

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

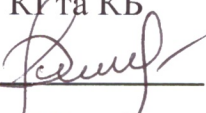
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту підсистеми
моніторингу мережної інфраструктури»

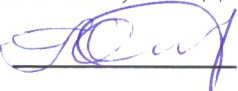
Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»

 Б.О. Яворенко

Керівник ст. викладач кафедри КІ та КБ

 Є.М. Трокоз

Рецензент доцент кафедри КІ та КБ, к.пед.н.

 О.С. Головня

Житомир – 2023

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 Сфіменко

13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Яворенко Богдан Олександрович

Тема роботи: «Методи та технології захисту підсистеми моніторингу мережної інфраструктури»

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 11 грудня 2023 р.

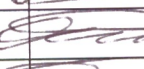
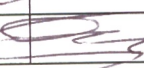
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Захист системи моніторингу
2. Протоколи SNMP, NetFlow та IPFIX

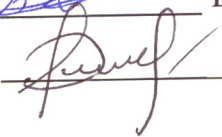
Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 3995 та Cisco 3660
2. Комутатор Cisco 2960
3. Операційні системи Windows 7, Kali Linux, Cisco IOS
4. Топологія мережі

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

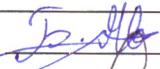
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 15.10.2023	 15.10.2023
2	Єфіменко А.А.	 14.11.2023	 14.11.2023
3	Єфіменко А.А.	 02.12.2023	 02.12.2023

Студент  Б.О. Яворенко

Керівник  Є.М. Трокоз

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	14 жовтня 2022	Виконано
2	Пошук інформації щодо реалізації системи моніторингу	15 жовтня 2022 – 19 жовтня 2022	Виконано
3	Аналіз технологій захисту систем моніторингу	22 жовтня 2022 – 25 жовтня 2022	Виконано
4	Проектування загальної топології	26 жовтня 2022 – 30 жовтня 2022	Виконано
5	Розробка IP-адресації та вибір обладнання	02 листопада 2022 – 06 листопада 2022	Виконано
6	Налаштування пристроїв мережі	09 листопада 2023 – 14 листопада 2023	Виконано
7	Тестування налаштованої мережі на проникнення	15 листопада 2023 – 17 листопада 2023	Виконано
8	Налаштування засобів захисту підсистеми моніторингу	19 листопада 2023 – 25 листопада 2023	Виконано
9	Перевірка закритих вразливостей	27 листопада 2023 – 01 грудня 2023	Виконано
10	Написання пояснювальної записки	02 грудня 2023 – 09 грудня 2023	Виконано
11	Підготовка додаткових матеріалів	10 грудня 2023 – 11 грудня 2023	Виконано
12	Отримання відгуку та рецензії на кваліфікаційну роботу	11 грудня 2023 – 12 грудня 2023	Виконано
13	Захист кваліфікаційної роботи	28 грудня 2023	Виконано

Студент  Б.О. Яворенко

Керівник  Є.М. Трокоз

АНОТАЦІЯ

Кваліфікаційна робота містить опис повного циклу проектування, розробки та налаштування проєкту підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколів SNMP, NetFlow та IPFIX. Пояснювальна записка складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 84 сторінках друкованого тексту. Пояснювальна записка має 3 сторінки додатків. Список використаних джерел містить 21 найменування і займає 2 сторінки. В роботі наведено 64 рисунки та 6 таблиць. Загальний обсяг роботи – 87 сторінок.

Метою роботи є дослідження методів та технологій захисту розробленого проєкту підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколів SNMP, NetFlow та IPFIX.

У роботі проаналізовано прикладні реалізації використання протоколів моніторингу мережі, порівняно варіанти реалізації моніторингу за допомогою додатків на базі ОС Windows та Linux. Спроектовано загальну топологію мережі та проекти локальних ділянок, розроблено схему адресації всіх пристроїв мережі з урахуванням можливості розширення, здійснено вибір відповідного проєкту топології обладнання мережі. Побудовано модель загроз мережі організації. Налаштовано мережу у відповідності до проєкту та перевірено правильність функціонування налаштованих протоколів. Проведено тестування на проникнення та реалізовано атаки відповідно до виявлених проблем безпеки, після чого налаштовано засоби захисту від атак на протоколи та механізми мережі.

Ключові слова: МЕРЕЖА, ЗАХИСТ ТРАФІКУ, МЕНЕДЖЕР, АГЕНТ, СЕРВЕР, КЛІЄНТ, МОНІТОРИНГ, ПРОТОКОЛ, КОРИСТУВАЧ, АТАКА, ПРОНИКНЕННЯ, ТЕСТУВАННЯ, SNMP, NETFLOW, IPFIX, СЕНСОР, АНАЛІЗАТОР, КОЛЕКТОР, ЗАГРОЗА, РЯДОК СПІЛЬНОТИ, ШИФРУВАННЯ.

ANNOTATION

The qualification work comprises a description of the entire cycle of designing, developing, and configuring the project subsystem for the protection of the monitoring system of the network infrastructure based on SNMP, NetFlow, and IPFIX protocols. The explanatory note consists of an introduction, three chapters, conclusions, a list of used literature, and appendices. The textual part is presented in 84 pages of printed text, and the explanatory note includes 3 pages of appendices. The list of used sources contains 21 items and spans 2 pages. The work includes 64 figures and 6 tables. The total volume of the work is 87 pages.

The aim of the work is to explore methods and technologies for protecting the developed subsystem project for the protection of the monitoring system of the network infrastructure built on SNMP, NetFlow, and IPFIX protocols.

The paper analyzes practical implementations of using network monitoring protocols, compares implementation options for monitoring using applications on Windows and Linux operating systems. The general network topology and local area projects are designed, addressing schemes for all network devices are developed considering expansion possibilities. The selection of the appropriate topology project for network equipment is made. A model of threats to the organization's network is constructed. The network is configured according to the project, and the correctness of the functioning of the configured protocols is verified. Penetration testing is conducted, and attacks are implemented based on identified security issues. Subsequently, security measures against attacks on network protocols and mechanisms are configured.

Keywords: NETWORK, TRAFFIC PROTECTION, MANAGER, AGENT, SERVER, CLIENT, MONITORING, PROTOCOL, USER, ATTACK, PENETRATION, TESTING, SNMP, NETFLOW, IPFIX, SENSOR, ANALYZER, COLLECTOR, THREAT, COMMUNITY STRING, ENCRYPTION.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	10
1.1 Принципи побудови та функціонування протоколів моніторингу.....	10
1.2 Застосування протоколів SNMP, Netflow та IPFIX для моніторингу пристроїв мережної інфраструктури.....	20
1.3 Проблеми безпеки протоколів моніторингу.....	27
1.4 Застосування протоколів моніторингу мережі для побудови систем кіберзахисту.....	34
Висновки до першого розділу.....	38
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КМ НА БАЗІ ПРОТОКОЛІВ SNMP, NETFLOW І IPFIX ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ.....	39
2.1 Проектування підсистеми моніторингу вразливостей та комп'ютерної мережі.....	39
2.2 Аналіз загроз підсистеми моніторингу.....	45
2.3 Побудова моделі загроз підсистеми моніторингу.....	50
Висновки до другого розділу.....	51
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІДСИСТЕМИ МОНІТОРИНГУ КМ.....	52
3.1 Налагодження КМ та підсистеми моніторингу.....	52
3.2 Дослідження рівня захищеності підсистеми моніторингу.....	71
3.3 Налагодження засобів захисту та дослідження стійкості системи моніторингу.....	76
Висновки до третього розділу.....	81
ВИСНОВКИ.....	82
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	83
ДОДАТКИ.....	85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система
ПЗ – програмне забезпечення
ІКС – інформаційно-комунікаційна система
ПК – персональний комп'ютер
IP – Internet Protocol
EIGRP – Enhanced Interior Gateway Protocol
DUAL – Diffusing Update Algorithm
DHCP – Dynamic Host Configuration Protocol
HTTP – HyperText Transfer Protocol
DNS – Domain Name System
AAA – Authentication, Authorization, Accounting
SNMP – Simple Network Management Protocol
OID – Object identifier
MIB – management information base
NMS – Network management system
SSH – Secure Shell
UDP – User Datagram Protocol
TCP – Transmission Control Protocol
IPFIX – IP Flow Information Export
IOS – Internetwork Operating System
ICMP – Internet Control Message Protocol

ВСТУП

Актуальність теми. У сучасному світі майже всі процеси перейшли у віртуальний простір. Доступність мережних рішень суттєво полегшила щоденні завдання великого бізнесу, а Інформаційно-комунікаційні системи (ІКС) стали основою для функціонування різних корпорацій. Таким чином, завдання створення універсальних мереж, які можуть однаково ефективно надавати послуги різних типів і при цьому бути максимально захищеними, стає все більш актуальним кожен день. Також не менш важливою є можливість моніторингу мережі, оскільки це дозволяє зменшити ризики перебоїв у роботі мережі.

Метою кваліфікаційної роботи є дослідження методів захисту спроектованої та розробленої підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколів SNMP, NetFlow та IPFIX.

Визначена мета обумовлює наступні завдання:

- аналіз та дослідження технологій моніторингу та їх захисту;
- розробка проекту системи захисту підсистеми моніторингу;
- налаштування та тестування спроектованої мережі в емуляторі;
- тестування стійкості до загроз та налаштування засобів захисту.

Об'єктом дослідження є процес аналізу технологій захисту побудованої підсистеми моніторингу мережної інфраструктури.

Предметом дослідження є протоколи SNMP, NetFlow та IPFIX, їх питання безпеки та питання застосування протоколів моніторингу у мережах малого та середнього розмірів, а також можливості поточних протоколів для проведення процедур моніторингу мережних пристроїв та мережних вузлів.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту системи моніторингу мережної інфраструктури на базі протоколів моніторингу SNMP, NetFlow та IPFIX, досліджено їх можливості, запропоновано та реалізовано безпекові рішення, а також протестовано стійкість системи до атак.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Принципи побудови та функціонування протоколів моніторингу

В сучасному світі для моніторингу даних комп'ютерних мереж розумно використовувати легкі, багатофункціональні протоколи. Важливо дотримуватися правил сумісності при виборі компонентів і забезпечити їх взаємодоповнення. Серед різноманітних протоколів, що широко використовуються для подібних завдань, можна виділити SNMP, Netflow та IPFIX.

Simple Network Management Protocol (SNMP) - це протокол на прикладному рівні, призначений для обміну даними між мережевими пристроями [1]. Це стандартний інтернет-протокол для управління пристроями в IP-мережах, що базується на архітектурі TCP/UDP. SNMP дозволяє відстежувати стан керованих мережеских пристроїв, таких як маршрутизатори, комутатори, сервери, принтери та інші пристрої, що підключені до IP через єдину систему управління/програмне забезпечення. SNMP - це не конкретний продукт, а набір правил, визначений Радою з архітектури Інтернету та пакетом TCP/IP. Інженерна група Інтернету (IETF) відповідає за його розробку та підтримку.

Спочатку протокол був створений для забезпечення системних адміністраторів інструментом для управління мережею Інтернет. Проте гнучка архітектура SNMP дозволила розширити його застосування на моніторинг всіх мережеских пристроїв та їх управління з одного інтерфейсу. Це спричинило широке поширення протоколу, який дозволяє системному адміністратору моніторити, контролювати продуктивність мережі та змінювати конфігурацію підключених пристроїв. Використовується в мережах будь-якого розміру, SNMP відзначається здатністю переглядати, контролювати та керувати вузлами через один інтерфейс з функціями пакетних команд та автоматичного сповіщення. SNMP визначається та підтримується Інженерною групою Інтернету (IETF) і пройшов три ітерації, при цьому друга версія (SNMPv2c) залишається найбільш поширеною протягом історії протоколу.

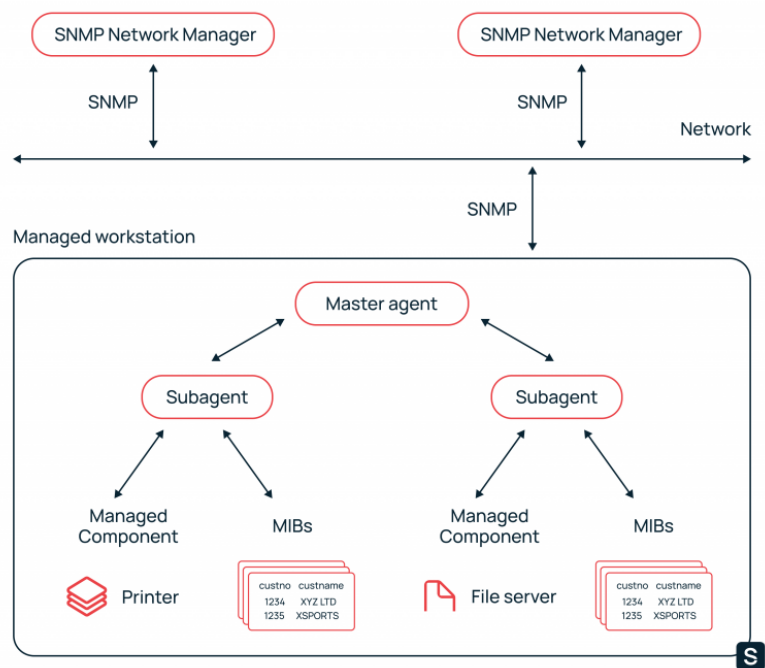


Рисунок 1.1 – Схема функціонування протоколу SNMP

Протокол SNMP функціонує на базі трьох основних компонентів:

- Мережева станція управління, що включає мережевого менеджера
- Агенти
- Керовані компоненти

Кожен з компонентів системи грає важливу роль у функціонуванні системи та виконує відповідний функціонал [4]. Важливим є описати кожен з них:

Network Management Station (NMS) - це консоль системи, NMS віддалено моніторить керовані пристрої, отримує дані, зібрані майстер-агентами, відстежує продуктивність і представляє отриману інформацію у графічному вигляді. Вбудований менеджер NMS відповідає за зв'язок із агентами.

Агент SNMP приймає запити від диспетчера SNMP та передає йому відповіді. Крім того, агент SNMP здійснює обмін даними з усіма субагентами DPI2 та вузлами SMUX у системі. Агент SNMP керує певними змінними MIB, і всі субагенти DPI2 та вузли SMUX реєструють свої змінні MIB на агенті SNMP. Виділяються два типи агентів:

- Майстер-агент
- Субагент

Майстер-агент – це програма, що з'єднує мережевих менеджерів та субагентів. Майстер-агент аналізує отримані запити від мережевого менеджера NMS і пересилає їх субагентам, отримує інформацію, створює відповіді і відправляє їх менеджеру. Майстер-агент повідомляє менеджера, якщо запит є некоректним, неправильно сформульованим або інформація, яку він запитує, недоступна.

Субагент – це програма, яка постачається вендором разом із мережевим пристроєм і використовується в конкретній базі інформації, якою управляє (MIB). Субагент збирає інформацію для майстер-агента, налаштовує параметри майстер-агента та відповідає на запити менеджера. Кожен керований компонент має відповідний субагент.

Керований компонент представляє собою пристрої, що підключені до мережі комп'ютерів або програмне забезпечення з вбудованим субагентом. Це можуть бути не лише маршрутизатори, комутатори, та сервери, але й пристрої, такі як IP-відеокамери, багатофункціональні принтери та IP-телефони. До програмного забезпечення з субагентами відносяться антивірусні програми, системи резервного копіювання, та програми для управління базами даних.

SNMP також включає базу управлінської інформації (MIB) та ідентифікатор об'єкта (OID). MIB представляє собою базу даних, яка містить інформацію про стан керованого пристрою, доступну для систем управління. Кожен тип пристрою має свою власну MIB-таблицю, і завдяки MIB, менеджер може знати, яку інформацію може запитати у субагента пристрою. OID, або ідентифікатор об'єкта, є унікальним ідентифікатором, який дозволяє ідентифікувати конкретний пристрій. OID подібний цифровому шляху до файлу, а його частина містить дані про виробника обладнання, що полегшує отримання інформації про пристрій.

Менеджери та агенти обмінюються даними за допомогою протоколу UDP. Зазвичай SNMP використовує порти UDP 161 і 162. Менеджер надсилає запити на порт 161 агента, і агент відправляє відповіді на цей самий порт. У процесі взаємодії запиту менеджера додається ідентифікатор (ID), який агент включає в свою відповідь, щоб менеджер міг пов'язати запит із відповіддю агента.

Агент надсилає пастки на порт 162 менеджерам. Використовуючи DLTs або TLS, агент може відправляти повідомлення на порт 10162, а менеджер – на порт 10161. Адміністратор може змінювати порти SNMP за замовчуванням на будь-які інші за потребою.

МІВ – це ієрархічна база даних із відомостями про пристрій. У кожного типу пристрою своя МІВ-таблиця: у принтера міститься інформація про стан картриджів, а у комутатора - дані про трафік. Завдяки МІВ менеджер знає, яку інформацію може запросити у агента пристрою.

Кожен об'єкт у MIB має свій унікальний ID-OID, який представлений у числовому форматі та має ієрархічну структуру. OID – це числовий еквівалент шляху до файлу. Він надає значення кожної таблиці в MIB, кожному стовпцю в таблиці та кожному значенню в стовпці.

Наприклад, OID 1.3.6.1.4.868.2.4.1.1.1.3.3562.3. означає iso.org.dod.internet.private.transition.products.chassis.card.slotCps.cpsSlotSummary.cpsModuleTable.cpsModuleEntry.cpsModuleModel.3562.3.

Використовуючи перші 6 цифр цього OID, можна пройти дерево на схемі.

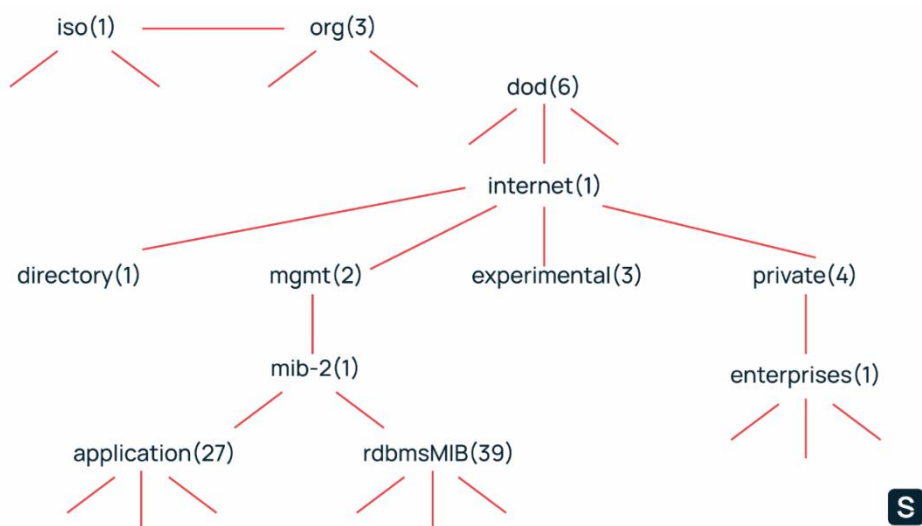


Рисунок 1.2 – Схематичне представлення дерева OID

Частина значень OID містить дані про виробника пристрою, що дозволяє швидко отримати певну інформацію про девайс.

Деревоподібна ієрархія MIB і OID у SNMP виглядає дещо заплутаною, але має свої переваги. Це проста та гнучка система організації мережевих пристроїв, вона працює незалежно від розміру мережі.

Унікальною особливістю протоколу SNMP є використання спеціальних пакетів – пасток. Пастка (Trap) – це найважливіший спосіб комунікації у SNMP. Менеджер відповідає за багато пристроїв, на багатьох з них може бути кілька керованих компонентів. Агент відправляє пастку з власної ініціативи, коли потрібно повідомити менеджера про подію. Наприклад, пастка може надіслати звіт про перегрівання машини або про те, що в тонері закінчилося чорнило.

Отримавши повідомлення, менеджер вибирає потрібну дію, наприклад, опитує агента, щоб отримати повне уявлення про те, що сталося. Перелік повідомлень, які надсилає пастка:

- 0 – coldStart – Холодний запуск пристрою.
- 1 - warmStart - Гарячий запуск пристрою.
- 2 - linkDown - Інтерфейс відключився.
- 3 - linkUp - Інтерфейс увімкнувся.
- 4 — authenticationFailure — Менеджер надіслав повідомлення з неправильним рядком спільноти.
- 5 - egpNeighborLoss - Агент втратив зв'язок з хостом за протоколом Exterior Gateway Protocol (EGP).
- 6 - enterpriseSpecific - Сталася подія, характерна для виробника цього пристрою.

SNMP має два варіанти пасток: Trap та Inform. Trap та Inform представляють собою автоматичні дії керованого пристрою. Коли виникає умова, яка спричиняє пастку, керований пристрій відправляє Trap до системи управління мережею (NMS) для сповіщення. Inform аналогічний Trap, але для Inform потрібно отримати підтвердження від NMS, в той час як Trap може відсилатися без підтвердження. У випадку, якщо керований пристрій не отримує підтвердження, він зберігає Inform у буфері або повторює процес, доки NMS не підтвердить отримання. Якщо кіль-

кість повторних відправлень досягає максимального ліміту, керований пристрій реєструє інформацію про це в журналі для подальшого запиту на повідомлення. У випадку, якщо повідомлення не досягло менеджера, агент не отримає про це повідомлення.

NetFlow - це протокол, розроблений компанією Cisco Systems, також відомий як стандарт IPFIX - компонент Cisco IOS. Протокол NetFlow працює на IP-пристроях (маршрутизаторах, комутаторах 3-го рівня) і забезпечує статистику IP-трафіку. Кілька виробників впровадили цей стандарт (наприклад, Juniper випустила аналогічне рішення під назвою jFlow). Інші компанії (наприклад, HP, Foundry і Extreme) використовують технологію контролю потоку даних sFlow.

Незважаючи на свою назву, NetFlow охоплює значний обсяг даних і є багатим джерелом інформації, що оновлюється в режимі реального часу; ця інформація доступна в будь-який момент і містить безліч параметрів щодо трафіку даних у мережі.

Система візуалізує не лише параметри TCP/IP на 3-му і 4-му рівнях (IP-адреса джерела та призначення, протокол, порт), але й додаткові атрибути трафіку (Type of Service, DSCP, ідентифікатор джерела та призначення в протоколі BGP) та додаткову інформацію про маршрутизацію і трафік - наступний транзитний вузол, вхідні та вихідні інтерфейси, мережева адреса джерела та призначення.

Як і будь-яке інше рішення протокол NetFlow має як переваги, так і певні недоліки. Технологія NetFlow дозволяє виявляти проблеми, узкі місця в мережі, перевіряти налаштування класів трафіку (CoS/ToS), визначати відправлений трафік та додатки, а також дозволяє прив'язувати його до конкретного користувача в певний період часу. Більше того, як технологія, інтегрована в Cisco IOS, NetFlow не вимагає використання додаткових пристроїв або придбання ліцензій. Більшість платформ Cisco, починаючи від маршрутизаторів Cisco ISR, сумісні з NetFlow.

За допомогою NetFlow можна створити відносно недорогу та просту систему моніторингу мережевого трафіку.

