Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Створення тренувального середовища для навчання роботи з IDS/IPS"

Виконав: студент (ка) IV курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Костишин Володимир Вікторович
підпис (прізвище та ініціали)

Керівник Козак Р. О.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т. В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Мацюк.Г.Р
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Костишину Володимиру Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення тренувального середовища для навчання роботи з IDS/IPS

Керівник роботи Козак Руслан Орестович, к.т.н., доцент кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Вимоги до IPS/IDS. Документація pfSsense, OPNsens, Snort, Suricata. Документація Parrot Security, Kali Linux. Документація Ubuntu Linux, Windows Server 2022.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Розробка тренувального середовища
3. Тестування та оцінка ефективності тренувального середовища
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Актуальність дослідження. 3. Мета, Об'єкт, Предмет дослідження. 4. Задачі. 5. Типи IDS та IPS. 6. Структура тренувального середовища. 7. Елементи тренувального середовища (Гіпервізор VMware ESXi). 8. Елементи тренувального середовища (Маршрутизатори OPNsense та pfSense). 9. Елементи тренувального середовища (Операційні системи для тестування безпеки). 10. Елементи тренувального середовища (Віртуальні сервери). 11. Сценарій 1: Тестування pfSense та Snort в режимі IPS 12. Відпрацювання сценарію 1. 13. Сценарій 2: Тестування OPNsense та Suricata в режимі IDS. 14. Відпрацювання сценарію 2. 15. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Розробка тренувального середовища»	11.03 – 25.03	
5.	Оформлення розділу «Тестування та оцінка ефективності тренувального середовища»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2025	

Студент _____ Костишин В. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р. О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Створення тренувального середовища для навчання роботи з IDS/IPS // Кваліфікаційна робота ОР «Бакалавр» // Костишин Володимир Вікторович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 83, рис. – 28, табл. 2 - , кресл. – 14, додат. – 1.

Ключові слова: pfSense, OPNsense, VMware ESXi, Kali Linux, Parrot Security, Snort, Suricata, IDS, IPS.

У кваліфікаційній роботі бакалавра розглянуто питання розробки та тестування тренувального середовища для навчання роботі з системами виявлення та запобігання вторгненням (IDS/IPS). Запропоноване середовище побудовано на базі гіпервізора VMware ESXi з використанням віртуалізованих маршрутизаторів (pfSense, OPNsense), операційних систем для тестування безпеки (Kali Linux, Parrot Security) та серверних ОС (Windows Server 2022, Ubuntu Linux тощо).

У роботі проаналізовано класифікацію та принципи роботи IDS/IPS, охарактеризовано переваги тренувальних платформ для підготовки фахівців з кібербезпеки, а також розглянуто існуючі комерційні та відкриті рішення в цій галузі. За допомогою практичних експериментів продемонстровано можливості Snort та Suricata як інструментів виявлення й запобігання різним видам атак (DDoS, brute force, сканування портів тощо). Одержані результати підтверджують ефективність запропонованої тренувальної платформи для моделювання реалістичних сценаріїв кібератак, аналізу роботи IDS/IPS та підвищення рівня підготовки майбутніх фахівців з інформаційної безпеки.

ANNOTATION

Training Environment for Learning to Work with IDS/IPS // Thesis of educational level "Bachelor"// Volodymyr Kostyshyn // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 83, figs. 28, tables 2, drawings 14, added. 1.

Keywords: pfSense, OPNsense, VMware ESXi, Kali Linux, Parrot Security, Snort, Suricata, IDS, IPS..

The bachelor's thesis deals with the development and testing of a training environment for learning to work with intrusion detection and prevention systems (IDS/IPS). The proposed environment is built on the VMware ESXi hypervisor using virtualised routers (pfSense, OPNsense), security testing operating systems (Kali Linux, Parrot Security) and server OSes (Windows Server 2022, Ubuntu Linux, etc.).

The work analyses the classification and principles of IDS/IPS operation, describes the advantages of training platforms for cybersecurity professionals, and reviews existing commercial and open source solutions in this area. Practical experiments demonstrate the capabilities of Snort and Suricata as tools for detecting and preventing various types of attacks (DDoS, brute force, port scanning, etc.). The obtained results confirm the effectiveness of the proposed training platform for modelling realistic cyberattack scenarios, analysing IDS/IPS performance and improving the level of training of future information security professionals.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IPS	—	Intrusion Prevention System
IDS	—	Intrusion Detection System
NIDS/NIPS	—	Network-based IDS/IPS
HIDS/HIPS	—	Host-based IDS/IPS
DDoS	—	Distributed Denial of Service
MITM	—	Man-in-the-Middle
VMFS	—	Virtual Machine File System
VLAN	—	Virtual Local Area Network
VPN	—	Virtual Private Network
NAT	—	Network Address Translation
RDP	—	Remote Desktop Protocol
RDS	—	Remote Desktop Services
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ВМ	—	Віртуальна машина
WAN	—	Wide Area Network
LAN	—	Local Area Network
SSH	—	Secure Shell
DHCP	—	Dynamic Host Configuration Protocol
DNS	—	Domain Name System
HTTP	—	Hypertext Transfer Protocol

ВСТУП

Актуальність теми. З кожним роком кіберзагрози еволюціонують а методи атак стають дедалі витонченішими. Виявлення та запобігання вторгненням є ключовими аспектами забезпечення інформаційної безпеки будь-якої організації. Системи виявлення та запобігання вторгненням (IDS/IPS) дозволяють своєчасно реагувати на шкідливі дії в мережі та мінімізувати можливі ризики. Однак ефективне використання IDS/IPS вимагає від спеціалістів високого рівня підготовки, що можливо лише за умови практичного навчання. Використання спеціалізованих тренувальних середовищ дозволяє не тільки ознайомитися з основами роботи IDS/IPS, а й практично випробувати їх у різних сценаріях атак. Таким чином, розробка навчального середовища для відпрацювання роботи з IDS/IPS є актуальним завданням у сфері підготовки фахівців з кібербезпеки.

Мета і задачі дослідження. Метою даної роботи є розробка та тестування тренувального середовища для навчання роботи з IDS/IPS, що дозволяє імітувати реальні кібератаки та аналізувати ефективність систем виявлення та запобігання вторгненням.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз предметної області, розглянути переваги використання симуляційних середовищ у навчанні кібербезпеці;
- дослідити існуючі підходи до реалізації тренувальних середовищ для IDS/IPS;
- спроектувати та розгорнути віртуальне середовище на базі гіпервізора VMware ESXi із використанням IDS/IPS (Snort, Suricata) та операційних систем (Parrot Security, Kali Linux, Ubuntu Linux, Windows Server 2022);
- провести тестування середовища в режимах IDS та IPS, використовуючи різні сценарії атак;
- оцінити ефективність запропонованого середовища.

Об’єкт дослідження. Об’єктом дослідження є методи та засоби виявлення і запобігання вторгненням у комп’ютерні мережі.

Предмет дослідження. Предметом дослідження є процес розгортання, налаштування та тестування тренувального середовища для роботи з IDS/IPS на базі гіпервізора VMware ESXi.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані для підготовки фахівців з кібербезпеки, оскільки запропоноване середовище дозволяє моделювати реальні атаки та аналізувати ефективність механізмів захисту. Тренувальна платформа може бути застосована як у навчальних закладах, так і в організаціях для внутрішньої підготовки персоналу, що займається безпекою мережевої інфраструктури. Отримані результати також можуть бути основою для подальших досліджень у сфері покращення механізмів виявлення та запобігання вторгненням.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальні відомості про системи виявлення та запобігання вторгненням

Система виявлення вторгнень – це програмний комплекс, який аналізує мережевий трафік або журнали подій у системі для виявлення потенційних атак чи порушень безпеки. IDS самостійно не блокує загрози, а лише повідомляє адміністратора про підозрілу активність [1]. Система запобігання вторгнень – це розширений варіант IDS, який не лише виявляє потенційні загрози, але й може автоматично вживати заходів для їх нейтралізації (наприклад, блокувати трафік, змінювати конфігурацію брандмауера, завершувати з'єднання тощо) [2].

Класифікація систем IDS/IPS за методом збору даних передбачає їх поділ на дві основні категорії: мережеві (NIDS/NIPS) і хостові (HIDS/HIPS) (див. рисунок 1.1).

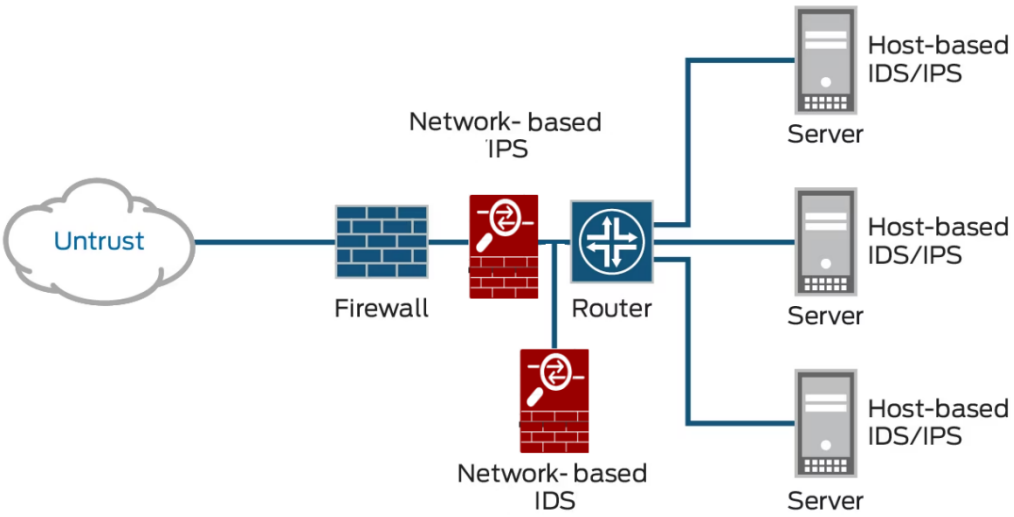


Рисунок 1.1 – Мережеві і хостові IDS/IPS

Мережеві IDS/IPS (NIDS/NIPS) здійснюють моніторинг мережевого трафіку на рівні сегмента мережі та аналізують вхідні й вихідні пакети для виявлення потенційних загроз [3]. Вони розташовуються на точках перехоплення трафіку, таких як мережеві комутатори з увімкненим дзеркалюванням портів (port mirroring) або на шлюзах між внутрішньою

мережею і зовнішнім інтернетом. Такі системи здатні виявляти широкий спектр атак, включаючи сканування портів, DDoS-атаки [4] [5] [6], експлойти, шкідливе програмне забезпечення, спроби несанкціонованого доступу та інші загрози, що передаються через мережу. Мережеві IDS є пасивними – вони лише виявляють і повідомляють про загрозу, тоді як NIPS можуть активно реагувати, блокуючи підозрілий трафік або змінюючи маршрутизацію. Основною перевагою NIDS/NIPS є їхня здатність контролювати великий обсяг трафіку без необхідності встановлення на кожному окремому хості, проте їхньою слабкою стороною є неможливість детального аналізу подій усередині конкретної системи, таких як локальні процеси або файли.

Хостові IDS/IPS (HIDS/HIPS) працюють безпосередньо на окремих вузлах, таких як сервери або робочі станції, здійснюючи моніторинг подій у межах конкретної операційної системи [7]. Вони аналізують системні журнали, перевіряють цілісність файлів, відстежують активність процесів, зміни в реєстрі, запущені служби та інші внутрішні параметри. HIDS/HIPS здатні виявляти загрози, які не фіксуються мережевими системами, наприклад, використання локальних експлойтів, спроби ескалації привілеїв, підозрілі зміни файлів або несанкціоновані дії користувачів. Хостові системи є більш детальними в аналізі поведінки конкретного пристрою, проте мають певні недоліки – для їхньої ефективної роботи необхідно розгортати окремі агенти на кожному хості, що може ускладнювати масштабування системи. HIPS, на відміну від HIDS, не лише фіксують підозрілу активність, а й можуть блокувати потенційні загрози, запобігаючи виконанню шкідливих дій.

Мережеві IDS/IPS більш ефективні для моніторингу загального потоку трафіку та захисту великих корпоративних мереж, тоді як хостові IDS/IPS забезпечують детальний контроль окремих систем. В ідеальному випадку обидва типи використовуються разом для створення багаторівневої системи безпеки, що дозволяє ефективно виявляти та блокувати широкий спектр атак як на рівні мережі, так і на рівні окремих пристроїв.

За методом аналізу загроз IDS/IPS поділяється на два основні підходи: сигнатурний та поведінковий (на основі аномалій) [8] [9] (див. рисунок 1.2).

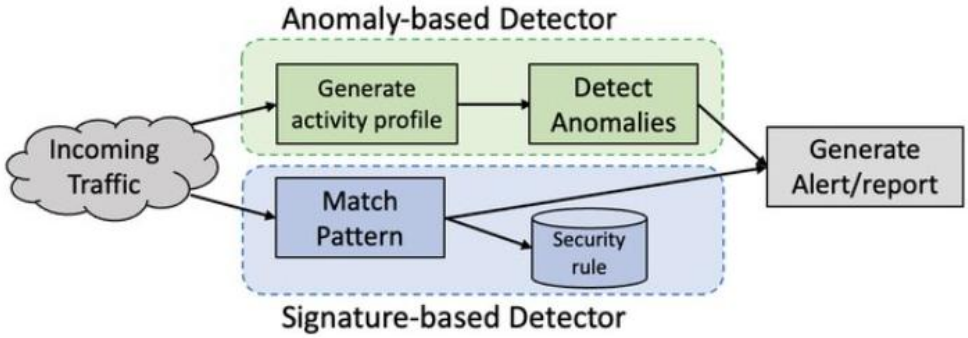


Рисунок 1.2 – Сигнатурний та поведінковий методи аналізу загроз в IDS/IPS

Сигнатурний аналіз базується на використанні бази даних відомих сигнатур атак, яка містить шаблони та правила, що ідентифікують конкретні загрози. При виявленні відповідності між вхідним трафіком або діями в системі та існуючими сигнатурами, система генерує сповіщення або застосовує заходи щодо запобігання атаці. Цей метод є дуже ефективним для виявлення вже відомих атак, таких як SQL-ін'єкції, експлойти, відомі види шкідливого програмного забезпечення. Однак він має значний недолік – нездатність розпізнавати нові, невідомі загрози, які ще не були внесені до бази сигнатур. Системи, що працюють на основі цього підходу, вимагають регулярного оновлення бази даних для забезпечення актуальності захисту.

Поведінковий аналіз працює за принципом визначення відхилень від нормальної поведінки в мережі або на хості. Ця методика передбачає створення базової моделі "нормальної" активності, яка формується на основі попереднього моніторингу та навчання системи. Якщо активність користувача, процесу чи мережевого трафіку відхиляється від стандартної поведінки, система розцінює це як потенційну загрозу. Основна перевага цього підходу полягає в здатності виявляти невідомі раніше атаки, включаючи атаки нульового дня та складні загрози. Проте його недоліком є можливість високого рівня хибних спрацьовувань, оскільки не всі відхилення обов’язково є зловмисними. Для покращення точності поведінковий аналіз часто доповнюється методами машинного навчання, які допомагають визначати складні закономірності та адаптувати систему до змін у мережевій активності.

Гібридний підхід поєднує сигнатурний та поведінковий аналіз для досягнення балансу між точністю виявлення відомих загроз і здатністю реагувати на нові атаки. Такі системи спочатку перевіряють трафік або події на відповідність відомим сигнатурам, а потім аналізують їх за поведінковими характеристиками. Це дозволяє зменшити ризик хибних спрацьовувань і підвищити ефективність виявлення загроз.

Вибір методу аналізу загроз залежить від вимог до безпеки та ресурсів організації. Сигнатурний аналіз забезпечує швидке виявлення відомих атак, поведінковий підхід дозволяє розпізнавати нові загрози, а гібридний варіант пропонує найбільш збалансоване рішення для комплексного захисту інформаційних систем.

1.2 Переваги використання тренувальних середовищ

Використання тренувальних середовищ для навчання роботи з IDS/IPS має значні переваги, оскільки дозволяє ефективно відпрацьовувати навички аналізу трафіку, виявлення загроз та реагування на інциденти у безпечному та контрольованому середовищі [10]. Однією з головних переваг є можливість створення реалістичних умов для відпрацювання атак і виявлення загроз, що дозволяє користувачам глибше зрозуміти принципи роботи систем IDS/IPS. У такому середовищі можна моделювати різні типи атак, включаючи DDoS, експлойти, SQL-ін'єкції, атаки типу MITM, сканування портів та спроби підбору паролів, що дає змогу протестувати ефективність механізмів захисту у різних сценаріях [11].

Ще однією важливою перевагою є безпека експериментів. Оскільки тренувальне середовище працює ізольовано від реальних мереж, це мінімізує ризик небажаних наслідків при виконанні експериментів із реальними загрозами. Студенти та спеціалісти можуть без побоювань запускати атаки, тестувати нові конфігурації IDS/IPS та змінювати параметри без ризику порушення роботи продуктивних систем. Також це дозволяє тренуватися у

реагуванні на інциденти в реальному часі, навчаючись оперативно аналізувати журнали подій, фільтрувати трафік та налаштовувати захисні політики.

Масштабованість є ще одним важливим аспектом тренувальних середовищ. Використання віртуалізації дозволяє створювати різні конфігурації мереж із кількома вузлами, маршрутизаторами, міжмережевими екранами та різними типами IDS/IPS. Це дає можливість досліджувати поведінку захисних механізмів у різних топологіях мереж та вивчати відмінності між різними реалізаціями IDS/IPS, такими як Snort, Suricata а також рішення на базі pfSense та OPNsense. Тренувальні середовища можна легко розширювати або адаптувати під конкретні навчальні потреби, додаючи нові вузли або змінюючи конфігурацію.

Практичний досвід, отриманий у таких середовищах, значно підвищує рівень підготовки фахівців з кібербезпеки. На відміну від теоретичних знань, які можуть залишитися поверхневими, робота з реальними атаками та аналіз захисних механізмів дає змогу глибше зрозуміти внутрішню логіку IDS/IPS та навчитися правильно їх налаштовувати. Це особливо важливо для спеціалістів, які готуються до роботи в сфері кібербезпеки, оскільки вміння швидко розпізнавати атаки, аналізувати трафік і приймати рішення є критично важливими навичками для SOC-аналітиків, інженерів з безпеки та адміністратора мереж.

Ще одним важливим моментом є економічна ефективність тренувальних середовищ. Використання віртуалізації дозволяє організаціям або навчальним закладам економити на обладнанні, оскільки немає необхідності розгортати фізичну інфраструктуру з реальними серверами та мережевими пристроями. Більше того, сучасні open-source рішення, такі як Snort та Suricata дозволяють створювати потужні тренувальні майданчики без значних фінансових витрат, що робить їх доступними для широкого кола користувачів.

Завдяки можливості тестування нових технологій тренувальні середовища стають корисними не лише для навчання, а й для професійних досліджень у сфері інформаційної безпеки. Фахівці можуть експериментувати з різними конфігураціями, тестувати нові методи виявлення загроз та покращувати

налаштування IDS/IPS, адаптуючи їх під специфічні потреби компаній чи дослідницьких лабораторій. Це також корисно для розробників та інтеграторів безпекових рішень, які можуть проводити випробування нових правил виявлення загроз та методів аналізу трафіку.

Використання тренувальних середовищ для навчання роботи з IDS/IPS є одним із найефективніших способів підготовки кваліфікованих спеціалістів у сфері кібербезпеки. Вони дозволяють не лише отримати практичний досвід роботи з системами виявлення та запобігання вторгненням, але й експериментувати з новими технологіями, вивчати методи атак та аналізувати ефективність захисних механізмів у реальних умовах. Завдяки безпечному тестуванню, масштабованості та економічній ефективності такі середовища стають невід’ємною частиною підготовки спеціалістів з інформаційної безпеки та професійного вдосконалення існуючих систем кіберзахисту.

