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

магістр
(освітній рівень)

на тему: "Розробка оптимізованих правил IPS для виявлення багатовекторних атак "

Виконав: студент VI курсу, групи СБм-61
Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Михайловський Олександр Петрович
підпис (прізвище та ініціали)

Керівник Оробчук О. Р.
підпис (прізвище та ініціали)
Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

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

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

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)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Михайловському Олександру Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка оптимізованих правил IPS для виявлення багатовекторних 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 «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 12.12.2024

3. Вихідні дані до роботи Тестове лабораторне середовище, побудоване на базі гіпервізора VMware ESXi, з використанням маршрутизатора pfSense та системи виявлення і запобігання вторгненням Snort, сервера Ubuntu Linux і атакуючих машин Parrot Security OS.

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз сучасних кіберзагроз. Розробка сценаріїв моделювання кібератак для тестування ефективності систем IDS/IPS. Налаштування тестового середовища на базі VMware ESXi, pfSense, Snort та Ubuntu Linux. Оптимізація правил для систем виявлення та запобігання вторгненням. Проведення тестування ефективності налаштованих правил в умовах моделювання реальних атак. Оцінка впливу оптимізованих налаштувань на продуктивність системи.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, об'єкт, предмет дослідження.
Наукова новизна та практичне значення. Завдання дослідження.
Багатовекторні DDoS-атаки. Схема розташування IPS для контролю трафіку.
Тестове лабораторне середовище на основі VMware ESXi.
Елементи тестового лабораторного середовища.
Моделювання кіберзагроз. Мережева статистика підчас атаки.
Правила для IPS Snort. Повідомлення IPS Snort про виявлення атаки.
Зблоковані IP-адреси системою IPS Snort.
Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел для аналізу правил IPS	25.09 – 10.10	Виконано
3.	Опрацювання джерел в галузі дослідження	11.10 – 15.10	Виконано
4.	Налаштування тестового лабораторного середовища	16.10 – 25.10	Виконано
5.	Розроблення оптимізованих правил IPS для виявлення багатовекторних атак	25.10 - 30.10	Виконано
6.	Оформлення розділу «Огляд предметної області»	30.10 – 05.11	Виконано
7.	Оформлення розділу «Налаштування тестового лабораторного середовища»	06.11 – 10.11	Виконано
8.	Оформлення розділу «Впровадження системи виявлення та запобігання вторгненням»	11.11 – 25.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-01.12	
10.	Оформлення кваліфікаційної роботи	02.12 – 10.12	Виконано
11.	Нормоконтроль	08.12 – 10.12	Виконано
12.	Перевірка на плагіат	12.12 – 14.12	Виконано
13.	Попередній захист кваліфікаційної роботи	20.12 – 15.12	Виконано
14.	Захист кваліфікаційної роботи	26.12.2024	

Студент _____ Михайловський О. П.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Розробка оптимізованих правил IPS для виявлення багатовекторних атак // ОР «Магістр» // Михайловський Олександр Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 78, рис. – 29, табл. – - , кресл. – 15, додат. – 1.

Ключові слова: DDoS, IPS, Snort, pfSense, Cybersecurity, Brute-force.

У кваліфікаційній роботі магістра проведено дослідження методів захисту мережевої інфраструктури від багатовекторних DDoS-атак та інших кіберзагроз шляхом впровадження системи виявлення та запобігання вторгненням (IPS) на базі маршрутизатора pfSense та системи Snort.

У першому розділі здійснено огляд різних типів DDoS-атак, їхніх характеристик та наслідків для організацій. У другому розділі розроблено та налаштовано тестове лабораторне середовище на базі гіпервізора VMware ESXi. Це середовище включає маршрутизатор pfSense, сервер Ubuntu Linux та атакуючі машини на базі Parrot Security OS. Проведено тестування середовища, яке підтвердило коректну взаємодію між усіма компонентами та готовність до моделювання кіберзагроз. У третьому розділі змодельовано різні типи кіберзагроз, включаючи DDoS-атаки типів SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, а також атаки типу Brute-force. Розроблено оптимізовані правила для системи Snort, спрямовані на ефективне виявлення та блокування цих загроз з мінімізацією хибних спрацьовувань. Проведено тестування розроблених правил IPS, яке підтвердило їхню ефективність у виявленні та блокуванні різних типів атак, включаючи багатовекторні.

ABSTRACT

Development of optimized IPS rules for detecting multivector attacks // Thesis of educational level "Master"// Mykhailovskyi Oleksandr // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2024 // P. 78, figs. 29, tables -, drawings 15, added. 1.

Keywords: DDoS, IPS, Snort, pfSense, Cybersecurity, Brute-force.

In the master's thesis, the researchers investigated methods of protecting network infrastructure from multi-vector DDoS attacks and other cyber threats by implementing an intrusion detection and prevention system (IPS) based on the pfSense router and Snort system.

The first section provides an overview of the different types of DDoS attacks, their characteristics, and the consequences for organisations. In the second section, a test lab environment based on the VMware ESXi hypervisor is designed and configured. This environment includes a pfSense router, an Ubuntu Linux server, and attack machines based on Parrot Security OS. The environment was tested, which confirmed the correct interaction between all components and readiness for cyber threat modelling. In the third section, various types of cyber threats were modelled, including DDoS attacks such as SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, and Brute-force attacks. Optimised rules for the Snort system were developed to effectively detect and block these threats while minimising false positives. The developed IPS rules were tested, which confirmed their effectiveness in detecting and blocking various types of attacks, including multi-vector attacks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS	—	Distributed Denial of Service
IPS	—	Intrusion Prevention System
OSI	—	Open Systems Interconnection
UDP	—	User Datagram Protocol
TCP	—	Transmission Control Protocol
ICMP	—	Internet Control Message Protocol
HTTP	—	Hypertext Transfer Protocol
DNS	—	Domain Name System
SIP	—	Session Initiation Protocol
SMTP	—	Simple Mail Transfer Protocol
IMAP	—	Internet Message Access Protocol
IoT	—	Internet of Things
CDN	—	Content Delivery Network
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
WWW	—	World Wide Web
DHCP	—	Dynamic Host Configuration Protocol
SSH	—	Secure Shell
NAT	—	Network Address Translation

ВСТУП

Актуальність теми. У кіберпросторі спостерігається збільшення кількості та складності багатовекторних DDoS-атак, які стають серйозною загрозою для інформаційної безпеки організацій та підприємств. Традиційні методи захисту часто не здатні виявити й нейтралізувати такі атаки, що вимагає розробки спеціалізованих рішень, здатних до швидкої адаптації. Використання системи запобігання вторгненням (IPS) з оптимізованими правилами для виявлення багатовекторних DDoS-атак є актуальною темою, яка сприятиме покращенню захисту критичних ресурсів та мереж від кіберзагроз.

Мета і задачі дослідження. Метою дослідження є розробка та впровадження оптимізованих правил для системи IPS на базі pfSense з метою ефективного виявлення багатовекторних DDoS-атак.

Основні задачі включають:

- аналіз існуючих методів захисту від DDoS-атак та визначення їх обмежень;
- дослідження можливостей pfSense та Snort для виявлення різних типів DDoS-атак;
- розробка оптимізованих правил для виявлення багатовекторних атак;
- тестування розробленої системи та аналіз її ефективності у різних сценаріях.

Об’єкт дослідження. Процеси виявлення та запобігання багатовекторним DDoS-атакам у мережевих середовищах.

Предмет дослідження. Методи та засоби для виявлення багатовекторних DDoS-атак за допомогою системи IPS на основі платформи pfSense.

Наукова новизна одержаних результатів кваліфікаційної роботи. В роботі запропоновано удосконалений підхід до налаштування правил для системи IPS, що дозволяє значно підвищити ефективність виявлення багатовекторних DDoS-атак у реальному часі. Оптимізовані правила були розроблені на основі аналізу різних типів трафіку та специфіки багатовекторних

атак, що забезпечило їхню адаптивність та зменшило кількість хибних спрацьовувань.

Практичне значення одержаних результатів. Розроблена система IPS з оптимізованими правилами може бути впроваджена в організаціях, які прагнуть захистити свої мережі від багатовекторних DDoS-атак. Це дозволяє забезпечити надійніший рівень безпеки мережевих ресурсів та зменшити ризики простою важливих сервісів через кіберзагрози.

Апробація результатів магістерської роботи. Основні результати дослідження були представлені на VIII Міжнародної наукової конференції «Здобутки та досягнення прикладних та фундаментальних наук XXI століття».

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд DDoS атак

DDoS-атаки є одними з найпоширеніших та найнебезпечніших кіберзагроз сучасності [1]. Вони спрямовані на порушення доступності інтернет-ресурсів, серверів або мережевих інфраструктур шляхом перевантаження системи надмірною кількістю запитів, що призводить до неможливості обслуговувати легітимних користувачів. Особливістю DDoS-атак є те, що вони здійснюються з великої кількості пристроїв, часто заражених шкідливим програмним забезпеченням, і керованих через ботнети, що значно ускладнює їхнє виявлення та блокування.