Однак, без відповідних інструментів для обробки зібраних даних, NetFlow не особливо корисний. Його вигода та роль в управлінні продуктивністю мережі залежать від способу отримання даних ІТ-спеціалістами. Зважаючи на обсяг доступної інформації, немає сенсу аналізувати дані з точки зору їхнього потоку від окремого елемента мережі. Для повноцінного використання протоколу NetFlow необхідно зібрати зовнішню базу даних та забезпечити інтуїтивний інтерфейс, який дозволить знаходити інформацію, яка нас цікавить, виявляти аномальну активність мережі, а також допоможе планувати розширення мережевої інфраструктури.

Система обробки інформації, зібраної за допомогою NetFlow, складається з наступних компонентів:

- Агент NetFlow
- Колектор NetFlow
- Модуль візуалізації

Агент NetFlow: Збирає дані про трафік, який проходить через мережеві пристрої, та відправляє їх до центрального сховища (так званий колектор). Фактично, будь-який маршрутизатор Cisco, на якому встановлено програмне забезпечення IOS (починаючи з версії 12.3T і вище, NetFlow доступний в функціоналі SP Services), може використовуватися як агент. Комутатори Catalyst 6500 також підтримують протокол NetFlow, а в комутаторі Catalyst 4500 він вбудований як додаткова функція.

Колектор NetFlow: Збирає інформацію від агентів. Зважаючи на великий обсяг даних, колектор зазвичай фільтрує, агрегує та видаляє дані перед їхнім занесенням до бази.

Модуль візуалізації: Використовується для подання даних, зібраних у колекторі NetFlow. Він підтримує ряд функцій, таких як забезпечення мережевого планування, співставлення користувачів або моніторинг трафіку.

За допомогою модуля візуалізації можна отримати наступну інформацію:

- Які застосунки використовуються? Чи є вони всі законними?
- Хто використовує ці застосунки?
- Які сервери є джерелами трафіку?

- Чи є вони дійсно серверами? До яких серверів йде трафік? Чи необхідно досягати ці сервери?
- Які застосунки створюють найбільше трафіку?
- Хто використовує увесь доступний пропускний здатність?
- Чи виконується тегування вхідного трафіку оператором належним чином?
- Які інтерфейси відображають найбільше навантаження?
- Які маршрутизатори відображають найбільше навантаження?

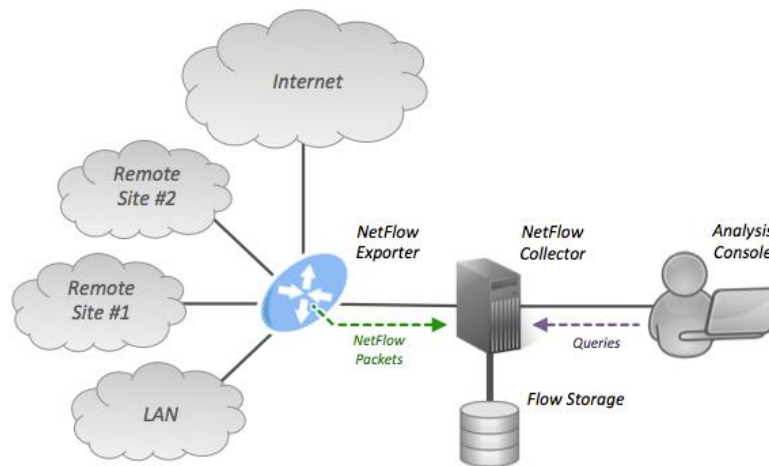


Рисунок 1.3 – Схема функціонування протоколу Netflow

Головна перевага NetFlow полягає в тому, що при правильному використанні можна створити відносно недорогу та просту систему моніторингу мережевого трафіку. Єдині витрати будуть пов'язані з придбанням додатка для візуалізації даних.

Крім того, за допомогою NetFlow можна моніторити будь-який канал у мережі. Оскільки налаштування NetFlow на маршрутизаторі виконується на програмному рівні, можна вибірково активувати його на пристроях моніторингу, а також на інших критичних пристроях (наприклад, концентраторі, маршрутизаторі, який забезпечує підключення до Інтернету або в місцях, де виникають проблеми в мережі).

Більше того, NetFlow - це відкритий протокол, тому він підтримує ряд сторонніх додатків для моніторингу мережі в режимі реального часу, створення звітів

та співставлення користувачів у мережі. Зазвичай додатки розробляються під індивідуального клієнта та конкретні вимоги.

Переваги використання системи на основі NetFlow:

- Підвищена безпека мережі: моніторинг мережевої активності є одним з ключових елементів забезпечення безпеки. За допомогою інтерфейсу візуалізації можна виконувати сканування портів, виявляти DoS-атаки та перемикання між IP-адресами.
- Можливість повного відображення мережевого трафіку та його джерела: дозволяє виявляти незаконні дії та уникати великих штрафів (наприклад, за використання неліцензійного ПЗ).
- Планування розвитку мережі: визначення моделей трафіку та адаптація до ширини каналу до досягнення максимальної пропускної здатності мережі (наприклад, виявлення серверів із неправильним розташуванням та їх переміщення для уникнення чрезмерного навантаження на глобальну мережу).
- Швидке вирішення проблем (наприклад, оптимізація налаштувань QoS для правильної пріоритизації важливих додатків, що забезпечує швидшу відповідь).
- Проста установка та конфігурація - впровадження на базовому рівні, при якому експортна конфігурація основного потоку займає один день.

IPFIX (Internet Protocol Flow Information eXport) фактично є розвитком протоколу NetFlow версії 9 від компанії Cisco Systems. Є частиною робочої групи IETF. Вона була створена внаслідок потреби в загальному, універсальному стандарті експорту даних про IP-потоки з маршрутизаторів, проб (зондів) та інших пристроїв, що використовуються системами контролю та обліку, а також системами управління мережею для керування різноманітними сервісами. Стандарт IPFIX повинен визначати, як інформація про IP-потоки має бути відформатована та передана від експортера до колектора. До цього часу більшість аналітичних та управляючих систем використовували для цього розроблений стандартом Cisco NetFlow або CFlow, розроблений компанією Juniper Networks. Вимоги до стандарту IPFIX наведено в

RFC 3917. Робоча група вибрала за основу для IPFIX стандарт NetFlow v9. Специфікацію протоколу IPFIX робоча група представила на розгляд у IESG для затвердження в 2006 році.

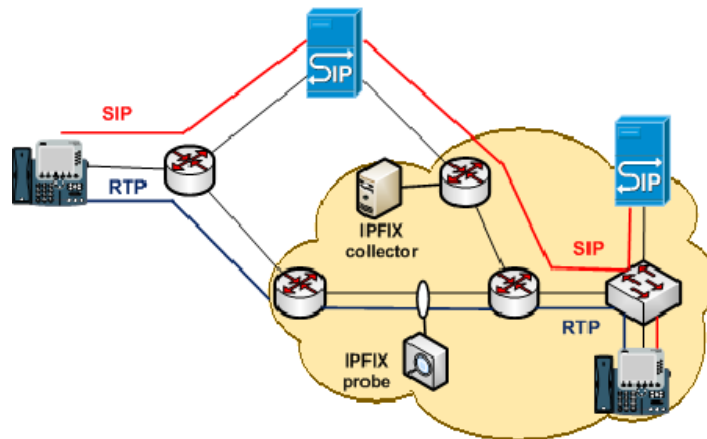


Рисунок 1.4 – Схема функціонування протоколу Netflow

Експортер (маршрутизатор, комутатор та інші) збирає пакети даних в точці спостереження, опціонально фільтрує їх та агрегує інформацію про ці пакети. Використовуючи протокол IPFIX, експортер висилає цю інформацію в колектор. Експортер та колектор працюють за принципом "багато-до-багатьох": один експортер може відправляти дані до багатьох колекторів, і один колектор може отримувати дані від багатьох експортерів.

Так само, як і протокол NetFlow, IPFIX розглядає потік як будь-яку кількість потоків, спостережуваних протягом певного інтервалу часу та мають ряд спільних властивостей, тобто "один джерело, один приймач, один протокол". Використовуючи IPFIX, пристрої типу маршрутизатора можуть повідомляти центральну систему моніторингу про характеристики потенційно великої мережі. IPFIX - це протокол "push", тобто кожен відправник періодично висилатиме повідомлення IPFIX до налаштованих отримувачів без будь-якої взаємодії з отримувачем.

Структура даних в повідомленнях IPFIX має достатньо великий розмір та можливості розширення для отримувача. Дані передаються отримувачеві за допомогою спеціальних шаблонів. Отримувач може використовувати визначені ним самим типи даних у цих повідомленнях, тому протокол легко розширюється та може бути адаптований до різних сценаріїв.

IPFIX віддає перевагу використанню протоколу Stream Control Transmission Protocol в якості транспортного протоколу, але також може використовувати протоколи Transmission Control Protocol (TCP) чи User Datagram Protocol (UDP).

1.2 Застосування протоколів SNMP, Netflow та IPFIX для моніторингу пристроїв мережної інфраструктури

Протокол простого керування мережею (SNMP) був створений для полегшення можливості моніторингу мережі, який мережеві адміністратори можуть використовувати для різних моделей пристроїв та отримують змогу виявлення різних аспектів продукту. Таку інформацію, як завантаження процесора, таблиці маршрутизації та статистику мережевого трафіку, серед багатьох інших, можна отримати віддалено за допомогою SNMP. Можна також використовувати SNMP для встановлення конфігурацій на пристроях, що підтримують його.

Зчитування в SNMP здійснюється за допомогою функції рядку community. Першочергове завдання адміністратора – налаштування такого рядку. Після підключення до пристрою потрібно "витягнути" його для моніторингу за допомогою OID.

Реалізуючи моніторингову систему з використанням протоколів NetFlow та IPFIX перед адміністратором стає головна задача – налаштування сенсора. Для цього на мережевому устаткуванні потрібно вказати IP-адреси колекторів та порти, на яку потрібно направляти трафік.

Для моніторингу пристроїв використовуються в основному робочі станції на базі ОС Windows та Linux з встановленим на нього програмним забезпеченням [5]. В сучасності існує досить багато таких реалізацій від різних розробників. Одними з найбільш популярних є:

- MRTG
- Cacti
- ManageEngine NetFlow Analyzer
- ntopng

– PRTG Network Monitor

Multi Router Traffic Grapher або MRTG є одним з найбільш давніх інструментів моніторингу за протолом SNMP. Він існує з 1995 року і все ще широко використовується в сучасності. Це абсолютно безкоштовна система із відкритим вихідним кодом. MRTG не найкрасивішим та найзручнішим, але, можливо, найгнучкішим. Окрім смуги пропускання MRTG може контролювати безліч параметрів. Фактично, він може відстежувати, реєструвати та відображати будь-які параметри SNMP.

Для встановлення MRTG необхідно спочатку встановити та налаштувати Perl. Після встановлення MRTG налаштовується шляхом редагування файлу конфігурації в старому стилі Linux. Адміністратори, які звикли до налаштування графічного інтерфейсу, можуть зіткнутися з певними проблемами на даному етапі.

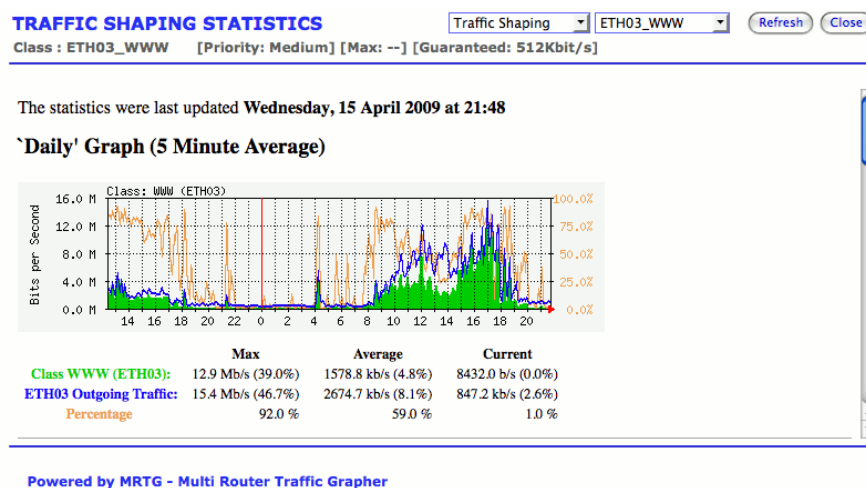


Рисунок 1.5 – Приклад моніторингу трафіку за допомогою ПЗ MRTG

Sacti вважається покращеною версією MRTG. Візуально та функціонально будь-який з графіків Sacti схожий з MRTG. Sacti створений на основі RRDTools, розробленої тим самим розробником і є прямим нащадком MRTG.

Sacti більш досконалий, ніж MRTG, з веб-інтерфейсом конфігурації, який дозволяє проводити налаштування простіше та інтуїтивніше. Це повний пакет моніторингу та побудови мережі. Інструмент забезпечений швидким опитуванням, розширеними шаблонами пристроїв та графіків, декількома методами збору даних

та функціями керування користувачами. Це чудово підходить для невеликих локальних мереж, але так само добре для складних мереж із тисячами пристроїв на кількох сайтах.

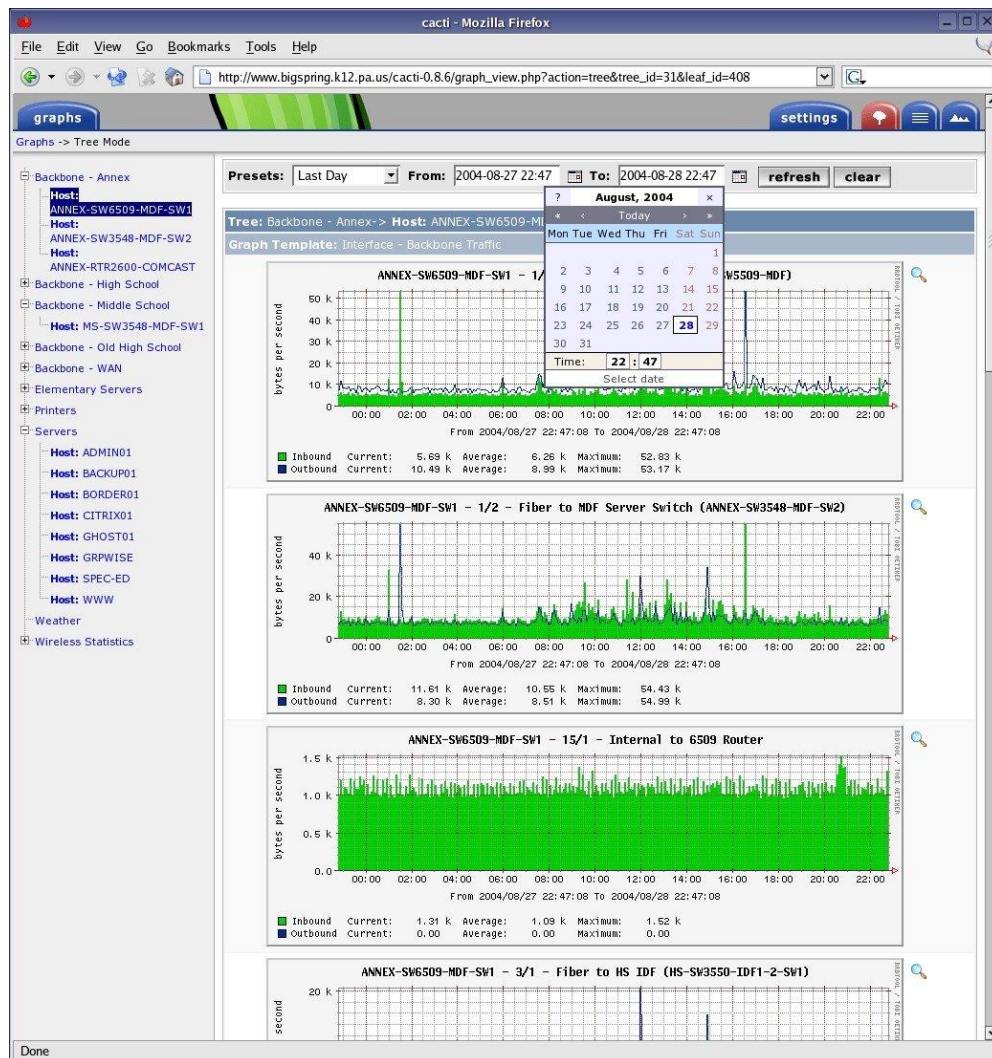


Рисунок 1.6 – Приклад моніторингу трафіку за допомогою ПЗ Cacti

Cacti створено на основі ПЗ RRDtool. За словами його розробника, «RRDtool – це галузевий стандарт OpenSource, високопродуктивна система реєстрації та відображення даних для тимчасових рядів. RRDtool може бути легко інтегрований у сценарії оболонки, програми Perl, Python, Ruby, Lua або Tcl». RRDtool є прямим нащадком MRTG. RRDTool є розвитком програмного додатку MRTG на С.

Підсумовуючи Cacti – це інтерфейс RRDTool. Він зберігає необхідні дані для створення графіків та заповнення їх даними у базі даних MySQL. Він повністю

написаний на мові програмування PHP. Програмне забезпечення підтримує свої графіки, джерела даних та циклічні архіви у базі даних, а також обробляє збір даних, залишаючи графіки для RRDTool. Багато користувачів Sacti є колишніми користувачами MRTG.

Сервіс ManageEngine пропонує колектор і аналізатор NetFlow, який за своєю функціональністю дуже схожий на рішення, описане вище. Це потужний програмний продукт із повним спектром можливостей для збору даних про потоки в вашій мережі та аналізу цієї інформації. ManageEngine NetFlow Analyzer підтримує різні технології для збору інформації про потоки, такі як NetFlow, J-Flow та NetStream, і призначений для аналізу мережевого трафіку, а також моніторингу пропускної здатності в реальному часі.

Крім того, ManageEngine NetFlow Analyzer має кілька цікавих можливостей, таких як:

- Налаштовувана панель моніторингу для виведення узагальнених даних по додатках, протоколах та використовуваних ресурсах;
- Вбудована система сповіщень при досягненні порогових значень;
- Підтримка звітів Cisco Medianet і Cisco WAAS.

ManageEngine пропонує онлайн-демонстрацію свого аналізатора NetFlow, що дозволить оцінити його можливості, перш ніж прийняти рішення про повнофункціональне використання. ManageEngine NetFlow Analyzer доступний у двох версіях: Essential (для малих, середніх і великих компаній) і Distributed (для корпорацій). Обидві версії можуть бути протестовані безкоштовно протягом 30 днів. Ціна версії Essential залежить від обраної функціональності та кількості інтерфейсів, які моніторяться. Також існує можливість використання безкоштовної версії рішення без необхідності в будь-якій ліцензії, яка може бути застосована для моніторингу не більше двох інтерфейсів.

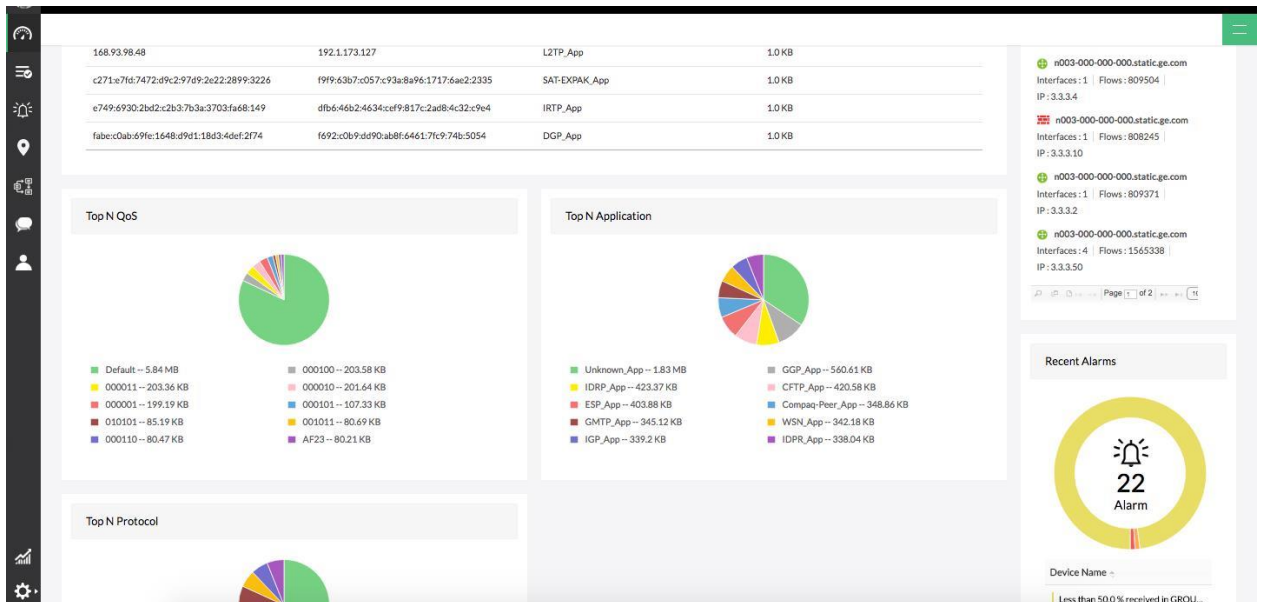


Рисунок 1.7 – Приклад моніторингу трафіку за допомогою
ПЗ ManageEngine NetFlow Analyzer

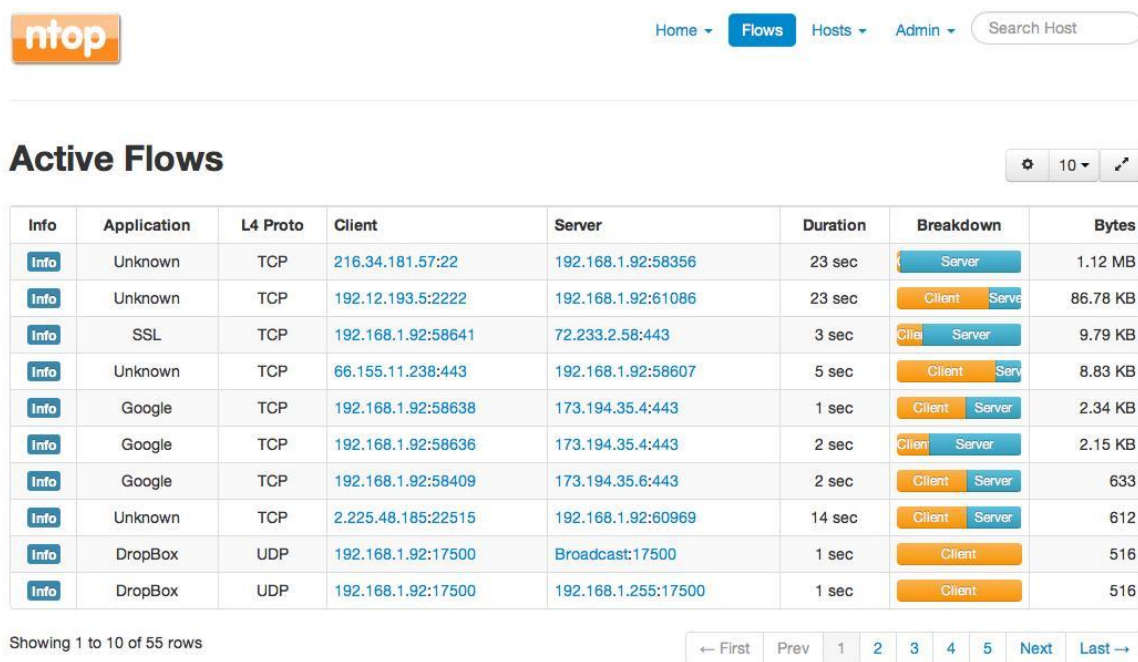
Рішення ntopng - це веб-інструмент з відкритим вихідним кодом для моніторингу та аналізу мережевого трафіку. Програма розроблена для використання на мобільних пристроях під управлінням будь-якої з популярних платформ: Unix, MacOS і Windows. Дані про передані пакети надходять через зашифрований інтерфейс. Програма аналізує їх і надає різноманітну корисну інформацію щодо функціонування вашої мережі. Наприклад, за допомогою ПЗ ntopng можна:

- сортувати інформацію про мережевий трафік за багатьма параметрами, включаючи IP-адреси, порти, протоколи, пропускну здатність і т. д.;
- в реальному часі відстежувати найактивніші хости і додатки, які потребують найбільше пропускну здатності;
- відстежувати інформацію про передані байти, а також кількість відправлених, отриманих і втрачених пакетів;
- зберігати на диск історію мережевого трафіку для подальшого аналізу;
- визначати географічне розташування та будувати схеми з'єднань хостів на карті місцевості.

