 dfn-cert: DFN-CERT-2015-0980
 dfn-cert: DFN-CERT-2015-0977
 dfn-cert: DFN-CERT-2015-0976
 dfn-cert: DFN-CERT-2015-0960
 dfn-cert: DFN-CERT-2015-0956
 dfn-cert: DFN-CERT-2015-0944
 dfn-cert: DFN-CERT-2015-0925
 dfn-cert: DFN-CERT-2015-0879
 dfn-cert: DFN-CERT-2015-0844
 dfn-cert: DFN-CERT-2015-0737


Issue
-----
NVT:    SSL/TLS: SSLv3 Protocol CBC
Cipher Suites Information Disclosure
Vulnerability (POODLE)
OID:    1.3.6.1.4.1.25623.1.0.802087
Threat: Low (CVSS: 3.4)
Port:   25/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Report
Supported Cipher Suites (OID:
1.3.6.1.4.1.25623.1.0.802067)

Summary:
This host is prone to an information
disclosure vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Impact:
Successful exploitation will allow a
man-in-the-middle attackers gain
access to!
 the plain text data stream.

Solution:
Solution type: Mitigation
Possible Mitigations are:
  - Disable SSLv3
  - Disable cipher suites supporting
CBC cipher modes
  - Enable TLS_FALLBACK_SCSV if the
service is providing TLSv1.0+

