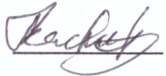


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

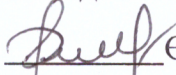
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми виявлення та аналізу мережевих загроз на базі рішень Snort та Suricata»

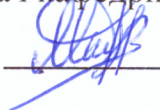
Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Іван КУЛИКІВСЬКИЙ

Керівник старший викладач кафедри КІ та КБ,

 Єлизавета ТРОКОЗ

Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Олександр МАЄВСЬКИЙ

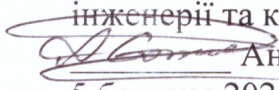
Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Куликівський Іван Дмитрович

Тема роботи: «Проект підсистеми виявлення та аналізу мережесих загроз на базі рішень Snort та Suricata»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

- типи мережесих загроз та системи їх виявлення;
- розробка та налаштування тестової мережі;
- порівняльний аналіз Snort та Suricata;

Предметом дослідження є проектування підсистеми виявлення та аналізу мережесих загроз на базі рішень Snort та Suricata.

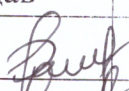
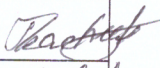
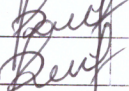
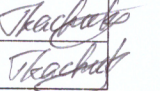
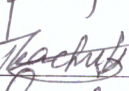
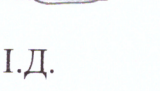
Об'єктом дослідження є процес проектування підсистеми аналізу та виявлення мережесих загроз на базі рішень Snort та Suricata та аналіз функціонування цих інструментів шляхом проведення можливих атак.

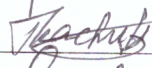
Обладнання та програмне забезпечення:

1. GNS3
2. Oracle VM VirtualBox
3. ОС Windows 10
4. ОС Ubuntu
5. ОС Windows 7

6. ОС Kali Linux
7. Інструмент Snort
8. Інструмент Suricata

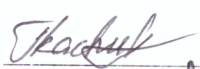
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

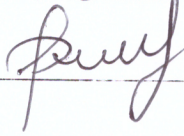
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	11.03.2024 	11.03.2024 
2	Трокоз Є.М.	07.04.2024 	07.04.2024 
3	Трокоз Є.М.	18.05.2024 	18.05.2024 

Студент  Куликівський І.Д.
Керівник  Трокоз Є.М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2024	Виконано
2	Аналіз отримано завдання	05.02.2024	Виконано
3	Розробка плану роботи	10.03.2024	Виконано
4	Аналіз літературних джерел	14.03.2024	Виконано
5	Аналіз об'єкта досліджень	26.03.2024	Виконано
6	Розробка структурованої моделі	08.05.2024	Виконано
7	Розробка мережі	19.05.2024	Виконано
8	Налаштування мережі та ПЗ	27.05.2024	Виконано
9	Оформлення пояснювальної записки	04.06.2024	Виконано
10	Захист кваліфікаційної роботи	26.06.2024	Виконано

Студент  Куликівський І.Д.

Керівник  Трокоз Є.М.

АНОТАЦІЯ

Кваліфікаційна робота на тему “Проект підсистеми виявлення та аналізу мережевих загроз на базі рішень Snort та Suricata” складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Пояснювальна записка містить 80 рисунків та займає 72 сторінок. Список використаних джерел містить 20 найменувань і розташований на 2 сторінках.

Метою даної роботи є ознайомлення з такими інструментами як Snort та Suricata для аналізу та виявлення мережевих загроз.

У роботі визначено основні види мережевих загроз, такі як DoS-атаки, сканування портів, і шкідливе програмне забезпечення, а також проаналізовано системи виявлення та запобігання вторгнень (IDS/IPS), включаючи їхні можливості та функціональні особливості. Показано розробку тестової мережі, що включає проектування її архітектури, створення схеми адресації, та налаштування критичних мережевих компонентів, таких як NTP для синхронізації часу та OSPF для динамічної маршрутизації. Наведено результати тестування інструментів виявлення загроз Snort та Suricata, де на основі проведеного аналізу та практичного використання встановлено, що Suricata є більш зручною в налаштуванні і експлуатації, завдяки простішій конфігурації та доступності інформації.

У додатку представлена схема спроектованої мережі, таблиця адресації та конфігурація пристроїв.

Ключові слова: МЕРЕЖЕВІ ЗАГРОЗИ, DOS-АТАКА, СКАНУВАННЯ ПОРТІВ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, IDS/IPS, SNORT, SURICATA, KALI LINUX, МОНІТОРИНГ АТАК.

					ККІК.КР.Б - 125 - 09 - ПЗ			
Змн.	Арк	№ докум.	Підпис	Дата	Проект підсистеми виявлення та аналізу мережевих загроз на базі рішень Snort та Suricata	Літ.	Арк.	Аркуші
Розроб.		Куликівський І.Д.	<i>[Підпис]</i>	24.06				
Керівник		Трокоз Є.М.	<i>[Підпис]</i>	24.06			2	75
Реценз.		Масвський О.В.	<i>[Підпис]</i>	24.06		ФІКТ, Гр. КБ-20-1		
Н. контр.		Трокоз Є.М.	<i>[Підпис]</i>	24.06				
Затверд.		Сфіменко А.А.	<i>[Підпис]</i>	24.06				

ANNOTATION

The qualification work on the topic "Project of a subsystem for detecting and analysing detecting multiple threats based on Snort and Suricata solutions" consists of a list of abbreviations, an introduction, three chapters, conclusions, a list of references and appendices.

The explanatory note contains 80 pictures and covers 72 pages. The list of references includes 20 titles and is located on 2 pages.

The purpose of this paper is to introduce such tools as Snort and Suricata for analysing and detecting network threats.

The paper identifies the main types of network threats, such as DoS attacks, port scanning, and malware, and analyses intrusion detection and prevention systems (IDS/IPS), including their capabilities and functional features. The development of a test network is shown, including the design of its architecture, creation of an addressing scheme, and configuration of critical network components, such as NTP for time synchronisation and OSPF for dynamic routing. The article presents the results of testing the Snort and Suricata threat detection tools, where, based on the analysis and practical use, it was found that Suricata is more convenient to set up and operate due to simpler configuration and availability of information.

The appendix contains a diagram of the designed network, an addressing table, and device configuration.

Keywords: NETWORK THREATS, DOS ATTACK, PORT SCANNING, MALWARE, IDS/IPS, SNORT, SURI-CATA, KALI LINUX, ATTACK MONITORING.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ОГЛЯД МОЖЛИВИХ ЗАГРОЗ ТА ВІДОМОСТІ ПРО ПРОГРАМИ ...	9
1.1 Мережеві загрози: класифікація та характеристика.....	9
1.2 Системи виявлення атак (IDS) та системи запобігання вторгненням (IPS)	16
1.3 Опис, функціонал можливостей та архітектура програмного забезпечення	19
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ТЕСТУВАННЯ ІНСТРУМЕНТІВ ЗАХИСТУ	24
2.1 Вибір обладнання та операційної системи.....	24
2.2 Опис та архітектура тестової мережі	27
2.3 Розробка схеми адресації мережі	30
РОЗДІЛ 3. ПРОВЕДЕННЯ АНАЛІЗУ ТА ВИЯВЛЕННЯ МЕРЕЖЕВИХ ЗАГРОЗ ЗА ДОПОМОГОЮ SNORT ТА SURICATA	34
3.1 Проведення налаштування мережі.....	34
3.2 Дослідження інструментів Snort.....	43
3.3 Дослідження інструментів Suricata	60
ВИСНОВКИ.....	71
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	73
ДОДАТКИ.....	75

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система
ПЗ – програмне забезпечення
IPS – intrusion prevention system
IDS – intrusion detection system
PING – packet internet groper
IP – internet protocol
BSD – Berkeley software distribution
DHCP – dynamic host configuration protocol
ICMP – internet control message protocol
UDP – user datagram protocol
SID – signature identifier
GID – generator identifier
SMB – server message block
HTTP – hypertext transfer protocol
OSPF – open shortest path first

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Кількість кібератак та їх складність постійно зростають, що створює серйозні загрози для організацій різного рівня. Виявлення та аналіз мережевих загроз стають невід’ємною частиною забезпечення надійного функціонування мереж та захисту конфіденційних даних. Для цього можуть використовуватися безліч інструментів, серед яких особливе місце займають Snort та Suricata. Ці відкриті програмні рішення широко використовуються у світовій практиці завдяки своїй гнучкості, функціональності та можливостям налаштування під конкретні потреби.

Метою кваліфікаційної роботи є розробка проєкту підсистеми виявлення та аналізу мережевих загроз на базі рішень Snort та Suricata. Проєкт має забезпечити ефективне виявлення різноманітних видів атак та загроз.

Визначена мета обумовлює наступні завдання:

- описати функціональні можливості та архітектуру Snort та Suricata;
- розробити архітектуру підсистеми виявлення та аналізу загроз на базі Snort та Suricata;
- здійснити налаштування та тестування створеної підсистеми у реальних умовах;
- провести порівняльний аналіз ефективності Snort та Suricata у виявленні різних типів загроз.

Об’єктом дослідження є процеси виявлення та аналізу мережевих загроз у комп’ютерних мережах.

Предметом дослідження є програмні рішення Snort та Suricata, їх функціональні можливості та ефективність у виявленні та аналізі мережевих загроз.

Дана робота спрямована на створення ефективної підсистеми виявлення та аналізу мережевих загроз, що забезпечить надійний захист мережевих ресурсів від потенційних атак та дозволить своєчасно виявляти та нейтралізувати загрози.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОГЛЯД МОЖЛИВИХ ЗАГРОЗ ТА ВІДОМОСТІ ПРО ПРОГРАМИ

1.1 Мережеві загрози: класифікація та характеристика

Мережеві загрози це випадки або дії, які мають потенціал пошкодити дані, завдати шкоди мережі або комп'ютерним системам. Існує багато різновидів мережевих загроз, які можна класифікувати за різними критеріями:

1. За типом цілі:

- атаки на доступність: мають на меті зробити систему недоступною для користувачів;
- атаки на цілісність: мають на меті змінити або пошкодити дані;
- атаки на конфіденційність: мають на меті отримати доступ до конфіденційної інформації.

2. За методом атаки:

- атаки з експлуатацією вразливостей: використовують відомі вразливості в програмному забезпеченні або системах;
- атаки з використанням соціальної інженерії: намагаються обдурити користувачів, щоб вони розкрили конфіденційну інформацію або виконали дії, які можуть призвести до зараження системи;
- атаки грубої сили: намагаються зламати паролі або інші ключі автентифікації, використовуючи перебір проб.

3. За типом зловмисника:

- хакер: людина, яка має на меті отримати доступ до комп'ютерних систем або мереж з несанкціонованими цілями;
- кіберзлочинці: люди, які використовують комп'ютери для скоєння злочинів, таких як крадіжка особистих даних або фінансове шахрайство;
- державні хакери: хакери, які працюють на уряди або інші державні органи.

У сучасному цифровому світі, мережеві загрози стають більш складними та швидко поширюються. Кожна загроза реалізована по своєму та може мати різні методи здійснення що може завдати серйозної шкоди організаціям або окремим

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

користувачам. До найпоширеніших типів мережесих загроз можна віднести DDoS-атаки, сканування портів та шкідливе програмне забезпечення [3].

DDoS-атаки (Distributed Denial of Service) – це тип кібератаки, мета якої полягає в тому, щоб зруйнувати онлайн-сервіс, переповнюючи його запитами з різних джерел одночасно. Основною метою DDoS-атак є перешкоджати звичайним користувачам отримати доступ до веб-сайтів, серверів та інших інтернет-ресурсів. Атаки на мережеві інфраструктури можуть включати брандамауери, мережеві марш-рутизатори, сервери та інші мережеві пристрої. Зловмисники створюють ботнети-мережі зламаних комп'ютерів, які можна контролювати за допомогою зловмисного програмного забезпечення. Ботнети можуть складатися з тисяч або навіть мільйонів різних пристроїв, таких як комп'ютери, смартфони та пристрої Інтернету речей (IoT) [11]. Існують різні типи DDoS-атак, наприклад:

1. Атаки на рівні мережі (Layer 3 та Layer 4):

- UDP-флуд: Атака з великою кількістю UDP-пакетів на цільовий сервер, щоб переповнити його здатність обробляти запити;
- ICMP-флуд: Атака з великою кількістю ICMP (Ping) запитів, щоб перезавантажити цільовий сервер;
- SYN-флуд: Атака, яка використовується для вичерпання ресурсів сервера, відправляючи велику кількість запитів на встановлення з'єднання (TCP SYN).

2. Атаки на рівні додатків (Layer 7):

- HTTP-флуд: Відправка великої кількості HTTP-запитів до веб-сервера з метою вичерпання його ресурсів;
- Slowloris: Атака, яка відправляє часткові HTTP-запити до веб-сервера, утримуючи з'єднання відкритим та змушуючи сервер тримати ресурси, необхідні для обробки цих запитів.

Зловмисники можуть атакувати компанії з метою шантажу та вимагати викуп, щоб припинити атаку (DDoS за викуп). Крім того, атаки можуть бути спрямовані на громадські або урядові організації з метою саботажу чи протесту проти політики. Іноді конкуренти можуть ініціювати атаки, щоб зруйнувати бізнес конкурента.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Методи захисту від DDoS-атак:

- мережеві брандмауери та системи виявлення вторгень (IDS/IPS): ці інструменти можуть виявляти та блокувати підозрілі трафіки;
- захист на рівні провайдера: інтернет-провайдери можуть надати захист від DDoS, відхиляючи шкідливий трафік до його досягнення цільової мережі;
- хмарні рішення: використання хмарних сервісів для розподілу трафіку та захисту від DDoS-атак;
- моніторинг та аналітика: постійний моніторинг трафіку та аналіз патернів допомагають вчасно виявити та реагувати на атаки.

Anycast мережі: використовується для розподілу трафіку між декількома дата-центрами, що зменшує навантаження на окремі вузли.

DDoS-атаки можуть мати значні наслідки, такі як переривання бізнес-процесів і втрата грошей. Крім того, компанії, які зазнали пошкоджень, можуть зазнати репутаційних втрат, оскільки клієнти та партнери можуть втратити довіру до того, що вони можуть безпечно використовувати свої ресурси. Відновлення після атак вимагає великих витрат, оскільки необхідно виявити та ліквідувати наслідки атаки, впровадити додаткові засоби захисту, а іноді навіть заплатити зловмисникам за викуп [11].

Сканування портів – це метод дослідження комп’ютерних мереж, який дозволяє виявити відкриті порти на комп’ютері або сервері. Цей підхід використовується зловмисниками для виявлення активних портів, а також послуг і програм, які доступні на цих портах, щоб визначити потенційні вразливості для подальших атак [1].

Процес сканування автоматизується за допомогою спеціалізованого програмного забезпечення, як-от Nmap. Ці програми відправляють пакети на цільові порти та аналізують їхній стан. Відкритий порт вказує на активний сервіс, закритий порт вказує на відсутність сервісу або блокування доступу, а фільтрований порт вказує на обмежений доступ до нього брандмауером або іншим захисним механізмом. Існують такі типи сканування портів:

1. TCP SYN-сканування (напіввідкрите сканування):

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

– використовує початковий SYN-пакет для відкриття з'єднання. Якщо порт відкритий, сервер відповідає SYN/ACK, після чого скануючий пристрій відправляє RST (скидання) для завершення з'єднання, не встановлюючи повноцінного TCP-з'єднання. До переваг можна віднести менше навантаження на цільову систему, менша ймовірність виявлення.

2. TCP Connect-сканування:

– встановлює повне TCP-з'єднання з цільовим портом. Відправляє SYN-пакет, отримує SYN/ACK відповідь і відповідає ACK, потім закриває з'єднання;

– переваги: легше реалізувати та інтерпретувати результати. Недоліки: більш легко виявляється.

3. UDP-сканування:

– відправляє UDP-пакети на цільові порти. Якщо порт закритий, система відповідає ICMP Port Unreachable повідомленням. Відсутність відповіді може свідчити про те, що порт відкритий або фільтрується;

– переваги: можливість виявлення UDP-сервісів. Недоліки: більш складне та повільне, оскільки відсутність відповідей може мати різні причини.

4. FIN, Xmas та Null-сканування:

– використовують пакети з незвичними комбінаціями прапорців (наприклад, FIN, Xmas з усіма прапорцями встановленими, Null з жодним встановленим прапорцем). Відкриті порти ігнорують ці пакети, а закриті порти відповідають RST;

– переваги: часто проходить через фільтри та брандмауери. Недоліки: не працює на системах Windows.

5. ACK-сканування:

– використовуються для визначення фільтрованих портів. Відправляє ACK-пакети, щоб перевірити чи фільтрується порт;

– переваги: дозволяє дізнатися про наявність фільтрації портів. Недоліки: не вказує, чи порт відкритий чи закритий.

Хоча сканування портів не завдає шкоди, це важливий інструмент для виявлення вразливостей, які зловмисники можуть використовувати для наступних атак. Несанкціонований доступ, впровадження шкідливого програмного забезпечення

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

або виконання інших зловмисних дій можуть бути прикладами цього. Часто більш складні атаки, такі як експлойти або DDoS-атаки, починаються зі сканування портів.

Методи захисту від сканування портів:

- брандмауери: конфігурація брандмауерів для блокування невідомих або небажаних запитів;
- системи виявлення вторгнень (IDS): використання IDS для виявлення підозрілих активностей, включаючи сканування портів;
- закриття невикористовуваних портів: зменшення поверхні атаки шляхом закриття всіх портів, які не використовуються;
- маскування відповідей: налаштування систем для приховування або затримки відповідей на підозрілі запити;
- сегментація мережі: розділення мережі на сегменти з різними рівнями доступу та контролю.

Розуміння методів та наслідків сканування портів допомагає краще підготуватися до можливих загроз і впровадити ефективні заходи безпеки [1].

Шкідливе програмне забезпечення, також відоме як malware (malicious software) - це будь-яке програмне забезпечення, створене з метою пошкодження, порушення, крадіжки або несанкціонованого доступу до комп'ютерних систем. Malware може бути використано для багатьох злочинів, таких як крадіжка даних, шантаж, шпигунство та саботаж.

Фішингові атаки, заражені файли або підроблені оновлення програмного забезпечення можуть спричинити проникнення вірусів у систему. Malware активується після проникнення в систему, часто приховуючи свою присутність. Шкідливе програмне забезпечення може робити багато речей, таких як шифрування файлів, крадіжка даних, відправка спаму або створення бекдорів. Malware часто намагається уникати виявлення, використовуючи такі методи маскування, як руткіти або шифрування свого коду [2].

Існують такі типи шкідливого програмного забезпечення:

1. Віруси

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

– Механізм: самовідтворювальне програмне забезпечення, яке прикріплюється до інших програм або файлів і активується при їх запуску.

– Наслідки: може пошкодити або знищити файли, уповільнити роботу системи або стати шлюзом для інших видів malware.

2. Черв'яки

– Механізм: самостійно поширюване ПЗ, яке не потребує інтеграції з іншими файлами або програмами. Поширюється через мережі та вразливості в системах.

– Наслідки: може перевантажити мережі, споживати ресурси системи та поширювати інші види malware.

3. Троянські програми (трояни)

– Механізм: маскуються під легітимне ПЗ, але виконують шкідливі дії, такі як крадіжка даних або надання віддаленого доступу зловмисникам.

– Наслідки: використовуються для викрадення конфіденційної інформації, встановлення додаткового malware або створення бекдорів.

4. Руткіти

– Механізм: набір інструментів, що дозволяє зловмисникам приховувати свою присутність на системі та отримати привілейований доступ.

– Наслідки: ускладнює виявлення інших видів malware, може надавати зловмисникам повний контроль над системою.

5. Рансомваре (вимагачі)

– Механізм: шифрує файли на комп'ютері жертви та вимагає викуп за їх розшифровку.

– Наслідки: втрата доступу до важливих даних, фінансові витрати на сплату викупу та відновлення системи.

6. Шпигунське ПЗ

– Механізм: непомітно збирає інформацію про користувача, включаючи паролі, історію браузера та особисті дані.

– Наслідки: порушення приватності, крадіжка ідентифікаційних даних та конфіденційної інформації.

7. Adware

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

– Механізм: відображає небажану рекламу на комп'ютері жертви. Може бути інтегроване в інше ПЗ або працювати самостійно.

– Наслідки: уповільнює роботу системи, створює навантаження на мережу та може стати шлюзом для іншого malware.

8. Боти та ботнети

– Механізм: заражені пристрої, які об'єднуються в мережу (ботнет) та керуються зловмисниками для виконання різних шкідливих дій, таких як DDoS-атаки або розсилка спаму.

– Наслідки: використання ресурсів системи для зловмисних цілей, участь у великих масштабних атаках без відома користувача.

Шкідливе програмне забезпечення може призвести до значних фінансових втрат, втрати даних, порушення конфіденційності, зниження продуктивності мереж і систем, а також до втрати репутації компанії. Наприклад, рансомваре мають здатність шифрувати важливі файли, вимагаючи викуп за їх розшифрування, тоді як трояни можуть дозволити зловмисникам отримати доступ до систем або конфіденційної інформації [12].

Методи захисту від шкідливого ПЗ:

– антивірусне ПЗ: Використання надійного антивірусного програмного забезпечення для виявлення та видалення шкідливих програм;

– оновлення системи: Регулярне оновлення операційної системи та програмного забезпечення для закриття відомих вразливостей;

– файрволи: Використання брандмауерів для контролю мережевого трафіку та блокування підозрілих запитів;

– навчання користувачів: Підвищення обізнаності користувачів щодо фішингових атак, підозрілих електронних листів та небезпечних веб-сайтів;

– резервне копіювання: Регулярне створення резервних копій даних для можливості відновлення в разі атаки;

– моніторинг і аудит: Постійний моніторинг систем і аудит безпеки для виявлення підозрілої активності.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Шкідливе програмне забезпечення є серйозною загрозою і ефективний захист вимагає комплексного підходу, що включає технічні засоби, процедури безпеки та навчання користувачів.

1.2 Системи виявлення атак (IDS) та системи запобігання вторгненням (IPS)

Системи виявлення та запобігання вторгненням (IDS/IPS) – це апаратні або програмні системи, які використовуються для моніторингу мережі та виявлення потенційних загроз. Вони можуть бути використані для виявлення та блокування різноманітних загроз, таких як шкідливе програмне забезпечення, атаки типу MITM, DoS або DDoS.

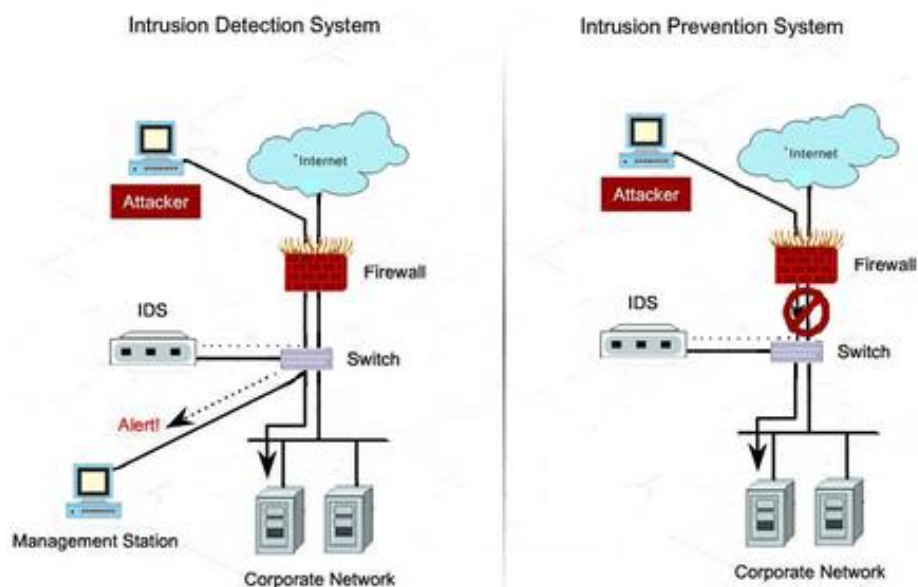


Рисунок 1.1 – Система виявлення і запобігання вторгненням

IDS/IPS працюють, аналізуючи мережевий трафік та поведінку користувачів. Вони можуть використовувати різні методи для виявлення загроз, включаючи:

- фільтрацію пакетів. Цей метод передбачає аналіз заголовків мережевих пакетів і блокування пакетів, які не відповідають встановленим правилам;
- аналіз поведінки. Цей метод передбачає аналіз поведінки мережевого трафіку та блокування трафіку, який виявляє ознаки загрози;
- сканування портів. Цей метод передбачає сканування мережі на наявність відкритих портів, які можуть бути використані зловмисниками для доступу до системи або мережі.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

IDS/IPS є життєво важливим компонентом будь-якої системи безпеки. Вони здатні захистити комп'ютер або мережу від безлічі небезпек. Ось деякі приклади використання виявлення та блокування загроз IDS/IPS:

IDS може бути налаштований для виявлення пакетів, які містять певні ознаки шкідливого програмного забезпечення, такі як певні IP-адреси або порти.

Існує можливість налаштувати системи запобігання вторгнень (IPS) для блокування доступу до певних веб-сайтів або IP-адрес, які можуть бути джерелами шкідливого програмного забезпечення.

IDS може бути налаштований для виявлення повторюваних запитів або великих пакетів даних, які можуть свідчити про атаку DoS.

Налаштування системи виявлення та запобігання вторгненням:

1. Визначення сигнатур:

– Створення та оновлення сигнатур: Розробка та регулярне оновлення сигнатур для виявлення відомих атак та вразливостей.

2. Конфігурація аналізаторів:

– Налаштування порогів виявлення: Встановлення порогів виявлення для забезпечення точності виявлення атак на мінімізації неправдивих спрацьовувань.