Програма ntopng може підключатися до nProbe, який є колектором NetFlow/IPFIX. У цьому тандемі ролі розподілені наступним чином: nProbe збирає

дані про потоки та відправляє цю інформацію в ntopng, який, у свою чергу, аналізує її і подає у зручному для сприйняття вигляді.

Навіть якщо ntopng доступний у безкоштовній версії (також існують розширені платні версії продукту), для використання nProbe знадобиться ліцензія (за винятком некомерційних організацій або навчальних закладів). Програмне забезпечення nProbe постачається у двох версіях: Standard та Pro з плагінами.



Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	Server	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	Client Server	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	Client Server	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	Client Server	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	Client Server	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	Client Server	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	Client Server	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	Client Server	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	Client	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	Client	516

Рисунок 1.8 – Приклад моніторингу трафіку за допомогою ПЗ ntopng

PRTG Network Monitor - це універсальне програмне рішення для моніторингу мережі, яке включає в себе відслідковування продуктивності, контроль обмежень пропускної здатності, спостереження за роботою серверів, центральних процесорів, додатків, веб-сайтів, хмарних служб та багато іншого. Стандартна установка спочатку забезпечує усіма необхідними інструментами для моніторингу всього трафіку в вашій мережі. PRTG Network Monitor може використовувати різні версії стандарту NetFlow (v5 і v9), відкритий універсальний стандарт IPFIX, а також інші технології для обліку мережевого трафіку, такі як sFlow і J-Flow.

Однією з можливостей використання моніторингу NetFlow, доступною в PRTG Network Monitor, є розширений аналіз пропускної здатності. Звіти візуалізуються у вигляді рейтингових списків, що дозволяє відслідковувати дані за різними налаштовуваними категоріями, що значно полегшує вам завдання. Наприклад, можна відслідковувати і порівнювати одразу результати для різних IP-адрес, для з'єднань, для протоколів, для додатків і т. д. Це дуже корисно при усуненні неполадок в роботі мережі.

Як вже відзначалося вище, програмне забезпечення PRTG Network Monitor включає в себе NetFlow Collector, який працює автоматично на будь-якому локальному чи віддаленому комп'ютері із встановленим зондом PRTG. PRTG Network Monitor використовує зонди як платформу для моніторингу всієї мережевої інфраструктури. Всі об'єкти, сконфігуровані під конкретним зондом, будуть контролюватися через цей зонд.

Для ціноутворення компанії Paessler важливе значення в ієрархії об'єктів програмного забезпечення PRTG має поняття сенсора. На кожному пристрої (практично на будь-якому фізичному чи віртуальному пристрої в мережі, у якого є власний IP-адрес) можна створити кілька сенсорів. Кожен сенсор контролює один аспект роботи пристрою. Наприклад, це може бути:

- один пристрій NetFlow;
- один мережевий сервіс, такий як SMTP, FTP, HTTP і т. д.;
- трафік одного порта мережевого комутатора;
- завантаження центрального процесора пристрою;
- завантаження пам'яті пристрою;
- трафік на одній мережевій карті;
- загальний стан системи на пристрої;
- різноманітний вміст (наприклад, використання бази даних, електронної пошти, HTTP, XML, файлів і т. д.).

Програмне забезпечення PRTG Network Monitor доступне в двох версіях: комерційній та безкоштовній. Безкоштовна редакція - це повністю функціональне рішення PRTG Network Monitor, яке дозволяє контролювати до 100 сенсорів. Якщо потрібно використовувати моніторинг понад 100 сенсорів, може знадобитися вже комерційна ліцензія. Крім того, спочатку доступна безкоштовна пробна версія, яка протягом перших 30 днів не має жодних обмежень.

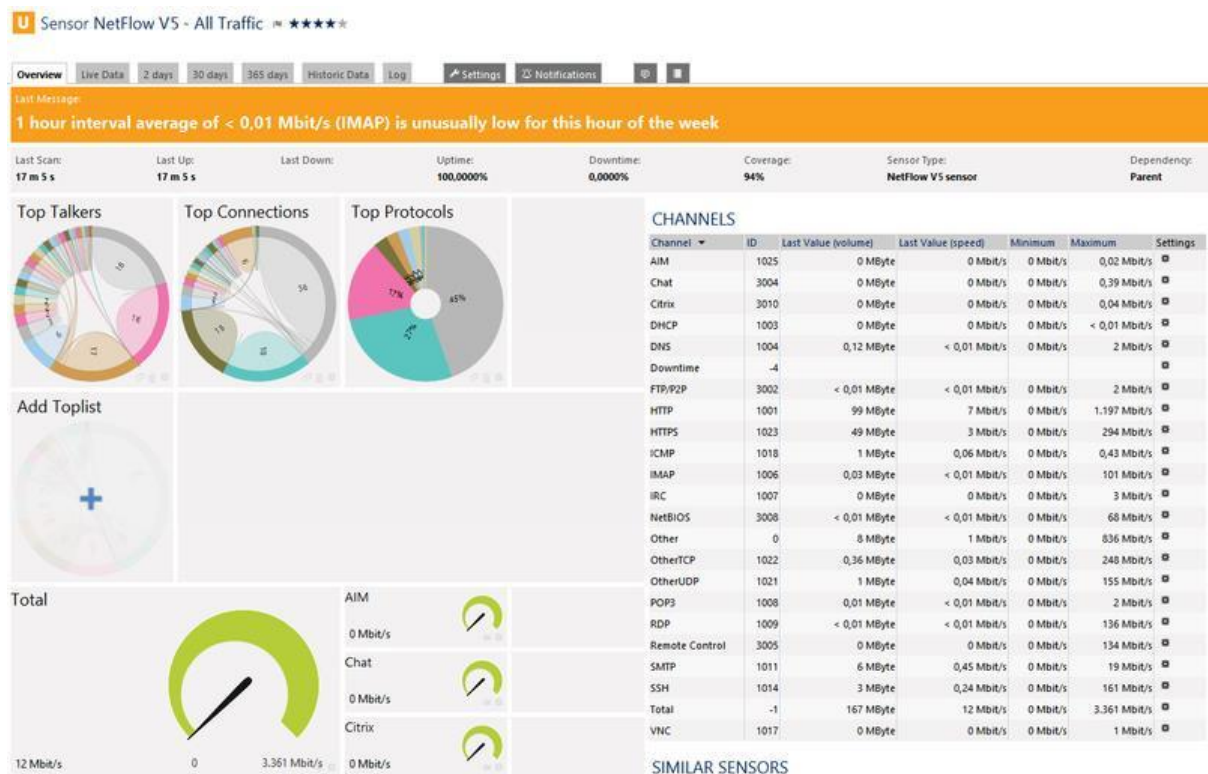


Рисунок 1.9 – Приклад моніторингу трафіку за допомогою ПЗ PRTG

1.3 Проблеми безпеки протоколів моніторингу

У даному дипломному проекті розглядається 3 основні протоколи моніторингу мережі: SNMP, NetFlow та IPFIX. Наразі немає відомих загальноприйнятих атак або вразливостей, які специфічно впливають на протоколи NetFlow та IPFIX. Однак, як і з будь-якими мережевими протоколами, існує кілька загальних видів атак, які можуть впливати на їх безпеку:

- Атака отруєння (Poisoning Attack): Атака, при якій атакуючий відправляє в мережу неправдиві або маніпульовані дані NetFlow або IPFIX, щоб спотворити відображення стану мережі або отримати неправильні дані про трафік.
- Атака на відмову в обслуговуванні (Denial of Service - DoS): Атака, яка полягає в переповненні каналів звіту NetFlow або IPFIX або завищенні навантаження, що може призвести до втрати даних та відмови в обслуговуванні.
- Атака на маскування (Spoofing Attack): Використання підроблених IP-адрес для відправки маніпульованих даних NetFlow або IPFIX, щоб приховати справжній джерела або спроби обману систем моніторингу.
- Перехоплення (Eavesdropping): Неправомірне перехоплення та аналіз даних NetFlow або IPFIX з метою здобуття конфіденційної інформації про трафік.
- Маніпулювання трафіком (Traffic Manipulation): Зміна або вилучення даних NetFlow або IPFIX для спотворення інформації про трафік або приховування зловживань.

Важливо відзначити, що безпека NetFlow та IPFIX в значній мірі залежить від правильного конфігурування та застосування заходів безпеки в мережі загалом. Захист мережі від різноманітних загроз включає в себе використання шифрування, аутентифікації, моніторингу та використання заходів безпеки на рівні інфраструктури.

Враховуючи описане вище, можна зробити висновок, що найбільш вразливим місцем підсистеми моніторингу є SNMP. На момент написання дипломного проекту існує 3 основні версії протоколу SNMP. Під час кожного з етапів еволюції версій було значно покращено захист протоколу. Важливим є детально розглянути проблеми безпеки кожної з версій [6].

Один із основних недоліків у SNMP v1 полягає у відсутності розширеної системи захисту даних, що відповідає масштабам підприємств. У SNMPv1 захист адміністративної інформації був розгляданий надто просто, використовуючи колективне ім'я (Community Name), яке, будучи включеним у заголовок SNMP, несло всі можливості захисту повідомлень. Цей метод, відомий як тривіальний протокол, передбачав, що програма-агент і менеджер повинні впізнати спільне колективне ім'я

перед продовженням мережевих адміністративних операцій. Часто це обмежувало адміністраторів у функціях крім моніторингу, забороняючи використання команди SET, яка може змінювати конфігураційні параметри віддаленого пристрою. Такий примітивний метод захисту, як колективне ім'я, спричинив уникання користувачами команд SET, які, в свою чергу, можуть змінювати параметри, необов'язково повідомляючи користувачів. Додатково, критична інформація передавалася у відкритому вигляді.

У зв'язку з цим, були внесені пропозиції щодо поліпшення захисту у рамках SNMPv1, які згодом стали основою захисту для SNMPv2. Протягом 1993 року було опубліковано 11 RFC, що визначали нові стандарти SNMP, з першим із них, RFC 1441, який вводив SNMP версії 2 (SNMPv2).

Стандарти захисту SNMPv2 включають методи аутентифікації (DAP – Digest Authentication Protocol) та забезпечення конфіденційності (SPP – Symmetric Privacy Protocol) для інформації адміністративного характеру. Основною концепцією є учасник (party) - унікальний набір параметрів захисту, який може включати розташування мережі, протоколи аутентифікації та забезпечення конфіденційності, що використовуються між агентом і менеджером.

SNMPv2 впроваджує новий тип пакетів get-bulk-request для ефективної обробки великих блоків даних. Також введено новий тип пакетів inform-request, який дозволяє одному менеджеру надсилати інформацію іншому менеджеру. Визначено два нових MIB: MIB SNMPv2 та MIB SNMPv2-M2M (менеджер-менеджер). SNMPv2 покращує секретність порівняно з SNMPv1, де ім'я спільноти передавалося відкритим паролем. SNMPv2 надає аутентифікацію та розширену секретність.

Незважаючи на ці поліпшення, SNMPv2 не отримала широкої підтримки виробників мережевого обладнання і не отримала значення. Однак в останні роки розробники стандартів IETF намагаються виправити ситуацію, пропонуючи специфікацію третьої версії SNMP. Вдосконалення протоколу, спрямоване на гнучке адміністрування агентів систем управління та захист керуючої інформації, разом із зворотною сумісністю із системами, що використовують базову версію SNMPv1,

та відкритою архітектурою, дозволяє розробникам SNMPv3 сподіватися на успішне практичне впровадження цієї версії.

Під час розробки SNMPv3 велика увага була приділена забезпеченню безпеки протоколу. У цій версії була впроваджена модель, орієнтована на користувача (User-Based Security Model, скорочено USM), що дозволяє додавати модулі аутентифікації і шифрування без внесення змін до базової архітектури. Модель USM включає модуль аутентифікації, модуль шифрування і модуль контролю часу. При цьому модуль аутентифікації і шифрування відповідають за захист даних, а модуль контролю часу синхронізує час між сутностями SNMP.

Основні проблеми, які було необхідно вирішити за допомогою моделі USM, включають:

- Можливість відкладання дій на невизначений час або повторення одних і тих же дій з довільними інтервалами;
- Зміна даних сутностями, які не пройшли аутентифікацію;
- Блокування обміну даними між сутностями;
- Перехоплення трафіку при передачі між сутностями;

Проблему було вирішено за допомогою трансформації паролю кожного мережевого пристрою в унікальний ключ. Це забезпечує додатковий захист, навіть якщо ключ буде перехоплено, зломисник матиме доступ тільки до одного мережевого пристрою. Для шифрування пароля використовується алгоритм MD5, але розробники вирішили, що це не забезпечить достатнього захисту, тому блок PDU двічі хешується за допомогою двох різних ключів, які генеруються з закритого ключа. Пізніше перші 12 октетів використовуються як код аутентифікації повідомлення, який додається до повідомлення. Той же процес проводиться на іншому боці, але тільки у зворотному порядку. Незважаючи на складність та енергоефективність процесу передачі даних між сутностями SNMP, розробники вважають, що алгоритм шифрування (DES) насправді не забезпечує достатнього захисту інформації, тому планується використовувати інші алгоритми в майбутньому.

Розробники передбачили три рівні безпеки для SNMPv3:

- noAuthNoPriv (Без аутентифікації та конфіденційності): Паролі передаються у відкритому вигляді, і конфіденційність даних відсутня.

- authNoPriv (Аутентифікація без конфіденційності): Здійснюється лише аутентифікація без шифрування. Більшість користувачів використовують цей рівень безпеки, оскільки він є досить високим, і мережеві пристрої не перевантажуються шифруванням даних.

- authPriv (Аутентифікація та конфіденційність): Максимальний рівень захисту, оскільки включає як аутентифікацію, так і шифрування.

Адміністратори, як правило, спочатку обирають другий рівень безпеки (authNoPriv), і лише деякі з них, за необхідності, переходять на третій рівень (authPriv). Однією з причин обмеженого використання третього рівня є його здатність перевантажувати мережеві пристрої.

Наразі завершено розробку нової специфікації Data Over Cable Service Interface Specification (DOCSIS), і багато користувачів уже використовують алгоритми Діффі-Хеллмана та Kerberos замість DES для управління ключами. Це свідчить про тенденцію до вдосконалення безпеки, і можна очікувати виходу нової версії протоколу SNMP найближчим часом. Таким чином, третя версія SNMP вважається найбільш захищеною на даний момент і вимагає детального вивчення атак на її безпеку.

Основними вразливостями та атаками на протокол SNMP є:

- SNMP Amplification (DDoS-атака)
- Вразливість у стандартній конфігурації Windows SNMP-сервісу.
- Проблема в OS Solaris версії до 2.6.

Суть атаки SNMP Amplification полягає у тому, щоб спричинити повторне високо збільшене відправлення відповідей на SNMP-запити. Із початку створені для автоматизації отримання табличних даних за мінімізації відсиланих пакетів, BULK-запити виявилися ефективним інструментом для вчинення DDoS-атак з боку злоумисників. Згідно з RFC3416, GetBulkRequest, який реалізований у SNMP версії

2, призначений для здійснення запитів із великим обсягом даних, чим активно користуються атакуючі, використовуючи неправильно налаштовані сервери в Інтернеті.

Якщо встановити максимальну кількість рядків, що повертаються в таблиці, наприклад, 20000, і надіслати запит на адресу неправильно налаштованого сервера або пристрою, відповідь буде приблизно наступною:
iso.3.6.1.6.3.18.1.1.1.8.123.123.12.123.123.12.12. 123.123.12 .123.123.12 = No more variables left in this MIB View (It is past the end of the MIB tree).

Відповідь на такий запит, розмір якої становить приблизно 70 байт з урахуванням заголовків, майже в 150 разів більша, ніж сам запит. Коефіцієнт посилення не є фіксованим і може бути як більшим (до 1700 разів), так і меншим значенням, залежно від типу операційної системи та конфігурації пристрою. Під час формування такого запиту, з використанням заміни IP-адреси відправника на адресу жертви та високої інтенсивності звернень до вразливого сервера, DDoS-атака може бути успішно виконана.

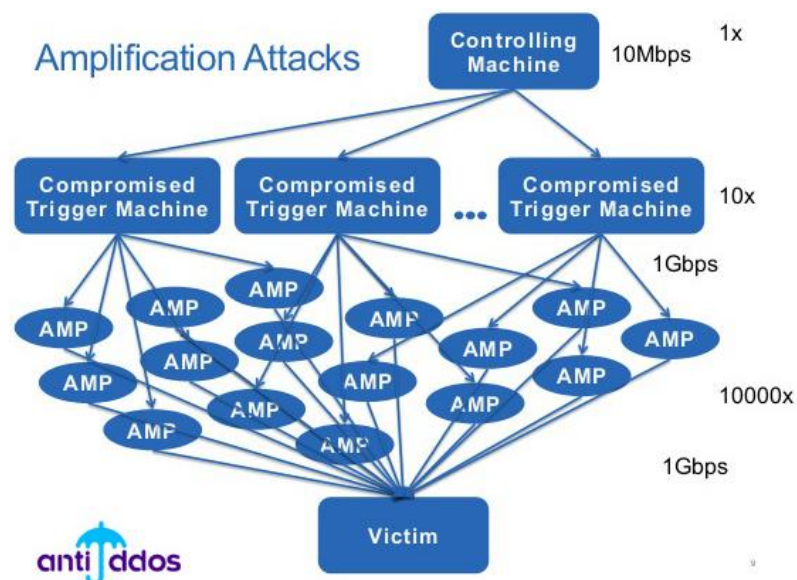


Рисунок 1.10 – Схематичне зображення атаки SNMP Amplification

Захист від DDoS атак типу SNMP Amplification передбачає усунення можливостей підміни адрес та усунення вразливостей протоколу UDP. Загальні

рекомендації для вразливих атак з використанням заміни адреси протоколів на базі UDP надані в BCP38 і RFC2827.

Специфічні для SNMP рекомендації щодо забезпечення безпеки сервера або мережного обладнання можна поділити на такі напрямки:

- Архітектурне: дозвіл на обробку лише на інтерфейсах, недоступних із не довірених мереж.
- Зміна community на більш непередбачуване.
- Обмеження IP-адрес керуючих станцій.
- Обмеження гілки OID, яка доступна для отримання/зміни SNMP.
- Мінімізація використання community у режимі читання і запис.
- Перехід на SNMPv3 для додаткових параметрів аутентифікації та шифрування.
- Вимкнення SNMP, якщо не використовується.

Вразливість у стандартній конфігурації Windows SNMP сервісу дозволяє віддалено налаштовувати мережеві параметри, які впливають на безпеку та правильне функціонування системи (при умові, що адміністратор самотійно запустив службу SNMP).

При конфігурації за замовчуванням служба SNMP відповідає стандартному "community" (ім'я) "public" з правами на читання і запис. "Community" виконує роль, аналогічну логіну та паролю в інших системах.

Протокол SNMP надає два рівні повноважень: "read-only" (тільки для читання) та "read-write" (читання і запис), проте до виходу SP4 для Windows NT SNMP Service не дозволяв налаштовувати "communities" доступу, відмінні від "read-write"!

При спробі забезпечити безпеку служби SNMP шляхом перейменування "community" для доступу, система залишається незахищеною від крєкера, який має обліковий запис на машині, оскільки параметри SNMP Service знаходяться в реєстрі і доступні всім користувачам для читання. Крім того, служба Windows NT SNMP має можливість обмежувати доступ за списками IP-адрес. На перший по-

гляд, це може забезпечити захист від атак невідомих систем, але це не є неproblemною для крєкерів, які розуміють, оскільки протокол SNMP використовує UDP для обміну інформацією, що дозволяє змінювати вихідну адресу (за умови переробки вихідних даних SNMP менеджерів під Unix і освоїти UDP підробку).

Операції SNMP "set" (дозволяють змінювати значення змінних) можуть бути виконані зі зміною зворотної адреси на будь-яку, оскільки відповідь не потрібна. Проте, якщо обмеження за довіреними IP-адресами включено, атакуючому слід знайти обліковий запис на атакованій системі та отримати довірену інформацію з реєстру.

Завдяки налаштованій за замовчуванням службі SNMP в Windows NT, майже вся інформація про пристрої може бути отримана за допомогою SNMP-менеджера, що надає можливості для різноманітних маніпуляцій з боку зловмисника.

В OS Solaris версії до 2.6 згідно з ISS Security Advisory від 2 листопада 1998 року, існують реальні загрози отримання доступу на рівні "root" та маніпулювання процесами та параметрами машини через агент SNMP, який за замовчуванням активний в цій системі.

Для доступу до MIB-інформації існує прихована "undocumented community string", яка дозволяє атакуючому змінити більшість системних параметрів.

На жаль, саме цей "community" не є публічно вказаним, але ISS Internet Scanner та ISS RealSecure real-time intrusion detection можуть виявити цю проблему, що можна перевірити в їх вихідних файлах.

1.4 Застосування протоколів моніторингу мережі для побудови систем кіберзахисту

Протоколи NetFlow та IPFIX (IP Flow Information Export) грають важливу роль у побудові систем кіберзахисту, надаючи засоби для моніторингу, аналізу та виявлення потенційних загроз безпеці в мережах. Ось кілька аспектів їх застосування у системах кіберзахисту:

- Моніторинг мережевого трафіку: NetFlow та IPFIX дозволяють збирати детальну інформацію про мережевий трафік, включаючи джерела, призначення, протоколи та обсяг передачі даних. Це допомагає адміністраторам відстежувати та моніторити всі аспекти мережевої активності.

- Виявлення аномалій та загроз: Аналіз NetFlow/IPFIX даних дозволяє виявляти аномалії та потенційні загрози безпеки, такі як атаки, несправедливо великий обсяг трафіку, незвичайні патерни поведінки тощо.

- Аналіз підозрілого трафіку: За допомогою зібраної інформації можна аналізувати трафік, який викликає підозри, ідентифікувати потенційно шкідливі або зловмисні активності, а також виявляти атаки на різних рівнях мережі.

- Виявлення DDoS-атак: NetFlow та IPFIX можуть використовуватися для виявлення розподілених атак на сервіс (DDoS). Аналіз змін у розподілі трафіку дозволяє реагувати на атаки та захищати мережеву інфраструктуру.