DDoS-атаки мають різноманітні форми та можуть бути спрямовані на різні рівні мережевого стека, що дозволяє зловмисникам обирати найбільш ефективні методи впливу на систему. Основними мотивами для здійснення таких атак можуть бути:

- фінансовий шантаж: вимога викупу за відновлення доступності сервісу;
- конкурентна боротьба: атака для зниження продуктивності або тимчасової зупинки діяльності конкурентів;
- протест: демонстрація невдоволення шляхом атаки на веб-сайти чи сервіси, що асоціюються з опонентом;
- політичні мотиви: атаки на ресурси державних органів або політичних установ для підриву їхньої репутації чи демонстрації невдоволення.

1.1.1 Основні види DDoS-атак

DDoS-атаки можуть бути класифіковані за рівнями моделі OSI, що дозволяє глибше розуміти їх механізми та ефективніше розробляти стратегії захисту. Модель OSI складається з семи рівнів, кожен з яких відповідає за певні функції в процесі передачі даних. Розглянемо докладно основні види DDoS-атак, що впливають на різні рівні цієї моделі.

Мережевий рівень 3 (Network Layer) відповідає за маршрутизацію пакетів даних між пристроями в мережі [2]. DDoS-атаки на цьому рівні спрямовані на перевантаження мережевої інфраструктури. Прикладом атаки на даному рівні є ICMP Flood [3]. Атакуючі надсилають великий обсяг ICMP Echo Request (Ping) пакетів до цільової системи. Сервер витрачає ресурси на обробку та відповідь на кожен запит, що призводить до виснаження мережевих ресурсів. Наслідками є перевантаження пропускної здатності мережі та недоступність сервісів для легітимних користувачів. В Smurf Attack використовується широкомовна адреса мережі [4]. Атакуючий надсилає ICMP Echo Request з підробленою IP-адресою жертви на широкомовну адресу. Усі пристрої в мережі відповідають на цей запит, спрямовуючи відповіді на жертву. Наслідком є створення масивного потоку трафіку до жертви, що перевантажує її мережеві ресурси. В атаці IP Fragmentation Attacks (Ping of Death) зловмисник надсилає ICMP-пакети, розмір яких перевищує максимальний за стандартом [5]. Ці пакети фрагментуються, і при збиранні на стороні отримувача можуть спричинити переповнення буфера. Наслідком може бути аварійне завершення роботи системи або її зависання.

Транспортний рівень 4 (Transport Layer) відповідає за надійну передачу даних між хостами [6]. Атаки на цьому рівні націлені на вразливості протоколів TCP та UDP. Прикладом атаки є SYN Flood де атакуючий надсилає великий обсяг TCP SYN-запитів для ініціації з'єднань, але не завершує триетапний процес рукостискання (SYN-ACK-ACK) [7]. Сервер резервує ресурси для кожного незавершеного з'єднання. Наслідком є виснаження ресурсів сервера, недоступність для нових легітимних з'єднань. В UDP Flood атаці відбувається надсилання великої кількості UDP-пакетів на випадкові або конкретні порти цільової системи [8]. Сервер намагається обробити ці пакети, але якщо порт закритий, він надсилає ICMP-повідомлення про недоступність. Наслідком є перевантаження мережевої інфраструктури та серверних ресурсів. Атаки типу ACK Flood відбувається з надсиланням великої кількості TCP ACK пакетів. Це змушує сервер перевіряти таблиці стану та витрачати ресурси на обробку несподіваних пакетів [9]. Наслідком є перевантаження процесора та пам'яті сервера, зниження продуктивності.

Рівень 7 застосунків (Application Layer) відповідає за інтерфейс між прикладними програмами та мережею [10]. Атаки на цьому рівні спрямовані на конкретні сервіси та програми, імітуючи легітимну активність. Прикладом є HTTP Flood де атакуючий надсилає великий обсяг HTTP GET або POST запитів до вебсервера [11]. Запити можуть бути спрямовані на ресурсоємні операції. Наслідком є виснаження ресурсів сервера (процесора, пам'яті), недоступність вебсайту для користувачів. Атака типу Slowloris відбувається за допомогою встановлення великої кількості HTTP-з'єднань і повільне надсилання неповних HTTP-заголовків [12]. Сервер тримає з'єднання відкритими, очікуючи завершення запитів. Наслідком є вичерпання максимальної кількості доступних з'єднань, недоступність сервера для нових запитів. При атаці DNS Query Flood надсилається великий обсягу DNS-запитів до DNS-сервера [13]. Запити можуть бути складними або спеціально сформованими для максимального навантаження. Наслідком є перевантаження DNS-сервера, неможливість обробки легітимних запитів, недоступність сервісів, що залежать від DNS. Тип атаки SIP Flood це атака на VoIP-сервіси, надсилання великої кількості SIP-запитів. Наслідки проявляються в перевантаженні серверів VoIP та перериванні телефонних послуг.

Хоча більшість DDoS-атак зосереджені на рівнях 3, 4 та 7, деякі атаки можуть впливати на інші рівні. Наприклад MAC Flooding Attack при якій відбувається надсилання великої кількості пакетів з різними MAC-адресами до комутатора, що перевантажує його таблицю MAC-адрес та спотворює її [14].

1.1.2 Наслідки DDoS-атак

Наслідки DDoS-атак можуть бути вкрай серйозними та багатогранними, впливаючи на різні аспекти діяльності організацій, інфраструктуру мережі, а також на користувачів та клієнтів. Одним із найбільш помітних наслідків є втрата доступності сервісів. Оскільки DDoS-атаки спрямовані на перевантаження ресурсів системи або мережі, вони призводять до того, що легітимні користувачі не можуть отримати доступ до веб-сайтів, застосунків або інших онлайн-сервісів.

Це особливо критично для компаній, діяльність яких безпосередньо пов'язана з інтернетом, таких як інтернет-магазини, фінансові установи або сервіси електронної пошти.

Фінансові втрати є ще одним суттєвим наслідком DDoS-атак. Втрата доступу до сервісів може призвести до прямих фінансових збитків через зниження продажів, втрату транзакцій або втрату можливостей для бізнесу. Крім того, організації можуть нести додаткові витрати на відновлення роботи систем, інвестування в додаткові засоби захисту та оплату послуг спеціалізованих компаній з кібербезпеки. Витрати можуть також включати штрафи за невиконання договірних зобов'язань перед клієнтами або партнерами.

Втрата репутації є довготривалим наслідком, який може вплинути на довіру клієнтів та партнерів до організації. Повторні або тривалі перебої в роботі сервісів можуть призвести до негативного сприйняття бренду, зниження лояльності клієнтів та втрати конкурентних переваг. У сучасному інформаційному середовищі негативні відгуки та публікації в засобах масової інформації можуть швидко поширюватися, посилюючи репутаційні ризики. Вплив на клієнтів та партнерів може бути значним, оскільки перебої в роботі сервісів безпосередньо впливають на їхню діяльність. Клієнти можуть втратити доступ до важливих послуг, що призводить до незадоволення та переходу до конкурентів. Партнери можуть зазнати збитків через порушення спільних бізнес-процесів, що може негативно вплинути на ділові відносини.

Операційні втрати також є значними. Під час DDoS-атак працівники організації можуть бути обмежені в доступі до необхідних ресурсів, що впливає на їхню здатність виконувати свої обов'язки. Це може призвести до затримок у виконанні проектів, зниження продуктивності та загального ефективності бізнес-процесів.

Витрати на відновлення та модернізацію інфраструктури після DDoS-атак можуть бути значними. Організації часто змушені інвестувати в оновлення мережевих пристроїв, програмного забезпечення та засобів захисту, щоб запобігти майбутнім атакам. Це може включати впровадження спеціалізованих

рішень для захисту від DDoS, оновлення брандмауерів, систем виявлення та запобігання вторгненням, а також навчання персоналу.

Потенційні юридичні наслідки також не можна ігнорувати. Якщо в результаті DDoS-атаки відбувся витік конфіденційної інформації або порушено вимоги регуляторних органів щодо забезпечення безпеки даних, організація може зіткнутися з юридичними позовами, штрафами та іншими санкціями. Це особливо актуально для галузей, де безпека даних є критично важливою, таких як фінансовий сектор або охорона здоров'я.

Ризик повторних атак також зростає після успішної DDoS-атаки. Зловмисники можуть сприйняти успішну атаку як сигнал про вразливість системи та продовжувати атаки або вимагати викуп за припинення атак. Це може призвести до тривалого протистояння та необхідності постійного вдосконалення засобів захисту.

Психологічний вплив на співробітників організації також може бути суттєвим. Постійний стрес від необхідності реагувати на кіберзагрози, а також почуття незахищеності можуть негативно вплинути на моральний дух команди та призвести до вигорання.

1.1.3 Використання ботнет

Ботнети, або мережі ботів, є групами комп'ютерних пристроїв, заражених шкідливим програмним забезпеченням і керованих віддалено зловмисниками. Ці пристрої, відомі як "боти" або "зомбі", використовуються для виконання різних шкідливих дій, серед яких одним із найпоширеніших є DDoS-атаки [15].

Ботнети формуються шляхом масового зараження комп'ютерів і пристроїв за допомогою різних методів розповсюдження шкідливого програмного забезпечення. Зловмисники використовують фішингові атаки, розсилаючи електронні листи з посиланнями на шкідливі сайти або зараженими вкладеннями. Вони також експлуатують відомі вразливості у програмному забезпеченні для автоматизованого зараження систем. Методи соціальної інженерії дозволяють обманювати користувачів і змушувати їх самостійно

встановлювати шкідливі програми. Крім того, зловмисники заражають пристрої Інтернету речей (IoT), використовуючи слабкі паролі або відсутність оновлень безпеки [16].