3. Моніторинг та аудит:

– Журналювання подій: Ведення детальних журналів подій для вивчення та аналізу атак та інцидентів.

4. Реакція на атаку:

– Автоматична реакція: Налаштування системи на автоматичну реакцію на виявлені загрози (блокування атак та блокування атакуючого пристрою).

5. Встановлення та вдосконалення політик безпеки:

– Конфігурація правил: Визначення правил та політик безпеки для взаємодії з існуючими архітектурами та обмежень мережі.

6. Впровадження мережевих топологій:

– Конфігурація мережевих топологій: Вибір та встановлення мережевих топологій для ефективного розгортання IDS/IPS у відповідності до потреб мережі.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Ці методи дозволяють налаштувати IDS/IPS для максимальної ефективності у виявленні та блокуванні потенційних загроз в мережі.

Обидві системи використовують три основні підходи для виявлення та запобігання загрозам:

- сигнатурний підхід: використовує базу даних з відомими сигнатурами атак для виявлення збігів у поточному трафіку або діях. Ефективний проти відомих атак, але може бути безсилим проти нових;

- аномальний підхід: створює модель нормальної поведінки системи або мережі і виявляє або блокує відхилення цієї моделі. Може виявляти нові атаки, але має високу ймовірність хибнопозитивних спрацьовувань;

- підхід на основі політик: Використовує заздалегідь визначені правила або політики для виявлення та блокування підозрілої активності. Легко налаштовується під конкретні вимоги організації, але потребує ретельної розробки та підтримки правил.

IDS та IPS забезпечують раннє виявлення загроз, підвищення рівня безпеки та звільнення адміністраторів від навантаження завдяки автоматичному реагуванню на загрози. IPS забезпечує комплексний захист, додаючи брандмауери та антивірусні програми. Але обидві системи можуть мати хибнопозитивні спрацьовування, що викликає додаткові сповіщення та час, витрачений на перевірку. Крім того, складність впровадження та витрати можуть бути високими, особливо для великих мереж або організацій, які мають високі вимоги до безпеки.

До прикладів використання IDS можна віднести Snort – це відкрите ПЗ для мережевого виявлення вторгнень, яке широко використовується завдяки своїй гнучкості та можливостям налаштування; Suricata – це високопродуктивна мережева IDS, яка підтримує багатопоточну обробку та здатна працювати з великим обсягом трафіку; OSSEC – це відкрита хостова IDS, яка забезпечує моніторинг файлових систем, системних журналів та інших дій на хості.

До прикладів використання IPS можна віднести Cisco Firepower – це високопродуктивна мережева IPS, яка забезпечує сигнатурне та аномальне запобігання, а також інтеграцію з іншими системами безпеки; Snort (у режимі IPS) – може

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

працювати як мережева IDS або IPS, забезпечуючи сигнатурне виявлення та запобігання; McAfee Host Intrusion Prevention – це потужна хостова IPS, яка забезпечує захист на рівні окремих комп’ютерів та серверів.

Системи IDS та IPS є важливими компонентами комплексної стратегії кібербезпеки, забезпечуючи своєчасне виявлення та реагування на загрози, що дозволяє значно зменшити ризик компрометації систем та даних.

1.3 Опис, функціонал можливостей та архітектура програмного забезпечення

Snort – це популярна відкрита система виявлення та запобігання вторгнень (IDS/IPS), призначена для відстеження мережевого трафіку в режимі реального часу. За допомогою аналізу мережевих пакетів Snort знаходить різноманітні атаки та підозрілу активність.

Функціональні можливості Snort:

1. Виявлення вторгнень (IDS)

- аналіз трафіку: Snort аналізує вхідні та вихідні мережеві пакети для виявлення підозрілої активності;
- сигнатурне виявлення: використовує базу даних з відомими сигнатурами атак для ідентифікації зловмисних дій;
- виявлення аномалій: підтримує аналіз поведінки для виявлення аномальних патернів трафіку, які можуть свідчити про атаки.

2. Запобігання вторгнень (IPS)

- реагування в реальному часі: Snort може автоматично блокувати підозрілий трафік, запобігаючи атакам у реальному часі;
- інтеграція з брандмауером: може працювати разом з брандмауерами для забезпечення комплексного захисту мережі.

3. Моніторинг та аналіз трафіку

- логування та звітність: Snort логує всі виявлені інциденти, забезпечуючи детальні звіти для подальшого аналізу;

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

– гнучке налаштування: користувачі можуть налаштовувати правила та політики виявлення відповідно до специфічних потреб своєї мережі.

4. Підтрима різних режимів роботи

– Sniffer mode: просте прослуховування мережевого трафіку та його відображення.

– Packet Logger mode: логування мережевого трафіку для подальшого аналізу.

– Network Intrusion Detection mode: повноцінний режим виявлення вторгнень з використанням бази сигнатур та правил.

Архітектура Snort складається з кількох основних компонентів, які забезпечують його функціональні можливості. Одним з ключових елементів є препроцесори (Preprocessor Plugins), які попередньо обробляють мережевий трафік, нормалізують пакети та виконують спеціалізовані функції, такі як дефрагментація IP-пакетів або нормалізація HTTP-трафіку, що допомагає виявляти складні атаки. Детекційний механізм (Detection Engine) є основним компонентом Snort, який аналізує мережевий трафік за допомогою правил та сигнатур для виявлення підозрілої активності. Він порівнює трафік з базою даних сигнатур атак, виявляючи відповідності. Вихідні плагіни (Output Plugins) визначають, як буде оброблятися і зберігатися інформація про виявлені інциденти, підтримуючи різні формати виводу даних, включаючи логування у файли, бази даних, сповіщення через електронну пошту або інтеграцію з системами управління інформаційною безпекою (SIEM). Snort використовує спеціалізовану мову для написання правил (Rule-Based Language), які описують патерни зловмисної активності, що дозволяє гнучко налаштовувати систему під конкретні вимоги. Нарешті, інтерфейс управління (Management Interface) забезпечує зручне адміністрування системи, дозволяючи користувачам керувати правилами, переглядати логи та звіти, а також налаштовувати параметри роботи. Ця комплексна архітектура забезпечує Snort потужними можливостями для виявлення та запобігання вторгнень у мережі.

Snort забезпечує комплексний захист мережі від широкого спектру загроз за допомогою ефективної та адаптивної системи виявлення та запобігання вторгнень.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Snort підходить як для малих мереж, так і для великих корпоративних середовищ завдяки своїй відкритості та широкому спектру функціональних можливостей.

Suricata – це потужна, відкрита система виявлення та запобігання вторгнень (IDS/IPS), яка розроблена для забезпечення високоефективного аналізу трафіку мережі. Обробка великої кількості трафіку в реальному часі є можливою завдяки підтримці багатопотокового аналізу. Порівняно з іншими системами виявлення проникнення та захисту інформації (IDS/IPS), Suricata має більше функцій і працює на різних платформах.

Функціональні можливості Suricata:

1. Виявлення та запобігання вторгнень (IDS/IPS)

- аналіз трафіку: Suricata моніторить мережевий трафік у реальному часі, використовуючи сигнатури та правила для виявлення зловмисних дій;
- сигнатурне виявлення: використовує базу даних з відомими сигнатурами атак для ідентифікації зловмисних дій;
- виявлення аномалій: підтримує аналіз поведінки для виявлення аномальних патернів трафіку, які можуть свідчити про атаки.

2. Розширені функціональні можливості

- аналіз протоколів: підтримує глибокий аналіз різних мережевих протоколів (HTTP, FTP, SMB, TLS, тощо), що дозволяє детально розглядати трафік і виявити складні атаки;
- многопоточний аналіз: використовує всі доступні ядра процесора для забезпечення високої продуктивності аналізу трафіку;
- журналістика: забезпечує детальне логування та генерування звітів про виявлену активність (HTTP-журнали, DNS-журнали, файлові журнали).

3. Інтеграція з іншими системами

- підтримка NetFlow: може генерувати NetFlow дані для подальшого аналізу мережевого трафіку;
- підтримка EVE JSON: формат виводу EVE JSON дозволяє інтеграцію з системами управління інформаційною безпекою (SIEM) та іншими аналітичними платформами.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Налаштування та розширюваність

- гнучка мова правил: Suricata використовує потужну мову правил для визначення підозрілих патернів трафіку, що дозволяє створювати кастомні правила;
- плагіни та модулі: можливість розширення функціональності за допомогою плагінів та модулів.

Архітектура Suricata включає кілька ключових компонентів, які забезпечують її високу продуктивність та розширені можливості аналізу трафіку. Основним модулем є Packet Acquisition Module, який відповідає за захоплення мережевого трафіку з використанням різних технологій, таких як pcap, PF_RING, Netmap і DPDK, забезпечуючи швидке та ефективне захоплення пакетів для подальшого аналізу. Препроцесинг модуль (Preprocessing Module) попередньо обробляє захоплені пакети, нормалізує трафік, виконує дефрагментацію IP-пакетів та рекомпіляцію TCP-сесій, готуючи трафік для детального аналізу та забезпечуючи коректність і повноту даних.

Основним компонентом для виявлення загроз є Detection Engine, який використовує базу сигнатур та правил для аналізу трафіку та виявлення підозрілої активності. Парсери протоколів (Protocol Parsers) виконують глибокий аналіз мережевих протоколів, таких як HTTP, FTP, SMB і TLS, ідентифікуючи структуру та зміст трафіку, що дозволяє виявляти складні атаки, які використовують специфічні особливості протоколів. Вихідний модуль (Output Module) відповідає за обробку та зберігання даних про виявлені інциденти, підтримуючи різні формати виводу, включаючи EVE JSON, PCAP і NetFlow, що забезпечує інтеграцію з зовнішніми системами.

Інтерфейс управління (Management Interface) забезпечує користувацький інтерфейс для налаштування, моніторингу та керування Suricata, що полегшує адміністрування системи, дозволяючи керувати правилами, переглядати логи та звіти та налаштовувати параметри роботи. Suricata може забезпечувати ефективний аналіз мережевого трафіку та захист від загроз у реальному часі завдяки цій складній архітектурі.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Suricata це потужна система виявлення та запобігання вторгненням, яка аналізує мережевий трафік у режимі реального часу. Її гнучка архітектура та розширені функціональні можливості дозволяють її ефективно використовувати для захисту від широкого спектру загроз у різних мережевих середовищах.

Кожна з двох потужних систем виявлення та запобігання вторгненням (IDS/IPS) – Snort і Suricata – має свої особливості та переваги. Обидві системи забезпечують ефективний захист мереж від різноманітних загроз, що робить їх надзвичайно важливими для сучасної кібербезпеки. Обсяг трафіку, підтримка різних протоколів, інтеграція з іншими системами безпеки, а також необхідність багатопотокового аналізу визначають, чи використовується Snort чи Suricata для задоволення конкретних потреб компанії.

Висновки до першого розділу:

В першому розділі представлено огляд ключових мережевих загроз, таких як DoS-атаки, сканування портів та шкідливе програмне забезпечення, а також основні засоби для їх виявлення та запобігання. Поглиблене дослідження систем виявлення та запобігання вторгнень (IDS/IPS) показує їхню критичну роль у сучасній кібербезпеці, забезпечуючи моніторинг і реагування на потенційні загрози в реальному часі. Зокрема, аналіз двох популярних систем, Snort і Suricata, продемонстрував, що Snort є широко вживаним рішенням завдяки своїй простоті та надійності, тоді як Suricata відрізняється покращеною продуктивністю і багатопоточністю, що робить її придатною для високонавантажених мереж. Водночас Snort переважає у простоті налаштування та меншому використанні ресурсів, що робить її ефективною для менших інфраструктур, тоді як Suricata забезпечує гнучкість та розширюваність завдяки підтримці сучасних протоколів та технологій.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ТЕСТУВАННЯ ІНСТРУМЕНТІВ ЗАХИСТУ

2.1 Вибір обладнання та операційної системи

Windows – найпопулярніша ОС для персональних комп'ютерів. Майже всі настільні ПК та ноутбуки продаються з попередньо встановленою Windows. Причина такої популярності цього пропрієтарного проєкту криється в далеких 90-х, коли інших зручних альтернатив просто не було. [14]

ОС Ubuntu – це опенсорсний проєкт, який базується на Debian GNU/Linux. Випускає його Canonical із жовтня 2004 року. У 2005 році цю ОС визнали найкращим дистрибутивом Linux. Зараз є безліч різновидів Ubuntu, серед найпопулярніших: xUbuntu, Kubuntu, Linux Mint, Elementary OS та інші. Усі вони мають трохи різний функціонал під різні потреби [14].



Рисунок 2.1 – Операційна система Windows 10

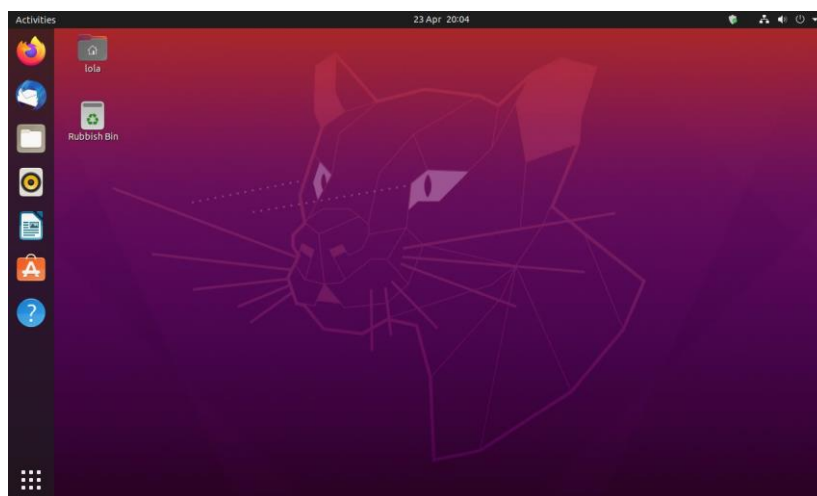


Рисунок 2.2 – Операційна система Ubuntu 20.04

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Порівняльна таблиця Windows 10 та Ubuntu

Характеристика	Windows 10	Ubuntu
Ліцензування	Закрита ліцензія	Відкрита ліцензія (GPL)
Простота використання	Вважається більш простою для користувачів	Може бути складнішою для нових користувачів
Вартість	Платна	Безкоштовна
Сумісність програмного забезпечення	Широкий спектр програмного забезпечення доступного для Windows	Більш обмежений спектр програмного забезпечення доступного для linux, але багато програмного забезпечення з windows має еквіваленти для linux
Безпека	Вважається менш безпечною за Linux через свою популярність та закриту ліцензію	Більш безпечна завдяки відкритому коду та меншій популярності
Налаштування та кастомізація	Менш гнучка за Linux	Більш гнучка, з широкими можливостями налаштування та кастомізації
Продуктивність	Зазвичай вважається більш ресурсомісткою за Linux	Може бути економною з ресурсами, але це залежить від конфігурації

Для проведення атак використовувалась ОС Kali Linux. Це безкоштовна операційна система, заснована на дистрибутиві Debian GNU/Linux, призначена для спеціалістів з кібербезпеки, цифрової криміналістики та тестування на проникнення. Дистрибутив доступний у вигляді різних версій для різних пристроїв

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

та платформ (32/64bit, x86/ARM, Raspberri PI, Live CD/USB) [16]. З Kali Linux злом стає набагато легшим, оскільки у вас є всі інструменти (понад 300 встановлених утиліт), які можуть вам для цього знадобитися. Крім того, ви можете легко завантажити додаткові програми [15].

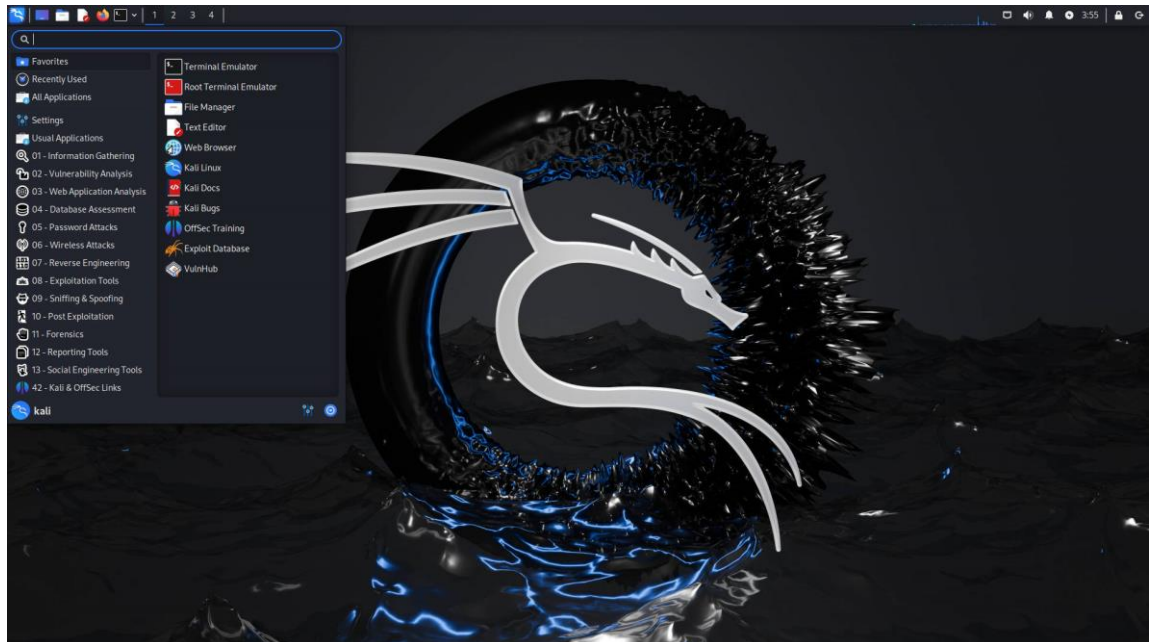


Рисунок 2.3 – Операційна система Kali Linux



Рисунок 2.4 – Маршрутизатор Cisco 7200

Маршрутизатор серії Cisco 7200 – це високопродуктивний маршрутизатор, призначений для використання в корпоративних мережах і мережах провайдерів послуг. Cisco 7200 підтримує широкий спектр інтерфейсів, таких як Ethernet, ATM, POS і послідовне з'єднання, що дозволяє підключати його до різних пристроїв. Цей маршрутизатор також оснащений потужними процесорами та великим об'ємом пам'яті, що дозволяє йому обробляти великі обсяги трафіку та виконувати складну маршрутизацію. Завдяки підтримці різних мережевих протоколів і функцій

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки, Cisco 7200 Series є надійним рішенням для організацій, що потребують стабільної і продуктивної мережевої інфраструктури.



Рисунок 2.5 – Комутатор Cisco Catalyst 2960

Cisco Catalyst 2960 Series є хорошим варіантом для даної мережі, оскільки даний комутатор бюджетний та може забезпечити базову функціональність комутації з можливістю управління. Він підходить для невеликої мережі з помірними вимогами до пропускної здатності та функціональності, забезпечуючи стабільну роботу, енергоефективність та простоту налаштування. Якщо мережа буде збільшуватись та буде потрібність у більшій продуктивності, можна також розглянути більш просунуті моделі, такі як Cisco Catalyst 9300 або 3850, які надають кращу масштабованість, високу продуктивність та підтримку сучасних технологій.

2.2 Опис та архітектура тестової мережі

Комп'ютерна мережа складається з двох окремих сегментів, кожен з яких підключений до окремого маршрутизатора. Незважаючи на те, що маршрутизатори не пов'язані між собою, кожен із них має можливість підключення до Інтернету. Налаштування мережі гарантує, що системи виявлення атак та запобігання вторгненням (IDS/IPS) Snort і Suricata працюють у двох окремих сегментах. При проектуванні налаштовано трирівневу структуру для кожного сегменту для більш реального моделювання ситуації та мережі.

Для проектування великих і складних мереж трирівнева структура мережі є важливим архітектурним підходом. Вона гарантує високу продуктивність, масштабованість і надійність завдяки ефективній організації мережевих інфраструктур.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Основною метою використання трирівневої структури є розподіл мережевих функцій на три різні рівні: ядро (Core), розподілу (Distribution) та доступу (Access). Кожен із цих рівнів виконує певні завдання та є важливим для загального функціонування мережі.

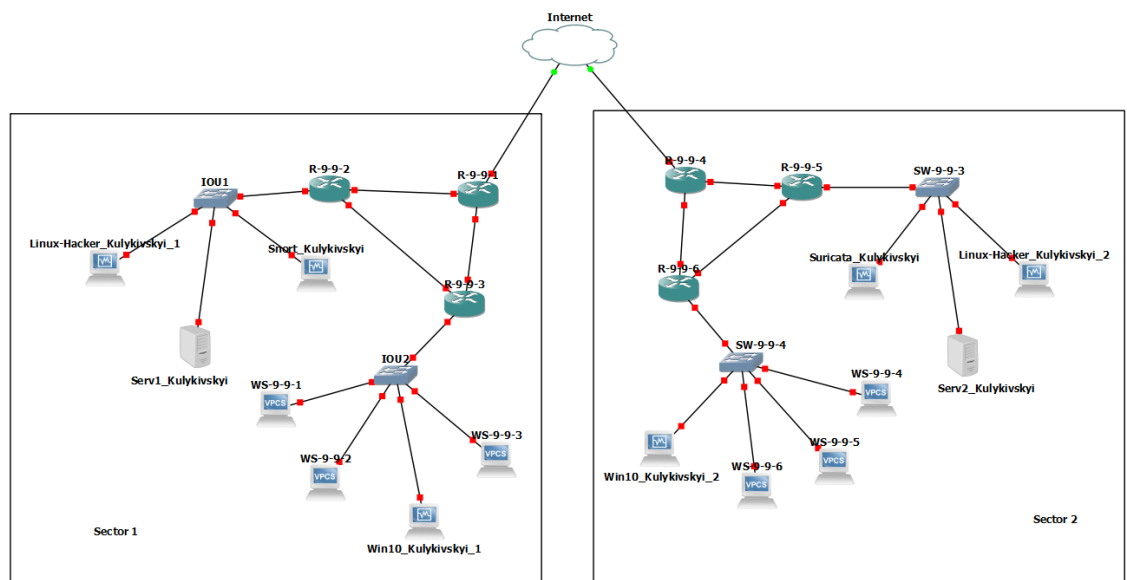


Рисунок 2.6 – Мережа для тестування IDS/IPS

На рівні ядра знаходяться основні маршрутизатори, які забезпечують високу пропускну здатність та швидке пересилання даних між різними сегментами мережі. У цій топології до рівня ядра належать такі пристрої, як R-9-9-1, R-9-9-2, R-9-9-3, R-9-9-4, R-9-9-5, R-9-9-6.

На рівні розподілу знаходяться комутатори, які забезпечують об'єднання мережевих сегментів та розподіл трафіку між кінцевими пристроями та ядром мережі. У даній топології до цього рівня належать наступні пристрої:

- SW-9-9-1 – комутатор сектору 1;
- SW-9-9-2 – комутатор сектору 1;
- SW-9-9-3 – комутатор сектору 2;
- SW-9-9-4 – комутатор сектору 2.

На рівні доступу знаходяться всі кінцеві пристрої та підключення, що забезпечують доступ користувачів до мережі. На цьому рівні здійснюється підключення ПК, серверів та інших пристроїв. У даній топології до рівня доступу належать:

- Linux-Hacker_Kulykivskyi-1 – віртуальна машина Kali Linux для проведення тестів та атак у секторі 1;
- Snort_Kulykivskyi – пристрій зі встановленню системою IDS Snort;
- Serv1_Kulykivskyi – сервер у секторі 1;
- PC-9-9-1 – віртуальний ПК у секторі 1;
- PC-9-9-2 – віртуальний ПК у секторі 1;
- PC-9-9-3 – віртуальний ПК у секторі 1;
- Win10_Kulykivskyi_1 – віртуальна машина з Windows 10 у секторі 1;
- Suricata_Kulykivskyi – пристрій зі встановленню системою IDS Snort;
- Serv2_Kulykivskyi – сервер у секторі 2;
- PC-9-9-4 – віртуальний ПК у секторі 2;
- PC-9-9-5 – віртуальний ПК у секторі 2;
- PC-9-9-6 – віртуальний ПК у секторі 2;
- Win10_Kulykivskyi_2 – віртуальна машина з Windows 10 у секторі 2.

Така архітектура забезпечує високу надійність та ефективність роботи мережі. Ядро мережі забезпечує високошвидкісне пересилання даних, рівень дистрибуції відповідає за об'єднання та управління трафіком між сегментами мережі, а рівень доступу забезпечує підключення кінцевих пристроїв до мережі. Це дозволяє ефективно тестувати та порівнювати роботу систем виявлення загроз Snort та Suricata у різних умовах.

Метою створення даної мережі є тестування та порівняння двох систем виявлення загроз – Snort та Suricata. Мережа розділена на два сектори для забезпечення незалежного середовища для кожної системи, що дозволяє проводити аналіз їх ефективності в реальних умовах. Призначення мережі включає виявлення та аналіз різних типів мережевих загроз, таких як DDoS-атаки, сканування портів та впровадження шкідливого програмного забезпечення.

Мережа складається з маршрутизаторів, комутаторів, серверів та кінцевих пристроїв. Маршрутизатори (R-9-9-1, R-9-9-2, R-9-9-3, R-9-9-4, R-9-9-5, R-9-9-6) забезпечують з'єднання між секторами та підключення до Інтернету. Комутатори (SW-9-9-1, SW-9-9-2, SW-9-9-3, SW-9-9-4) відповідають за об'єднання мережевих

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

сегментів та управління трафіком. Сервери (Serv1_Kulykivskyi, Serv2_Kulykivskyi) забезпечують зберігання та обробку даних, необхідних для роботи систем виявлення загроз. Кінцеві пристрої, такі як ПК, віртуальні машини з Linux та Windows використовуються для проведення тестів та атак.