1.3 Огляд існуючих рішень тренувальних середовищ

Існує декілька тренувальних середовищ, призначених для навчання роботи з системами виявлення та запобігання вторгненням (IDS/IPS).

Check Point Cyber Range - це сучасна платформа, розроблена для надання інтерактивного та практичного навчання в галузі кібербезпеки, зокрема для роботи з системами IDS/IPS. Ця платформа створює реалістичне середовище, де фахівці можуть відпрацьовувати навички виявлення, аналізу та реагування на різноманітні кіберзагрози. У рамках тренувань на Check Point Cyber Range користувачі стикаються з різними сценаріями атак, що дозволяє їм глибше зрозуміти принципи роботи IDS/IPS та ефективно налаштовувати ці системи для захисту мережевої інфраструктури. Платформа надає можливість працювати з реальними інструментами та технологіями, що використовуються в сучасних системах безпеки, забезпечуючи практичний досвід у безпечному та контрольованому середовищі. Крім того, Check Point Cyber Range пропонує детальний аналіз дій користувача під час тренувань, надаючи зворотний зв'язок

та рекомендації щодо покращення навичок. Це сприяє підвищенню кваліфікації фахівців та підготовці їх до реальних викликів у сфері кібербезпеки.

Cyberbit Range - це передова платформа для навчання кібербезпеці, яка надає можливість практичного відпрацювання навичок роботи з системами виявлення та запобігання вторгненням у реалістичних умовах. Платформа створює гіперреалістичні симуляції кібератак, що дозволяє фахівцям зануритися в сценарії, максимально наближені до реальних інцидентів [12]. У рамках Cyberbit Range користувачі мають змогу працювати з комерційними інструментами, які вони використовують у повсякденній діяльності. Це забезпечує безцінний досвід налаштування та оптимізації IDS/IPS у середовищі, що відображає реальні мережеві архітектури та загрози. Платформа пропонує найширший каталог сценаріїв атак, доступних на вимогу, що дозволяє командам безпеки відпрацьовувати навички виявлення та реагування на різноманітні техніки та тактики зловмисників. Це включає симуляції атак на хмарні та гібридні середовища, що є критично важливим у сучасному ландшафті кіберзагроз. Cyberbit Range також надає можливість оцінки ефективності навчання через автоматизовану систему відстеження прогресу, яка базується на реальних діях користувачів під час симуляцій. Це дозволяє ідентифікувати прогалини в знаннях та навичках, забезпечуючи цілеспрямований підхід до підвищення кваліфікації фахівців з кібербезпеки. Використання Cyberbit Range для навчання роботи з IDS/IPS сприяє значному покращенню часу реагування на інциденти, підвищенню ефективності команд безпеки та забезпечує готовність до реальних кібератак. Це досягається завдяки інтеграції реальних інструментів, гіперреалістичних сценаріїв та детального аналізу дій користувачів у безпечному та контрольованому середовищі.

RangeForce - це інтерактивна платформа для навчання з кібербезпеки, яка надає можливість практичного освоєння роботи з системами виявлення та запобігання вторгненням у реалістичних умовах [13]. Платформа пропонує широкий спектр навчальних модулів, зокрема присвячених Suricata - потужному інструменту для моніторингу мережевої безпеки. У рамках навчання на RangeForce користувачі мають змогу встановлювати,

налаштовувати та керувати Suricata, вивчаючи процес створення та оптимізації правил для виявлення та блокування шкідливої активності. Платформа забезпечує детальні інструкції щодо інтеграції Suricata з такими інструментами, як iptables, що дозволяє ефективно налаштувати систему в режимі IPS. Крім того, користувачі отримують практичний досвід у написанні правил для Suricata. Платформа RangeForce також надає можливість відпрацювання навичок аналізу мережевого трафіку та виявлення аномалій, використовуючи реальні інструменти та сценарії атак. Це дозволяє фахівцям з кібербезпеки підготуватися до реальних викликів, покращити свої навички та впевненість у роботі з IDS/IPS-системами.

Cisco Cyber Range - це хмарна платформа, яка імітує мережу та додатки типового корпоративного середовища, надаючи можливість проведення кібервоєнних навчань та практичних занять з окремих технологій [14]. Це дозволяє фахівцям з кібербезпеки відпрацьовувати навички роботи з системами IDS/IPS у реалістичних умовах. Платформа пропонує віртуальні тренінги, розроблені експертами з реагування на інциденти Cisco Talos. Навчання побудоване за принципом "від простого до складного", де учасники спочатку вивчають різні інструменти та техніки, а потім застосовують їх у реальних сценаріях. Це забезпечує глибоке розуміння методологій та технік, необхідних для ефективного реагування на кіберзагрози. Під час тренувань учасники отримують досвід роботи з реальними інструментами та технологіями, що використовуються в сучасних системах IDS/IPS. Це включає аналіз мережевого трафіку, виявлення аномалій та впровадження політик безпеки для запобігання вторгненням. Крім того, платформа надає можливість відпрацювання командної взаємодії та покращення технічних і комунікативних навичок, що є критично важливими для ефективної роботи команд безпеки. Використання Cisco Cyber Range для навчання роботи з IDS/IPS дозволяє фахівцям з кібербезпеки підвищити свою готовність до реальних атак, покращити навички виявлення та реагування на загрози, а також забезпечити більш надійний захист інформаційних систем організації.

IBM X-Force Cyber Range - це передова платформа, розроблена для підготовки фахівців до ефективного реагування на кіберінциденти, зокрема шляхом навчання роботи з системами виявлення та запобігання вторгненням [15]. Платформа створює інтерактивні симуляції, що занурюють команди у реалістичні сценарії порушень безпеки, допомагаючи їм відпрацьовувати навички виявлення загроз, аналізу та координації дій у відповідь. Це дозволяє учасникам отримати практичний досвід роботи з IDS/IPS у контрольованому середовищі, що імітує реальні умови. Крім того, IBM X-Force Cyber Range надає можливість оцінити готовність організації до кіберзагроз та вдосконалити стратегії захисту, забезпечуючи більш глибоке розуміння сучасних методів атак та засобів їхнього виявлення.

Ринок пропонує широкий вибір комерційних платформ для навчання кібербезпеці, проте їх висока вартість часто стає бар’єром для навчальних закладів, малого та середнього бізнесу, а також організацій із обмеженими фінансовими ресурсами. Витрати на ліцензування, технічну підтримку та оновлення таких рішень можуть бути значними, що обмежує доступ до необхідних інструментів для ефективної підготовки спеціалістів з кіберзахисту. Багато установ стикаються з труднощами при впровадженні дорогих платформ, таких як Cyberbit Range, Cisco Cyber Range або IBM X-Force Cyber Range, через їхню високу вартість.

Відповіддю на ці виклики стає використання відкритого програмного забезпечення та безкоштовних рішень. Такі платформи, як pfSense, ONPsense та системи віртуалізації дозволяють створювати навчальні лабораторії без необхідності значних фінансових вкладень. Це забезпечує установам можливість гнучкого налаштування середовища відповідно до конкретних потреб навчального процесу, а також дозволяє експериментувати з різними конфігураціями та сценаріями кіберзахисту. Альтернативні рішення не тільки значно знижують фінансове навантаження, а й надають більшу свободу в адаптації інфраструктури під вимоги навчальних курсів або корпоративного навчання. Це дає змогу забезпечити високоякісну підготовку фахівців, використовуючи доступні ресурси та сучасні підходи до навчання, сприяючи

більш ефективному впровадженню навичок виявлення та запобігання кіберзагрозам у реальних умовах.

1.4 Висновки до першого розділу

В першому розділі було проведено аналіз систем виявлення та запобігання вторгненням. Описано принципи роботи та їх класифікацію. Розглянуто основні типи IDS/IPS за методом збору даних, а саме мережеві (NIDS/NIPS) та хостові (HIDS/HIPS), їхні особливості, переваги та недоліки. Також було детально розглянуто методи аналізу загроз, що використовуються у системах IDS/IPS, зокрема сигнатурний, поведінковий та гібридний підходи. Окрім теоретичного огляду, було проаналізовано переваги використання тренувальних середовищ для навчання роботи з IDS/IPS. Відзначено, що такі середовища дозволяють ефективно відпрацьовувати навички аналізу трафіку, виявлення загроз та реагування на інциденти у безпечному та контрольованому середовищі. Завдяки використанню віртуалізації можна створювати різноманітні сценарії атак та виявлення загроз, що значно підвищує якість підготовки фахівців з кібербезпеки.

Також було проведено огляд існуючих комерційних рішень для навчання роботи з IDS/IPS, таких як Check Point Cyber Range, Cyberbit Range, RangeForce, Cisco Cyber Range, IBM X-Force Cyber Range. Визначено, що хоча ці рішення пропонують високоякісне навчання та реалістичні сценарії кібератак, їх висока вартість може бути значною перешкодою для навчальних закладів, малого та середнього бізнесу, а також організацій з обмеженим бюджетом. Альтернативним підходом є використання відкритого програмного забезпечення та безкоштовних платформ, таких як pfSense та OPNsense, а також інструментів віртуалізації. Це дозволяє значно знизити фінансові витрати, забезпечуючи при цьому ефективне навчання роботі з IDS/IPS.

Таким чином, розглянуті підходи до створення та використання тренувальних середовищ демонструють важливість практичного навчання з кібербезпеки. Вони дають змогу не лише глибше зрозуміти принципи роботи

IDS/IPS, але й адаптувати навчальний процес під конкретні потреби, що є важливим для підготовки висококваліфікованих спеціалістів у сфері інформаційної безпеки.

РОЗДІЛ 2 РОЗРОБКА ТРЕНУВАЛЬНОГО СЕРЕДОВИЩА

2.1 Структура тренувального середовища

Архітектура тренувального середовища для навчання роботи з IDS/IPS базується на використанні гіпервізора VMware ESXi, який забезпечує створення та управління віртуальними машинами, що моделюють різні компоненти мережевої інфраструктури [16].

На рисунку 2.1 показана структура тренувального середовища.

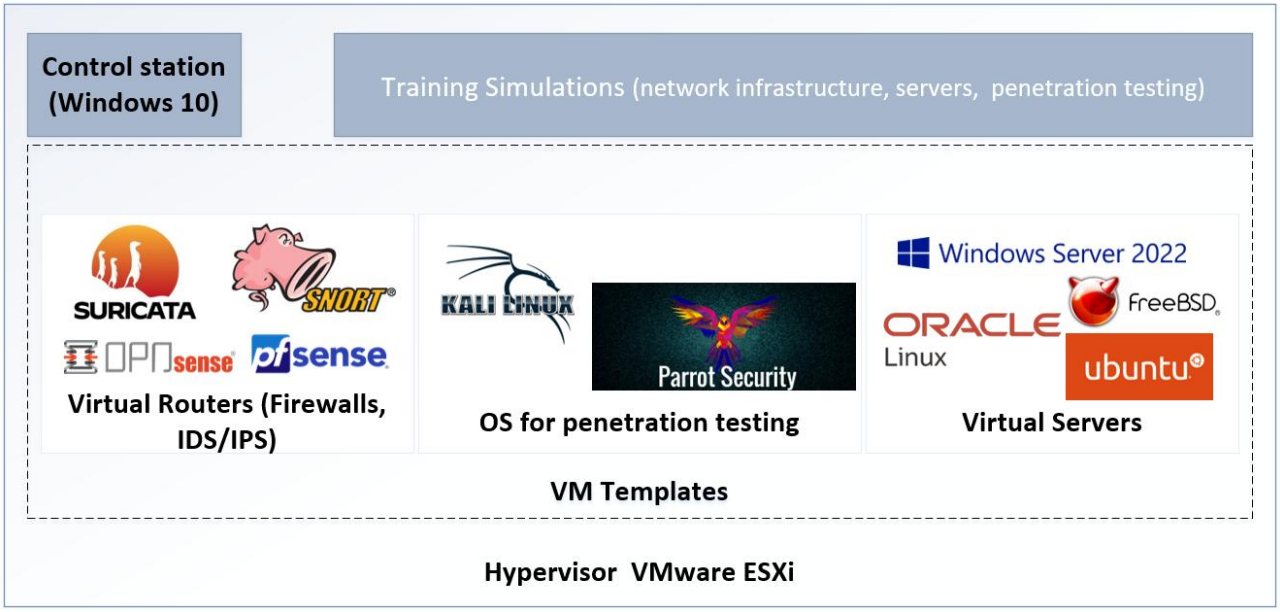


Рисунок 2.1 – Структура тренувального середовища

Контрольна станція (Control Station), яка працює під керуванням Windows 10 виконує роль платформи для керування тренувальним середовищем, дозволяючи адміністраторам і студентам взаємодіяти з віртуалізованими компонентами, здійснювати моніторинг, налаштування та аналіз мережевого трафіку та інцидентів безпеки.

Навчальні симуляції охоплюють різні аспекти інформаційної безпеки, включаючи мережеву інфраструктуру, сервери та тестування на проникнення. Для цього у віртуальному середовищі розгорнуті три основні групи компонентів.

Перша група включає віртуальні маршрутизатори та міжмережеві екрани з вбудованими IDS/IPS. Сюди входять такі рішення, як OPNsense та pfSense з Suricata та Snort, Вони використовуються для аналізу мережевого трафіку, виявлення вторгнень, запобігання атакам та управління політиками доступу. Кожна з цих систем має свої особливості та використовується для тестування ефективності різних методів виявлення загроз і реагування на них.

Друга група складається з операційних систем, призначених для тестування безпеки та проведення атак. Серед них представлені Kali Linux та Parrot Security, які містять широкий набір інструментів для тестування на проникнення, аналізу трафіку та дослідження кіберзагроз. Вони дозволяють моделювати реальні атаки на мережу та аналізувати реакцію IDS/IPS-систем.

Третя група включає віртуальні сервери, які імітують стандартну корпоративну інфраструктуру. Це Windows Server 2022, Oracle Linux, FreeBSD та Ubuntu, які слугують цілями для атак та джерелами реального мережевого трафіку. Їх використання дозволяє відпрацьовувати сценарії атак на серверні операційні системи та аналізувати їхню стійкість до загроз.

Усі ці компоненти існують у вигляді віртуальних машин (VM templates), що забезпечує швидке розгортання та налаштування середовища під різні навчальні завдання.

Завдяки такій архітектурі тренувальне середовище дозволяє вивчати принципи роботи IDS/IPS, відпрацьовувати виявлення та запобігання вторгненням, тестувати різні методи атак та оцінювати ефективність захисних механізмів у реальних умовах.

2.2 Елементи тренувального середовища

2.2.1 Гіпервізор VMware ESXi

VMware ESXi – це гіпервізор типу 1 (bare-metal), який встановлюється безпосередньо на апаратне забезпечення серверів та забезпечує віртуалізацію без необхідності встановлення додаткової операційної системи [17]. Він є

основою для створення та управління віртуалізованим середовищем у дата-центрах, корпоративних мережах та навчальних лабораторіях.

Гіпервізор має архітектуру, що базується на ядрі VMkernel, яке безпосередньо працює з апаратним забезпеченням сервера та керує всіма ресурсами, такими як процесор, пам’ять, мережеві інтерфейси та сховища. На відміну від гіпервізорів типу 2, які встановлюються поверх операційної системи, ESXi працює як самостійна система, що дозволяє зменшити накладні витрати та покращити продуктивність.

Основний принцип роботи VMware ESXi полягає у створенні та керуванні віртуальними машинами, які ізольовані одна від одної та можуть працювати з різними операційними системами. Кожна віртуальна машина має власний набір ресурсів, включаючи віртуальні процесори (vCPU), оперативну пам’ять (vRAM), мережеві адаптери (vNIC) та віртуальні диски. ESXi використовує технологію апаратної віртуалізації, яка дозволяє забезпечити безпосередній доступ віртуальних машин до ресурсів фізичного обладнання з мінімальними затримками.

Гіпервізор VMware ESXi забезпечує ефективну підтримку апаратної віртуалізації завдяки використанню вбудованих технологій сучасних процесорів, таких як Intel VT-x та AMD-V. Ці технології дозволяють запускати віртуальні машини без значних накладних витрат на емуляцію, оскільки інструкції гостьової операційної системи можуть виконуватися безпосередньо на фізичному процесорі.

Під час роботи ESXi використовує апаратну підтримку розширених таблиць сторінок пам’яті (EPT для Intel, RVI для AMD), що значно покращує продуктивність віртуальних машин за рахунок ефективного управління пам’яттю. Завдяки цьому віртуальні машини можуть працювати майже на рівні продуктивності фізичних серверів, оскільки операції трансляції адрес здійснюються апаратно, без залучення додаткових програмних механізмів.

VMware ESXi також підтримує технологію Intel VT-d та AMD IOMMU, яка дозволяє безпосередньо передавати пристрої введення-виведення (I/O) до віртуальних машин. Це означає, що гостьові операційні системи можуть

отримати повний контроль над фізичними пристроями, такими як графічні карти (GPU), мережеві адаптери (NIC) або контролери зберігання даних. Така функція є критично важливою для високопродуктивних обчислень, віртуалізації мережевих функцій (NFV) та тренувальних середовищ, що моделюють реальні мережеві атаки та аналіз загроз у режимі реального часу.

Ще однією важливою особливістю є підтримка прив’язка процесорних ядер (CPU pinning), яка дозволяє виділяти певні фізичні ядра для конкретних віртуальних машин, забезпечуючи передбачувану продуктивність для критично важливих навантажень.

VMware ESXi також має вбудовані механізми для динамічного керування ресурсами (DRS), що дозволяють автоматично балансувати навантаження між віртуальними машинами залежно від їхніх потреб у продуктивності. Це забезпечує ефективний розподіл обчислювальних потужностей та мінімізує простої віртуальних середовищ.

Після встановлення VMware ESXi гіпервізор завантажується з консольним інтерфейсом, який відображає основну інформацію. Це включає версію ESXi, модель процесора, обсяг оперативної пам’яті та IP-адреси, призначені хосту для мережевого доступу. Інтерфейс також надає можливість управління основними параметрами системи, такими як мережеві налаштування, конфігурація збереження даних та безпекові опції (див. рисунок 2.2).