Після зараження бот отримує інструкції від командно-контрольного сервера (C&C-сервера), що дозволяє зловмисникам координувати дії ботнету. Ботнети є ключовим інструментом для здійснення DDoS-атак з кількох причин. По-перше, вони забезпечують масштабність: ботнети можуть складатися з десятків тисяч або навіть мільйонів пристроїв, що дозволяє генерувати величезний обсяг трафіку, перевищуючи можливості пропускної здатності цільової мережі або сервера. По-друге, розподіленість атак ускладнює їхнє виявлення та блокування, оскільки трафік надходить з різних IP-адрес та мереж. По-третє, анонімність зловмисників забезпечується завдяки тому, що керування ботнетом здійснюється через посередницькі сервери або зашифровані канали зв'язку, що ускладнює ідентифікацію та притягнення до відповідальності організаторів атак.

Ботнети можуть використовуватися для різних типів DDoS-атак. Вони здатні здійснювати потужні атаки, генеруючи великий обсяг трафіку, наприклад, через UDP Flood або ICMP Flood, щоб перевантажити пропускну здатність мережі. Також ботнети використовуються для атак на рівень 4, які експлуатують вразливості протоколів для виснаження ресурсів серверів та мережевих пристроїв. Крім того, вони можуть здійснювати атаки на рівні застосунків, націлюючись на конкретні сервіси, наприклад, проводячи HTTP Flood для перевантаження серверних ресурсів.

Прикладами відомих ботнетів є Mirai та Reaper (IoTroop). Mirai став відомим тим, що використовував заражені IoT-пристрої для здійснення масштабних DDoS-атак, зокрема в 2016 році на DNS-провайдера Dyn, що призвело до недоступності багатьох популярних інтернет-сервісів [17]. Reaper використовує більш складні методи зараження IoT-пристроїв, експлуатуючи відомі вразливості без потреби у слабких паролях.

Зловмисники використовують різні архітектури для контролю ботнетів. Централізоване управління через C&C-сервери дозволяє всім ботам отримувати команди від одного або декількох центральних серверів, але такий підхід

вразливий до виявлення та блокування цих серверів. Децентралізоване управління на основі P2P-мереж підвищує стійкість ботнету до відключення, оскільки боти обмінюються інформацією між собою без центрального вузла. Також зловмисники можуть використовувати соціальні мережі та стеганографію для передачі команд, приховуючи їх у публікаціях або зображеннях, що ускладнює виявлення каналів управління.

Використання ботнетів значно підвищує ефективність DDoS-атак. Завдяки підсиленню атаки, ботнети дозволяють значно збільшити обсяг шкідливого трафіку, зокрема через атаки типу DNS Amplification [18]. Розподіленість ботнету ускладнює фільтрацію трафіку на основі IP-адрес або географічного розташування, що дозволяє обходити засоби захисту. Динамічність ботнетів дає можливість швидко змінювати вектори атак, переходячи між різними типами DDoS-атак для обходу засобів захисту.

На рисунку 1.1 представлено схему атаки типу SYN Flood на сервер електронної пошти (SMTP/IMAP).

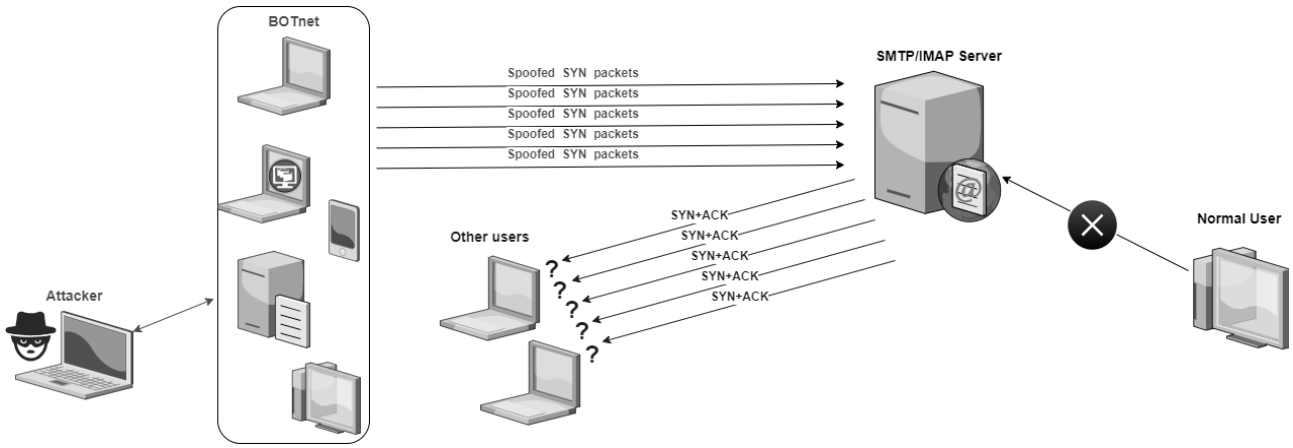


Рисунок 1.1 – Загальний принци здійснення DDoS атаки типу SYN Flood

Від ботнету до сервера надходять підроблені пакети SYN, позначені. Вони мають на меті перевантажити сервер, надсилаючи безліч запитів, які вимагають відповіді SYN+ACK. Сервер намагається обробити ці запити, але через перевантаження не встигає відповідати іншим користувачам, які надсилають легітимні запити.

1.1.4 Багатовекторні DDoS-атаки

Багатовекторні DDoS-атаки є складним і динамічним типом кіберзагроз, які поєднують кілька різних методів і технік для досягнення максимальної ефективності виведення з ладу цільової системи або мережі. На відміну від традиційних DDoS-атак, що зосереджені на одному векторі або типі атаки, багатовекторні атаки використовують комбінацію різних методів одночасно або послідовно, щоб обійти засоби захисту і зробити виявлення та нейтралізацію більш складними [19].

Однією з ключових характеристик багатовекторних DDoS-атак є їхня здатність адаптуватися до контрзаходів, які застосовує жертва. Атакуючі можуть почати атаку з одного типу трафіку, наприклад, атаки типу UDP Flood, і, коли система захисту починає фільтрувати цей трафік, швидко переключитися на інший тип, такий як SYN Flood або HTTP Flood. Ця динамічність ускладнює процес виявлення і вимагає від засобів захисту високого рівня гнучкості та адаптивності.

Багатовекторні атаки можуть поєднувати атаки, спрямовані на перевантаження пропускної здатності мережі, з атаками, які експлуатують вразливості мережевих протоколів, та атаками на рівні застосувань, що націлені на виснаження ресурсів серверів і сервісів. Наприклад, одночасне використання DNS Amplification для генерування великого обсягу трафіку, SYN Flood для виснаження таблиць стану з'єднань на сервері та HTTP Flood для перевантаження веб-застосунків створює комплексну загрозу, з якою важко впоратися традиційними методами.

Застосування ботнетів є ключовим фактором у реалізації багатовекторних DDoS-атак. Завдяки великій кількості заражених пристроїв, атакуючі можуть генерувати різні типи трафіку з різних географічних місць. Це не лише збільшує масштаб атаки, але й ускладнює її фільтрацію, оскільки трафік надходить з легітимних IP-адрес і може імітувати звичайну поведінку користувачів. Заражені пристрої IoT, такі як камери спостереження, роутери та інші пристрої з низьким

рівнем безпеки, часто стають частиною таких ботнетів, що збільшує їхній потенціал.

Однією з особливостей багатовекторних атак є їхня здатність використовувати техніки підсилення і рефлекції. Це дозволяє атакуючим збільшити обсяг трафіку без значного навантаження на власні ресурси. Наприклад, атаки типу DNS Amplification та NTP Amplification використовують відкриті сервери для підсилення трафіку, спрямованого на жертву. Таким чином, зловмисники можуть використовувати невелику кількість ресурсів для запуску масштабних атак.

Багатовекторні DDoS-атаки також можуть бути складовою частиною складніших кібератак, де DDoS використовується як відволікаючий маневр. Поки організація зосереджена на відбитті DDoS-атаки, зловмисники можуть спробувати проникнути в систему, викрасти конфіденційну інформацію або встановити шкідливе програмне забезпечення. Це підкреслює необхідність комплексного підходу до кібербезпеки, де захист від DDoS є лише одним з елементів загальної стратегії безпеки.

Для ефективного захисту від багатовекторних DDoS-атак необхідний багаторівневий підхід. Це включає в себе використання спеціалізованих систем виявлення та запобігання вторгненням, здатних аналізувати трафік на різних рівнях мережевої моделі OSI. Поведінковий аналіз трафіку дозволяє виявляти аномалії, що можуть свідчити про початок багатовекторної атаки. Крім того, використання хмарних сервісів захисту від DDoS може допомогти відфільтрувати шкідливий трафік на рівні провайдера, до того, як він досягне мережі організації.

Оптимізація правил фільтрації та налаштування систем IPS є критично важливими. Оскільки багатовекторні атаки можуть швидко змінювати свій характер, системи захисту повинні бути здатні адаптуватися в реальному часі. Це може включати автоматичне оновлення сигнатур атак, використання алгоритмів машинного навчання для прогнозування нових векторів атак та інтеграцію з глобальними мережами обміну інформацією про загрози.