Для забезпечення безпеки мережа розділена на два окремі сектори, що дозволяє ізолювати трафік та уникати перехресних загроз. Кожен сектор має свою власну систему виявлення загроз (Snort у секторі 1 та Suricata у секторі 2), що дозволяє проводити незалежне тестування та порівняння їх ефективності. Крім того, комутатори та маршрутизатори налаштовані таким чином, щоб забезпечити безпеку та надійність з'єднань між пристроями, включаючи використання VLAN для ізоляції трафіку та запобігання несанкціонованому доступу.

Аналіз трафіку є ключовою частиною роботи мережі. Snort та Suricata встановлені на окремих пристроях у кожному секторі та налаштовані для виявлення та аналізу мережових загроз. Ці системи використовують правила та сигнатури для ідентифікації підозрілого трафіку, таких як DDoS-атаки, сканування портів та впровадження шкідливого програмного забезпечення. Вони забезпечують реальний час моніторинг трафіку та генерують звіти про виявлені загрози, що дозволяє швидко реагувати на інциденти та покращувати загальний рівень безпеки мережі.

Створена мережа забезпечує оптимальне середовище для тестування та порівняння систем виявлення загроз Snort та Suricata. Завдяки розділенню на два сектори, належному налаштуванню підключень та обладнання, ізоляції та забезпеченню безпеки, а також ефективному аналізу трафіку, мережа дозволяє проводити детальні дослідження та покращувати навички у сфері кібербезпеки.

2.3 Розробка схеми адресації мережі

Схема адресації мережі є важливою частиною планування та управління комп'ютерними мережами. Вона забезпечує унікальну ідентифікацію кожного пристрою в мережі, дозволяє ефективно керувати ресурсами та забезпечує належний рівень безпеки. Адресація допомагає уникати конфліктів IP-адрес, сприяє легкому

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

масштабуванню мережі та забезпечує можливість точного моніторингу і управління трафіком.

У цій схемі адресації мережі для двох незалежних сегментів, буде описано розподіл IP-адрес, шлюзів та масок підмереж для кожного пристрою, що дозволить чітко зрозуміти, як організовано мережеве середовище для тестування систем виявлення та запобігання вторгнень (IDS/IPS).

Таблиця 2.2

IP адресація мережі першого сектору

Мережа / Пристрій	Інтерфейс / Ме- режний адаптер / Шлюз	IP-адреса	Маска	Префікс
Підмережа А	-	10.9.9.0	255.255.255.0	/24
Підмережа В	-	11.9.9.0	255.255.255.0	/24
Підмережа С	-	12.9.9.0	255.255.255.0	/24
Підмережа D	-	200.9.9.0	255.255.255.0	/24
Підмережа Е	-	201.9.9.0	255.255.255.0	/24
R-9-9-1	Fa1/0	10.9.9.1	255.255.255.0	/24
	Fa1/1	11.9.9.1	255.255.255.0	/24
R-9-9-2	Fa0/0	10.9.9.2	255.255.255.0	/24
	Fa1/0	12.9.9.1	255.255.255.0	/24
	Fa1/1	200.9.9.1	255.255.255.0	/24
R-9-9-3	Fa0/0	11.9.9.2	255.255.255.0	/24
	Fa1/0	12.9.9.2	255.255.255.0	/24
	Fa1/1	201.9.9.1	255.255.255.0	/24
Serv1_Kulykivskyi	М. адаптер	200.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
Snort PC	М. адаптер	200.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
Linux- Hacker_Kulykivskyi_1	М. адаптер	200.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
WS-9-9-1	М. адаптер	201.9.9.5	255.255.255.0	/24

	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
--	-----------------	-----------	---------------	-----

Продовження таблиці 2.2

IP-адресація мережі першого сектору

Мережа / Пристрій	Інтерфейс / Мережний адаптер / Шлюз	IP-адреса	Маска	Префікс
WS-9-9-2	М. адаптер	201.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
WS-9-9-3	М. адаптер	201.9.9.8	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
Win10_Kulykivskyi_1	М. адаптер	201.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24

Таблиця 2.3

IP адресація мережі другого сектору

Мережа / Пристрій	Інтерфейс / Мережний адаптер / Шлюз	IP-адреса	Маска	Префікс
Підмережа F	-	13.9.9.0	255.255.255.0	/24
Підмережа G	-	14.9.9.0	255.255.255.0	/24
Підмережа H	-	15.9.9.0	255.255.255.0	/24
Підмережа I	-	202.9.9.0	255.255.255.0	/24
Підмережа J	-	203.9.9.0	255.255.255.0	/24
R-9-9-4	Fa1/1	13.9.9.1	255.255.255.0	/24
	Fa1/0	14.9.9.1	255.255.255.0	/24
R-9-9-5	Fa0/0	13.9.9.2	255.255.255.0	/24
	Fa1/0	15.9.9.1	255.255.255.0	/24
	Fa1/1	202.9.9.1	255.255.255.0	/24
R-9-9-6	Fa0/0	14.9.9.2	255.255.255.0	/24
	Fa1/0	15.9.9.2	255.255.255.0	/24

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

	Fa1/1	203.9.9.1	255.255.255.0	/24
--	-------	-----------	---------------	-----

Продовження таблиці 2.3

IP адресація мережі другого сектору

Мережа / Пристрій	Інтерфейс / Ме- режний адаптер / Шлюз	IP-адреса	Маска	Префікс
Serv2_Kulykivskyi	М. адаптер	202.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	202.9.9.1	255.255.255.0	/24
Suricata PC	М. адаптер	202.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	202.9.9.1	255.255.255.0	/24
Linux- Hacker_Kulykivskyi_2	М. адаптер	202.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	202.9.9.1	255.255.255.0	/24
WS-9-9-4	М. адаптер	203.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
WS-9-9-5	М. адаптер	203.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
WS-9-9-6	М. адаптер	203.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
Win10_Kulykivskyi_2	М. адаптер	203.9.9.8	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24

Висновки до другого розділу:

Другий розділ присвячений розробці мережі для тестування, що включає в себе докладний опис її архітектури, схему адресації та опис вибраних операційних систем. Архітектура тестової мережі була спроектована для імітації реальних умов, з урахуванням масштабованості та безпеки, що дозволяє ефективно випробувати різні мережеві конфігурації і протоколи. Схема адресації була розроблена для забезпечення оптимального управління IP-адресами, спрощення маршрутизації та полегшення адміністрування мережі.

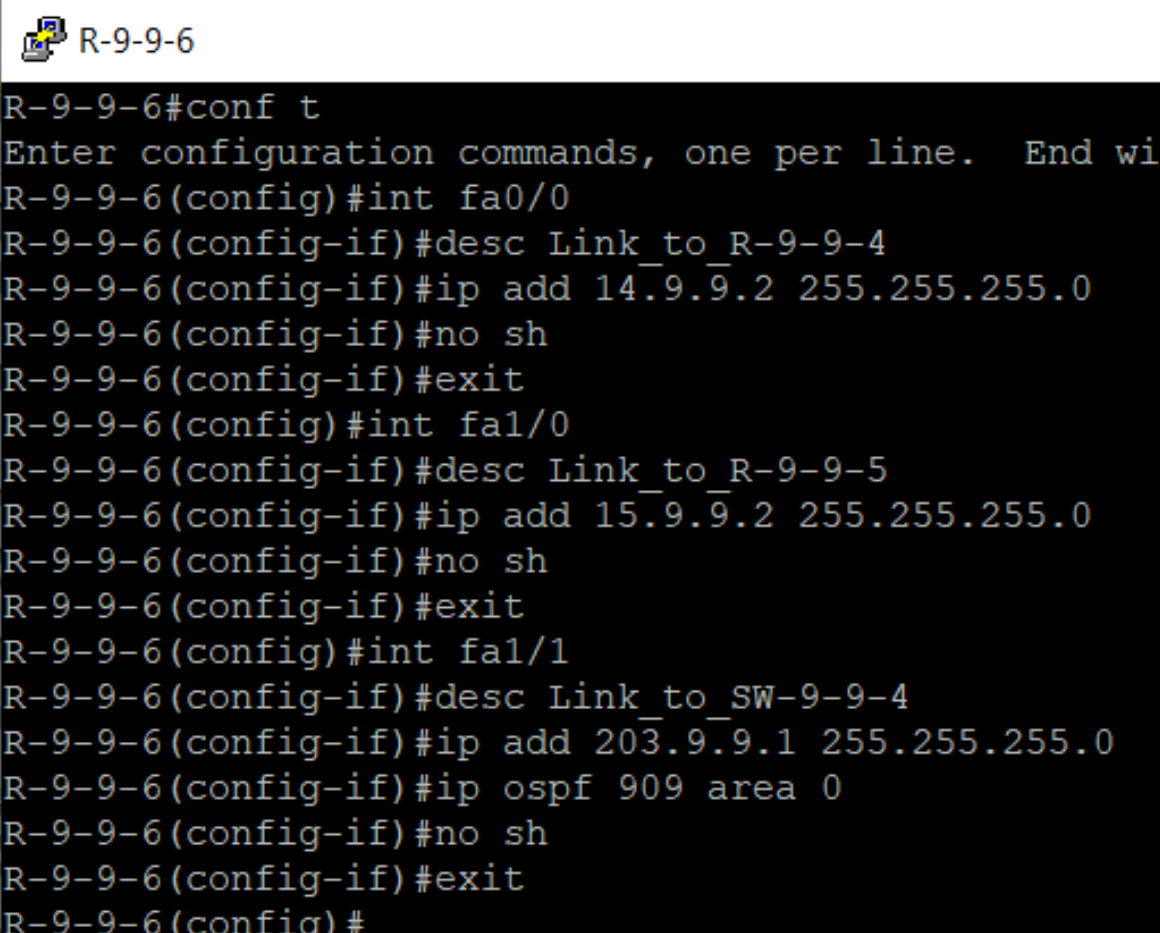
		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 3. ПРОВЕДЕННЯ АНАЛІЗУ ТА ВИЯВЛЕННЯ МЕРЕЖЕВИХ ЗА- ГРОЗ ЗА ДОПОМОГОЮ SNORT ТА SURICATA

3.1 Проведення налаштування мережі

Налаштування IP-адресації є необхідним для ідентифікації всіх пристроїв у мережі, оскільки кожен пристрій повинен мати окрему IP-адресу, яка дозволяє його ідентифікувати. IP-адреси також використовуються для маршрутизації даних, щоб визначити шлях, яким пакети даних мають йти, щоб дістатися до місця призначення.

На кожному пристрої було проведено налаштування IP-адресації для правильної комунікації, що дозволить їм ефективно обмінюватися даними.



```
R-9-9-6#conf t
Enter configuration commands, one per line.  End with Ctrl-Z.
R-9-9-6(config)#int fa0/0
R-9-9-6(config-if)#desc Link_to_R-9-9-4
R-9-9-6(config-if)#ip add 14.9.9.2 255.255.255.0
R-9-9-6(config-if)#no sh
R-9-9-6(config-if)#exit
R-9-9-6(config)#int fa1/0
R-9-9-6(config-if)#desc Link_to_R-9-9-5
R-9-9-6(config-if)#ip add 15.9.9.2 255.255.255.0
R-9-9-6(config-if)#no sh
R-9-9-6(config-if)#exit
R-9-9-6(config)#int fa1/1
R-9-9-6(config-if)#desc Link_to_SW-9-9-4
R-9-9-6(config-if)#ip add 203.9.9.1 255.255.255.0
R-9-9-6(config-if)#ip ospf 909 area 0
R-9-9-6(config-if)#no sh
R-9-9-6(config-if)#exit
R-9-9-6(config)#
```

Рисунок 3.1 – Налаштування маршрутизатора R-9-9-6

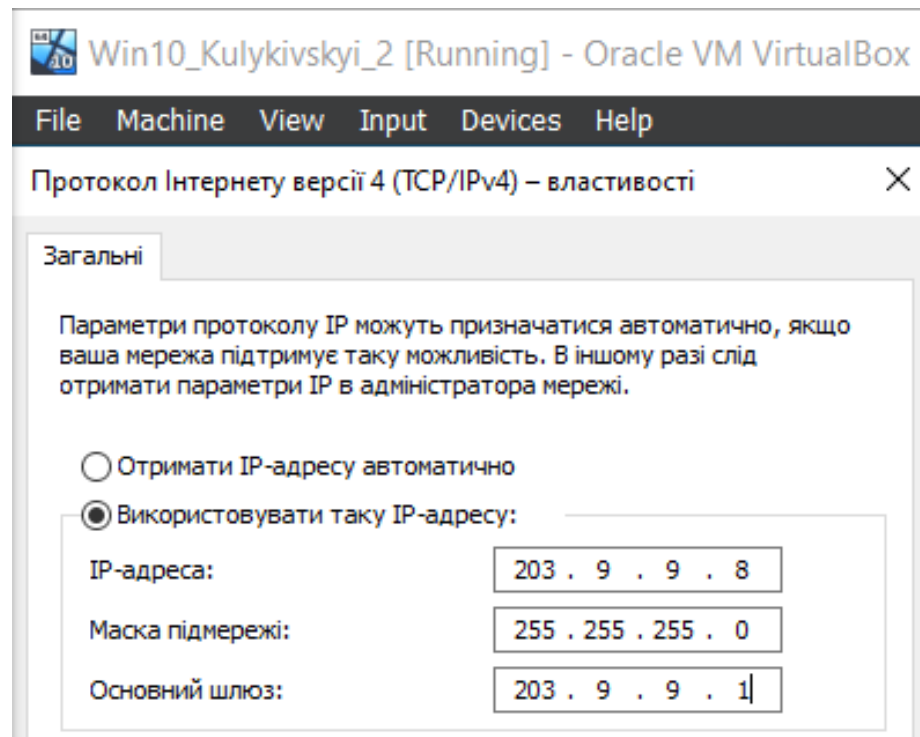


Рисунок 3.2 – Налаштування робочої станції Win10

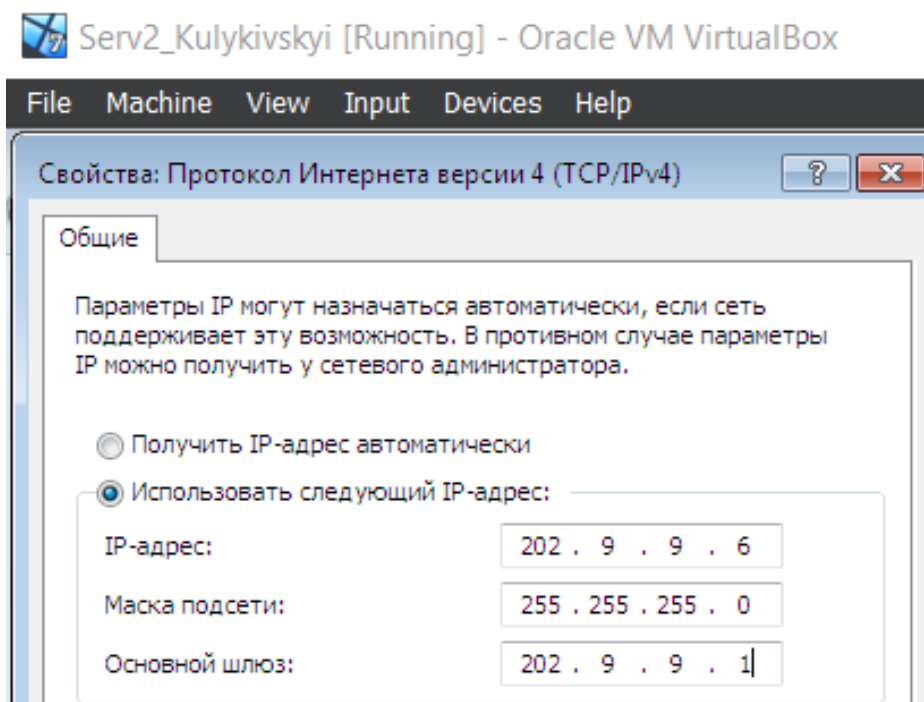


Рисунок 3.3 – Налаштування серверу на базі Win7

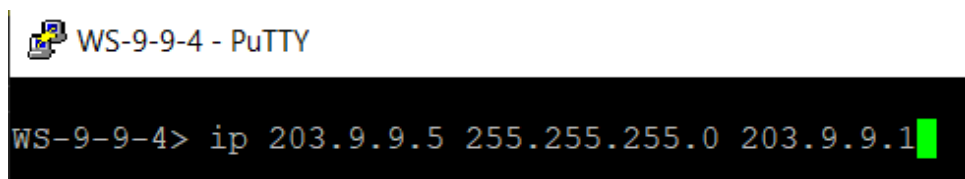


Рисунок 3.4 – Налаштування робочої станції WS-9-9-4

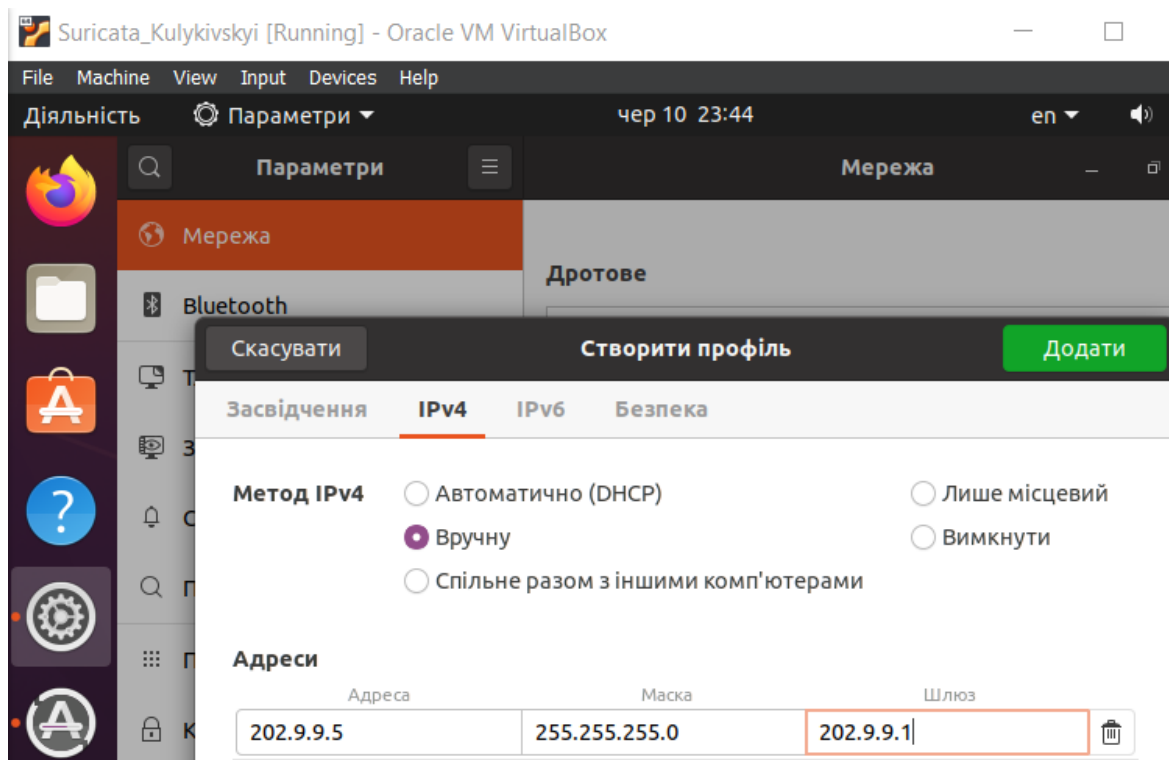


Рисунок 3.5 – Налаштування робочої станції Ubuntu

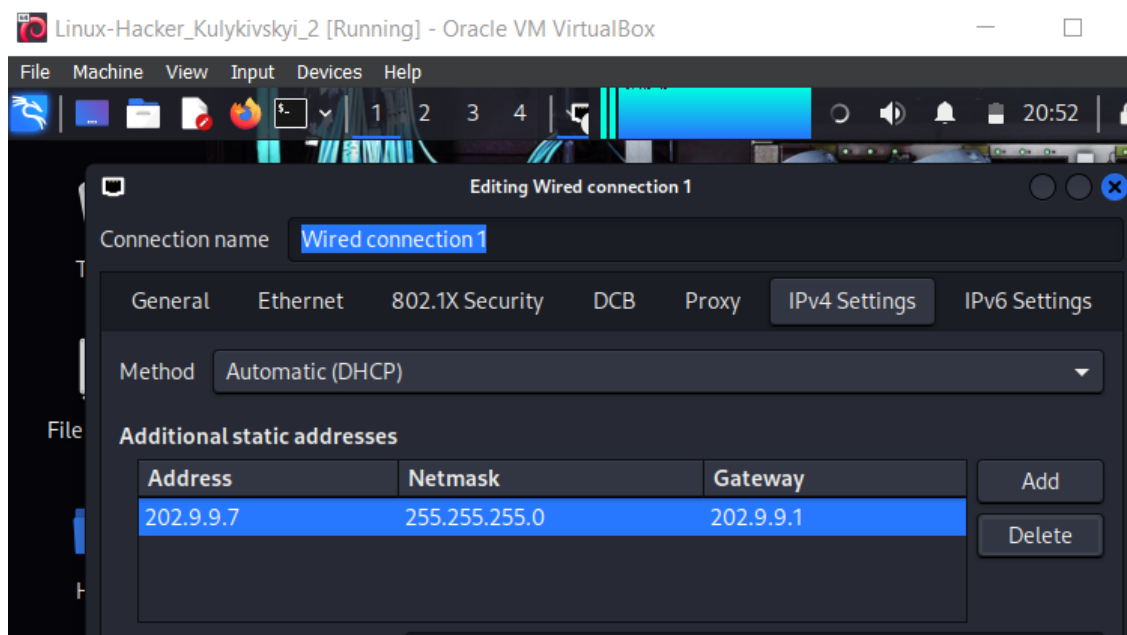


Рисунок 3.6 – Налаштування робочої станції Linux-Hacker

Для інших пристроїв налаштування відбувалися ідентично до наведених рисунків, змінюючи при цьому лише IP-адресу. Для перевірки працездатності мережі було проведено пінгування пристроїв.

```

Win10_Kulykivskiy_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(с) Корпорація Майкрософт. Усі права захищені.
C:\Users\Student>ping 201.9.9.8

Pinging 201.9.9.8 with 32 bytes of data:
Reply from 201.9.9.8: bytes=32 time=1ms TTL=64
Reply from 201.9.9.8: bytes=32 time<1ms TTL=64

Ping statistics for 201.9.9.8:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\Student>ping 200.9.9.6

Pinging 200.9.9.6 with 32 bytes of data:
Reply from 200.9.9.6: bytes=32 time=37ms TTL=126
Reply from 200.9.9.6: bytes=32 time=33ms TTL=126

Ping statistics for 200.9.9.6:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 37ms, Average = 35ms
Control-C
^C
C:\Users\Student>

```

Рисунок 3.7 – Пінгування машини Win10 з іншими пристроями

```

Serv1_Kulykivskiy [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\Windows\system32\cmd.exe
C:\Users\admin>ping 201.9.9.8

Обмен пакетами с 201.9.9.8 по 32 байтам данных:
Ответ от 201.9.9.8: число байт=32 время=40мс TTL=62
Ответ от 201.9.9.8: число байт=32 время=39мс TTL=62

Статистика Ping для 201.9.9.8:
    Пакетов: отправлено = 2, получено = 2, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
        Минимальное = 39мсек, Максимальное = 40 мсек, Среднее = 39 мсек
Control-C
^C
C:\Users\admin>ping 201.9.9.7

Обмен пакетами с 201.9.9.7 по 32 байтам данных:
Ответ от 201.9.9.7: число байт=32 время=33мс TTL=126
Ответ от 201.9.9.7: число байт=32 время=37мс TTL=126

Статистика Ping для 201.9.9.7:
    Пакетов: отправлено = 2, получено = 2, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
        Минимальное = 33мсек, Максимальное = 37 мсек, Среднее = 35 мсек
Control-C
^C

```

Рисунок 3.8 – Пінгування серверу Serv1 з іншими пристроями

Для динамічної маршрутизації використовується протокол OSPF (Open Shortest Path First). Цей протокол автоматично визначає найкращі маршрути для

передачі даних між маршрутизаторами. Він забезпечує масштабованість мережі, що дозволяє легко додати нові маршрутизатори та маршрути без необхідності ручної конфігурації кожного пристрою. Крім того, він швидко реагує на зміни в топології мережі, автоматично перебудовуючи маршрути, якщо стан з'єднання змінюється або додаються нові пристрої. Також використано ntp для узгодженості у логах та інших часових мітках.

```

R-9-9-5
R-9-9-5(config-if)#ex
R-9-9-5(config)#router ospf 909
R-9-9-5(config-router)#network 13.9.9.0 0.0.0.255 area 0
R-9-9-5(config-router)#network 15.9.9.0 0.0.0.255 area 0
R-9-9-5(config-router)#network 15.9.9.0 0.0.0.255 area 0
*Jun 12 00:47:57.811: %OSPF-5-ADJCHG: Process 909, Nbr 14.9.9.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R-9-9-5(config-router)#network 202.9.9.0 0.0.0.255 area 0
R-9-9-5(config-router)#ex
R-9-9-5(config)#exit
R-9-9-5#
*Jun 12 00:48:25.523: %SYS-5-CONFIG_I: Configured from console by console
R-9-9-5#
*Jun 12 00:49:42.831: %OSPF-5-ADJCHG: Process 909, Nbr 15.9.9.2 on FastEthernet1/0 from LOADING to FULL, Loading Done
R-9-9-5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-5(config)#ntp server 192.168.1.10
R-9-9-5(config)#ex
R-9-9-5#
*Jun 12 00:52:42.419: %SYS-5-CONFIG_I: Configured from console by console
R-9-9-5#write memory
Building configuration...
[OK]
R-9-9-5#

```

Рисунок 3.9 – Налаштування протоколу OSPF та NTP

Перевірка статусу OSPF сусідів є критично важливою для виявлення з'єднань і моніторингу стабільності мережі. Команда `show ip ospf neighbor` дозволяє перевірити, чи всі сусіди OSPF правильно налаштовані та підключені. Це допомагає виявити проблеми з логічними або фізичними зв'язками, які потрібно вирішити, а також швидко реагувати на будь-які зміни або відхилення.