Vulnerability Insight:
The flaw is due to the block cipher
padding not being deterministic and
not cove!
red by the Message Authentication
Code
```

Vulnerability Detection Method:
Evaluate previous collected
information about this service.
Details:
SSL/TLS: SSLv3 Protocol CBC Cipher
Suites Information Disclosure
Vulnerabili...
(OID: 1.3.6.1.4.1.25623.1.0.802087)
Version used: 2026-03-13T05:54:58Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_
security

Method:SSL/TLS: Report Supported
Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.802067)

References:
 cve: CVE-2014-3566
 url:
https://www.openssl.org/~bodo/ssl-
poodle.pdf
 url:
http://www.securityfocus.com/bid/705
74
 url:
https://www.imperialviolet.org/2014/
10/14/poodle.html
 url:
https://www.dfranke.us/posts/2014-
10-14-how-poodle-happened.html
 url:
http://googleonlinesecurity.blogspot
.in/2014/10/this-poodle-bites-
exploiting-ssl-30.html
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2025-1658
 cert-bund: WID-SEC-2023-0431
 cert-bund: CB-K17/1198
 cert-bund: CB-K17/1196
 cert-bund: CB-K16/1828
 cert-bund: CB-K16/1438
 cert-bund: CB-K16/1384
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0156
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1358
 cert-bund: CB-K15/1021
 cert-bund: CB-K15/0972
 cert-bund: CB-K15/0637
 cert-bund: CB-K15/0590
 cert-bund: CB-K15/0525
 cert-bund: CB-K15/0393
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0287
 cert-bund: CB-K15/0252
 cert-bund: CB-K15/0246
 cert-bund: CB-K15/0237
 cert-bund: CB-K15/0118
 cert-bund: CB-K15/0110
 cert-bund: CB-K15/0108
 cert-bund: CB-K15/0080
 cert-bund: CB-K15/0078
 cert-bund: CB-K15/0077
 cert-bund: CB-K15/0075
 cert-bund: CB-K14/1617
 cert-bund: CB-K14/1581
 cert-bund: CB-K14/1537
 cert-bund: CB-K14/1479
 cert-bund: CB-K14/1458
 cert-bund: CB-K14/1342
 cert-bund: CB-K14/1314
 cert-bund: CB-K14/1313
 cert-bund: CB-K14/1311
 cert-bund: CB-K14/1304
 cert-bund: CB-K14/1296
 dfn-cert: DFN-CERT-2017-1238
 dfn-cert: DFN-CERT-2017-1236
 dfn-cert: DFN-CERT-2016-1929
 dfn-cert: DFN-CERT-2016-1527
 dfn-cert: DFN-CERT-2016-1468
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0884
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2016-0171
 dfn-cert: DFN-CERT-2015-1431
 dfn-cert: DFN-CERT-2015-1075
 dfn-cert: DFN-CERT-2015-1026
 dfn-cert: DFN-CERT-2015-0664
 dfn-cert: DFN-CERT-2015-0548
 dfn-cert: DFN-CERT-2015-0404
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0259
 dfn-cert: DFN-CERT-2015-0254
 dfn-cert: DFN-CERT-2015-0245
 dfn-cert: DFN-CERT-2015-0118
 dfn-cert: DFN-CERT-2015-0114
 dfn-cert: DFN-CERT-2015-0083
 dfn-cert: DFN-CERT-2015-0082
 dfn-cert: DFN-CERT-2015-0081
 dfn-cert: DFN-CERT-2015-0076
 dfn-cert: DFN-CERT-2014-1717
 dfn-cert: DFN-CERT-2014-1680
 dfn-cert: DFN-CERT-2014-1632
 dfn-cert: DFN-CERT-2014-1564
 dfn-cert: DFN-CERT-2014-1542
 dfn-cert: DFN-CERT-2014-1414
 dfn-cert: DFN-CERT-2014-1366
 dfn-cert: DFN-CERT-2014-1354

Issue

NVT: SSL/TLS: SSLv3 Protocol CBC
Cipher Suites Information Disclosure
Vulnerability (POODLE)
OID: 1.3.6.1.4.1.25623.1.0.802087
Threat: Low (CVSS: 3.4)
Port: 5432/tcp

Product detection result:
cpe:/a:ietf:transport_layer_security
Detected by: SSL/TLS: Report
Supported Cipher Suites (OID:
1.3.6.1.4.1.25623.1.0.802067)

Summary:
This host is prone to an information
disclosure vulnerability.

Vulnerability Detection Result:
Vulnerability was detected according
to the Vulnerability Detection
Method.

Impact:
Successful exploitation will allow a
man-in-the-middle attackers gain
access to!
 the plain text data stream.

Solution:
Solution type: Mitigation
Possible Mitigations are:
  - Disable SSLv3
  - Disable cipher suites supporting
CBC cipher modes
  - Enable TLS_FALLBACK_SCSV if the
service is providing TLSv1.0+

Vulnerability Insight:
The flaw is due to the block cipher
padding not being deterministic and
not cove!
red by the Message Authentication
Code

Vulnerability Detection Method:
Evaluate previous collected
information about this service.
Details:
SSL/TLS: SSLv3 Protocol CBC Cipher
Suites Information Disclosure
Vulnerabili...
(OID: 1.3.6.1.4.1.25623.1.0.802087)
Version used: 2026-03-13T05:54:58Z

Product Detection Result:
Product:cpe:/a:ietf:transport_layer_
security

Method:SSL/TLS: Report Supported
Cipher Suites
(OID: 1.3.6.1.4.1.25623.1.0.802067)

References:
 cve: CVE-2014-3566
 url:
https://www.openssl.org/~bodo/ssl-
poodle.pdf
 url:
http://www.securityfocus.com/bid/705
74
 url:
https://www.imperialviolet.org/2014/
10/14/poodle.html
 url:
https://www.dfranke.us/posts/2014-
10-14-how-poodle-happened.html
 url:
http://googleonlinesecurity.blogspot
.in/2014/10/this-poodle-bites-
exploiting-ssl-30.html
 cert-bund: WID-SEC-2026-0180
 cert-bund: WID-SEC-2025-1658
 cert-bund: WID-SEC-2023-0431
 cert-bund: CB-K17/1198
 cert-bund: CB-K17/1196
 cert-bund: CB-K16/1828
 cert-bund: CB-K16/1438
 cert-bund: CB-K16/1384
 cert-bund: CB-K16/1102
 cert-bund: CB-K16/0599
 cert-bund: CB-K16/0156
 cert-bund: CB-K15/1514
 cert-bund: CB-K15/1358
 cert-bund: CB-K15/1021
 cert-bund: CB-K15/0972
 cert-bund: CB-K15/0637
 cert-bund: CB-K15/0590
 cert-bund: CB-K15/0525
 cert-bund: CB-K15/0393
 cert-bund: CB-K15/0384
 cert-bund: CB-K15/0287
 cert-bund: CB-K15/0252
 cert-bund: CB-K15/0246
 cert-bund: CB-K15/0237
 cert-bund: CB-K15/0118
 cert-bund: CB-K15/0110
 cert-bund: CB-K15/0108
 cert-bund: CB-K15/0080
 cert-bund: CB-K15/0078
 cert-bund: CB-K15/0077
 cert-bund: CB-K15/0075
 cert-bund: CB-K14/1617
 cert-bund: CB-K14/1581
 cert-bund: CB-K14/1537
 cert-bund: CB-K14/1479
 cert-bund: CB-K14/1458
 cert-bund: CB-K14/1342
 cert-bund: CB-K14/1314
 cert-bund: CB-K14/1313
 cert-bund: CB-K14/1311
 cert-bund: CB-K14/1304
 cert-bund: CB-K14/1296
 dfn-cert: DFN-CERT-2017-1238
 dfn-cert: DFN-CERT-2017-1236
 dfn-cert: DFN-CERT-2016-1929
 dfn-cert: DFN-CERT-2016-1527
 dfn-cert: DFN-CERT-2016-1468
 dfn-cert: DFN-CERT-2016-1168
 dfn-cert: DFN-CERT-2016-0884
 dfn-cert: DFN-CERT-2016-0642
 dfn-cert: DFN-CERT-2016-0388
 dfn-cert: DFN-CERT-2016-0171
 dfn-cert: DFN-CERT-2015-1431
 dfn-cert: DFN-CERT-2015-1075
 dfn-cert: DFN-CERT-2015-1026
 dfn-cert: DFN-CERT-2015-0664
 dfn-cert: DFN-CERT-2015-0548
 dfn-cert: DFN-CERT-2015-0404
 dfn-cert: DFN-CERT-2015-0396
 dfn-cert: DFN-CERT-2015-0259
 dfn-cert: DFN-CERT-2015-0254
 dfn-cert: DFN-CERT-2015-0245
 dfn-cert: DFN-CERT-2015-0118
 dfn-cert: DFN-CERT-2015-0114
 dfn-cert: DFN-CERT-2015-0083
 dfn-cert: DFN-CERT-2015-0082
 dfn-cert: DFN-CERT-2015-0081
 dfn-cert: DFN-CERT-2015-0076
 dfn-cert: DFN-CERT-2014-1717
 dfn-cert: DFN-CERT-2014-1680