1.2 Огляд існуючих підходів до захисту від DDoS атак

Захист від DDoS-атак є критично важливим завданням для забезпечення безперебійної роботи інформаційних систем і мереж. Існує широкий спектр методів і технологій, спрямованих на виявлення, запобігання та нейтралізацію DDoS-атак. Кожен із цих підходів має свої особливості, переваги та обмеження, і часто найефективнішим є їхнє комбіноване використання.

Одним із традиційних методів захисту є використання брандмауерів та систем фільтрації трафіку [20]. Брандмауери дозволяють контролювати вхідний та вихідний трафік на основі встановлених правил, блокуючи небажані з'єднання. Вони можуть бути налаштовані на фільтрацію певних типів трафіку або блокування підозрілих IP-адрес. Однак брандмауери мають обмежену ефективність проти великих та складних DDoS-атак, оскільки можуть стати "вузьким місцем" і самі піддатися перевантаженню.

Хмарні сервіси захисту від DDoS є ще одним підходом, що передбачає перенаправлення трафіку через мережі провайдерів із високою пропускною здатністю та спеціалізованими засобами фільтрації. Ці сервіси, такі як Cloudflare, Akamai чи Amazon AWS Shield, здатні масштабуватися для обробки масивних обсягів трафіку та використовують передові технології для виявлення та блокування різних типів DDoS-атак. Вони можуть фільтрувати трафік ще до того, як він досягне мережі клієнта, зменшуючи навантаження на інфраструктуру та забезпечуючи високу доступність сервісів. Проте використання таких сервісів може бути дорогим, і вони не завжди підходять для специфічних або конфіденційних середовищ.

Мережі доставки контенту також відіграють важливу роль у захисті від DDoS-атак [21]. CDN розподіляють контент по глобальній мережі серверів, що зменшує навантаження на основний сервер і покращує швидкість доступу до контенту. Під час DDoS-атак трафік розподіляється між різними вузлами CDN, що допомагає поглинути шкідливий трафік та забезпечити стійкість сервісів.

Системи виявлення та запобігання вторгненням є більш просунутими рішеннями, що аналізують мережевий трафік для виявлення ознак атак. IDS

здійснюють моніторинг та повідомляють про підозрілу активність [22], тоді як IPS додатково можуть автоматично блокувати шкідливий трафік [23]. Вони використовують сигнатурний аналіз для порівняння трафіку з відомими шаблонами атак та поведінковий аналіз для виявлення аномалій.

На рисунку 1.2 показано схему розташування IPS для контролю трафіку.

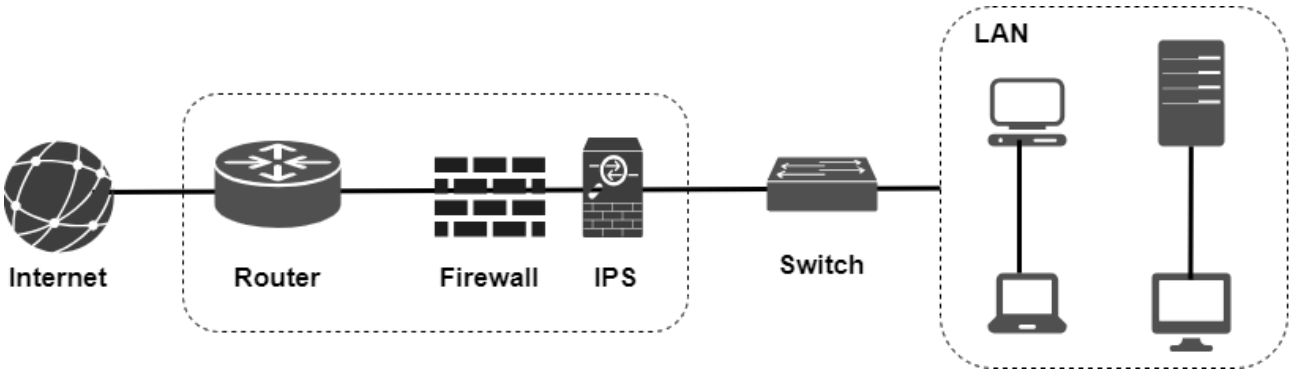


Рисунок 1.2 – Схема розташування IPS для контролю трафіку

Дані обробляються IPS, яка аналізує трафік для виявлення загроз і атак. Поведінковий аналіз трафіку є інноваційним підходом, що використовує методи машинного навчання та штучного інтелекту для виявлення аномальної мережевої активності. Системи, які застосовують цей підхід, створюють базову лінію нормальної поведінки мережі та виявляють відхилення, які можуть свідчити про DDoS-атаку. Це дозволяє виявляти навіть невідомі або модифіковані типи атак. Проте такі системи потребують складного налаштування та можуть генерувати помилкові спрацьовування у випадку різких змін легітимного трафіку.

Використання протоколів та технологій, стійких до DDoS-атак, також є важливим напрямком захисту. Наприклад, технологія Anycast дозволяє розподілити трафік між кількома серверами на основі найближчого маршруту, що зменшує ризик перевантаження окремих вузлів. Протоколи з вбудованими механізмами аутентифікації та перевірки, такі як TLS, можуть запобігати деяким типам атак на рівні застосунків.

Превентивні заходи, такі як збільшення пропускної здатності мережі та впровадження надлишковості в інфраструктурі, допомагають витримати

короткочасні сплески трафіку. Регулярні аудити безпеки, оновлення програмного забезпечення та виправлення вразливостей знижують ризик успішних атак. Крім того, налаштування обмежень швидкості та кількості запитів може запобігти виснаженню ресурсів серверів.

Організаційні заходи включають розробку планів реагування на інциденти, навчання персоналу та проведення тренувань. Швидка та скоординована реакція на DDoS-атаку може значно зменшити її вплив. Співпраця з провайдерами інтернет-послуг та іншими організаціями дозволяє обмінюватися інформацією про загрози та ефективніше протидіяти атакам.

Використання технологій чорних та білих списків IP-адрес дозволяє блокувати трафік з відомих джерел атак та дозволяти доступ лише для перевірених користувачів. Проте цей метод має обмежену ефективність проти розподілених атак, де зловмисники використовують велику кількість різних IP-адрес, часто легітимних або підроблених.

У випадку багатовекторних DDoS-атак, які поєднують кілька різних методів одночасно, особливо важливо застосовувати багаторівневий підхід до захисту. Це включає комбінування різних технологій та методів, таких як фільтрація на рівні мережі, аналіз на рівні застосувань, поведінковий аналіз та використання хмарних сервісів. Системи повинні бути здатні адаптуватися до змін характеру атаки в реальному часі та забезпечувати безперервність роботи сервісів.

Забезпечення ефективного захисту від DDoS-атак вимагає комплексного підходу, що поєднує технічні, організаційні та процедурні заходи. Інтеграція різних систем та технологій, постійний моніторинг та аналіз трафіку, а також підвищення обізнаності персоналу є ключовими елементами успішної стратегії захисту. Розробка та впровадження оптимізованих правил для систем IPS, таких як Snort на базі pfSense, дозволяє покращити виявлення та блокування шкідливого трафіку, забезпечуючи додатковий рівень захисту від складних та багатовекторних DDoS-атак.

1.3 Висновки до розділу 1

В першому розділі було проведено огляд предметної області, пов'язаної з DDoS-атаками та методами захисту від них. Розглянуто сутність DDoS-атак, їхні основні характеристики та особливості. Детально проаналізовано основні види DDoS-атак з точки зору моделі OSI, включаючи атаки на мережевому рівні (ICMP Flood, Smurf Attack, Ping of Death), транспортному рівні (SYN Flood, UDP Flood, ACK Flood) та на рівні застосунків (HTTP Flood, Slowloris, DNS Query Flood, SIP Flood).

Були досліджені наслідки DDoS-атак для організацій, такі як втрата доступності сервісів, фінансові втрати, погіршення репутації, операційні втрати та потенційні юридичні наслідки. Особлива увага приділена використанню ботнетів у здійсненні DDoS-атак, їхньому механізму роботи та впливу на ефективність атак. Розглянуто приклади відомих ботнетів, таких як Mirai та Reaper, та їхній вплив на глобальну кібербезпеку.

Окремо було проаналізовано багатовекторні DDoS-атаки, які поєднують різні методи для обходу засобів захисту та ускладнення процесу виявлення і нейтралізації. Підкреслено важливість розуміння цих атак та необхідність адаптивних і гнучких засобів захисту для ефективного протистояння їм.

Проведено огляд існуючих підходів до захисту від DDoS-атак. Розглянуто традиційні методи, такі як використання брандмауерів та систем фільтрації трафіку, а також сучасні підходи, включаючи хмарні сервіси захисту, мережі CDN, системи IDS/IPS та поведінковий аналіз трафіку. Висвітлено переваги та обмеження кожного з цих підходів, а також підкреслено важливість комплексного та багаторівневого підходу до забезпечення ефективного захисту від DDoS-атак.

Закладено теоретичну основу для подальших досліджень і розробки оптимізованих правил IPS для виявлення багатовекторних DDoS-атак, що є актуальним завданням у сфері інформаційної безпеки.