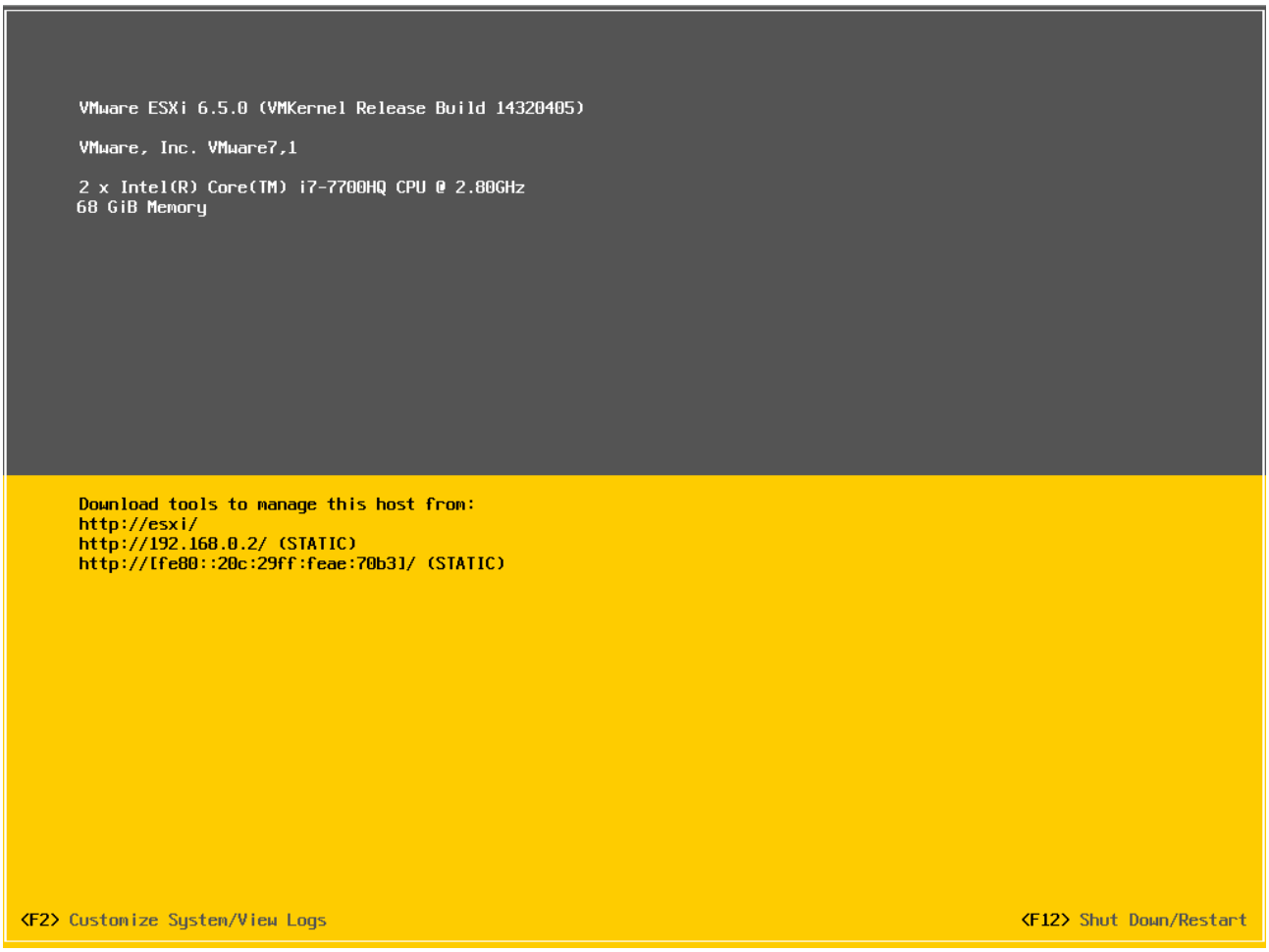


Рисунок 2.2 – Консольний інтерфейс гіпервізора VMware ESXi

Після виконання базових налаштувань VMware ESXi готовий до створення та запуску віртуальних машин. Далі можна почати розгортання віртуалізованої інфраструктури безпосередньо через вбудований веб-інтерфейс.

Управління ESXi здійснюється через веб-інтерфейс vSphere Client, який дозволяє створювати, змінювати, керувати та моніторити віртуальні машини (див. рисунок 2.3).

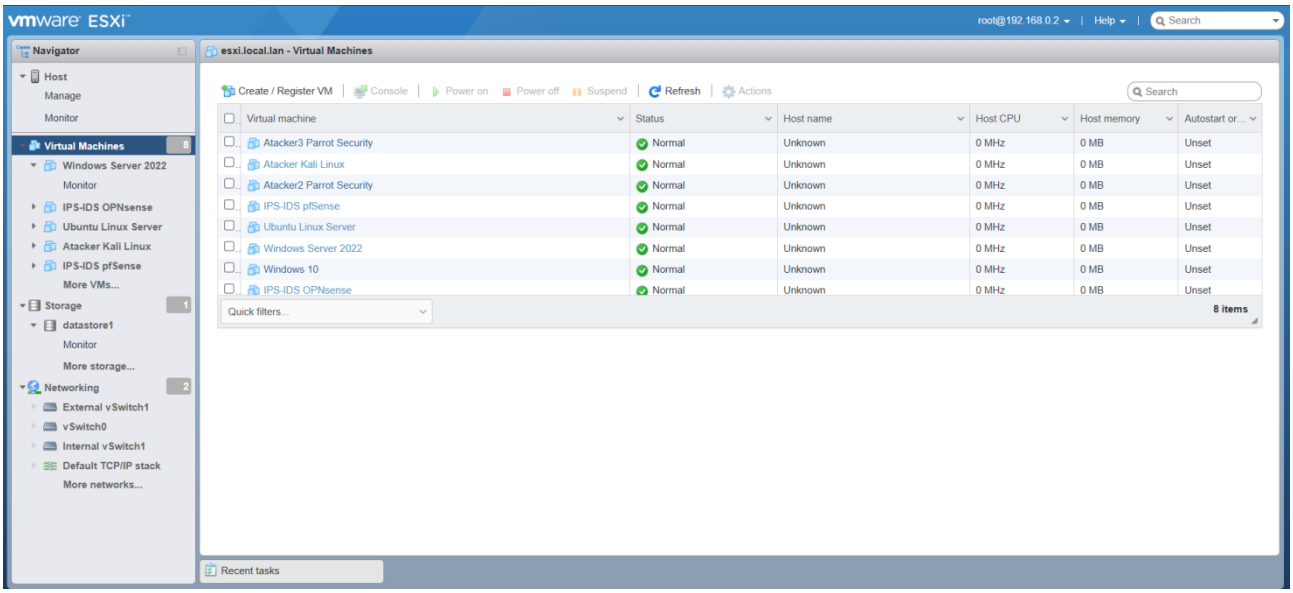


Рисунок 2.3 – Веб-інтерфейс керування VMware ESXi

Додатково може використовуватися vCenter Server, який забезпечує централізоване управління кількома ESXi-хостами, балансування навантаження та автоматизацію процесів.

Для керування збереженням даних використовується спеціалізована файлова система VMFS, яка оптимізована для зберігання образів віртуальних машин та забезпечує швидкий доступ до даних. Вона підтримує одночасний доступ до файлів із кількох вузлів, що дозволяє реалізовувати високонадійні рішення, такі як кластеризація та резервне копіювання.

VMware ESXi також підтримує віртуалізацію мережі, дозволяючи створювати віртуальні комутатори (vSwitch) (див. рисунок 2.4).

Рисунок 2.4 – Віртуальні комутатори (vSwitch) в VMware ESXi

Також є можливість використовувати VLAN, об’єднувати кілька фізичних мережевих інтерфейсів у групи.

2.2.2 Маршрутизатори OPNsense та pfSense

Маршрутизатори OPNsense та pfSense є популярними програмно-апаратними рішеннями для побудови мережевих шлюзів, міжмережевих екранів та систем виявлення та запобігання вторгнень (IDS/IPS). Обидві системи засновані на операційній системі FreeBSD і надають гнучкі можливості для управління мережею та забезпечення кібербезпеки.

Маршрутизатор pfSense є старішим проєктом, який з'явився як форк проєкту m0n0wall. Він широко використовується в корпоративних мережах, центрах обробки даних та навчальних середовищах через свою стабільність і багатий функціонал [18]. pfSense підтримує балансування навантаження, VPN-тунелі, систему IDS/IPS (на основі Snort або Suricata), VLAN, а також інтеграцію з зовнішніми SIEM-системами для моніторингу подій безпеки. Адміністрування відбувається через веб-інтерфейс (див. рисунок 2.5), що дозволяє легко налаштовувати політики безпеки та мережеві правила.

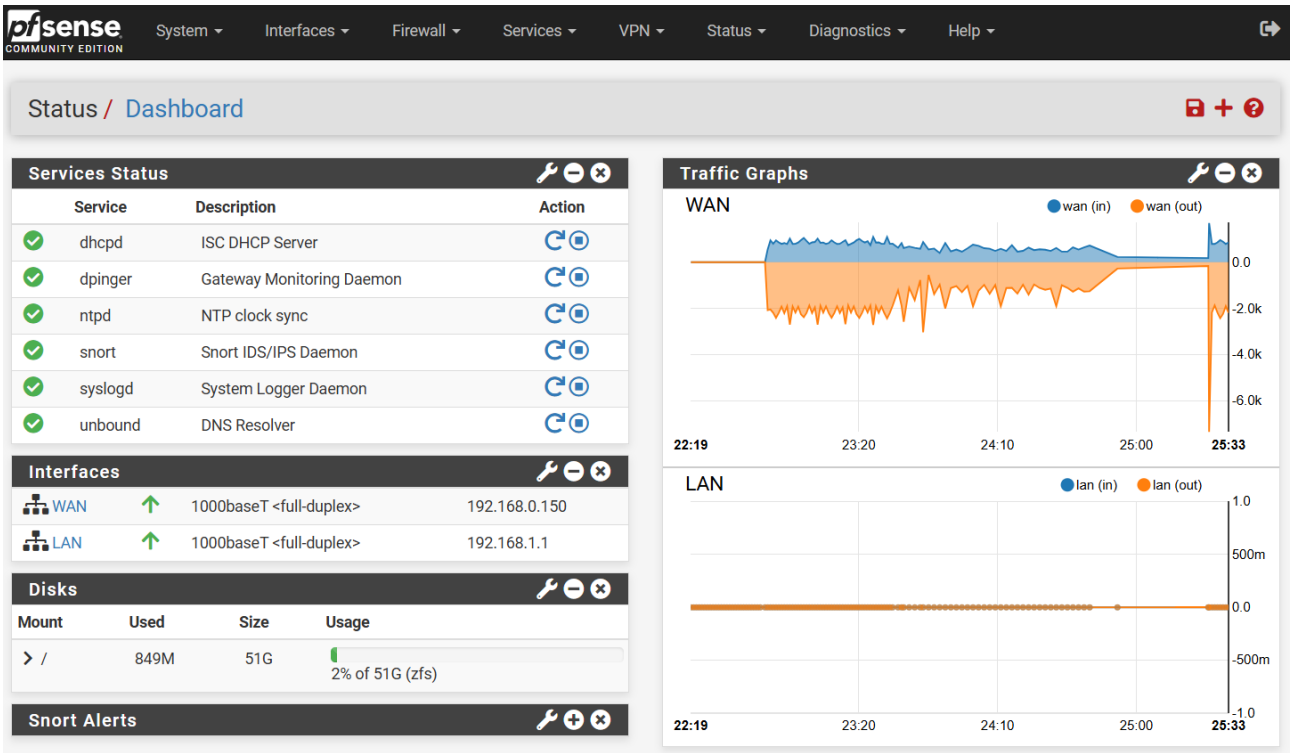


Рисунок 2.5 – Веб-інтерфейс адміністрування pfSense

Маршрутизатор pfSense має як відкриту безкоштовну версію, так і комерційну, яка пропонує додаткові функції та підтримку.

OPNsense є відгалуженням pfSense. Його відмінністю є поліпшений інтерфейс, що базується на сучасних веб-технологіях. OPNsense включає такі функції, як автоматичне оновлення, інтеграція з хмарними сервісами, вбудований проксі-сервер, можливість глибокого аналізу трафіку та підтримка API для автоматизації налаштувань. Як і pfSense, він підтримує Suricata та Snort для реалізації IDS/IPS-функцій, а також VPN, NAT, балансування навантаження та контроль доступу [19].

Веб-інтерфейс OPNsense надає зручний інструмент для моніторингу та управління мережею, забезпечуючи адміністраторів детальною інформацією про продуктивність системи, стан шлюзів, міжмережевий екран і запущені сервіси (див. рисунок 2.6).

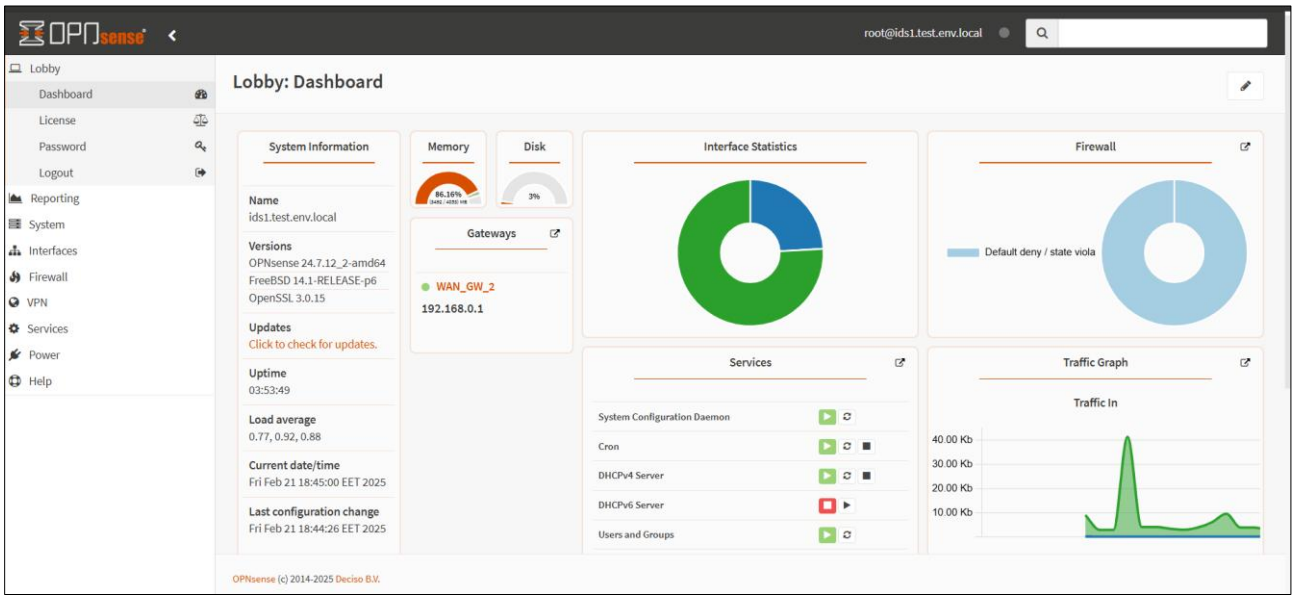


Рисунок 2.6 – Веб-інтерфейс адміністрування OPNsense

Це дозволяє оперативно реагувати на зміни в мережі, контролювати трафік та налаштовувати параметри безпеки відповідно до вимог.

Головна різниця між pfSense та OPNsense полягає у філософії розробки та частоті оновлень. OPNsense оновлюється частіше, забезпечуючи швидке виправлення вразливостей та нові можливості, тоді як pfSense зосереджений на

стабільності та довготривалому циклі підтримки. Вибір між цими двома платформами залежить від конкретних вимог до безпеки, продуктивності та адміністрування мережі.

Обидва рішення були використані як віртуалізовані маршрутизатори на VMware ESXi що робить їх зручними для тренувальних середовищ та тестових стендів. Вони дозволяють створювати складні мережеві конфігурації з багаторівневим захистом, аналізувати трафік та відпрацьовувати сценарії виявлення та запобігання вторгненням.

2.2.3 Операційні системи для тестування безпеки

Kali Linux та Parrot Security – це дві популярні операційні системи, призначені для тестування безпеки, аналізу мереж, цифрової криміналістики та етичного хакінгу. Обидві системи базуються на Debian і містять широкий набір попередньо встановлених інструментів для тестування на проникнення, аналізу вразливостей та зламу паролів.

Kali Linux була розроблена компанією Offensive Security як спадкоємець BackTrack і стала стандартом у сфері тестування безпеки [20]. Вона містить сотні інструментів для атак на мережі, аналізу веб-додатків, експлуатації вразливостей, створення експлойтів, перехоплення трафіку та роботи з бездротовими мережами. Kali часто використовується спеціалістами з кібербезпеки, етичними хакерами та адміністраторами мереж для проведення тестів на проникнення.

На рисунок 2.7 показані мережеві налаштування Kali Linux, які містять детальну інформацію про активні мережеві інтерфейси, їхні IP-адреси та таблицю маршрутизації.

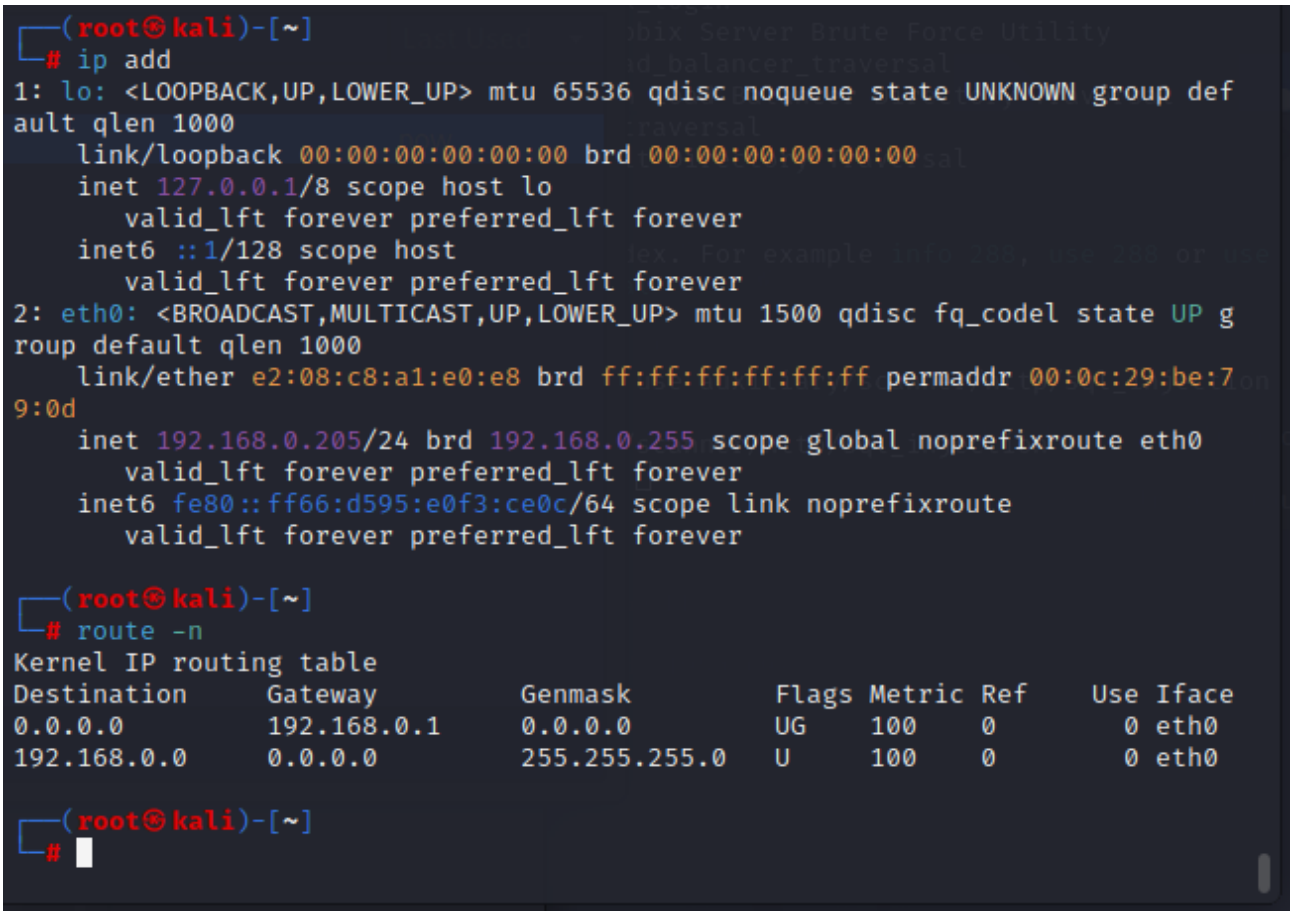


Рисунок 2.7 – Мережеві налаштування Kali Linux

Parrot Security OS була створена розробниками компанії ParrotSec і орієнтована на тестування безпеки і цифрову криміналістику [21]. Вона пропонує більш оптимізовану систему з меншою витратою ресурсів, ніж Kali Linux, що робить її ідеальною для пристроїв із слабшим апаратним забезпеченням. Parrot включає всі ключові інструменти для тестування на проникнення, а також додаткові засоби для розробників, цифрової криміналістики, анонімного перегляду вебсторінок та аналізу шкідливого ПЗ. Однією з основних переваг є більш суворий підхід до безпеки, включаючи Sandboxing для ізоляції потенційно небезпечних програм. Parrot Security підтримує захищене ядро Linux, шифрування диска та інтеграцію з анонімною мережею Tor.

На рисунок 2.8 показані мережеві налаштування Parrot Security.

