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: "Оцінка ефективності систем IPS для різних сценаріїв атак"

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

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

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

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

Рецензент
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 Степанюку Назарію Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка ефективності систем IPS для різних сценаріїв атак

Керівник роботи Оробчук Олександра Романівна, доктор філософії, старший викладач 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 Документація pfSsense та IPS Suricata, вимоги до IPS. Документація Metasploitable VM

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Налаштування лабораторного середовища тестування
3. Тестування ефективності IPS Suricata
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. Основа інформаційної безпеки. 6. Схема лабораторного середовища. 7. Складові лабораторного середовища. 8. Інтерфейс налаштування наборів правил IPS Suricata. 9. Тестові атаки на Metasploitable VM: Flood атаки. 10. Тестові атаки на Metasploitable VM: Атаки на DNS сервіс. 11. Тестові атаки на Metasploitable VM: Brute force атаки. 12. Блокування IP-адрес в IPS Suricata. 13. Висновки. 14. Завершальний.

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 «Налаштування лабораторного середовища тестування»	11.03 – 25.03	
5.	Оформлення розділу «Тестування ефективності IPS Suricata»	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	25.06.2025	

Студент _____ Степанюк Н. Д.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Оцінка ефективності систем IPS для різних сценаріїв атак // Кваліфікаційна робота ОР «Бакалавр» // Степанюк Назарій Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 71, рис. – 38, табл. – - , кресл. – 14, додат. – 1.

Ключові слова: IPS Suricata, pfSense, Hyper-V, Kali Linux, Metasploitable VM.

У кваліфікаційній роботі бакалавра було досліджено ефективність роботи системи запобігання вторгненням IPS Suricata, інтегрованої у маршрутизатор pfSense, з метою підвищення рівня захисту інформаційних систем від сучасних кіберзагроз. Робота охоплює аналіз сучасних мережевих атак, класифікацію загроз а також вивчення механізмів роботи IPS-рішень. Для дослідження було розроблено лабораторне середовище на базі гіпервізора Hyper-V із використанням операційних систем pfSense, Kali Linux та вразливої системи Metasploitable VM, що дозволило змоделювати реалістичні сценарії атак, зокрема SYN Flood, brute force та атаки на DNS-сервіс.

Отримані результати тестування показали, що IPS Suricata ефективно виявляє та блокує підозрілий мережевий трафік у режимі реального часу, що підтверджується аналізом журналів подій та сповіщень. Результати роботи підтверджують доцільність застосування IPS Suricata як ефективного інструменту захисту інформаційних систем у сучасних умовах кіберзагроз.

ANNOTATION

Evaluation of IPS Effectiveness for Different Attack Scenarios // Thesis of educational level "Bachelor"// Nazarii Stepaniuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 63, figs. 38, tables -, drawings 14, added. 1.

Keywords: IPS Suricata, pfSense, Hyper-V, Kali Linux, Metasploitable VM.

In this bachelor's thesis, the author investigated the effectiveness of the IPS Suricata intrusion prevention system integrated into the pfSense router to improve the level of protection of information systems from modern cyber threats. The work includes the analysis of modern network attacks, threat classification, and the study of the mechanisms of IPS solutions. For the study, a laboratory environment based on the Hyper-V hypervisor was developed using pfSense, Kali Linux and the vulnerable Metasploitable VM system, which allowed to simulate realistic attack scenarios, including SYN Flood, brute force and DNS service attacks.

The test results showed that IPS Suricata effectively detects and blocks suspicious network traffic in real time, which is confirmed by the analysis of event and notification logs. The results confirm the feasibility of using IPS Suricata as an effective tool for protecting information systems in the current cyber threat environment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IPS	—	Intrusion Prevention System
CIA	—	Confidentiality, Integrity, Availability
MITM	—	Man-in-the-Middle
ARP	—	Address Resolution Protocol
DNS	—	Domain Name System
SSL	—	Secure Sockets Layer
TLS	—	Transport Layer Security
VPN	—	Virtual Private Network
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
IDS	—	Intrusion Detection System
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

ВСТУП

Актуальність теми. Атаки на інформаційні системи можуть призводити до суттєвих фінансових та репутаційних втрат для організацій. Це створює необхідність у впровадженні ефективних систем захисту мережевої інфраструктури. Системи запобігання вторгненням (IPS) відіграють важливу роль у забезпеченні інформаційної безпеки, оскільки дозволяють оперативно виявляти та блокувати шкідливий трафік. Одним із поширених рішень є використання IPS Suricata, яка інтегрується в маршрутизатор pfSense і забезпечує ефективний моніторинг та захист мережі. Це дослідження спрямоване на аналіз продуктивності та точності IPS Suricata у сценаріях реальних атак, що дозволить визначити її сильні та слабкі сторони.

Мета і задачі дослідження. Мета дослідження – оцінити ефективність роботи системи IPS Suricata для різних сценаріїв атак шляхом практичного тестування.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- провести аналіз сучасних мережевих атак;
- дослідити принципи роботи систем IPS, їх типи та механізми виявлення загроз;
- розробити тестове середовище, що включає pfSense із IPS Suricata, атакуючу систему Kali Linux та ціль атаки Metasploitable VM.
- створити сценарії атак;
- провести тестування IPS та проаналізувати ефективність її роботи щодо різних типів атак.

Об’єкт дослідження. Об'єктом дослідження є системи IPS.

Предмет дослідження. Предметом дослідження є ефективність роботи системи IPS Suricata, яка розгорнута як модуль програмного маршрутизатора pfSense у протидії різним сценаріям мережевих атак.

Практичне значення одержаних результатів. Результати цього дослідження можуть бути використані для покращення налаштувань IPS Suricata з метою підвищення рівня захисту корпоративних мереж від кіберзагроз.

Запропонована методологія тестування дозволить системним адміністраторам та фахівцям з кібербезпеки оцінювати ефективність IPS-рішень у реальних умовах експлуатації.

Матеріали роботи можуть бути використані у навчальних програмах з інформаційної безпеки для практичного вивчення функціоналу IPS-систем, принципів їх роботи та методів тестування на прикладі реальних атак. Це сприятиме підвищенню рівня обізнаності та підготовки спеціалістів у сфері кібербезпеки.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Інформаційна безпека та класифікація мережевих атак

Інформаційна безпека – це сукупність методів, засобів та процедур, що забезпечують захист інформації від несанкціонованого доступу, модифікації, знищення або розголошення. Вона є важливим аспектом функціонування інформаційних систем, оскільки дані, що обробляються, передаються та зберігаються, повинні залишатися захищеними від кіберзагроз, технічних збоїв та людських помилок. Основою інформаційної безпеки є три ключові принципи: конфіденційність, цілісність і доступність (CIA-тріада) [1] (див. рисунок 1.1).

Рисунок 1.1 – CIA-тріада

Конфіденційність передбачає, що інформація доступна лише для авторизованих користувачів і не може бути розкрита стороннім особам. Цілісність означає, що дані залишаються незмінними та достовірними, без несанкціонованих модифікацій. Доступність гарантує, що інформація та ресурси залишаються доступними для законних користувачів у потрібний час.

Атаки на конфіденційність спрямовані на отримання несанкціонованого доступу до інформації, що передається, зберігається або обробляється в мережі [2]. Основна мета таких атак – викрадення даних, які можуть включати персональну інформацію, фінансові дані, облікові дані, корпоративну інформацію та комерційні таємниці. Одним із найпоширеніших методів атак на конфіденційність є перехоплення трафіку (sniffing), коли зловмисники використовують спеціалізоване програмне забезпечення для аналізу мережевих пакетів. Якщо дані передаються у відкритому вигляді без шифрування, зловмисник може отримати паролі, банківську інформацію та інші конфіденційні дані. Особливо небезпечними такі атаки є у відкритих Wi-Fi мережах, де трафік користувачів може легко аналізуватися без їхнього відома. Ще одним ефективним способом компрометації конфіденційності є атака MITM [3], при якій зловмисник перехоплює та змінює передані між двома сторонами дані. Вона може здійснюватися через ARP-спуфінг, що дозволяє злочинцю не лише спостерігати за трафіком, а й змінювати його в реальному часі (див. рисунок 1.2).

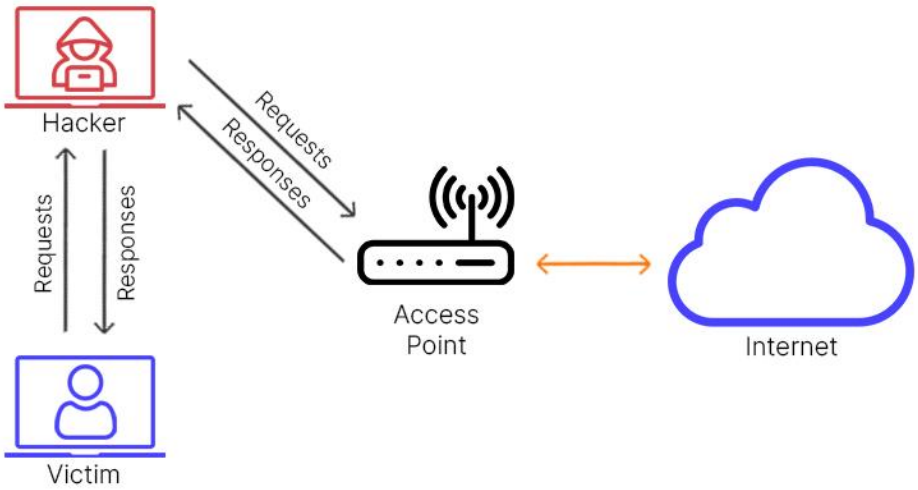


Рисунок 1.2 – ARP spoofing

Фішингові атаки також є ефективним методом компрометації конфіденційної інформації. Вони використовують соціальну інженерію для введення користувачів в оману з метою змусити їх розкрити свої облікові дані або персональну інформацію. Зловмисники можуть створювати підроблені веб-сайти банків, соціальних мереж або поштових сервісів, які виглядають ідентично

справжнім. Користувачі, не підозрюючи обману, вводять свої паролі, які одразу потрапляють до атакуючих. Розкриття конфіденційної інформації через слабкі паролі також є серйозною загрозою. Атакуючі можуть застосовувати метод brute-force для підбору паролів або використовувати готові бази даних облікових записів із попередніх витоків інформації [4] [5] (див. рисунок 1.3).

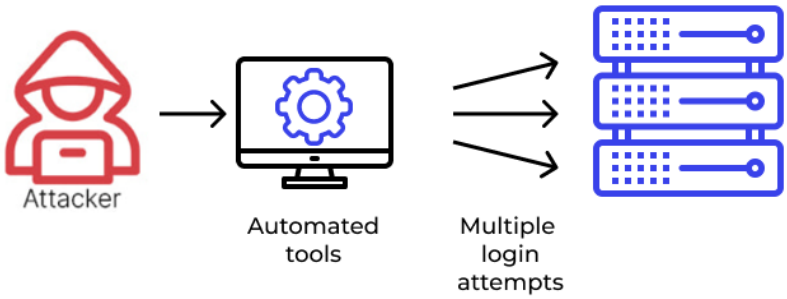


Рисунок 1.3 – Brute-force attack

Для захисту від атак на конфіденційність рекомендується використовувати шифрування даних, двофакторну автентифікацію (2FA) та складні паролі.

Атаки на цілісність спрямовані на несанкціоновану зміну, підробку або знищення даних у процесі їх передавання, обробки або зберігання. Основна мета таких атак – спотворення інформації, введення жертви в оману або порушення нормального функціонування системи. Вони можуть завдавати серйозної шкоди організаціям, оскільки підроблені дані можуть використовуватися для фінансових махінацій, зміни критично важливих конфігурацій або дезінформації. Одним із найпоширеніших методів атак на цілісність є атака MITM під час якої зловмисник перехоплює трафік між двома сторонами, змінює його та передає далі, зберігаючи ілюзію справжнього з'єднання. Це може призвести до зміни фінансових транзакцій, підміни файлів або маніпуляції з електронною поштою. DNS-спуфінг є ще одним видом атак, що спрямовані на зміну даних. У цьому випадку зловмисник підмінює DNS-записи, спрямовуючи користувачів на підроблені сайти, що візуально не відрізняються від оригінальних [6] (див. рисунок 1.4).

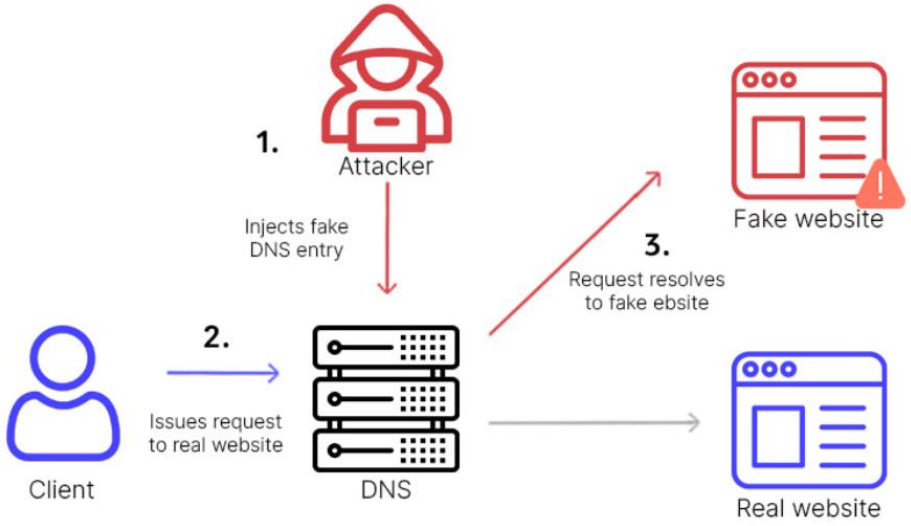


Рисунок 1.4 – DNS spoofing

Таким чином, жертви можуть вводити свої облікові дані або конфіденційну інформацію, навіть не підозрюючи про загрозу. Не менш небезпечними є атаки на бази даних, зокрема SQL-ін'єкції (SQL Injection). Вони дозволяють зловмиснику вставляти шкідливі SQL-запити у веб-форми, що може призвести до зміни, видалення або витоку критично важливої інформації. Наприклад, уразливий веб-додаток може дозволити атакуючому змінювати баланси користувачів у фінансових системах або видаляти цілі таблиці бази даних. Атаки на файлові системи також є поширеним методом порушення цілісності. Віруси-шифрувальники можуть модифікувати файли так, що вони стають непридатними для використання, а у випадку програм-вимагачів (WannaCry або Locky) доступ до зашифрованих файлів можна відновити лише після сплати викупу. Атаки на цілісність можуть також включати маніпуляцію журналами подій, коли зловмисники редагують або видаляють записи у логах, щоб приховати сліди своєї присутності у системі. Це ускладнює розслідування інцидентів безпеки, оскільки фахівці з кібербезпеки не можуть отримати достовірні відомості про події у системі. Для захисту від атак на цілісність необхідно використовувати контроль цілісності даних за допомогою хеш-функцій (SHA та інші), цифрові підписи, контроль доступу на основі ролей (RBAC), регулярний аудит логів, оновлення програмного забезпечення та резервне копіювання даних. Також

важливу роль відіграє шифрування каналів зв’язку (SSL/TLS, VPN), що зменшує ймовірність атак MITM та спуфінгу.

Атаки на доступність спрямовані на порушення нормальної роботи інформаційних систем, серверів, мережевих ресурсів або окремих сервісів з метою зробити їх недоступними для легітимних користувачів. Вони можуть реалізовуватися шляхом перевантаження ресурсів, вразливостей у програмному забезпеченні або фізичного впливу на обладнання. Одним із найпоширеніших методів є атаки типу DoS та DDoS. DoS-атаки здійснюються шляхом надсилання величезної кількості запитів на сервер, що перевантажує його ресурси та призводить до недоступності послуг. DDoS-атаки є складнішою версією DoS, оскільки здійснюються з великої кількості скомпрометованих пристроїв (ботнетів), що ускладнює їхню нейтралізацію [7] [8] [9] (див. рисунок 1.5).

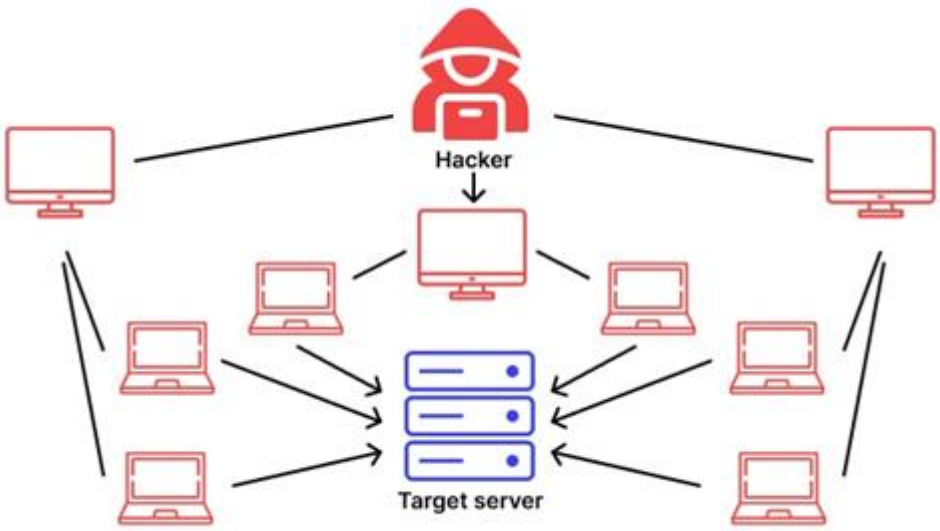


Рисунок 1.5 – DDoS атака

Прикладами таких атак є SYN Flood, коли атакуючий надсилає велику кількість запитів на встановлення з’єднання, але не завершує процес тристороннього рукостискання TCP [10] [11] (див. рисунок 1.6), та UDP Flood, коли на сервер надсилаються великі обсяги беззмістовних UDP-пакетів, що вичерпує його обчислювальні ресурси [12] [13] (див. рисунок 1.7).