РОЗДІЛ 2 НАЛАШТУВАННЯ ТЕСТОВОГО ЛАБОРАТОРНОГО СЕРЕДОВИЩА

2.1 Схема лабораторного середовища

Тестове лабораторне середовище є невід'ємною частиною сучасних досліджень у галузі кібербезпеки. Воно надає дослідникам, інженерам та фахівцям з безпеки контрольоване та безпечне місце для вивчення кіберзагроз, розробки та тестування методів захисту, а також для відпрацювання сценаріїв реагування на інциденти. Головною перевагою тестового лабораторного середовища є його ізольованість від реальних мереж та систем. Це дозволяє дослідникам безпечно моделювати та аналізувати шкідливу активність, не ризикуючи випадково поширити шкідливий код або вплинути на реальні сервіси. Ізольоване середовище забезпечує повний контроль над параметрами та умовами експерименту, що дозволяє точно відтворювати сценарії атак та вивчати їхній вплив. У лабораторному середовищі можна точно відтворити конфігурацію мереж, систем та пристроїв, які використовуються в реальному світі. Це дозволяє дослідникам моделювати складні багатовекторні атаки, вивчати їхню динаміку та ефективність різних методів захисту. Можливість налаштування різних параметрів мережі та систем дає змогу досліджувати, як певні зміни впливають на безпеку та стійкість до атак.

Тестове середовище є ідеальним місцем для розробки та вдосконалення засобів захисту, таких як брандмауери, системи IDS/IPS, антивірусне програмне забезпечення та інші інструменти. Дослідники можуть без ризику для реальних систем тестувати нові підходи, оптимізувати налаштування та правила, а також оцінювати ефективність захисних механізмів проти різних типів загроз.

Використання тестового середовища дозволяє знизити витрати, пов'язані з дослідженнями та розробками в галузі кібербезпеки. Можливість використовувати віртуалізацію та емулювання зменшує потребу в дорогому фізичному обладнанні. Крім того, виявлення та усунення вразливостей на етапі тестування допомагає уникнути значних витрат, які можуть виникнути внаслідок успішних кібератак на реальні системи. Відпрацювання сценаріїв атак у

лабораторному середовищі дозволяє організаціям підготуватися до можливих реальних загроз.

На рисунку 2.1 показано тестове лабораторне середовище на основі гіпервізора VMware ESXi.

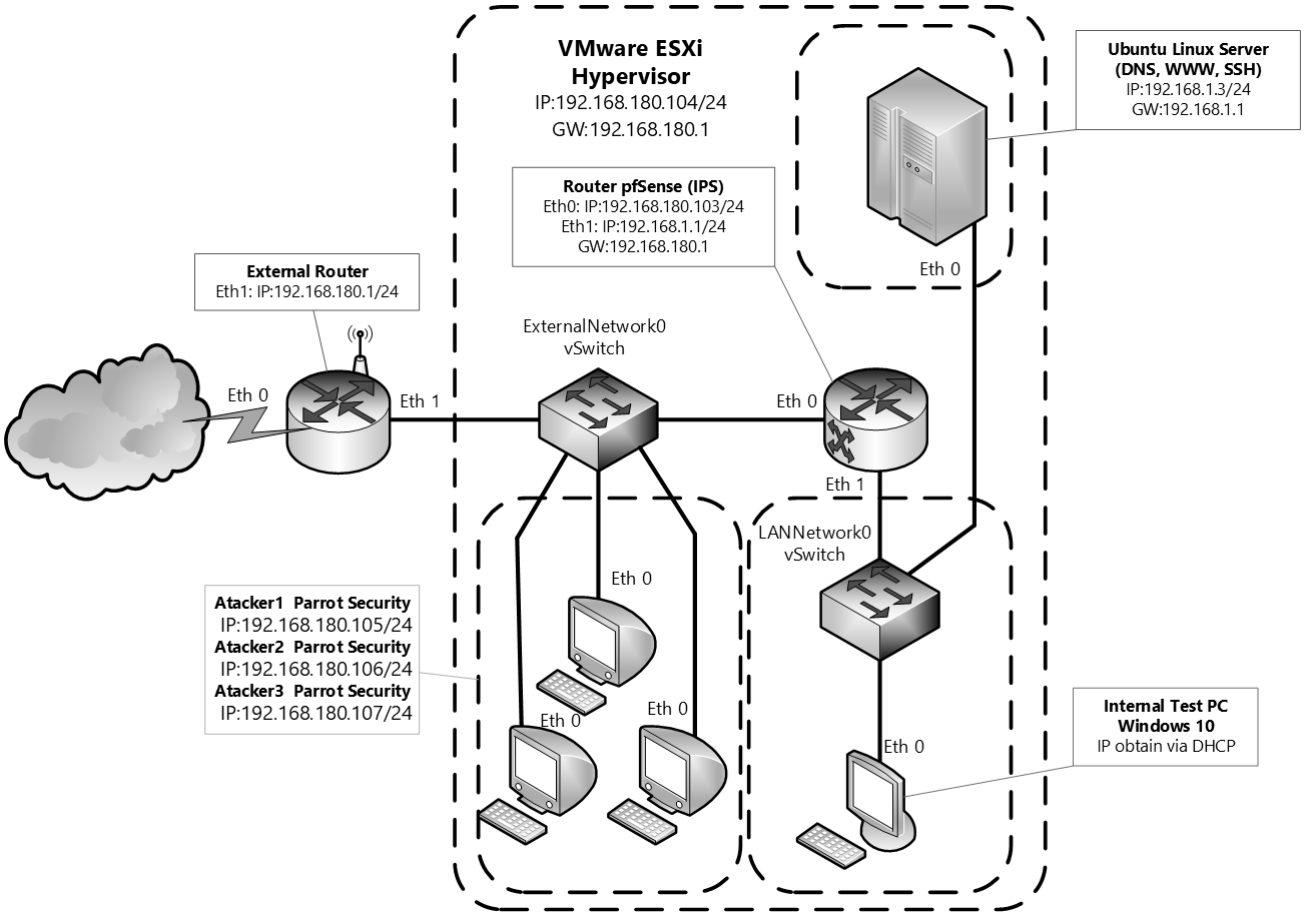


Рисунок 2.1 – Схема тестового середовища

Тестова інфраструктура розроблена з метою моделювання та дослідження кіберзагроз, а також тестування методів захисту в контрольованому середовищі. Вона складається з кількох компонентів, кожен з яких виконує специфічні функції для забезпечення максимально реалістичного та ефективного тестування.

Гіпервізор VMware ESXi встановлений на фізичному сервері з IP-адресою 192.168.180.104/24 та використовує шлюз за замовчуванням 192.168.180.1. ESXi виконує роль основи для віртуалізації, надаючи можливість створювати та керувати віртуальними машинами та мережами. Він забезпечує ресурси для

роботи віртуальних машин і підтримує ізоляцію між ними, що є критично важливим для безпечного моделювання атак та тестування захисних механізмів.

За допомогою гіпервізора ESXi створено дві віртуальні мережі: ExternalNetwork0 та LANNetwork0. Мережа ExternalNetwork0 імітує зовнішню мережу Інтернет або мережу потенційних атакуючих. Вона зв'язана з відповідним віртуальним комутатором (vSwitch) та дозволяє моделювати атаки ззовні. Внутрішня мережа LANNetwork0 представляє корпоративну мережу або мережу організації, яку необхідно захистити. Вона також зв'язана зі своїм віртуальним комутатором і містить сервери та робочі станції.

Зовнішній маршрутизатор (External Router) має IP-адресу 192.168.180.1/24 і виступає як шлюз за замовчуванням для всього віртуалізованого тестового середовища.

Маршрутизатор pfSense забезпечує маршрутизацію трафіку між зовнішньою та внутрішньою віртуальними мережами, фільтрує вхідний та вихідний трафік на основі встановлених правил безпеки та використовує Snort для виявлення та блокування шкідливого трафіку та атак. PfSense має два мережеві інтерфейси. Зовнішній інтерфейс Eth з IP-адресою 192.168.180.103/24, підключений до ExternalNetwork0 vSwitch, і використовує шлюз 192.168.180.1. Внутрішній інтерфейс Eth1 з IP-адресою 192.168.1.1/24, підключений до LANNetwork0.

Це дозволяє pfSense ефективно контролювати та фільтрувати трафік між зовнішньою та внутрішньою мережами, захищаючи внутрішні ресурси від зовнішніх загроз.

Три віртуальні машини під керуванням Parrot Security OS, Attacker1: IP-адреса 192.168.180.105/24, Attacker2: IP-адреса 192.168.180.106/24 та Attacker3: IP-адреса 192.168.180.107/24 використовуються для моделювання атак у лабораторному середовищі. Вони підключені до ExternalNetwork0 та можуть генерувати різні типи шкідливого трафіку для тестування ефективності захисних механізмів pfSense.

Внутрішня мережа (LANNetwork0) представляє корпоративну мережу та включає кілька комп'ютерів та серверів. Сервер Ubuntu Linux виконує роль

сервера DNS, веб-сервера (WWW) та SSH-сервера. Має IP-адресу 192.168.1.130/24 та використовує шлюз 192.168.1.1 (Eth1 pfSense). Цей сервер є ключовою ціллю для атакуючих машин та використовується для моделювання атак на реальні сервіси. Тестовий комп'ютер з Windows 10 підключений до LANNetwork0 та отримує IP-адресу через DHCP-сервер, налаштований на pfSense. Ця машина використовується для моделювання роботи кінцевих користувачів та тестування доступності сервісів під час атак.