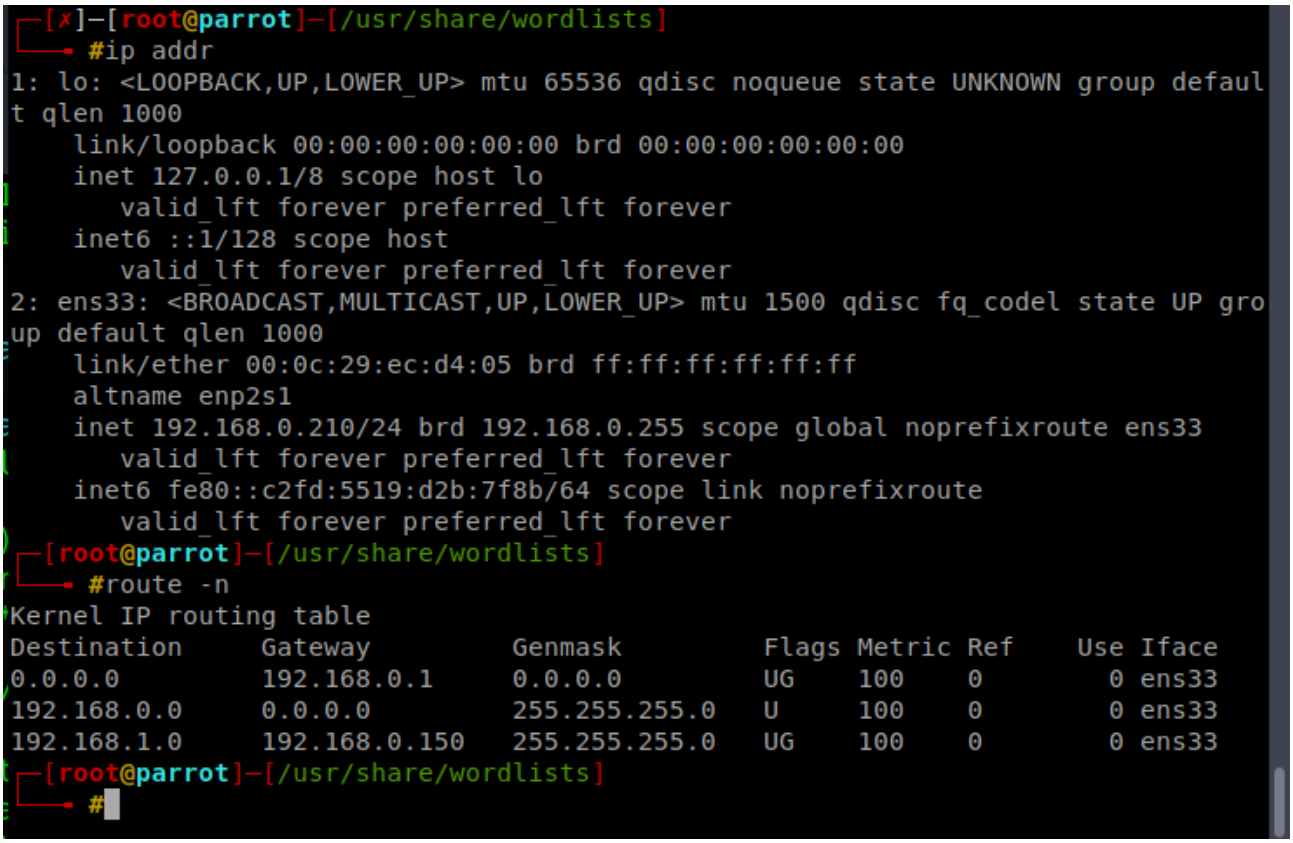


Рисунок 2.8 – Мережеві налаштування Parrot Security

Використання Kali Linux та Parrot Security у тренувальному середовищі для навчання роботи з IDS/IPS є ключовим елементом підготовки фахівців з кібербезпеки. Обидві операційні системи розроблені для тестування на проникнення, аналізу вразливостей, перехоплення мережевого трафіку та імітації атак, що дозволяє створювати реалістичні сценарії для оцінки ефективності систем виявлення та запобігання вторгненням.

У такому середовищі Kali Linux та Parrot Security використовуються як атакуючі платформи, що дозволяють виконувати різні типи атак на мережеву інфраструктуру, сервери та кінцеві пристрої. Це включає сканування мережі за допомогою Nmap, виявлення вразливостей через Metasploit Framework, експлуатацію слабких паролів за допомогою Hydra та перехоплення трафіку через Wireshark або Ettercap. Такі атаки генерують аномалії у мережевому трафіку, які можуть бути виявлені системами IDS, такими як Snort, Suricata.

Використання Kali Linux дозволяє тестувати поведінковий та сигнатурний підходи в IDS/IPS, налаштовувати правила виявлення вторгнень та оцінювати ефективність існуючих захисних механізмів. Наприклад, виконання атак типу

SQL-ін’єкції або експлуатації відомих CVE дозволяє перевірити, чи правильно налаштовані сигнатури в системі виявлення вторгнень. Також можна здійснювати DDoS-тестування через такі інструменти, як hping3, щоб оцінити здатність IPS виявляти та блокувати підозрілий трафік.

Віртуалізація цих операційних систем на платформі VMware ESXi дозволяє створювати ізольовані середовища для безпечного проведення атак та експериментів з конфігураціями IDS/IPS. Важливою перевагою є можливість моделювання складних сценаріїв кібератак, перевірки реакції системи безпеки та навчання швидкого реагування на інциденти.

Таким чином, використання Kali Linux та Parrot Security у тренувальному середовищі дозволяє студентам та спеціалістам з кібербезпеки отримати практичний досвід роботи з IDS/IPS, навчитися ефективно виявляти та блокувати атаки, тестувати сигнатурний та поведінковий аналіз загроз, а також розробляти стратегії захисту для реальних мережевих інфраструктур.

2.2.3 Віртуальні сервери

Віртуальні сервери Windows Server 2022, Oracle Linux, FreeBSD та Ubuntu Linux у тренувальному середовищі з IDS/IPS використовуються як цільові системи для імітації атак і тестування ефективності систем виявлення та запобігання вторгненням. Вони дозволяють змоделювати реальні мережеві середовища, що зустрічаються в корпоративних та хмарних інфраструктурах, і перевірити, наскільки добре IDS/IPS може виявляти аномальну активність, реагувати на загрози та запобігати компрометації.

Windows Server 2022 часто виступає ціллю атак через його широке використання в корпоративних мережах [22]. Найпоширенішими векторами атак є експлуатація вразливостей RDP, brute-force атаки на служби авторизації, використання вразливостей Active Directory, віддалене виконання коду або вразливі вебсервери IIS.

На рисунку 2.9 представлено робоче середовище Windows Server 2022 з ролю сервера віддалених робочих столів (RDS).

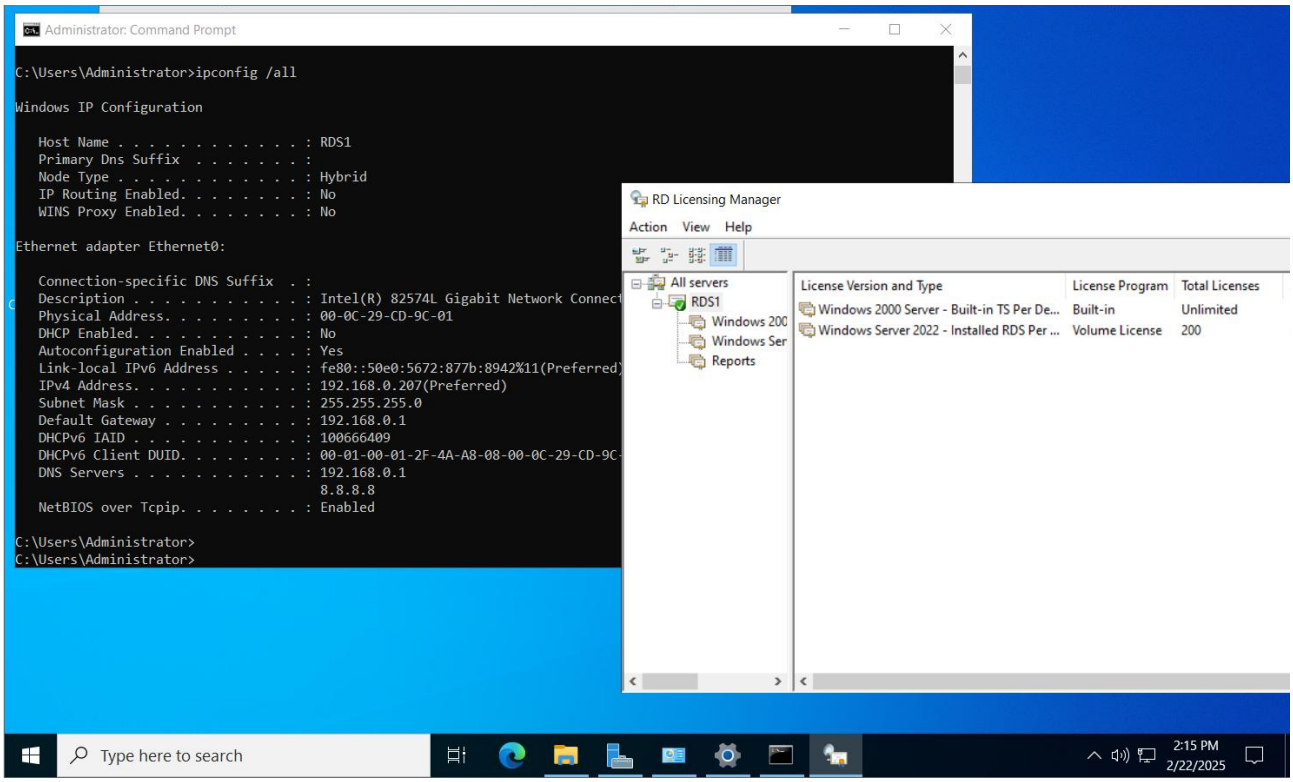


Рисунок 2.9 – Мережеві налаштування Windows Server 2022

Сервер налаштований для роботи у корпоративному середовищі з фіксованими IP-адресами та ліцензованими службами RDS [23]. Він використовується для надання віддаленого доступу користувачам і може бути ціллю для тестування безпеки, зокрема аналізу вразливостей у службах RDP та атак на авторизацію.

Oracle Linux як цільова система використовується для перевірки атак на серверні служби, такі як MySQL, Apache, Nginx та SSH [24]. До поширених атак належать SQL-ін'єкції, DoS-атаки, brute-force атаки на SSH.

FreeBSD є популярною платформою для хостингу серверів, файрволів та спеціалізованих мережевих пристроїв, що робить його важливою мішенню для атак [25].

Ubuntu Linux часто використовується як серверна ОС у хмарних середовищах, контейнерних рішеннях та веб-хостингу [26]. Найчастішими загрозами є brute-force атаки на SSH, DDoS-атаки на вебсервери Apache/Nginx, атаки на DNS.

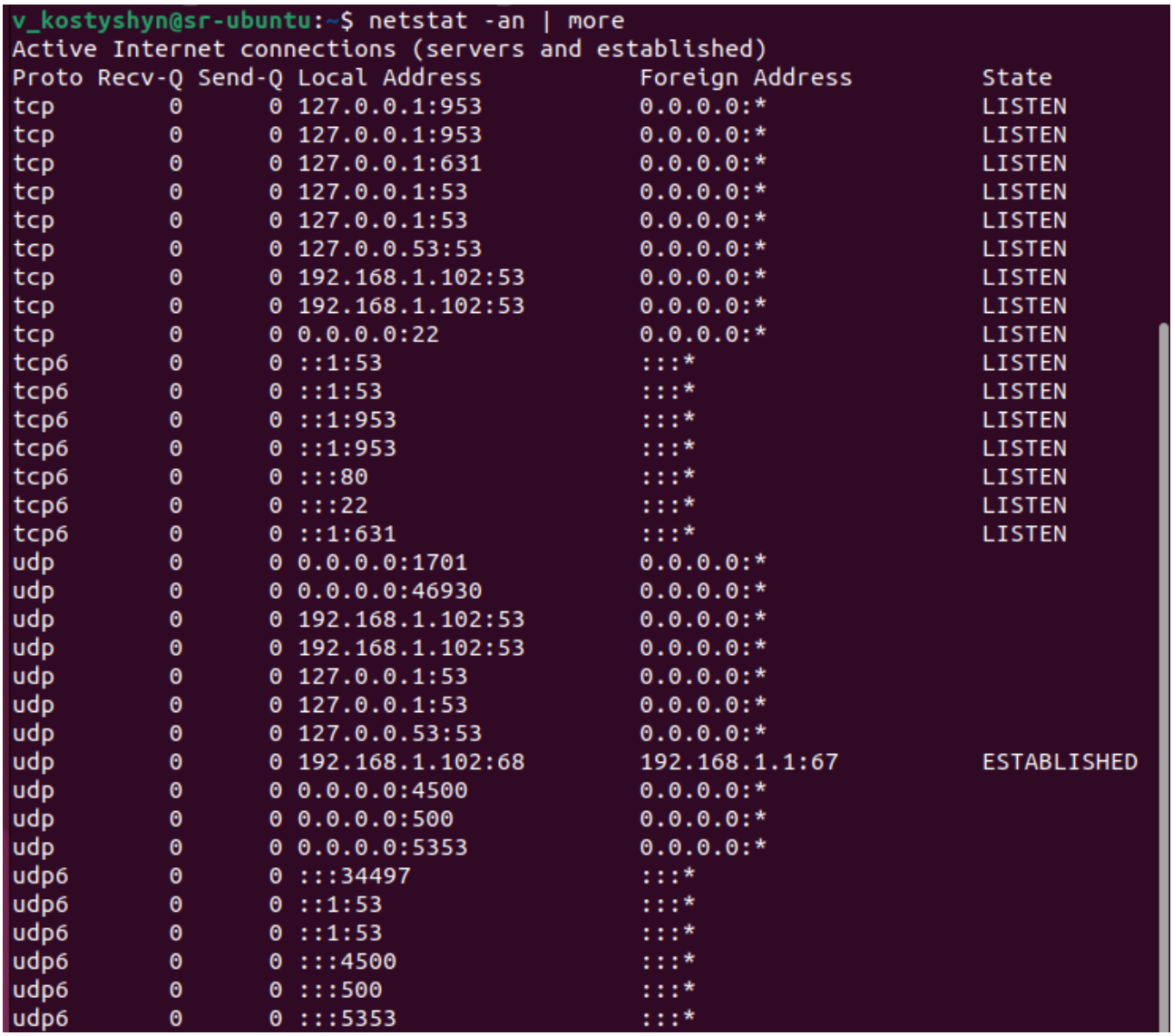
На рисунок 2.10 показані мережеві налаштування Ubuntu Linux.

```
v_kostyshyn@sr-ubuntu:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:e9:ce:80 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.102/24 brd 192.168.1.255 scope global dynamic noprefixroute e
ns33
       valid_lft 4983sec preferred_lft 4983sec
v_kostyshyn@sr-ubuntu:~$
```

Рисунок 2.10 – Мережеві налаштування Ubuntu Linux

На рисунку 3.11 показано вивід команди `netstat -an` у терміналі операційної системи Ubuntu Linux, яка використовується для відображення активних мережевих з'єднань, портів, що прослуховуються, та встановлених підключень.

У списку видно, що сервер слухає DNS-запити, що означає, що сервер працює як локальний DNS та відповідає на запити з локальної мережі. Також порт 22/TCP відкритий для підключень через SSH та порт 80/TCP відкритий для підключень через HTTP.



```
v_kostyshyn@sr-ubuntu:~$ netstat -an | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.102:53        0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.102:53        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 ::1:53                  :::*                    LISTEN
tcp6       0      0 ::1:53                  :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 0.0.0.0:1701            0.0.0.0:*
udp        0      0 0.0.0.0:46930           0.0.0.0:*
udp        0      0 192.168.1.102:53        0.0.0.0:*
udp        0      0 192.168.1.102:53        0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.1.102:68        192.168.1.1:67          ESTABLISHED
udp        0      0 0.0.0.0:4500            0.0.0.0:*
udp        0      0 0.0.0.0:500             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp6       0      0 :::34497                :::*
udp6       0      0 ::1:53                  :::*
udp6       0      0 ::1:53                  :::*
udp6       0      0 :::4500                 :::*
udp6       0      0 :::500                  :::*
udp6       0      0 :::5353                 :::*
```

Рисунок 2.11 – Вивід команди `netstat -an` в Ubuntu Linux

Використання цих серверних операційних систем як цілей атак дозволяє відпрацьовувати різні методи проникнення, перевіряти ефективність політик безпеки, тестувати поведінковий та сигнатурний підхід в IDS/IPS та аналізувати сценарії реагування на кіберзагрози в реальному часі. Завдяки цьому спеціалісти з кібербезпеки отримують практичний досвід роботи з захистом реальних серверних середовищ та удосконалюють навички виявлення та запобігання вторгненням.

2.3 Висновки до другого розділу

В другому розділі було проведено детальний аналіз архітектури та структури тренувального середовища, призначеного для навчання роботи з IDS/IPS. Було описано ключові компоненти середовища, включаючи гіпервізор VMware ESXi, віртуалізовані маршрутизатори pfSense та OPNsense, операційні системи для тестування безпеки Kali Linux та Parrot Security, а також серверні ОС, які використовуються як цілі атак, серед яких Windows Server 2022, Oracle Linux, FreeBSD та Ubuntu Linux. Розгляд гіпервізора VMware ESXi продемонстрував його важливу роль у створенні ізольованого та безпечного середовища для тестування IDS/IPS. Було висвітлено його ключові можливості, включаючи підтримку апаратної віртуалізації, ефективне управління ресурсами та інтеграцію з механізмами динамічного балансування навантаження. Описано методи керування ESXi через веб-інтерфейс vSphere Client та використання віртуальних комутаторів для організації мережевої взаємодії між віртуальними машинами. Аналіз маршрутизаторів OPNsense та pfSense показав, що ці рішення дозволяють створювати міжмережеві екрани з системами IDS/IPS на базі Snort та Suricata. Розглянуто їхні функції для управління мережею, моніторингу трафіку та захисту від вторгнень. Детально розглянуто Kali Linux та Parrot Security як платформи для тестування безпеки та моделювання атак. Підкреслено їхній широкий набір інструментів для тестування на проникнення. Описано їхню роль у створенні реалістичних сценаріїв атак, аналізу трафіку та оцінки реакції IDS/IPS. Описані віртуальні сервери Windows Server 2022, Oracle Linux, FreeBSD та Ubuntu Linux як цілі атак. Визначено типові загрози для кожної операційної системи, включаючи brute-force атаки на SSH та RDP, DDoS-атаки на вебсервери, DNS.

Таким чином, тренувальне середовище забезпечує комплексний підхід до навчання роботи з IDS/IPS, дозволяючи моделювати реальні сценарії атак, аналізувати мережевий трафік, тестувати механізми виявлення та запобігання загрозам. Використання віртуалізації, спеціалізованих маршрутизаторів,

атакуючих та цільових серверів дає можливість відпрацювати різні методики атак та оцінити ефективність сучасних засобів кіберзахисту.

РОЗДІЛ 3 ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ТРЕНУВАЛЬНОГО СЕРЕДОВИЩА

3.1 Сценарій 1: Тестування pfSense та Snort в режимі IPS

3.1.1 Схема сценарію

Сценарій 1 передбачає тестування pfSense із інтегрованим Snort у режимі IPS. Це означає, що система не лише виявлятиме загрози, а й активно блокуватиме шкідливий трафік. Архітектура середовища побудована таким чином, що весь трафік проходить через pfSense, де Snort аналізує пакети та запобігає потенційним атакам (див. рисунок 3.1).