- Інцидентний аналіз: Збір та аналіз даних NetFlow та IPFIX допомагає в проведенні інцидентного аналізу у випадку кібератак або порушень безпеки. Це дозволяє оперативно реагувати та розслідувати події.

- Моніторинг пропускної здатності: За допомогою цих протоколів можна ефективно вимірювати та моніторити використання пропускної здатності мережі, виявляти перевантаження та планувати оптимальне використання ресурсів.

- Системи кореляції подій: Дані NetFlow та IPFIX можуть бути використані у системах кореляції подій для ідентифікації складних злочинних сценаріїв та взаємодії різних подій.

- Управління доступом та політика безпеки: Інформація, отримана з NetFlow та IPFIX, дозволяє розробляти та вдосконалювати політику безпеки, визначати правила контролю доступу та ефективно вдосконалювати заходи забезпечення безпеки.

Використання протоколів NetFlow та IPFIX є важливим компонентом комплексних систем кіберзахисту, які сприяють вчасному виявленню, аналізу та запобіганню загрозам безпеки в мережах.

Використання протоколу SNMP у системах кіберзахисту потребує більш детального аналізу та порівняння з найближчими аналогами, оскільки є більш масштабним рішенням. Крім цього при неправильному налаштуванні пристрої мережі, які використовують цю технологію, будуть доволі вразливим місцем.

Протокол простого мережевого управління (SNMP) був розроблений для віддаленого моніторингу мережевих пристроїв через IP-мережі. Використовуючи SNMP, можна збирати інформацію з різноманітних мережевих пристроїв, таких як маршрутизатори, комутатори, а також пристрої на основі операційних систем Windows і IBM Power Systems. Протокол також застосовується для конфігурації та внесення змін. Шляхом використання SNMP компанії отримують можливість перехоплювати повідомлення в межах рішень SIEM або систем моніторингу, а також сповіщати зацікавлених осіб про отримання конкретного повідомлення. Оскільки SNMP також може використовуватися для внесення змін до конфігурації пристроїв, компанії отримують можливість реагувати на конкретні повідомлення з метою автоматизації виправлення проблем.

Найближчим по функціоналу рішенням замість протоколу SNMP вважається Syslog [7]. Саме тому досить важливим є порівняння даних протоколів.

Ось основні відмінності між SNMP та системним журналом:

- Сповіщення в режимі реального часу порівняно з історичними даними – SNMP був розроблений, щоб попередити вас про подію в режимі реального часу. Syslog був розроблений, щоб забезпечити спосіб централізації інформації журналу для історичних цілей.

- Pull або push – SNMP надсилає запит на пристрій, який шукає інформацію, тоді як сервер системного журналу просто є сховищем інформації, яку потім можна запитати для отримання більш детальної інформації.

- Надійність – пристрої системного журналу не можуть гарантувати, що їхнє повідомлення надходить до сервера системного журналу. SNMP опитує пристрій, щоб отримати інформацію, і тому не може втратити дані.

- Проактивне проти реактивного – SNMP може реагувати на пастку і вживати певних заходів. Syslog не може цього зробити.

- Зміна статусу або детальна інформація – SNMP попереджає про зміну статусу, наприклад, рядок тепер недоступний. Syslog може містити більш детальну інформацію про те, чому щось сталося.

- Безпечні проти незахищених – SNMP-повідомлення безпечні і не можуть бути підроблені. Хоча Syslog не захищений, і повідомлення можна підробити.

Навіть при зусиллях з підвищення рівня безпеки, компанії також вдосконалюють свою автоматизацію. SNMP надає можливість підприємствам активно реагувати на проблеми здоров'я системи, що визначально впливає на доступність та продуктивність системи. SNMP дозволяє проводити опитування для виявлення конкретних подій та реагувати на їхні відповіді. Якщо виникла подія, адміністратор може прийняти заходи для її усунення. Це значущий крок вперед для бізнесу.

Syslog дозволяє компаніям централізувати всю аудиторську інформацію в єдиному місці, що є особливо корисним для підготовки аудиторських звітів. Після цього вони можуть використовувати рішення моніторингу, такі як AbsMessage, для сповіщення про отримання конкретного повідомлення або автоматичного ініціювання відповіді, що забезпечує реагування на потенційні загрози в режимі реального часу та знижує ризики.

Добра новина полягає в тому, що користувачам не потрібно обирати між SNMP і syslog. Головне - знайти рішення моніторингу, яке підтримує формати як SNMP, так і syslog, для підвищення рівня безпеки, ефективності та продуктивності на платформі IBM i.

Загалом протокол SNMP є однією з кращих опцій для моніторингу мережі. У контексті кіберзахисту, моніторинг мережі визначається як один із ключових етапів розслідування кіберзагроз. Зокрема, версія SNMPv3 відзначається високим рівнем захисту, що робить її важливим інструментом у системах кіберзахисту.

Висновки до першого розділу

У першому підрозділі було розглянуто основні теоретичні відомості щодо протоколів SNMP, NetFlow та IPFIX. Наведено їх архітектуру, основні реалізації обміну повідомленнями.

У другому підрозділі було наведено прикладні реалізації використання протоколу моніторингу мережі. Було порівняно варіанти реалізації моніторингу за допомогою додатків на базі ОС Windows та Linux. В результаті порівняння з'ясовано, що найкращим рішенням буде використання ПО ManageEngine NetFlow Analyzer та PRTG.

У третьому підрозділі проаналізовано основні проблеми безпеки протоколів SNMP, NetFlow та IPFIX. З'ясовано, що незважаючи на досить сильний захист протоколу SNMP третьої версії все ж існують певні проблеми, які найчастіше зв'язані з бекдорами ПО на різних ОС.

У четвертому підрозділі розглянуто роль протоколів моніторингу у проектуванні та будівництві системи кібрзахисту на базі моделі додатків SIEM.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КМ НА БАЗІ ПРОТОКОЛІВ SNMP, NETFLOW І IPFIX ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ

2.1 Проектування підсистеми моніторингу вразливостей та комп'ютерної мережі

При проектуванні було використано трьохрівневу модель мережі від компанії Cisco Systems [8]. Дана модель є ієрархічною та складається з трьох безпосередньо залежних один від одного рівнів:

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

Глобальну мережу організації було спроектовано за допомогою графічного редактору Draw.io. Загальну топологію мережі наведено на рис. 2.1:

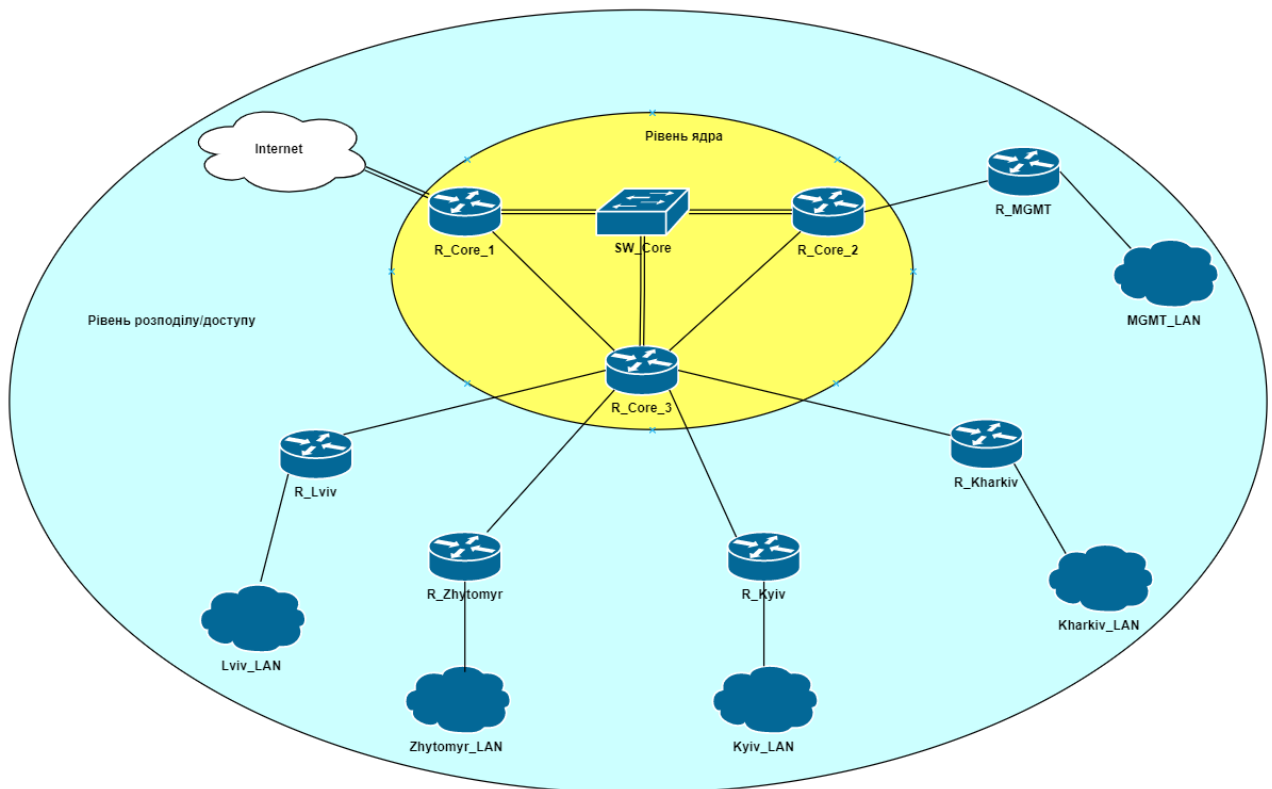


Рисунок 2.1 – Загальна топологія мережі

Ядро мережі складається із трьох маршрутизаторів та одного комутатора, які взаємодіють через високошвидкісні канали зв'язку на базі технології Gigabit Ethernet. Канали, що з'єднують роутери з комутатором, агреговані для збільшення пропускної здатності мережі. Крім того, один із маршрутизаторів має забезпечений вихід в глобальну мережу за допомогою трансляції адрес за протоколом NAT.

Рівень розподілу та доступу включає п'ять маршрутизаторів, які з'єднані з ядром мережі та обладнанням кінцевих користувачів. Ці пристрої важливі для передачі трафіку віддалених мереж. Підключення до ядра реалізовано за допомогою витої пари Gigabit Ethernet. Канали між роутерами розподілу та роутерами ядра проагреговані для підвищення продуктивності мережі. Крім того, одна з локальних мереж служить для адміністрування пристроїв за допомогою протоколів SNMP, Net-Flow та IPFIX.

В загальному у мережі використано 8 маршрутизаторів, 6-ти комутаторів. Мережа складається з 5 локальних мереж.

До кожного маршрутизатора доступу підключено 1-2 мережі. Розглянемо детальніше кожен з них.

Від маршрутизатора R_Zhytomyr виходить локальна мережа LAN_Zhytomyr. Проект даної ділянки зображено на рисунку 2.2.

Мережа LAN_Zhytomyr включає в себе 186 ПК і 9 комутаторів на 24 порти. Кожен комутатор підключений до 21 ПК, і один порт SW_Zhytomyr використовується для з'єднання з R_Zhytomyr, з додатковими 2 портами на кожному комутаторі для агрегованого каналу між ними. Це важливо для забезпечення достатньої пропускної здатності в такій топології. На всіх комутаторах, за винятком того, який з'єднаний з R_Zhytomyr, залишається вільним один порт. Підключення до маршрутизатора виконане за допомогою витої пари за технологією Gigabit Ethernet. Усі інші підключення в мережах даних реалізовані за допомогою технології Fast Ethernet і також використовують виту пару. Для прикладу даної мережі створено кілька додаткових LAN для міст з можливістю розширення. Ці мережі представляють собою LAN, до яких підключаються користувачі головної мережі.

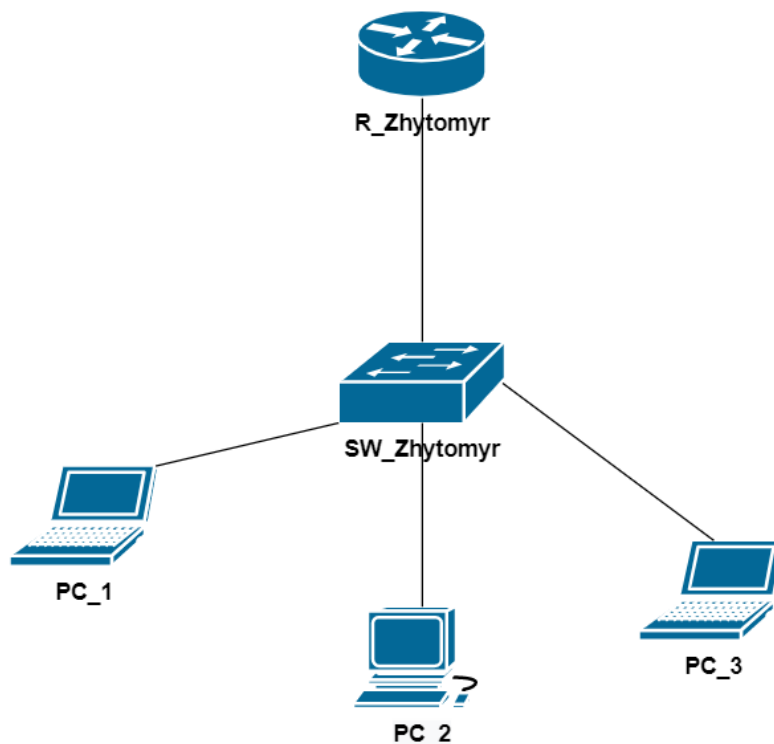


Рисунок 2.2 – Загальний вигляд мережі LAN_Zhytomyr

Маршрутизатор R_Core_1 виконує роль з'єднуючого елемента між топологією та глобальною мережею. На цьому маршрутизаторі налаштовано трансляцію адрес локальних мереж за протоколом PAT (NAT). Адреси для доступу до мережі отримуються використовуючи протокол динамічної адресації DHCP. Структура даного вузла відображена на рисунку 2.3.

Ця мережа складається з одного маршрутизатора та хмари, що представляє Інтернет. Маршрутизатор у цій мережі є частиною ядра, що забезпечує всім пристроям топології можливість отримувати доступ до глобальної мережі. Для надання цього доступу використано динамічну маршрутизацію за допомогою протоколу EIGRP.

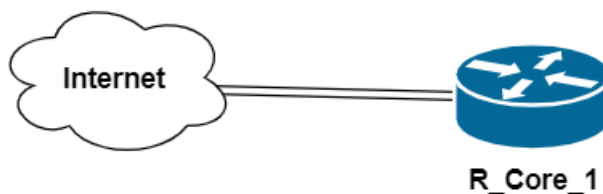


Рисунок 2.3 – Загальний вигляд ділянки доступу до WAN

Від маршрутизатора R_MGMT виходить одна мережа - MGMT. Ця мережа використовується для віддаленого адміністрування, моніторингу та тестування безпеки мережі. Схему даного сегмента можна побачити на рисунку 2.5.

Мережа MGMT включає 28 ПК та 2 комутатори з 26 портами. Кожен комутатор підключений до 14 ПК, використовуючи 1 порт для підключення до R_MGMT та для взаємодії між комутаторами. Кожен з комутаторів має 10 вільних портів, що служать як резервні. Підключення до маршрутизатора та між комутаторами виконано за допомогою витієї пари технології Gigabit Ethernet. Усі інші підключення цієї мережі реалізовані за допомогою технології Fast Ethernet та також витієї пари.

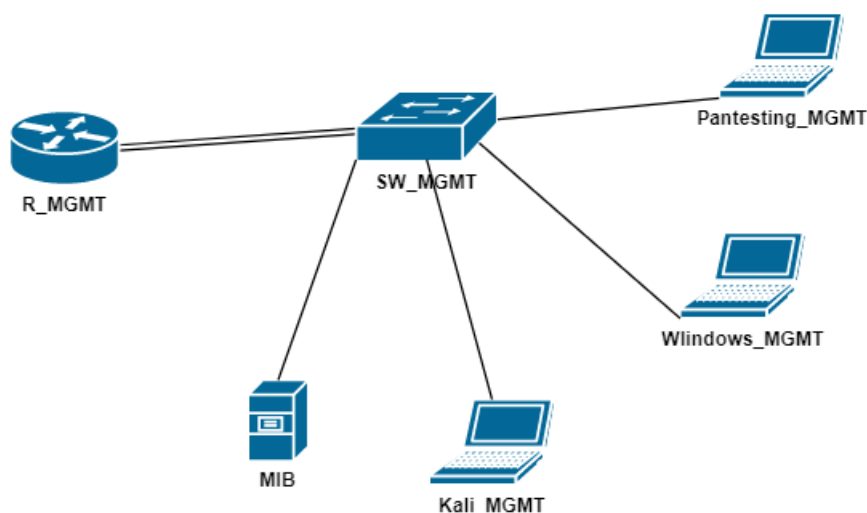


Рисунок 2.4 – Загальний вигляд мережі MGMT

Однією з ключових фаз під час розробки топології є створення схеми адресації мережі, спрямованої на уникнення конфліктів адрес та можливих перешкод у функціонуванні мережі. При розробці цієї схеми основна увага була приділена оптимізації кількості IP-адрес, з урахуванням можливості розширення існуючих мереж.

Для пристроїв рівня ядра були розраховані відповідні IP-адреси мережі. Деякі з цих IP-адрес будуть призначені пристроям рівня розподілу/доступу для забезпечення їх взаємодії. Розрахунки наведено в таблиці 2.1.

Таблиця 2.1 – Параметри адресації пристроїв ядра

Пристрої	Мережа
R_Core_1, R_Core_2, R_Core_3	192.168.1.0/28
R_Core_1, Internet	DHCP (192.168.122.0/24)
R_Core_2, R_MGMT	192.168.20.0/30
R_Core_3, R_Lviv	192.168.10.0/30
R_Core_3, R_Zhytomyr	192.168.11.0/30
R_Core_3, R_Kyiv	192.168.12.0/30
R_Core_3, R_Kharkiv	192.168.13.0/30

Більш детального огляду потребує розрахунок IP-адрес локальних мереж. Результати розрахунків подано у вигляді таблиць 2.2-2.6.

Таблиця 2.2 – Параметри адресації мережі LAN_Lviv

Призначення	IP-адреса
Адреса мережі	192.168.110.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.110.1
Максимальна адреса вузла	192.168.110.254
Широкомовна адреса	192.168.110.255
Шлюз по замовчуванню	192.168.110.1
Діапазон статичних адрес	192.168.110.10 – 192.168.110.10
Діапазон адрес майбутніх ПК	192.168.110.11 – 192.168.110.156
Діапазон вільних адрес	192.168.110.157 – 192.168.110.254

Таблиця 2.3 – Параметри адресації мережі LAN_Zhytomyr

Призначення	IP-адреса
Адреса мережі	192.168.111.0

Продовження таблиці 2.3 – Параметри адресації мережі LAN_Zhytomyr

Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.111.1
Максимальна адреса вузла	192.168.111.254
Широкомовна адреса	192.168.111.255
Шлюз по замовчуванню	192.168.111.1
Діапазон статичних адрес	192.168.111.10 – 192.168.111.10
Діапазон адрес майбутніх ПК	192.168.111.11 – 192.168.111.206
Діапазон вільних адрес	192.168.111.207 – 192.168.111.254

Таблиця 2.4 – Параметри адресації мережі LAN_Kyiv

Призначення	ІР-адреса
Адреса мережі	192.168.112.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.112.1
Максимальна адреса вузла	192.168.112.254
Широкомовна адреса	192.168.112.255
Шлюз по замовчуванню	192.168.112.1
Діапазон статичних адрес	192.168.112.10 – 192.168.112.10
Діапазон адрес майбутніх ПК	192.168.112.11 – 192.168.112.171
Діапазон вільних адрес	192.168.112.172 – 192.168.112.254

Таблиця 2.5 – Параметри адресації мережі LAN_Kharkiv

Призначення	ІР-адреса
Адреса мережі	192.168.113.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.113.1
Максимальна адреса вузла	192.168.113.254
Широкомовна адреса	192.168.113.255
Шлюз по замовчуванню	192.168.113.1
Діапазон статичних адрес	192.168.113.10 – 192.168.113.10
Діапазон адрес майбутніх ПК	192.168.113.11 – 192.168.113.171

Продовження таблиці 2.5 – Параметри адресації мережі LAN_Kharkiv

Діапазон вільних адрес	192.168.113.172 – 192.168.113.254
------------------------	-----------------------------------

Таблиця 2.6 – Параметри адресації мережі LAN_MGMT

Призначення	ІР-адреса
Адреса мережі	192.168.254.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31
Мінімальна адреса вузла	192.168.254.1
Максимальна адреса вузла	192.168.254.30
Широкомовна адреса	192.168.254.31
Шлюз по замовчуванню	192.168.254.1
Діапазон статичних адрес	192.168.254.1 – 192.168.254.30
Діапазон адрес майбутніх ПК	–
Діапазон вільних адрес	–

2.2 Аналіз загроз підсистеми моніторингу

Аналіз загроз підсистеми моніторингу полягає у детальному огляді протоколів та технологій налаштованих на пристроях мережі та перевірці можливих атак на них. У спроектованій топології будуть функціонувати наступні протоколи:

- DHCP
- SNMPv3
- NetFlow v9
- IPFIX
- EIGRP, який “з коробки” є досить захищеним
- SSHv2
- ARP

Окрім атак на протоколи також можливе проникнення до адміністративних панелей пристроїв мережі з метою отримання привілеїв з подальшою шкодою для системи.

Один із перших протоколів, який стає вразливим до можливих атак, - це DHCP. Його порушення може дозволити зловмиснику "відрізати" локальні мережі

з великою кількістю пристроїв від мережі або, перехопивши трафік, заволодіти критично важливою інформацією. Основними способами реалізації атак на протокол DHCP у спроектованій топології є:

- Атака DHCP Starvation
- Атака DHCP Spoofing

У процесі атаки на виснаження ресурсів DHCP зломисник генерує масоване розсилання DHCP-запитів на DHCP-сервер, з метою вичерпати всі доступні IP-адреси, які сервер DHCP може виділити [10]. Після розподілу всіх доступних IP-адрес, які DHCP-сервер може призначити, виникає відмова в обслуговуванні (DoS-атака). Це призводить до того, що нові клієнти не можуть отримати доступ до мережі. DoS-атака полягає у використанні будь-яких методів для перевантаження конкретних пристроїв та мережевих сервісів несанкціонованим трафіком, у результаті чого легітимний трафік не може користуватися цими ресурсами.

Під час атаки DHCP Spoofing зломисник конфігурує фальшивий DHCP-сервер в мережі, який видаватиме клієнтам DHCP-адреси. Мета цієї атаки полягає в тому, щоб змусити клієнтів використовувати невірні служби доменних імен (DNS) та службу імен Інтернету в системі Windows (сервер WINS), а також використовувати вузол або пристрій зломисника як стандартний шлюз [10]. До атаки DHCP Spoofing часто використовується атака DHCP Starvation для вимкнення легітимного DHCP-сервера, що робить набагато простішим впровадження фіктивного DHCP-сервера в мережу.