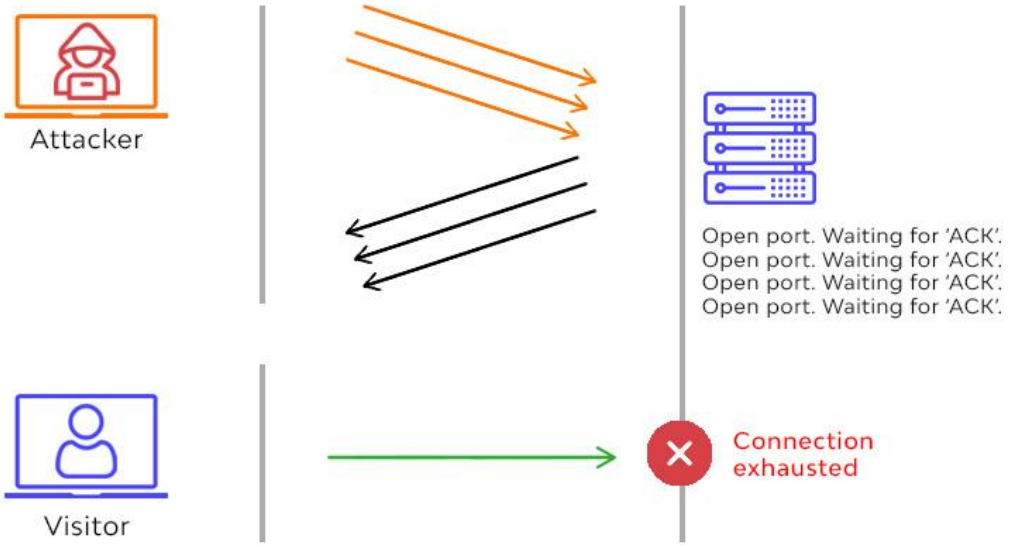


Рисунок 1.6 – SYN flood

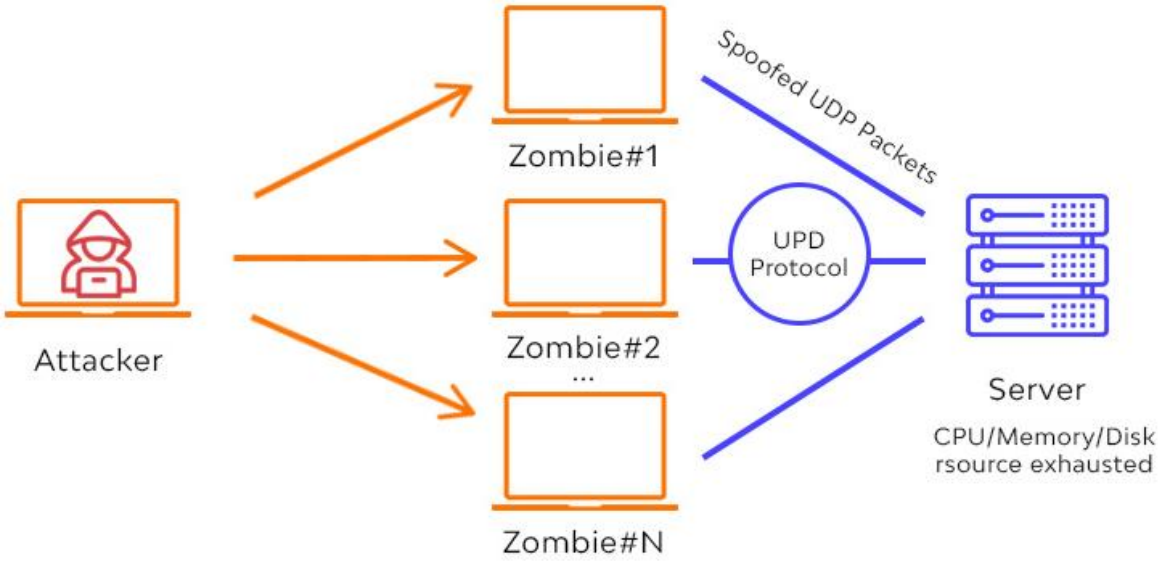


Рисунок 1.7 – UDP flood

Для захисту від атак на доступність використовується фільтрація аномального трафіку за допомогою IPS-систем [14], хмарні сервіси DDoS захисту (Cloudflare, Akamai).

1.2 Наслідки атак для інформаційних систем

Кібератаки можуть мати серйозні наслідки для інформаційних систем, зачіпаючи їхню конфіденційність, цілісність і доступність. Вони можуть призводити до втрати даних, фінансових збитків, порушення роботи бізнес-

процесів та репутаційних втрат. Вплив атак залежить від їхнього типу, масштабів та ефективності захисних заходів, застосованих у системі [15].

Одним із найбільш серйозних наслідків є втрата конфіденційності, коли зловмисники отримують доступ до інформації з обмеженим доступом, такої як персональні дані, фінансові звіти, корпоративні секрети або урядові документи. Це може статися внаслідок атак типу MITM або фішингу. Витік інформації може використовуватися для шахрайства, шантажу або конкурентної розвідки, завдаючи значної шкоди жертвам атаки.

Ще одним критичним наслідком атак є порушення цілісності даних, що може призвести до зміни, підробки або знищення важливих інформаційних ресурсів. Якщо атакуючі отримують доступ до баз даних або файлових систем, вони можуть маніпулювати записами, що може мати катастрофічні наслідки для фінансових установ, медичних систем або державних організацій. Наприклад, зміна банківських операцій, фальсифікація медичних діагнозів або підміна юридичних документів можуть спричинити серйозні правові, фінансові або соціальні проблеми.

Недоступність інформаційних систем унаслідок атак може спричинити зупинку роботи бізнесу, промислових підприємств, транспортних систем або державних сервісів. DDoS-атаки, віруси-вимагачі та інші методи саботажу можуть паралізувати роботу критично важливих сервісів, викликаючи значні економічні збитки. Наприклад, якщо веб-сайт компанії або платіжна система недоступні навіть на кілька годин, це може призвести до втрати клієнтів, штрафних санкцій та зниження довіри з боку користувачів.

Кібератаки також можуть спричинити фінансові збитки, пов’язані з відновленням систем, розслідуванням інцидентів, судовими витратами та виплатою штрафів за витік конфіденційної інформації. Компанії можуть бути змушені інвестувати значні кошти у модернізацію своєї кібербезпеки, навчання персоналу та розробку стратегій реагування на атаки. Особливо великі втрати можуть зазнати фінансові установи, якщо зловмисники отримають доступ до банківських рахунків або електронних платіжних систем. Підрив довіри та репутаційні втрати можуть бути навіть серйознішими, ніж прямі фінансові

збитки. Якщо компанія не може гарантувати безпеку даних своїх клієнтів, це може призвести до масових відмов від її послуг, падіння акцій та втрати конкурентоспроможності. Крім того, деякі атаки можуть загрожувати фізичній безпеці, особливо якщо вони спрямовані на промислові або інфраструктурні системи. Кібератаки на енергетичні компанії, водопостачальні системи або транспортні мережі можуть призвести до катастрофічних наслідків, таких як збої в електромережах, зупинка транспорту або навіть загроза життю людей. Атаки також можуть використовуватися для політичного чи військового тиску, коли державні або приватні хакерські групи здійснюють кібератаки з метою дестабілізації економіки, збору розвідувальних даних або саботажу. Кіберрозвідка, шпигунство та вплив на вибори через маніпуляцію інформацією є реальними загрозами, які використовуються у сучасних гібридних війнах.

Таким чином, наслідки атак на інформаційні системи можуть бути різноманітними та мати як локальний так і глобальний характер. Вони зачіпають не лише окремі організації, а й цілі сектори економіки, державні установи та критичні інфраструктури. Ефективний захист вимагає комплексного підходу, що включає технічні засоби безпеки, організаційні заходи та постійний моніторинг загроз.

1.4 Огляд технології IPS

Системи запобігання вторгненням (IPS) є ключовими компонентами сучасної кібербезпеки, призначеними для активного виявлення та блокування атак у режимі реального часу [16]. Вони розширюють можливості систем виявлення вторгнень (IDS), автоматично реагуючи на загрози та запобігаючи їх подальшому розвитку [17]. IPS працюють на різних рівнях мережевої моделі та можуть бути розгорнуті у вигляді окремих пристроїв, вбудованих модулів у брандмауерах або програмних рішень для серверів і кінцевих точок.

Основний принцип роботи IPS полягає в аналізі мережевого трафіку, виявленні підозрілих або шкідливих активностей та автоматичному блокуванні атак [18]. На рисунку 1.8 показано схему розташування IPS.

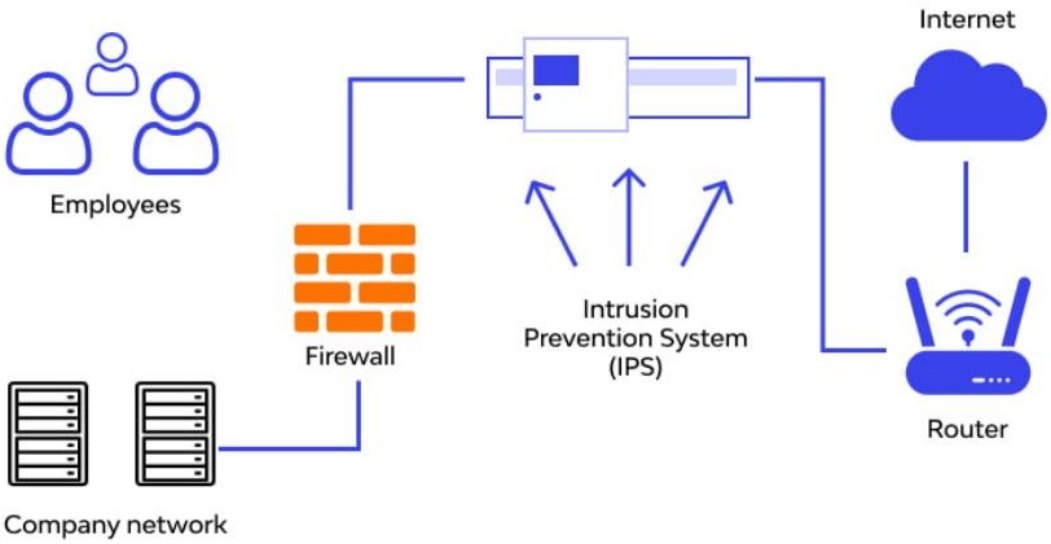


Рисунок 1.8 – Схема розташування IPS

Система використовує сигнатурний та поведінковий аналіз для розпізнавання кіберзагроз. Сигнатурний аналіз дозволяє швидко ідентифікувати відомі загрози за допомогою бази даних сигнатур, проте він має обмеження у виявленні нових або модифікованих атак. Поведінковий аналіз оцінює аномальні дії в мережі, такі як незвично висока кількість підключень або нетипові запити до серверів. Евристичний підхід використовує штучний інтелект і алгоритми машинного навчання для прогнозування нових загроз на основі аналізу поведінкових моделей.

IPS-системи можуть бути розгорнуті у вигляді мережевих або хостових рішень. Мережева IPS (NIPS) працює на рівні мережевого периметра та перевіряє весь вхідний і вихідний трафік, що проходить через неї. Вона ефективна для запобігання DDoS-атак, експлуатації вразливостей у мережевих протоколах та шкідливого трафіку [19] (див. рисунок 1.9).

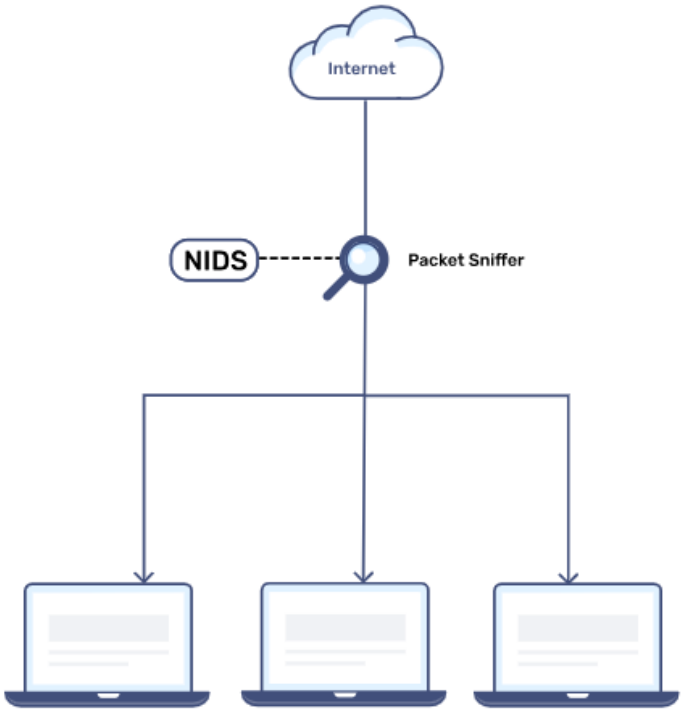


Рисунок 1.9 – NIPS

Хостова IPS (HIPS) функціонує безпосередньо на кінцевих пристроях або серверах, захищаючи їх від локальних атак, експлойтів та несанкціонованих змін у файловій системі (див. рисунок 1.10).

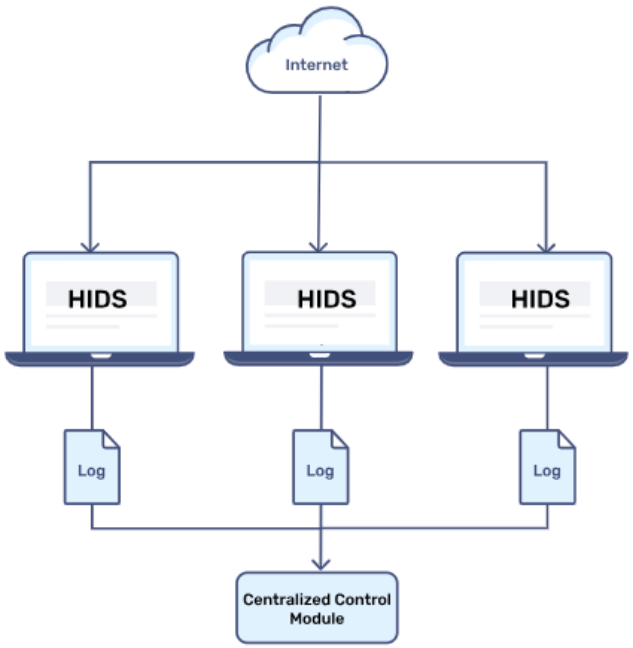


Рисунок 1.10 – HIPS

Однією з важливих особливостей IPS є її інтеграція з іншими засобами захисту, такими як міжмережеві екрани (firewalls) та SIEM-рішення для централізованого моніторингу подій безпеки. Вбудовані механізми логування та сповіщень дозволяють системним адміністраторам отримувати детальну інформацію про зафіксовані атаки, аналізувати їхні джерела та вживати відповідних заходів для посилення безпеки. IPS-системи можуть реагувати на загрози різними способами. Вони можуть блокувати шкідливий трафік, змінювати конфігурацію мережевого обладнання для запобігання подальшому поширенню атаки, завершувати небезпечні сесії або ізолювати скомпрометовані пристрої. Деякі IPS-рішення підтримують інтеграцію з threat intelligence-платформами, що дозволяє їм оновлювати бази даних загроз у реальному часі та підвищувати ефективність виявлення нових атак.

Популярні IPS-рішення включають як комерційні продукти, такі як Cisco Firepower, Palo Alto Networks, Fortinet FortiGate, так і open-source системи, наприклад, Suricata та Snort. Open-source IPS, такі як Suricata, широко використовуються в поєднанні з маршрутизаторами та брандмауерами pfSense або OPNsense для забезпечення комплексного мережевого захисту.

Системи IPS відіграють важливу роль у забезпеченні безпеки сучасних мережевих інфраструктур [20]. Їхня здатність працювати в режимі реального часу, аналізувати трафік та реагувати на загрози робить їх незамінним елементом захисту інформаційних систем, особливо у великих корпоративних середовищах та критично важливих інфраструктурних об'єктах.

1.5 Висновки до першого розділу

У першому розділі було розглянуто основні поняття інформаційної безпеки, класифікацію мережевих атак, їх наслідки для інформаційних систем, а також принципи роботи технології IPS. Аналіз класифікації мережевих атак дозволив виокремити основні категорії загроз, серед яких атаки на конфіденційність, цілісність та доступність. Було розглянуто їхні методи реалізації, включаючи MITM, DNS-спуфінг, brute-force, SQL-ін'єкції, DoS/DDoS та інші. Було також

розглянуто наслідки атак для інформаційних систем, які можуть варіюватися від втрати конфіденційності та модифікації даних до повного виходу з ладу інформаційних систем. Зокрема, кібератаки можуть спричиняти фінансові збитки, репутаційні ризики, втрату довіри користувачів та загрози критичним інфраструктурам. Огляд технології IPS дозволив визначити основні принципи роботи цих систем, методи виявлення загроз та їхню роль у забезпеченні кібербезпеки. Було розглянуто мережеві (NIPS) та хостові (HIPS) IPS, їхню інтеграцію з іншими засобами захисту, а також механізми запобігання атакам у реальному часі.