Перевірка таблиці маршрутизації за допомогою команди `show ip route` дозволяє переконатися у правильності маршрутів, що використовуються для передачі даних. Це допомагає виявити проблеми з маршрутизацією, такі як відсутні або неправильно налаштовані маршрути, і забезпечує найефективніший маршрут передачі даних.

Перевірка стану інтерфейсів за допомогою команди `show ip interface brief` дозволяє визначити статус усіх інтерфейсів на маршрутизаторі, швидко виявляючи які інтерфейси активні, а які ні. Це необхідно для виявлення проблем з

підключенням або маршрутизацією, а також для спостереження за станом мережі та забезпечення її надійної роботи.

```

R-9-9-1
1/0 from LOADING to FULL, Loading Done
R-9-9-1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
201.9.9.1        1     FULL/DR         00:00:39    11.9.9.2       FastEthernet1/
1
200.9.9.1        1     FULL/DR         00:00:38    10.9.9.2       FastEthernet1/
0
R-9-9-1#

```

Рисунок 3.10 – Перевірка статусу OSPF на маршрутизаторі R-9-9-1

```

R-9-9-1
R-9-9-1#show ip int brief
Interface                IP-Address      OK? Method Status  Prot
ocol
FastEthernet0/0          unassigned      YES NVRAM  up      up
FastEthernet1/0          10.9.9.1        YES NVRAM  up      up
FastEthernet1/1          11.9.9.1        YES NVRAM  up      up
R-9-9-1#

```

Рисунок 3.11 – Перевірка стану інтерфейсів на маршрутизаторі R-9-9-1

```

R-9-9-1
R-9-9-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C       10.9.9.0 is directly connected, FastEthernet1/0
    11.0.0.0/24 is subnetted, 1 subnets
C       11.9.9.0 is directly connected, FastEthernet1/1
O       201.9.9.0/24 [110/2] via 11.9.9.2, 00:10:42, FastEthernet1/1
    12.0.0.0/24 is subnetted, 1 subnets
O       12.9.9.0 [110/2] via 11.9.9.2, 00:10:42, FastEthernet1/1
        [110/2] via 10.9.9.2, 00:10:32, FastEthernet1/0
O       200.9.9.0/24 [110/2] via 10.9.9.2, 00:10:32, FastEthernet1/0
R-9-9-1#

```

Рисунок 3.12 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-1

```

R-9-9-2
R-9-9-2#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
201.9.9.1        1     FULL/DR         00:00:31    12.9.9.2     FastEthernet1/0
11.9.9.1         1     FULL/BDR        00:00:30    10.9.9.1     FastEthernet0/0
R-9-9-2#show ip int brief
Interface        IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0  10.9.9.2        YES NVRAM  up          up
FastEthernet1/0  12.9.9.1        YES NVRAM  up          up
FastEthernet1/1  200.9.9.1       YES NVRAM  up          up
R-9-9-2#

```

Рисунок 3.13 – Перевірка статусу OSPF стану інтерфейсів на маршрутизаторі R-9-9-2

```

R-9-9-2
Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 1 subnets
C    10.9.9.0 is directly connected, FastEthernet0/0
  11.0.0.0/24 is subnetted, 1 subnets
O    11.9.9.0 [110/2] via 12.9.9.2, 00:18:21, FastEthernet1/0
      [110/2] via 10.9.9.1, 00:18:31, FastEthernet0/0
O    201.9.9.0/24 [110/2] via 12.9.9.2, 00:18:21, FastEthernet1/0
  12.0.0.0/24 is subnetted, 1 subnets
C    12.9.9.0 is directly connected, FastEthernet1/0
C    200.9.9.0/24 is directly connected, FastEthernet1/1
R-9-9-2#

```

Рисунок 3.14 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-2

```

R-9-9-3
R-9-9-3#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
200.9.9.1        1     FULL/BDR        00:00:34    12.9.9.1     FastEthernet1/0
11.9.9.1         1     FULL/BDR        00:00:33    11.9.9.1     FastEthernet0/0
R-9-9-3#show ip int brief
Interface        IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0  11.9.9.2        YES NVRAM  up          up
FastEthernet1/0  12.9.9.2        YES NVRAM  up          up
FastEthernet1/1  201.9.9.1       YES NVRAM  up          up
R-9-9-3#

```

Рисунок 3.15 – Перевірка статусу OSPF стану інтерфейсів на маршрутизаторі R-9-9-3

```

R-9-9-3
10.0.0.0/24 is subnetted, 1 subnets
O    10.9.9.0 [110/2] via 12.9.9.1, 00:24:11, FastEthernet1/0
      [110/2] via 11.9.9.1, 00:24:11, FastEthernet0/0
11.0.0.0/24 is subnetted, 1 subnets
C    11.9.9.0 is directly connected, FastEthernet0/0
C    201.9.9.0/24 is directly connected, FastEthernet1/1
12.0.0.0/24 is subnetted, 1 subnets
C    12.9.9.0 is directly connected, FastEthernet1/0
O    200.9.9.0/24 [110/2] via 12.9.9.1, 00:24:11, FastEthernet1/0
R-9-9-3#

```

Рисунок 3.16 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-3

```

R-9-9-4
R-9-9-4#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address        Interface
203.9.9.1        1     FULL/DR         00:00:39    14.9.9.2       FastEthernet1/0
202.9.9.1        1     FULL/DR         00:00:32    13.9.9.2       FastEthernet1/1
R-9-9-4#show ip int brief
Interface        IP-Address      OK? Method Status  Prot
ocol
FastEthernet0/0  unassigned      YES NVRAM  up      up
FastEthernet1/0  14.9.9.1        YES NVRAM  up      up
FastEthernet1/1  13.9.9.1        YES NVRAM  up      up
R-9-9-4#

```

Рисунок 3.17 – Перевірка статусу OSPF стану інтерфейсів
на маршрутизаторі R-9-9-4

```

R-9-9-4
13.0.0.0/24 is subnetted, 1 subnets
C    13.9.9.0 is directly connected, FastEthernet1/1
O    203.9.9.0/24 [110/2] via 14.9.9.2, 00:01:38, FastEthernet1/0
14.0.0.0/24 is subnetted, 1 subnets
C    14.9.9.0 is directly connected, FastEthernet1/0
O    202.9.9.0/24 [110/2] via 13.9.9.2, 00:01:28, FastEthernet1/1
15.0.0.0/24 is subnetted, 1 subnets
O    15.9.9.0 [110/2] via 14.9.9.2, 00:01:38, FastEthernet1/0
      [110/2] via 13.9.9.2, 00:01:28, FastEthernet1/1
R-9-9-4#

```

Рисунок 3.18 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-4

```

R-9-9-5
R-9-9-5#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
203.9.9.1        1     FULL/DR         00:00:37    15.9.9.2     FastEthernet1/0
14.9.9.1         1     FULL/BDR        00:00:35    13.9.9.1     FastEthernet0/0

R-9-9-5#show ip int brief

Interface          IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0    13.9.9.2        YES NVRAM  up          up
FastEthernet1/0    15.9.9.1        YES NVRAM  up          up
FastEthernet1/1    202.9.9.1       YES NVRAM  up          up

R-9-9-5#

```

Рисунок 3.19 – Перевірка статусу OSPF стану інтерфейсів
на маршрутизаторі R-9-9-5

```

R-9-9-5
13.0.0.0/24 is subnetted, 1 subnets
C    13.9.9.0 is directly connected, FastEthernet0/0
O    203.9.9.0/24 [110/2] via 15.9.9.2, 00:03:34, FastEthernet1/0
14.0.0.0/24 is subnetted, 1 subnets
O    14.9.9.0 [110/2] via 15.9.9.2, 00:03:34, FastEthernet1/0
      [110/2] via 13.9.9.1, 00:03:44, FastEthernet0/0
C    202.9.9.0/24 is directly connected, FastEthernet1/1
15.0.0.0/24 is subnetted, 1 subnets
C    15.9.9.0 is directly connected, FastEthernet1/0

R-9-9-5#

```

Рисунок 3.20 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-5

```

R-9-9-6
R-9-9-6#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
202.9.9.1        1     FULL/BDR        00:00:38    15.9.9.1     FastEthernet1/0
14.9.9.1         1     FULL/BDR        00:00:34    14.9.9.1     FastEthernet0/0

R-9-9-6#show ip int brief

Interface          IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0    14.9.9.2        YES NVRAM  up          up
FastEthernet1/0    15.9.9.2        YES NVRAM  up          up
FastEthernet1/1    203.9.9.1       YES NVRAM  up          up

R-9-9-6#

```

Рисунок 3.21 – Перевірка статусу OSPF стану інтерфейсів
на маршрутизаторі R-9-9-6

R-9-9-6

```

13.0.0.0/24 is subnetted, 1 subnets
O    13.9.9.0 [110/2] via 15.9.9.1, 00:04:52, FastEthernet1/0
    [110/2] via 14.9.9.1, 00:04:52, FastEthernet0/0
C    203.9.9.0/24 is directly connected, FastEthernet1/1
14.0.0.0/24 is subnetted, 1 subnets
C    14.9.9.0 is directly connected, FastEthernet0/0
O    202.9.9.0/24 [110/2] via 15.9.9.1, 00:04:52, FastEthernet1/0
15.0.0.0/24 is subnetted, 1 subnets
C    15.9.9.0 is directly connected, FastEthernet1/0
R-9-9-6#

```

Рисунок 3.22 – Перевірка таблиці маршрутизації на маршрутизаторі R-9-9-6

Налаштування IP-адресації та протоколу OSPF є життєво важливими, щоб мережа працювала правильно. OSPF автоматизує процес визначення найкращих маршрутів, забезпечуючи гнучкість і масштабованість мережі, тоді як IP-адресація дозволяє унікально ідентифікувати пристрої та маршрутизувати дані між ними. Регулярна перевірка стану інтерфейсу, таблиці маршрутизації та статусу OSPF сусідів допомагає підтримувати ефективність і стабільність мережі, оскільки це дозволяє швидко знайти та вирішити будь-які проблеми.

3.2 Дослідження інструментів Snort

Snort є потужним інструментом для виявлення мережових атак. Перед встановленням необхідно оновити систему, щоб переконатися що всі пакети є актуальними.

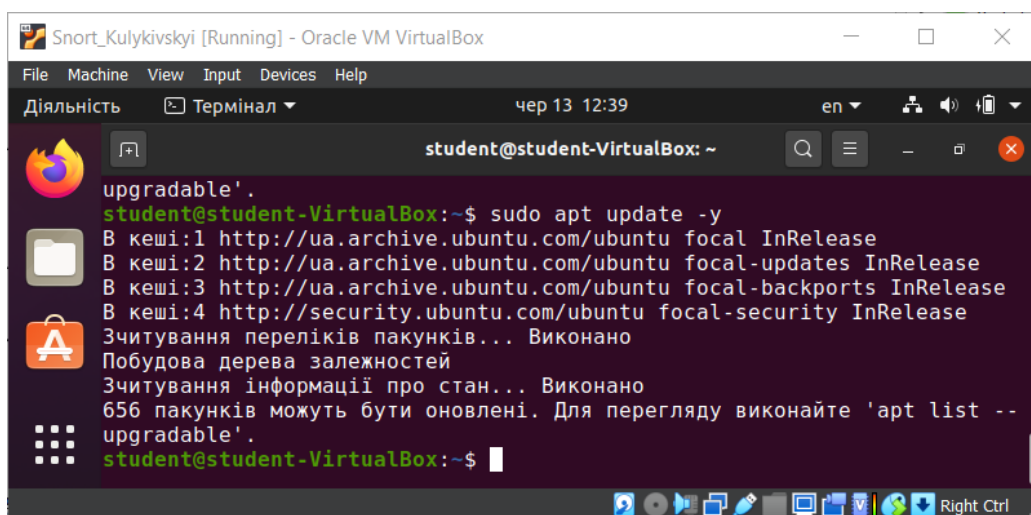


Рисунок 3.23 – Оновлення системи Ubuntu

Snort потребує декілька додаткових пакетів для правильної роботи.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

```

student@student-VirtualBox: ~
upgradable'.
student@student-VirtualBox:~$ sudo apt install -y build-essential libpc
ap-dev libpcrc3-dev libdumbnet-dev bison flex zliblg-dev
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
Буде встановлено такі додаткові пакунки:
  libdumbnet1 libfl-dev libfl2 libpcap0.8-dev libpcrc16-3 libpcrc3
  libpcrc32-3 libpcrcpp0v5 libsigsegv2 m4 zliblg
Пропоновані пакунки:
  bison-doc flex-doc m4-doc
НОВІ пакунки, які будуть встановлені:
  bison flex libdumbnet-dev libdumbnet1 libfl-dev libfl2 libpcap-dev
  libpcap0.8-dev libpcrc16-3 libpcrc3-dev libpcrc32-3 libpcrcpp0v5
  libsigsegv2 m4 zliblg-dev
Пакунки, які будуть ОНОВЛЕНІ:
  build-essential libpcrc3 zliblg
с Параметри, встановлено 15 нових, 0 відмічено для видалення і 653 не он
овлено.
Необхідно завантажити 2 826 kB архівів.
Після цієї операції об'єм зайнятого дискового простору зросте на 8 934
kB.

```

Рисунок 3.24 – Встановлення додаткових пакетів

```

student@student-VirtualBox: ~
student@student-VirtualBox:~$ wget https://www.snort.org/downloads/snor
t/daq-2.0.7.tar.gz
--2024-06-13 12:43:40-- https://www.snort.org/downloads/snort/daq-2.0.
7.tar.gz
Визначення імені www.snort.org (www.snort.org)... 104.19.222.12, 104.19.2
21.12, 2606:4700::6813:de0c, ...
Встановлення з'єднання з www.snort.org (www.snort.org)|104.19.222.12|:4
43... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 302 Found
Розміщення: https://snort-org-site.s3.amazonaws.com/production/release
_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXGB2W5%2F20240613%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20240613T094340Z&X-Amz-Expires=3600&X-
Amz-SignedHeaders=host&X-Amz-Signature=0b5e4c648df7fed12486e1af31598637
65fb86168aab8138d9116468016a22f7 [перехід]
--2024-06-13 12:43:40-- https://snort-org-site.s3.amazonaws.com/produc
tion/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Al
gorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXGB2W5%2F202406
13%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240613T094340Z&X-Amz-Ex

```

Рисунок 3.25 – Встановлення DAQ (Data Acquisition Library)

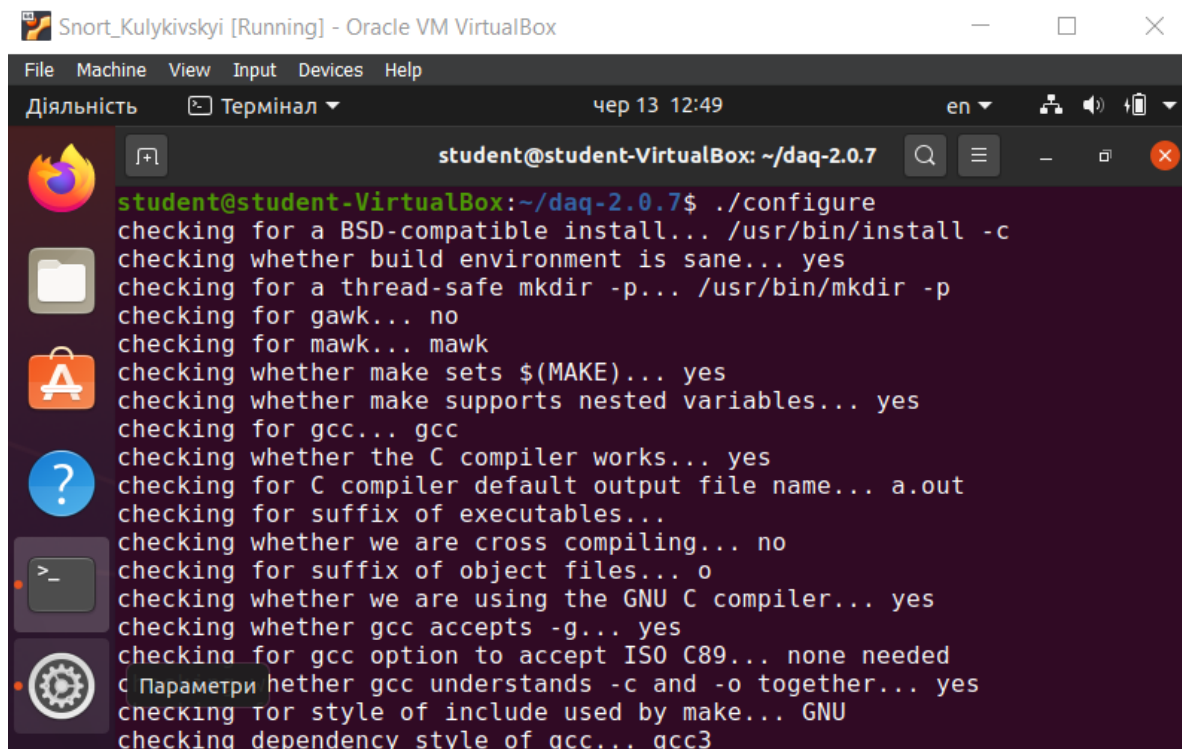


Рисунок 3.26 – Встановлення DAQ (Data Acquisition Library)