Навіть при наявності досить міцного захисту у протоколі SNMPv3, існує можливість виконання деяких атак за умови отримання відповідних авторизаційних даних. Ризики представлені наступними вразливостями та атаками:

- Атака SNMP Amplification
- Вразливість у реалізації SNMPv3 у продуктах Cisco

Суть атаки SNMP Amplification полягає в ініціюванні повторюваних великих відповідей на SNMP-запити. По-перше, цей вид атаки був розроблений для автоматизації отримання табличних даних з мінімізацією кількості відправлених пакетів. BULK-запити, спочатку створені для оптимізації отримання значень з таблиць,

стали ефективним інструментом для DDoS-атак в руках зловмисників. За стандартом RFC3416, GetBulkRequest, реалізований у SNMP версії 2 [11], призначений для отримання великої кількості даних. Зловмисники використовують цю можливість, зокрема, зловживаючи неправильно налаштованими серверами в мережі.

Якщо встановити максимальну кількість рядків, які повертаються в таблиці на значення, наприклад, 20000, і виконати запит на адресу неправильно налаштованого сервера чи пристрою, то у відповідь розміром приблизно 70 байт (з урахуванням заголовків) сервер поверне відповідь розміром приблизно 10 кілобайт, що майже в 150 разів більше. Коефіцієнт посилення не є фіксованим і може змінюватися в залежності від типу операційної системи та конфігурації пристрою.

Інша загроза полягає в вразливості реалізації SNMP 3-ьої версії у продуктах Cisco. Ця вразливість пов'язана з кодом аутентифікації в різних реалізаціях протоколу SNMPv3. Атакувач може використовувати спеціально сформований пакет SNMPv3 з використанням HMAC-MD5-96 або HMAC-SHA-96 як аутентифікаційного протоколу. Це дозволяє виконати атаку спуфінгу та отримати доступ до деяких даних або змінити конфігурацію пристрою.

SSHv2 – це безпечний протокол зв'язку, який охоплює кілька рівнів архітектури, але протягом його використання було виявлено кілька безпекових ураз, які дозволяють проводити атаки на мережу. Серед таких атак можна виділити:

- SSH Brute-force
- MITM-атака
- Timing attack

Однією з найпоширеніших атак на протокол SSH є атака методом перебору паролів. Часто використовується додаткове програмне забезпечення та певна відкрита база даних паролів (словник). При запуску сервісу SSH, який доступний з Інтернету, у журналі аутентифікації користувачів можна помітити багато записів про невдалий вхід користувача admin/root, якщо він неправильно вводить пароль. Це типовий вигляд атаки методом перебору паролів, відомої як "bruteforce". Простим заходом захисту може бути створення правила, що блокує весь доступ. Проте

це може призвести до проблем, таких як надання доступу легітимним користувачам. Іншим варіантом є зміна порту роботи протоколу. Статистика показує, що зміна SSH-порту на порт з верхнього діапазону значно зменшує кількість спроб не-санкціонованого доступу, але, звісно, не виключає їх повністю. Важливо зауважити, що той, хто здійснював сканування порту 22, може знайти і порт 22222, на якому, ймовірно, також налаштовано роботу SSH [12]. Однак це може бути лише додатковим заходом для досягнення успіху. Також рекомендується використовувати нестандартні імена користувачів і паролі для зменшення ефективності атаки методом перебору паролів.

Man-in-the-middle – це вид атаки, що ґрунтується на перенаправленні трафіка між двома комп'ютерами для перехоплення інформації, в подальшому її вивчення, знищення або модифікації, тобто порушення цілісності та конфіденційності інформації. Атакуюча сторона отримує дані авторизації користувача і здійснює журналювання усього сеансу зв'язку, запуск команд та їх виконання.

Атака по часу представляє собою прийом, при якому зловмисник використовує сторонній канал для загрози криптосистемі, проводячи аналіз часу, необхідного для виконання різних операцій. Кожна дія на комп'ютері вимагає певного часу, який може змінюватися в залежності від вхідних даних. У випадку атаки по часу на SSH зловмисник може визначити момент, коли користувач вводить дані для авторизації і перехопити їх. На рисунку 1 показано, що після натискання клавіші виконується операція відправлення символу на SSH-сервер.

В даному контексті зловмисник може виявити, коли користувач використовував команду "su", яка складається з двох 20-бітових пакетів, за якими слідує пакет "Password:" розміром 28 біт. Усі наступні пакети до пакету "Prompt" є символами пароля, отримавши які, зловмисник може отримати доступ до сервера.

Незважаючи на механізми шифрування та автентифікації, які використовує протокол SSH, він має дві слабкості, що сприяють атакам по часу. По-перше, передані пакети обмежені лише восьми байтами (у випадку блокового шифру), що вказує на приблизний розмір вихідних даних. По-друге, в інтерактивному режимі

кожне натискання клавіші, яке користувач відправляє на віддалену машину, передається окремим IP-пакетом відразу після натискання кнопки, що розкриває інформацію про часові інтервали між різними клавішами.

Протокол ARP є одним із ключових у передачі даних у мережі та функціонує на канальному рівні. Виведення з ладу цього протоколу призведе до неможливості обміну трафіком у мережі, тому йому приділяється високий пріоритет щодо захисту. Основні атаки на ARP включають:

- ARP-spoofing
- ARP-poisoning

Спуфінг ARP — це тип атаки, під час якої зловмисник надсилає фальсифіковані повідомлення ARP (протоколу розпізнавання адрес) через локальну мережу. Це призводить до пов'язування MAC-адреси зловмисника з IP-адресою законного комп'ютера або сервера в мережі. Як тільки MAC-адреса зловмисника буде підключена до аутентичної IP-адреси, зловмисник почне отримувати будь-які дані, призначені для цієї IP-адреси. Підробка ARP може дозволити зловмисникам перехоплення, змінення або навіть зупинку передачі даних. Атаки підробки ARP можуть відбуватися лише в локальних мережах, які використовують протокол розділення адрес.

Отруєння ARP (заміна ARP) – це форма атаки, спрямована на локальні мережі з метою відправлення шкідливих ARP-пакетів на шлюз. Головною метою цієї атаки є зміна відповідності між "IP-адреса - MAC-адреса". Початково протокол ARP був розроблений виключно для забезпечення максимальної ефективності роботи, і принципи безпеки не були враховані.

Атака полягає в відсиланні підробленої ARP-відповіді з метою асоціації MAC-адреси атакуючого з IP-адресою жертви і навпаки. Як тільки шлюз отримує таку відповідь, відбувається широкомовне розповсюдження цих змін, і всі пристрої в мережі отримують підроблені дані. Цей етап дозволяє атакуючому перенаправляти трафік через свій комп'ютер. В результаті до тих пір, поки пакети досягають реальної IP-адреси призначення, вони обробляються/модифікуються атакуючим.

Використовуючи цей метод, зломисник може легко здійснювати шкідливі дії, маючи доступ до комп'ютера в локальній мережі. Крім того, цей вид атаки, наряду з атакою MITM, може призвести до "відмови в обслуговуванні", перенаправляючи або відкидаючи вхідний/вихідний трафік.

2.3 Побудова моделі загроз підсистеми моніторингу

Для безперебійної роботи мережі на етапі проектування важливо провести аналіз всіх можливих загроз. Ефективним методом для цього є графічне моделювання, яке дозволяє візуально виділити вразливі елементи системи та ідентифікувати процеси та суб'єкти, які можуть становити загрозу мережі.

Моделювання ризиків – це постійний процес, спрямований на виявлення та зменшення кількості загроз у системі за допомогою вжиття відповідних заходів. Використання моделювання інформаційних ризиків дозволяє отримати розуміння реальних атак, визначити зв'язки між компонентами системи, розробити сценарії та оцінити ймовірності використання вразливостей, а також зрозуміти вплив атак на систему.

Для повного розуміння аспектів безпеки мережі необхідно визначити наступне під час моделювання:

- вимоги безпеки;
- загрози та потенційні вразливості;
- оцінку критичності загроз і вразливостей.

Після моделювання було визначено повний перелік можливих загроз мережі, проаналізовано основні процеси, бази даних та користувачів на стійкість до різноманітних загроз, оцінено критичність кожної з них.

Загрози проектованої мережі можна класифікувати за природою на об'єктивні (атаки від користувачів, хакерів, зломисників) та суб'єктивні (природні та техногенні катастрофи). Для кожної загрози були визначені властивості інформації, можливі способи реалізації та джерела виникнення.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІДСИСТЕМИ МОНІТОРИНГУ КМ

3.1 Налагодження КМ та підсистеми моніторингу

Для забезпечення коректної роботи мережі важливо встановити всі параметри в правильному порядку і використовувати відповідні налаштування. У даному випадку використовуються ті параметри, які були розраховані під час проектування топології.

Початково були налаштовані параметри IP-адресації для всіх пристроїв мережі. Розглянемо цей процес на прикладі ядерного роутера R_Core_3:

```
R_Core_3#configure terminal
R_Core_3(config)#interface fastEthernet0/0
R_Core_3(config-if)#description link_to_SW_Core
R_Core_3(config-if)#ip address 192.168.1.3 255.255.255.240
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Lviv
R_Core_3(config-if)#ip address 192.168.10.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Zhytomyr
R_Core_3(config-if)#ip address 192.168.11.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Kyiv
R_Core_3(config-if)#ip address 192.168.12.1 255.255.255.252
R_Core_3(config-if)#no shutdown
```

```
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Kharkiv
R_Core_3(config-if)#ip address 192.168.13.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3#write
```

Роутери доступу налаштовано, як DHCP-сервери. Приклад налаштування показано на основі R_Zhytomyr:

```
R_Zhytomyr#configure terminal
R_Zhytomyr(config)#ip dhcp excluded-address 192.168.111.1 192.168.111.10
R_Zhytomyr(config)#ip dhcp pool LAN_Zhytomyr
R_Zhytomyr(dhcp-config)#network 192.168.111.0 255.255.255.0
R_Zhytomyr(dhcp-config)#default-router 192.168.111.1
R_Zhytomyr(dhcp-config)#dns-server 8.8.8.8
R_Zhytomyr(dhcp-config)#domain-name yavorenko.local
R_Zhytomyr(dhcp-config)#end
```

На всіх маршрутизаторах встановлено налаштування для використання протоколу EIGRP для маршрутизації. Інтерфейси на роутерах доступу, які ведуть до LAN, були переведені у пасивний режим. Маршрутизатор ядра, що має з'єднання з глобальною мережею, отримав статичний маршрут і був доданий до загальної таблиці маршрутизації через редистрибуцію протоколу EIGRP. Приклад налаштування на R_Core_3:

```
R_Core_3#configure terminal
R_Core_3(config)#router eigrp 1
R_Core_3(config-router)#no auto-summary
R_Core_3(config-router)#network 192.168.1.0 0.0.0.15
R_Core_3(config-router)#network 192.168.10.0 0.0.0.3
```

```
R_Core_3(config-router)#network 192.168.11.0 0.0.0.3
R_Core_3(config-router)#network 192.168.12.0 0.0.0.3
R_Core_3(config-router)#network 192.168.13.0 0.0.0.3
R_Core_3(config-router)#end
```

Для надання доступу до глобальної мережі на одному з маршрутизаторів ядра була налаштована трансляція адрес мережі за допомогою протоколу PAT (NAT). IP-адресу з глобальної мережі було отримано через протокол DHCP. Також був встановлений статичний маршрут для маршрутизації цього маршруту іншим пристроям мережі та доданий до глобальної таблиці маршрутизації через редистрибуцію статичних маршрутів. Приклад налаштування на R_Core_1:

```
R_Core_1#configure terminal
R_Core_1(config)#interface FastEthernet0/0
R_Core_1(config-if)#ip address dhcp
R_Core_1(config-if)#ip nat outside
R_Core_1(config-if)#exit
R_Core_1(config)#interface FastEthernet0/1
R_Core_1(config-if)#ip nat inside
R_Core_1(config-if)#exit
R_Core_1(config)#access-list 1 permit any
R_Core_1(config)#ip nat inside source list 1 interface FastEthernet0/0 overload
R_Core_1(config)#ip route 0.0.0.0 0.0.0.0 fastEthernet0/1
R_Core_1(config)#router eigrp 1
R_Core_1(config-router)#redistribute static
R_Core_1(config-router)#end
R_Core_1#write
```

Для моніторингу та управління мережею використовується протокол SNMP. На маршрутизаторах та комутаторах критичного рівня (ядра) був налаштований SNMP-сервер за протоколом третьої версії, який вважається найбільш захищеним

варіантом. Доступ до серверу реалізовано лише з ПК головного адміністратора мережі MGMT за допомогою списків контролю доступу. Приклад налаштування на комутаторі SW_Core:

```
SW_Core#configure terminal
SW_Core(conf)#ip access-list standard YAVORENKO_SNMP_ACL
SW_Core(config-std-nacl)#permit 192.168.254.3
SW_Core(config-std-nacl)#exit
SW_Core(conf)#snmp-server group ADMIN v3 priv match exact write YAVORENKO_SNMP-RW access YAVORENKO_SNMP_ACL
SW_Core(conf)#snmp-server view YAVORENKO_SNMP-RW iso included
SW_Core(conf)#snmp-server user YAVORENKO_ADMIN ADMIN v3 auth md5
cisco12345 pri des cisco54321
SW_Core(conf)#snmp-server location Ukraine_WAN
SW_Core(conf)#snmp-server contact admin@yavorenko.local.net
SW_Core(conf)#snmp-server enable traps
SW_Core(conf)#end
SW_Core#write
```

На рівні доступу реалізовано сервери менеджменту та моніторингу за протоколом SNMP версії 2с. Для кожної з задач реалізовано відповіді рядки спільноти з розгалуженням доступу до мережі відповідно до прав доступу. Таким чином, менеджмент дозволений лише з ПК головного адміністратора мережі MGMT, а моніторинг доступний всім адміністраторам цієї ж мережі. Приклад налаштування на R_Kyiv:

```
R_Kyiv#configure terminal
R_Kyiv(conf)#ip access-list standard ADMIN_SNMP_ACL
R_Kyiv(config-std-nacl)#permit 192.168.254.3
R_Kyiv(config-std-nacl)#exit
R_Kyiv(conf)#ip access-list standard SNMP_ACL
R_Kyiv(config-std-nacl)#permit 192.168.254.0 0.0.0.31
```

```

R_Kyiv(config-std-nacl)#exit
R_Kyiv(conf)#snmp-server community SNMP_MONITOR_RO RO SNMP_ACL
R_Kyiv(conf)#snmp-server community SNMP_MANAGER_RW RW ADMIN_SNMP_ACL
R_Kyiv(conf)#snmp-server location Kyiv_LAN
R_Kyiv(conf)#snmp-server contact admin@kyiv.yavorenko.net
R_Kyiv(conf)#snmp-server host 192.168.254.3 version 2c SNMP_MONITOR_RO
R_Kyiv(conf)#end

```

Для кращих результатів у виявленні загроз, перебоїв та підвищення адміністративної стійкості мережі доцільно налаштувати моніторингові дані в комбінації з протоколом NetFlow 9 версії. Трафік з даного протоколу має більш розширені дані, ніж SNMP, що дозволить зробити більш глибокий аналіз поточного стану мережі. Для правильного функціонування потрібно налаштувати головний компонент – сенсор. В поточній мережі доцільно буде використати два сенсори для маршрутизаторів R_Core_1 та R_Core_3. Через перший маршрутизатор буде проходити весь трафік від мережі Internet, а через другий весь трафік усіх локальних мереж. Налаштування продемонстроване на базі маршрутизатора R_Core_3:

```

R_Core_3#configure terminal
R_Core_3(config)#ip flow-export destination 192.168.254.4 9996
R_Core_3(config)#ip flow-export version 9
R_Core_3(config)#ip flow-cache timeout active 1
R_Core_3(config)#ip flow-cache timeout inactive 15
R_Core_3(config)#ip flow-export source FastEthernet1/0
R_Core_3(config)#interface FastEthernet1/0
R_Core_3(config-if)#ip route-cache flow
R_Core_3(config)#interface Ethernet1/0
R_Core_3(config-if)#ip flow ingress
R_Core_3(config-if)#ip flow egress

```

```
R_Core_3(config)#interface Ethernet1/1
R_Core_3(config-if)#ip flow ingress
R_Core_3(config-if)#ip flow egress
R_Core_3(config)#interface Ethernet1/2
R_Core_3(config-if)#ip flow ingress
R_Core_3(config-if)#ip flow egress
R_Core_3(config)#interface Ethernet1/3
R_Core_3(config-if)#ip flow ingress
R_Core_3(config-if)#ip flow egress
R_Core_3(config-if)#end
```

Для кращого обліку використання мережевий ресурсів локальних мереж на маршрутизаторах доступу налаштовано моніторинг трафіку за протоколом IPFIX. Враховуючи, що вірогідність появи зловмисників саме в цих ділянках мережі за допомогою несанкціонованого доступу досить важливо моніторити трафік за покращеною версією протоколу NetFlow. Приклад налаштування точки спостереження IPFIX на маршрутизаторі R_Zhytomyr:

```
R_Zhytomyr#configure terminal
R_Zhytomyr(config)#flow exporter-map fem_ipfix
R_Zhytomyr(config-fem)#destination 192.168.254.4
R_Zhytomyr(config-fem)#source Ethernet0/0
R_Zhytomyr(config-fem)#transport udp 1025
R_Zhytomyr(config-fem)#exit
R_Zhytomyr(config)#version ipfix
R_Zhytomyr(config-fem-ver)#template data timeout 600
R_Zhytomyr(config-fem-ver)#options sampler-table
R_Zhytomyr(config-fem-ver)#end
```

Після реалізації налаштувань на пристроях створеної топології важливо перевірити працездатність мережі.

Перш за все, у створеній топології потрібно перевірити наявність наскрізного з'єднання між віддаленими вузлами мереж. Перевіряємо за допомогою команд `tracert` та `ping` (рис. 3.1 та 3.2).

```
C:\Documents and Settings\Admin>ping 192.168.111.1
Обмен пакетами с 192.168.111.1 по 32 байт:
Ответ от 192.168.111.1: число байт=32 время=80мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=74мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=53мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=49мс TTL=253

Статистика Ping для 192.168.111.1:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь).
Примерное время приема-передачи в мс:
  Минимальное = 49мсек, Максимальное = 80 мсек, Среднее = 64 мсек

C:\Documents and Settings\Admin>ping 192.168.1.1
Обмен пакетами с 192.168.1.1 по 32 байт:
Ответ от 192.168.1.1: число байт=32 время=157мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=49мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=45мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=50мс TTL=253

Статистика Ping для 192.168.1.1:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь).
Примерное время приема-передачи в мс:
  Минимальное = 45мсек, Максимальное = 157 мсек, Среднее = 75 мсек

C:\Documents and Settings\Admin>ping 192.168.112.11
Обмен пакетами с 192.168.112.11 по 32 байт:
Ответ от 192.168.112.11: число байт=32 время=108мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=138мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=68мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=86мс TTL=61

Статистика Ping для 192.168.112.11:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь).
Примерное время приема-передачи в мс:
  Минимальное = 68мсек, Максимальное = 138 мсек, Среднее = 100 мсек
```

Рисунок 3.1 – Перевірка зв'язку між PC_Zhytomyr_1 та R_Zhytomyr, R_Core_1, PC_Kyiv_3

```
C:\Documents and Settings\Admin>tracert 192.168.1.2
Трассировка маршрута к 192.168.1.2 с максимальным числом прыжков 30
  1    9 ms    22 ms    20 ms    192.168.111.1
  2   28 ms    31 ms    32 ms    192.168.111.1
  3   91 ms    73 ms    86 ms    192.168.1.2

Трассировка завершена.

C:\Documents and Settings\Admin>tracert 192.168.112.11
Трассировка маршрута к 192.168.112.11 с максимальным числом прыжков 30
  1    20 ms    21 ms    10 ms    192.168.111.1
  2    32 ms    53 ms    32 ms    192.168.111.1
  3    76 ms    53 ms    74 ms    192.168.112.2
  4    91 ms    86 ms    74 ms    192.168.112.11

Трассировка завершена.

C:\Documents and Settings\Admin>
```

Рисунок 3.2 – Перевірка зв'язку між PC_Zhytomyr та R_Core_2, PC_Kyiv_1

Для перевірки функціонування DHCP кінцеве устаткування налаштовано як DHCP-клієнти. Результат отримання пристроями IP-адрес наведено на рис. 3.3-3.5.