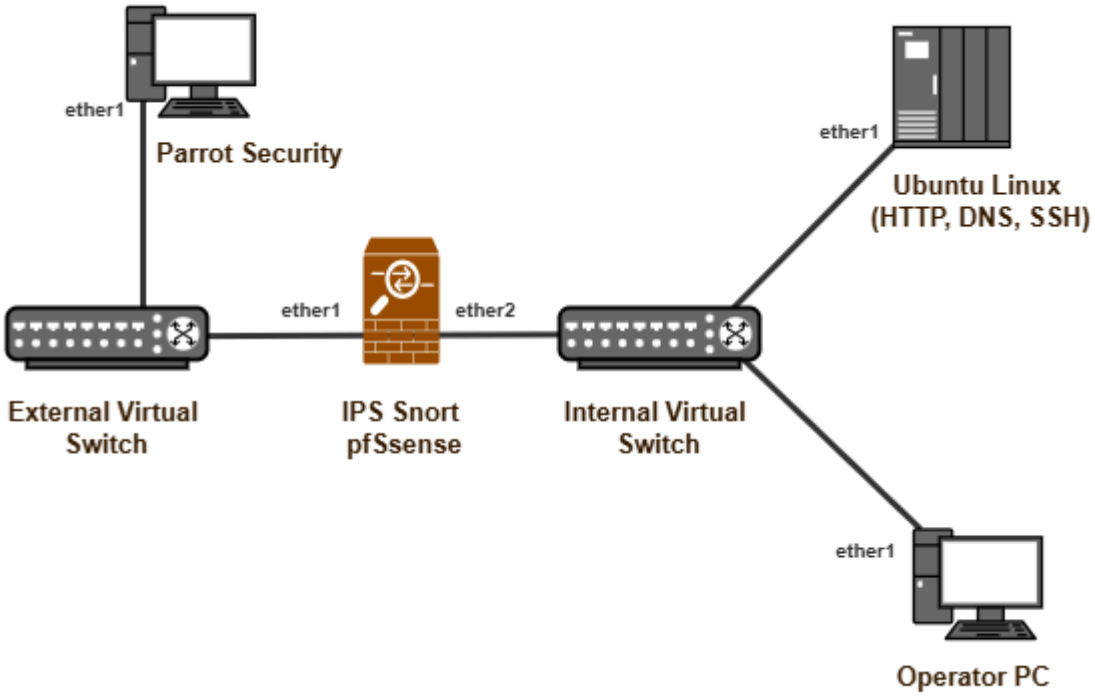


Рисунок 3.1 – Схема сценарію 1

Віртуальна інфраструктура складається з зовнішнього та внутрішнього віртуальних комутаторів (External Virtual Switch та Internal Virtual Switch), які забезпечують логічний поділ мережі. Parrot Security виступає в ролі атакуючої

системи, що використовується для моделювання кіберзагроз. Вона підключена до зовнішнього комутатора та має доступ до мережі, що дозволяє виконувати атаки на внутрішні ресурси. pfSense із Snort працює в ролі IPS і виконує функцію міжмережевого екрану, аналізуючи вхідний трафік і блокуючи потенційно небезпечні пакети. Він має два мережевих інтерфейси: ether1 (WAN) підключений до зовнішньої мережі, а ether2 (LAN) – до внутрішньої.

Внутрішня мережа містить Ubuntu Linux, що виконує роль цільового сервера з веб-сервісом (HTTP), службою доменних імен (DNS) та SSH. Цей сервер є основною мішенню атак. Також у мережі є Operator PC, який використовується для моніторингу та аналізу робити складових середовища.

У таблиці 3.1 наведені мережеві налаштування пристроїв, що беруть участь у сценарії тестування pfSense із Snort у режимі IPS.

Таблиця 3.1 – Мережеві налаштування сценарію 1

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Шлюз
pfSense	ether1	192.168.0.150	255.255.255.0	192.168.0.1
	ether2	192.168.1.1	255.255.255.0	
Parrot Security	ether1	192.168.0.210	255.255.255.0	192.168.0.1
Ubuntu Linux	ether1	192.168.1.102	255.255.255.0	192.168.1.1
Operator PC	ether1	192.168.1.112	255.255.255.0	192.168.1.1

Архітектура побудована на двох окремих підмережах:

- 192.168.0.0/24 – зовнішня мережа, через яку атакуючий вузол Parrot Security надсилає запити;

- 192.168.1.0/24 – внутрішня мережа, що містить цільовий сервер Ubuntu Linux та робочу станція Operator PC

Маршрутизатор pfSense працює як міжмережевий екран і точка фільтрації трафіку, маючи два мережеві інтерфейси. Інтерфейс ether1 (WAN) з IP-адресою 192.168.0.150/24 – підключений до зовнішньої мережі, де розташований Parrot Security. Трафік із цієї мережі проходить через IPS Snort для перевірки.

Інтерфейс ether2 (LAN) з IP-адресою 192.168.1.1/24 – підключений до внутрішньої мережі, де працює цільова система Ubuntu Linux. Це шлюз для всіх внутрішніх пристроїв.

Parrot Security розташований у зовнішній мережі з IP-адресою 192.168.0.210/24. Використовуючи цей вузол, проводяться атаки на цільовий сервер. Його шлюз – 192.168.0.1, що вказує на можливість виходу в Інтернет та доступу до інших мереж. Ubuntu Linux, який виконує роль сервера, має IP-адресу 192.168.1.102/24 і використовує шлюз 192.168.1.1 (pfSense). Відкриті порти, такі як 22 (SSH), 53 (DNS), 80 (HTTP) є стати ціллю для атак із зовнішньої мережі.

Такий поділ мереж дозволяє створити реалістичний сценарій атак та оцінити ефективність роботи Snort у режимі IPS, де він не тільки виявляє, але й блокує шкідливий трафік між сегментами 192.168.0.0/24 та 192.168.1.0/24.

3.1.2 Сканування відкритих портів Ubuntu Linux

Сканування відкритих портів Ubuntu Linux за допомогою Parrot Security є одним із базових методів розвідки під час тестування на проникнення або атаки. Мета сканування – визначити активні служби, відкриті порти та потенційні вразливості цільової системи. Для цього використовуються спеціалізовані інструменти, такі як Nmap та інші, які дозволяють виявити відкриті TCP і UDP порти (див. рисунок 3.2).

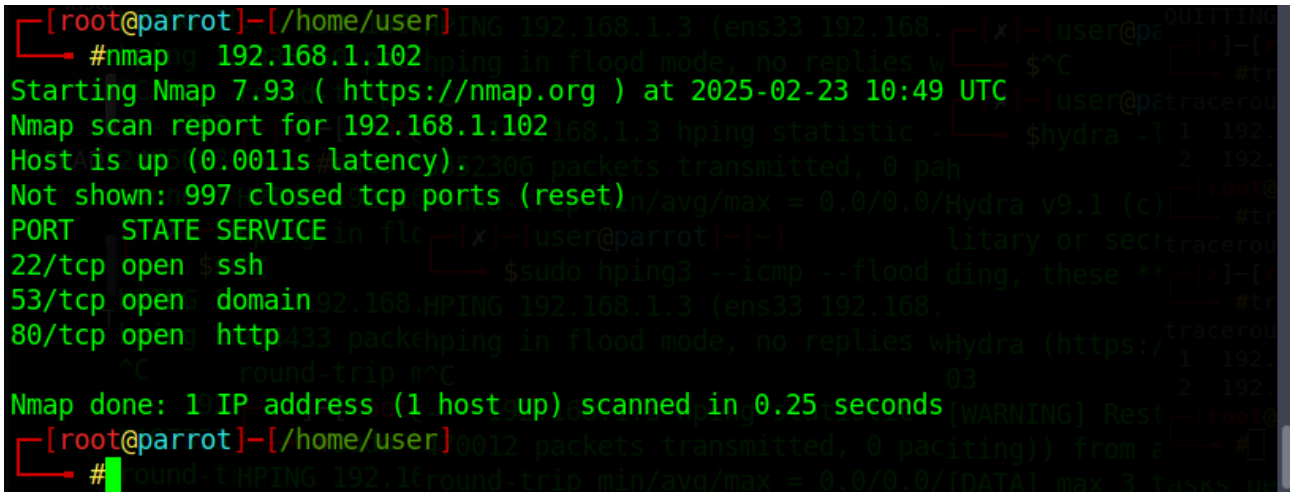


Рисунок 3.2 – Сканування відкритих портів в Ubuntu Linux

У результатах вказано, що 997 TCP-портів закриті (reset), а три порти відкриті:

- 22/tcp open ssh – вказує, що сервер має відкритий порт SSH, який може бути використаний для віддаленого доступу. Це потенційний вектор атаки, особливо якщо сервер використовує слабкі паролі або стандартні облікові записи;
- 53/tcp open domain – свідчить про запущений DNS-сервер, що може бути використано для DDoS атак;
- 80/tcp open http – означає, що на сервері працює веб-сервер, що може бути ціллю атак типу.

3.1.3 Здійснення brute force та DDoS атак

Brute force атака на SSH в Ubuntu Linux з Parrot Security за допомогою Hydra виконується для перевірки стійкості облікових записів до підбору паролів та тестування правил виявлення атаки в IPS Snort. Hydra – це багатопотоковий інструмент для автоматизованого підбору паролів до мережевих сервісів, включаючи SSH, HTTP, FTP, SMTP та інші.

На рисунку 3.3 показано виконання brute force атаки [27] [28] на SSH сервіс Ubuntu Linux за допомогою інструменту Hydra у Parrot Security.

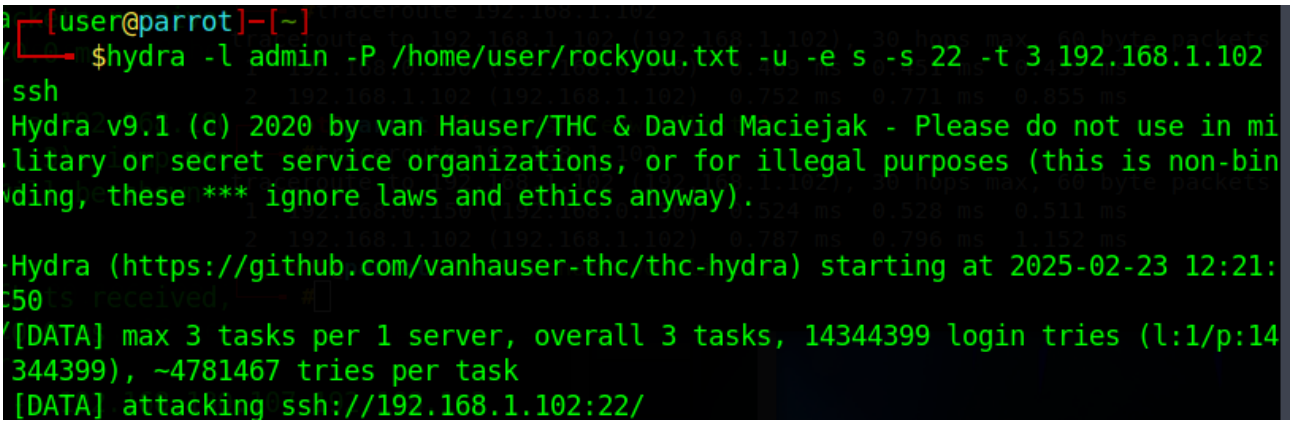


Рисунок 3.3 – Виконання brute force атаки на SSH сервіс

Максимальна кількість одночасних задач: 3 – це означає, що атака виконується в трьох потоках. Загальна кількість спроб 14 344 399 – стільки можливих комбінацій логінів і паролів міститься у вибраному словнику. 4 781 467 спроб на задачу – розподіл навантаження між потоками.

Hydra намагається підібрати пароль для користувача admin, використовуючи кожен рядок зі словника rockyou.txt, а також порожній пароль. Якщо в процесі атаки буде знайдено коректні облікові дані, програма виведе повідомлення із зазначенням правильного логіна і пароля.

DDoS-атака типу SYN Flood [29] та UDP Flood [30] спрямована на перевантаження цільового сервера великою кількістю запитів, що може спричинити його недоступність. SYN Flood використовує підроблені запити для встановлення TCP-з'єднань, а UDP Flood генерує великий обсяг UDP-пакетів, що перевантажує сервер.

SYN Flood використовує підроблені запити на встановлення TCP-з'єднань, які сервер обробляє, залишаючи ресурси зайнятими очікуванням підтвердження, що призводить до вичерпання ресурсів [31].

На рисунку 3.4 показано запуск SYN Flood атаки на веб-сервер Ubuntu Linux з Parrot Security за допомогою утиліти hping3.

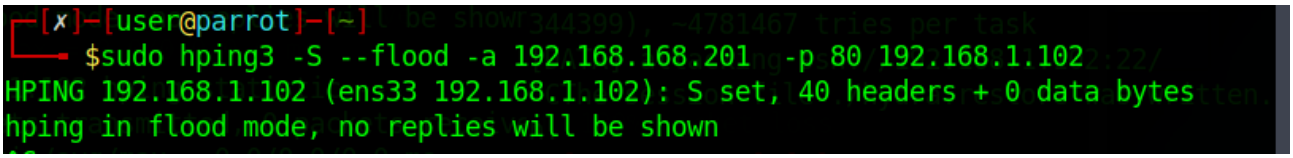


Рисунок 3.4 – Виконання SYN Flood атаки на веб-сервер

Параметри запуску:

– `-S` – використовується SYN-флаг для створення підроблених запитів на встановлення TCP-з'єднань;

– `--flood` – відправляє запити без пауз, генерує потік трафіку на максимальній швидкості, створюючи перевантаження цільового сервера;
– `-a 192.168.168.201` – використовується IP Spoofing (підробка вихідної IP-адреси), що ускладнює виявлення реального джерела атаки;
– `-p 80` – атака спрямована на порт 80, який відповідає за HTTP-запити;
– `192.168.1.102` – IP-адреса цільового сервера Ubuntu Linux.

При тестування було запущено одночасно чотири сесії hping3, які надсилали SYN-пакети від імені підроблених IP-адрес (192.168.168.201, 192.168.168.202, 192.168.168.203, 192.168.168.204), використовуючи IP Spoofing.

Ця атака є ефективним тестом на стійкість сервера до DDoS-атак [32] і дозволяє перевірити роботу систем IPS Snort що до виявлення аномального трафіку.

UDP Flood генерує величезний потік UDP-пакетів на цільовий сервер, змушуючи його обробляти запити, що навантажує мережу та ресурси сервера [33].

На рисунку 3.5 показано виконання UDP Flood-атаки на DNS-сервер Ubuntu Linux за допомогою утиліти hping3.

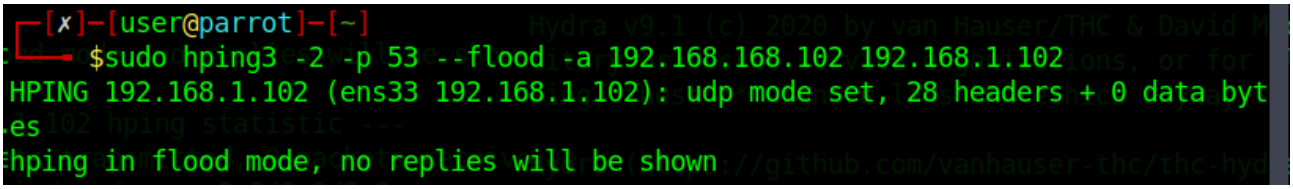


Рисунок 3.5 – Виконання UDP Flood атаки на DNS-сервер

Параметри запуску:

– `-2` – вказує, що атака здійснюється за допомогою UDP;
– `-p 53` – вказує порт 53, який використовується DNS-серверами для обробки запитів;

– `--flood` – надсилає пакети у режимі максимальної швидкості, без очікування відповіді від сервера, що викликає перевантаження;
– `-a 192.168.168.102` – використовується IP Spoofing (підробка вихідної IP-адреси), що ускладнює ідентифікацію джерела атаки;
– `192.168.1.102` – цільова IP-адреса Ubuntu Linux, на яку спрямовується атака.

UDP Flood-атака на DNS є ефективним способом перевантаження сервера, що може зробити його недоступним для легітимних користувачів. При тестування було запущено одночасно чотири сесії hping3, які надсилали UDP-пакети від імені підроблених IP-адрес (192.168.168.101, 192.168.168.102, 192.168.168.103, 192.168.168.104), використовуючи IP Spoofing. Використання hping3 дозволяє імітувати реальні атаки, які можуть бути виявлені за допомогою систем IPS Snort.

3.1.4 Оцінка ефективності IPS Snort

Після запуску атак проводилась оцінка ефективності Snort. Аналізувалось чи були атаки успішно виявлені та заблоковані за допомогою IPS.

На рисунку 3.6 відображено журнал подій системи IPS Snort, яка зафіксувала атаку brute force на SSH. Виявлена подія свідчить про спробу підбору паролів до сервера Ubuntu Linux через порт 22.

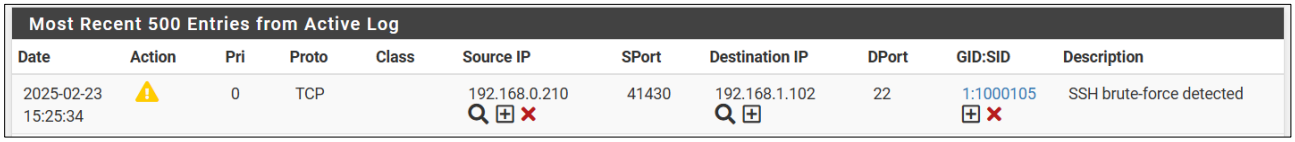
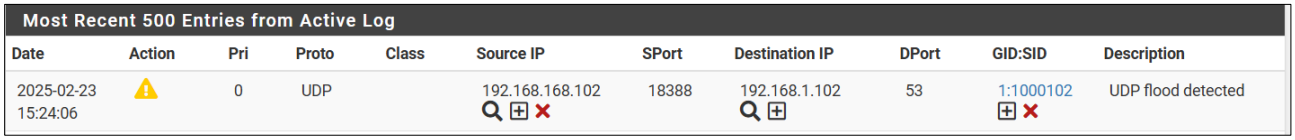


Рисунок 3.6 – Виявлена brute force атака на SSH

Цей запис підтверджує, що IPS Snort ефективно розпізнав атаку та зафіксувала підозрілу активність.

На рисунку 3.7 представлений журнал подій IPS Snort, який зафіксував атаку UDP Flood на DNS-сервер Ubuntu Linux.



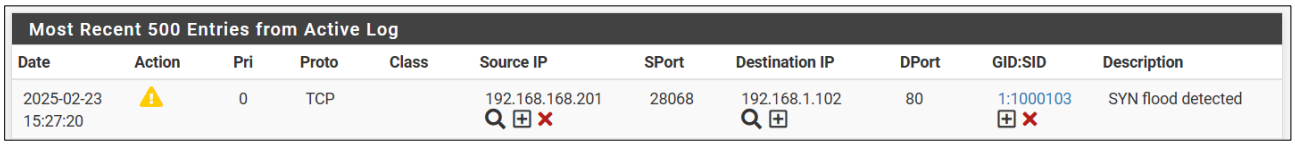
Most Recent 500 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-02-23 15:24:06	⚠	0	UDP		192.168.168.102	18388	192.168.1.102	53	1:1000102	UDP flood detected

Рисунок 3.7 – Виявлена UDP Flood атака на DNS-сервер

Цей запис демонструє ефективність Snort у виявленні DDoS-атак типу UDP Flood,

На рисунку 3.8 представлений журнал подій системи IPS Snort, який зафіксував атаку SYN Flood на веб-сервер Ubuntu Linux.