Атакуючі машини (Attacker1-3) генерують шкідливий трафік та намагаються атакувати сервер Ubuntu Linux або інші ресурси у внутрішній мережі. Маршрутизатор pfSense аналізує весь вхідний та вихідний трафік між ExternalNetwork0 та LANNetwork0, застосовує правила брандмауера та IPS для виявлення та блокування шкідливих пакетів. Сервер Ubuntu Linux надає сервіси DNS, веб та SSH для внутрішніх та, за потреби, зовнішніх клієнтів. Тестовий комп'ютер з Windows 10 використовується для перевірки доступності сервісів та оцінки впливу атак на користувачів. У цій інфраструктурі можна моделювати різні типи атак, включаючи багатовекторні DDoS-атаки, та тестувати ефективність захисних механізмів. Завдяки використанню реалістичних конфігурацій та сервісів, результати тестування будуть максимально наближеними до реальних умов.

2.2 Налаштування компонентів лабораторного середовища

2.2.1 Гіпервізор VMware ESXi

VMware ESXi є одним із провідних гіпервізорів типу 1 (bare-metal), розробленим компанією VMware (Broadcom) [24]. Він встановлюється безпосередньо на фізичне обладнання, замінюючи традиційну операційну систему, і забезпечує платформу для віртуалізації серверів. Це дозволяє запускати декілька віртуальних машин на одному фізичному сервері, ефективно використовуючи його ресурси та ізолюючи віртуальні машини одна від одної. Архітектура VMware ESXi базується на ядрі VMkernel, яке є спеціалізованою

операційною системою, оптимізованою для віртуалізації. VMkernel керує апаратними ресурсами сервера, такими як процесор, пам'ять, дискові пристрої та мережеві інтерфейси, розподіляючи їх між віртуальними машинами. Гіпервізор, вбудований у VMkernel, забезпечує абстракцію апаратного забезпечення та ізоляцію віртуальних машин, що дозволяє запускати різні операційні системи, включаючи Windows, Linux та інші. З підтримкою апаратної віртуалізації від процесорів Intel (Intel VT-x) та AMD (AMD-V), VMkernel має прямий доступ до процесорів та інструкцій, необхідних для підтримки ізоляції та управління ресурсами віртуальних машин. Це забезпечує високу продуктивність та зменшує накладні витрати, які виникають при використанні гіпервізорів, що працюють на рівні операційної системи.

VMware ESXi підтримує створення віртуальних мереж, що дозволяє налаштовувати складні мережеві топології всередині гіпервізора. За допомогою віртуальних комутаторів (vSwitches) можна налаштовувати віртуальні локальні мережі (VLAN), політики безпеки та якість обслуговування (QoS). Це дає змогу моделювати реалістичні мережеві середовища та контролювати мережевий трафік між віртуальними машинами. Сховище даних в ESXi може бути реалізоване через різні типи сховищ, включаючи локальні диски, мережеві файлові системи NFS, iSCSI та Fibre Channel, що забезпечує гнучкість у виборі сховища для віртуальних машин.

Однією з ключових переваг VMware ESXi є його висока продуктивність. Гіпервізор оптимізований для мінімізації накладних витрат на віртуалізацію, що дозволяє максимально ефективно використовувати апаратні ресурси сервера. Крім того, ESXi забезпечує високий рівень безпеки завдяки малій поверхні атаки, оскільки ядро має невеликий розмір і включає лише необхідні компоненти.

VMware ESXi забезпечує ізоляцію між віртуальними машинами, що дозволяє безпечно моделювати кіберзагрози без ризику впливу на інші системи або мережі. Використання ESXi дозволяє швидко створювати, налаштовувати та видаляти віртуальні машини та мережі, що є критично важливим для тестування різних сценаріїв атак та методів захисту.

Керування VMware ESXi здійснюється через веб-інтерфейс, що надає можливості для управління віртуальними машинами, мережами, сховищами та іншими параметрами гіпервізора (див. рисунок 2.2).

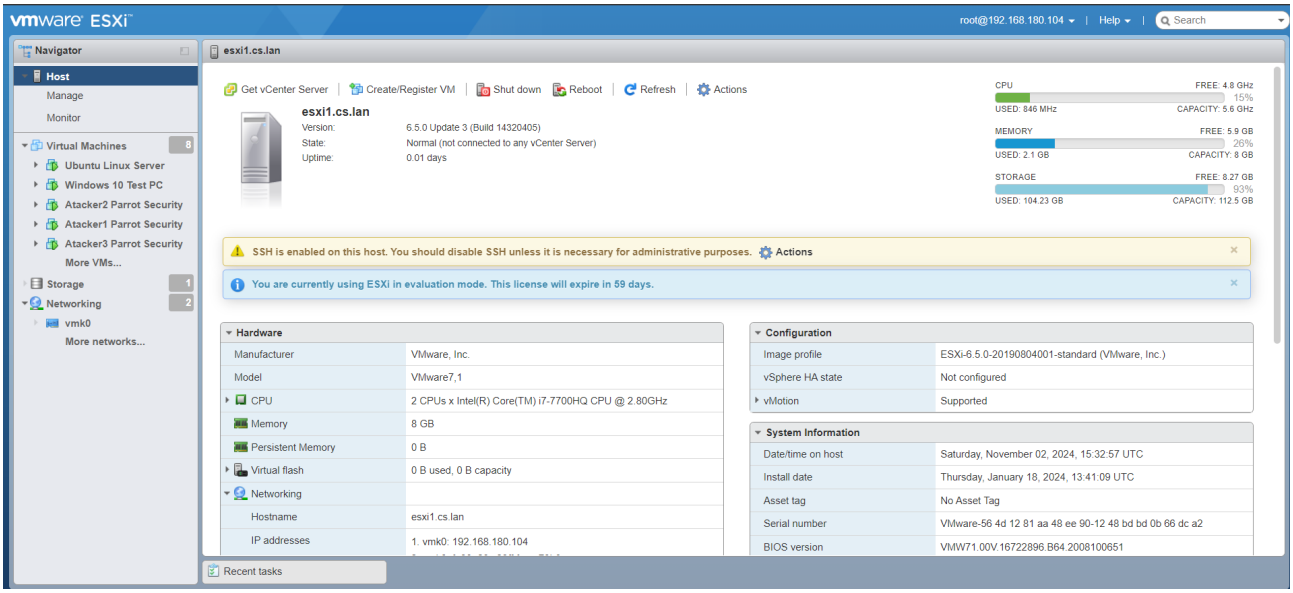


Рисунок 2.2 – Вебінтерфейс керування VMware ESXi

ESXi підтримує рольову модель доступу, що дозволяє надавати різні рівні прав користувачам та групам, забезпечуючи безпеку та контроль доступу. Інтеграція з VMware vCenter Server дозволяє централізовано керувати декількома серверами ESXi, автоматизувати операції, виконувати резервне копіювання та відновлення віртуальних машин, що особливо корисно в масштабних середовищах.

Безпека в ESXi забезпечується через регулярні оновлення та патчі, які VMware надає для усунення вразливостей та покращення стабільності системи. Вбудовані засоби логування та аудиту дозволяють відслідковувати дії користувачів та події системи, що важливо для діагностики та забезпечення безпеки. Серед розширених можливостей VMware ESXi варто відзначити підтримку високої доступності (HA), розподіленого ресурсного планування (DRS) та функції міграції віртуальних машин без простою (vMotion). Це забезпечує безперервність сервісів та гнучкість управління ресурсами в корпоративних середовищах.

2.2.2 Маршрутизатор pfSense

Операційна система pfSense — це популярний програмний маршрутизатор з відкритим вихідним кодом, заснований на FreeBSD, який також виконує функції брандмауера та IPS [25]. Розроблений з акцентом на безпеку, гнучкість та функціональність, pfSense широко використовується як у великих корпоративних мережах, так і в домашніх середовищах, де потрібно ефективне та надійне мережеве рішення. Pfsense підтримує повний набір функцій для маршрутизації трафіку між різними мережами, включаючи IPv4 та IPv6. Це рішення може використовуватися як шлюз між зовнішньою та внутрішньою мережею, забезпечуючи маршрутизацію з високою пропускною здатністю. З його допомогою можна налаштовувати статичні маршрути, використовувати протоколи динамічної маршрутизації, такі як OSPF і BGP, а також створювати віртуальні локальні мережі для сегментації трафіку. Це дозволяє адаптувати pfSense до вимог складних мережевих середовищ та забезпечити гнучкість у конфігурації маршрутів.

Маршрутизатор pfSense також виконує роль повнофункціонального брандмауера, підтримуючи налаштування правил фільтрації трафіку на основі IP-адрес, портів, протоколів та інших параметрів. Це дозволяє обмежувати доступ до мережі, блокувати небажаний трафік і захищати внутрішню мережу від зовнішніх загроз. Брандмауер pfSense також підтримує налаштування політик безпеки на основі часу, що дозволяє активувати або деактивувати певні правила в задані періоди, що є корисним для планування обмежень у мережевій діяльності. Pfsense має інтеграцію з системою виявлення та запобігання вторгненням Snort або Suricata, які можна встановити як додаткові модулі. Ці інструменти використовуються для моніторингу трафіку в реальному часі та виявлення шкідливих активностей, таких як атаки, експлойти та інші аномальні дії. Налаштування IPS дозволяє блокувати шкідливий трафік ще до того, як він досягне внутрішньої мережі, що значно підвищує рівень захисту. Це робить pfSense потужним інструментом для протидії кіберзагрозам і забезпечує активний захист мережі.