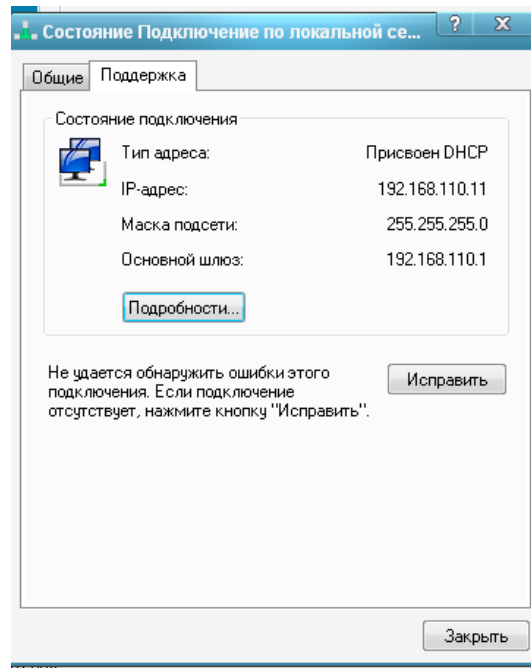


Рисунок 3.3 – Отримання IP-адреси клієнтом PC_Lviv_1

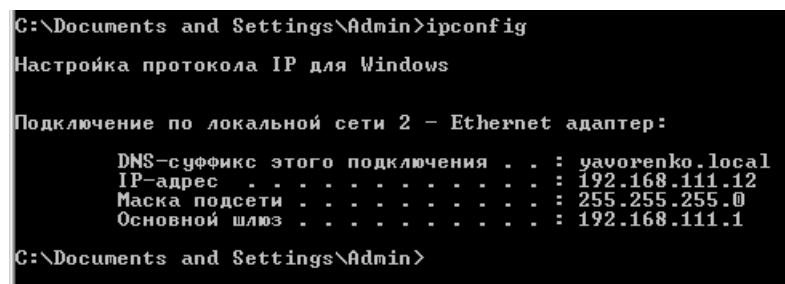


Рисунок 3.4 – Перевірка IP-адреси клієнтом PC_Zhytomyr_2

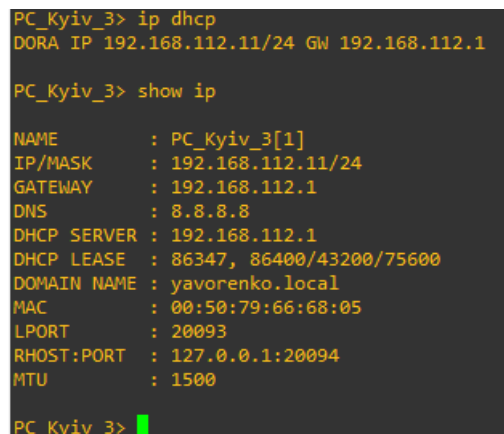


Рисунок 3.5 – Перевірка IP-адреси клієнтом PC_Kyiv_3

Для перевірки правильної роботи протоколу EIGRP виведено таблиці маршрутизації, топології та сусідів. Показано на основі маршрутизатора ядра R_Core_2. На рисунку 3.6 виведено таблицю маршрутизації. На рисунку 3.7 виведено таблицю сусідів.

```
R_Core_2#show ip route eigrp
 192.168.12.0/30 is subnetted, 1 subnets
D    192.168.12.0 [90/284160] via 192.168.1.3, 01:50:13, FastEthernet0/1
 192.168.13.0/30 is subnetted, 1 subnets
D    192.168.13.0 [90/284160] via 192.168.1.3, 01:50:05, FastEthernet0/1
D    192.168.110.0/24 [90/286720] via 192.168.1.3, 01:50:18, FastEthernet0/1
D    192.168.111.0/24 [90/286720] via 192.168.1.3, 02:29:48, FastEthernet0/1
 192.168.10.0/30 is subnetted, 1 subnets
D    192.168.10.0 [90/284160] via 192.168.1.3, 01:50:23, FastEthernet0/1
 192.168.11.0/30 is subnetted, 1 subnets
D    192.168.11.0 [90/284160] via 192.168.1.3, 03:01:34, FastEthernet0/1
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.20.0/24 is a summary, 03:01:36, Null0
D    192.168.113.0/24 [90/286720] via 192.168.1.3, 01:50:00, FastEthernet0/1
D    192.168.112.0/24 [90/286720] via 192.168.1.3, 01:50:10, FastEthernet0/1
D    192.168.254.0/24 [90/30720] via 192.168.20.2, 03:01:34, FastEthernet0/0
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.1.0/24 is a summary, 03:01:37, Null0
D*EX 0.0.0.0/0 [170/30720] via 192.168.1.1, 03:01:27, FastEthernet0/1
R_Core_2#
```

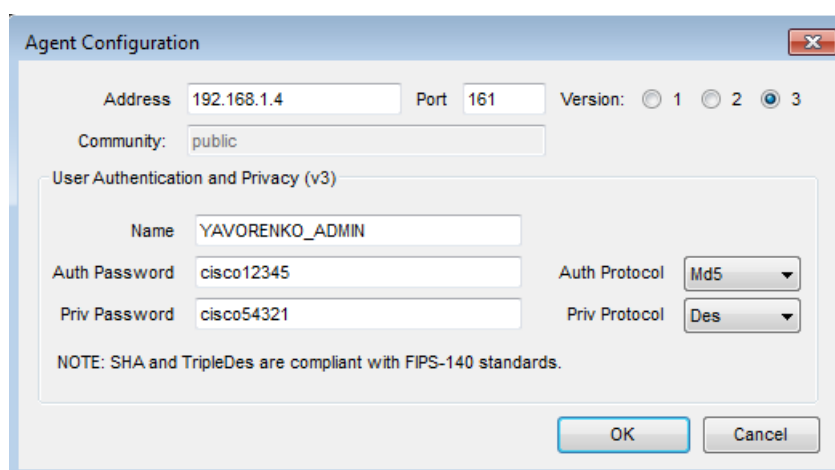
Рисунок 3.6 – Таблиця маршрутизації протоколу EIGRP на R_Core_2

```
R_Core_2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime    SRTT    RTO    Q    Seq
   (sec)                  (ms)
3   192.168.1.4              Fa0/1        14 02:46:23    27    200    0    14
2   192.168.1.1              Fa0/1        11 03:02:10    34    204    0    17
1   192.168.1.3              Fa0/1        10 03:02:12    37    222    0    49
0   192.168.20.2             Fa0/0        12 03:02:12    39    234    0    11
R_Core_2#
```

Рисунок 3.7 – Таблиця маршрутизації протоколу EIGRP на R_Core_2

Для перевірки налаштувань SNMP-серверів використано наступні технології: програмні додатки для ОС Windows PowerSNMP Free Manager від Dart [14] та MIB Browser Free Tool від ManageEngine [15], для ОС Linux утиліту SNMP-Check. Моніторинг мереж більш зручний у першому додатку для ОС Windows, крім того він підходить для протоколу третьої версії. Для початку потрібно додати SNMP-агенти до NMS. Для цього потрібно ввести IP-адресу, порт, обрати версію та ввести параметри аутентифікації протоколу (рис. 3.8). Якщо дані введено вірно – додаток виведе пристрій з мінімальними відомостями про нього у попередньому перегляді (рис. 3.9). Після цього пристрій можна додати до групи агентів, що дозволить його подальший моніторинг (рис. 3. 10). За допомогою OID протоколу можна отримати

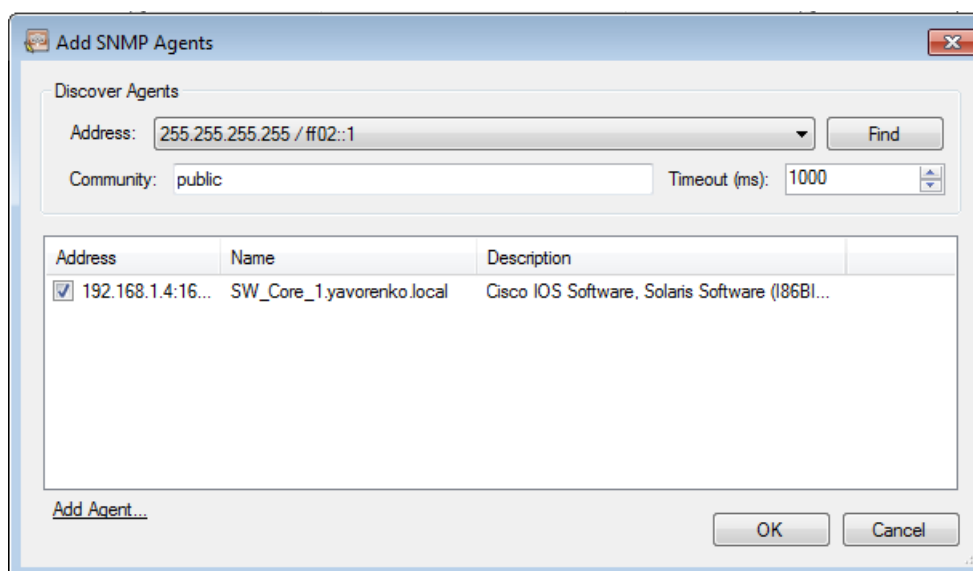
різні відомості про пристрій, наприклад його локацію(рис. 3. 11). Окрім цього, додаток дозволяє виводити великі об'єми значень у вигляді таблиць. Для прикладу виведено таблицю IP-адресації пристрою R_Lviv (рис. 3.12). Для зручності є можливість стежити за змінами значень OID та додати їх на головний екран (рис. 3. 13 - 3. 14). Також додаток дозволяє стежити за пропускнуою здатністю мережі, що також є досить зручною опцією, оскільки швидкість мережі – один з найважливіших моментів (рис. 3. 15).



The 'Agent Configuration' dialog box contains the following fields and controls:

- Address: 192.168.1.4
- Port: 161
- Version: Radio buttons for 1, 2, and 3 (3 is selected).
- Community: public
- User Authentication and Privacy (v3) section:
 - Name: YAVORENKO_ADMIN
 - Auth Password: cisco12345
 - Auth Protocol: Md5 (dropdown)
 - Priv Password: cisco54321
 - Priv Protocol: Des (dropdown)
- NOTE: SHA and TripleDes are compliant with FIPS-140 standards.
- Buttons: OK, Cancel

Рисунок 3.8 – Вікно додавання нового агента



The 'Add SNMP Agents' dialog box contains the following fields and controls:

- Discover Agents section:
 - Address: 255.255.255.255 / ff02::1 (dropdown)
 - Find button
 - Community: public
 - Timeout (ms): 1000 (spinner)
- Table with 3 columns: Address, Name, Description.

Address	Name	Description
☒ 192.168.1.4:16...	SW_Core_1.yavorenko.local	Cisco IOS Software, Solaris Software (I86BI...
- Buttons: Add Agent..., OK, Cancel

Рисунок 3.9 – Попередній перегляд агентів, що додаються

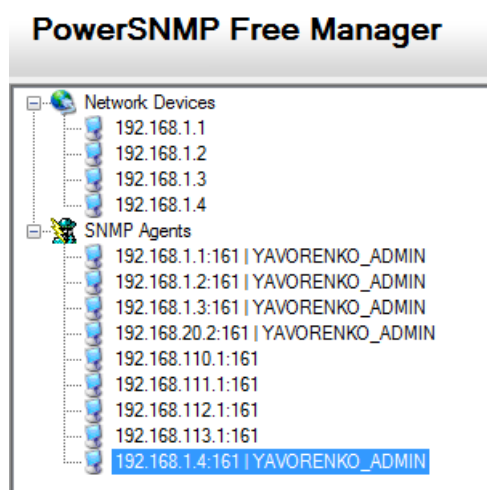


Рисунок 3.10 – Список доданих SNMP-агентів

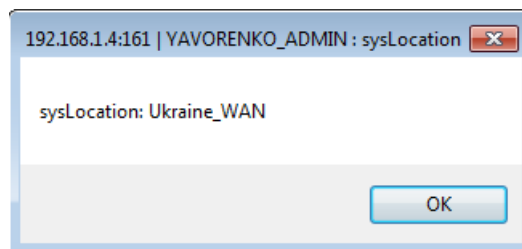


Рисунок 3.11 – Виведення інформації з агента за допомогою GET-запиту

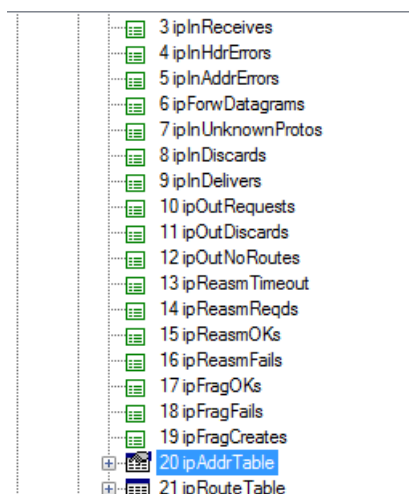


Рисунок 3.12 – Список доступних об'єктів у human-readable форматі замість OID

ipAddrTable					
ipAdEntAddr	ipAdEntIfIndex	ipAdEntNetMask	ipAdEntBcastAddr	ipAdEntReasmMaxSize	
192.168.10.2	1	255.255.255.252	1	18024	
192.168.110.1	2	255.255.255.0	1	18024	

Рисунок 3.13 – Виведення таблиці IP-адресації на R_Lviv за допомогою GET-запиту

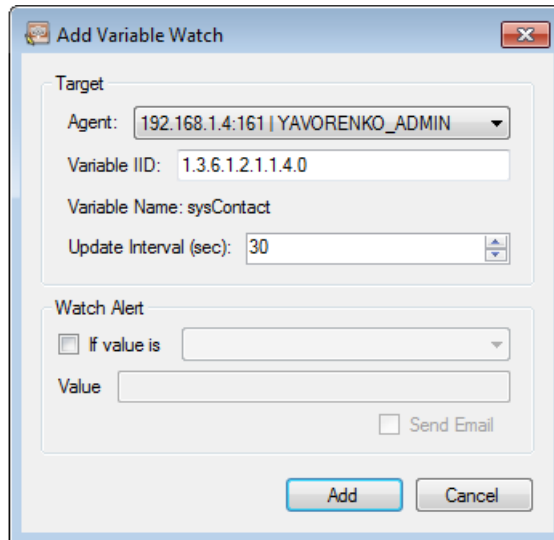


Рисунок 3.14 – Додавання змінної для постійного моніторингу

Device Address	Variable/IID	Value
Variable Watches		
192.168.1.1:161	sysName (1.3.6.1.2.1.1.5.0)	R_Core_1.yavorenko.local
192.168.1.1:161	sysUpTime (1.3.6.1.2.1.1.3.0)	1167866
192.168.1.4:161	sysName (1.3.6.1.2.1.1.5.0)	SW_Core_1.yavorenko.local
192.168.1.4:161	sysUpTime (1.3.6.1.2.1.1.3.0)	1459414
192.168.1.4:161	sysLocation (1.3.6.1.2.1.1.6.0)	Ukraine_WAN
192.168.1.4:161	sysContact (1.3.6.1.2.1.1.4.0)	admin@yavorenko.local.net

Рисунок 3.15 – Список поточних змінних, які моніторяться

Ping Watches	
192.168.1.1	54 ms
192.168.1.2	31 ms
192.168.1.3	48 ms
192.168.1.4	37 ms

Рисунок 3.16 – Список пристроїв, у яких тестується пропускна здатність (затримка під час передачі трафіку)

Для реалізації менеджменту використано інший додаток – ManageEngine MIB Browser Free Tool. Процес налаштування схожий з попереднім додатком. Для початку потрібно додати SNMP-агент, записавши його IP-адресу, порт, параметри аутентифікації та рівень захисту хоста (рис. 3. 17). В результаті до бази користувачів та агентів буде додано новий запис (рис. 3. 18). Після цього з’являється можливість повного керування агентом за допомогою SET-запитів, обравши OID та записавши нове значення параметру (рис. 3. 19 – 3. 20)

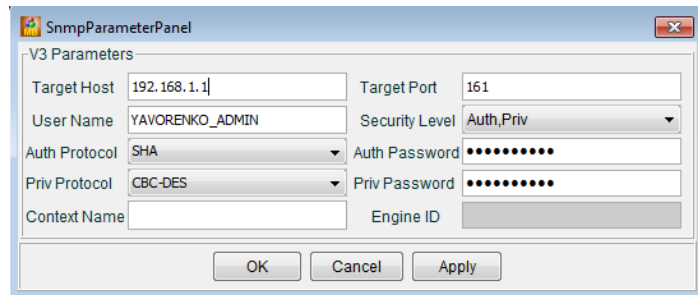


Рисунок 3.17 – Налаштування нового SNMPv3-агента

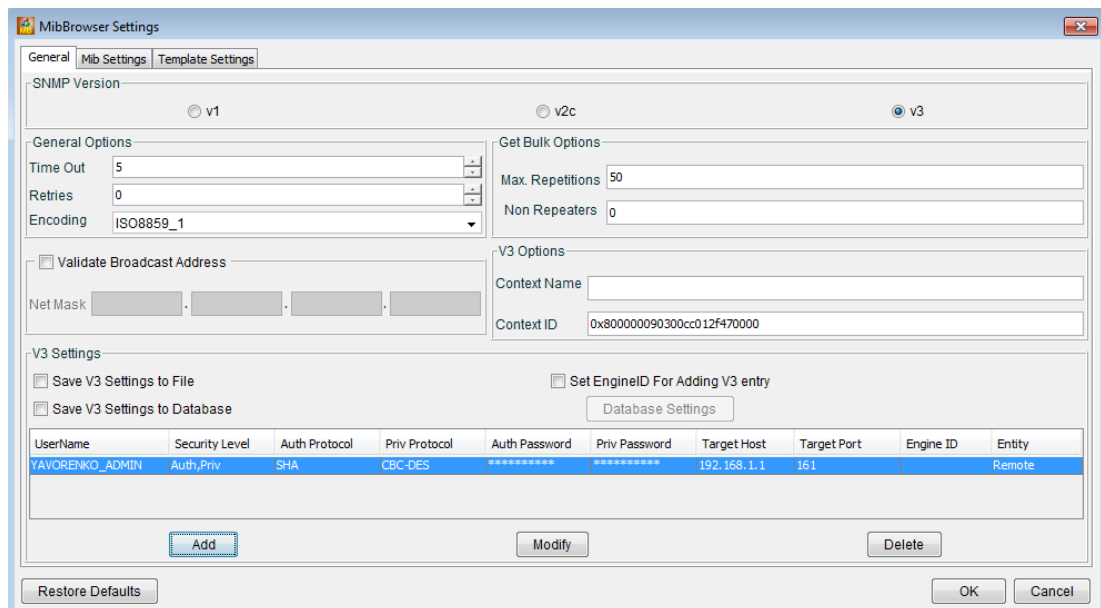


Рисунок 3.18 – Результат додавання нового SNMPv3-агента

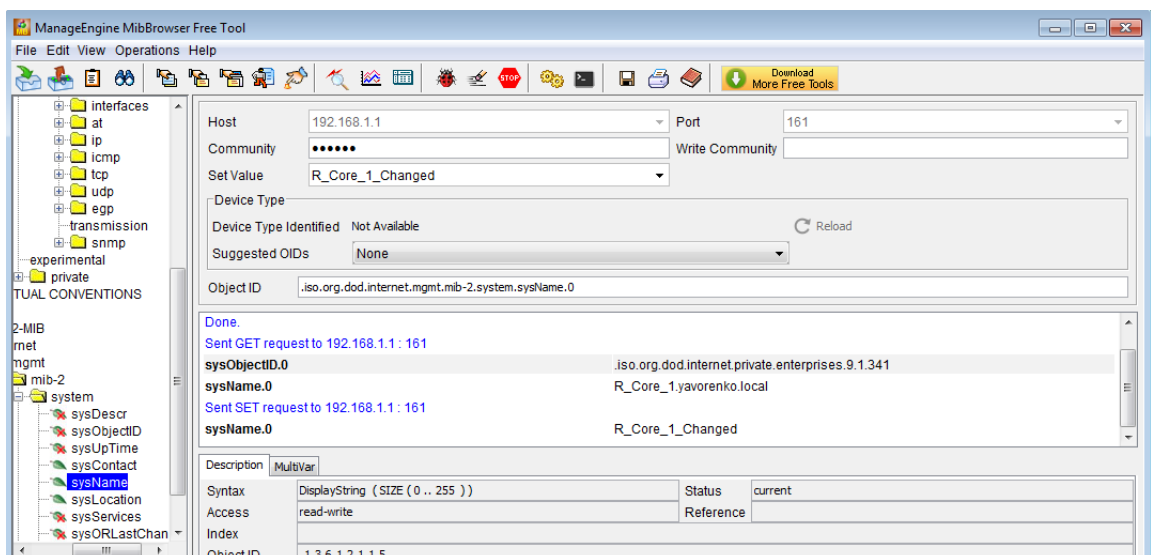


Рисунок 3.19 – Результат виконання GET та SET-запитів до агента

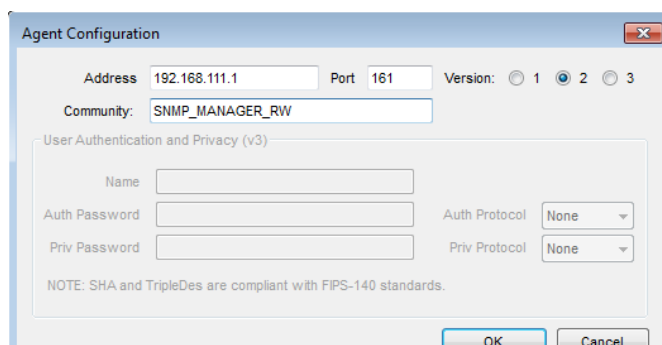
```

R_Core_1#
*Mar  1 03:20:50.831: %SYS-5-CONFIG_I: Configured from 192.168.254.3 by snmp
R_Core_1#
R_Core_1_Changed#
R_Core_1_Changed#

```

Рисунок 3.20 – Результат менеджменту R_Core_1 за протоколом SNMP

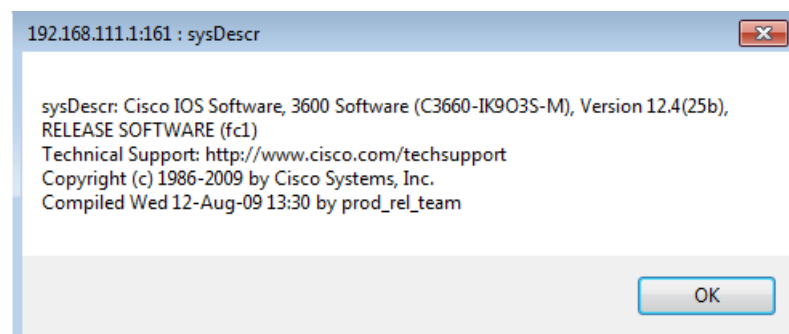
Для менш критичних пристроїв налаштовано протокол SNMPv2c з використанням рядків спільнот, як механізму аутентифікації. За рахунок розповсюдженості даної версії з'явилася велика кількість зручних рішень для моніторингу та менеджменту. Процес додавання нових агентів також спрощено. Для цього потрібно вказати IP-адресу, версію та рядок спільноти (рис. 3. 21). В результаті з'являється можливість моніторингу та менеджменту, ідентична третій версії протоколу (рис 3. 22). Для реалізації менеджменту потрібно вказати рядки спільнот для різних режимів – read та write, або тільки write (рис 3. 23 – 3. 24).



The 'Agent Configuration' dialog box contains the following fields and options:

- Address:** 192.168.111.1
- Port:** 161
- Version:** Radio buttons for 1, 2 (selected), and 3.
- Community:** SNMP_MANAGER_RW
- User Authentication and Privacy (v3):**
 - Name:** (empty text box)
 - Auth Password:** (empty text box)
 - Priv Password:** (empty text box)
 - Auth Protocol:** None (dropdown menu)
 - Priv Protocol:** None (dropdown menu)
- NOTE:** SHA and TripleDes are compliant with FIPS-140 standards.
- Buttons:** OK and Cancel.