Отже, проведений огляд предметної області показав важливість використання IPS-рішень для забезпечення безпеки інформаційних систем. У подальших розділах буде проведено практичне тестування IPS Suricata у складі pfSense, оцінено її ефективність для різних сценаріїв атак.

РОЗДІЛ 2 НАЛАШТУВАННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ТЕСТУВАННЯ

2.1 Схема лабораторного середовища

Для оцінки ефективності системи IPS у реальних сценаріях атак необхідно створити тестове лабораторне середовище, яке дозволить імітувати різні типи кібератак та аналізувати реакцію IPS [21]. Лабораторне середовище має відповідати вимогам реального мережевого середовища, включати атакуючі та цільові системи, а також компоненти захисту. Причинами створення такого середовища є необхідність дослідження ефективності роботи IPS у різних сценаріях атак, перевірка її здатності виявляти та блокувати загрози. Оскільки IPS працює в реальному часі та має запобігати вторгненням до мережі, важливо оцінити її реакцію на типові атаки, включаючи DDoS [22] та brute-force. Основними компонентами тестового середовища є міжмережевий екран pfSense із вбудованою системою IPS Suricata, атакуючий хост з ОС Kali Linux та вразливий сервер Metasploitable VM, що дозволяє проводити моделювання атак у контрольованому середовищі (див. рисунок 2.1).

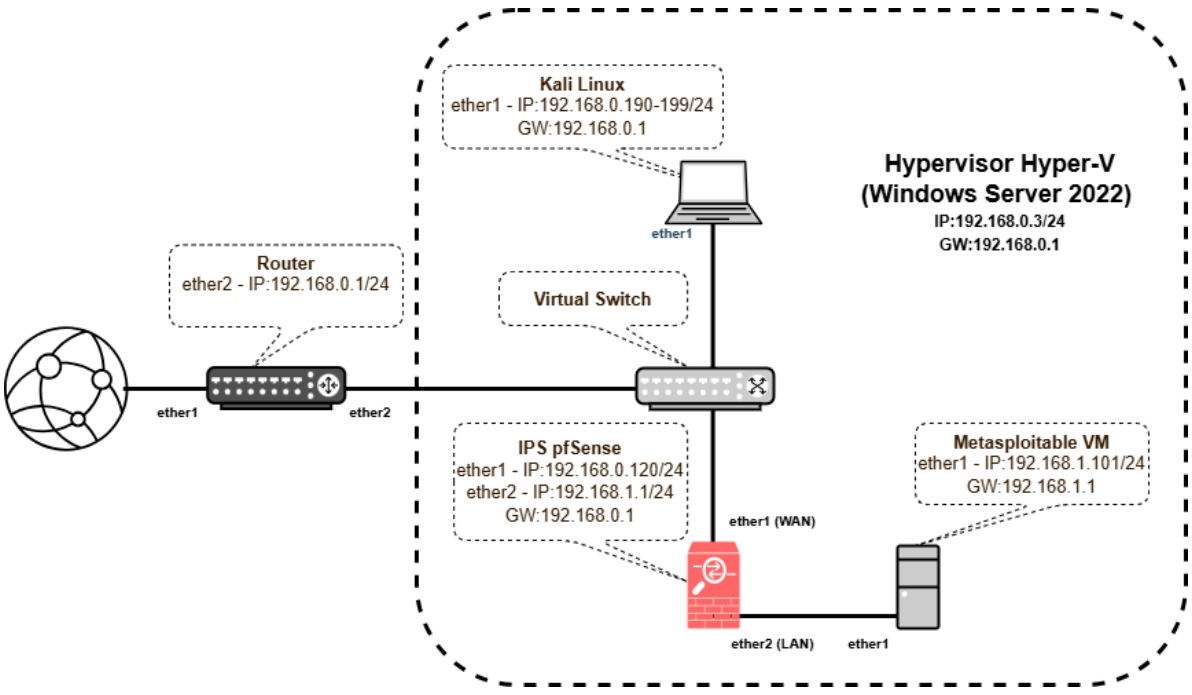


Рисунок 2.1 – Схема лабораторного середовища

Представлена схема лабораторного середовища ілюструє архітектуру, яка використовується для тестування ефективності системи IPS у контрольованих умовах.

Середовище розгорнуте на гіпервізорі Hyper-V, який працює на операційній системі Windows Server 2022, та містить декілька компонентів, з'єднаних через віртуальний комутатор (Virtual Switch). Віртуальний комутатор забезпечує внутрішню мережеву комунікацію між усіма компонентами, розгорнутими в Hyper-V. Гіпервізор Hyper-V виступає платформою для створення та управління віртуальними машинами, які беруть участь у тестуванні. Він має IP-адресу 192.168.0.3/24 із шлюзом 192.168.0.1. Віртуальні машини, розгорнуті на цьому гіпервізорі, включають pfSense, Kali Linux та Metasploitable VM.

Фізичний роутер забезпечує зв’язок між лабораторним середовищем, де знаходиться pfSense та інші віртуальні машини, та глобальною мережею Інтернет. Зовнішній інтерфейс роутера підключений до зовнішньої мережі, а внутрішній інтерфейс має IP-адресу 192.168.0.1/24, яка є шлюзом для гіпервізора та інших пристроїв у віртуальному середовищі. Маршрутизатор pfSense виконує роль шлюзу між WAN- і LAN-мережами в лабораторному середовищі. WAN-інтерфейс pfSense має IP-адресу 192.168.0.120/24 та використовує шлюз 192.168.0.1. LAN-інтерфейс pfSense підключений до внутрішньої мережі з IP-адресою 192.168.1.1/24, забезпечуючи зв’язок із вразливим сервером Metasploitable VM. На pfSense встановлено IPS, яка аналізує мережевий трафік у реальному часі, виявляє та блокує атаки. Kali Linux підключений до WAN-мережі та має IP-адресу 192.168.0.180/24 із шлюзом 192.168.0.1. Kali Linux використовується як атакуюча система для генерування шкідливого трафіку. Metasploitable – це вразлива віртуальна машина, яка служить ціллю атак із Kali Linux. Вона підключена до LAN-інтерфейсу pfSense із IP-адресою 192.168.1.101/24 та шлюзом 192.168.1.1. Дана віртуальні машина включає вразливості в різних сервісах, які можуть бути експлуатовані для моделювання атак.

Лабораторне середовище дає змогу провести детальний аналіз журналів Suricata, оцінити кількість виявлених і заблокованих атак. Таке тестування дає змогу визначити, наскільки ефективно Suricata IPS працює в умовах наближених до реальних атак, які методи захисту є найбільш дієвими, а також як можна покращити її продуктивність та точність виявлення загроз. Середовище також дозволяє експериментувати з різними конфігураціями Suricata, змінювати сигнатури загроз, адаптувати правила фільтрації та виявлення атак. Це дає можливість дослідити, як зміна конфігурацій впливає на рівень безпеки та продуктивність мережі. Крім того, така модель дозволяє оцінити, як IPS реагує на атаки з різних джерел, як швидко вона здатна заблокувати загрози та які методи атаки можуть залишитися непоміченими.

2.2 Windows Server 2022 Core з функцією Hyper-V

Windows Server 2022 - це сучасна серверна операційна система, розроблена компанією Microsoft, яка представляє наступне покоління серверних платформ, орієнтованих на високий рівень безпеки, продуктивності та стабільності. Вона призначена для підтримки інфраструктури, управління корпоративними мережами, хмарних рішень і віртуалізації, що робить її ідеальним вибором для сучасних IT-організацій [23].

Однією з ключових особливостей Windows Server 2022 є підвищений рівень безпеки. Ця версія впроваджує концепцію Secured-core Server, яка забезпечує захист від атак на рівні апаратного та мікропрограмного забезпечення. Це включає безпечне завантаження системи (Secure Boot), функцію ізоляції віртуалізації (VBS) і апаратну підтримку TPM 2.0 для шифрування даних. Вбудовані механізми, такі як Windows Defender Exploit Guard і Advanced Threat Protection, допомагають виявляти та запобігати сучасним загрозам, що сприяє забезпеченню стійкості системи до кібератак.

Windows Server 2022 Core - це версія серверної операційної системи Windows Server 2022, яка орієнтована на максимальну продуктивність, зменшення використання ресурсів і підвищення безпеки. У цій редакції

виключено графічний інтерфейс користувача (GUI), що дозволяє знизити поверхню атаки, мінімізувати потреби у системних ресурсах і створити платформу для серверів із високим навантаженням або критично важливими завданнями.

Основна концепція Server Core полягає у створенні серверної платформи, яка виконує ключові функції без додаткових візуальних компонентів. Усі операції в Windows Server 2022 Core виконуються через командний рядок (Command Prompt), PowerShell або віддалені інструменти управління, такі як Windows Admin Center. Відсутність графічного інтерфейсу дозволяє знизити споживання оперативної пам’яті та процесорних ресурсів, а також зменшити кількість вразливих компонентів, які можуть бути використані зловмисниками для атак. Windows Server 2022 Core підтримує всі основні серверні ролі та функції, включаючи службу Active Directory, сервери файлів та друку, Hyper-V, DNS, DHCP, веб-сервери (IIS), а також роль хосту контейнерів для розгортання контейнеризованих додатків. Завдяки цьому вона ідеально підходить для серверів, які виконують специфічні завдання, наприклад, віртуалізацію, керування мережею або хостинг додатків.

Оскільки Server Core не має графічного інтерфейсу, управління системою здійснюється через командний рядок, PowerShell або віддалені інструменти, такі як Windows Admin Center або Remote Server Administration Tools (RSAT). Це дозволяє адміністраторам ефективно керувати серверами навіть у великих мережах. Інтеграція з PowerShell забезпечує широкий спектр можливостей для автоматизації, написання скриптів і виконання рутинних завдань.

На рисунку 2.2 представлено інтерфейс SConfig (Server Configuration), який використовується в Windows Server 2022 Standard Core.

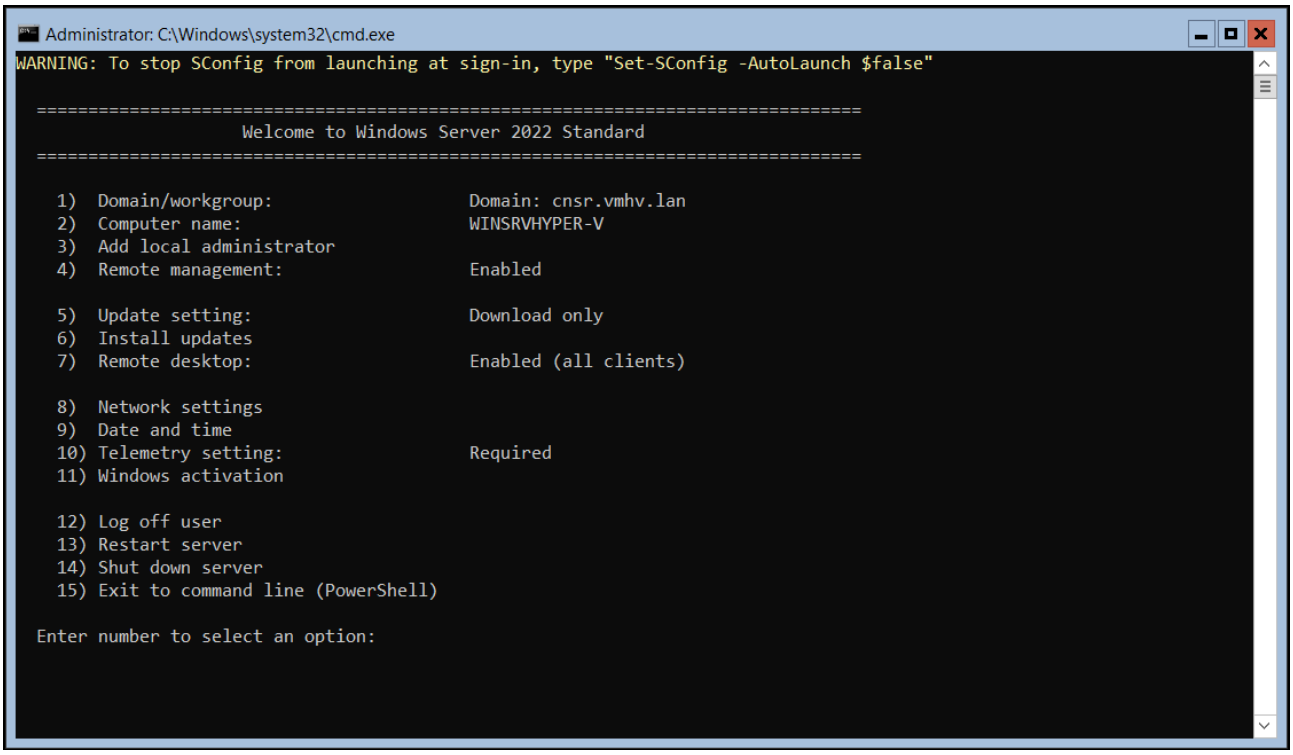


Рисунок 2.2 – Інтерактивний текстовий інтерфейс для базового налаштування Windows Server 2022 Core

SConfig - це інтерактивний текстовий інтерфейс для базового налаштування сервера без використання графічного інтерфейсу користувача. Він забезпечує швидкий доступ до ключових параметрів і дозволяє адміністраторам виконувати основні завдання налаштування системи через командний рядок або PowerShell. Цей інструмент автоматично запускається після входу в систему адміністратором.

Інтерфейс SConfig є простим, але надійним інструментом для адміністратора, який працює в Windows Server Core. Завдяки його використанню можна швидко налаштувати сервер, не вдаючись до графічних засобів управління. Це особливо зручно в середовищах, де сервери розгорнуті у віддалених дата-центрах або працюють у віртуальних середовищах без графічного доступу. SConfig також забезпечує більшу безпеку, оскільки зменшує поверхню атаки, яка часто пов'язана з графічним інтерфейсом.

Гіпервізор Hyper-V у Windows Server 2022 Core є вбудованою технологією віртуалізації, яка дозволяє створювати та керувати віртуальними машинами на фізичному сервері [24]. Це гіпервізор типу 1, який працює безпосередньо на

апаратному забезпеченні і забезпечує ізоляцію, розподіл ресурсів і безпеку для кожної віртуальної машини [25]. Він оптимізований для продуктивності, безпеки та масштабованості, що робить його ідеальним рішенням для сучасних корпоративних і хмарних середовищ.

У середовищі Windows Server 2022 Core гіпервізор Hyper-V функціонує без графічного інтерфейсу, і всі операції з його налаштування та управління виконуються через PowerShell або віддалені інструменти, такі як Windows Admin Center або Hyper-V Manager. Цей підхід забезпечує зменшення споживання ресурсів і підвищення безпеки завдяки відсутності зайвих компонентів інтерфейсу. Hyper-V підтримує широкий спектр функціональності, що робить його потужним інструментом для реалізації віртуалізації. Hyper-V у Windows Server 2022 Core дозволяє запускати кілька віртуальних машин на одному фізичному сервері. Кожна ВМ працює у своєму ізольованому середовищі, що забезпечує безпеку та стабільність. Hyper-V підтримує різні операційні системи, включаючи Windows, Linux і FreeBSD, що дозволяє організаціям використовувати різноманітні додатки та сервіси на одній фізичній платформі. Віртуальні машини можуть мати різні конфігурації ресурсів, таких як процесори, пам'ять, мережеві адаптери та дисковий простір, що дозволяє адаптувати їх під конкретні потреби. Однією з ключових функцій Hyper-V є підтримка динамічного розподілу ресурсів. Це означає, що ресурси сервера можуть автоматично перерозподілятися між віртуальними машинами залежно від їхніх потреб, що підвищує ефективність використання апаратного забезпечення. Крім того, Hyper-V підтримує механізми високої доступності, такі як Live Migration і Failover Clustering, які дозволяють переміщувати віртуальні машини між фізичними хостами без простоїв, забезпечуючи безперервність роботи додатків.

Безпека є одним із головних пріоритетів Hyper-V у Windows Server 2022 Core. Захист віртуальних машин реалізується за допомогою технології Shielded VMs, яка забезпечує шифрування дисків і запобігає несанкціонованому доступу до ВМ навіть на рівні адміністратора хоста. Крім того, Hyper-V підтримує ізоляцію мережевого трафіку між віртуальними машинами, а також інтеграцію з функціями безпеки, такими як Credential Guard і Device Guard.

Мережеві можливості Hyper-V включають підтримку віртуальних комутаторів (Virtual Switch), що забезпечують управління мережевим трафіком між віртуальними машинами, а також між ВМ і зовнішньою мережею. Віртуальні комутатори підтримують такі функції, як VLAN, фільтрація мережевого трафіку та віддзеркалення портів, що дозволяє реалізувати складні мережеві сценарії.

На рисунку 2.3 представлено інтерфейс Hyper-V Manager у Windows Server, який використовується для управління віртуальними машинами.