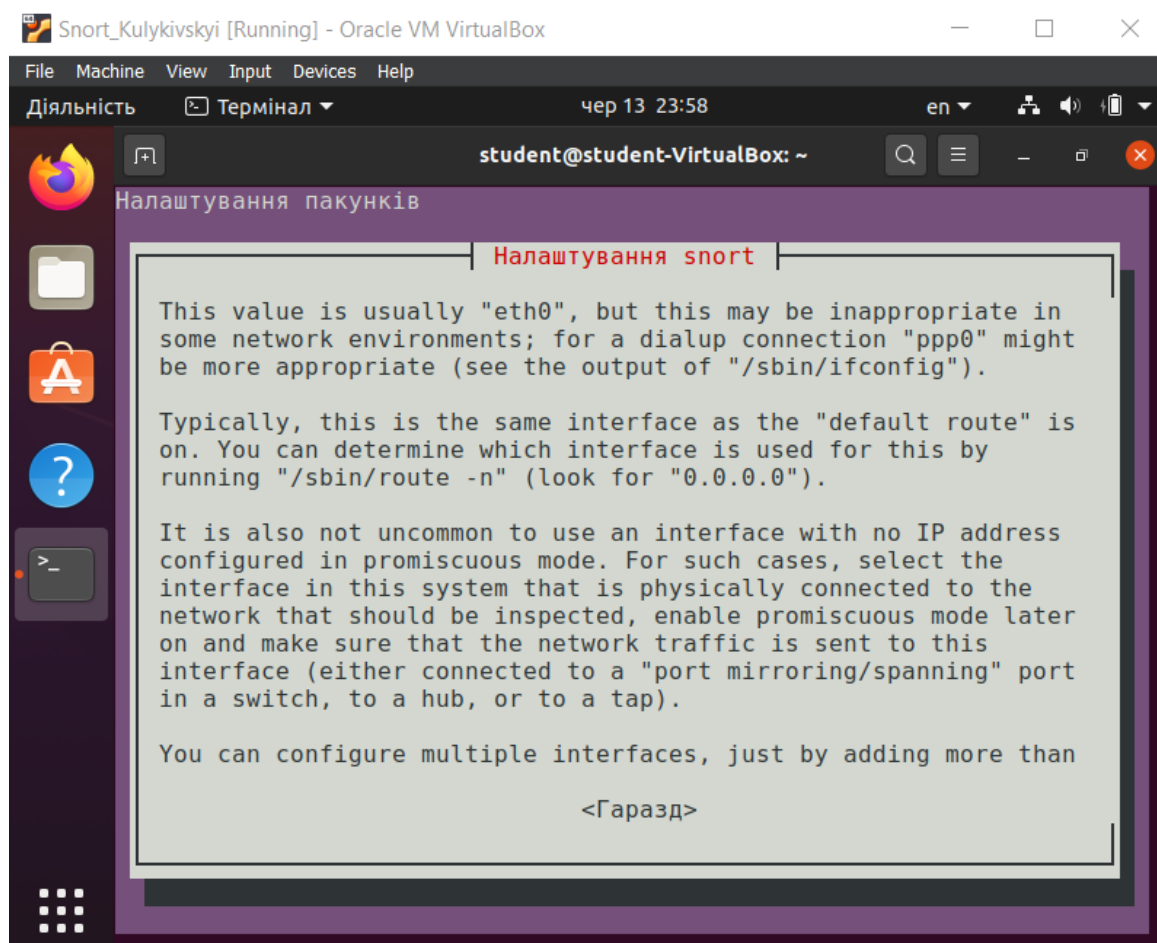


Рисунок 3.27 – Налаштування пакунків Snort

		Куликівський ІД			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

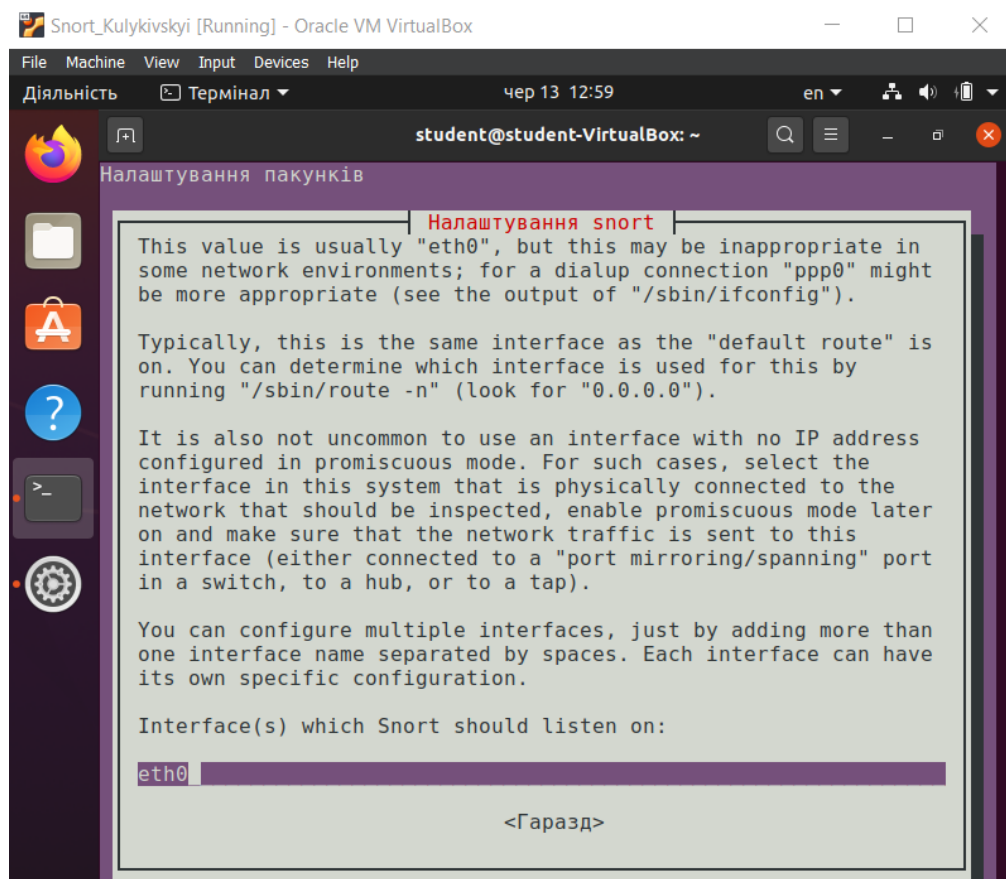


Рисунок 3.28 – Налаштування Snort

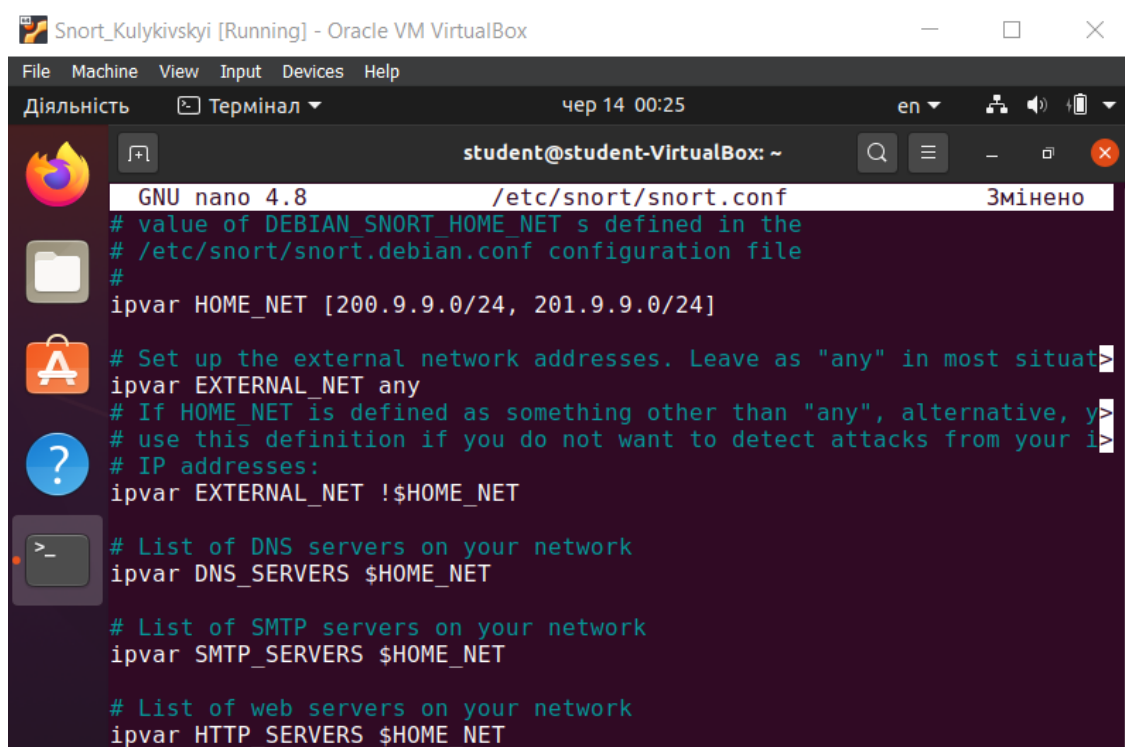


Рисунок 3.29 – Налаштування конфігураційного файлу Snort

		Куликівський ІД			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

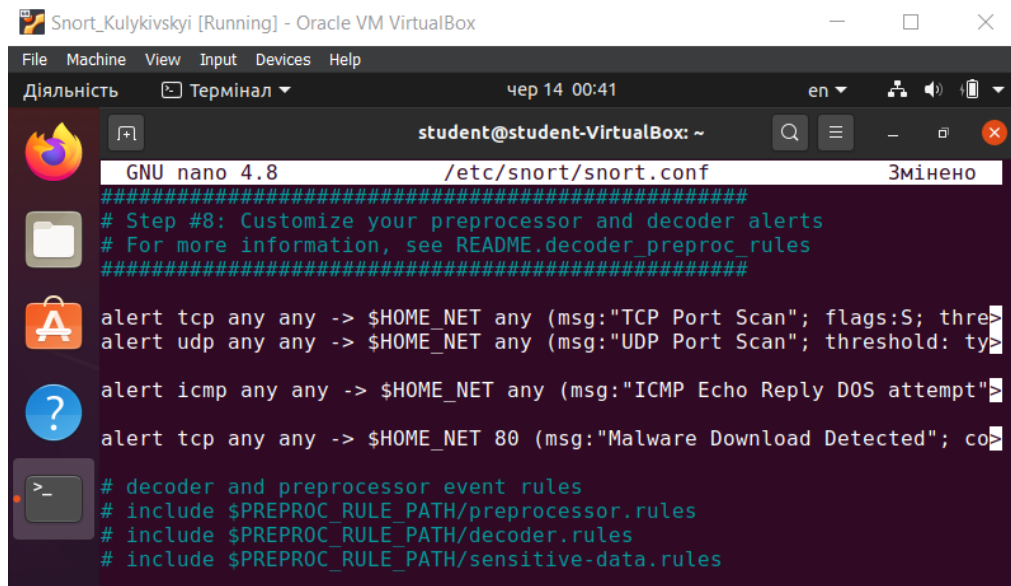


Рисунок 3.30 – Налаштування конфігурації для виявлення атак

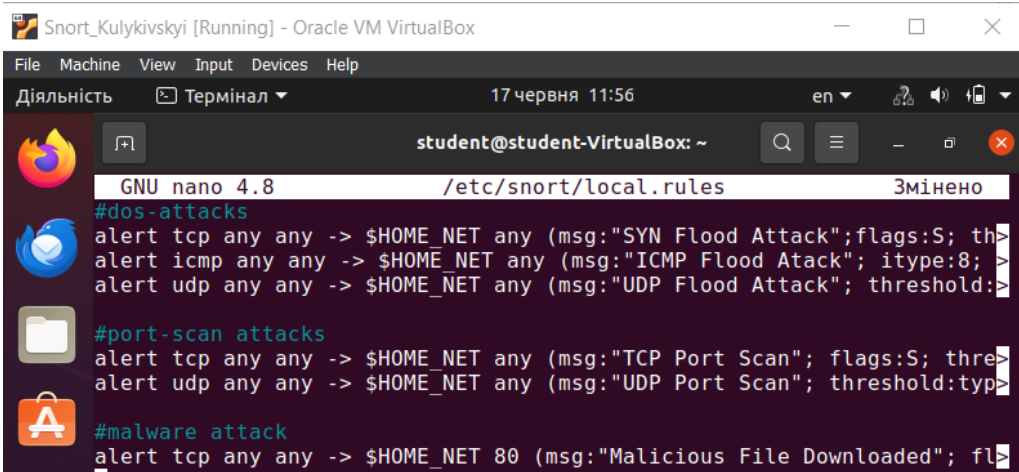


Рисунок 3.31 – Правила для виявлення атак у файлі local.rules

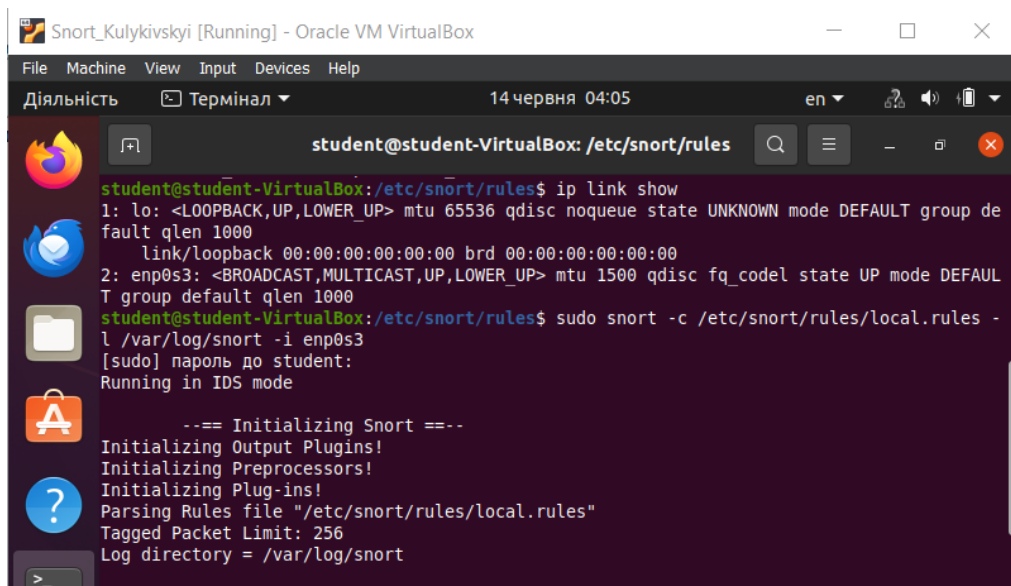


Рисунок 3.32 – Перевірка мережевих інтерфейсів та запуск Snort

На рисунку використано команди для перевірки мережевих інтерфейсів та запуск Snort у режимі IDS на віртуальній машині Ubuntu. Перевірено інтерфейс `enp0s3` і запущено Snort з використанням правил з файлу `local.rules`. Вихідний журнал зберігається в `/var/log/snort`.

Вивід показує, що Snort працює в режимі виявлення (IDS). Це можна побачити по рядку `Running in IDS mode`. Рядок `Tagged Packet Limit: 256` вказує максимальну кількість помічених пакетів. Директорію для журналів можна дізнатися з рядку `Log directory = /var/log/snort`.

```

-----[Rule Port Counts]-----
|      tcp      udp      icmp      ip
|  src          0          0          0          0
|  dst          0          0          0          0
|  any          0          0          0          0
|  nc           0          0          0          0
|  s+d          0          0          0          0
-----

-----[detection-filter-config]-----
| memory-cap : 1048576 bytes
-----[detection-filter-rules]-----
| none
-----

-----[rate-filter-config]-----
| memory-cap : 1048576 bytes
-----[rate-filter-rules]-----
| none
-----

-----[event-filter-config]-----
| memory-cap : 1048576 bytes
-----[event-filter-global]-----
| none
-----[event-filter-local]-----
| none
-----[suppression]-----
| none
-----

```

Рисунок 3.33 – Результат запуску Snort з інформацією про конфігурацію правил та фільтрів

Таблиця *Rule Port Counts* показує кількість правил, які налаштовані для моніторингу різних типів трафіку. Кількість правил, що застосовуються до джерел (відправника) трафіку – src (source). Кількість правил, що застосовується до місця призначення (отримувача) трафіку – dst (destination). Правила, які застосовуються до будь-якого трафіку, незалежно від джерела або місця призначення – any. Правила без конкретного налаштування – nc (Not Configured). Правила, які застосовуються одночасно до джерела і місця призначення – s+d. З таблиці видно, що на даний момент немає налаштованих правил для TCP, UDP, ICMP або IP трафіку.

Таблиця *Detection-filter* – фільтри виявлення. `Detection-filter config` вказує максимальне обмеження пам'яті для конфігурації фільтра виявлення (`1048576 bytes`, тобто 1 МБ). `Detection-filter rules` показує, що наразі немає правил фільтра виявлення, налаштованих у конфігураціях.

Таблиця *Rate-filter* – фільтри швидкості. `Rate-filter config` вказує обмеження пам'яті для фільтрів швидкості (1048576 bytes). `Rate-filter rules` показує, що наразі немає немає налаштованих правил для фільтрації швидкості трафіку.

Таблиця *Event-filter* – фільтрові події. `Event-filter-config` показує обмеження пам'яті для конфігурації, а інші вказують відсутність правил фільтрації.

```

=====
Run time for packet processing was 1132.286032 seconds
Snort processed 3 packets.
Snort ran for 0 days 0 hours 18 minutes 52 seconds
  Pkts/min:      0
  Pkts/sec:      0
=====
Memory usage summary:
  Total non-mmapped bytes (arena):      4849664
  Bytes in mapped regions (hblkhd):     21590016
  Total allocated space (uordblks):     4584912
  Total free space (fordblks):          264752
  Topmost releasable block (keepcost):  122560
=====
Packet I/O Totals:
  Received:      4
  Analyzed:      3 ( 75.000%)
  Dropped:       0 (  0.000%)
  Filtered:      0 (  0.000%)
  Outstanding:   1 ( 25.000%)
  Injected:      0
  
```

Рисунок 3.34 – Вивід Snort після завершення його роботи

Інформація включає підсумок обробки пакетів, використання пам'яті та загальні дані по вводу/виводу пакетів.

Час, протягом якого Snort обробляв пакети = 1132,286032 секунди.

По загальним результатам обробки можна сказати, що всього оброблено 3 пакети; Snort працював 18 хвилин 52 секунди; 0 пакетів на секунду/хвилину.

За майже 19 хвилин роботи, Snort обробив 4 пакети, з яких 3 були проаналізовані, а 1 залишився невирішеним. Загальна використана пам'ять складає 4849664 байти (незамаплена область), 21590016 байт – у відображених областях пам'яті, із загальною виділеною пам'яттю 4584912 байт і вільною пам'яттю 264752 байт.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Найбільший вивільнюваний блок пам'яті становить 122560 байт. Відсоток проаналізованих пакетів складає 75%, з них 33.333% пакетів є IPv4, 33.333% – UDP, і 66.667% – IPv6. Інформація по обробці пакетів показує, що Snort успішно виконав аналіз отриманих даних, не фільтруючи і не відкидаючи жодного пакета.

По загальним даним по вводу/виводу пакетів можна сказати, що отримано 4 пакети; проаналізовано 3 пакети (75%); відкинута 0 пакетів; відфільтровано 0 пакетів; непроаналізовано 1 пакет (25%); введено 0 пакетів.

```

student@student-VirtualBox: ~
[sudo] пароль до student:
Running in Test mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
  Tagged Packet Limit: 256
  
```

Рисунок 3.35 – Перевірка конфігурації перед запуском Snort

```

1>
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>

Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_S7COMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>

Total snort Fixed Memory Cost - MaxRss:50028
Snort successfully validated the configuration!
Snort exiting
student@student-VirtualBox:~$
  
```

Рисунок 3.36 – Вдала перевірка конфігурації

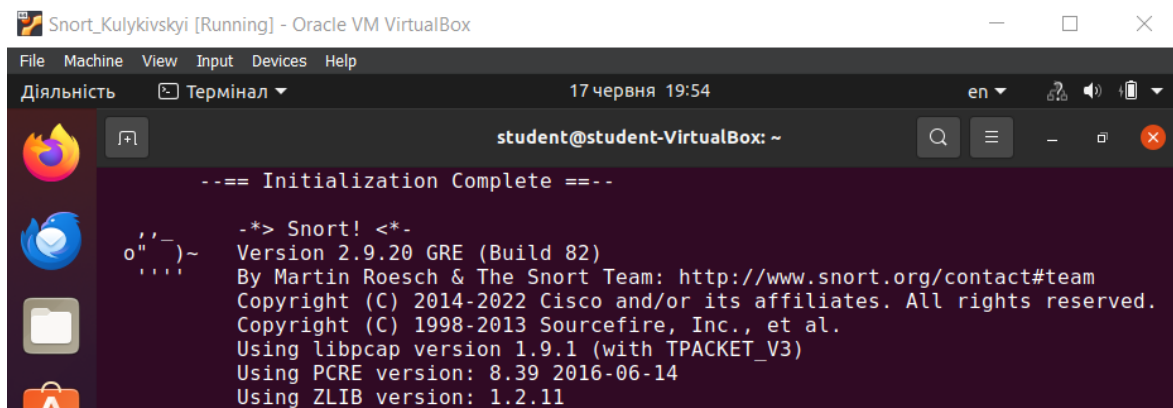


Рисунок 3.37 – Запуск Snort для моніторингу мережі

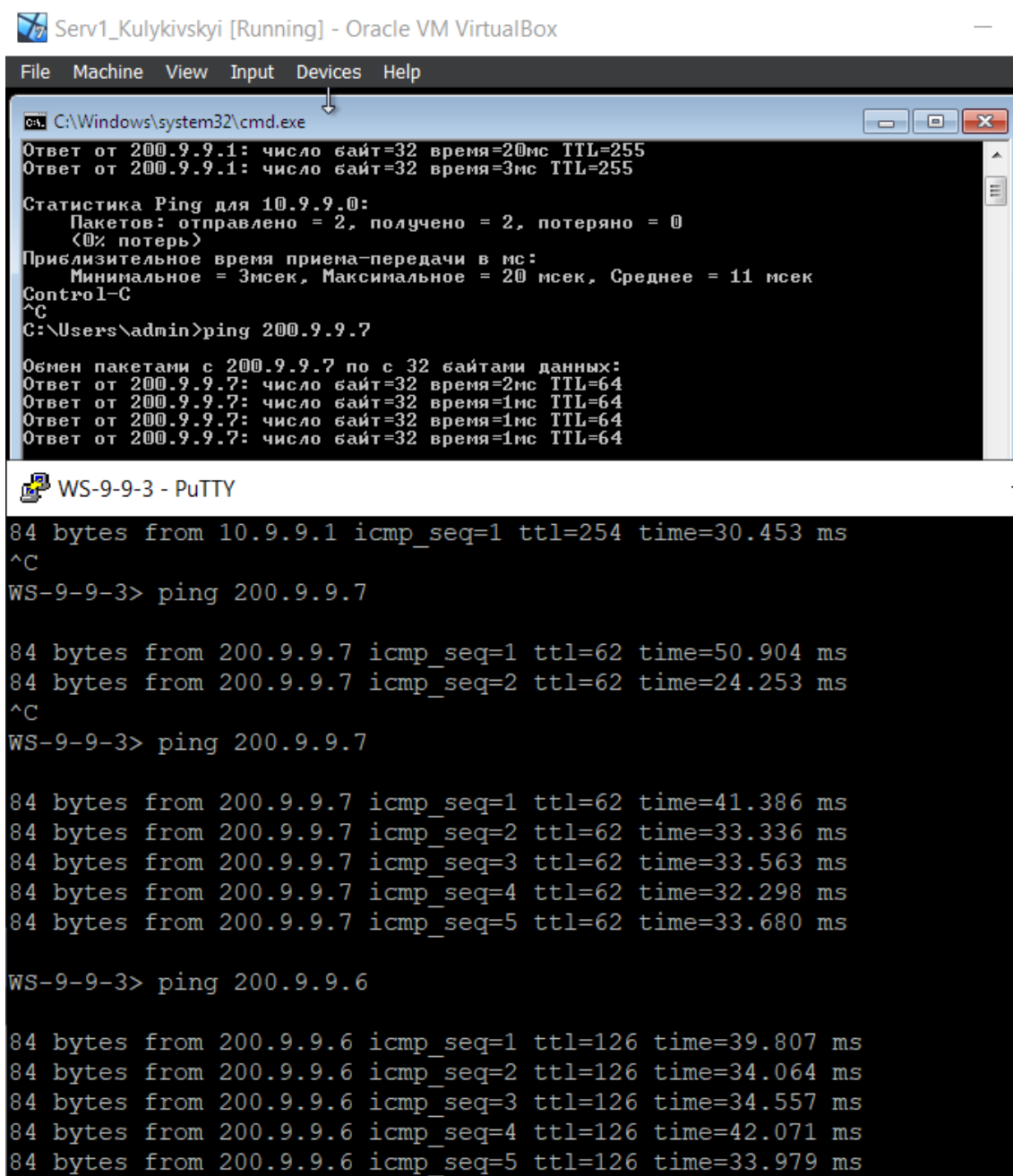


Рисунок 3.38 – Успішна перевірка зв'язку між пристроями

		Куликівський ІД			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

Snort_Kulykivskiy [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Діяльність Термінал 17 червня 19:59
student@student-VirtualBox: ~

Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Commencing packet processing (pid=2142)
^C*** Caught Int-Signal
=====
Run time for packet processing was 167.39613 seconds
S Файли rocessed 144 packets.
Snort ran for 0 days 0 hours 2 minutes 47 seconds
Pkts/min: 72
Pkts/sec: 0
=====
Memory usage summary:
Total non-mmapped bytes (arena): 11149312
Bytes in mapped regions (hblkhd): 30797824
Total allocated space (uordblks): 8859056
Total free space (fordblks): 2290256
Topmost releasable block (keepcost): 17872
=====
Packet I/O Totals:
Received: 146
Analyzed: 144 ( 98.630%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 2 ( 1.370%)
Injected: 0

```

Рисунок 3.39 – Результат моніторингу інструменту Snort

На рисунку показано результат роботи інструменту Snort після проведення атаки типу ping. Snort працював протягом 167.39613 секунд, або близько 2 годин 2 хвилин та 47 секунд. За цей час було оброблено 144 пакети, всі з яких були проаналізовані, не було жодного відфільтрованого або втраченого пакету, що свідчить про 100% ефективність обробки. Використання пам'яті включало загальний обсяг виділеної пам'яті (arena) близько 11.4 млн байтів, з яких 3 млн байтів використано для мапованих регіонів (hblkhd). Загальний обсяг виділеного простору становив 8.9 млн байтів, з яких 3.3 млн байтів були доступні для виділення. Найбільший блок, який може бути звільнений, становив 17872 байти. Пакетні операції вводу/виводу показали, що було прийнято 146 пакетів, з яких 144 були проаналізовані, не було жодного дропнутого чи відфільтрованого пакету, і лише 2 пакети залишилися непроаналізованими. Ці дані свідчать про ефективну роботу Snort при моніторингу та аналізі мережевого трафіку під час проведення ping-атаки, демонструючи його здатність до виявлення та аналізу мережевих подій.

```

(kali@kali)-[~]
$ ping 201.9.9.8
PING 201.9.9.8 (201.9.9.8) 56(84) bytes of data:
64 bytes from 201.9.9.8: icmp_seq=1 ttl=62 time=49.1 ms
64 bytes from 201.9.9.8: icmp_seq=2 ttl=62 time=33.1 ms
64 bytes from 201.9.9.8: icmp_seq=3 ttl=62 time=41.4 ms
64 bytes from 201.9.9.8: icmp_seq=4 ttl=62 time=39.5 ms
64 bytes from 201.9.9.8: icmp_seq=5 ttl=62 time=39.4 ms
^C
--- 201.9.9.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 33.132/40.512/49.147/5.140 ms

(kali@kali)-[~]
$ nmap -p- 200.9.9.6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-17 17:21 UTC
Nmap scan report for 200.9.9.6
Host is up (0.015s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 31.96 seconds
  
```

Рисунок 3.40 – Перевірка зв’язку машини Kali-Linux та проведення атаки сканування портів за допомогою команди nmap

```

Preprocessor Object: appid Version 1.1 <Build 5>
Commencing packet processing (pid=2244)
06/18-14:09:01.636399  [*] [1:1000006:1] UDP Port Scan  [*] [Priority:
0] {UDP} 200.9.9.6:137 -> 200.9.9.255:137
06/18-14:15:15.591916  [*] [1:1000006:1] UDP Port Scan  [*] [Priority:
0] {UDP} 200.9.9.6:137 -> 200.9.9.255:137
  
```

Рисунок 3.41 – Сповіщення про сканування портів на машину Serv1 (200.9.9.6)

```

Linux-Hacker_Kulykivskiy_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ hping3 -S- --flood -V 200.9.9.6
hping3: invalid option -- S
Try hping3 --help
(kali@kali)-[~]
$ ping -s 65507 200.9.9.6
PING 200.9.9.6 (200.9.9.6) 65507(65535) bytes of data.
^C
— 200.9.9.6 ping statistics —
1538 packets transmitted, 0 received, 100% packet loss, time 1538829ms
pipe 60
(kali@kali)-[~]
$

```

Рисунок 3.42 – Проведення атаки `Ping of Death` за допомогою команди ping

```

Snort_Kulykivskiy [Running] - Oracle VM VirtualBox
Діяльність Термінал 17 червня 20:58
student@student-VirtualBox: ~
=====
Run time for packet processing was 1704.465002 seconds
Snort processed 1483 packets.
Snort ran for 0 days 0 hours 28 minutes 24 seconds
Pkts/min: 52
Pkts/sec: 0
=====
Memory usage summary:
Total non-mmapped bytes (arena): 11149312
Bytes in mapped regions (hblkhd): 30797824
Total allocated space (uordblks): 8858848
Total free space (fordblks): 2290464
Topmost releasable block (keepcost): 25008
=====
Packet I/O Totals:
Received: 1483
Analyzed: 1483 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
Injected: 0
=====

```

Рисунок 3.43 – Результат аналізу Snort

На рисунку зображено результат роботи Snort після обробки мережевого трафіку. Загальний час роботи становить 1704.465002 секунди, протягом якого Snort обробив 1483 пакети. Середня швидкість обробки становила 52 пакети на хвилину. Всі 1483 пакети були проаналізовані, жоден пакет не було відкинуто або відфільтровано.

Загальний обсяг невіртуальної пам'яті становить 11149312 байтів, обсяг пам'яті в відображених регіонах становить 30797824 байти, а загальний виділений простір — 8858848 байтів. Вільний простір становить 2290464 байти.