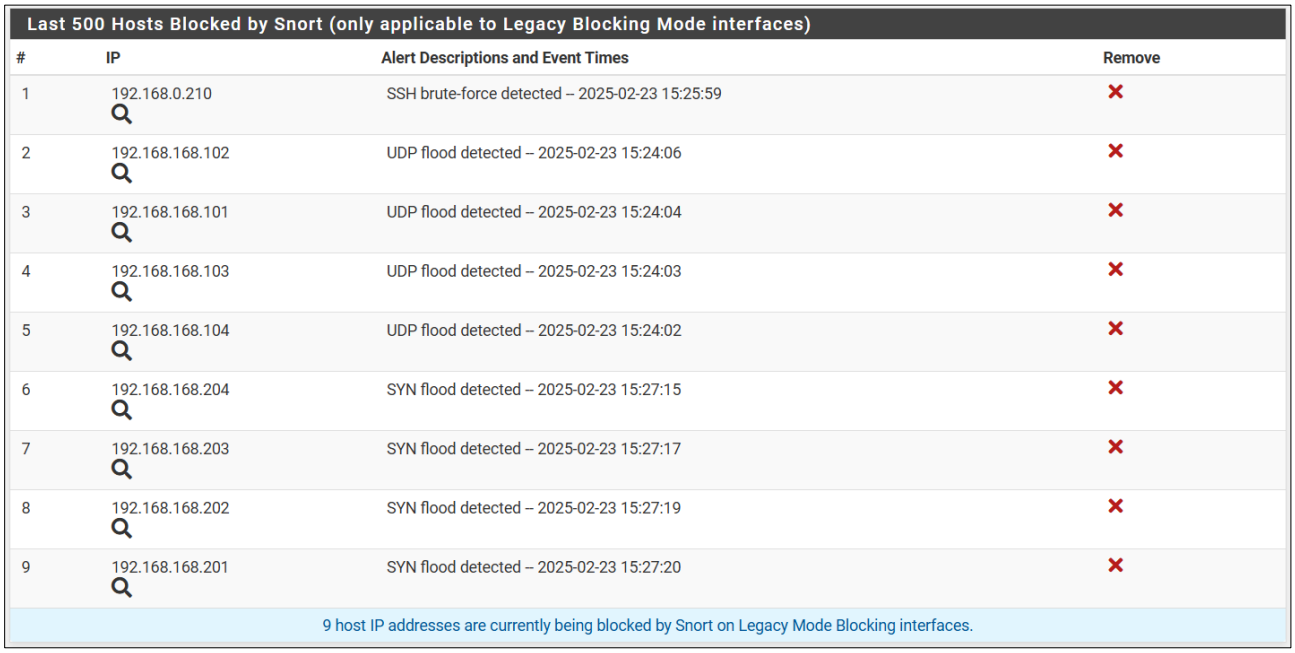
Most Recent 500 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-02-23 15:27:20	⚠	0	TCP		192.168.168.201	28068	192.168.1.102	80	1:1000103	SYN flood detected

Рисунок 3.8 – Виявлена SYN Flood атака на веб-сервер

Цей запис демонструє ефективність Snort у виявленні атак SYN Flood.

На рисунку 3.9 представлений інтерфейс pfSense Snort, що відображає список заблокованих IP-адрес, які були виявлені як зловмисні та внесені до блоку IPS Snort. Система не тільки виявляє загрози, але й автоматично блокує атакуючі IP-адреси.



Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	192.168.0.210	SSH brute-force detected – 2025-02-23 15:25:59	✕
2	192.168.168.102	UDP flood detected – 2025-02-23 15:24:06	✕
3	192.168.168.101	UDP flood detected – 2025-02-23 15:24:04	✕
4	192.168.168.103	UDP flood detected – 2025-02-23 15:24:03	✕
5	192.168.168.104	UDP flood detected – 2025-02-23 15:24:02	✕
6	192.168.168.204	SYN flood detected – 2025-02-23 15:27:15	✕
7	192.168.168.203	SYN flood detected – 2025-02-23 15:27:17	✕
8	192.168.168.202	SYN flood detected – 2025-02-23 15:27:19	✕
9	192.168.168.201	SYN flood detected – 2025-02-23 15:27:20	✕

9 host IP addresses are currently being blocked by Snort on Legacy Mode Blocking interfaces.

Рисунок 3.9 – Список заблокованих IP-адрес

У pfSense система IPS Snort працює у взаємодії з брандмауером PF для автоматичного блокування IP-адрес, що виявлені як потенційно шкідливі. При виявленні аномальної поведінки Snort автоматично передає виявлені IP-адреси в PF для блокування.

При спрацьовуванні правила Snort надсилає відповідне повідомлення в брандмауер PF, який заносить IP-адресу в таблицю snort2c (див. рисунок 3.10).

```
[2.7.2-RELEASE][root@ips1.test.env.local]/root: pfctl -v -t snort2c -T show
   192.168.0.210
        Cleared:     Sun Feb 23 15:25:35 2025
   192.168.168.101
        Cleared:     Sun Feb 23 15:23:39 2025
   192.168.168.102
        Cleared:     Sun Feb 23 15:23:37 2025
   192.168.168.103
        Cleared:     Sun Feb 23 15:23:40 2025
   192.168.168.104
        Cleared:     Sun Feb 23 15:23:42 2025
   192.168.168.201
        Cleared:     Sun Feb 23 15:26:55 2025
   192.168.168.202
        Cleared:     Sun Feb 23 15:26:47 2025
   192.168.168.203
        Cleared:     Sun Feb 23 15:26:39 2025
   192.168.168.204
        Cleared:     Sun Feb 23 15:26:31 2025
[2.7.2-RELEASE][root@ips1.test.env.local]/root:
```

Рисунок 3.10 – Вміст таблиці snort2c в PF

Це дозволяє миттєво блокувати підозрілий трафік і запобігати подальшій шкідливій активності з цього джерела. PF діє як міжмережевий екран, контролюючи всі підключення і застосовуючи політики блокування, які можуть бути налаштовані користувачем. Ця взаємодія забезпечує ефективний механізм захисту від атак шляхом автоматичного блокування зловмисного трафіку, використовуючи комбіновану функціональність Snort як системи виявлення та PF як механізму реалізації правил блокування.

Система IPS Snort ефективно блокує загрози у реальному часі, забезпечуючи захист сервісів від атак.

3.2 Сценарій 2: Тестування OPNsense та Suricata в режимі IDS

3.2.1 Схема сценарію

Сценарій 2 передбачає тестування системи OPNsense з Suricata у режимі IDS. Архітектура середовища складається з Windows Server 2022 як цільової системи, Kali Linux як атакуючої машини, та OPNsense з Suricata як засобу моніторингу та виявлення загроз. Віртуальне середовище побудоване на основі віртуальних комутаторів, що розділяють мережу на внутрішній та зовнішній сегменти (див. рисунок 3.11).

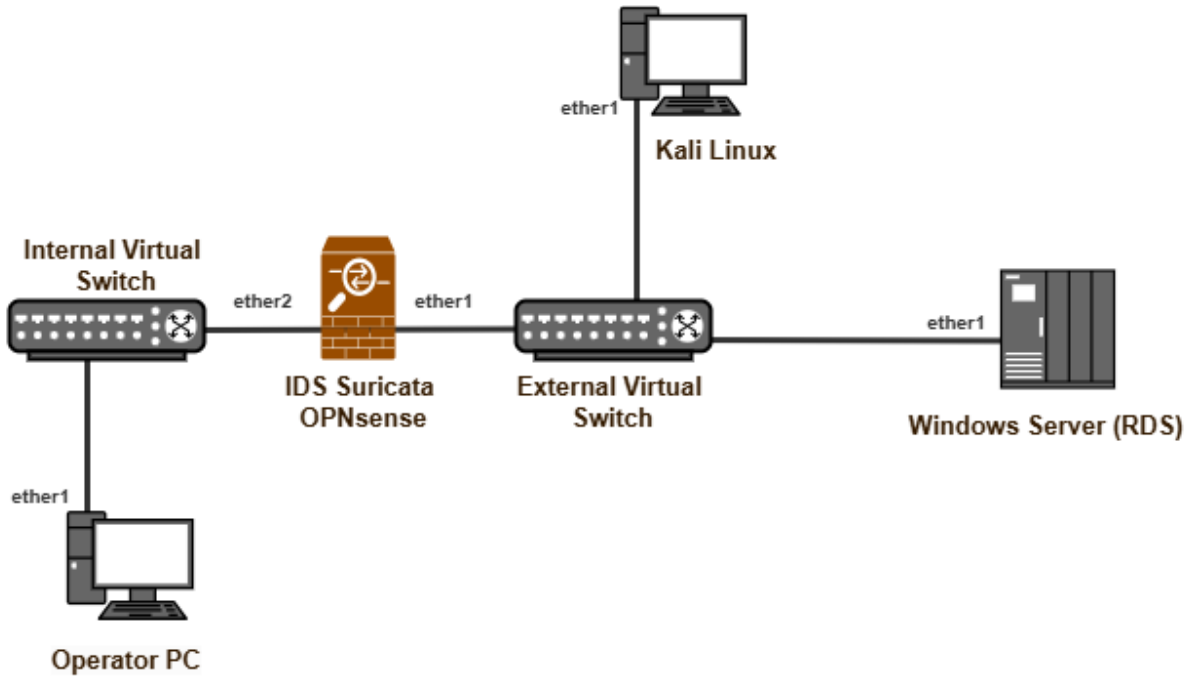


Рисунок 3.11 – Схема сценарію 2

Windows Server 2022 надає служби віддаленого робочого столу (RDS), що є частою ціллю атак, таких як brute-force на RDP. Kali Linux використовується для імітації атак, які включають сканування портів та підбір паролів до RDP-сервісу,.

OPNsense із Suricata працює у режимі IDS, що означає, що вона моніторить весь мережевий трафік, аналізує пакети відповідно правил, але не блокує підозрілі пакети автоматично. Це дозволяє тестувати ефективність виявлення атак без активного втручання у мережевий трафік. Suricata налаштована на прослуховування зовнішнього мережевого інтерфейсу, що з'єднаний із комутатором, через який проходять атаки. Вона використовує базу правил Emerging Threats, що містить правила для виявлення атаки на RDP, DoS-атак, сканування портів та експлуатації вразливостей Windows.

У таблиці 3.2 наведені мережеві налаштування пристроїв, що беруть участь у сценарії тестування OPNsense із Suricata у режимі IDS.

Таблиця 3.2 – Мережеві налаштування сценарію 2

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Шлюз

OPNsense	ether1	192.168.0.160	255.255.255.0	192.168.0.1
	ether2	192.168.1.1	255.255.255.0	
Kali Linux	ether1	192.168.0.205	255.255.255.0	192.168.0.1
Windows Server 2022	ether1	192.168.0.207	255.255.255.0	192.168.0.1
Operator PC	ether1	192.168.1.112	255.255.255.0	192.168.1.1

У сценарії 2 тестування OPNsense та Suricata в режимі IDS виконується у середовищі з наступними мережевими налаштуваннями.

Маршрутизатор OPNsense має два мережеві інтерфейси. Інтерфейс ether1 підключений до зовнішнього віртуального комутатора, і ether2, підключений до внутрішнього віртуального комутатора. Він виконує роль шлюза та системи аналізу трафіку.

Kali Linux підключений до зовнішнього комутатора через інтерфейс ether1, що дозволяє йому здійснювати атаки на Windows Server 2022. Його трафік аналізується Suricata. Це забезпечує можливість відстеження атак та аналізу потенційних загроз.

Windows Server 2022 розміщений у тій самій зовнішній мережі, що і Kali Linux. Він імітує сервер, що надає RDP-доступ, який є ціллю для сканування портів та brute-force.

Operator PC розташований у внутрішній мережі та підключений до OPNsense через ether2. Він використовується для перегляду журналів Suricata та адміністрування OPNsense.

Ця конфігурація дозволяє OPNsense із Suricata працювати у режимі IDS, перехоплювати та аналізувати трафік між атакуючим Kali Linux і ціллю Windows Server 2022. Сценарій 2 демонструє можливості OPNsense та Suricata у моніторингу мережевого трафіку, аналізі атак та виявленні загроз без втручання у роботу мережевих пристроїв. Використання Suricata у режимі IDS дозволяє налаштувати детальний аналіз атак перед переходом у режим IPS.

3.2.2 Сканування відкритих портів Windows Server 2022

Під час тестування проводилось сканування відкритих портів Windows Server з Kali Linux за допомогою Nmap, що дозволяє перевірити, чи Suricata виявляє підозрілу активність.

На рисунку 3.12 показано результати сканування відкритих портів Windows Server 2022 за допомогою утиліти Nmap з Kali Linux.

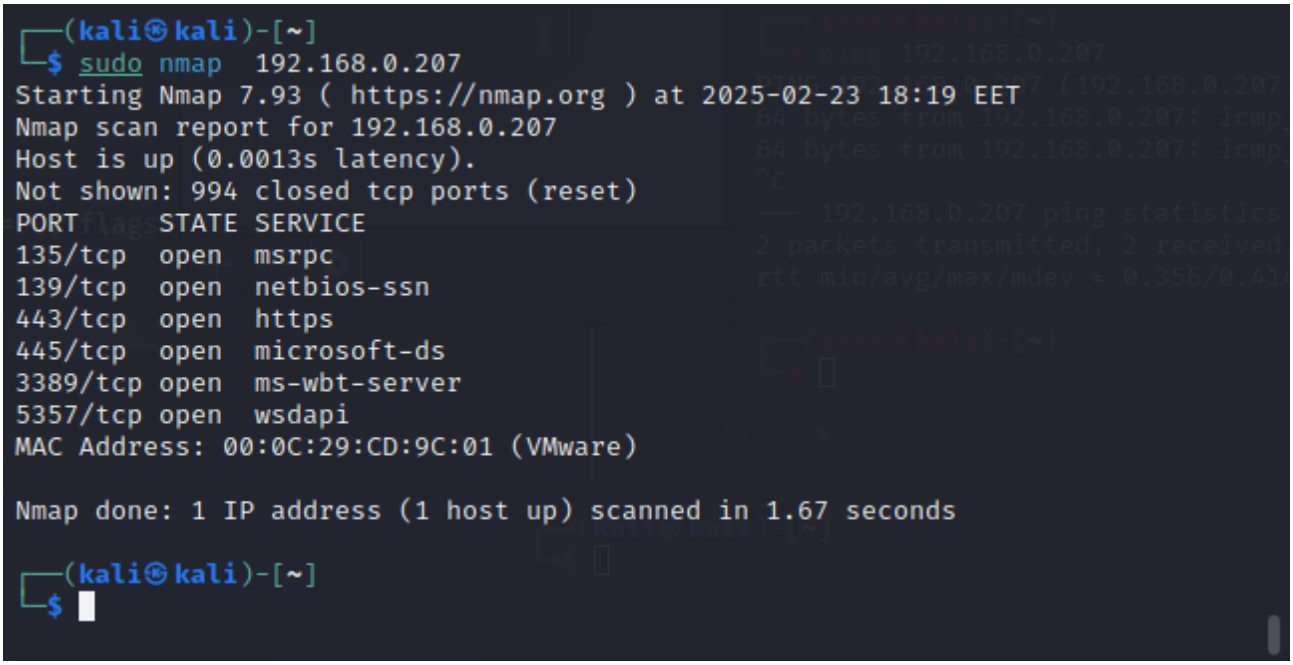


Рисунок 3.12 – Результати сканування відкритих портів Windows Server 2022

Це сканування дозволяє атакуючому визначити відкриті порти та запущені сервіси, що буде використано для подальшого brute force атаки на RDP. В додатку А представлено результати розширеного сканування відкритих TCP та UDP портів.

3.2.3 Здійснення brute force атаки на RDS

Brute force атака на RDS сервіс Windows Server 2022 виконується з Kali Linux за допомогою утиліти Hydra (див. рисунок 3.13). Ця атака передбачає автоматичний перебір облікових даних, намагаючись знайти правильний логін

та пароль для підключення до RDS, який працює на порту 3389/tcp по протоколу RDP.

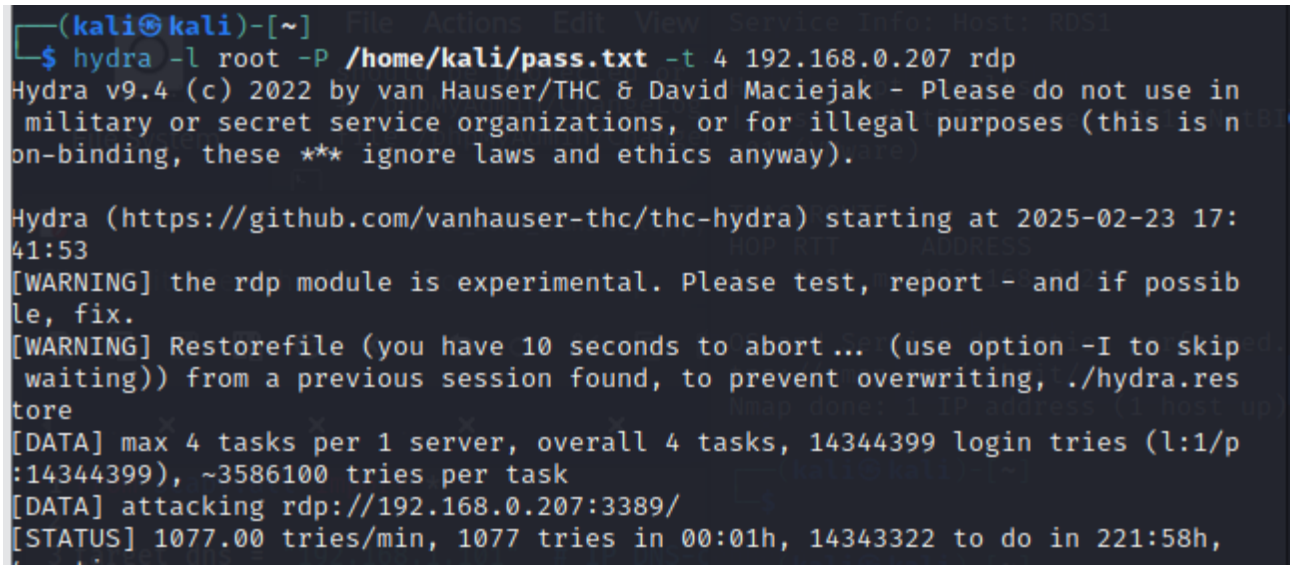


Рисунок 3.13 – Виконання brute force атаки на RDS сервіс

Brute force атаки на RDP є поширеним методом злому серверів, особливо у випадках використання слабких паролів. Такі атаки можуть бути виявлені через IDS Suricata на OPNsense, яка фіксує підозрілу активність, таку як висока кількість невдалих спроб авторизації.

3.2.4 Оцінка ефективності IDS Suricata

Suricata у режимі IDS реєструє виявлені загрози у журналах OPNsense, надаючи детальну інформацію про IP-адреси джерела і цілі атаки, тип загрози та відповідне правило сигнатури. Це дозволяє аналізувати атаки та визначати ефективність виявлення.

На рисунку 3.14 представлено журнал сповіщень IDS Suricata при виявленні сканування портів.

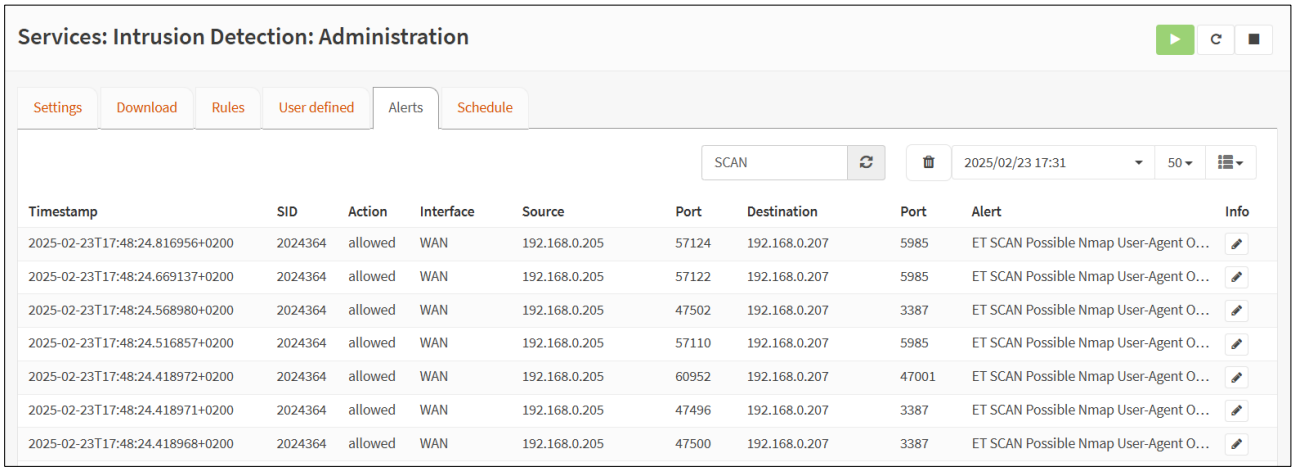


Рисунок 3.14 – Журнал сповіщень IDS Suricata при виявленні сканування портів

Suricata зафіксувала використання Nmap, що вказує на збір інформації про відкриті порти та запущені сервіси на сервері. Журнал реєструє деталі кожного інциденту, включаючи час події, унікальний ідентифікатор правила, тип протоколу, вихідний і цільовий порти, а також статус дії. Всі ці події мають статус allowed, що означає, що система IDS лише зафіксувала їх, але не блокувала з’єднання.