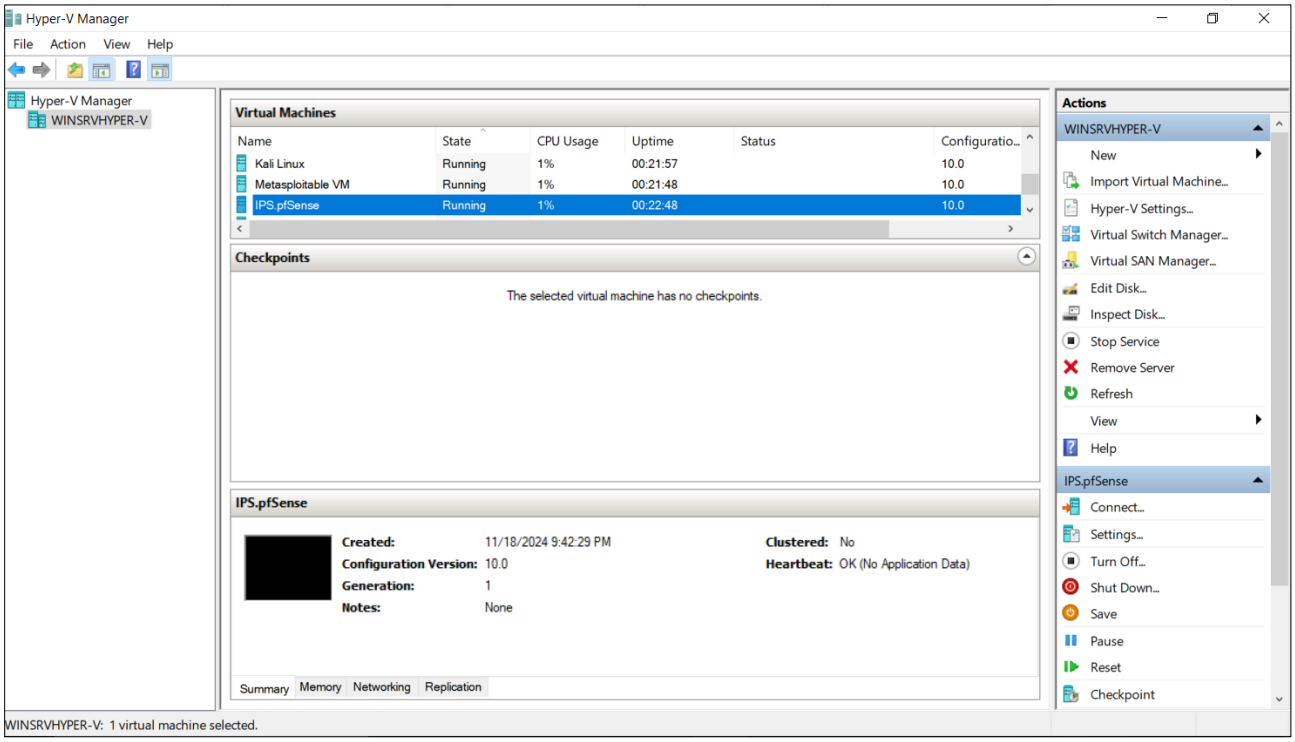


Рисунок 2.3 – Інтерфейс Hyper-V Manager

В Hyper-V Manager під’єднано сервер з назвою WINSRVHYPER-V, який виконує роль гіпервізора для кількох віртуальних машин. Цей інструмент дозволяє адміністратору здійснювати повний контроль над віртуальним середовищем, забезпечуючи управління віртуальними машинами, мережевими налаштуваннями та ресурсами. Доступні налаштування також включають управління мережевими комутаторами (Virtual Switch Manager) і віртуальними сховищами (Virtual SAN Manager). Панель дій також дозволяє виконувати

операції з віртуальними машинами, наприклад, запуск, зупинку, експортування, зміну конфігурації або видалення.

2.3 Брандмауер pfSense

Брандмауер pfSense заснований на операційній системі FreeBSD. Він поєднує функції брандмауера та маршрутизатора, що робить його універсальним рішенням для забезпечення мережевої безпеки [26]. pfSense відомий своєю високою продуктивністю, стабільністю та багатим набором функцій, які можуть задовольнити потреби як малих організацій, так і великих корпоративних мереж. pfSense забезпечує ефективний захист мережі, працюючи як боандмауер із функціями глибокого аналізу трафіку. Він підтримує stateful режим роботи, що дозволяє відслідковувати стан кожного з'єднання та приймати рішення про його дозвіл чи блокування на основі попередньо визначених правил. Завдяки цьому pfSense може блокувати небажаний трафік.

Однією з ключових переваг pfSense є його розширюваність через модулі (пакети). Наприклад, інтеграція системи запобігання вторгненням Suricata дозволяє реалізувати функції IPS. Suricata, встановлена на pfSense, аналізує вхідний і вихідний трафік у реальному часі, виявляючи підозрілу активність та блокуючи атаки. Це робить pfSense не лише брандмауером, але й ефективною платформою для моніторингу мережевих загроз.

Маршрутизатор pfSense підтримує всі сучасні мережеві функції, включаючи NAT (Network Address Translation), VPN (Virtual Private Network), VLAN (Virtual LAN), QoS (Quality of Service) і Load Balancing. NAT дозволяє керувати маршрутизацією трафіку між внутрішньою та зовнішньою мережами, приховуючи реальні IP-адреси внутрішніх хостів. VPN-функціональність підтримує протоколи OpenVPN, IPSec та WireGuard, що забезпечує безпечний віддалений доступ до мережі. VLAN дозволяє сегментувати мережу для підвищення її продуктивності та безпеки, а QoS - пріоритизувати трафік, що важливо для роботи додатків із високими вимогами до пропускної здатності, наприклад VoIP. pfSense також відзначається зручним веб-інтерфейсом для

управління, який дозволяє адміністратору легко створювати правила брандмауера, налаштовувати мережеві сервіси та моніторити стан мережі (див. рисунок 2.4).

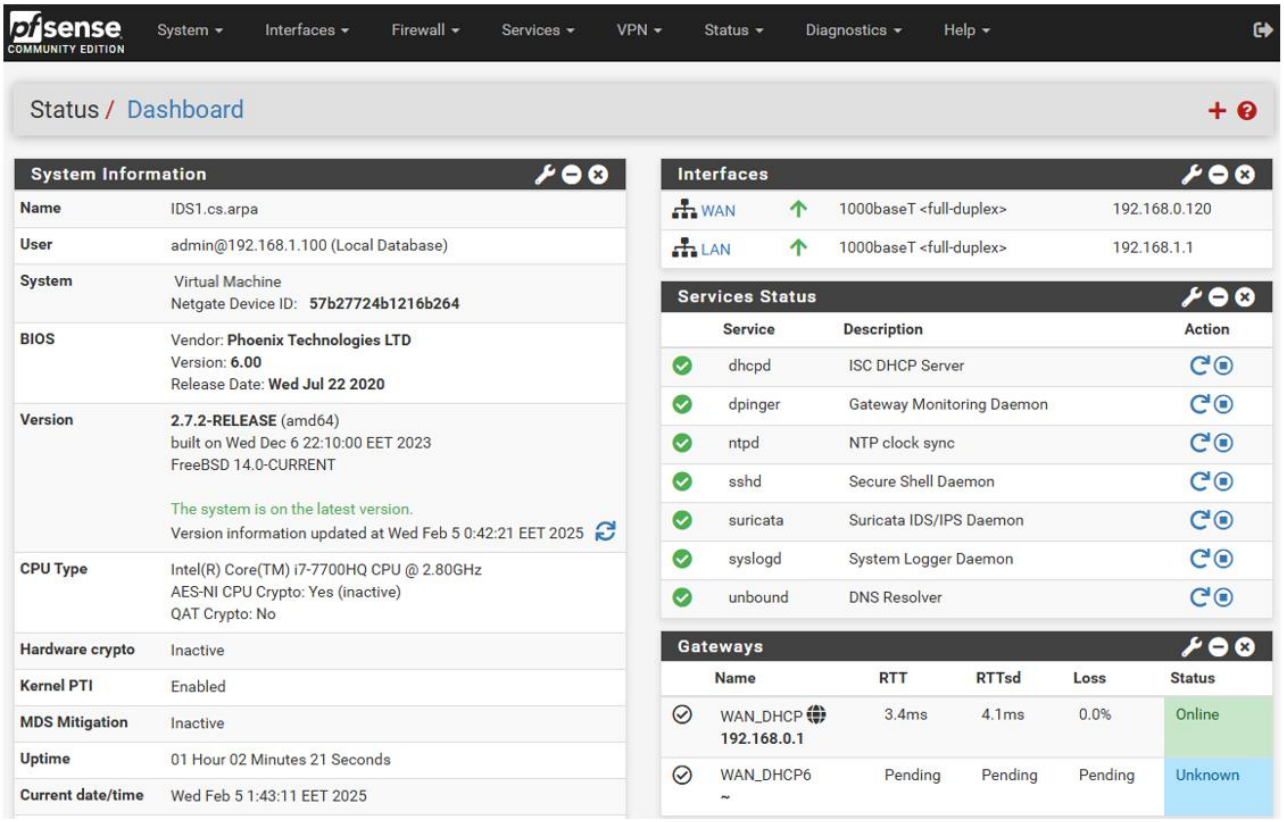


Рисунок 2.4 – Веб-інтерфейс pfSense

Крім того, pfSense підтримує доступ через SSH і консоль (див рисунок 2.5) для виконання розширених завдань.

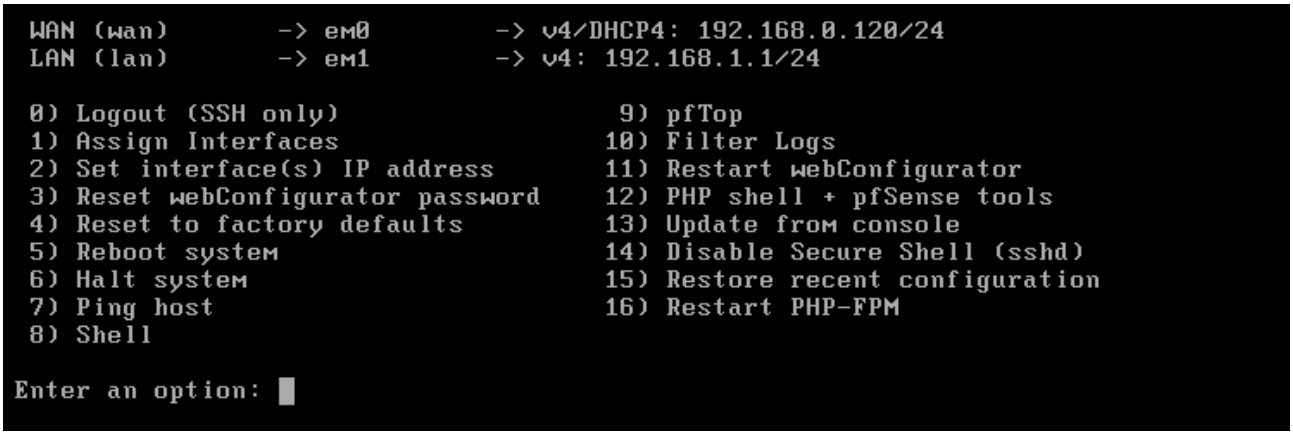


Рисунок 2.5 – Консоль pfSense

Брандмауер також підтримує функції логування та звітності. Він дозволяє записувати всі події, пов'язані з мережею, включаючи дозволені або заблоковані з'єднання. Ці журнали можуть бути проаналізовані для виявлення підозрілої активності, забезпечуючи детальний огляд роботи мережі. Завдяки підтримці SIEM-систем і зовнішніх серверів журналювання (наприклад, Syslog), pfSense легко інтегрується в існуючу інфраструктуру моніторингу безпеки.

На рисунку 2.6 показаний веб-інтерфейс брандмауера pfSense, а саме сторінка статистики DHCP-сервіса, яка містить інформацію про видані IP-адреси через DHCP.

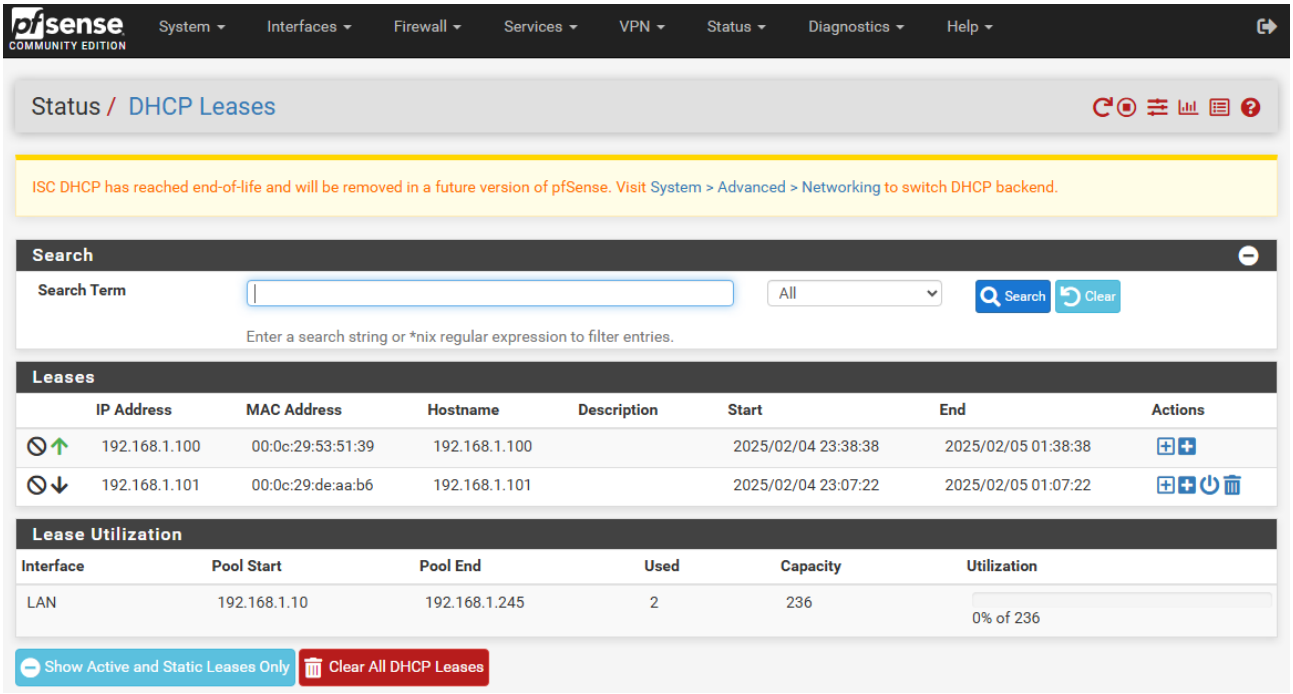


Рисунок 2.6 – Сторінка статистики DHCP-сервіса в pfSsense

Цей інтерфейс дозволяє адміністратору легко контролювати розподіл IP-адрес у мережі, перевіряти стан підключень клієнтів.

На рисунку 2.7 показано веб-інтерфейс брандмауера pfSense, сторінка налаштувань IPS Suricata.

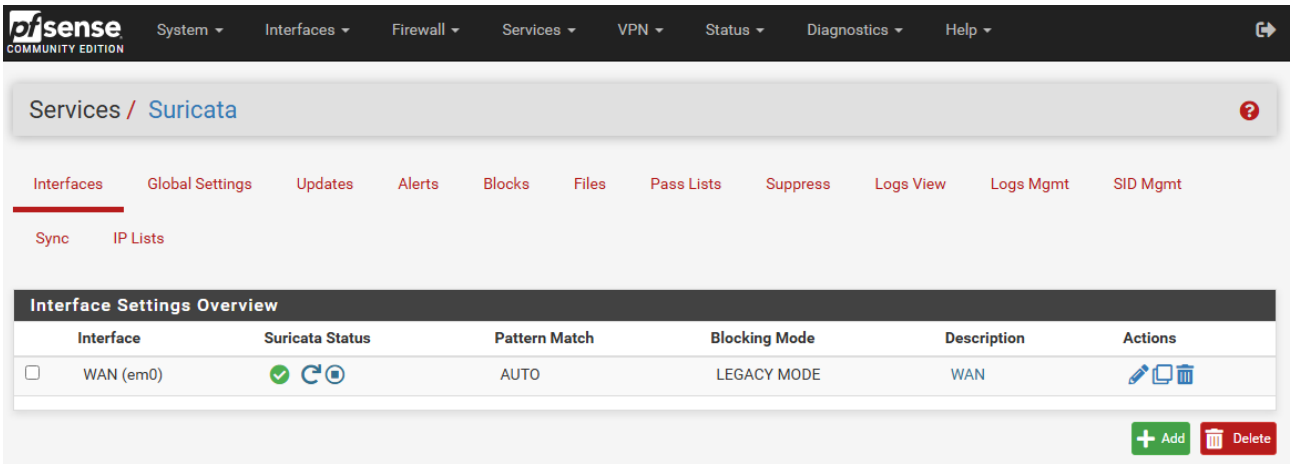


Рисунок 2.7 – Статус IPS Suricata в pfSsense

Цей інтерфейс забезпечує простий доступ до конфігурації та дозволяє легко адаптувати Suricata до потреб мережі [27]. У нашому прикладі система налаштована для роботи на інтерфейсі WAN.