```
 dfn-cert: DFN-CERT-2014-1632
 dfn-cert: DFN-CERT-2014-1564
 dfn-cert: DFN-CERT-2014-1542
 dfn-cert: DFN-CERT-2014-1414
 dfn-cert: DFN-CERT-2014-1366
 dfn-cert: DFN-CERT-2014-1354


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
umac-64@openssh.com
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    TCP Timestamps Information
Disclosure
OID:    1.3.6.1.4.1.25623.1.0.80091
Threat: Low (CVSS: 2.6)
Port:   general/tcp

Summary:
The remote host implements TCP
timestamps and therefore allows
  to compute the uptime.

Vulnerability Detection Result:
It was detected that the host
implements RFC1323/RFC7323.
The following timestamps were
retrieved with a delay of 1 seconds
in-between:
Packet 1: 1664703
Packet 2: 1664807

Impact:
A side effect of this feature is
that the uptime of the remote
  host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux
add the line
  'net.ipv4.tcp_timestamps = 0' to
/etc/sysctl.conf. Execute 'sysctl -
p' to appl!
y the settings at
  runtime.
  To disable TCP timestamps on
Windows execute 'netsh int tcp set
global timesta!
mps=disabled'
  Starting with Windows Server 2008
and Vista, the timestamp can not be
complete!
ly disabled.
  The default behavior of the TCP/IP
stack on this Systems is to not use
the Tim!
estamp options when
  initiating TCP connections, but
use them if the TCP peer that is
initiating co!
mmunication includes
  them in their synchronize (SYN)
segment.
  See the references for more
information.