Ще однією важливою функцією pfSense є можливість налаштування VPN-з’єднань. Він підтримує різні протоколи VPN, такі як OpenVPN та IPsec, що дозволяє створювати безпечні канали зв’язку між віддаленими мережами або користувачами. Це особливо корисно для організацій, які потребують захищеного доступу до ресурсів внутрішньої мережі з віддалених локацій. VPN на базі pfSense може бути налаштований як клієнт або сервер, що забезпечує гнучкість у побудові інфраструктури віддаленого доступу. Маршрутизатор pfSense включає вбудовані засоби моніторингу та аналізу трафіку, що дозволяє адміністраторам стежити за станом мережі та ідентифікувати потенційні проблеми. Веб-інтерфейс pfSense дозволяє зручно налаштовувати та контролювати всі параметри маршрутизатора, брандмауера, VPN і IPS, а також відстежувати продуктивність мережі. Також є можливість переглядати журнали подій та налаштовувати сповіщення, що дозволяє швидко реагувати на інциденти безпеки та зміни в мережевій активності. Pfsense підтримує балансування навантаження та агрегацію каналів, що дозволяє оптимізувати використання інтернет-з'єднань. Це корисно для забезпечення стабільності з'єднань та підвищення загальної пропускної здатності мережі, особливо в умовах великого обсягу трафіку або коли потрібен резервний канал для підвищення надійності. Завдяки цій функції pfSense здатний розподіляти навантаження між кількома інтернет-з’єднаннями та автоматично перемикатися на альтернативне з’єднання у випадку збоїв.

Завдяки своїй гнучкості та розширюваності, pfSense підтримує встановлення додаткових пакетів, таких як Squid для кешування та фільтрації веб-контенту або pfBlockerNG для блокування реклами та зловмисних IP-адрес. Це дозволяє легко розширювати функціональність pfSense та адаптувати його до специфічних потреб мережі, забезпечуючи інструменти для контролю доступу до веб-ресурсів і захисту від небажаного контенту. Маршрутизатор pfSense використовується в багатьох професійних середовищах, оскільки він є стабільним, надійним і економічно вигідним рішенням. Його гнучкість дозволяє налаштовувати та оптимізувати мережу для вирішення як базових, так і складних завдань з безпеки та маршрутизації. Можливість оновлення та обслуговування в

реальному часі забезпечує безперервність роботи мережі та надає адміністраторам інструменти для швидкого внесення змін.

Маршрутизатор pfSense забезпечує високу ізоляцію між різними мережами, дозволяючи будувати складні багатошарові мережі з поділом на зони безпеки (DMZ, гостьові мережі та ін.). Це дозволяє захищати критично важливі сервіси та обмежувати доступ між сегментами, підвищуючи загальний рівень безпеки. Здатність pfSense функціонувати як багатофункціональний маршрутизатор і брандмауер робить його ідеальним рішенням для розгортання в тестових і продуктивних середовищах, де необхідно контролювати трафік та забезпечувати захист від загроз.

Панель адміністрування pfSense є веб-інтерфейсом, який забезпечує доступ до всіх функцій маршрутизатора, брандмауера, VPN та інших компонентів. Вона дозволяє налаштовувати мережеві параметри, керувати захистом, стежити за станом мережі та здійснювати діагностику. Доступ до панелі адміністрування здійснюється через веб-браузер за IP-адресою маршрутизатора (зазвичай 192.168.1.1) після введення логіна і пароля адміністратора (див. рисунок 2.3).

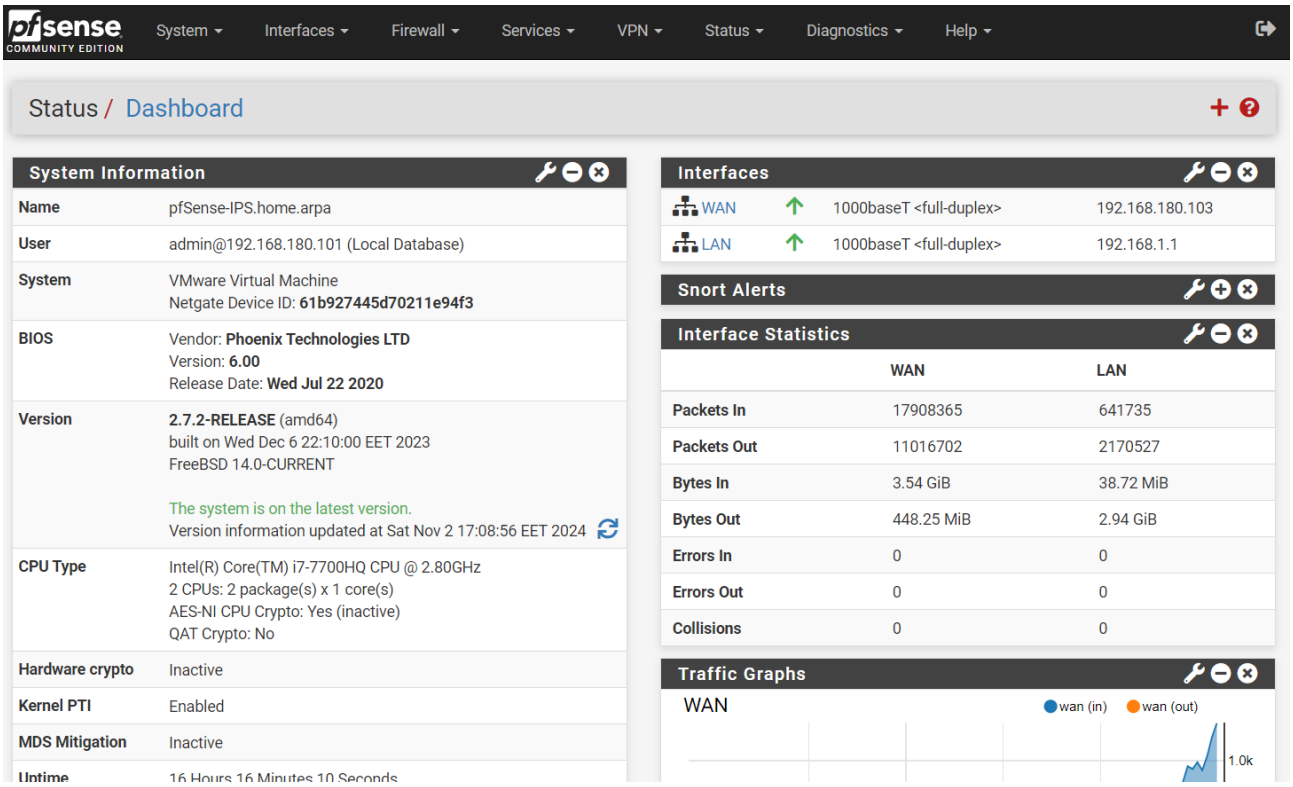


Рисунок 2.3 – Панель адміністрування pfSense

Панель адміністрування має чіткий і структурований інтерфейс з навігаційним меню, яке включає різні розділи для управління налаштуваннями. Основна сторінка панелі надає інформацію про стан системи, включаючи IP-адресу, стан підключень, використання ресурсів, завантаження процесора та пам’яті, версію pfSense та доступні оновлення. Це дозволяє адміністраторам одразу бачити загальну інформацію про поточний стан системи та її продуктивність.

Розділ System містить налаштування системи, такі як адміністрування користувачів, резервне копіювання конфігурації, оновлення та налаштування часу. Тут також можна налаштувати основні параметри мережевих інтерфейсів та створити резервну копію поточної конфігурації. Розділ Interfaces призначений для управління мережевими інтерфейсами, такими як WAN, LAN і будь-які додаткові інтерфейси. Адміністратори можуть призначати IP-адреси, налаштовувати параметри DHCP, додавати нові мережеві інтерфейси та налаштовувати VLAN. Це дозволяє гнучко адаптувати мережеву конфігурацію під потреби конкретного середовища. Розділ Firewall є один з найважливіших розділів, який дозволяє налаштовувати правила брандмауера для керування потоком трафіку між інтерфейсами. У цьому розділі можна створювати правила на основі IP-адрес, портів, протоколів та встановлювати правила для обмеження доступу, блокування трафіку або його дозволу. Тут також налаштовуються політики NAT, що дозволяє перетворювати внутрішні IP-адреси у зовнішні для доступу до інтернету. Розділ VPN використовується для налаштування віртуальних приватних мереж. pfSense підтримує кілька типів VPN, зокрема OpenVPN, IPsec та інші. Через цей розділ можна налаштувати VPN-сервер або клієнт, що дозволяє користувачам підключатися до мережі безпечно з віддалених місць. Адміністратори можуть налаштовувати аутентифікацію, параметри шифрування та контроль доступу для забезпечення високого рівня безпеки. Services використовується для управління додатковими сервісами, такими як DHCP-сервер, DNS-сервер, Dynamic DNS, SNMP, та інших служб. Тут також налаштовуються сервіси кешування (Squid) та фільтрації веб-контенту (SquidGuard) для контролю доступу до веб-ресурсів та оптимізації використання

мережевих ресурсів. Розділ Diagnostics призначений для діагностики та містить інструменти для тестування мережевих підключень, пінгування, трасування маршрутів, перегляду журналів і стану підключень. Ці інструменти дозволяють швидко виявляти та виправляти мережеві проблеми. Також у цьому розділі доступні журнали активності, що допомагають відстежувати події в мережі та аналізувати інциденти безпеки. У розділі Status відображається інформація про поточний стан системи, включаючи інформацію про використання ресурсів, стан мережевих інтерфейсів, активні VPN-з'єднання, використання смуги пропускання та інші показники. Тут можна відслідковувати поточний трафік і спостерігати за змінами в реальному часі, що є корисним для моніторингу продуктивності. Розділ Packages призначений для управління додатковими пакетами, які розширюють функціональність pfSense. Через цей розділ можна встановлювати пакети, такі як Snort для виявлення загроз, pfBlockerNG для блокування зловмисних IP-адрес, Squid для кешування та інші. Завдяки цьому можна легко адаптувати pfSense під потреби конкретної мережі та забезпечити високий рівень безпеки.