На зображенні відображено журнал сповіщень у веб-інтерфейсі OPNsense, який містить інформацію про виявлені підозрілі дії системою виявлення вторгнень Suricata.

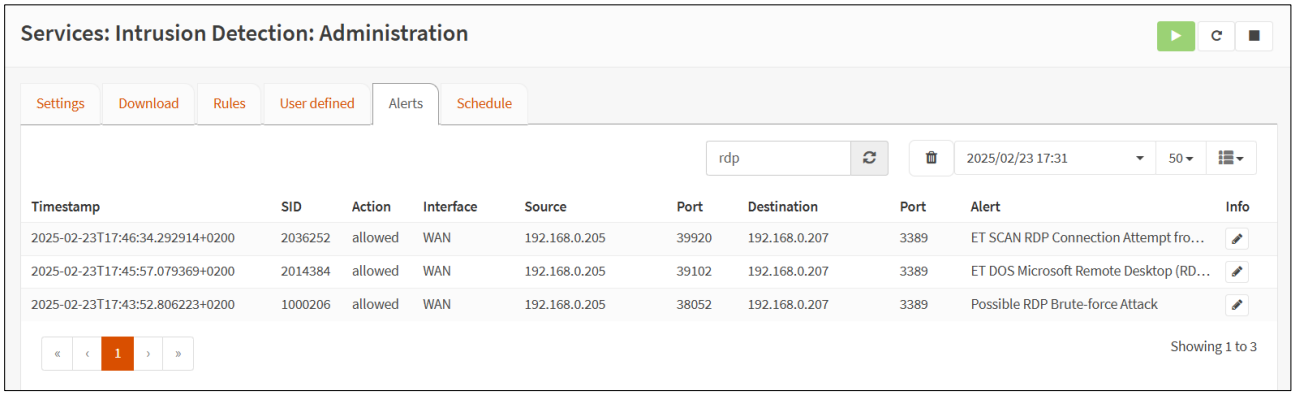


Рисунок 3.15 – Журнал сповіщень IDS Suricata при виявленні brute force атаки на RDS сервіс

Джерелом усіх сповіщень є IP-адреса 192.168.0.205, яка належить Kali Linux, що використовується для тестування. Цільовий сервер з IP-адресою 192.168.0.207 є Windows Server 2022, який обробляє підключення до порту 3389, що використовується для доступу до RDS. У журналі відображаються три типи подій, які сигналізують про можливі атаки. Перша подія містить повідомлення "ET SCAN RDP Connection Attempt", що вказує на те, що Suricata зафіксувала спробу встановлення з'єднання через RDP, яка може бути частиною збору інформації перед подальшими атаками. Друга подія позначена як "ET DOS Microsoft Remote Desktop", що свідчить про можливу атаку типу DoS на службу RDP спричинену інтенсивним перебором паролів. Третя подія з міткою "Possible RDP Brute-force Attack" вказує на можливу атаку методом перебору паролів.

Фіксація цих подій у режимі IDS дозволяє адміністраторам аналізувати активність у мережі та своєчасно реагувати на потенційні загрози [34].

3.3 Висновки до третього розділу

В третьому розділі було проведено тестування та оцінку ефективності тренувального середовища для навчання роботи з IDS/IPS на базі віртуалізованої інфраструктури. Було розглянуто два основні сценарії: тестування pfSense із Snort у режимі IPS та тестування OPNsense із Suricata у режимі IDS. Для перевірки ефективності роботи систем захисту було здійснено моделювання атак, таких як сканування портів, brute force, SYN Flood, UDP Flood.

У першому сценарії pfSense з IPS Snort працював у режимі активного запобігання вторгненням, що дозволило не лише виявляти загрози, а й блокувати атакуючі IP-адреси. У ролі атакуючого вузла використовувався Parrot Security. Проведене сканування портів цільового сервера Ubuntu Linux дозволило визначити активні сервіси, які стали об’єктом атак. Використання інструментів Hydra та hping3 дозволило змоделювати brute force атаку на SSH та DDoS-атаки на HTTP і DNS сервіси. Аналіз журналів подій у Snort показав,

що всі атаки були виявлені та ідентифіковані, а IP-адреси зловмисників автоматично заблоковані через механізм інтеграції з брандмауером PF у pfSense. Це підтвердило ефективність Snort у запобіганні несанкціонованому доступу та атакам на мережеві сервіси.

У другому сценарії було протестовано OPNsense із Suricata у режимі IDS, де система працювала виключно в режимі виявлення загроз без активного блокування атак. У ролі атакуючого вузла використовувався Kali Linux. Було проведено сканування відкритих портів та brute force атаку на RDP сервіс Windows Server 2022. Аналіз журналів Suricata показав, що всі зловмисні дії були зафіксовані та класифіковані як підозрілі, включаючи сканування портів, підбір паролів та потенційні DoS-атаки на RDP. Це підтвердило здатність Suricata до ефективного моніторингу мережевого трафіку та виявлення аномальної активності.

Оцінка ефективності Snort та Suricata показала, що обидві системи здатні ефективно виявляти мережеві атаки. Snort у режимі IPS забезпечує не лише фіксацію загроз, а й активний захист, що запобігає подальшій активності зловмисників. Suricata у режимі IDS дозволяє адміністратору отримувати детальну інформацію про можливі загрози без внесення змін у трафік, що є корисним для аналізу безпеки перед впровадженням автоматичних механізмів блокування.

Тренувальне середовище довело свою ефективність у навчальних цілях, дозволяючи моделювати реальні кібератаки, досліджувати роботу IDS/IPS та відпрацьовувати методи реагування на загрози. Завдяки використанню віртуальних платформ та відкритого програмного забезпечення середовище є масштабованим та придатним для навчання та тестування безпеки в корпоративних і дослідницьких мережах.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при ураженні електричним струмом

Українське законодавство містить низку положень, що регулюють питання долікарської допомоги при ураженні електричним струмом.

Зокрема, Закон України "Про охорону праці" від 14.10.1992 № 2694-XII зобов'язує роботодавців забезпечувати безпеку та охорону праці працівників, в тому числі і при роботі з електроустановками. Роботодавець має забезпечити належний стан та регулярну перевірку електроустановок, використовувати електрообладнання, яке відповідає вимогам безпеки та має сертифікат відповідності [35].

Для забезпечення безпеки під час роботи з ПК, на робочому місці повинні бути встановлені заходи технічного захисту від електричного струму. Закон України "Про охорону праці" встановлює вимоги щодо надання працівникам інструктажу з охорони праці та безпеки під час роботи з електроустановками.

У випадку, коли в результаті ураження електричним струмом настала смерть або тілесні ушкодження потерпілого, винна особа може бути притягнута до кримінальної відповідальності відповідно до Кримінального кодексу України.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання долікарської допомоги особам при невідкладних станах, в тому числі у разі ураження електричним струмом [36].

Отже, у випадку ураження електричним струмом, долікарська допомога має невідкладний характер та повинна надаватися на місці події.

Ось послідовність дій, які потрібно виконати:

– припинити контакт з джерелом струму (для цього можна вимкнути лінію живлення, виключити пристрій, що спричиняє ураження або

від'єднати жертву від джерела струму за допомогою ізольованого предмета (наприклад, дерев'яної палиці, резинової шини));

- перед наданням допомоги переконатися у відсутності небезпеки для себе, оточуючих, постраждалого та тільки за її відсутності перейти до наступного кроку;
- якщо постраждалий у свідомості, заспокоїти та пояснити свої наступні дії;
- здійснити виклик екстреної медичної допомоги та дотримуватись вказівок диспетчера прийому виклику;
- забезпечити постійний нагляд за постраждалим до приїзду бригади екстреної (швидкої) медичної допомоги;
- при погіршенні стану постраждалого до приїзду бригади екстреної (швидкої) медичної допомоги повторно здійснити виклик екстреної медичної допомоги;
- за можливості зібрати у постраждалого чи оточуючих максимально можливу інформацію стосовно обставин отримання травми;
- всю отриману інформацію передати працівникам бригади екстреної (швидкої) медичної допомоги або диспетчеру служби екстреної медичної допомоги;
- якщо до приїзду бригади екстреної (швидкої) медичної допомоги постраждалий втратив свідомість, слід перейти до Порядку надання домедичної допомоги дорослим при раптовій зупинці кровообігу або Порядку надання домедичної допомоги дітям при раптовій зупинці кровообігу, затверджених наказом Міністерства охорони здоров’я України від 09 березня 2022 року № 441.

Потерпілий може мати різні види ушкоджень: від легких опіків до серйозних травм та порушень функцій внутрішніх органів. Необхідність подальшого лікування та реабілітації залежить від ступеня тяжкості ушкодження.

Отже, долікарська допомога при ураженні електричним струмом має важливе значення для збереження життя та здоров'я потерпілого. Важливо

дотримуватися вимог законодавства та правил безпеки праці при роботі з електричними установками, щоб запобігти подібним випадкам та забезпечити безпеку праці на виробництві.

4.2 Вимоги до профілактичних медичних оглядів для працівників ПК

Працівники, які використовують у своїй роботі персональні комп'ютери, підлягають обов'язковим медичним оглядам. Але водночас згідно з роз'ясненням МОЗ від 20.01.2006 р. № 05.0101-18-58/21 проведення обов'язкових медоглядів поширюється на роботу з комп'ютерами на основі електронно-променевих трубок та не поширюється на роботу з рідкокристалічними терміналами.

У сучасних умовах важко знайти галузь економіки, де б не використовувалися комп'ютери. Бюджетні організації не є винятком, адже в них за комп'ютерами працюють бухгалтери, секретарі, економісти, юристи, оператори комп'ютерного набору тощо.

Обов'язковість проведення медичних оглядів для працівників, які працюють за електронно-обчислювальними машинами, передбачена розд. 6 Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 р. № 7 (далі — ДСанПіН № 7).

Так, працюючі з візуальними дисплейними терміналами (ВДТ) електронно- обчислювальних машин (ЕОМ) колективного використання та персональних ЕОМ (ПЕОМ) підлягають обов'язковим медичним оглядам: попереднім — при влаштуванні на роботу і періодичним — протягом трудової діяльності (п. 6.1 розд. 6 ДСанПіН № 7).

Такі медичні огляди проводяться відповідно до вимог Порядку проведення медичних оглядів працівників певних категорій, затвердженого наказом МОЗ від 21.05.2007 р. № 246 (далі — Порядок № 246).

Періодичні медичні огляди мають проводитися раз на два роки комісією в складі терапевта, невропатолога та офтальмолога.

До складу комісії, що проводить попередні та періодичні медичні огляди, при необхідності (за наявності медичних показань) можуть залучати лікарів інших спеціальностей.

Основними критеріями оцінки придатності до роботи з ВДТ ЕОМ і ПЕОМ мають бути показники стану органів зору: гострота зору, показники рефракції, акомодації, стану бінокулярного апарату ока тощо [37]. При цьому також враховується стан організму в цілому.

У розд. 6 ДСанПіН № 7 передбачено й протипоказання для роботи за комп'ютерами. До них відносять усі хронічні форми психічних захворювань, ендокринні захворювання, тяжкий ступінь бронхіальної системи, гіпертонічна хвороба III стадії та інші захворювання.

До відома зазначимо, що монітор або дисплей — це електронний пристрій для відображення інформації. Комп'ютерні монітори бувають кількох типів:

- на основі електронно-променевої трубки(CRT);
- рідкокристалічні(LCD, TFT як підвид LCD);
- плазмові;
- проекційні;
- OLED-монітори.

Плазмові і проекційні монітори використовують там, де потрібен великий розмір екрану (діагональ метр і більше).

На питання чи необхідно проходити обов'язкові медогляди працівникам, які працюють за більш сучасними «тонкими» моніторами було надано роз'яснення заступника Головного державного санітарного лікаря України в листі від 20.01.2006 р. № 05.01.01-18-58/21. У цьому листі зазначено, що ДСанПіН № 7 поширюються на ВДТ усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок, тому вимога щодо проведення попередніх та періодичних медичних оглядів на працюючих з рідкокристалічними відеотерміналами ЕОМ машин у цьому випадку не діє.

Нагадаємо деякі правила проведення обов'язкових медоглядів.

Як уже було зазначено вище, працівники, які працюють за комп'ютерами, підлягають обов'язковим попередньому та періодичним медоглядам.

Попередній медичний огляд проводиться під час прийняття на роботу з метою:

- визначення стану здоров'я працівника і реєстрації вихідних об'єктивних показників здоров'я та можливості виконання без погіршення стану здоров'я про- фесійних обов'язків в умовах дії конкретних шкідливих та небезпечних факторів виробничого середовища і трудового процесу;
- виявлення професійних захворювань (отруєнь), що виникли раніше при роботі на попередніх виробництвах, та попередження виробничо зумовлених і професійних захворювань (отруєнь).

Періодичні медичні огляди проводяться з метою:

- своєчасного виявлення ранніх ознак гострих і хронічних професійних захворювань (отруєнь), загальних та виробничо зумовлених захворювань у працівників;
- забезпечення динамічного спостереження за станом здоров'я працівників в умовах дії шкідливих та небезпечних виробничих факторів і трудового процесу;
- вирішення питання щодо можливості працівника продовжувати роботу в умовах дії конкретних шкідливих та небезпечних виробничих факторів і трудового процесу;
- розробки індивідуальних та групових лікувально-профілактичних та реабілітаційних заходів працівникам, що віднесені за результатами медичного огляду до групи ризику;
- проведення відповідних оздоровчих заходів.

Заклади державної санітарно-епідеміологічної служби щорічно за заявкою роботодавця (його представника), за участю представника первинної профспілкової організації або уповноваженої працівниками особи, визначають категорії працівників, які підлягають попередньому (періодичним) медичному огляду та до 1 грудня складають Акт визначення категорій працівників, які

підлягають попередньому (періодичним) медичному огляду за формою, зазначеною у додатку 1 до Порядку № 246.

Потім на підставі зазначеного Акта роботодавець складає протягом місяця у чотирьох примірниках поіменні списки працівників, які підлягають періодичним медичним оглядам. Форма таких списків наведена у додатку 2 до Порядку № 246.

Ці списки на паперовому та електронному носіях узгоджують у санітарно-епідеміологічній станції. Один примірник списку залишається на підприємстві (у відповідальної за організацію медогляду посадової особи), другий надсилається до закладу охорони здоров'я, третій — до закладу державної санітарно- епідеміологічної служби, четвертий — до робочого органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Отже, як видно, списки працівників, які мають пройти медогляди, надаються та узгоджуються з санепідслужбою.

Для проведення попереднього (періодичних) медичного огляду працівників роботодавець повинен укласти або вчасно поновити договір із закладом охорони здоров'я та надати йому список працівників, які підлягають попередньому (періодичним) медичному огляду.

Питання придатності до роботи в кожному окремому випадку вирішується індивідуально з урахуванням особливостей функціонального стану організму (характеру, ступеня прояву патологічного процесу, наявності хронічних захворювань), умов праці та результатів додаткових методів обстеження.

При цьому кожен лікар, який бере участь в обстеженні пацієнта, дає висновок щодо стану здоров'я працівника, підтверджує його особистим підписом та особистою печаткою, бере участь в остаточному обговоренні придатності обстежуваної особи до роботи в обраній професії та в разі необхідності визначає лікувально-оздоровчі заходи.

За результатами періодичних медичних оглядів (протягом місяця після їх закінчення) комісія з проведення медичних оглядів закладів охорони здоров'я оформляє Заключний акт за результатами періодичного медичного огляду

працівників. Форма цього акта наведена у додатку 9 до Порядку № 246 (ср. 025069200). Такий акт складається у шести примірниках — один примірник залишається в закладі охорони здоров'я, що проводив медогляд, інші надаються роботодавцю, представнику профспілкової організації або вповноваженій працівниками особі, профпатологу, закладу державної санітарно-епідеміологічної служби, робочому органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Також зазначимо, що роботодавець зберігає за працівником на період проходження медогляду місце роботи (посаду) і середній заробіток та за результатами медичного огляду інформує працівника про можливість (неможливість) продовжувати роботу за професією (п. 2.21 Порядку № 246).

Наприкінці також звернемо вашу увагу на те, що право на додаткову відпустку за роботу на комп'ютері мають усі працівники, незалежно від того, за якими моніторами вони працюють.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було розроблено та протестовано тренувальне середовище для навчання роботи з IDS/IPS, що ґрунтується на використанні гіпервізора VMware ESXi, віртуалізованих маршрутизаторів OPNsense і pfSense, а також операційних систем Kali Linux, Parrot Security, Ubuntu Linux, Windows Server 2022 та інших. У результаті виконаних досліджень та експериментів можна сформулювати такі висновки:

1) Розроблено архітектуру та структуру тренувального середовища, що імітує реальні мережеві умови: побудовано дві мережі (зовнішню та внутрішню), налаштовано сегментацію трафіку, розгорнуто різні операційні системи й інструменти для моніторингу, аналізу та моделювання кібератак.
2) Аргументовано використання гіпервізора VMware ESXi у поєднанні з відкритим програмним забезпеченням, таким як pfSense, OPNsense, Snort та Suricata. Віртуалізація дозволила швидко розгортати та змінювати конфігурацію середовища, а також створювати безпечні умови для проведення дослідів з реальними методами атак.
3) Проведено порівняльне тестування режимів IDS та IPS. Snort у pfSense продемонстрував ефективне блокування атак (SYN Flood, UDP Flood, brute force на SSH) у режимі IPS, автоматично блокуючи IP-адреси атакуючих. Suricata в OPNsense, налаштована в режимі IDS, успішно виявляла та реєструвала різні типи атак (сканування портів, brute force на RDP), що дозволяє адміністраторам детально проаналізувати загрози перед увімкненням активного блокування.
4) Підтверджено доцільність використання Kali Linux та Parrot Security у ролі атакуючих систем. На практиці перевірено сценарії сканування портів, підбору паролів, DDoS-атак. Ці дистрибутиви містять великий набір інструментів для тестування безпеки, що надало можливість імітувати реальні дії зловмисників.

5) Проведена оцінка ефективності тренувального середовища засвідчила його придатність для навчальних цілей і поглиблення практичних навичок у сфері кібербезпеки. Студенти та фахівці можуть моделювати різноманітні кібератаки, аналізувати роботу IDS/IPS у реальному часі, відпрацьовувати навички реагування й управління інцидентами інформаційної безпеки.

Запропоноване тренувальне середовище є масштабованим та економічно виправданим. Використання безкоштовного або відкритого програмного забезпечення (Snort, Suricata, pfSense, OPNsense) та віртуалізації дає змогу розгортати подібні лабораторії як у навчальних закладах, так і в організаціях без значних фінансових витрат.