Affected Software/OS:
TCP implementations that implement
RFC1323/RFC7323.

Vulnerability Insight:
The remote host implements TCP
timestamps, as defined by
  RFC1323/RFC7323.

Vulnerability Detection Method:
Special IP packets are forged and
sent with a little delay in
  between to the target IP. The
responses are searched for a
timestamps. If foun!
d, the timestamps
  are reported.
Details:
TCP Timestamps Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.80091)
Version used: 2023-12-15T16:10:08Z

References:
 url:
https://datatracker.ietf.org/doc/htm
l/rfc1323
 url:
https://datatracker.ietf.org/doc/htm
l/rfc7323
 url:
https://web.archive.org/web/20151213
072445/http://www.microsoft.com/en-
us/download/details.aspx?id=9152
 url:
https://www.fortiguard.com/psirt/FG-
IR-16-090

Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.25
*****************

Scanning of this host started at:
Fri Jun 12 19:41:40 2026 UTC
Number of results: 0

Port Summary for Host 193.42.15.25
-----------------------------------

Service (Port)          Threat Level

Security Issues for Host
193.42.15.25
-----------------------------------
-
```

```
Host 193.42.15.27
*****************

Scanning of this host started at:
Fri Jun 12 20:01:57 2026 UTC
Number of results: 2

Port Summary for Host 193.42.15.27
----------------------------------

Service (Port)          Threat Level
135/tcp                 Medium
(CVSS: 5.0)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host
193.42.15.27
-----------------------------------
-

Issue
-----
NVT:    DCE/RPC and MSRPC Services
Enumeration Reporting
OID:    1.3.6.1.4.1.25623.1.0.10736
Threat: Medium (CVSS: 5.0)
Port:   135/tcp

Summary:
Distributed Computing Environment /
Remote Procedure Calls
  (DCE/RPC) or MSRPC based service
enumeration reporting.

Vulnerability Detection Result:
Here is the list of DCE/RPC or MSRPC
services running on this host via
the TCP p!
rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-
0123456789ac, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49664]
     Named pipe : lsass
     Win32 service or process :
lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-
1ac9557a1018, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-
9ef9a191fe1b, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-
8ca7272a0e86, version 2
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-
2c84da1ddb0d, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-
b89e2018337c, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-
09ad57031823, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49667]
     UUID: 86d35949-83c9-4044-b424-
db363231fd0c, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-
942b1eca65d1, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49668]
     UUID: 12345678-1234-abcd-ef00-
0123456789ab, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49668]
     Named pipe : spoolss
     Win32 service or process :
spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-
7f4093a94978, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-
64950a001209, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49668]
     UUID: ae33069b-a2a8-46ee-a235-
ddfd339be281, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49668]
Port: 49669/tcp
     UUID: 367abb81-9844-35f1-ad32-
98f038001003, version 2
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49669]
Port: 49670/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-
a4079be4fe48, version 1
     Endpoint:
ncacn_ip_tcp:193.42.15.27[49670]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services
running on this host locally were
identified. Re!
porting this list is not enabled by
default due to the possible large
size of th!
is list. See the script preferences
to enable this reporting.

Impact:
An attacker may use this information
to gain more knowledge about
  the remote host and to conduct
further attacks based on it.

Solution:
Solution type: Mitigation
Filter incoming traffic to this
ports.

Affected Software/OS:
All systems exposing / disclosing
information via DCE/RPC or
  MSRPC services.