На рисунку 2.8 представлений розділ Alert and Block Settings IPS Suricata.

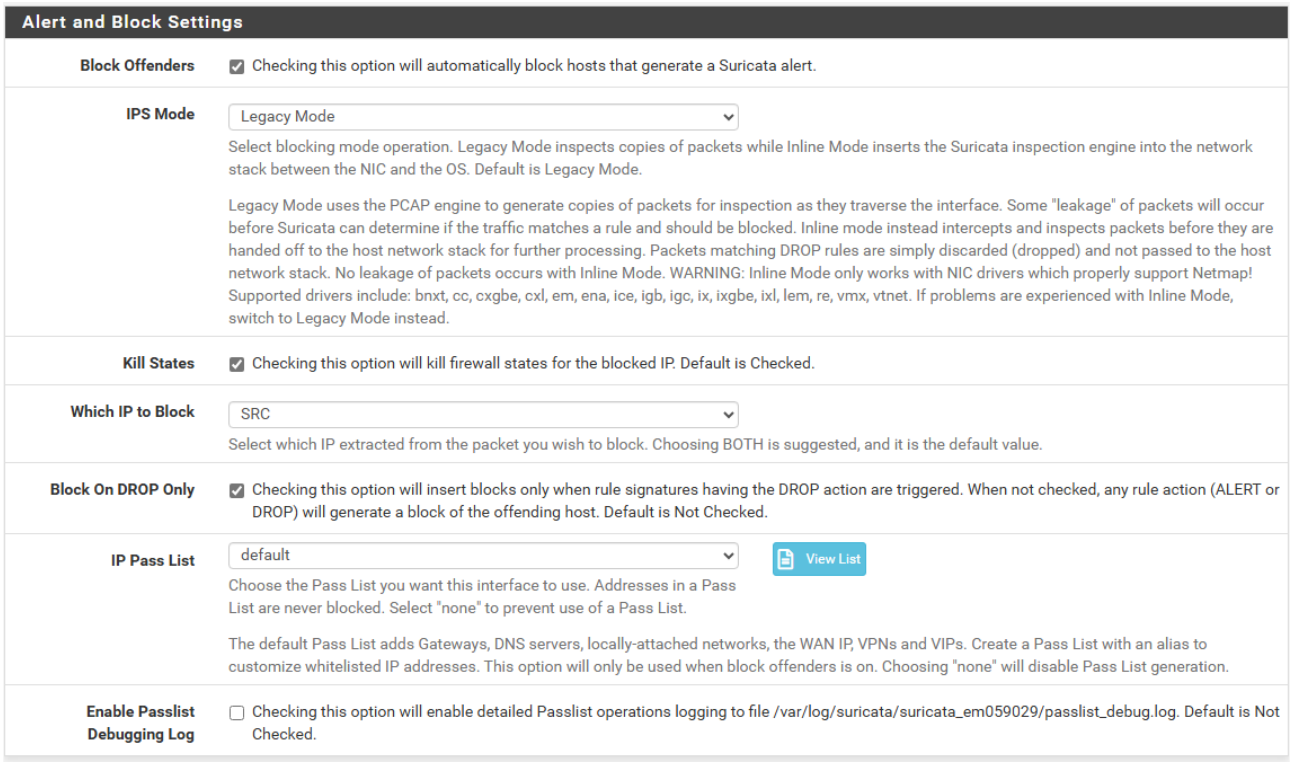


Рисунок 2.8 – Розділ Alert and Block Settings IPS Suricata

Цей розділ дозволяє конфігурувати параметри блокування підозрілих дій і реагування системи на виявлені загрози.

Увімкнена опція автоматичного блокування IP-адрес хостів, які генерують події (alerts) Suricata. Це означає, що якщо Suricata виявить підозрілий або шкідливий трафік, IP-адреса джерела буде додана до списку блокувань.

В IPS Mode обраний режим роботи Legacy Mode. У цьому режимі Suricata створює копії пакетів для аналізу, використовуючи механізм PCAP. Якщо пакет вважається шкідливим, його блокування виконується за допомогою брандмауера. Legacy Mode є стандартним режимом, але він може пропускати незначну частину трафіку до моменту, коли Suricata визначить, чи є він шкідливим. Режим Inline Mode інтегрує Suricata безпосередньо в мережевий стек, але вимагає відповідних драйверів для підтримки Netmap.

Опція Kill States дозволяє видаляти активні стани (states) брандмауера для IP-адрес, які були заблоковані Suricata. Це гарантує, що навіть існуючі з'єднання від будуть негайно розірвані. Suricata блокує IP-адресу джерела підозрілого трафіку. Це варіант, що дозволяє запобігти новим з'єднанням із джерела. Існує також можливість блокувати інші IP-адреси, наприклад, обидві сторони з'єднання. Pass List визначає IP-адреси, які Suricata ніколи не блокує.

На рисунку 2.9 показаний інтерфейс налаштування наборів правил (rulesets) для IPS Suricata в pfSense.

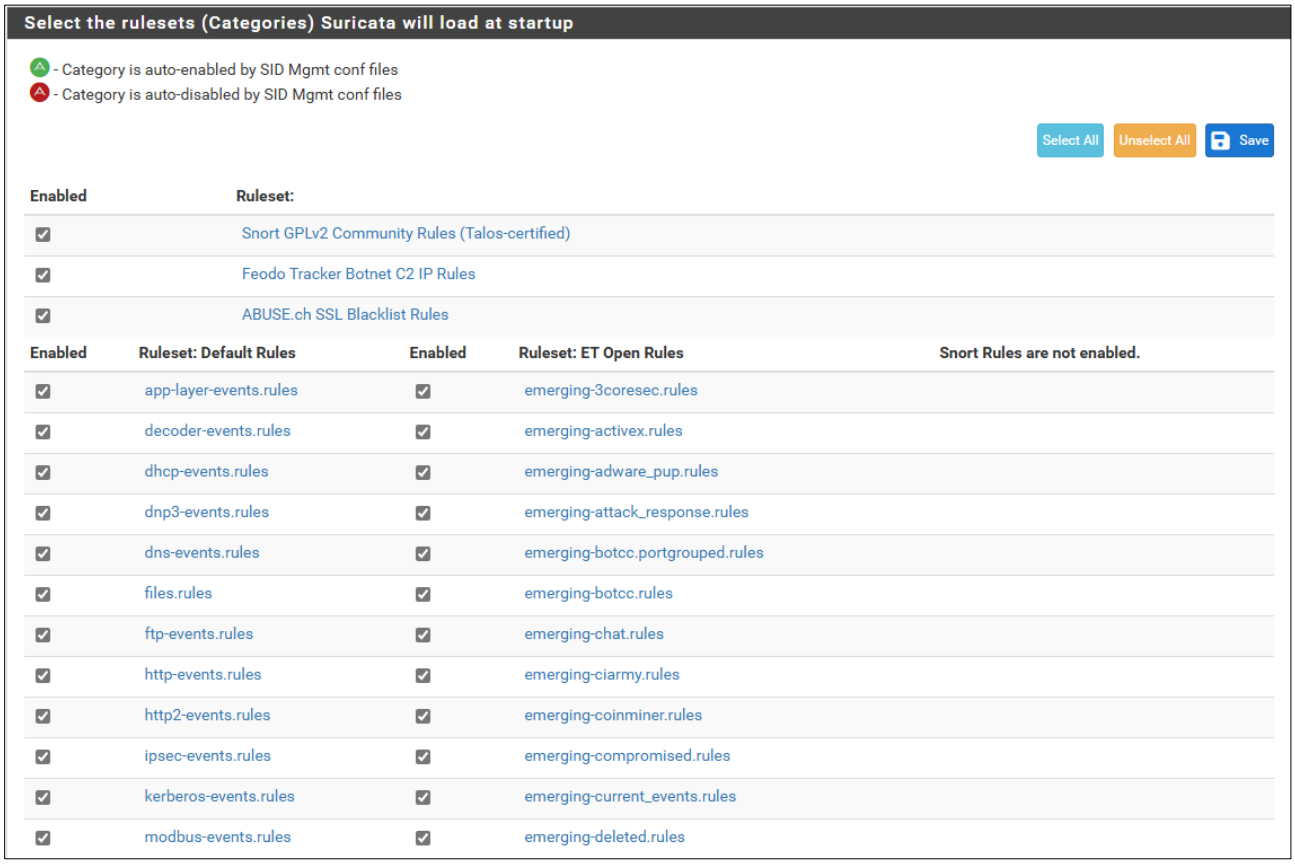


Рисунок 2.9 – Інтерфейс налаштування наборів правил IPS Suricata

Цей розділ дозволяє адміністратору вибирати, які категорії правил будуть завантажені та використовуватися Suricata під час запуску для аналізу мережевого трафіку.

Вибрано як базові набори, так і спеціалізовані правила, такі як правила Feodo Tracker або ABUSE.ch SSL Blacklist, які зосереджені на певних типах загроз, наприклад, ботнетах або шкідливих сертифікатах SSL. ET Open Rules (Emerging Threats Open) - це додаткові правила, спрямовані на виявлення нових загроз. Вибір конкретних правил залежить від потреб мережі, що дозволяє зосередитися на найбільш критичних аспектах безпеки.

2.4 Вразлива ОС Metasploitable VM

Metasploitable VM - це спеціально створена віртуальна машина, яка використовується для тестування вразливостей, навчання кібербезпеці та моделювання атак у контрольованому середовищі [28]. Вона базується на

операційній системі Ubuntu Linux і включає свідомо вразливі служби, додатки та конфігурації, що дозволяють моделювати різноманітні кібератаки. Ця ОС є ідеальним інструментом для роботи з платформою для створення та тестування експлойтів, і широко використовується фахівцями з кібербезпеки, студентами й адміністраторами мереж для навчання методам тестування на проникнення.

Metasploitable VM містить вразливі мережеві служби, такі як FTP (vsftpd), SSH, MySQL, Telnet і Apache, які можна експлуатувати для отримання несанкціонованого доступу. У складі системи також присутні веб-додатки, такі як Mutillidae та Damn Vulnerable Web Application (DVWA), які дозволяють відпрацьовувати веб-атаки, включаючи SQL, XSS і CSRF. Операційна система включає версії ядра Linux з відомими вразливостями, які підходять для тестування методів ескалації привілеїв. Це забезпечує можливість перевірки, як зловмисники можуть отримати доступ до облікових записів із підвищеними правами. Metasploitable також дозволяє моделювати складні сценарії атак, такі як brute force для підбору паролів, атаки типу DoS, а також використання експлойтів для компрометації систем. Завдяки підтримці таких інструментів, як Metasploit, Nmap, Nessus і Burp Suite, система забезпечує інтегроване середовище для моделювання реальних атак і вивчення захисних стратегій. Важливою особливістю є безпечне локальне розгортання цієї системи, яка працює у віртуальному середовищі, що забезпечує повну ізоляцію від реальних мереж (див. рисунок 2.10).

Рисунок 2.10 – Консоль Metasploitable VM

Вона не призначена для використання у відкритих або продуктивних мережах, оскільки її вразливості можуть бути використані зловмисниками.

Metasploitable є ідеальною платформою для вивчення роботи систем IPS Suricata. Трафік, який генерується атакуючим хостом Kali Linux може бути проаналізований і заблокований, що дозволяє оцінити ефективність захисних механізмів. Metasploitable VM надає можливість навчатися й відпрацьовувати сучасні методи атак у контрольованих умовах, що робить її цінним інструментом для спеціалістів із кібербезпеки.

2.5 Операційна система Kali Linux

Kali Linux - це спеціалізована операційна система на основі Debian, розроблена для фахівців з кібербезпеки, тестування на проникнення (penetration testing) і цифрової криміналістики [29]. Вона створена розробниками Offensive Security і включає велику кількість попередньо встановлених інструментів для аналізу мереж, пошуку вразливостей, атак і розслідування інцидентів. Kali Linux широко використовується в навчальних і професійних середовищах, де необхідно тестувати системи безпеки та досліджувати сучасні загрози.

Операційна система має зручний дизайн, оптимізований для спеціалізованих завдань у сфері кібербезпеки. Kali Linux містить велику кількість попередньо встановлених інструментів для різних аспектів кібербезпеки.

У контексті лабораторного середовища Kali Linux виступає атакуючою стороною, яка дозволяє імітувати широкий спектр шкідливих дій. Вона надає користувачам усі необхідні інструменти для аналізу мережевих вразливостей, проведення атак і оцінки ефективності засобів захисту, таких як системи IPS. У лабораторних умовах Kali Linux використовується для ініціації атак на цільову систему Metasploitable VM. Завдяки вбудованим інструментам, таким як Nmap, Metasploit Framework і Hydra, Kali Linux дозволяє проводити сканування мережі,

виявляти відкриті порти, тестувати слабкі паролі та експлуатувати вразливості в мережевих службах. Це робить її ідеальною платформою для вивчення та практики таких методів атак, як brute force та інші. Kali Linux використовується для перевірки ефективності системи IPS Suricata, встановленої на pfSense. Вона генерує шкідливий трафік, який проходить через IPS, дозволяючи оцінити, чи система здатна виявляти та блокувати атаки. Завдяки таким інструментам, як hping3, можна моделювати DDoS-атаки, перевіряючи, наскільки добре IPS фільтрує аномальний трафік.

Kali Linux використовується також для автоматизації тестування безпеки, що є важливим у великих мережах. За допомогою скриптів на Python і Bash можна створювати автоматизовані сценарії для виконання серій атак, що спрощує процес навчання та дослідження. Це особливо корисно для відтворення складних сценаріїв атак і оцінки ефективності захисту за різних умов.

2.6 Висновки до другого розділу

В другому розділі було описано процес створення лабораторного середовища для тестування ефективності системи IPS. Детально розглянуто всі ключові компоненти середовища, включаючи гіпервізор Hyper-V на базі Windows Server 2022 Core, брандмауер pfSense із інтегрованою IPS Suricata, атакуючу систему Kali Linux, а також вразливу операційну систему Metasploitable VM. Було також описано зв’язок між цими компонентами через віртуальний комутатор, що ілюструє архітектуру тестового середовища. Детально розглянуто режими роботи IPS, функції Pass List і можливості налаштування наборів правил для адаптації системи до різних типів атак.

Створена інфраструктура є повноцінною платформою для тестування та аналізу кіберзагроз. Лабораторне середовище дозволяє досліджувати ефективність IPS Suricata у реальних сценаріях атак, оптимізувати її налаштування та адаптувати до різних типів загроз.

РОЗДІЛ 3 ТЕСТУВАННЯ ЕФЕКТИВНОСТІ IPS SURICATA

3.1 Проведення тестових атак на Metasploitable VM

3.1.1 Сканування відкритих портів

Сканування відкритих портів на Metasploitable VM з використанням Kali Linux є початковим етапом у тестуванні на проникнення, що дозволяє визначити доступні мережеві служби на цільовій системі. У Kali Linux було використано Nmap, який надає можливість виконувати різні типи сканування мережі. Metasploitable VM, як свідомо вразлива операційна система, містить великий спектр відкритих портів і сервісів, що дозволяє практикувати різноманітні методи атак. В Додатку А наведено результати сканування відкритих TCP та UDP портів.

Результати сканування портів Metasploitable VM демонструють широкий спектр відкритих TCP та UDP портів, а також інформацію про служби, що працюють на цих портах. Використання інструмента Nmap дозволило отримати детальну інформацію про активні мережеві сервіси, їх версії та супутні уразливості.

Для TCP-сервісів виконано сканування з параметрами -p-, -sV, -A, які забезпечують виявлення всіх доступних портів (від 1 до 65535), визначення версій сервісів та глибший аналіз їхніх функціональних можливостей. ля UDP-сервісів виконано сканування з параметром –sU. Результати сканування вказують на використання старих версій програмного забезпечення на Metasploitable VM, багато з яких мають добре відомі уразливості.

Результати сканування використовуються для подальших етапів тестування, таких як експлуатація вразливостей. Процес сканування відкритих портів на Metasploitable VM із Kali Linux є базовим етапом тестування, який дає змогу зрозуміти структуру цільової системи, ідентифікувати слабкі місця та розробити подальші дії для оцінки ефективності захисних механізмів.

3.1.2 Flood атаки

Атака SYN Flood - це одна з форм атак типу DDoS, спрямована на виснаження ресурсів сервера або мережевого пристрою шляхом перевантаження його великою кількістю напіввідкритих з'єднань. Вона використовує уразливість протоколу TCP, пов’язану з процесом встановлення з'єднання. Атакуючий надсилає велику кількість SYN-пакетів до сервера-цілі, але не завершує тристоронній процес рукостискання, залишаючи сервер із великою кількістю відкритих з'єднань у стані очікування. Це може призвести до перевантаження таблиці з'єднань сервера, виснаження його ресурсів і недоступності для легітимних користувачів.

Для реалізації атаки SYN Flood з використанням Kali Linux було використано hping3. Інструмент hping3 дозволяє створювати змінені пакети TCP для проведення атаки.

На рисунку 3.1 відображено термінал Kali Linux із виконанням команди для запуску атаки SYN Flood за допомогою утиліти hping3 [30].