Рисунок 3.21 – Додавання нового агента за протоколом SNMPv2c



The dialog box displays the following information:

```

192.168.111.1:161 : sysDescr

sysDescr: Cisco IOS Software, 3600 Software (C3660-IK9O3S-M), Version 12.4(25b),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 12-Aug-09 13:30 by prod_rel_team

```

Button: OK

Рисунок 3.22 – Виведення значення об'єкту sysDescr

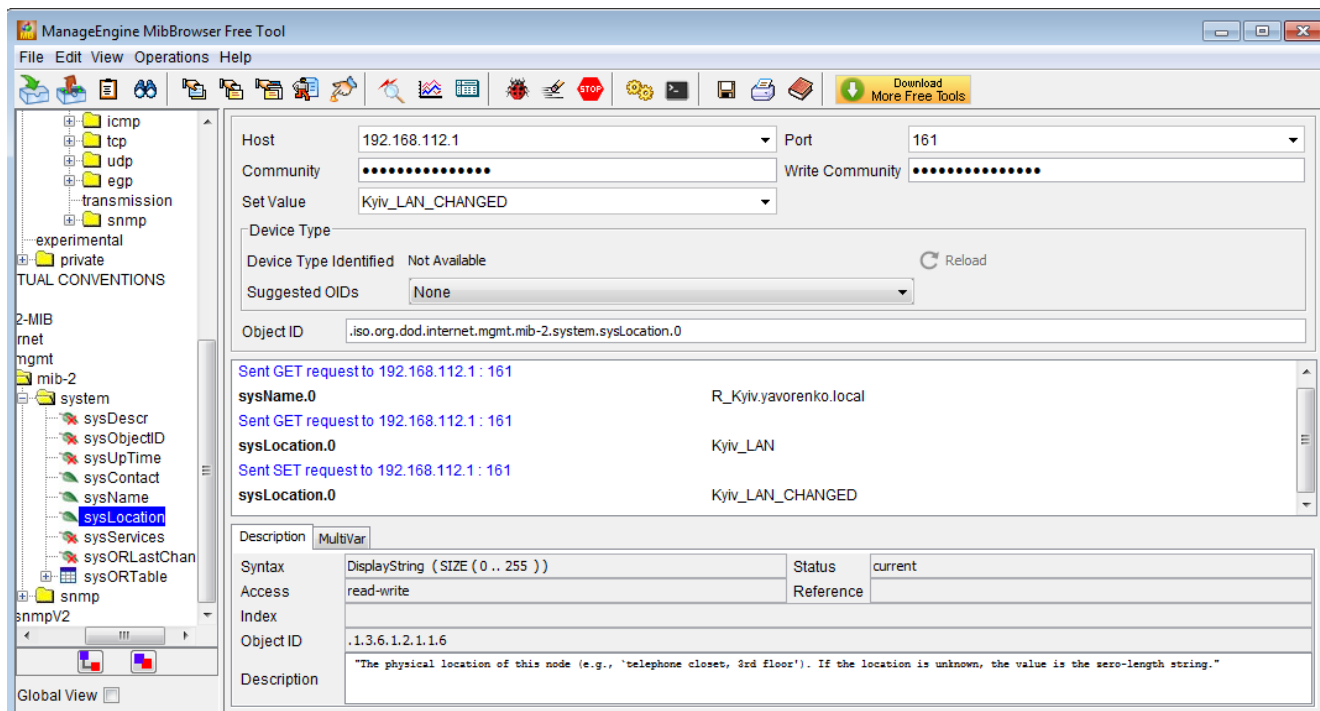


Рисунок 3.23 – Виведення та зміна значення об'єкту sysLocation

```
R_Kyiv#
*Mar 1 02:55:10.375: %SYS-5-CONFIG_I: Configured from 192.168.254.3 by snmp
R_Kyiv#show snmp location
Kyiv_LAN_CHANGED
R_Kyiv#
```

Рисунок 3.24 – Результат зміни значення об'єкту sysLocation на R_Kyiv

На ОС Linux чудовим інструментом для моніторингу агентів є утиліта SNMP-Check, яка дозволяє виводити важливі об'єкти за протоколом версії 2с у зручному вигляді. В якості параметрів лише потрібно передати порт, версію протоколу, рядок спільноти та IP-адресу (рис. 3. 25 – 3. 26).

```

(kali@kali)-[~]
└─$ snmp-check -p 161 -v 2c -c SNMP_MONITOR_RO 192.168.112.1
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.112.1:161 using SNMPv2c and community 'SNMP_MONITOR_RO'

[*] System information:

Host IP address      : 192.168.112.1
Hostname             : R_Kyiv.yavorenko.local
Description          : Cisco IOS Software, 3600 Software (C3660-IK903S-M),
d Wed 12-Aug-09 13:30 by prod_rel_team
Contact              : admin@kyiv.yavorenko.net
Location             : Kyiv_LAN
Uptime snmp          : noSuchObject
Uptime system        : 02:56:17.41
System date          : -

[*] Network information:

IP forwarding enabled : yes
Default TTL           : 255
TCP segments received : 0
TCP segments sent     : 0
TCP segments retrans  : 0
Input datagrams       : 3402
Delivered datagrams   : 3279
Output datagrams      : 3810

[*] Network interfaces:

Interface            : [ up ] FastEthernet0/0
Id                   : 1
Mac Address          : cc:08:2f:b8:00:00
Type                 : ethernet-csmacd
Speed                : 100 Mbps
MTU                  : 1500
In octets             : 191637
Out octets            : 310282

Interface            : [ up ] FastEthernet0/1
Id                   : 2
Mac Address          : cc:08:2f:b8:00:01
Type                 : ethernet-csmacd
Speed                : 100 Mbps
MTU                  : 1500
In octets             : 405999
Out octets            : 249731

```

Рисунок 3.25 – Результат виведення інформації утилітою SNMP-Check (частина)

```

[*] Network IP:

Id      IP Address      Netmask      Broadcast
1       192.168.12.2      255.255.255.252  1
2       192.168.112.1    255.255.255.0   1

[*] Routing information:

Destination      Next hop      Mask          Metric
0.0.0.0          192.168.12.1  0.0.0.0       33280
192.168.1.0      192.168.12.1  255.255.255.240 30720
192.168.10.0     192.168.12.1  255.255.255.252 284160
192.168.11.0     192.168.12.1  255.255.255.252 284160
192.168.12.0     192.168.12.2  255.255.255.252 0
192.168.13.0     192.168.12.1  255.255.255.252 284160
192.168.20.0     192.168.12.1  255.255.255.0   33280
192.168.110.0    192.168.12.1  255.255.255.0   286720
192.168.111.0    192.168.12.1  255.255.255.0   286720
192.168.112.0    192.168.112.1 255.255.255.0   0
192.168.113.0    192.168.12.1  255.255.255.0   286720
192.168.254.0    192.168.12.1  255.255.255.0   35840

[*] Listening UDP ports:

Local address      Local port
192.168.12.2       162
192.168.12.2       57001
192.168.112.1      67
192.168.112.1      161

[*] File system information:

Index              : noSuchObject
Mount point        : noSuchObject
Access             : noSuchObject
Bootable           : noSuchObject

```

Рисунок 3.26 – Результат виведення інформації утилітою SNMP-Check (частина)

Для моніторингу мережі на базі протоколу NetFlow обрано програмне забезпечення від компанії ManageEngine – NetFlow Analyzer, яке слугує як в якості колектора, так і аналізатора даних. Для початку потрібно додати сенсори мережі за допомогою налаштувань програми. Для цього потрібно вказати IP-адресу, обрати протокол віддаленого доступу, вказати аутентифікаційні дані до пристрою мережі та його конфігураційних рівнів, також вказати команди доступу до устаткування (рис. 3.27). В результаті успішного додавання додаток сповіщує про закінчення команди (рис. 3.28).

NetFlow Analyzer

Dashboard Inventory WLC Security DPI NCM IPAM IPSLA Alarms Maps Reports Settings

General Settings Discovery Monitoring Tools NetFlow NCM OpUtils ITOM Agents

Discovery

Export Flow

Export Cloud Flow

NCM Discovery

Discovery Report

Credentials

Inventory Updater

Non Inventoried Devices

Predefined Flow Export Custom Flow Export Network Packet Sensor

Export flow using the predefined template in NetFlow Analyzer.

Hostname/ IP Address * 192.168.10.1

Select SNMP credential * Public (SNMP v1/v2)

Protocol ? ☐ Telnet ☒ SSH

Login Name * admin

Password *

Prompt * >,\$,#

Enable Command enable

Enable UserName admin

Enable Password

Enable Prompt >,\$,#

Рисунок 3.27 – Налаштування нового сенсору для експорту потоку

Test Credentials

Ping Test ✓

Telnet/SSH Test ✓

SNMP Test ✓

Commands Availability ✓

Рисунок 3.28 – Результат успішного додавання сенсору

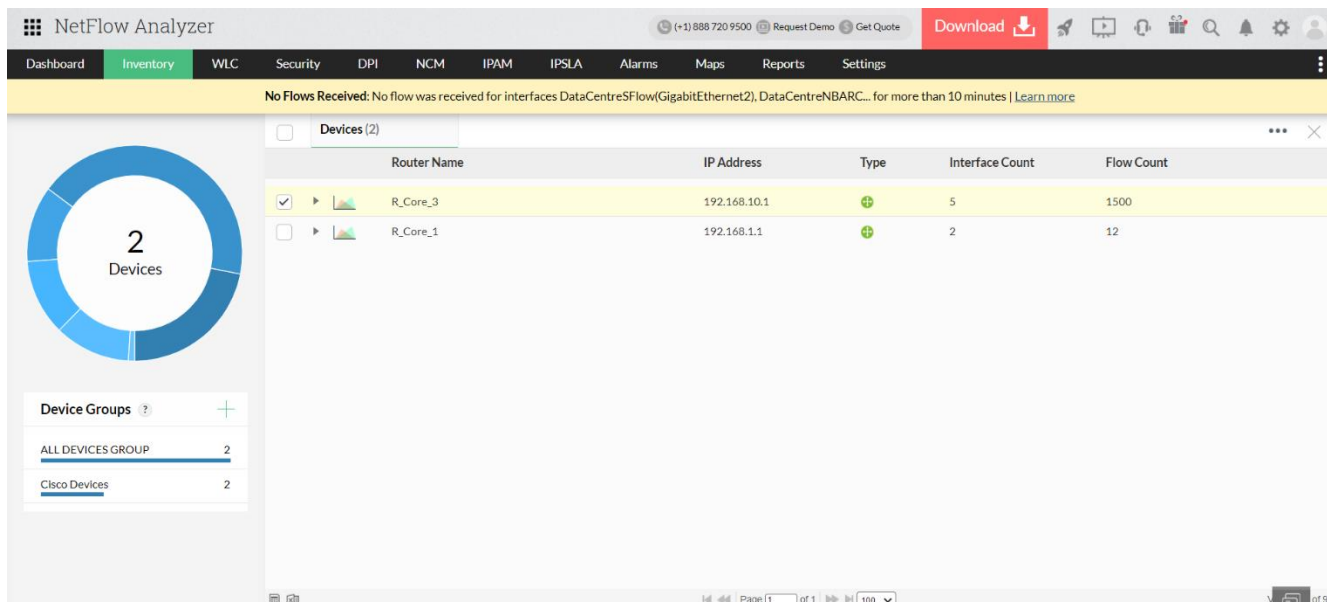


Рисунок 3.29 – Додані до аналізатора пристрої мережі

В результаті налаштування аналізатора та отримання доступу до пакетів з сенсорів мережі адміністратору відкривається доступ до деталізованих графіків щодо даних мережі. Головна сторінка додатку налаштована для відображення стану поточних пристроїв мережі та їх інтерфейсів (3.30). У випадку, якщо якийсь із пристроїв мережі втратить робоздатність додаток терміново відправить сповіщення, що дозволить швидко відреагувати на такий інцидент.

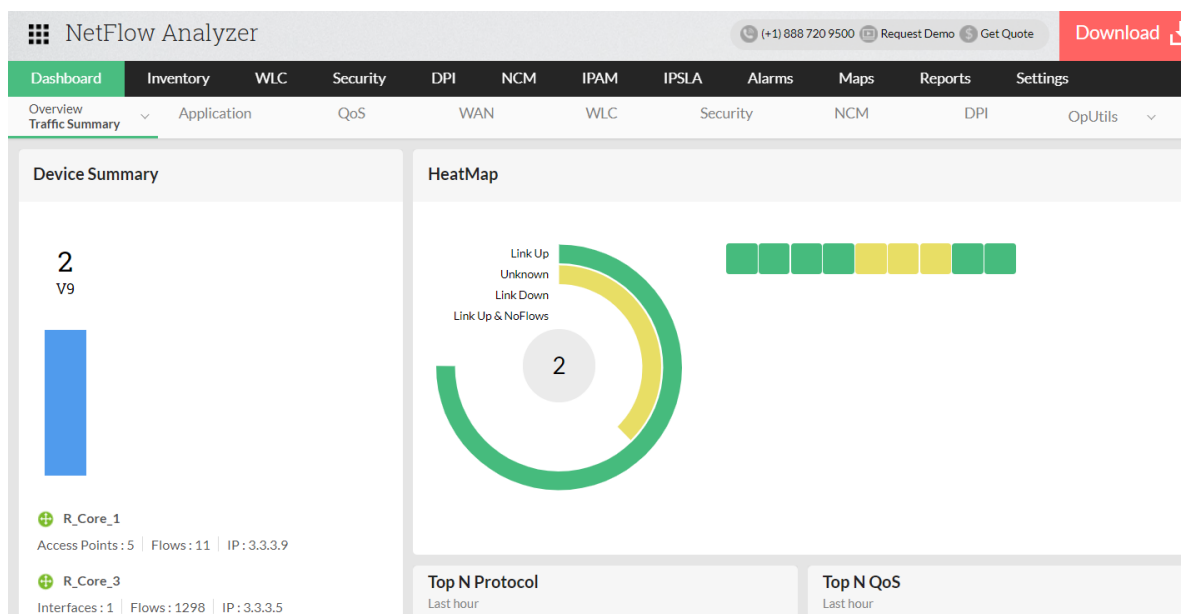


Рисунок 3.30 – Графіки робоздатності пристроїв та їх інтерфейсів

Для відображення проблем з безпекою певного пристрою реалізовано великий банер з сповіщенням і можливістю більше детального огляду цієї проблеми (рис. 3.31). Переглянути звіт щодо трафіку певного протоколу та його кількості можна переглянути на сегментній датаграмі (рис 3.32). Також важливим є графік отримання аналізатором пакетів за протоколом NetFlow, що дасть можливість попередити проблеми у функціонуванні даного протоколу (рис 3.33).

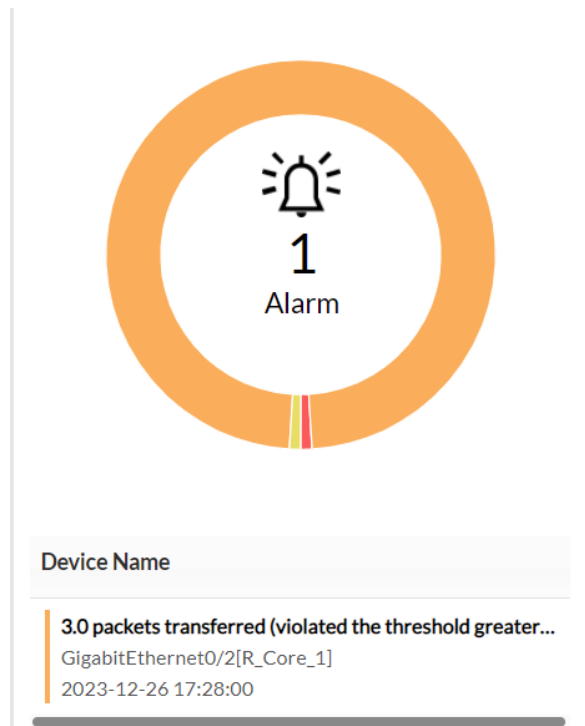


Рисунок 3.31 – Сповіщення-банер щодо проблем з безпекою

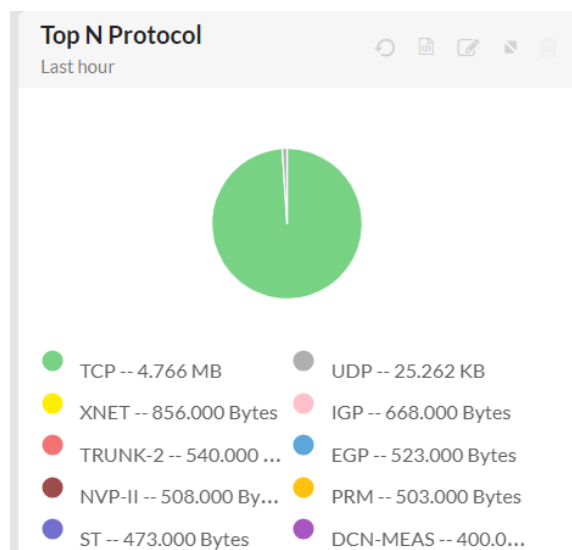


Рисунок 3.32 – Звіт кількості трафіку певних протоколів

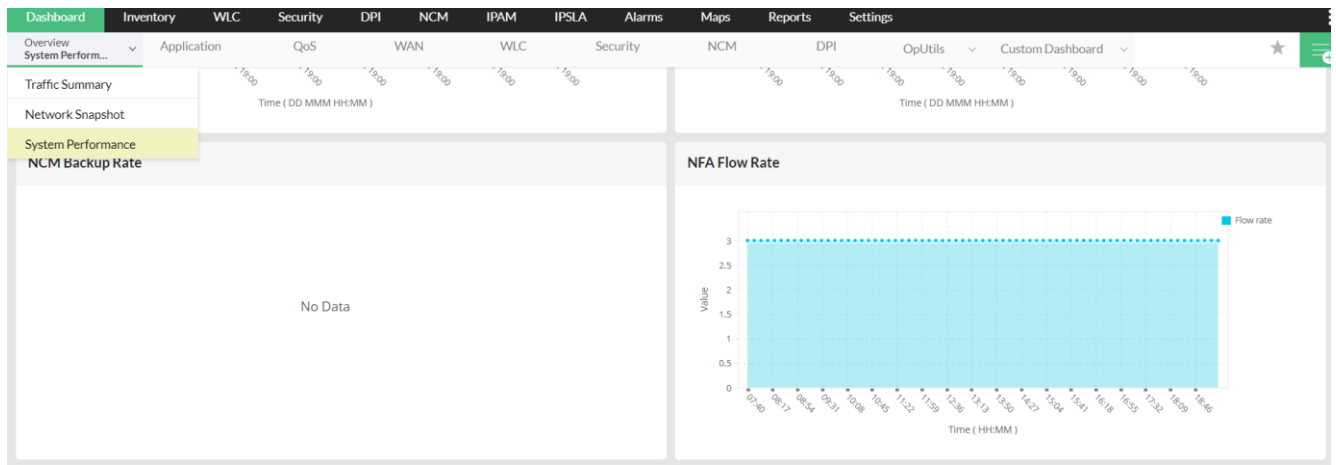


Рисунок 3.33 – Графік трансферингу трафіку за протоколом NetFlow

3.2 Дослідження рівня захищеності підсистеми моніторингу

Після налаштування мережі та перевірки правильності функціонування пристроїв важливо провести аналіз безпеки мережі. Один із найефективніших інструментів для цього завдання - Kali Linux.

Kali Linux є операційною системою Linux, спеціально розробленою для проведення цифрової криміналістичної експертизи та тестування на проникнення [16]. Цей дистрибутив підтримується та фінансується Offensive Security.

У Kali Linux налічується близько 600 програм (інструментів) для проведення тестів на проникнення, включаючи такі, як Armitage (графічний інструмент для керування кібератаками), Nmap (сканер портів), Wireshark (сніфер пакетів), Metasploit (фреймворк для тестування на проникнення), John the Ripper (утиліта для злому паролів), sqlmap (автоматична ін'єкція SQL та інструмент захоплення баз даних), Aircrack-ng (набір програм для тестування на проникнення бездротових локальних мереж), Burp Suite і сканери безпеки веб-додатків OWASP ZAP, і так далі.

На першому етапі тестування проводиться аналіз відкритих портів мережі, щоб визначити можливість здійснення атак на систему. Для цього використовується утиліта nmap. Було перевірено відкриті UDP та TCP-порти на маршрутизаторі доступу R_Lviv (див. рис. 3.27 – 3.28). Один з портів, який може бути цікавим для зловмисника, - це порт 161, який використовується протоколом SNMP. Отри-

мання інформації з цього порту може дозволити проводити різноманітні маніпуляції. Крім того, при невірному налаштуванні протоколу хакер може змінити дані пристрою та перенаправити трафік на свою робочу станцію, що може призвести до повного контролю над мережею.

З результатів сканування видно, що пристрій використовує 3-тю версію протоколу SNMP, хоча насправді на пристрої налаштована версія 2с. Ця версія використовує рядки спільноти для аутентифікації в різних режимах роботи. Тому розумно перевірити можливість зламу рядка спільноти за допомогою атаки грубої сили з використанням заготовленого словника [17], який містить найпоширеніші рядки спільноти (див. рис. 3.29).

```
(kali@kali)-[~]
└─$ sudo nmap 192.168.110.1 -Pn -sU -sV
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-21 14:41 EDT
Nmap scan report for 192.168.110.1
Host is up (0.096s latency).
Not shown: 996 filtered ports
PORT      STATE      SERVICE      VERSION
67/udp    open|filtered dhcpd
161/udp    open      snmp         Cisco SNMP service; ciscoSystems SNMPv3 server
162/udp    open|filtered snmptrap
4500/udp   open|filtered nat-t-ike

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.63 seconds
```

Рисунок 3.34 – Сканування UDP-портів за допомогою nmap

```
(kali@kali)-[~]
└─$ sudo nmap 192.168.110.1 -Pn -sV
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-21 14:44 EDT
Nmap scan report for 192.168.110.1
Host is up (0.089s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE      VERSION
23/tcp    open      telnet       Cisco router telnetd
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

Рисунок 3.35 – Сканування TCP-портів за допомогою nmap

```
(kali@kali)-[~]
└─$ sudo onesixtyone -c common-community-strings.txt -p 161 192.168.110.1
Scanning 1 hosts, 121 communities

(kali@kali)-[~]
└─$
```

Рисунок 3.36 – Результат виконання атаки грубої сили на SNMP-сервер

З результату, отриманого після виконання брут-форс атаки, зроблено висновок, що SNMP-сервер досить надійно захищений та можливість його зламу не висока. Крім того, на більш критичних пристроях налаштовано третю версію протоколу, яка “з коробки” вже має гарний захист та шифрування. Крім цього, під час проведення атак сервер отримує діагностичну інформацію щодо підозрілих пакетів (рис. 3.30), що дає змогу адміністратору мережі вчасно зреагувати та заблокувати робочу станцію зловмисника.

```
R_Lviv#
*Mar 1 02:06:52.983: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x83951194(22075840), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:14:30.183: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x911C1194(243453588), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:16:21.339: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x911D1194(243460124), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:17:29.471: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x1000(4096), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:18:59.915: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x21D8B76(35490678), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:20:19.911: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x10002(65538), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:21:39.595: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x1B00003D(452984895), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:23:21.111: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x3CDE39A1(102119675), srcaddr=192.168.254.4
```

Рисунок 3.37 – Виведення діагностичної інформації на R_Lviv

Ще однією потенційно вразливою частиною мережі є протокол DHCP. У випадку відсутності захисту від атак на цей протокол, зловмисник може здійснювати різновиди атак, такі як DHCP-starvation та підміна за допомогою DHCP Rogue Server. Для перевірки цієї гіпотези було проведено тестову атаку на підміну DHCP-сервера за допомогою Metasploit.

Спочатку були визначені параметри майбутнього DHCP-сервера, після чого він був запущений у мережі, яка використовується для моніторингу топології (див. рис. 3.31). Після запуску сервера на одній з робочих станцій LAN була проведена налаштування IP-адресації через протокол DHCP (див. рис. 3.32). Під час обміну трафіком були перехоплені пакети за допомогою сніфера Wireshark, які містили інформацію, надіслану з підставного сервера зловмисника (див. рис. 3.33). Також під час атаки було отримано діагностичну інформацію щодо підозрілих пакетів (див. рис. 3.34), що надає можливість реагувати своєчасно, але, на жаль, не є ефективним

варіантом стримування. Крім того, внаслідок проведення атаки, LAN втрачає можливість обміну інформацією через невірні адреси, отримані від підставного сервера (див. рис. 3.35).

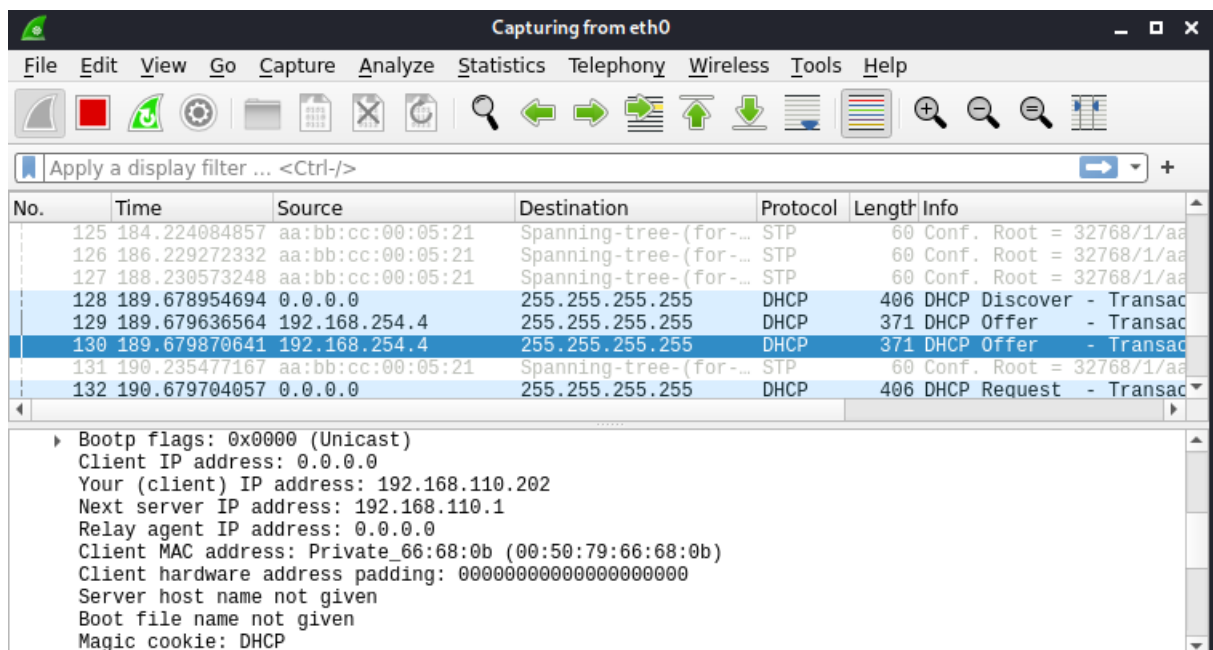
```
msf6 auxiliary(server/dhcp) > set srvhost 192.168.110.1
srvhost => 192.168.110.1
msf6 auxiliary(server/dhcp) > set netmask 255.255.255.0
netmask => 255.255.255.0
msf6 auxiliary(server/dhcp) > set DHCPSTART 192.168.110.201
DHCPSTART => 192.168.110.201
msf6 auxiliary(server/dhcp) > set DHCPEND 192.168.110.210
DHCPEND => 192.168.110.210
msf6 auxiliary(server/dhcp) > exploit
[*] Auxiliary module running as background job 1.