Vulnerability Insight:
DCE/RPC or MSRPC services running on
the remote host can be
  enumerated by connecting on port
135 and doing the appropriate
queries.

Vulnerability Detection Method:
Reports previously collected (via
'DCE/RPC and MSRPC Services
  Enumeration' OID:
1.3.6.1.4.1.25623.1.0.108044)
DCE/RPC or MSRPC services.
  This VT is reporting a severity by
default. If the scanned network is
e.g. a p!
rivate LAN / private
  WAN which contains systems not
accessible to the public (access
restricted) an!
d it is accepted
  that the service is disclosing
information to this network please
set the 'Net!
work type'
  configuration of the following VT
to e.g. 'Private LAN' or 'Private
WAN':
  Global variable settings (OID:
1.3.6.1.4.1.25623.1.0.12288)
  In this case a 'Log' level result
is used instead.
Details:
DCE/RPC and MSRPC Services
Enumeration Reporting
(OID: 1.3.6.1.4.1.25623.1.0.10736)
Version used: 2025-11-26T05:40:08Z


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658


Host 193.42.15.254
*****************

Scanning of this host started at:
Fri Jun 12 20:11:00 2026 UTC
Number of results: 4

Port Summary for Host 193.42.15.254
-----------------------------------

Service (Port)          Threat Level
```

```
22/tcp                  Medium
(CVSS: 5.3)
general/icmp            Low (CVSS:
2.1)

Security Issues for Host
193.42.15.254
------------------------------------
--

Issue
-----
NVT:    Weak Key Exchange (KEX)
Algorithm(s) Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.150713
Threat: Medium (CVSS: 5.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak key
  exchange (KEX) algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak KEX algorithm(s):
KEX algorithm                      |
Reason
------------------------------------
------------------------------------
--------!
-----------
diffie-hellman-group-exchange-sha1 |
Using SHA-1
diffie-hellman-group1-sha1         |
Using Oakley Group 2 (a 1024-bit
MODP group!
) and SHA-1

Impact:
An attacker can quickly break
individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX
algorithm(s)
  - 1024-bit MODP group / prime KEX
algorithms:
  Alternatively use elliptic-curve
Diffie-Hellmann in general, e.g.
Curve 25519.

Vulnerability Insight:
- 1024-bit MODP group / prime KEX
algorithms:
  Millions of HTTPS, SSH, and VPN
servers all use the same prime
numbers for Dif!
fie-Hellman key
  exchange. Practitioners believed
this was safe as long as new key
exchange mes!
sages were generated
  for every connection. However, the
first step in the number field
sieve-the mo!
st efficient
  algorithm for breaking a Diffie-
Hellman connection-is dependent only
on this p!
rime.
  A nation-state can break a 1024-
bit prime.

Vulnerability Detection Method:
Checks the supported KEX algorithms
of the remote SSH server.
  Currently weak KEX algorithms are
defined as the following:
  - non-elliptic-curve Diffie-
Hellmann (DH) KEX algorithms with
1024-bit MODP gr!
oup / prime
  - ephemerally generated key
exchange groups uses SHA-1
  - using RSA 1024-bit modulus key
Details:
Weak Key Exchange (KEX) Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.150713)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url:
https://weakdh.org/sysadmin.html
 url: https://www.rfc-
editor.org/rfc/rfc9142
 url: https://www.rfc-
editor.org/rfc/rfc9142#name-summary-
guidance-for-implem
 url: https://www.rfc-
editor.org/rfc/rfc6194
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.5


Issue
-----
NVT:    Weak Encryption Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105611
Threat: Medium (CVSS: 4.3)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak
  encryption algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
The remote SSH server supports the
following weak server-to-client
encryption al!
gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption
algorithm(s).