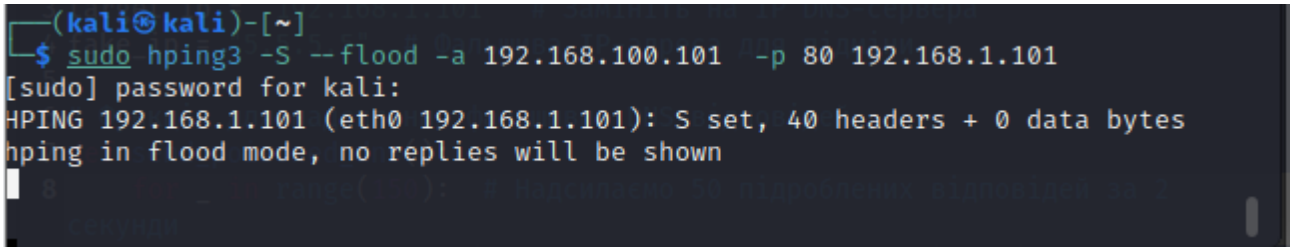


Рисунок 3.1 – Атака типу SYN Flood з Kali Linux

Команда ініціює надсилання SYN-пакетів до цільової системи з IP-адресою 192.168.1.101, спрямованих на порт 80. Опція -S активує генерацію SYN-пакетів, а параметр --flood забезпечує режим інтенсивного надсилання без очікування відповіді, створюючи максимальне навантаження на цільовий сервер. Спуфінг джерела трафіку реалізовано через опцію -a, яка встановлює IP-адресу відправника як 192.168.100.101, що ускладнює відстеження реального джерела атаки. Цільова система Metasploitable VM опиняється під значним

навантаженням через неможливість завершити тристоронній процес встановлення TCP-з'єднання.

На рисунку 3.2 представлено журнал подій, згенерований системою Suricata. Записи в журналі відображають сповіщення, пов’язані з атакою SYN Flood.

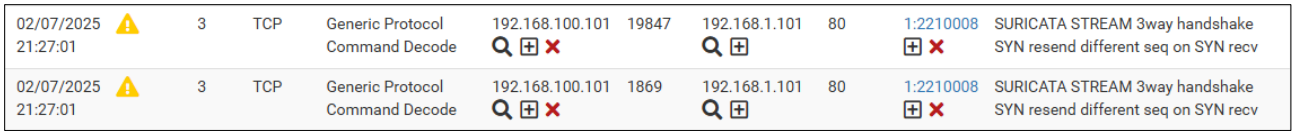


Рисунок 3.2 – Сповіщення про SYN Flood атаку

IPS Suricata виявила аномалії, пов’язані з TCP-з’єднаннями. Тип протоколу визначено як TCP, а опис події зазначає, що проблема стосується процесу тристороннього рукостискання (3-way handshake). IPS Suricata виявила повторну відправку SYN-пакетів із різними порядковими номерами (sequence numbers) під час отримання SYN-пакета. Така поведінка характерна для атак типу SYN Flood, де атакуючий надсилає великий обсяг SYN-пакетів, але не завершує тристоронній процес встановлення з’єднання. Джерело трафіку в обох записах має IP-адресу 192.168.100.101. Це IP-адреса, яка була підставлена (спуфінг) під час атаки за допомогою Kali Linux. Призначенням трафіку є цільовий сервер із IP-адресою 192.168.1.101, який працює на порту 80 (HTTP).

На рисунку 3.3 представлено деталі правила Suricata, яке відповідає за виявлення аномалій у процесі тристороннього рукостискання TCP.

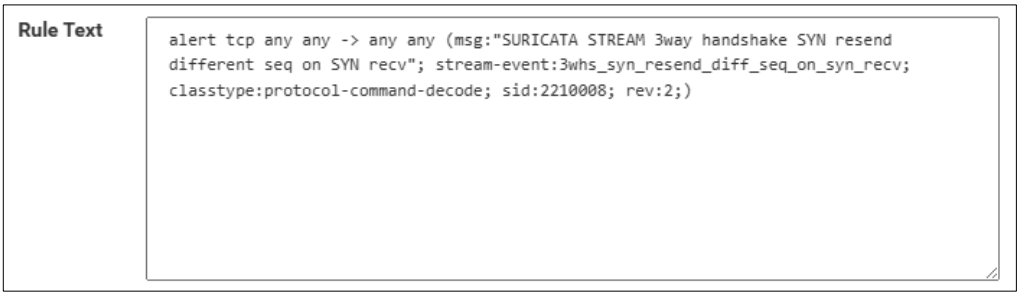


Рисунок 3.3 – Правило IPS Suricata для виявлення аномалій в SYN пакетах

Правило працює з протоколом TCP і активується, якщо трафік відповідає зазначеним критеріям.

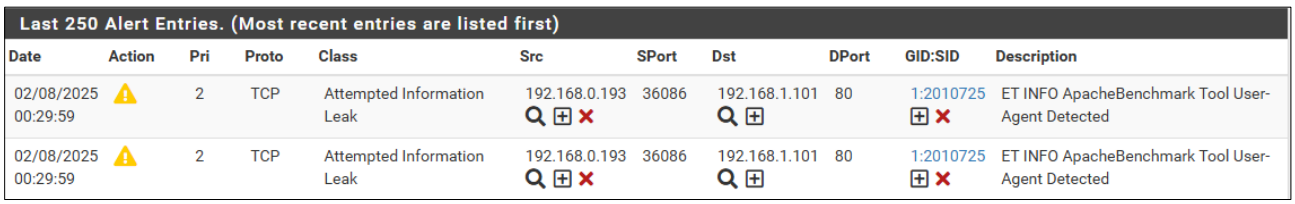
На рисунку 3.4 показано виконання команди в терміналі Kali Linux для тестування продуктивності веб-сервера, розгорнутого на Metasploitable VM, за допомогою інструмента ApacheBench (ab) [31].

Рисунок 3.4 – Тестування продуктивності веб-сервера

Згідно з конфігурацією, сервер обробляє 10 000 HTTP-запитів із 100 паралельними з'єднаннями. Цей тест дозволяє оцінити, як веб-сервер реагує на високі навантаження та чи витримує він велику кількість одночасних запитів.

Цей сценарій був використаний для перевірки ефективності системи запобігання вторгненням IPS Suricata. Таке тестування дозволяє оцінити стійкість веб-сервера до навантаження, виявити його потенційні вузькі місця, а також перевірити, чи здатна IPS-система правильно ідентифікувати легітимний трафік, відрізняючи його від атак на доступність. У нашому випадку HTTP flood.

На рисунку 3.5 відображено журнал подій Suricata з інформацією про зафіксовану активність, пов’язану з інструментом ApacheBench.



Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/08/2025 00:29:59	⚠	2	TCP	Attempted Information Leak	192.168.0.193	36086	192.168.1.101	80	1:2010725	ET INFO ApacheBenchmark Tool User-Agent Detected
02/08/2025 00:29:59	⚠	2	TCP	Attempted Information Leak	192.168.0.193	36086	192.168.1.101	80	1:2010725	ET INFO ApacheBenchmark Tool User-Agent Detected

Рисунок 3.5 – Сповіщення про виявлення інструменту ApacheBench

Suricata ідентифікувала трафік на основі User-Agent, який надсилається ApacheBench під час HTTP-запитів. Цей User-Agent специфічний і легко розпізнається, що дозволяє Suricata точно визначити джерело автоматизованого трафіку. Інструмент ApacheBench використовується для стрес-тестування веб-серверів, але така активність може бути помилково сприйнята як загроза, якщо вона створює надмірне навантаження, схоже на DoS-атаку.

Ця подія демонструє, як Suricata здатна виявляти навіть легітимний, але специфічний трафік, який можна використовувати для перевірки працездатності або стабільності веб-сервера. Це також підкреслює важливість правильного налаштування правил Suricata, щоб уникнути надмірного блокування легітимної активності під час тестування в контрольованому середовищі.

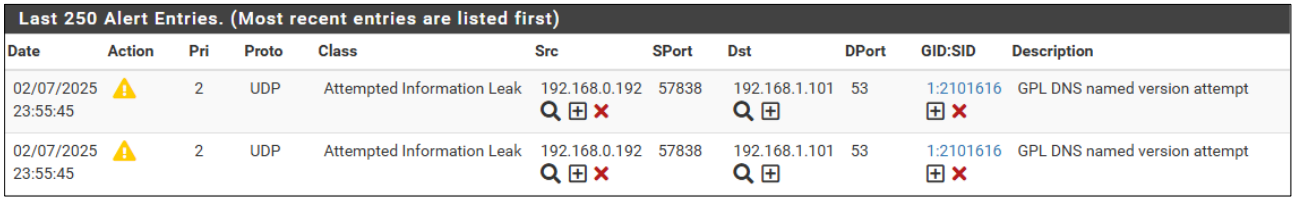
3.1.2 Атаки на DNS сервіс

Атаки на DNS-сервіс є одним із поширених способів зловмисників впливати на функціонування мереж і маніпулювати запитами користувачів. DNS - це критично важлива служба, яка забезпечує перетворення доменних імен на IP-адреси. Зловмисники можуть використовувати уразливості або помилки в конфігурації DNS для реалізації різних атак.

Команда `dig @192.168.1.101 -p 53 CHAOS TXT version.bind` використовується для отримання інформації про DNS-сервер. Вона надсилає спеціальний запит до DNS-сервера використовуючи запит типу CHAOS TXT. Цей запит з’ясовує версію програмного забезпечення DNS-сервера. Якщо сервер неправильно налаштований, він може розкрити цю інформацію, що дозволяє зловмисникам ідентифікувати можливі вразливості. Якщо сервер працює на старій версії програмного забезпечення зловмисники можуть використовувати відомі уразливості для отримання доступу або відмови в обслуговуванні.

Якщо сервер відповідає з точним номером версії, це може вказувати на потенційну уразливість. Правильно налаштований сервер DNS зазвичай відмовляється надавати таку інформацію або видає узагальнені відповіді.

На рисунку 3.6 відображено журнал подій системи запобігання вторгненням Suricata, який фіксує спроби доступу до інформації про версію DNS-сервера.



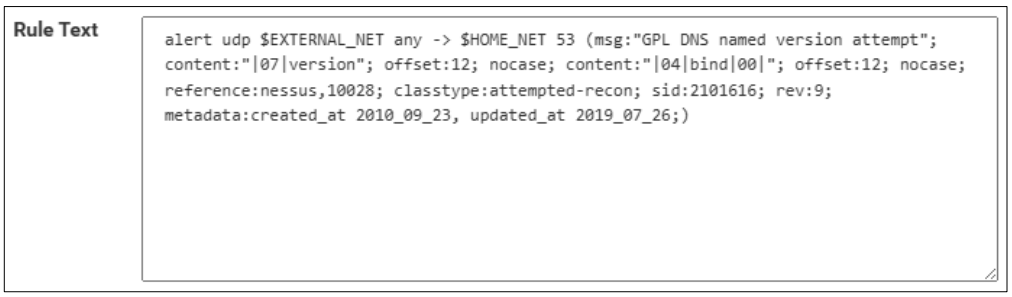
Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/07/2025 23:55:45	⚠	2	UDP	Attempted Information Leak	192.168.0.192	57838	192.168.1.101	53	1:2101616	GPL DNS named version attempt
02/07/2025 23:55:45	⚠	2	UDP	Attempted Information Leak	192.168.0.192	57838	192.168.1.101	53	1:2101616	GPL DNS named version attempt

Рисунок 3.6 – Сповіщення про спроби доступу до інформації про версію DNS-сервера

IPS Suricata зафіксувала ці події як спроби витоку інформації. Спроба отримати інформацію про версію DNS-сервера є першим кроком зловмисника для виявлення вразливостей. Suricata продемонструвала свою ефективність у виявленні запиту, захищаючи сервер від можливої компрометації.

На рисунку 3.7 представлено текст правила Suricata, яке відповідає за виявлення спроб визначення версії DNS-сервера.



Rule Text

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"GPL DNS named version attempt";
content:"|07|version"; offset:12; nocase; content:"|04|bind|00|"; offset:12; nocase;
reference:nessus,10028; classtype:attempted-recon; sid:2101616; rev:9;
metadata:created_at 2010_09_23, updated_at 2019_07_26;)
```

Рисунок 3.7 – Правило IPS Suricata для виявлення спроб визначення версії DNS-сервера

Це правило дозволяє виявляти спроби зловмисників визначити версію DNS-сервера за допомогою запиту CHAOS TXT. Suricata використовує це правило для виявлення та блокування таких запитів, що допомагає запобігти витоку інформації та підвищує безпеку мережі.

На рисунку 3.8 представлений код python, який використовує бібліотеку Scapy для створення та надсилання DNS-запиту на передачу зони (AXFR).

```python
from scapy.all import *

target_dns = "192.168.1.101"
domain = "test.com"

# AXFR (Zone Transfer)
dns_query_udp = IP(dst=target_dns)/UDP(dport=53)/DNS(rd=1,
  qd=DNSQR(qname=domain, qtype="AXFR"))

#
send(dns_query_udp)
```

Рисунок 3.8 – Код python для створення та надсилання DNS-запиту на передачу зони (AXFR)

Такий запит є важливим у контексті аналізу вразливостей DNS-сервісів, оскільки неправильна конфігурація DNS-сервера може дозволити неавторизованим клієнтам отримати всю інформацію про DNS-зону.

DNS-запит типу AXFR використовується для передачі всієї зони DNS, яка містить інформацію про домени, IP-адреси, поштові сервери та інші записи. Якщо DNS-сервер налаштований неправильно і дозволяє передачу зони неавторизованим клієнтам, це може призвести до витоку конфіденційної інформації про інфраструктуру мережі. У разі успіху зловмисник отримує доступ до всієї інформації про зону, яку може використати для підготовки інших атак, таких як фішинг, DNS-спуфінг або компрометація внутрішніх ресурсів.

На рисунку 3.9 показано журнал подій системи Suricata, який зафіксував спроби передачі зони DNS (DNS Zone Transfer) за допомогою UDP-запитів.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/07/2025 23:38:28	⚠	2	UDP	Attempted Information Leak	192.168.0.191	53	192.168.1.101	53	1:2101948	GPL DNS zone transfer UDP
02/07/2025 23:38:28	⚠	2	UDP	Attempted Information Leak	192.168.0.191	53	192.168.1.101	53	1:2101948	GPL DNS zone transfer UDP

Рисунок 3.9 – Сповіщення про спроби передачі зони DNS (DNS Zone Transfer)

Ці події класифікуються як спроби витоку інформації (Attempted Information Leak).

Передача зони DNS (AXFR) - це механізм, що дозволяє отримувати повну інформацію про записи DNS-зони. Вона зазвичай використовується для синхронізації даних між основним і вторинним DNS-серверами. Однак вразливі

або неправильно налаштовані DNS-сервери можуть дозволяти виконання запитів AXFR неавторизованим клієнтам, що може призвести до витоку інформації про внутрішню мережеву структуру. IPS Suricata розпізнала ці запити як потенційну загрозу та автоматично заблокувала їх, запобігаючи передачі інформації.

На рисунку 3.10 показано текст правила Suricata, яке використовується для виявлення спроб передачі зони DNS (AXFR) через протокол UDP.

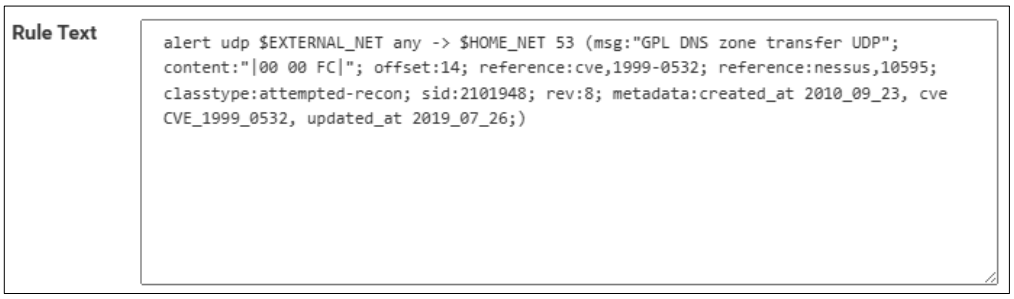


Рисунок 3.10 – Правило IPS Suricata для виявлення спроб передачі зони DNS (AXFR) через протокол UDP

Правило застосовується до UDP-трафіку, що надходить із зовнішньої мережі ($EXTERNAL_NET) з будь-якого порту (any) і спрямований до домашньої мережі ($HOME_NET) на порт 53 (стандартний порт DNS). У тілі пакета шукається специфічний байтовий патерн (00 00 FC), який є частиною DNS-запиту типу AXFR. Поле offset:14 вказує, що пошук цього вмісту починається з 14-го байта пакета. Класифікація події як спроби розвідки (reconnaissance) вказує на активність пов’язану з отриманням конфіденційної інформації.

3.1.3 Brute force атаки

Brute force атаки - це метод злому паролів для отримання доступу до системи шляхом перебору можливих комбінацій облікових даних. Зазвичай цей підхід застосовується до сервісів, які використовують автентифікацію, таких як Telnet, FTP, Rlogin та інші.

Команда `hydra -l root -P /home/kali/pass.txt -t 4 192.168.1.101 telnet` використовується для виконання brute force атаки на Telnet-сервіс, розгорнутий на хості з IP-адресою 192.168.1.101. Інструмент Hydra автоматизує перебір паролів для заданого облікового запису [32]. У цьому випадку цільовим користувачем є root. Hydra послідовно надсилає запити для автентифікації до Telnet-сервісу, використовуючи обліковий запис root та паролі зі списку /home/kali/pass.txt. У разі успішного збігу облікових даних, Hydra виводить знайдену комбінацію в консоль.

На рисунку 3.11 відображено журнал подій системи Suricata, яка зафіксувала спроби brute force атаки на сервіс Telnet.

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/08/2025 00:46:18	⚠	2	TCP	Potentially Bad Traffic	192.168.1.101	23	192.168.0.194	46016	1:2101251	GPL TELNET Bad Login
02/08/2025 00:46:18	⚠	2	TCP	Potentially Bad Traffic	192.168.1.101	23	192.168.0.194	46016	1:2101251	GPL TELNET Bad Login
02/08/2025 00:46:18	⚠	2	TCP	An attempted login using a suspicious username was detected	192.168.1.101	23	192.168.0.194	46016	1:2100719	GPL TELNET root login
02/08/2025 00:46:18	⚠	2	TCP	An attempted login using a suspicious username was detected	192.168.1.101	23	192.168.0.194	46016	1:2100719	GPL TELNET root login

Рисунок 3.11 – Сповіщення про спроби brute force атаки на сервіс Telnet

Правило Suricata на рисунку 3.12 призначене для виявлення невдалих спроб входу через Telnet.

Rule Text

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"GPL TELNET Bad Login";
flow:established,to_client; content:"Login incorrect"; nocase; fast_pattern;
classtype:bad-unknown; sid:2101251; rev:11; metadata:created_at 2010_09_23,
updated_at 2024_03_08;)
```

Рисунок 3.12 – Правило IPS Suricata для виявлення невдалих спроб входу через Telnet

Воно активується, коли в мережевому трафіку, пов’язаному з протоколом Telnet (TCP порт 23), виявляється текстове повідомлення "Login incorrect", яке вказує на невдалу спробу автентифікації.