Загалом, створене тренувальне середовище продемонструвало можливість моделювання реалістичних сценаріїв кібератак, ефективного виявлення та блокування загроз за допомогою сучасних IDS/IPS-рішень, а також відпрацювання практичних навичок забезпечення мережевої безпеки. Результати дослідження можуть слугувати основою для подальшого вдосконалення системи, зокрема для додавання нових типів атак, інтеграції з SIEM-платформами та реалізації складніших сценаріїв кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is intrusion detection systems (IDS)? How does it work? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

2. What is an intrusion prevention system (IPS)? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

4. What is a ddos attack? Definition, types and how to protect? (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/types-of-ddos-attack-and-measures-protection

5. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

6. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

7. Zenarmor. (n.d.). Host intrusion prevention system (HIPS). protect critical computer system - zenarmor.com. Zenarmor - Agile Service Edge Security. https://www.zenarmor.com/docs/network-security-tutorials/what-is-host-intrusion-prevention-system-hips

8. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

9. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

10. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

11. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

12. Cyber range. (n.d.). Cyberbit. https://www.cyberbit.com/platform/cyber-range/

13. Platform | cybersecurity training platform team readiness. (n.d.). RangeForce Cloud-Based Cyber Range | Cybersecurity Training. https://www.rangeforce.com/platform

14. Cisco: Software, network, and cybersecurity solutions. (n.d.). Cisco. https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf

15. X-Force cyber range | IBM. (n.d.). IBM - United States. https://www.ibm.com/services/xforce-cyber-range

16. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

17. VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/docs/vsphere-esxi-vcenter-server-80-performance-best-practices

18. PfSense documentation | pfsense documentation. (n.d.). Netgate Documentation | Netgate Documentation. https://docs.netgate.com/pfsense/en/latest/

19. Introduction — OPNsense documentation. (n.d.). OPNsense documentation. https://docs.opnsense.org/intro.html

20. Kali docs | kali linux documentation. (n.d.). Kali Linux. https://www.kali.org/docs/

21. ParrotOS documentation | parrotos documentation. (n.d.). Parrot Security. https://parrotsec.org/docs/

22. Windows Server documentation. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/

23. Remote desktop services overview in windows server. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remote-desktop-services-overview

24. Oracle linux - oracle linux. (n.d.). Oracle Help Center. https://docs.oracle.com/en/operating-systems/oracle-linux/

25. FreeBSD documentation portal. (n.d.). FreeBSD Documentation Portal. https://docs.freebsd.org/en/

26. Official ubuntu documentation. (n.d.). Official Ubuntu Documentation. https://help.ubuntu.com/

27. What is a brute force attack? Definition, types & how it works | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/brute-force-attack

28. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.

29. SYN flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

30. UDP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

31. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.

32. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

33. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

34. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

35. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.

36. Деркач, М. В., & Матюк, Д. С. (2020). Застосування модулю GY-521 для орієнтації БПЛА. Вісник Східноукраїнського національного університету імені Володимира Даля, (7 (263)), 24-28.

37. Деркач, М. В., & Матюк, Д. С. (2020). Альтернативний метод для роботи з датчиком MPu-6050 по шині даних I2C. *Вісник НТУ" ХПІ". Серія: Інформатика та моделювання. Харків: НТУ" ХПІ*.

38. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

39. SACHENKO, A. O., et al. Internet of Things for intelligent transport systems.

40. Про охорону праці. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/2694-12#Text

41. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. (n.d.). Офіційний вебпортал парламенту України. https://zakon.rada.gov.ua/laws/show/z0356-22#n769

42. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник / В.С. Стручок, – Тернопіль: ТНТУ ім. І.Пулюя, 2022. – 150 с.

Додаток А Розширені результати сканування відкритих TCP та UDP портів на Windows Server 2022

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -A 192.168.0.207
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-23 17:45 EET
Nmap scan report for 192.168.0.207
Host is up (0.00043s latency).
Not shown: 65515 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
443/tcp   open  ssl/https
| tls-alpn:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Sign in - Windows Admin Center
| ssl-cert: Subject: commonName=WindowsAdminCenterSelfSigned
| Subject Alternative Name: DNS:RDP-Server-CO
| Not valid before: 2025-01-18T17:51:18
|_Not valid after:  2025-03-19T18:01:18
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Connection: close
```

```
|     Date: Sun, 23 Feb 2025 15:46:41 GMT
|     Cache-Control: no-store
|     Cache-Control: max-age=0
|     Pragma: no-cache
|                                                     Set-Cookie:
.AspNetCore.Antiforgery.7Eyhia2WOxE=CfDJ8ODDJcYJKG1Aub8N5wDO2ri-
gcQaQxnSS8CM_Ba4gnvgkiMwWchmtDVRXplJmPqBLzwo0PulrZPqelNN6gNCDbnXYn
8_0RdqTzahR_jXgZ0nSCZ_EmP0auhrFJLDMFPxRl14ucnsx18enKao43E-XLM;
path=/; secure; samesite=none; Partitioned
|        Set-Cookie: WAC-SESSION=ad41bb1f765e491cb393881ae17bdd95;
expires=Mon, 24 Feb 2025 15:46:41 GMT; path=/; secure;
samesite=lax; httponly
|       Set-Cookie: WAC-TOKEN=; expires=Thu, 01 Jan 1970 00:00:00
GMT; path=/
|     Set-Cookie: WAC-AAD=; expires=Thu, 01 Jan 1970 00:00:00 GMT;
path=/
|      Set-Cookie: XSRF-TOKEN=; expires=Thu, 01 Jan 1970 00:00:00
GMT; path=/
|                    Strict-Transport-Security:    max-age=5184000;
includeSubDomains; preload
|     <!DOCTYPE html>
|     <html lang="en" xmlns="http://www.w3.org/1999/xhtml">
|     <head
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Connection: close
|     Date: Sun, 23 Feb 2025 15:46:41 GMT
|     Cache-Control: no-store
|     Cache-Control: max-age=0
```

```
|     Pragma: no-cache
|                                                    Set-Cookie:
.AspNetCore.Antiforgery.7Eyhia2WOxE=CfDJ8ODDJcYJKG1Aub8N5wDO2rioxD
b7t00_OFjnnKHCRKIgeRdEM-xYRwcvLBrgeNw8nbsGGmjGCiil-
N3k2RiFQmkCs7P6Z1hk1w-RjqfYpoBVQwx2jnOJsCj_8HFTRs1Zj8Mpfs-
IGXV5Wf2rxkJGjTM; path=/; secure; samesite=none; Partitioned
|       Set-Cookie: WAC-SESSION=2ed7bf7d93684b1aa8d904574d0e4602;
expires=Mon, 24 Feb 2025 15:46:41 GMT; path=/; secure;
samesite=lax; httponly
|      Set-Cookie: WAC-TOKEN=; expires=Thu, 01 Jan 1970 00:00:00
GMT; path=/
|     Set-Cookie: WAC-AAD=; expires=Thu, 01 Jan 1970 00:00:00 GMT;
path=/
|      Set-Cookie: XSRF-TOKEN=; expires=Thu, 01 Jan 1970 00:00:00
GMT; path=/
|                    Strict-Transport-Security:    max-age=5184000;
includeSubDomains; preload
|     <!DOCTYPE html>
|     <html lang="en" xmlns="http://www.w3.org/1999/xhtml">
|_    <head
445/tcp   open  microsoft-ds?
3387/tcp   open   http                 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
3389/tcp  open  ms-wbt-server    Microsoft Terminal Services
|_ssl-date: 2025-02-23T15:48:27+00:00; -3s from scanner time.
| rdp-ntlm-info:
|   Target_Name: RDS1
|   NetBIOS_Domain_Name: RDS1
```

```
|   NetBIOS_Computer_Name: RDS1
|   DNS_Domain_Name: RDS1
|   DNS_Computer_Name: RDS1
|   Product_Version: 10.0.20348
|_  System_Time: 2025-02-23T15:48:23+00:00
| ssl-cert: Subject: commonName=RDS1
| Not valid before: 2025-02-20T21:35:07
|_Not valid after:  2025-08-22T21:35:07
5357/tcp   open   http                Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp   open   http                Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6601/tcp  open  ssl/mstmg-sstp?
| tls-alpn:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=WindowsAdminCenterSelfSigned
| Subject Alternative Name: DNS:RDP-Server-CO
| Not valid before: 2025-01-18T17:51:18
|_Not valid after:  2025-03-19T18:01:18
| fingerprint-strings:
|   FourOhFourRequest:
```

```
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: application/json;charset=utf-8
|     Date: Sun, 23 Feb 2025 15:47:14 GMT
|                   Strict-Transport-Security:    max-age=5184000;
includeSubDomains; preload
|_    {"name":"Sub service process","status":"Insecure"}
6602/tcp  open  ssl/wsscomfrmwk?
| tls-alpn:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=WindowsAdminCenterSelfSigned
| Subject Alternative Name: DNS:RDP-Server-CO
| Not valid before: 2025-01-18T17:51:18
|_Not valid after:  2025-03-19T18:01:18
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: application/json;charset=utf-8
|     Date: Sun, 23 Feb 2025 15:47:14 GMT
|                   Strict-Transport-Security:    max-age=5184000;
includeSubDomains; preload
|     {"name":"Sub service process","status":"Insecure"}
|   HTTPOptions:
|     HTTP/1.1 200 OK
```

```
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Date: Sun, 23 Feb 2025 15:46:49 GMT
|                   Strict-Transport-Security:    max-age=5184000;
includeSubDomains; preload
|     <!doctype html>
|     <html>
|     <head>
|     <title>Sub service process</title>
|     <base href="/">
|     <meta charset="utf-8">
|     <meta http-equiv="cache-control" content="no-cache" />
|     <meta http-equiv="pragma" content="no-cache" />
|     <meta http-equiv="expires" content="0" />
|      <meta name="viewport" content="width=device-width, initial-
scale=1">
|     </head>
|     <body>
|     service process
|     </body>
|     </html>
|   TLSSessionReq:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|_    Date: Sun, 23 Feb 2025 15:47:04 GMT
```

```
47001/tcp open  http                Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc               Microsoft Windows RPC
49665/tcp open  msrpc               Microsoft Windows RPC
49666/tcp open  msrpc               Microsoft Windows RPC
49667/tcp open  msrpc               Microsoft Windows RPC
49681/tcp open  msrpc               Microsoft Windows RPC
49682/tcp open  msrpc               Microsoft Windows RPC
49684/tcp open  msrpc               Microsoft Windows RPC
49685/tcp open  msrpc               Microsoft Windows RPC
49690/tcp open  msrpc               Microsoft Windows RPC
3 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT        SERVICE        FINGERPRINT        (SUBMIT
INDIVIDUALLY)==============
SF-Port443-TCP:V=7.93%T=SSL%I=7%D=2/23%Time=67BB42E4%P=x86_64-pc-
linux-gnu
SF:%r(GetRequest,5EA0,"HTTP/1\.1\x20403\x20Forbidden\r\nConnection
:\x20clo
SF:se\r\nDate:\x20Sun,\x2023\x20Feb\x202025\x2015:46:41\x20GMT\r\n
Cache-Co
SF:ntrol:\x20no-store\r\nCache-Control:\x20max-
age=0\r\nPragma:\x20no-cach
SF:e\r\nSet-
Cookie:\x20\.AspNetCore\.Antiforgery\.7Eyhia2WOxE=CfDJ8ODDJcYJ
```

SF:KG1Aub8N5wDO2ri-gcQaQxnSS8CM_Ba4gnvgkiMwWchmtDVRXplJmPqBLzwo0PulrZPqelN

SF:N6gNCDbnXYn8_0RdqTzahR_jXgZ0nSCZ_EmP0auhrFJLDMFPxRl14ucnsx18enKao43E-XL

SF:M;\x20path=/;\x20secure;\x20samesite=none;\x20Partitioned\r\nSet-Cookie

SF::\x20WAC-SESSION=ad41bb1f765e491cb393881ae17bdd95;\x20expires=Mon,\x202

SF:4\x20Feb\x202025\x2015:46:41\x20GMT;\x20path=/;\x20secure;\x20samesite=

SF:lax;\x20httponly\r\nSet-Cookie:\x20WAC-TOKEN=;\x20expires=Thu,\x2001\x2

SF:0Jan\x201970\x2000:00:00\x20GMT;\x20path=/\r\nSet-Cookie:\x20WAC-AAD=;\

SF:x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT;\x20path=/\r\nS

SF:et-Cookie:\x20XSRF-TOKEN=;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:0

SF:0:00\x20GMT;\x20path=/\r\nStrict-Transport-Security:\x20max-age=5184000

SF:;\x20includeSubDomains;\x20preload\r\n\r\n<!DOCTYPE\x20html>\r\n<html\x

SF:20lang=\"en\"\x20xmlns=\"http://www\.w3\.org/1999/xhtml\">\r\n\r\n<head

SF:")%r(HTTPOptions,5EA0,"HTTP/1\.1\x20403\x20Forbidden\r\nConnection:\x20

SF:close\r\nDate:\x20Sun,\x2023\x20Feb\x202025\x2015:46:41\x20GMT\r\nCache

SF:-Control:\x20no-store\r\nCache-Control:\x20max-age=0\r\nPragma:\x20no-c

SF:ache\r\nSet-
Cookie:\x20\.AspNetCore\.Antiforgery\.7Eyhia2WOxE=CfDJ8ODDJ

SF:cYJKG1Aub8N5wDO2rioxDb7t00_OFjnnKHCRKIgeRdEM-
xYRwcvLBrgeNw8nbsGGmjGCiil

SF:-N3k2RiFQmkCs7P6Z1hk1w-RjqfYpoBVQwx2jnOJsCj_8HFTRs1Zj8Mpfs-
IGXV5Wf2rxkJ

SF:GjTM;\x20path=/;\x20secure;\x20samesite=none;\x20Partitioned\r\
nSet-Coo

SF:kie:\x20WAC-
SESSION=2ed7bf7d93684b1aa8d904574d0e4602;\x20expires=Mon,\x

SF:2024\x20Feb\x202025\x2015:46:41\x20GMT;\x20path=/;\x20secure;\x
20samesi

SF:te=lax;\x20httponly\r\nSet-Cookie:\x20WAC-
TOKEN=;\x20expires=Thu,\x2001

SF:\x20Jan\x201970\x2000:00:00\x20GMT;\x20path=/\r\nSet-
Cookie:\x20WAC-AAD

SF:=;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT;\x20
path=/\r

SF:\nSet-Cookie:\x20XSRF-
TOKEN=;\x20expires=Thu,\x2001\x20Jan\x201970\x200

SF:0:00:00\x20GMT;\x20path=/\r\nStrict-Transport-Security:\x20max-
age=5184

SF:000;\x20includeSubDomains;\x20preload\r\n\r\n<!DOCTYPE\x20html>
\r\n<htm

SF:l\x20lang=\"en\"\x20xmlns=\"http://www\.w3\.org/1999/xhtml\">\r
\n\r\n<h

SF:ead");

==============NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)==============

SF-Port6601-TCP:V=7.93%T=SSL%I=7%D=2/23%Time=67BB4305%P=x86_64-pc-
linux-gn

SF:u%r(FourOhFourRequest,FC,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnect

SF:ion:\x20close\r\nContent-Type:\x20application/json;charset=utf-8\r\nDat

SF:e:\x20Sun,\x2023\x20Feb\x202025\x2015:47:14\x20GMT\r\nStrict-Transport-

SF:Security:\x20max-age=5184000;\x20includeSubDomains;\x20preload\r\n\r\n{

SF:\"name\":\"Sub\x20service\x20process\",\"status\":\"Insecure\"}");

==========NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==========

SF-Port6602-TCP:V=7.93%T=SSL%I=7%D=2/23%Time=67BB42EC%P=x86_64-pc-linux-gn

SF:u%r(HTTPOptions,25C,"HTTP/1\.1\x20200\x20OK\r\nConnection:\x20close\r\n

SF:Content-Type:\x20text/html;charset=utf-8\r\nDate:\x20Sun,\x2023\x20Feb\

SF:x202025\x2015:46:49\x20GMT\r\nStrict-Transport-Security:\x20max-age=518

SF:4000;\x20includeSubDomains;\x20preload\r\n\r\n<!doctype\x20html>\r\n<ht

SF:ml>\r\n\x20\x20<head>\r\n\x20\x20\x20\x20<title>Sub\x20service\x20proce

SF:ss</title>\r\n\x20\x20\x20\x20<base\x20href=\"/\">\r\n\x20\x20\x20\x20<

SF:meta\x20charset=\"utf-8\">\r\n\x20\x20\x20\x20<meta\x20http-equiv=\"cac

SF:he-control\"\x20content=\"no-cache\"\x20/>\r\n\x20\x20\x20\x20<meta\x20

SF:http-equiv=\"pragma\"\x20content=\"no-
cache\"\x20/>\r\n\x20\x20\x20\x20

SF:<meta\x20http-
equiv=\"expires\"\x20content=\"0\"\x20/>\r\n\x20\x20\x20\

SF:x20<meta\x20name=\"viewport\"\x20content=\"width=device-
width,\x20initi

SF:al-
scale=1\">\r\n\x20\x20</head>\r\n\x20\x20<body>\r\nSub\x20service\
x2

SF:0process\r\n\x20\x20</body>\r\n</html>")%r(TLSSessionReq,67,"HT
TP/1\.1\

SF:x20400\x20Bad\x20Request\r\nContent-
Length:\x200\r\nConnection:\x20clos

SF:e\r\nDate:\x20Sun,\x2023\x20Feb\x202025\x2015:47:04\x20GMT\r\n\
r\n")%r(

SF:FourOhFourRequest,FC,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
nection:

SF:\x20close\r\nContent-Type:\x20application/json;charset=utf-
8\r\nDate:\x

SF:20Sun,\x2023\x20Feb\x202025\x2015:47:14\x20GMT\r\nStrict-
Transport-Secu

SF:rity:\x20max-
age=5184000;\x20includeSubDomains;\x20preload\r\n\r\n{\"na

SF:me\":\"Sub\x20service\x20process\",\"status\":\"Insecure\"}");

MAC Address: 00:0C:29:CD:9C:01 (VMware)

No exact OS matches for host (If you know what OS is running on
it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=2/23%OT=135%CT=1%CU=43536%PV=Y%DS=1%DC=D%G=Y%
M=000C29%

```
OS:TM=67BB434F%P=x86_64-pc-linux-
gnu)SEQ(SP=100%GCD=1%ISR=107%TI=I%CI=I%II=

OS:I%SS=S%TS=A)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O
4=M5B4NW8

OS:ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=
FFFF%W5=F

OS:FFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=
Y%DF=Y%T=

OS:80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%R
D=0%Q=)T3

OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0
%S=A%A=O%

OS:F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6
(R=Y%DF=Y

OS:%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%
F=AR%O=%R

OS:D=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
G%RUD=G)I

OS:E(R=Y%DFI=N%T=80%CD=Z)


Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:

| smb2-security-mode:

|   311:

|_    Message signing enabled but not required

| smb2-time:

|   date: 2025-02-23T15:48:21
```

```
|_  start_date: N/A

|_nbstat: NetBIOS name: RDS1, NetBIOS user: <unknown>, NetBIOS MAC: 000c29cd9c01 (VMware)

|_clock-skew: mean: -3s, deviation: 0s, median: -3s


TRACEROUTE

HOP RTT     ADDRESS

1   0.43 ms 192.168.0.207


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 152.32 seconds


┌──(kali㉿kali)-[~]

└─$ sudo nmap -sU -A 192.168.0.207

Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-23 17:50 EET

Nmap scan report for 192.168.0.207

Host is up (0.00039s latency).

Not shown: 991 closed udp ports (port-unreach)

PORT     STATE         SERVICE       VERSION

123/udp  open|filtered ntp

137/udp  open          netbios-ns    Microsoft Windows or Samba netbios-ns (workgroup: C-POLIGON)

| nbns-interfaces:

|   hostname: RDS1

|   interfaces:

|_    192.168.0.207
```

```
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
3389/udp open|filtered ms-wbt-server
3702/udp open|filtered ws-discovery
| wsdd-discover:
|   Devices
|     Message id: e4f32c67-14c0-4105-ba2d-71c6ccc8b4c6
|       Address: http://192.168.0.207:5357/031c9908-5880-4d67-92d7-ef1f61e631ed/
|_    Type: Device pub:Computer
4500/udp open|filtered nat-t-ike
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:CD:9C:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: RDS1

Host script results:
|_nbstat: NetBIOS name: RDS1, NetBIOS user: <unknown>, NetBIOS MAC: 000c29cd9c01 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.0.207
```

```
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1309.21 seconds


┌──(kali㉿kali)-[~]

└─$
```