Vulnerability Insight:
- The 'arcfour' cipher is the
Arcfour stream cipher with 128-bit
  keys. The Arcfour cipher is
believed to be compatible with the
RC4 cipher [SCH!
NEIER]. Arcfour
  (and RC4) has problems with weak
keys, and should not be used
anymore.
  - The 'none' algorithm specifies
that no encryption is to be done.
Note that t!
his method provides
  no confidentiality protection, and
it is NOT RECOMMENDED to use it.
  - A vulnerability exists in SSH
messages that employ CBC mode that
may allow a!
n attacker to
  recover plaintext from a block of
ciphertext.

Vulnerability Detection Method:
Checks the supported encryption
algorithms (client-to-server
  and server-to-client) of the
remote SSH server.
  Currently weak encryption
algorithms are defined as the
following:
  - Arcfour (RC4) cipher based
algorithms
  - 'none' algorithm
  - CBC mode cipher based algorithms
Details:
Weak Encryption Algorithm(s)
Supported (SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc8758
 url:
https://www.kb.cert.org/vuls/id/9585
63
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.3


Issue
-----
NVT:    Weak MAC Algorithm(s)
Supported (SSH)
OID:    1.3.6.1.4.1.25623.1.0.105610
Threat: Low (CVSS: 2.6)
Port:   22/tcp

Product detection result:
cpe:/a:ietf:secure_shell_protocol
Detected by: SSH Protocol Algorithms
Supported (OID:
1.3.6.1.4.1.25623.1.0.105565)

Summary:
The remote SSH server is configured
to allow / support weak MAC
  algorithm(s).

Vulnerability Detection Result:
The remote SSH server supports the
following weak client-to-server MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the
following weak server-to-client MAC
algorithm!
(s):
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the reported weak MAC
algorithm(s).

Vulnerability Detection Method:
Checks the supported MAC algorithms
(client-to-server and
```

```
  server-to-client) of the remote
SSH server.
  Currently weak MAC algorithms are
defined as the following:
  - MD5 based algorithms
  - 96-bit based algorithms
  - 64-bit based algorithms
  - 'none' algorithm
Details:
Weak MAC Algorithm(s) Supported
(SSH)
(OID: 1.3.6.1.4.1.25623.1.0.105610)
Version used: 2024-06-14T05:05:48Z

Product Detection Result:
Product:cpe:/a:ietf:secure_shell_pro
tocol

Method:SSH Protocol Algorithms
Supported
(OID: 1.3.6.1.4.1.25623.1.0.105565)

References:
 url: https://www.rfc-
editor.org/rfc/rfc6668
 url: https://www.rfc-
editor.org/rfc/rfc4253#section-6.4


Issue
-----
NVT:    ICMP Timestamp Reply
Information Disclosure
OID:    1.3.6.1.4.1.25623.1.0.103190
Threat: Low (CVSS: 2.1)
Port:   general/icmp

Summary:
The remote host responded to an ICMP
timestamp request.

Vulnerability Detection Result:
The following response / ICMP packet
has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact:
This information could theoretically
be used to exploit weak
  time-based random number
generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
  - Disable the support for ICMP
timestamp on the remote host
completely
  - Protect the remote host by a
firewall, and block ICMP packets
passing throug!
h the firewall in
  either direction (either
completely or only for untrusted
networks)

Vulnerability Insight:
The Timestamp Reply is an ICMP
message which replies to a
  Timestamp message. It consists of
the originating timestamp sent by
the sender!
 of the Timestamp as
  well as a receive timestamp and a
transmit timestamp.

Vulnerability Detection Method:
Sends an ICMP Timestamp (Type 13)
request and checks if a
  Timestamp Reply (Type 14) is
received.
Details:
ICMP Timestamp Reply Information
Disclosure
(OID: 1.3.6.1.4.1.25623.1.0.103190)
Version used: 2025-01-21T05:37:33Z

References:
 cve: CVE-1999-0524
 url:
https://datatracker.ietf.org/doc/htm
l/rfc792
 url:
https://datatracker.ietf.org/doc/htm
l/rfc2780
 cert-bund: CB-K15/1514
 cert-bund: CB-K14/0632
 dfn-cert: DFN-CERT-2014-0658
```