Правило Suricata на рисунку 3.13 спрямоване на виявлення підозрілих спроб входу через сервіс Telnet із використанням імені користувача root.

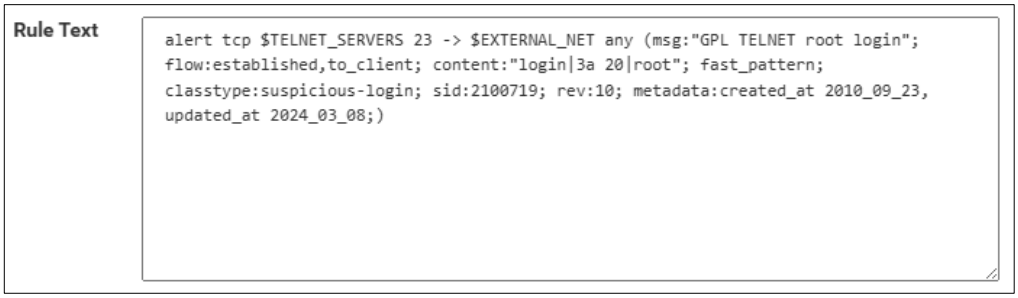


Рисунок 3.13 – Правило IPS Suricata для виявлення спроб входу з використанням імені користувача root

Це правило використовується для виявлення спроб входу до системи через Telnet із використанням облікового запису адміністратора root. Такі спроби часто є частиною brute force атак, спрямованих на злам систем із застосуванням стандартних або слабких паролів. Команда `hydra -l root -P /home/kali/pass.txt -t 4 192.168.1.101 ftp` використовується для проведення brute force атаки на FTP-сервер, розташований за IP-адресою 192.168.1.101. Ця команда виконує автоматизовану перевірку різних паролів для облікового запису root, намагаючись отримати доступ до сервісу FTP.

У представлених даних на рисунку 3.14 в журналі Suricata зафіксовано події, які вказують на спробу атаки типу brute force на FTP-сервер за допомогою облікового запису root.

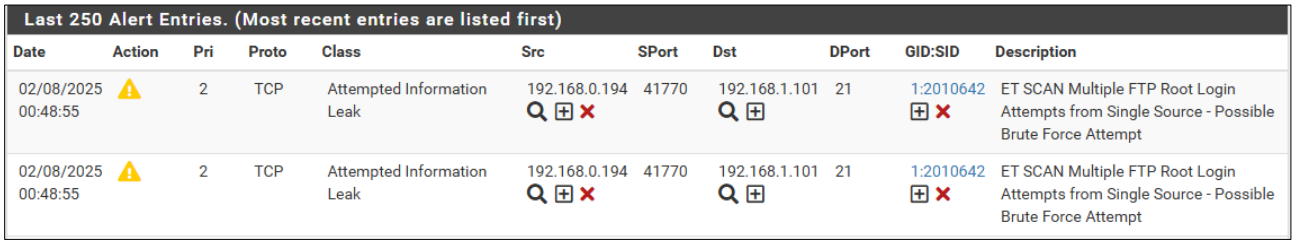


Рисунок 3.14 – Сповіщення про спроби brute force атаки на сервіс FTP

Правило Suricata, яке відповідає за виявлення багаторазових спроб входу на FTP-сервер із використанням облікового запису root представлено на рисунку 3.15.

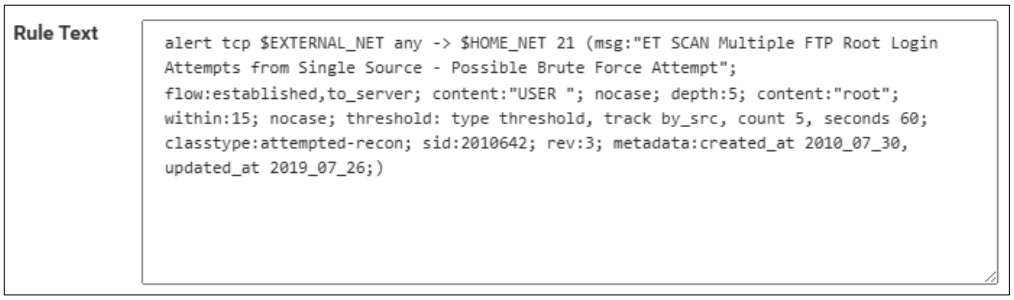


Рисунок 3.15 – Правило IPS Suricata для виявлення багаторазових спроб входу на FTP-сервер

Це правило дозволяє виявляти спроби brute force на FTP-сервер, орієнтуючись на багаторазові підключення із зазначенням користувача root. Воно спеціально розроблене для ситуацій, коли атаки надходять із одного джерела та можуть бути виявлені за кількістю спроб за короткий проміжок часу.

Команда `hydra -l root -P /home/kali/pass.txt -t 4 192.168.1.101 rlogin` використовується для виконання атаки типу brute force на сервіс rlogin (Remote Login) з метою зламу облікового запису root. У цьому випадку інструмент Hydra випробовує комбінації облікового запису root із паролями, які вказані у файлі /home/kali/pass.txt.

На рисунку 3.16 показано журнал подій Suricata де зафіксовано попередження про спроби атаки на сервіс rlogin із використанням облікового запису root. Дані свідчать про атаку типу brute force, спрямовану на отримання адміністративного доступу до цільової системи.

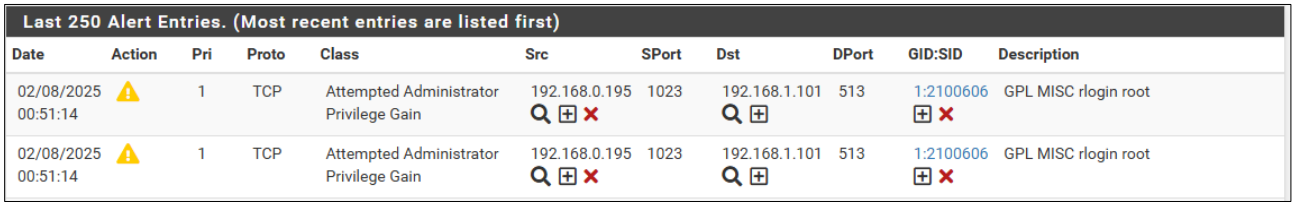


Рисунок 3.16 – Сповіщення про спроби brute force атаки на сервіс rlogin

Ця подія є типовою для brute force атаки, коли виконується багаторазовий підбір паролів для входу під обліковим записом root через rlogin.

На рисунку 3.17 показане правило Suricata, яке відповідає за виявлення атак brute force через сервіс rlogin із використанням облікового запису root.

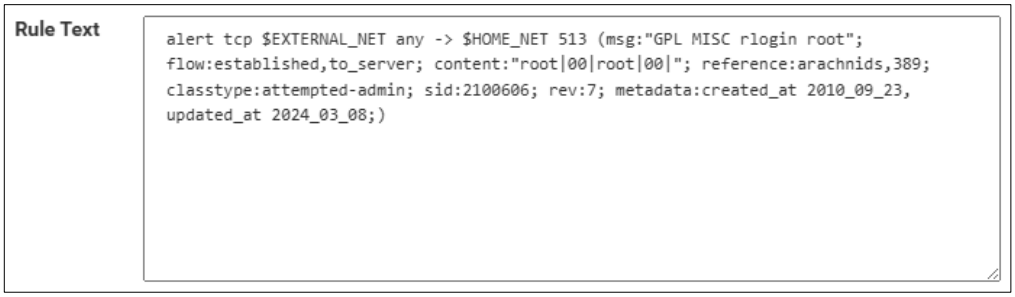


Рисунок 3.17 – Правило IPS Suricata для виявлення багаторазових спроб входу через сервіс rlogin

Це правило дозволяє Suricata виявляти підозрілу активність, пов'язану зі спробами brute force атак на сервіс rlogin. Suricata зафіксувала та класифікувала такі спроби як спробу підвищення привілеїв адміністратора, що створює загрозу для безпеки системи.

3.2 Аналіз результатів тестування

Аналіз результатів тестування системи IPS Suricata базується на оцінці її ефективності щодо виявлення та блокування різних сценаріїв атак у створеному лабораторному середовищі. Тестування включало моделювання кількох типів атак, таких як SYN Flood, brute force, атаки на DNS-сервіс і дослідження поведінки системи за умов аномального мережевого трафіку.

Для кожного сценарію проводився детальний аналіз роботи IPS, включаючи генерацію відповідного шкідливого трафіку з Kali Linux, обробку цього трафіку системою Suricata на брандмауері pfSense та вивчення створених журналів і сповіщень. Результати тестування SYN Flood показали, що Suricata успішно ідентифікувала аномальні спроби встановлення з'єднання (TCP SYN) і блокувала

їх, запобігаючи перевантаженню цільового сервера Metasploitable VM. У журналі подій були зафіксовані попередження про повторне надсилання SYN-пакетів із відхиленнями в параметрах. Це свідчить про ефективну роботу Suricata.

Під час brute force атак на сервіси Telnet, FTP і rlogin Suricata виявила багаторазові спроби входу з використанням облікового запису root. Правила побудовані на сигнатурному підході успішно класифікували ці дії як потенційні атаки на адміністративний доступ. У журналі подій зазначені відповідні сповіщення, що дозволило оперативно реагувати на такі загрози.

Атаки на DNS-сервіс, включаючи запити типу CHAOS TXT і Zone Transfer, також були ідентифіковані системою Suricata. У журналі подій фіксувалися попередження про можливу спробу інформаційного витоку. Це демонструє здатність IPS виявляти атаки, спрямовані на отримання конфіденційних даних про структуру мережі.

Тестування з використанням інструментів Apache Benchmark показало, що Suricata здатна розпізнати високий рівень активності як потенційно шкідливий. Це дозволяє вчасно відстежити аномальний трафік, спричинений Flood атаками.

Аналіз журналів Suricata показав, що більшість атак була виявлена завдяки правильно налаштованим сигнатурам і правил управління трафіком. Виявлення здійснювалося в режимі реального часу, а шкідливий трафік блокувався до досягнення цілі. Крім того, ефективність роботи системи не спричинила значного впливу на легітимний трафік.

На рисунку 3.18 представлено розділ блокування хостів (Blocked Hosts). Він відображає список IP-адрес, які були заблоковані системою Suricata через виявлення шкідливих дій або підозрілого трафіку. Кожне блокування пов'язане із конкретним правилом Suricata, позначеним його унікальним ідентифікатором (GID:SID). Адміністратор має можливість видалити блокування вручну. Це дозволяє швидко розблокувати IP-адреси, якщо вони були заблоковані помилково.

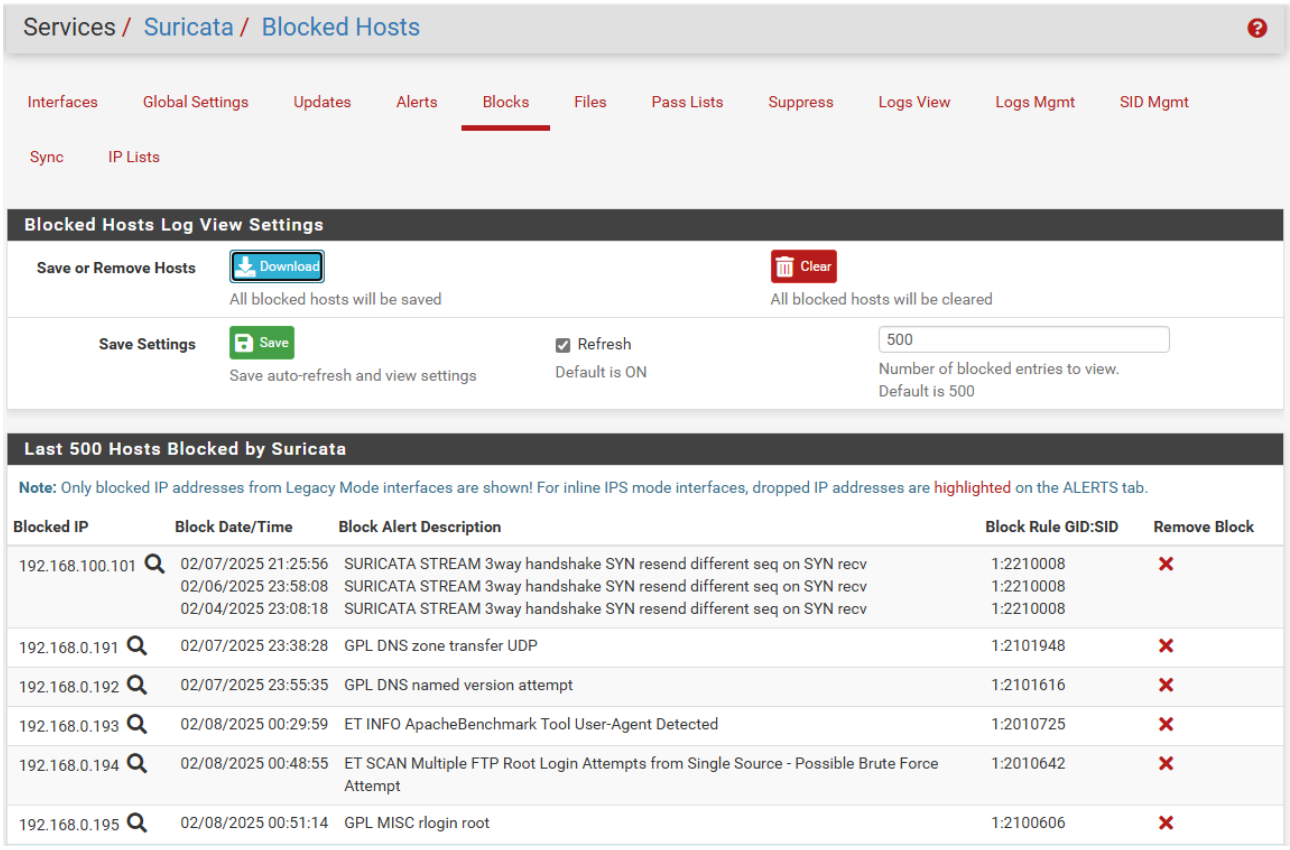


Рисунок 3.18 – Блокування IP-адрес в IPS Suricata

Загалом результати тестування підтверджують, що IPS Suricata у поєднанні з pfSense є ефективним рішенням для захисту мережі від широкого спектра атак. Проте є можливості для вдосконалення, такі як оптимізація налаштувань для зниження кількості хибних спрацювань і впровадження механізмів адаптивного аналізу поведінки, щоб підвищити точність виявлення нових загроз.

3.3 Висновки до третього розділу

В третьому розділі було розглянуто процес тестування ефективності системи IPS Suricata у лабораторному середовищі, що включав моделювання різних атак, таких як SYN Flood, brute force, атаки на DNS-сервіси та інші сценарії аномальної мережевої активності. Ключовою метою було оцінити здатність IPS виявляти та блокувати загрози в режимі реального часу, забезпечуючи захист вразливого сервера Metasploitable VM.

Результати тестування показали, що IPS Suricata успішно ідентифікувала та блокувала основні типи атак. Атака SYN Flood була розпізнана завдяки фіксації

аномалій у процесі встановлення TCP-з'єднань. У разі brute force атак Suricata зафіксувала багаторазові спроби входу до сервісів Telnet, FTP та rlogin із використанням облікового запису root. Це стало можливим завдяки налаштуванню правил, які базуються на сигнатурах відомих атак. Атаки на DNS-сервіси, включаючи запити CHAOS TXT і Zone Transfer, також були своєчасно виявлені, що запобігло витоку критично важливої інформації про структуру мережі. Дослідження впливу Flood-атак із використанням Apache Benchmark дозволило оцінити здатність Suricata відрізняти легітимний трафік від потенційно шкідливого. Виявлення високої активності під час стрес-тестування підтвердило чутливість IPS до подібних дій. Аналіз журналів Suricata продемонстрував ефективність правил, які дозволяють вчасно блокувати шкідливий трафік без суттєвого впливу на роботу легітимних сервісів.