```

student@student-VirtualBox: ~
=====
Memory Statistics of DCE at: Mon Jun 17 20:49:06 2024

dcerpc2 Preprocessor Statistics:
    Total sessions :      0
    Active sessions :      0
    Total SMB sessions :      0
    Total TCP sessions :      0
    Total UDP sessions :      0
    Total HTTP server sessions :      0
    Total HTTP proxy sessions :      0
Total Memory stats :
    Current total : 52428800
    Maximum total : 52515830
    Total memcap :      0
    Free total :      0

SMB Memory stats :
    Current total : 52428800
    Maximum total : 52428800
    Current session data : 52428800
    Maximum session data : 52428800
    Current segmentation buffer :      0
    Maximum segmentation buffer :      0

TCP Memory stats :
    Current total :      0
    Maximum total :      0
    Current session data :      0
    Maximum session data :      0

UDP Memory stats :
    Current total :      0
  
```

Рисунок 3.44 – Результат аналізу Snort

Підсумкова статистика стосується різних протоколів і видів сесій, таких як SMB, TCP, UDP, HTTP та HTTP проху, однак усі значення для цих сесій дорівнюють нулю, що означає, що жодних активних сесій не було виявлено. Статистика пам'яті показує, що поточне загальне використання пам'яті становить 52428800 байтів, з максимальним значенням 52515830 байтів, і жодної вільної пам'яті (memcap) не зареєстровано. Аналогічна ситуація спостерігається для SMB пам'яті,

де поточні та максимальні значення також складають 52428800 байтів, і немає даних про сегментацію. Для протоколів TCP і UDP не зареєстровано використання пам'яті, що підтверджує відсутність активних сесій.

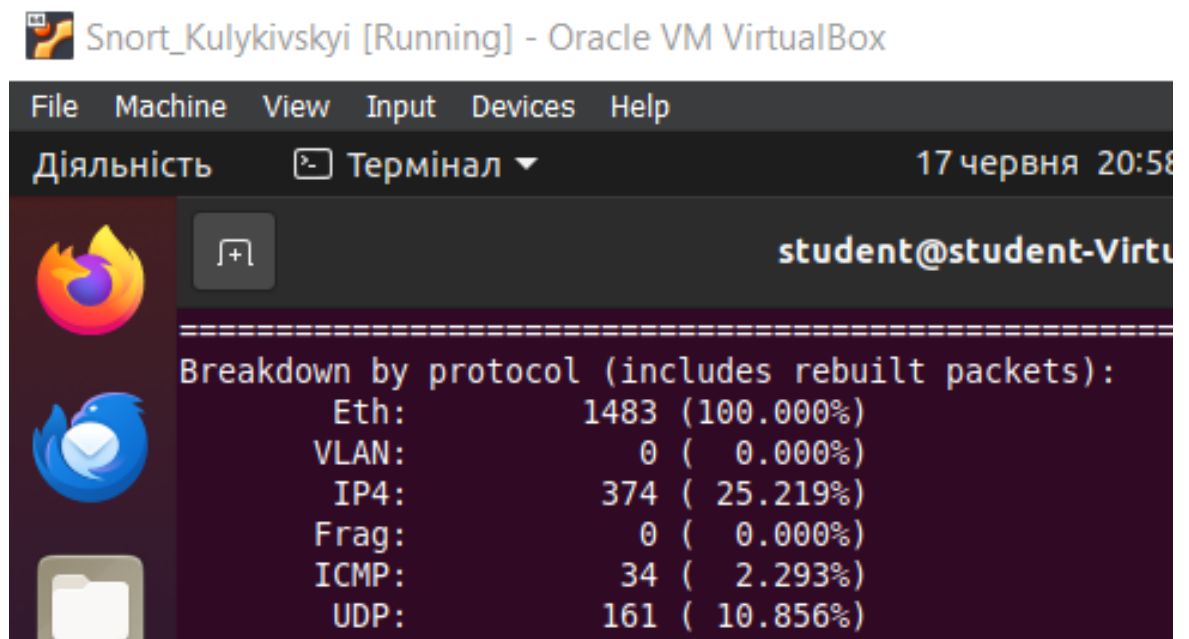


Рисунок 3.45 – Результат аналізу Snort

Загальна кількість пакетів Ethernet становить 1483, що становить 100% від усіх пакетів. Із них 374 пакети (25.219%) належать до протоколу IPv4, 34 пакети (3.293%) до ICMP, і 161 пакет (10.856%) до UDP. Пакетів протоколу VLAN та фрагментованих пакетів (Frag) не виявлено. Це дозволяє побачити загальну картину мережевого трафіку та визначити, які протоколи використовуються в мережі.

Аналіз показав, що мережевий трафік складався переважно з пакетів Ethernet, IPv4, ICMP та UDP, без фрагментованих або VLAN пакетів. Відсутність активних сесій для протоколів SMB, TCP, UDP та HTTP свідчить про специфіку трафіку у цій мережі або можливу відсутність атак з використанням цих протоколів. Також, значення пам'яті та інші ресурси системи використовувалися ефективно, не перевищуючи лімітів. Ці результати демонструють здатність Snort ефективно моніторити та аналізувати мережевий трафік, навіть у випадках атак, забезпечуючи детальну інформацію про склад і характер трафіку в мережі.

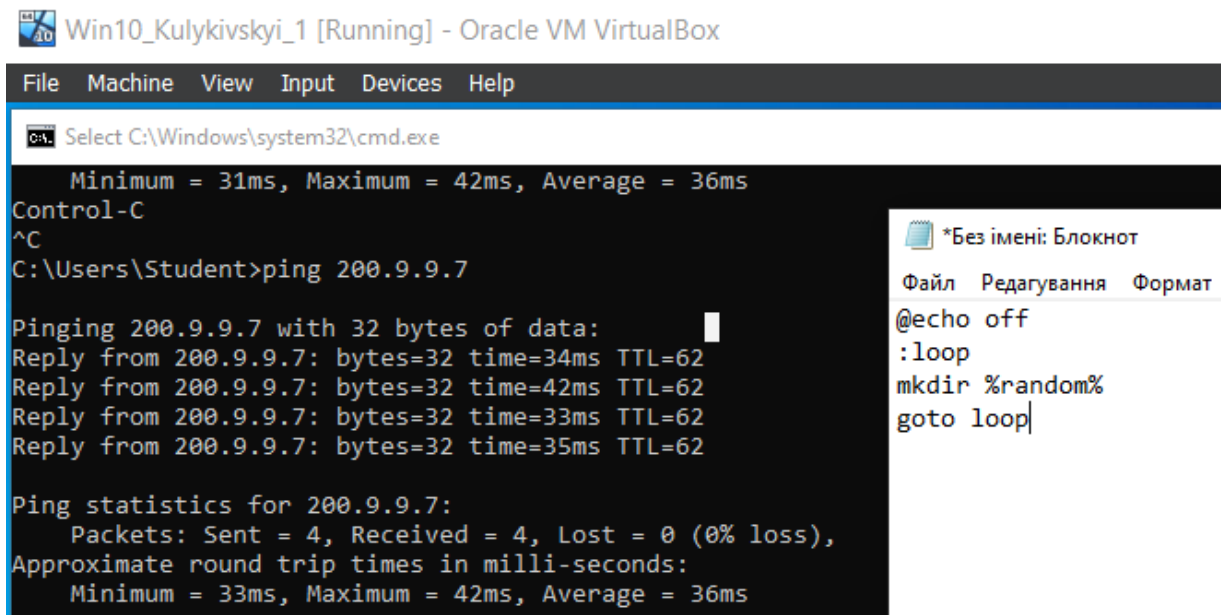


Рисунок 3.46 – Перевірка зв'язку та створення простого коду для виконання шкідливих дій

Шкідливий код створює нескінченну кількість папок. Створюємо мітку `loop`, після чого команда `mkdir %random%` створює папку та за допомогою команди `goto loop` повертається назад до мітки. Таким чином шкідливе ПЗ працює поки його не вимкнута.

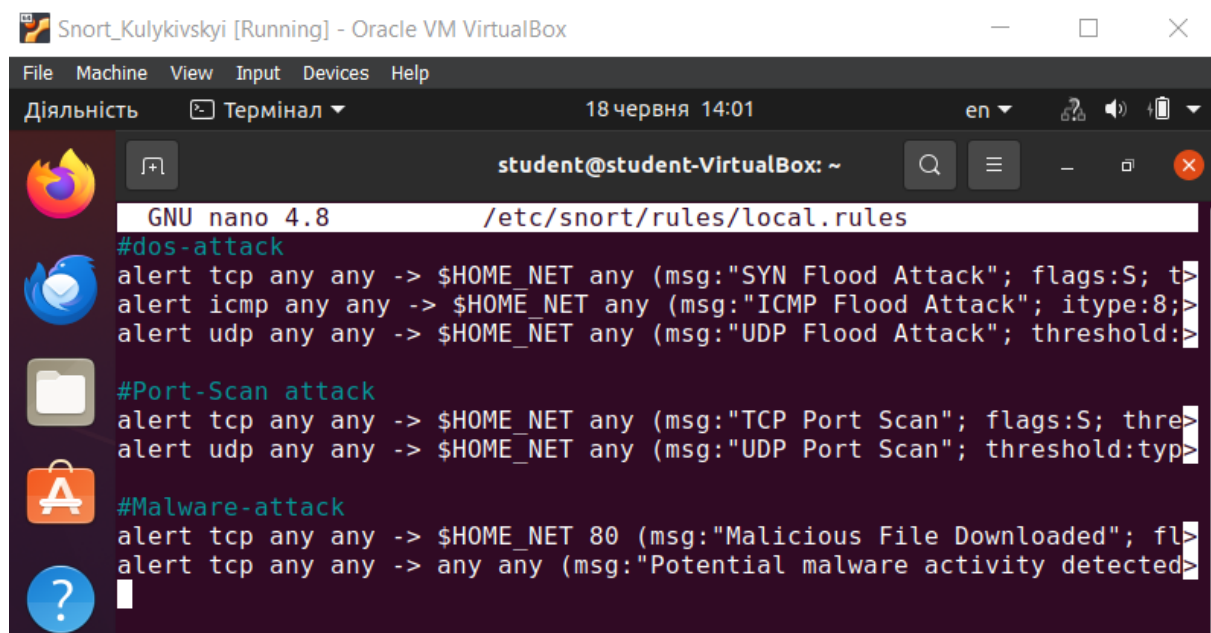


Рисунок 3.47 – Оновлення правил для виявлення підозрілої активності

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

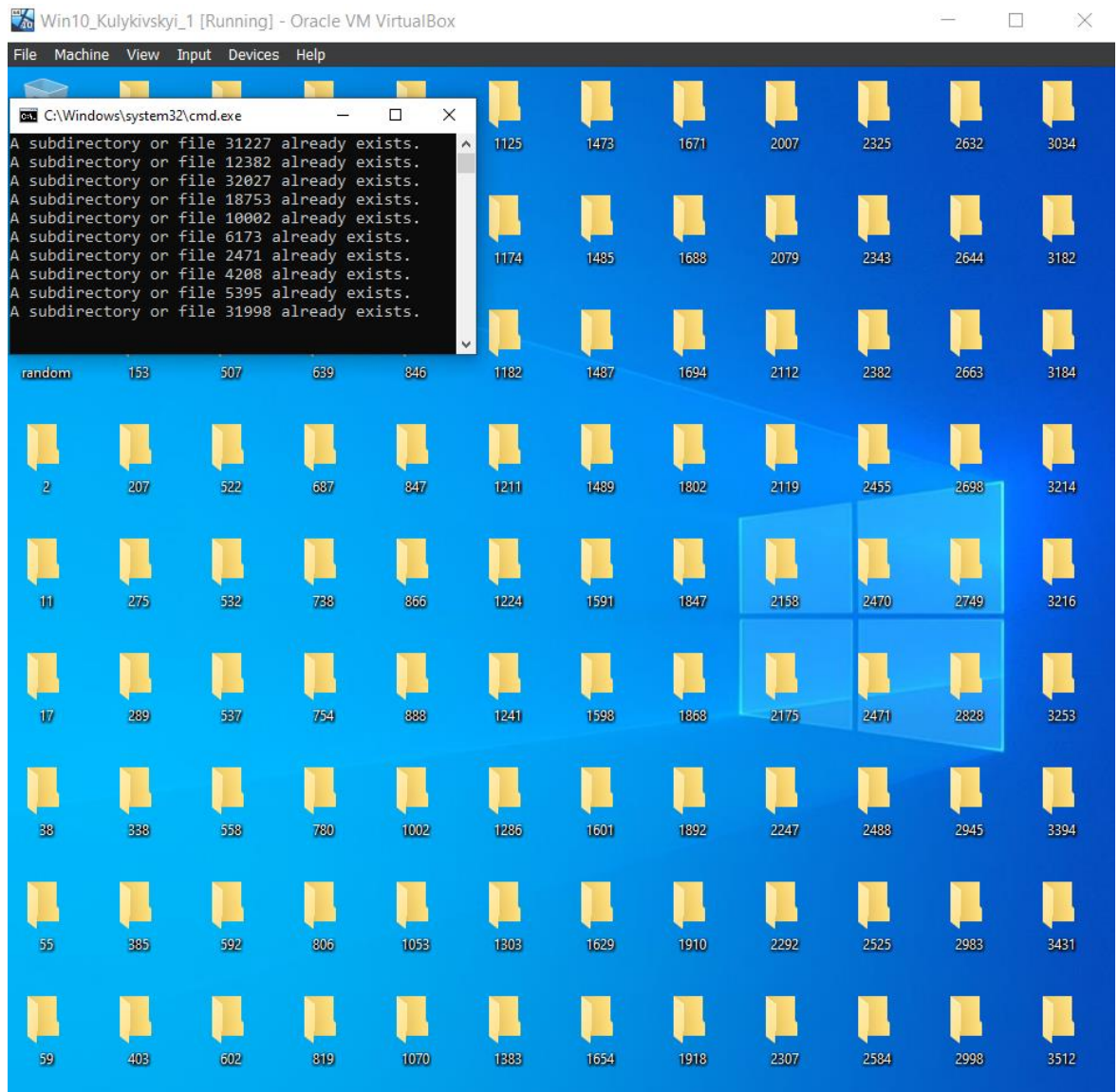


Рисунок 3.48 – Запуск шкідливого програмного забезпечення

```
WS-9-9-3 - PuTTY
WS-9-9-3> ping 201.9.9.7

84 bytes from 201.9.9.7 icmp_seq=1 ttl=128 time=0.738 ms
84 bytes from 201.9.9.7 icmp_seq=2 ttl=128 time=0.877 ms
84 bytes from 201.9.9.7 icmp_seq=3 ttl=128 time=1.227 ms
84 bytes from 201.9.9.7 icmp_seq=4 ttl=128 time=1.285 ms
84 bytes from 201.9.9.7 icmp_seq=5 ttl=128 time=1.019 ms

WS-9-9-3> ping 201.9.9.7

84 bytes from 201.9.9.7 icmp_seq=1 ttl=128 time=1.259 ms
84 bytes from 201.9.9.7 icmp_seq=2 ttl=128 time=1.244 ms
84 bytes from 201.9.9.7 icmp_seq=3 ttl=128 time=1.061 ms
84 bytes from 201.9.9.7 icmp_seq=4 ttl=128 time=1.010 ms
84 bytes from 201.9.9.7 icmp_seq=5 ttl=128 time=0.900 ms

WS-9-9-3> 
```

Рисунок 3.49 – Перевірка зв'язку з машиною

```
Snort_Kulykivskiy [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Діяльність Термінал 18 червня 14:40 en
student@student-VirtualBox: ~

=====
Run time for packet processing was 1355.400265 seconds
Snort processed 1378 packets.
Snort ran for 0 days 0 hours 22 minutes 35 seconds
  Pkts/min:      62
  Pkts/sec:       1
=====
Memory usage summary:
  Total non-mmapped bytes (arena):      11182080
  Bytes in mapped regions (hblkhd):     30797824
  Total allocated space (uordblks):     8882000
  Total free space (fordblks):          2300080
  Topmost releasable block (keepcost):  33168
=====
Packet I/O Totals:
  Received:      1378
  Analyzed:      1378 (100.000%)
  Dropped:        0 ( 0.000%)
  Filtered:       0 ( 0.000%)
  Outstanding:   0 ( 0.000%)
  Injected:       0
=====
Breakdown by protocol (includes rebuilt packets):
  Eth:           1378 (100.000%)
  VLAN:          0 ( 0.000%)
  IP4:           387 ( 28.084%)
=====
```

Рисунок 3.50 – Результат моніторингу програмою

```
Snort_Kulykivskiy [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Діяльність Термінал 18 червня 14:43 en
student@student-VirtualBox: ~

Heap Statistics of file:
  Total Statistics:
    Memory in use:      280 bytes
    No of allocs:       6
    No of frees:        1
  Session Statistics:
    Memory in use:      0 bytes
    No of allocs:       1
    No of frees:        1
  Mempool Statistics:
    Memory in use:      280 bytes
    No of allocs:       5
    No of frees:        0
=====
+-----[filtered events]-----
| gen-id=1      sig-id=1000005   type=Both   tracking=src count=20
seconds=3      filtered=124
| gen-id=1      sig-id=1000006   type=Both   tracking=src count=20
seconds=60     filtered=122
| gen-id=1      sig-id=1000004   type=Both   tracking=src count=20
seconds=3      filtered=31
Snort exiting
student@student-VirtualBox:~$
```

Рисунок 3.51 – Результат моніторингу програмою

На рисунку 3.50 можна побачити, що пам'ять, використана під час обробки, включає байтів невіртуальної пам'яті (arena), 30797824 байти пам'яті у відображених регіонах (hblkhd), 8882000 байтів виділеного простору (uordblks) і 2390080 байтів вільного простору (fordblks). Найвищий рівень звільняемого блоку (keepcost) становить 33168 байтів. Усі 1378 отриманих пакетів належать до протоколу Ethernet (100.000%), з яких 387 пакетів (28.084%) належать до протоколу IPv4.

На рисунку 3.51 з результататми роботи Snort показано кілька відфільтрованих подій. Перша подія (sig-id=1000005) має тип "Both" і відстежується за джерелом, з 20 випадками за 3 секунди та 124 відфільтрованими подіями. Друга подія (sig-id=1000006) також має тип "Both" і відстежується за джерелом, з 20 випадками за 60 секунд та 122 відфільтрованими подіями. Третя подія (sig-id=1000004) має ті ж характеристики, що і попередні, з 20 випадками за 3 секунди та 31 відфільтрованою подією. Ці дані відображають, як система фільтрує та відстежує підозрілу або потенційно небезпечну мережеву активність на основі заданих правил і сигнатур.

3.3 Дослідження інструментів Suricata

Тепер, провдемо дослідження Suricata. Для початку потрібно оновити всі пакети системи.

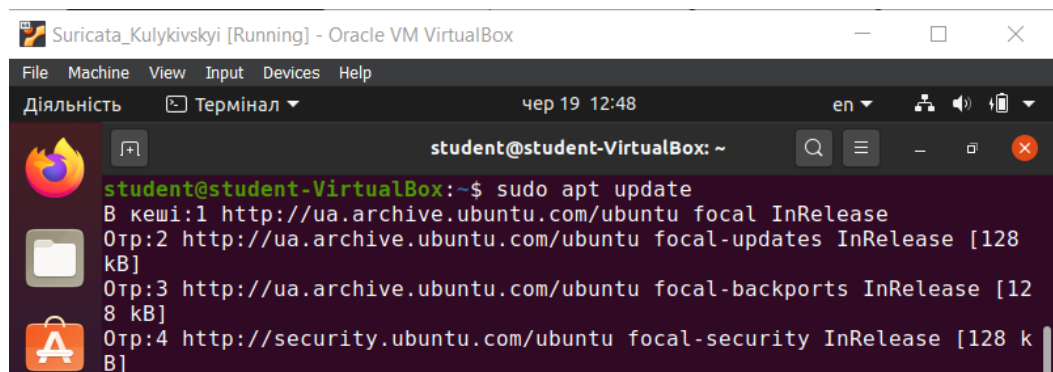


Рисунок 3.52 – Оновлення системи Ubuntu

Suricata потребує додаткові пакети для коректної роботи. Займемось їх встановленням.

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

```

student@student-VirtualBox:~$ sudo apt install -y software-properties-common
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
software-properties-common вже є новою версією (0.99.9.12).
software-properties-common позначений як встановлений вручну.
Наступні пакунки були встановлені автоматично і більше не потрібні:
gir1.2-goa-1.0 libfprint-2-tod1 libfwupdplugin1 libllvm10 libxmlb1
linux-headers-5.4.0-47 linux-headers-5.4.0-47-generic
linux-headers-5.4.0-48 linux-headers-5.4.0-48-generic
linux-image-5.4.0-47-generic linux-image-5.4.0-48-generic
linux-modules-5.4.0-47-generic linux-modules-5.4.0-48-generic
linux-modules-extra-5.4.0-47-generic
linux-modules-extra-5.4.0-48-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.
оновлено 0, встановлено 0 нових, 0 відмічено для видалення і 0 не оновлено.
student@student-VirtualBox:~$ sudo add-apt-repository -y ppa:oisf/suricata-stable
В кеші:1 http://ua.archive.ubuntu.com/ubuntu focal InRelease
В кеші:2 http://ua.archive.ubuntu.com/ubuntu focal-updates InRelease
В кеші:3 http://ua.archive.ubuntu.com/ubuntu focal-backports InRelease
Отр:4 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease [17,5 kB]
В кеші:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Отр:6 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal/main amd64 Packages [1 364 B]
Отр:7 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal/main Translation-en [1 204 B]
Отримано 20,1 kB за 2с (11,3 kB/s)
Зчитування переліків пакунків... Виконано
student@student-VirtualBox:~$

```

Рисунок 3.53 – Встановлення додаткових пакетів Suricata

Тепер встановимо Suricata за допомогою менеджера пакетів `apt`. Для цього використаємо команду *sudo apt install -y suricata*.

```

student@student-VirtualBox:~$ sudo apt install -y suricata
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
Наступні пакунки були встановлені автоматично і більше не потрібні:
gir1.2-goa-1.0 libfprint-2-tod1 libfwupdplugin1 libllvm10 libxmlb1 linux-headers-5.4.0-47
linux-headers-5.4.0-47-generic linux-headers-5.4.0-48 linux-headers-5.4.0-48-generic
linux-image-5.4.0-47-generic linux-image-5.4.0-48-generic linux-modules-5.4.0-47-generic
linux-modules-5.4.0-48-generic linux-modules-extra-5.4.0-47-generic
linux-modules-extra-5.4.0-48-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.
Буде встановлено такі додаткові пакунки:
libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2
libhyperscan5 liblua5.1-2 liblua5.1-common liblzma-dev libnet1
libnetfilter-queue1
Пропоновані пакунки:
liblzma-doc
НОВІ пакунки, які будуть встановлені:
libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2
libhyperscan5 liblua5.1-2 liblua5.1-common liblzma-dev libnet1
libnetfilter-queue1 suricata
оновлено 0, встановлено 12 нових, 0 відмічено для видалення і 0 не оновлено.
Необхідно завантажити 6 075 kB архівів.
Після цієї операції об'єм зайнятого дискового простору зростає на 27,5 MB.

```

Рисунок 3.54 – Встановлення Suricata

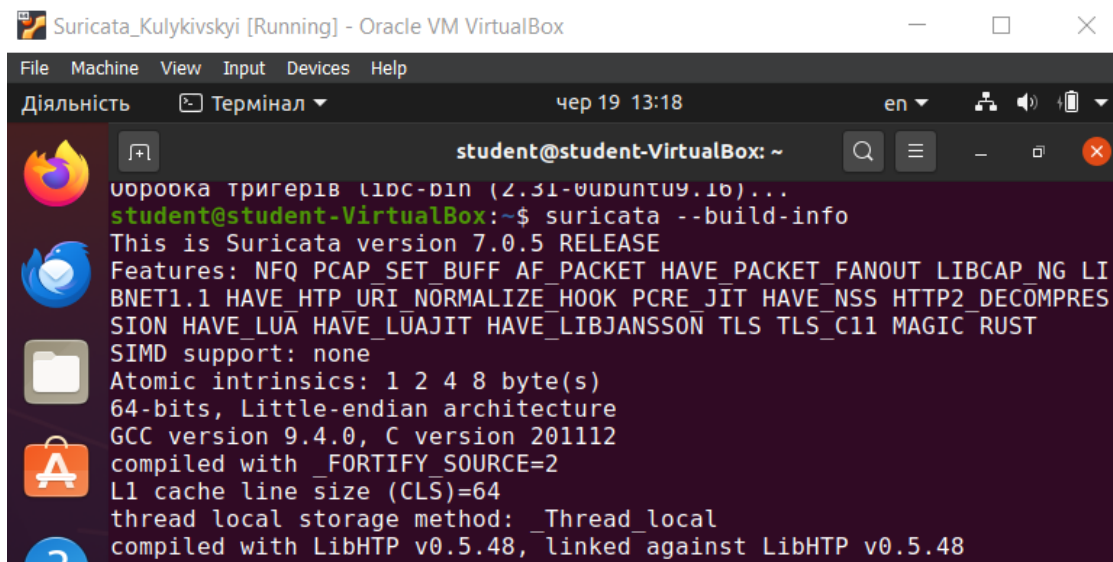


Рисунок 3.55 – Перевірка встановлення Suricata та її версії

Щоб налаштувати Suricata для моніторингу атак та сповіщень про них, необхідно налаштувати конфігураційний файл `suricata.yaml`, додати відповідні правила і переконатися, що вони активні.

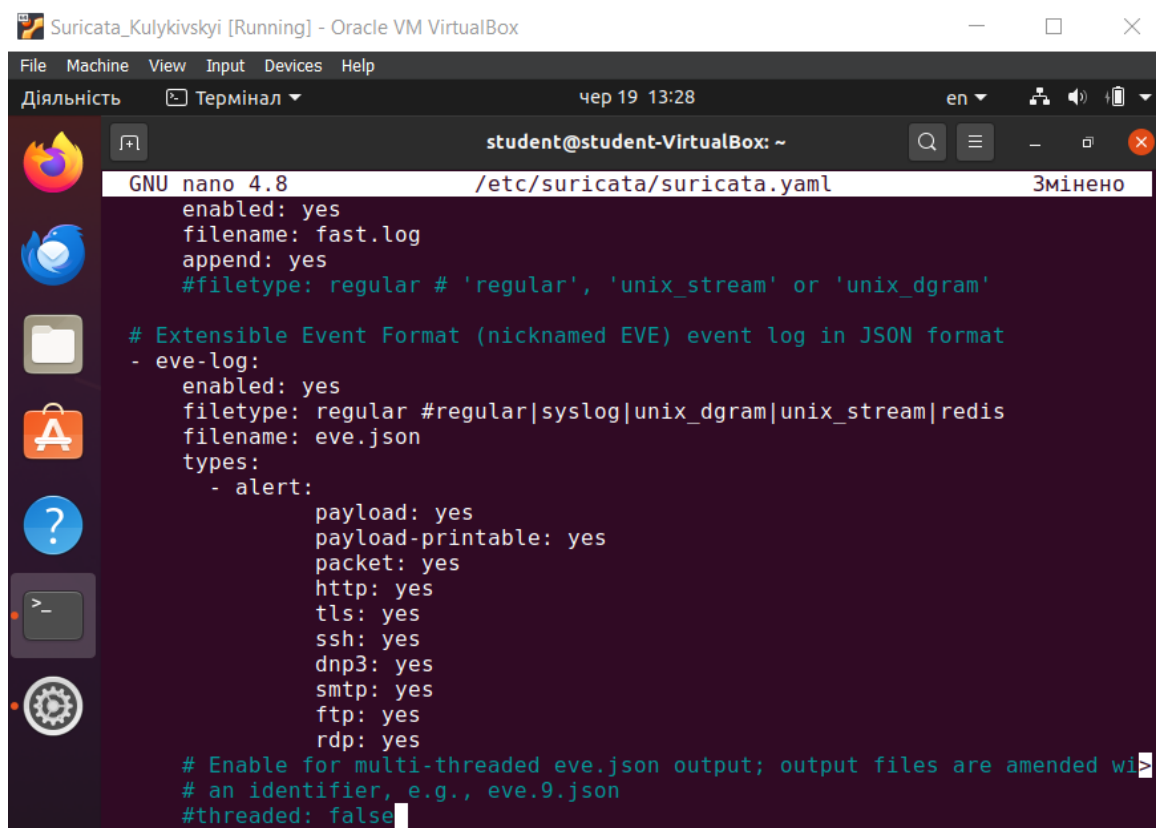


Рисунок 3.56 – Налаштування секції *outputs* для сповіщень (використовуються json журнал)

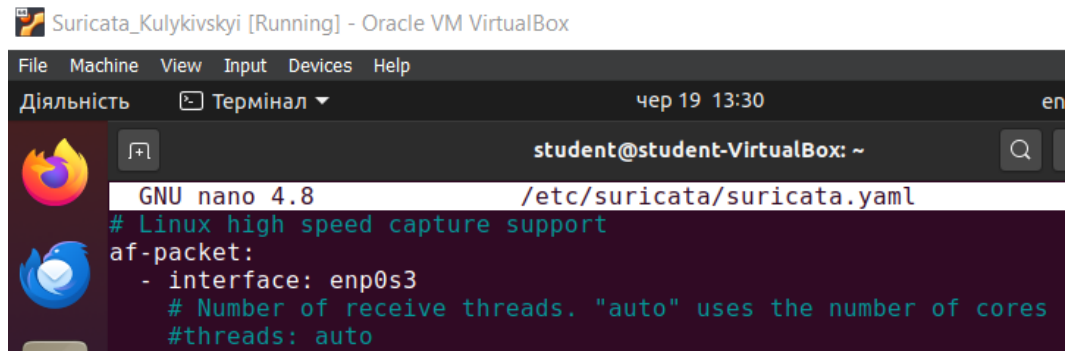


Рисунок 3.57 – Налаштування мережевого інтерфейсу

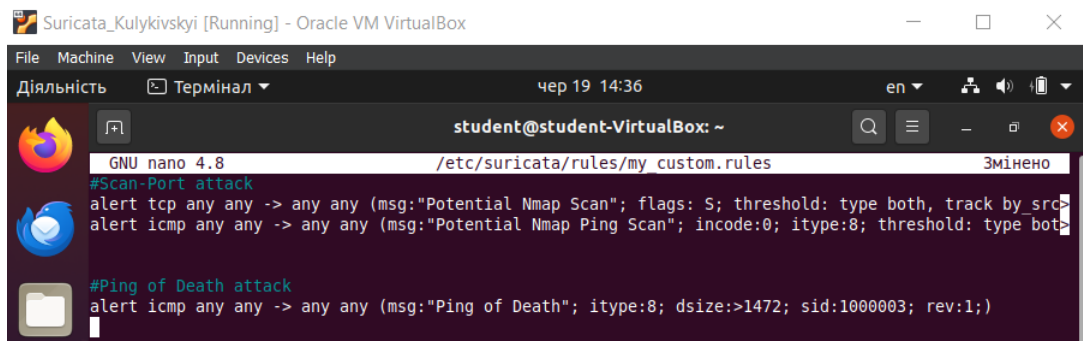


Рисунок 3.58 – Додавання власних правил для виявлення атак

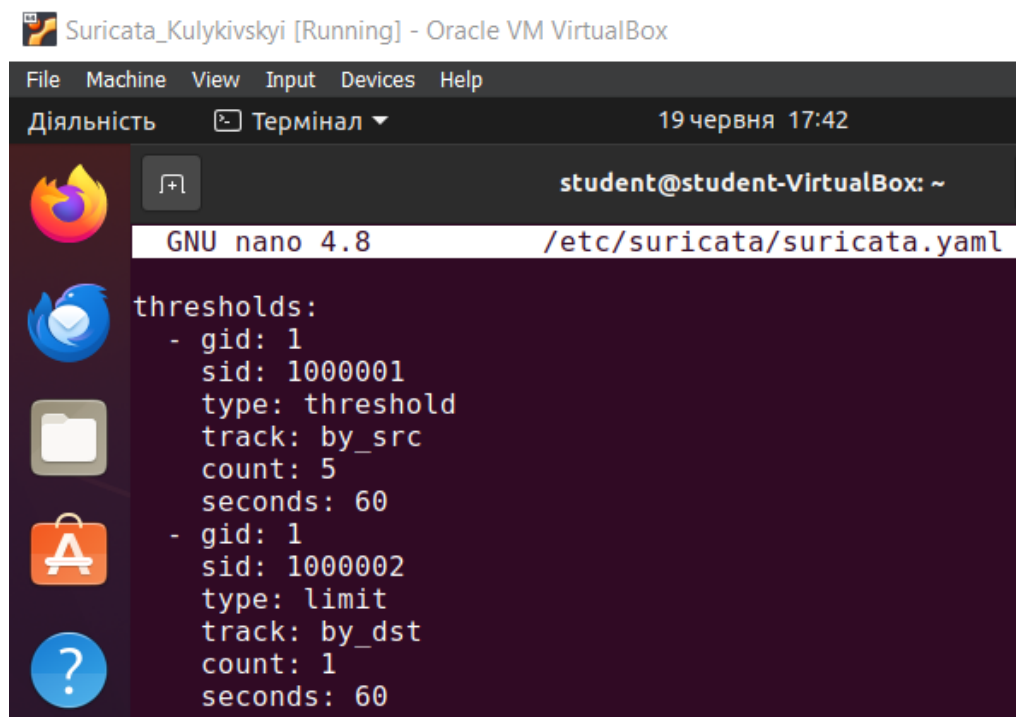


Рисунок 3.59 – Додавання параметрів для контролю порогових значень

Параметри для контролю порогових значень в Suricata вказуються в файлі конфігурації. Це дозволяє налаштовувати правила щодо порогів, щоб уникнути перевантаження системи або зменшити кількість помилкових спрацьовувань.

		Куликівський ІД			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

У цьому прикладі, *gid* це груповий ідентифікатор правила; *sid* це ідентифікатор правила; *type* це тип порогового значення; *track* вказує, що саме відслідковувати; *count* це кількість спрацювань правила за вказаний період; *seconds* це період у секундах.