[*] Starting DHCP server ...
msf6 auxiliary(server/dhcp) > █
```

Рисунок 3.38 – Створення DHCP-серверу для підміни у Metasploit

```
PC1> ip dhcp
DORA IP 192.168.110.202/24 GW 192.168.110.1
PC1> █
```

Рисунок 3.39 – Результат отримання IP-адреси однією з станцій мережі



No.	Time	Source	Destination	Protocol	Length	Info
125	184.224084857	aa:bb:cc:00:05:21	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/aa
126	186.229272332	aa:bb:cc:00:05:21	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/aa
127	188.230573248	aa:bb:cc:00:05:21	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/aa
128	189.678954694	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transac
129	189.679636564	192.168.254.4	255.255.255.255	DHCP	371	DHCP Offer - Transac
130	189.679870641	192.168.254.4	255.255.255.255	DHCP	371	DHCP Offer - Transac
131	190.235477167	aa:bb:cc:00:05:21	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/1/aa
132	190.679704057	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transac

▶ Bootp flags: 0x0000 (Unicast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 192.168.110.202
 Next server IP address: 192.168.110.1
 Relay agent IP address: 0.0.0.0
 Client MAC address: Private_66:68:0b (00:50:79:66:68:0b)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP

Рисунок 3.40 – Перехоплений пакет DHCP Offer

```

R_MGMT#
*Mar 1 05:10:59.142: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0xF3121194(4078047636), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:12:01.274: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x1000(4096), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:13:30.230: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x2000000(33554432), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:14:30.334: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x303A0201(809107969), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:15:33.642: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x1E000130(503316784), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:16:37.030: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x405000(4214784), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:18:01.126: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x2E62197D(778180989), srcaddr=192.168.254.4
R_MGMT#

```

Рисунок 3.41 – Виведення діагностичної інформації на R_MGMT

```

(kali@kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
43 packets transmitted, 0 received, 100% packet loss, time 43182ms

```

Рисунок 3.42 – Спроба інформаційного обміну після проведення атаки

Також, суттєвим ризикованим елементом в мережі є віддалений доступ через протокол Telnet. Цей протокол не передбачає використання шифрування або перевірки достовірності даних [18], тому він стає вразливим перед різними атаками на його транспорт, а саме протокол TCP. Крім того, на даному етапі на пристроях не налаштовані механізми авторизації та аутентифікації, що відкриває можливість зломиснику, як тільки він отримає доступ до пристрою, виконувати різноманітні команди та змінювати налаштування мережі. Це представляє серйозну проблему безпеки. Ключово важливо використовувати більш захищений протокол віддаленого доступу та налагоджувати паролі на пристроях мережі.

```

(kali@kali)-[~]
$ telnet -a 192.168.110.1
Trying 192.168.110.1 ...
Connected to 192.168.110.1.
Escape character is '^]'.

Password required, but none set
Connection closed by foreign host.

(kali@kali)-[~]
$

```

Рисунок 3.43 – Спроба підключення за протоколом Telnet до R_Lviv

3.3 Налагодження засобів захисту та дослідження стійкості системи моніторингу

Під час аналізу, проведеного в попередньому розділі, були виявлені критичні точки у захисті мережі, для яких належить налаштувати заходи безпеки. Після цього важливо оцінити стійкість мережі та ефективність вжитих заходів.

Однією з ключових проблем у сфері захисту були потенційні атаки на протокол DHCP [19]. Таким чином, пріоритетом стає забезпечення безпеки цього сегмента мережі. Для досягнення цієї мети рекомендується налаштувати функцію DHCP Snooping на комутаторах мережі. Важливою перевагою такого заходу є те, що DHCP Snooping регулює лише повідомлення DHCP і не має прямого впливу на трафік користувачів або інші протоколи. Для коректного конфігурування слід вказати довірені порти (призначені для комутаторів або DHCP-серверів) та недовірені порти (призначені для клієнтських пристроїв). Нижче представлено приклад конфігурації на SW_MGMT:

```
SW_MGMT#configure terminal
SW_MGMT(config)#int range eth0/1-3
SW_MGMT(config-if)#ip dhcp snooping trust
SW_MGMT(config-if)#ip dhcp snooping limit rate 256
SW_MGMT(config-if)#end
SW_MGMT#write
```

Після встановлення захисту від атак на DHCP було проведено повторну спробу підміни DHCP-сервера. Спочатку була отримана діагностична інформація відносно роботи DHCP Snooping на комутаторі (рис. 3.37). Після створення фіктивного сервера на одній із робочих станцій було спробувано отримати IP-адресу (рис. 3.38), проте це не вдалося, оскільки обмін DHCP-пакетами з ненадійними портами був заборонений. Таким чином, мережа залишається захищеною від атак на цей протокол.

```

SW_MGMT#show ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

```

Interface	Trusted	Allow option	Rate limit (pps)
Ethernet0/0	yes	yes	256
Custom circuit-ids:			
Ethernet0/1	yes	yes	256
Custom circuit-ids:			
Ethernet0/2	yes	yes	256
Custom circuit-ids:			
Interface	Trusted	Allow option	Rate limit (pps)
Ethernet0/3	yes	yes	256
Custom circuit-ids:			

Рисунок 3.44 – Виведення статистичних даних щодо функціонування DHCP Snooping

```

PC1> ip dhcp
DDD
Can't find dhcp server

```

Рисунок 3.45 – Спроба отримання IP-адреси з підставного серверу після налаштування DHCP Snooping

Для забезпечення безпеки таблиць маршрутизації рекомендується налаштувати аутентифікацію протоколу EIGRP. Без відповідних налаштувань, при з'яві невідомого маршрутизатора в мережі, де функціонує протокол EIGRP з тим самим номером автономної системи, пристрій почне обмінюватися таблицею маршрутизації з маршрутизатором зломисника, що може призвести до серйозних наслідків. Нижче подано приклад конфігурації на R_Kharkiv:

```

R_Kharkiv(config)#key chain EIGRP_KeyChain_Protected
R_Kharkiv(config-keychain)#key 1
R_Kharkiv(config-keychain-key)#key-string 123qwerty123
R_Kharkiv(config-keychain-key)#exit
R_Kharkiv(config-keychain)#exit

```

```
R_Kharkiv(config)#interface fastEthernet 0/0
R_Kharkiv(config-if)#ip authentication mode eigrp 1 md5
R_Kharkiv(config-if)#ip authentication key-chain eigrp 1 EIGRP_KeyChain_Protected
R_Kharkiv(config-if)#end
R_Kharkiv#write
```

Значущою є також конфігурація механізму паролів та привілеїв на пристроях мережі для зменшення ризику несанкціонованого доступу. Крім того, важливо замінити застарілий протокол віддаленого адміністрування Telnet на сучасний та безпечний. Один із ключових протоколів, який забезпечує цей функціонал, - це SSH другої версії [20]. Також рекомендується використовувати фільтрацію доступу до цього протоколу через списки контролю доступу так, щоб доступ до нього був можливий лише з мережі, відповідальної за управління, наприклад, LAN_MGMT. Приведено приклад конфігурації на основі R_Core_2:

```
R_Core_2#configure terminal
R_Core_2(config)#enable secret qwerty123
R_Core_2(config)#username admin privilege 15 secret qwerty123
R_Core_2(config)#username user privilege 1 secret qwerty123
R_Core_2(config)#crypto key generate rsa general-keys modulus 1024
R_Core_2(config)#ip ssh version 2
R_Core_2(config)#ip ssh time-out 90
R_Core_2(config)#ip ssh authentication-retries 3
R_Core_2(config)#banner motd #Unauthorized access is prohibited. For legal
users only.#
R_Core_2(config)#privilege exec level 4 ping
R_Core_2(config)#privilege exec level 4 show
R_Core_2(config)#privilege exec level 4 traceroute
R_Core_2(config)#ip access-list standard SSH_MGMT
R_Core_2(config-std-nacl)#permit 192.168.254.0 0.0.0.31
```

```

R_Core_2(config-std-nacl)#exit
R_Core_2(config)#line con 0
R_Core_2(config-line)#password qwerty123
R_Core_2(config-line)#logging synchronous
R_Core_2(config-line)#login local
R_Core_2(config-line)#exit
R_Core_2(config)#line vty 0 15
R_Core_2(config-line)#login local
R_Core_2(config-line)#transport input ssh
R_Core_2(config-line)#transport output none
R_Core_2(config-line)#access-class SSH_MGMT in
R_Core_2(config-line)#end

```

Для перевірки правильності налаштувань було виконано підключення до мережі з однієї з робочих станцій LAN_MGMT. Була перевірена можливість підключення під різними обліковими записами користувачів з різним рівнем привілеїв та можливості виконання налаштувань пристрою (рис. 3.39 – 3.40). Також було випробувано можливість підключення з пристрою мережі, яке не було дозволено в ACL, налаштованому на маршрутизаторі (рис. 3.41). В результаті аналізу стійкості прийшли до висновку, що мережа захищена від несанкціонованого доступу, тобто механізми контролю доступу та авторизації налаштовані правильно. Крім того, дані, що передаються під час обміну трафіком, зашифровані, що унеможливорює сніфінг.

```

(kali@kali)-[~]
└─$ ssh -l admin 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA key fingerprint is SHA256:R3Sq5SlJOEc6rmkKAizh6J9oii3InDI8D62ojSXbqGw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (RSA) to the list of known hosts.
Password:
Unauthorized access is prohibited. For legal users only
R_Core_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Core_2(config)#int fa0/0
R_Core_2(config-if)#description link_to_R_MGMT
R_Core_2(config-if)#end
R_Core_2#exit
Connection to 192.168.1.2 closed.

```

Рисунок 3.46 – Підключення за протоколом SSHv2 під обліковим записом адміна

```
(kali㉿kali)-[~]  
$ ssh -l user 192.168.1.2  
Password:  
Unauthorized access is prohibited. For legal users only  
R_Core_2>en  
Password:  
R_Core_2#show run  
Building configuration...  
  
Current configuration : 4732 bytes  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R_Core_2
```

Рисунок 3.47 – Підключення за протоколом SSHv2 під обліковим записом звичайного користувача

```
R_Core_2#  
*Mar 1 02:32:28.227: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.254.4)  
R_Core_2#sh int fa0/0  
FastEthernet0/0 is up, line protocol is up  
  Hardware is AmdFE, address is cc02.2f56.0000 (bia cc02.2f56.0000)  
  Description: link to R MGMT  
  Internet address is 192.168.20.1/30  
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,  
    reliability 255/255, txload 1/255, rxload 1/255  
  Encapsulation ARPA, loopback not set  
  Keepalive set (10 sec)  
  Full-duplex, 100Mb/s, 100BaseTX/FX  
  ARP type: ARPA, ARP Timeout 04:00:00  
  Last input 00:00:02, output 00:00:04, output hang never  
  Last clearing of "show interface" counters never  
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
  Queueing strategy: fifo  
  Output queue: 0/40 (size/max)  
  5 minute input rate 0 bits/sec, 0 packets/sec  
  5 minute output rate 0 bits/sec, 0 packets/sec  
    3809 packets input, 314915 bytes  
    Received 2156 broadcasts, 0 runs, 0 giants, 0 throttles
```

Рисунок 3.48 – Перевірка змін на маршрутизаторі R_Core_2

```
R_Kyiv#ssh -l admin 192.168.1.2  
% Connection refused by remote host  
R_Kyiv#
```

Рисунок 3.49 – Спроба підключення по SSHv2 до R_Core_2 з пристрою, який не належить до дозволених LAN

Висновки до третього розділу

У першому підрозділі було налаштовано параметри IP-адресації, DHCP та SNMP серверів, сенсори NetFlow та точки відстежування IPFIX, маршрутизацію за протоколом EIGRP та статичними маршрутами комп'ютерної мережі. Досліджено та перевірено правильність функціонування налаштованих протоколів.

У другому підрозділі було проведено аналіз основних проблем безпеки в сконфігурованій мережі. Здійснено тестування на проникнення та виявлення можливих інцидентів кібербезпеки, при цьому виконано атаки, спрямовані на виявлені уразливості.

У третьому підрозділі були налаштовані засоби захисту від атак на протоколи та механізми мережі. Проведено повторні спроби атак, перевірено правильність налаштувань та функціонування заходів забезпечення безпеки.

ВИСНОВКИ

Під час виконання випускної кваліфікаційної роботи було повністю розроблено підсистему захисту системи моніторингу мережної інфраструктури за допомогою емулятора GNS3. Проведено наукові дослідження, спрямовані на вивчення особливостей функціонування та забезпечення безпеки протоколів SNMP версій 2c та 3, NetFlow версії 9 та IPFIX. Проаналізовано та вирішено проблеми безпеки та вразливості, що виникали під час розгортання мережі.

У першому розділі розглянуті основні теоретичні концепції щодо протоколів моніторингу мережі, представлена архітектура та реалізації обміну повідомленнями. Проведено аналіз прикладних реалізацій використання протоколів SNMP, NetFlow та IPFIX для моніторингу мережі, порівняно варіанти реалізації моніторингу за допомогою додатків на операційних системах Windows та Linux, ідентифіковано ключові проблеми безпеки моніторингових протоколів.

У другому розділі розроблено загальну топологію мережі та проекти локальних ділянок, враховано схему адресації всіх пристроїв мережі з урахуванням можливості масштабування. Здійснено відбір відповідного проекту топології обладнання мережі. Здійснено аналіз можливих загроз мережі відповідно до протоколів, які будуть використовуватися у спроектованій мережі, та визначено найбільш поширені варіанти атак та їх потенційні наслідки. Побудовано модель загроз мережі організації за допомогою OWASP Threat Dragon.

У третьому розділі здійснено налаштування мережі відповідно до проекту та перевірено правильність функціонування налаштованих протоколів. Проаналізовано основні безпекові проблеми налаштованої мережі, проведено тестування на проникнення та реалізовано атаки відповідно до виявлених проблем безпеки. Налаштовано заходи захисту від атак на протоколи та механізми мережі. Перевірено правильність функціонування заходів забезпечення безпеки.

Враховуючи реалізацію проекту, його можна впроваджувати в маленьких та середніх організаціях з можливістю подальшого розширення. Стійкість мережі забезпечено рекомендаціями та практичними впровадженнями для посилення безпеки.

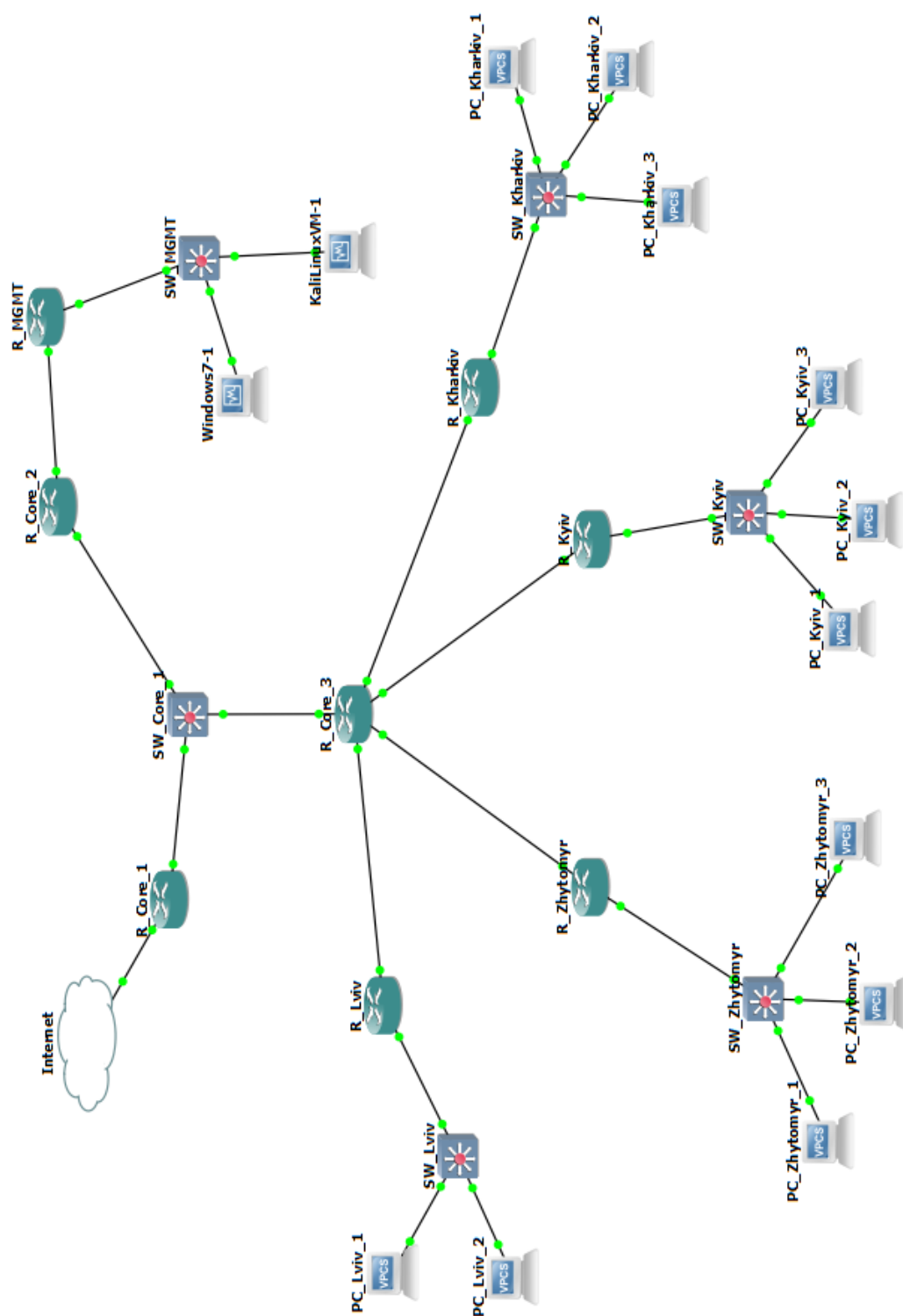
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is SNMP | SNMP Monitoring [Електронний ресурс] – Режим доступу до ресурсу: <https://www.site24x7.com/network/what-is-snmp.html>
2. NetFlow version 9 - Cisco [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/netflow-version-9/index.html>
3. IBM Docs - SNMPv3 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/docs/en/aix/7.2?topic=management-snmpv3>
4. IPFIX overview - IBM Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/docs/en/npi/1.3.1?topic=insight-ipfix-overview>
5. IPFIX Collector Tools | Kentik [Електронний ресурс] – Режим доступу до ресурсу: <https://www.kentik.com/kentipedia/ipfix-collector/>
6. What is NetFlow? | IBM [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/topics/netflow>
7. Common SNMP Vulnerability: 9-Step Guide to Protect Your Network [Електронний ресурс] – Режим доступу до ресурсу: <https://www.comparitech.com/net-admin/common-snmp-vulnerabilities/>
8. Differences Between SNMP and Syslog [Електронний ресурс] – Режим доступу до ресурсу: <https://www.dpstele.com/blog/differences-between-snmp-and-syslog.php>
9. IPFIX > NetFlow for Cybersecurity | Cisco Press [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ciscopress.com/articles/article.asp?p=2812391&seqNum=4>
10. Cisco three-layer hierarchical model [Електронний ресурс] – Режим доступу до ресурсу: <https://study-ccna.com/cisco-three-layer-hierarchical-model>
11. DHCP Starvation attacks and DHCP spoofing attacks – Режим доступу до ресурсу: <https://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>

12. What is SNMP Reflection and Amplification | DDoS Attack Glossary | Imperva [Электронный ресурс] – Режим доступа до ресурсу: <https://www.imperva.com/learn/ddos/snmp-reflection>
13. Inside SSH-2 (SSH, The Secure Shell: The Definitive Guide) [Электронный ресурс] – Режим доступа до ресурсу: https://docstore.mik.ua/oreilly/networking_2ndEd/ssh/ch03_05.html
14. Threat Modeling Process | OWASP Foundation [Электронный ресурс] – Режим доступа до ресурсу: https://owasp.org/www-community/Threat_Modeling_Process
15. SNMP - How can I test SNMP [Электронный ресурс] – Режим доступа до ресурсу: <https://store.chipkin.com/articles/snmp-how-can-i-test-snmp>
16. POPUP How to use MIB Broweser [Электронный ресурс] – Режим доступа до ресурсу: <https://pitstop.manageengine.com/portal/en/kb/articles/how-to-use-mib-browser>
17. What is Kali Linux [Электронный ресурс] – Режим доступа до ресурсу: <https://www.educative.io/answers/what-is-kali-linux>
18. SNMP – Simply Not My Problem. Or is it? | Pen Test Partners [Электронный ресурс] – Режим доступа до ресурсу: <https://www.pentestpartners.com/security-blog/snmp-simply-not-my-problem-or-is-it>
19. Secure Telnet Connection - Information Technology [Электронный ресурс] – Режим доступа до ресурсу: <https://it.mst.edu/policies/secure-telnet/>
20. What is DHCP Snooping [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf>
21. Cisco Content Hub - Configuring SSHv2 and Telnet [Электронный ресурс] – Режим доступа до ресурсу: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/routers/connected-grid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ssh_cgr1000.html.xml

ДОДАТКИ

Детальна схема побудованої мережі в GNS3



Модель загроз мережі організації