Лабораторне середовище забезпечило реалістичні умови для тестування Suricata, а також дозволило аналізувати ефективність роботи правил і налаштувань IPS. Висновки підтверджують, що система IPS Suricata є надійним інструментом для забезпечення мережевої безпеки, здатним виявляти та блокувати широкий спектр атак.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при масивній зовнішній кровотечі

Масивна зовнішня кровотеча є надзвичайно небезпечним станом, який може призвести до серйозної загрози життю постраждалої особи. Невідкладна надання домедичної допомоги може врятувати життя і запобігти подальшій крововтраті.

Долікарська допомога постраждалим при кровотечі є важливою процедурою, яку можуть виконувати особи без медичної освіти.

Ознаками масивної зовнішньої кровотечі є будь-що з нижченаведеного:

- швидке, інтенсивне витікання крові з рани;
- пульсуючий характер кровотечі (кров б’є фонтаном);
- пляма крові біля постраждалого, яка швидко збільшується;
- значне просякнення одягу постраждалого кров’ю;
- - порушення або втрата свідомості у постраждалого без ознак черепно-мозкової травми, при наявності зовнішньої кровотечі;
- бліда шкіра, холодні кінцівки тощо, при наявності зовнішньої кровотечі.

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 домедичної допомоги постраждалим при при масивній зовнішній кровотечі. У цьому порядку термін “тепловий удар” вживаються у такому значенні - невідкладний стан, викликаний дією високої температури навколишнього середовища, що спричиняє системні розлади у постраждалого [33].

Надання домедичної допомоги постраждалим при масивній зовнішній кровотечі передбачає такі кроки:

- переконайтесь що небезпеки для вас немає;
- закличте оточуючих на допомогу;

- перед початком надання допомоги, за можливості, захистіть себе за допомогою індивідуальних засобів захисту, таких як рукавички, маска і захист для очей;
- якщо є кровотеча з рани на кінцівці, і вона видно:
  a) здійсніть максимальний тиск на рану руками;
  b) накладіть пов'язку, що чинитиме тиск на рану, і оцініть її ефективність;
  c) якщо кровотеча зупинилась, заспокойте постраждалого, викличте екстрену медичну допомогу та слідуйте вказівкам диспетчера;
  d) якщо кровотеча не зупинилась, накладіть кровоспинний джгут на відстані 5-7 см вище рани;
  e) уникайте накладання джгута безпосередньо на суглоби ліктя або коліна;
  f) перевірте ефективність накладеного кровоспинного джгута.
- при кровотечі з рани кінцівки без можливості її чіткої візуалізації:
  a) накладіть кровоспинний джгут якомога вище на кінцівку;
  b) заспокойте постраждалого та поясніть подальші кроки;
  c) якщо можливо, розріжте одяг на кінцівці;
  d) оцініть ефективність накладання кровоспинного джгута.

Якщо кровотеча зупинилась, зафіксуйте точний час накладання джгута на самому джгуті або видимому місці. Якщо неможливо зафіксувати час, повідомте медичному персоналу та переконайтеся, що ця інформація буде внесена до медичних записів. Якщо у вас є навик перевірки пульсу на кінцівці нижче джгута, перевірте його. Якщо пульс присутній, збільште тиск кровоспинного джгута або накладіть додатковий джгут. Якщо кровотеча не зупинилась, збільште тиск на кровоспинному джгуті або накладіть ще один джгут в залежності від місця рани. Якщо другий джгут не є ефективним або неможливо його накласти, продовжуйте чинити прямий тиск на рану руками до прибуття медичної бригади або тампонуйте рану. Не знімайте або не послабляйте кровоспинний джгут до прибуття медичної бригади.

При кровотечі з рани, розташованої в пахвових ділянках, сідницях або основі шиї растосуйте максимальний тиск на рану, заспокойте постраждалого та поясніть подальші дії, тампонуйте рану тугим гемостатичним засобом або марлевим бинтом. Після тампонування продовжуйте здійсніть прямий тиск на рану протягом 3 хвилин (з гемостатиком) або 10 хвилин (з марлевим бинтом) та оцініть ефективність тампонування рани.

Якщо кровотеча зупинилась, продовжуйте надавати іншу домедичну допомогу, передбачену процедурою. Якщо кровотеча не зупинилась, спробуйте повторно тампонувати рану. Якщо це неможливо, продовжуйте чинити максимальний тиск на рану руками до прибуття швидкої медичної допомоги.

Це загальна послідовність дій, яку слід виконати, але завжди важливо дотримуватись інструкцій медичних фахівців та адаптувати допомогу до конкретної ситуації. Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Вимоги ергономіки до організації робочого місця оператора ПК

В сучасному інформаційному суспільстві комп'ютери використовуються на робочих місцях велика кількості людей. Ефективна робота з ПК залежить від відповідності організації робочого місця принципам ергономіки. Ергономічна організація робочого місця оператора ПК сприяє комфортній, безпечній та продуктивній роботі.

Один з головних аспектів ергономічної організації робочого місця оператора ПК - це правильне розташування обладнання. Комп'ютерний монітор повинен бути розташований на відстані 50-70 см від очей оператора, з вертикальним кутом огляду близько 15-20 градусів. Клавіатура та миша повинні бути розташовані таким чином, щоб зап'ястя знаходилися в прямому положенні, не перенапружуючись під час роботи. Також важливо, щоб стіл та стілець були підібрані з урахуванням зручності та підтримки правильної позиції тіла оператора.

Стілець з правильною підтримкою спини та регульованою висотою допомагає уникнути напруження спини та шийних м'язів.

Висота стола повинна бути такою, щоб плечі оператора були розслаблені, а передпліччя лежали на столі без напруження. Належне розташування робочої поверхні забезпечує комфортну роботу з клавіатурою та мишкою.

Освітлення є ще одним важливим аспектом ергономічної організації робочого місця. Робоче місце повинно мати достатнє освітлення, яке не створює відблиску на екрані монітора. Краще використовувати природне світло, а також штучне освітлення з регульованою яскравістю. Джерела світла повинні розташовуватись збоку або ззаду від оператора, щоб уникнути тіней та відблиску на робочій поверхні.

Правильна позиція тіла оператора є також важливою у ергономічній організації робочого місця. Оператор повинен сидіти зі спиною прямо, з підтримкою нижньої частини спини. Ноги повинні бути розташовані на підлозі з прогнутими колінами під кутом близько 90 градусів. Руки та зап'ястя повинні бути розташовані в нейтральному положенні, без напруження або перекручування.

До інших вимог ергономіки до організації робочого місця оператора ПК належить забезпечення достатнього простору для розташування обладнання та документів, використання антистатичного покриття для підлоги, що зменшує накопичення статичної електрики, та забезпечення належного провітрювання приміщення.

В законодавчій базі документів, які стосуються вимог безпеки до обладнання та технологічних процесів та враховують ергономічні аспекти у дизайні робочих місць. У якості прикладу можна навести такі нормативні документи:

– ДСТУ ISO 9241-1-2003 Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 1. Загальні положення.

– ДСТУ 7234:2011 Дизайн та ергономіка.

– ДСТУ 7299:2013 Дизайн та ергономіка. Робоче місце оператора Взаємне розташування елементів робочого місця. Загальні вимоги ергономіки Обладнання виробниче.

– ДСТУ 7950:2015 Дизайн і ергономіка. Робоче місце при виконанні робіт стоячи.

– ДСТУ 7951:2015 Дизайн і ергономіка. Крісло оператора. Загальні ергономічні вимоги Загальні ергономічні вимоги.

– ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги.

– ДСТУ EN 547-3:2018 Безпека машин. Розміри тіла людини. Частина 3. Антропометричні дані.

Ергономічна організація робочого місця оператора ПК має велике значення для забезпечення комфорту, безпеки та ефективності роботи. Відповідне розташування обладнання, належне освітлення, правильна позиція тіла та інші аспекти ергономічної організації робочого місця сприяють запобіганню втоми, м'язовим напруженням та іншим проблемам, пов'язаним з роботою на ПК. Робота на ергономічно організованому робочому місці підвищує продуктивність, знижує ризик розвитку травм та покращує загальне самопочуття оператора ПК.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було проведено комплексне дослідження ефективності роботи системи IPS Suricata, розгорнутої в складі маршрутизатора pfSense, з метою виявлення та запобігання широкого спектра кіберзагроз у контрольованому лабораторному середовищі. Ретельно спланована методологія дослідження, що включала аналіз сучасних мережевих атак, створення тестового середовища на базі гіпервізора Hyper-V з використанням віртуалізованих систем pfSense, Kali Linux та Metasploitable VM та моделювання реальних сценаріїв атак (SYN Flood, brute force, атаки на DNS-сервіс), дозволила оцінити працездатність та надійність інтегрованого рішення з IPS Suricata.

Основні висновки дослідження наступні:

1) Ефективність виявлення атак. IPS Suricata успішно виявляє та класифікує основні типи мережевих атак, зокрема SYN Flood, brute force атаки на сервіси Telnet, FTP і rlogin, а також спроби витоку інформації через DNS-запити (CHAOS TXT, Zone Transfer). Реєстрація відповідних сповіщень у журналі системи підтверджує її здатність оперативно реагувати на аномальну мережеву активність.

2) Надійність блокування шкідливого трафіку. Тестування показало, що налаштовані правила IPS Suricata ефективно блокують підозрілий трафік, не впливаючи значною мірою на легітимний мережевий трафік. Механізми автоматичного блокування та можливість подальшої корекції списку блокувань дозволяють швидко реагувати на загрози та мінімізувати вплив атак на цільові системи.

3) Практична цінність створеного лабораторного середовища. Розроблена інфраструктура дозволила змоделювати реалістичні умови атак та отримати детальний аналіз роботи IPS у різних сценаріях. Це сприяє підвищенню практичних навичок з кібербезпеки та може бути використане як навчальний матеріал для спеціалістів та системних адміністраторів.

4) Перспективи подальшого удосконалення системи. Незважаючи на високий рівень виявлення та блокування атак, дослідження вказало на можливості оптимізації налаштувань IPS для зниження кількості хибних спрацювань.

5) Внесок у забезпечення інформаційної безпеки. Отримані результати демонструють, що використання IPS Suricata у поєднанні з pfSense є ефективним рішенням для захисту корпоративних мереж від сучасних кіберзагроз. Практична реалізація системи дозволяє підвищити рівень інформаційної безпеки, забезпечити оперативну реакцію на атаки та зменшити потенційні фінансові та репутаційні збитки для організацій.

Таким чином, результати кваліфікаційної роботи підтверджують доцільність застосування IPS Suricata як ключового компонента системи мережевого захисту. Запропонована методологія тестування та аналіз отриманих даних можуть бути використані для подальшого вдосконалення систем безпеки, а також служити практичним керівництвом для впровадження ефективних заходів протидії кіберзагрозам у реальних умовах експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is the CIA triad and why is it important? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad

2. Types of network attacks against confidentiality, integrity and avilability. (n.d.). Free Networking tutorials, System Administration Tutorials and Security Tutorials - omnisecu.com. https://www.omnisecu.com/ccna-security/types-of-network-attacks.php

3. MITM - what is man in the middle attack? How to prevent? (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

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

5. What is DNS spoofing and cache poisoning. (n.d.). Wallarm | Advanced API Security. https://www.wallarm.com/what/what-is-dns-spoofing-dns-cache-poisoning

6. 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.

7. 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

8. 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.

9. 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.

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

11. 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.

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

13. 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.

14. 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.

15. 5 damaging consequences of data breach | metacompliance. (n.d.). MetaCompliance. https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

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

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

18. 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.

19. 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.

20. 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.

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

22. 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.

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

24. Virtualization documentation. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/virtualization/

25. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

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

27. Suricata User Guide (n.d.). Suricata documentation. https://docs.suricata.io/en/latest/

28. Metasploitable 2 | metasploit documentation. (n.d.). Docs @ Rapid7. https://docs.rapid7.com/metasploit/metasploitable-2

29. 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. Hping3 | kali linux tools. (n.d.). Kali Linux. https://www.kali.org/tools/hping3/

30. Ab - apache HTTP server benchmarking tool - apache HTTP server version 2.4. (n.d.). Welcome! - The Apache HTTP Server Project. https://httpd.apache.org/docs/2.4/programs/ab.html

31. Hydra | kali linux tools. (n.d.). Kali Linux. https://www.kali.org/tools/hydra/

32. Оробчук, О. Р., & Демчишин, М. (2024). Основні кіберзагрози та методи шифрування даних для автономних транспортних засобів. *Матеріали XII науково-технічної конференції „Інформаційні моделі, системи та технології “*, 68-69.
33. 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.
34. Sachenko, A. O., et al. "Internet of Things for intelligent transport systems."
35. Оробчук, О. Р., & Кивацький, І. М. (2023). Дослідження стратегій кіберзахисту систем керування розумним будинком. *Матеріали XI науково-технічної конференції „Інформаційні моделі, системи та технології “*, 53-53.
36. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.
37. Palamar, A., Karpinski, M. P., Palamar, M., Osukhivska, H., & Mytnyk, M. (2022, November). Remote Air Pollution Monitoring System Based on Internet of Things. In ITTAP (pp. 194-204).
38. T. Lechachenko, R. Kozak, Y. Skorenkyy, O. Kramar, O. Karelina. Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. CEUR Workshop Proceedings, 2023, 3628, pp. 325–329.
39. Lupenko, S., Orobchuk, O., Kateryniuk, I., Kozak, R., & Lypak, H. (2024, October 23–25). Secure information system for Chinese Image medicine knowledge consolidation. In Proceedings of the 4th International Workshop on Information Technologies: Theoretical and Applied Problems 2024 (ITTAP 2024), Ternopil, Ukraine and Opole, Poland (Vol. 3896, pp. 509–519). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-3896.
40. 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

Додаток А Результати сканування відкритих TCP та UDP портів

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -A 192.168.1.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-04 22:18 EET
Nmap scan report for 192.168.1.101
Host is up (0.0010s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.190
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0)
| ssh-hostkey:
```

```
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands:   metasploitable.localdomain,   PIPELINING,   SIZE
10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|         ssl-cert:         Subject:         commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There
is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-02-04T20:21:26+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      55418/tcp   mountd
|   100005  1,2,3      56663/udp   mountd
|   100021  1,3,4      53893/tcp   nlockmgr
|   100021  1,3,4      54360/udp   nlockmgr
|   100024  1          37671/tcp   status
|_  100024  1          54492/udp   status
139/tcp    open   netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp    open   netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 27
|   Capabilities flags: 43564
```

| Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase, SupportsCompression

| Status: Autocommit

|_ Salt: MIc90%fVZ@sC4x":AwV(

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|_Not valid after: 2010-04-16T14:07:45

|_ssl-date: 2025-02-04T20:21:26+00:00; +6s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

```
|   uptime: 0 days, 0:37:04
|   source ident: nmap
|   source host: 9DF8BC7.F0D9233E.FFFA6D49.IP
|_  error: Closing Link: xeoxpzlgq[192.168.0.190] (Quit: xeoxpzlgq)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
8787/tcp   open   drb              Ruby DRb RMI (Ruby 1.8; path
/usr/lib/ruby/1.8/drb)
37671/tcp open  status      1 (RPC #100024)
40535/tcp open  java-rmi    GNU Classpath grmiregistry
53893/tcp open  nlockmgr    1-4 (RPC #100021)
55418/tcp open  mountd      1-3 (RPC #100005)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 -
2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service     Info:     Hosts:          metasploitable.localdomain,
irc.Metasploitable.LAN;      OSs:      Unix,      Linux;      CPE:
cpe:/o:linux:linux_kernel


Host script results:
```

```
|_clock-skew: mean: 1h15m05s, deviation: 2h30m00s, median: 5s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-02-04T15:21:19-05:00
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   0.40 ms 192.168.0.120
2   1.16 ms 192.168.1.101

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 146.67 seconds

┌──(kali㉿kali)-[~]
```

```
└─$ sudo nmap -sU -A 192.168.1.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-02-05 00:43 EET
Nmap scan report for 192.168.1.101
Host is up (0.0010s latency).
Not shown: 951 closed udp ports (port-unreach), 45 open|filtered udp ports (no-response)
PORT     STATE SERVICE    VERSION
53/udp   open  domain     ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
111/udp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      55418/tcp   mountd
|   100005  1,2,3      56663/udp   mountd
|   100021  1,3,4      53893/tcp   nlockmgr
|   100021  1,3,4      54360/udp   nlockmgr
|   100024  1          37671/tcp   status
|_  100024  1          54492/udp   status
137/udp   open   netbios-ns  Samba nmbd netbios-ns (workgroup: WORKGROUP)
| nbns-interfaces:
```

```
|   hostname: METASPLOITABLE
|   interfaces:
|_    192.168.1.101
2049/udp open  nfs        2-4 (RPC #100003)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
Service Info: Host: METASPLOITABLE

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>,
NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE (using port 1014/udp)
HOP RTT     ADDRESS
1   0.36 ms 192.168.0.120
2   1.21 ms 192.168.1.101

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 1351.09 seconds
```