```

student@student-VirtualBox:~$ sudo suricata -T -c /etc/suricata/suricata.yaml
i: suricata: This is Suricata version 7.0.5 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/my_custom.rules
student@student-VirtualBox:~$

```

Рисунок 3.60 – Перевірка конфігурації Suricata

```

student@student-VirtualBox:~$ sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3 -v
Notice: suricata: This is Suricata version 7.0.5 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: ioctl: enp0s3: MTU 1500
Info: conf: Running in live mode, activating unix socket
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 38296 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 38299 signatures processed. 1105 are IP-only rules, 4124 are inspecting packet payload, 32856 inspect application layer, 108 are decoder event only
Info: runmodes: enp0s3: creating 1 thread
Info: unix-manager: unix socket '/var/run/suricata/suricata-command.socket'
Notice: threads: Threads created -> W: 1 FM: 1 FR: 1 Engine started.

```

Рисунок 3.61 – Успішний запуск Suricata

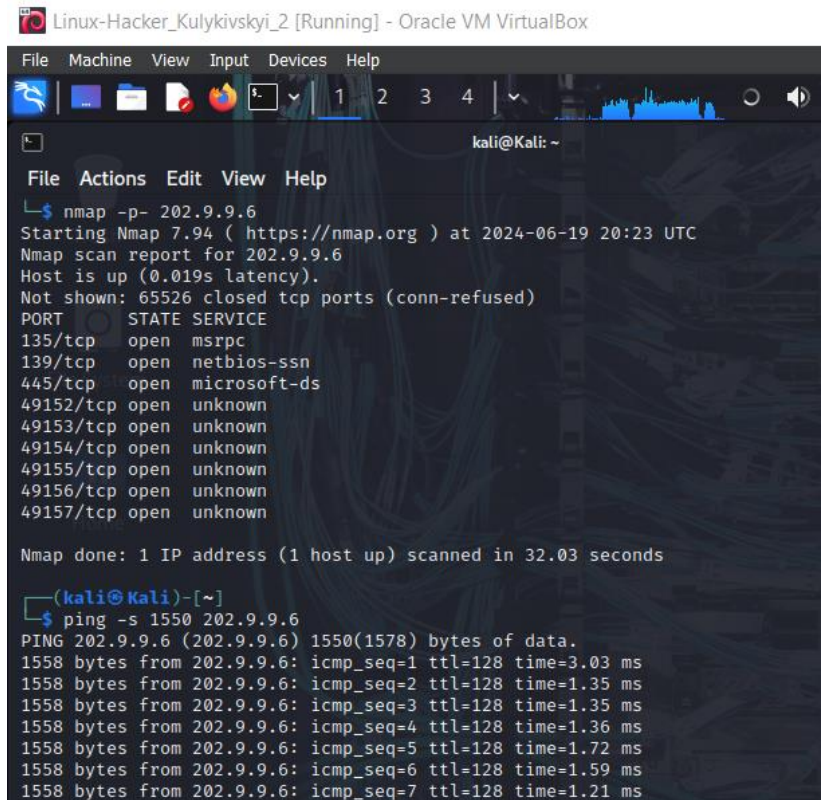


Рисунок 3.62 – Проведення атак на Serv2

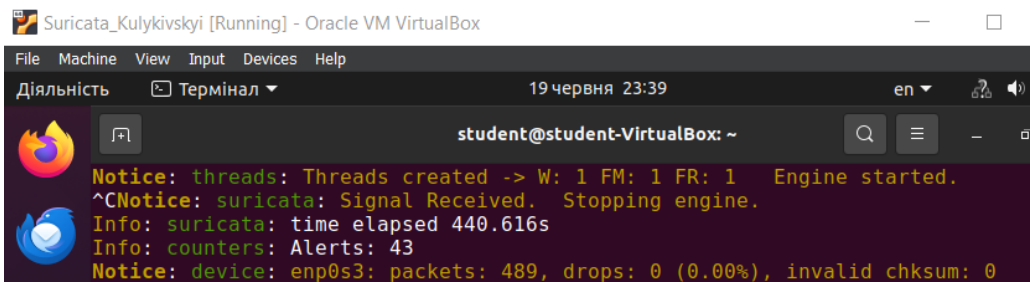


Рисунок 3.63 – Результат моніторингу

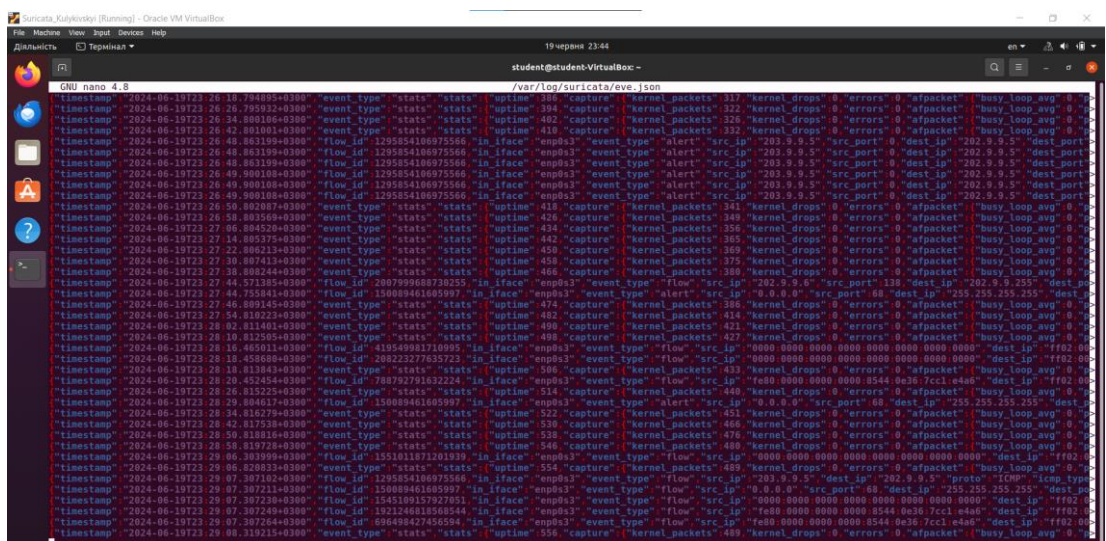


Рисунок 3.64 – Перегляд детальних результатів моніторингу атак у файлі eve.json

		Куликівський ІД			Арк.
		Трокоз Є.М.			ККІКБ.КР.Б – 125 – 09 – ПЗ
Змн.	Арк.	№ докум.	Підпис	Дата	65

Файл `eve.json` містить лог-записи з результатами моніторингу Suricata. Кожен запис у цьому файлі представляє собою JSON-об'єкт, який містить детальну інформацію про певну подію. Записи з `event_type:alert` зазвичай містять детальну інформацію про правило, яке спрацювало, наприклад, опис загрози та унікальний ідентифікатор правила (SID). Статичні дані (stats) включають інформацію про мережевий трафік, та можуть допомогти зрозуміти загальну картину мережевої активності. Вони можуть включати кількість оброблених пакетів, кількість виявлених помилок, використання різних протоколів, тощо.

На основі рисунку 3.64 можна зробити висновки, що було виявлено декілька подій типу `alert`, що означає, що Suricata виявила певну підозрілу активність або загрозу. Події типу `stats` надають загальну статистику про мережевий трафік, що може бути корисним для аналізу стану мережі та її навантаження.

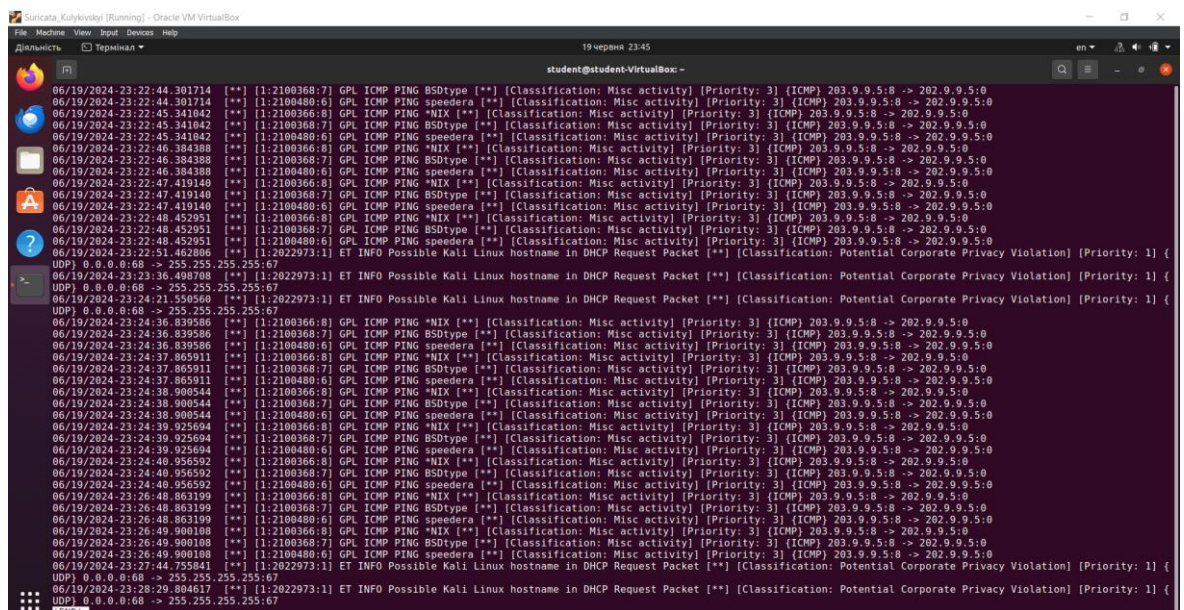


Рисунок 3.65 – Перегляд результатів моніторингу атак у файлі `fast.log` за допомогою команди `less` для зручного перегляду

Файл `fast.log` містить записи, які відображають виявлену активність, попередження та інші важливі, зафіксовані системою Suricata. Він забезпечує більш стислий і легкочитабельний формат порівняно з `eve.json`. На основі рисунку, можна побачити такі основні параметри та деталі, як час події, SID, повідомлення про атаку, класифікацію, IP-адреси та порти.

		Куликівський ІД			Арк.
		Трокоз Є.М.			66
Змн.	Арк.	№ докум.	Підпис	Дата	ККІКБ.КР.Б – 125 – 09 – ПЗ

З огляду на дані, що описані у файлі, можна зробити висновок, що Suricata виявила кілька типів ICMP пінгів, таких як Nmap, BSD та Specter, що можуть використовуватися для сканування мережі та виявлення активних хостів. Також було зафіксовано підозрілі DHCP запити з хостнеймом Kali Linux. Події, пов'язані з DHCP, мають високий пріоритет та вимагають негайної уваги, тоді як ICMP Ping атаки мають нижчий пріоритет, вказуючи на менш серйозну загрозу.

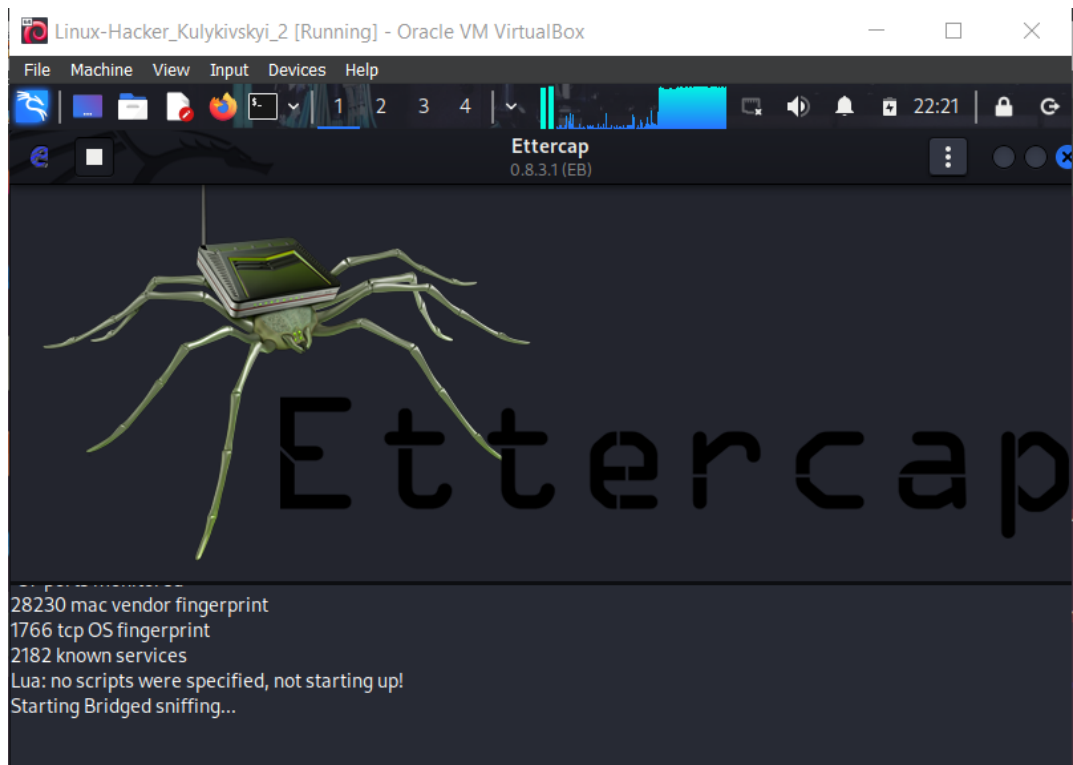


Рисунок 3.66 – Проведення атаки DNS Spoofing за допомогою Ettercap

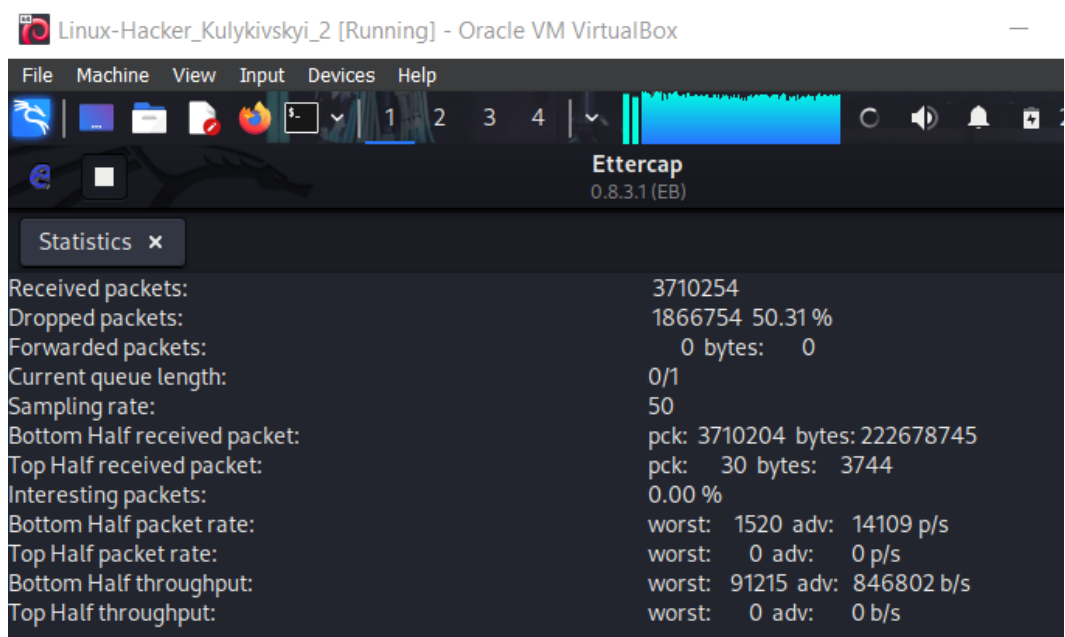


Рисунок 3.67 – Статистика атаки

		Куликівський ІД			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.68 – Результат моніторингу Suricata за допомогою команди less

Лог вказує на виявлення підозрілої активності в мережі. Видно декілька повідомлень про запити DHCP (на UDP порту 68) з можливими спробами ідентифікації хосту Kali Linux, що Suricata класифікує як потенційне порушення конфіденційності в корпоративній мережі з пріоритетом 1. Також зафіксовано блокування запитів, внесених у Spamhaus DROP списки, що мають відношення до IP-адреси 202.9.9.5 (пріоритет 2).

У логах також присутні численні попередження про активність ICMP типу PING з пріоритетом 3. Ці попередження стосуються різних систем, включаючи NIX, BSD та Speedera, які також вказують на підозрілу мережеву активність і можливі спроби сканування чи виявлення хостів.

Рисунок 3.69 – Результат моніторингу Suricata за допомогою команди more

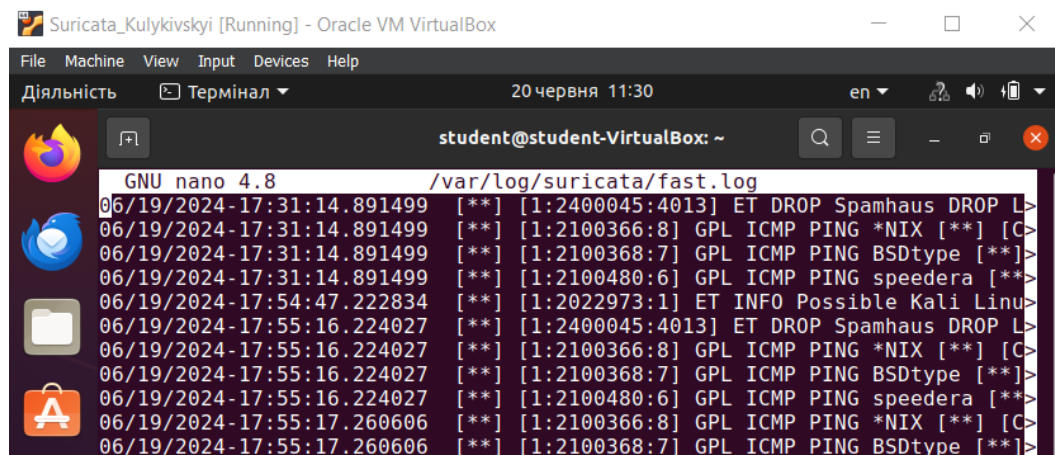


Рисунок 3.70 – Перегляд результатів моніторингу через редактор nano

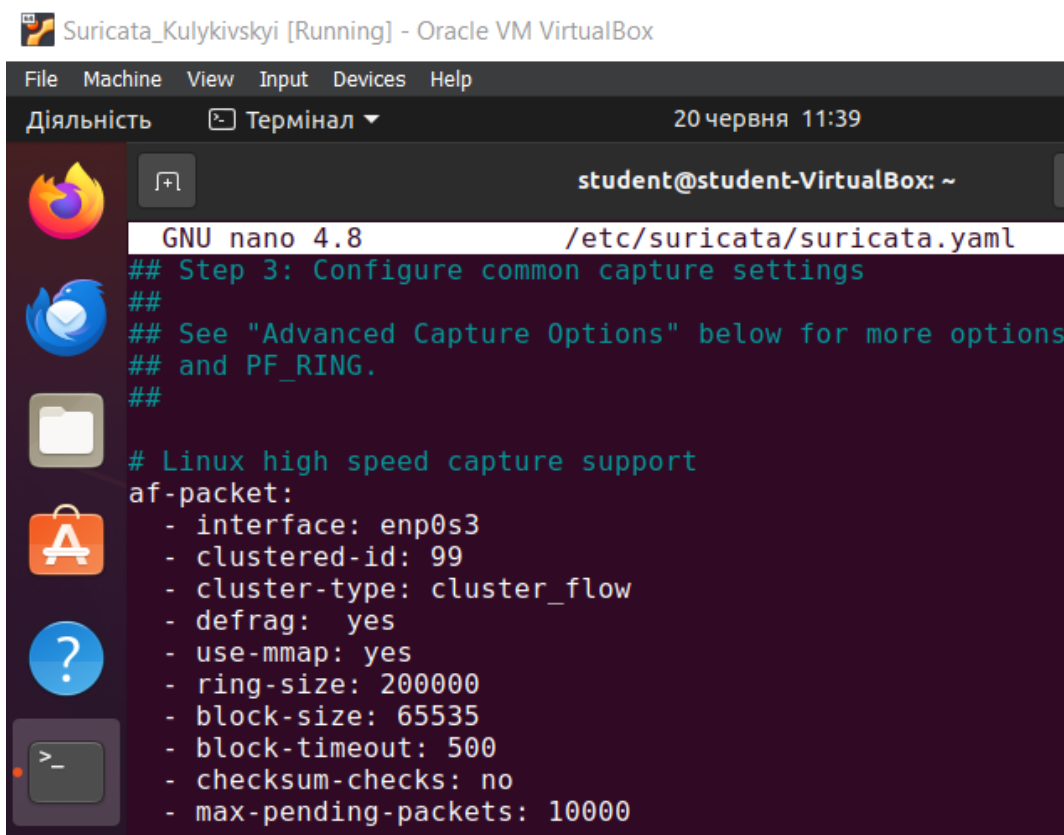


Рисунок 3.71 – Налаштування конфігурації для запуску Suricata в режимі IPS

Використання інтерфейсу `enp0s3` дозволяє Suricata приймати мережевий трафік для аналізу, а параметри на кшталт `cluster-flow` та `cluster-id` забезпечують ефективне розподілення навантаження при обробці потоків даних. Опція `defrag` дозволяє правильно обробляти фрагментовані пакети, що важливо для точного аналізу. Використання механізму `use-mmap` (memory-mapped I/O) та налаштування великого розміру кільцевого буфера (`ring-size: 200000`) покращує продуктивність

		Куликівський ІД			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

за рахунок швидкого доступу до даних. Параметри 'block-size' та 'block-timeout' оптимізують обробку пакетів, мінімізуючи затримки, тоді як відключення перевірки контрольних сум ('checksum-checks: no') знижує навантаження на систему.

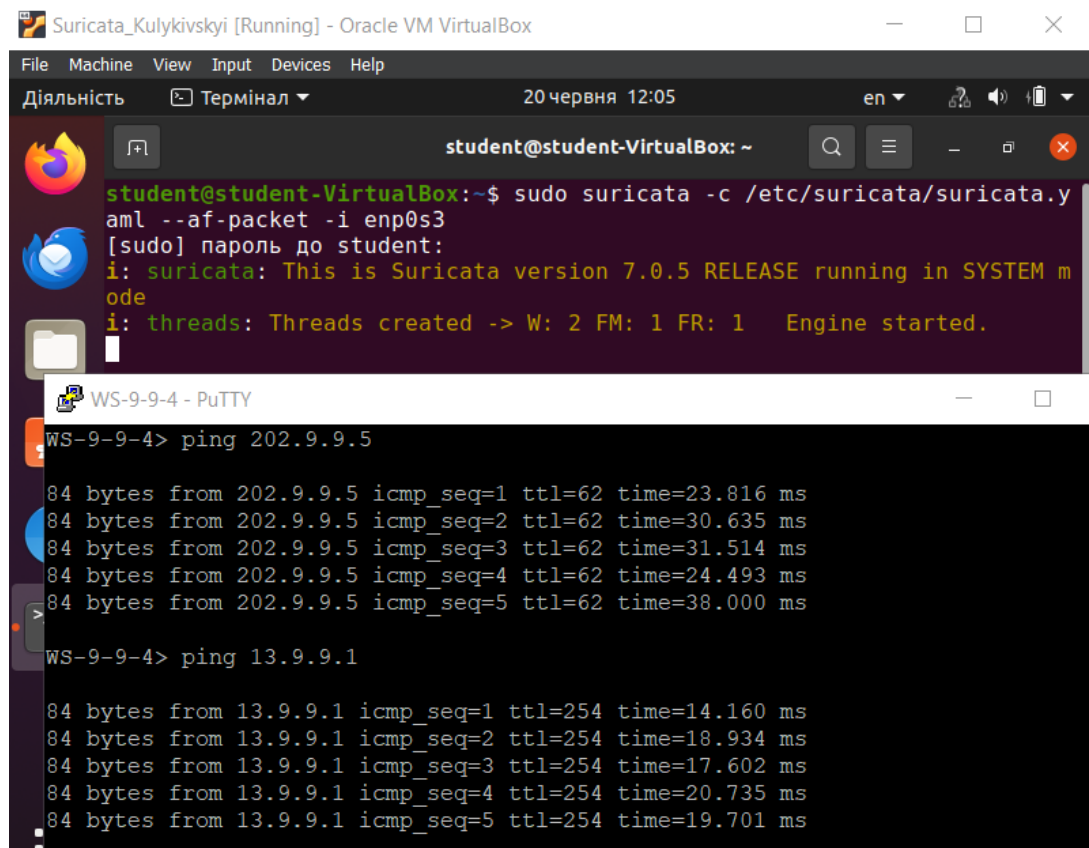


Рисунок 3.72 – Запуск Suricata в режимі IPS та перевірка зв’язку між пристроями

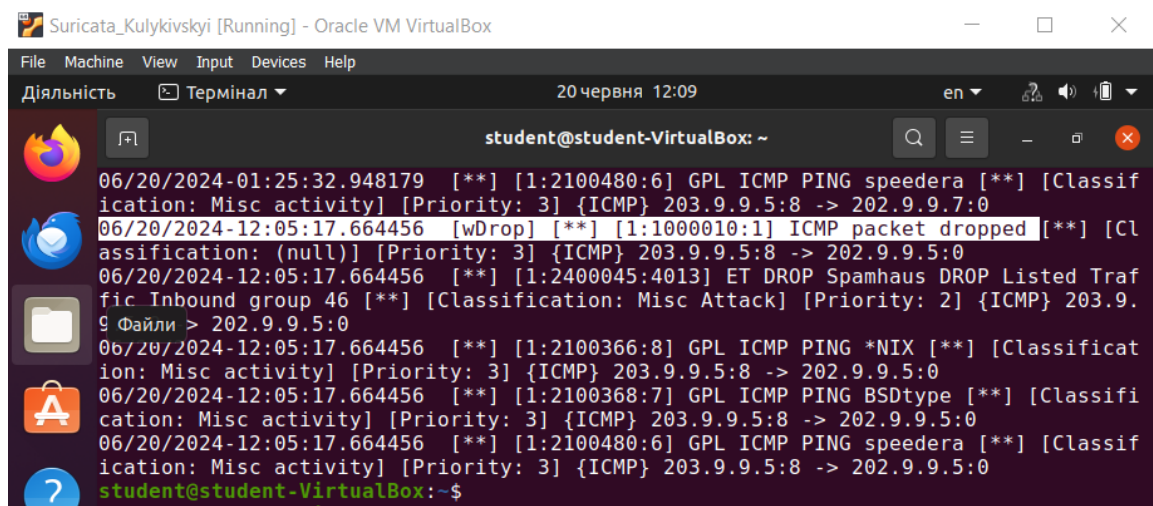


Рисунок 3.73 – Перевірка логів та повідомлення про успішне блокування пакетів

На рисунку 3.73 показані результати роботи системи виявлення та запобігання вторгнень (IPS) Suricata. Серед записів можна побачити повідомлення про

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

підозрілу активність типу ICMP PING, що класифікується як Misc Activity (різні види активності) з пріоритетом 3, включаючи PING-запити з різних джерел.

В записі 12:05:17, 664456 видно, що Suricata позначила та скасувала ICMP пакет, що свідчить про активну дію IPS для захисту мережі. Отже, система ефективно реагує на виявлені загрози, забезпечуючи підвищений рівень безпеки мережі в режимі реального часу.

Висновки до третього розділу:

Третій розділ зосереджений на налаштуванні мережі, а також на аналізі та виявленні мережевих загроз з використанням інструментів Snort і Suricata. Додаткові налаштування, включаючи синхронізацію часу за допомогою NTP і динамічний маршрутизуючий протокол OSPF, підвищили точність і надійність мережевих операцій. Синхронізація часу дозволила забезпечити узгодженість логів і подій, що є критично важливим для діагностики і безпеки, а OSPF оптимізував маршрутизацію, підвищивши ефективність передачі даних і адаптивність мережі до змін. Під час дослідження були встановлені та налаштовані обидві системи, після чого проведено серію атак з використанням Kali Linux для оцінки їх здатності виявляти і реагувати на загрози. Моніторинг та аналіз атак показали, що обидва інструменти ефективно ідентифікують різноманітні типи загроз. Проте, Suricata продемонструвала себе як більш зручний у налаштуванні та експлуатації інструмент, завдяки доступності детальної документації та більш інтуїтивному процесу конфігурації.

ВИСНОВКИ

В першому розділі представлено огляд мережевих загроз та програмного забезпечення для їх виявлення. Було детально розглянуто різні види атак, такі як DoS,

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

сканування портів та шкідливе програмне забезпечення, що показало, наскільки різноманітними та комплексними є сучасні кіберзагрози. Крім того, досліджено системи виявлення та запобігання вторгнень (IDS/IPS), зокрема Snort і Suricata, підкреслюючи їх архітектурні особливості та функціональні можливості. Виявлено, що Snort пропонує надійність і простоту, а Suricata – покращену продуктивність і гнучкість.

Другий розділ був присвячений розробці тестової мережі, що включала детальний опис її архітектури, створення схеми адресації та опису вибраних операційних систем для роботи. Ці налаштування забезпечили ефективне управління і синхронізацію мережевих ресурсів, підвищивши точність і надійність мережевих операцій.

У третьому розділі проведено налаштування мережі та практичний аналіз використання Snort і Suricata для виявлення мережевих загроз. Процес включав встановлення і налаштування обох систем, проведення атак за допомогою Kali Linux, та аналіз результатів моніторингу атак. В ході експерименту встановлено, що обидві системи ефективно ідентифікують загрози, проте Suricata виявилася зручнішою в налаштуванні і експлуатації, завдяки більш інтуїтивному інтерфейсу і доступній документації.

Проведене дослідження надає цілісне уявлення про актуальні загрози для мереж, методи їх виявлення та ефективність програмного забезпечення Snort і Suricata. Побудована тестова мережа дозволила імітувати реальні умови та оцінити практичні аспекти роботи IDS/IPS систем. На основі проведеного аналізу, Suricata рекомендовано для використання в тестовій мережі завдяки її більш зручній конфігурації та наявності докладної інформації, що сприяє ефективнішому управлінню загрозами. Це забезпечує комплексний підхід до забезпечення мережевої безпеки, об'єднуючи теоретичні аспекти з практичними інструментами і методами.

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ethical Hacking Labs. Сканування мереж. [Електронний ресурс]: Режим доступу: <https://hackyourmom.com/servisy/%E2%84%962-ethical-hacking-labs-skanuvannya-merezh/>
2. Ethical Hacking Labs. Шкідливе програмне забезпечення. [Електронний ресурс]: Режим доступу: <https://hackyourmom.com/servisy/%E2%84%964-ethical-hacking-labs-shkidlyve-programne-zabezpechennya/>
3. Типи мережевих загроз. [Електронний ресурс]: Режим доступу: <https://studfile.net/preview/8458711/page:2/>
4. Що таке IPS/IDS і де застосовується. [Електронний ресурс]: Режим доступу: <https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya>
5. Snort і Suricata – простий шлях до використання IDPS: від установки на сервер до грамотного налаштування. [Електронний ресурс]: Режим доступу: <https://habr.com/ru/companies/selectel/articles/744478/>
6. Suricata Installation. [Електронний ресурс]: Режим доступу: <https://docs.suricata.io/en/latest/install.html>
7. Suricata Features. [Електронний ресурс]: Режим доступу: <https://suricata.io/features/>
8. Snort downloads. [Електронний ресурс]: Режим доступу: <https://www.snort.org/downloads>
9. Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM). [Електронний ресурс]: Режим доступу: <https://skillsforall.com/launch?id=72540ddb-74fb-4ec8-85d5-924146e76987&tab=curriculum&view=3174f565-8ce2-5c17-aa59-88a41db574a8>
10. Install Snort on Ubuntu. [Електронний ресурс]: Режим доступу: <https://www.youtube.com/watch?v=NcNQZm-q29M>
11. DDoS-атака: визначення, механізм дій і способи захисту. [Електронний ресурс]: Режим доступу: <https://foxminded.ua/ddos-ataka/>

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

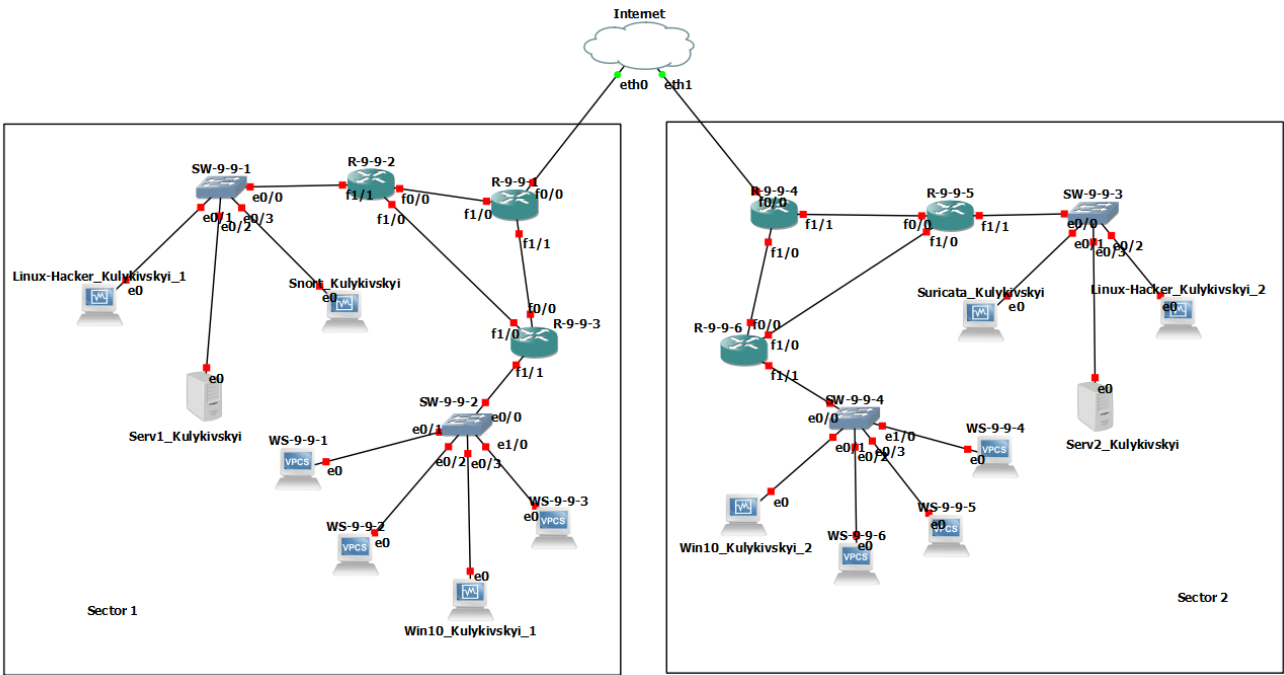
- 12.Що таке шкідливе програмне забезпечення. [Електронний ресурс]: Режим доступу: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware>
- 13.DoS проти DDoS-атак – що це таке та як від них захищатися.
[Електронний ресурс]: Режим доступу: <https://gigatrans.ua/ua/news/dos-protiv-ddos-atak-v-chem-raznica-i-kak-ot-nih-zash-ititsya>
- 14.Ubuntu vs Windows: яка ОС підійде саме вам. [Електронний ресурс]: Режим доступу: https://itedu.center.ua/blog/comparisons/ubuntu_vs_windows/
- 15.Посібник з хакінгу за допомогою Kali Linux. [Електронний ресурс]: Режим доступу: <https://hackyourmom.com/osvita/posibnyk-z-hakingu-za-dopomogoyu-kali-linux/>
- 16.Kali Linux: історія, встановлення, налаштування, огляд. [Електронний ресурс]: Режим доступу: <https://kr-labs.com.ua/blog/kali-linux-istoriya-vstanovlennya-nalashtuvannya-oglyad/>
- 17.Snort – network intrusion detection and prevention system. [Електронний ресурс]: Режим доступу: <https://www.fortinet.com/resources/cyberglossary/snort>
- 18.What is Snort and how does it work? [Електронний ресурс]: Режим доступу: <https://www.techtarget.com/searchnetworking/definition/Snort>
- 19.What is Suricata? [Електронний ресурс]: Режим доступу: <https://suricata.io/2024/04/15/what-is-suricata/>
- 20.Suricata: What is it and how can we use it. [Електронний ресурс]: Режим доступу: <https://www.infosecinstitute.com/resources/network-security-101/suricata-what-is-it-and-how-can-we-use-it/>

		Куликівський І.Д.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

ДОДАТКИ

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема побудованої мережі



Таблиця адресації пристроїв

Таблиця Б1

IP адресація мережі першого сектору

Мережа / Пристрій	Інтерфейс / Ме- режний адаптер / Шлюз	IP-адреса	Маска	Префікс
Підмережа А	-	10.9.9.0	255.255.255.0	/24
Підмережа В	-	11.9.9.0	255.255.255.0	/24
Підмережа С	-	13.9.9.0	255.255.255.0	/24
Підмережа D	-	200.9.9.0	255.255.255.0	/24
Підмережа E	-	201.9.9.0	255.255.255.0	/24
R-9-9-1	Fa1/0	10.9.9.1	255.255.255.0	/24
	Fa1/1	11.9.9.1	255.255.255.0	/24
R-9-9-2	Fa0/0	10.9.9.2	255.255.255.0	/24
	Fa1/0	13.9.9.1	255.255.255.0	/24
	Fa1/1	200.9.9.1	255.255.255.0	/24

IP адресація мережі першого сектору

Мережа / Пристрій	Інтерфейс / Ме- режний адаптер / Шлюз	IP-адреса	Маска	Префікс
R-9-9-3	Fa0/0	11.9.9.2	255.255.255.0	/24
	Fa1/0	13.9.9.2	255.255.255.0	/24
	Fa1/1	201.9.9.1	255.255.255.0	/24
Serv1_Kulykivskyi	М. адаптер	200.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
Snort PC	М. адаптер	200.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
Linux- Hacker_Kulykivskyi_1	М. адаптер	200.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	200.9.9.1	255.255.255.0	/24
WS-9-9-1	М. адаптер	201.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
WS-9-9-2	М. адаптер	201.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
WS-9-9-3	М. адаптер	201.9.9.8	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24
Win10_Kulykivskyi_1	М. адаптер	201.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	201.9.9.1	255.255.255.0	/24

Таблиця Б2

IP адресація мережі другого сектору

Мережа / Пристрій	Інтерфейс / Мере- жний адаптер / Шлюз	IP-адреса	Маска	Префікс
Підмережа F	-	13.9.9.0	255.255.255.0	/24
Підмережа G	-	14.9.9.0	255.255.255.0	/24
Підмережа H	-	15.9.9.0	255.255.255.0	/24

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

IP адресація мережі другого сектору

Мережа / Пристрій	Інтерфейс / Ме- режний адаптер / Шлюз	IP-адреса	Маска	Префікс
Підмережа I	-	203.9.9.0	255.255.255.0	/24
Підмережа J	-	203.9.9.0	255.255.255.0	/24
R-9-9-4	Fa1/1	13.9.9.1	255.255.255.0	/24
	Fa1/0	14.9.9.1	255.255.255.0	/24
R-9-9-5	Fa0/0	13.9.9.2	255.255.255.0	/24
	Fa1/0	15.9.9.1	255.255.255.0	/24
	Fa1/1	203.9.9.1	255.255.255.0	/24
R-9-9-6	Fa0/0	14.9.9.2	255.255.255.0	/24
	Fa1/0	15.9.9.2	255.255.255.0	/24
	Fa1/1	203.9.9.1	255.255.255.0	/24
Serv2_Kulykivskiyi	М. адаптер	203.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
Suricata PC	М. адаптер	203.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
Linux- Hacker_Kulykivskiyi_2	М. адаптер	203.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
WS-9-9-4	М. адаптер	203.9.9.5	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
WS-9-9-5	М. адаптер	203.9.9.6	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
WS-9-9-6	М. адаптер	203.9.9.7	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24
Win10_Kulykivskiyi_2	М. адаптер	203.9.9.8	255.255.255.0	/24
	Шлюз за замовч.	203.9.9.1	255.255.255.0	/24

Лістинг конфігурації пристроїв Маршрутизатори:

```
R-9-9-1#show run
hostname R-9-9-1
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 description Link_to_Internet
 no ip address
 duplex half
interface FastEthernet1/0
 description Link_to_R-9-9-2
 ip address 10.9.9.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet1/1
 description Link_to_R-9-9-3
 ip address 11.9.9.1 255.255.255.0
 duplex auto
 speed auto
router ospf 909
 log-adjacency-changes
 network 10.9.9.0 0.0.0.255 area 0
 network 11.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 ntp server 193.168.1.10
end
```

```
R-9-9-2#show run
Building configuration...
```

```
Current configuration : 1372 bytes
upgrade fpd auto
version 13.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-9-2
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 description Link_to_R-9-9-1
 ip address 10.9.9.2 255.255.255.0
 duplex half
interface FastEthernet1/0
 description Link_to_R-9-9-3
 ip address 13.9.9.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet1/1
 description Link_to_SW-9-9-1
 ip address 200.9.9.1 255.255.255.0
 ip ospf 909 area 0
 duplex auto
 speed auto
router ospf 909
 log-adjacency-changes
 network 10.9.9.0 0.0.0.255 area 0
 network 13.9.9.0 0.0.0.255 area 0
 network 200.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

line vty 0 4
 login
 ntp server 193.168.1.10
 end

```

```

R-9-9-3#show run
Building configuration...
Current configuration : 1372 bytes
upgrade fpd auto
version 13.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-9-3
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 description Link_to_R-9-9-1
 ip address 11.9.9.2 255.255.255.0
 duplex half
interface FastEthernet1/0
 description Link_to_R-9-9-2
 ip address 13.9.9.2 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet1/1
 description Link_to_SW-9-9-2
 ip address 201.9.9.1 255.255.255.0
 ip ospf 909 area 0
 duplex auto
 speed auto
router ospf 909
 log-adjacency-changes
 network 11.9.9.0 0.0.0.255 area 0
 network 13.9.9.0 0.0.0.255 area 0
 network 201.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0

```

```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
 login
 ntp server 193.168.1.10
 end

```

```

R-9-9-4#show run
Building configuration...
Current configuration : 1295 bytes
upgrade fpd auto
version 13.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-9-4
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
 description Link_to_Internet
 no ip address
 duplex half
interface FastEthernet1/0
 description Link_to_R-9-9-6
 ip address 14.9.9.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet1/1
 description Link_to_R-9-9-5
 ip address 13.9.9.1 255.255.255.0
 duplex auto
 speed auto
router ospf 909
 log-adjacency-changes
 network 13.9.9.0 0.0.0.255 area 0
 network 14.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0

```

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
ntp server 193.168.1.10
end

```

```

R-9-9-5#show run
Building configuration...
Current configuration : 1372 bytes
upgrade fpd auto
version 13.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-9-5
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link_to_R-9-9-4
ip address 13.9.9.2 255.255.255.0
duplex half
interface FastEthernet1/0
description Link_to_R-9-9-6
ip address 15.9.9.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/1
description Link_to_SW-9-9-3
ip address 203.9.9.1 255.255.255.0
ip ospf 909 area 0
duplex auto
speed auto
router ospf 909
log-adjacency-changes
network 13.9.9.0 0.0.0.255 area 0
network 15.9.9.0 0.0.0.255 area 0
network 203.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1

```

```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
ntp server 193.168.1.10
end

```

```

R-9-9-6#show run
Building configuration...
Current configuration : 1372 bytes
upgrade fpd auto
version 13.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-9-6
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link_to_R-9-9-4
ip address 14.9.9.2 255.255.255.0
duplex half
interface FastEthernet1/0
description Link_to_R-9-9-5
ip address 15.9.9.2 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/1
description Link_to_SW-9-9-4
ip address 203.9.9.1 255.255.255.0
ip ospf 909 area 0
duplex auto
speed auto
router ospf 909
log-adjacency-changes
network 14.9.9.0 0.0.0.255 area 0
network 15.9.9.0 0.0.0.255 area 0
network 203.9.9.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15

```

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

stopbits 1
line vty 0 4
login
ntp server 193.168.1.10
end

Комутатори:

SW-9-9-1#show run
Building configuration...
Current configuration : 1392 bytes
Last configuration change at 13:37:28 UTC Fri Jun 21 2024
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW-9-9-1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet2/0
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet3/0
interface Ethernet3/1
interface Ethernet3/2
interface Ethernet3/3
interface Vlan1
no ip address
shutdown
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
ntp server 193.168.1.10
end

SW-9-9-2#show run
Building configuration...
Current configuration : 1392 bytes
Last configuration change at 13:37:30 UTC Fri Jun 21 2024
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW-9-9-2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet2/0
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet3/0
interface Ethernet3/1
interface Ethernet3/2
interface Ethernet3/3
interface Vlan1
no ip address

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
ntp server 193.168.1.10
end

```

```

SW-9-9-3#show run
Building configuration...
Current configuration : 1368 bytes
Last configuration change at 13:43:52 UTC Fri Jun 21
2024
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW-9-9-3
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet2/0
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet3/0
interface Ethernet3/1
interface Ethernet3/2
interface Ethernet3/3
interface Vlan1
no ip address
shutdown

```

```

ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end

```

```

SW-9-9-4#show run
Building configuration...
Current configuration : 1368 bytes
Last configuration change at 13:43:54 UTC Fri Jun 21
2024
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW-9-9-4
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
no ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet2/0
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet3/0
interface Ethernet3/1
interface Ethernet3/2
interface Ethernet3/3
interface Vlan1
no ip address
shutdown
ip forward-protocol nd
no ip http server

```

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end

```

		Куликівський І.Д.			ККІКБ.КР.Б - 125 - 09 - ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		84