У панелі адміністрування також є можливість налаштування журналів подій та сповіщень, що дозволяє відстежувати критичні події та отримувати повідомлення про зміни у стані мережі або виявлення підозрілої активності. Така функція дозволяє адміністраторам оперативно реагувати на проблеми та потенційні загрози, забезпечуючи безперервний контроль за роботою системи.

Завдяки зручному інтерфейсу та розвиненій системі налаштувань панель адміністрування pfSense є потужним інструментом для управління мережею, забезпечення безпеки та гнучкого налаштування всіх параметрів. Вона дозволяє адміністраторам легко адаптувати pfSense до вимог конкретного середовища та забезпечувати стабільну роботу мережевої інфраструктури з високим рівнем захисту від зовнішніх та внутрішніх загроз.

2.2.3 Сервер Ubuntu Linux

Сервер на базі Ubuntu Linux є одним із найпопулярніших і найнадійніших рішень для розгортання серверних служб та забезпечення стабільної роботи мережевої інфраструктури [26]. Ubuntu Server, розроблений компанією Canonical, використовує ядро Linux і відрізняється високою стабільністю, безпекою та широкими можливостями налаштування. Він має відкритий вихідний код, що робить його гнучким і дозволяє адаптувати під специфічні потреби організації. Ubuntu Server підтримує регулярні оновлення та тривалу підтримку версій LTS (Long Term Support), що забезпечує надійну базу для використання в корпоративних середовищах.

Однією з головних переваг Ubuntu Server є його універсальність, оскільки він може виконувати різноманітні ролі в мережі. Він підтримує функції DNS-сервера, веб-сервера, FTP-сервера, поштового сервера, бази даних, а також виконує роль сервера додатків. Це дозволяє розгортати на одному сервері кілька критично важливих для мережі служб, що оптимізує використання ресурсів і знижує витрати на інфраструктуру. Крім того, Ubuntu Linux має потужну систему управління пакетами APT, що дозволяє легко встановлювати, оновлювати та налаштовувати необхідні програмні компоненти.

Сервер налаштований для виконання ролей DNS-сервера, веб-сервера та SSH-сервера, є основним компонентом тестового середовища та виступає як ціль для атакуючих машин. Цей сервер дозволяє моделювати реальні сценарії кіберзагроз, що спрямовані на критично важливі мережеві сервіси, які часто піддаються атакам у реальному житті. Вибір саме цих сервісів не випадковий, адже DNS, веб-сервіс і SSH часто є першочерговими цілями для зловмисників, оскільки кожен із них має унікальні вразливості та може бути використаний для різних типів атак.

DNS-сервер, налаштований на Ubuntu Linux за допомогою BIND, є одним із ключових сервісів, що забезпечують обслуговування запитів на перетворення доменних імен в IP-адреси. DNS-сервери часто стають мішенню для DDoS-атак.

Веб-сервер, розгорнутий на Ubuntu Linux, забезпечує обслуговування HTTP та HTTPS-запитів за допомогою Nginx. Цей сервіс дає змогу моделювати атаки

на веб-додатки, такі як HTTP Flood та інші загрози, що часто зустрічаються у веб-середовищах.

SSH-сервер, встановлений на Ubuntu, є критичним для забезпечення віддаленого доступу до системи. Він дозволяє адміністраторам підключатися до сервера для налаштування та управління, однак водночас є популярною ціллю для атак типу brute-force, де зловмисники намагаються підбирати паролі для отримання доступу до системи. У рамках моделювання атак SSH-сервер дозволяє досліджувати захисні механізми проти атак brute-force та інших спроб несанкціонованого доступу, таких як сканування портів і атаки на слабкі паролі.

Використання Ubuntu Linux для цих ролей забезпечує гнучкість та реалістичність тестового середовища. Оскільки кожен із цих сервісів є важливим для підтримки функціонування корпоративних мереж, сервер на Ubuntu дозволяє дослідникам моделювати складні сценарії атак та оцінювати, як захисні системи реагують на кіберзагрози, направлені на реальні сервіси. Це забезпечує більш достовірні результати, які можуть бути використані для вдосконалення стратегій захисту та виявлення вразливих місць у безпеці.

На рисунку 2.4 показано командний інтерфейс операційної системи Ubuntu, де відображені мережеві налаштування Ubuntu Linux.

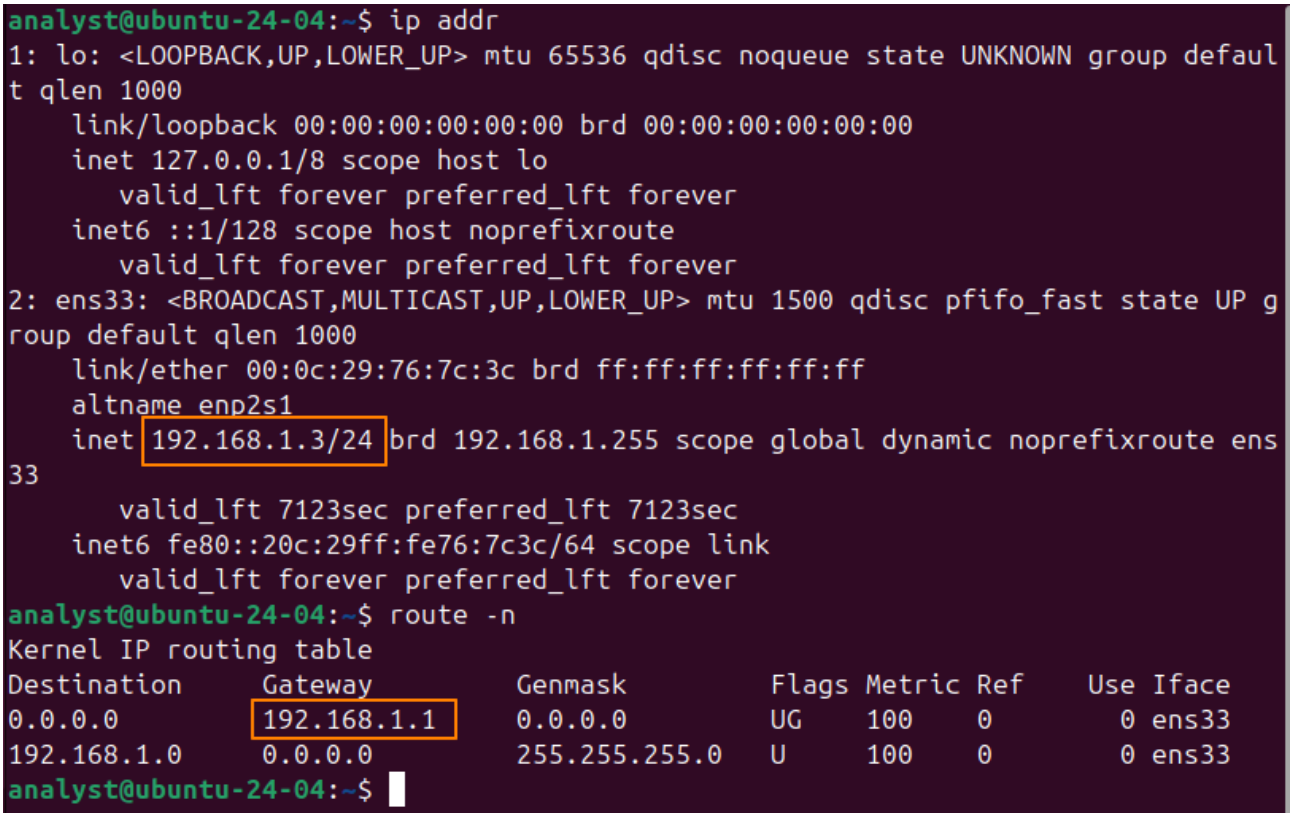


Рисунок 2.4 – Мережеві налаштування Ubuntu Linux

Команда `ip addr` показує інформацію про мережеві інтерфейси. Команда `route -n` показує таблицю маршрутизації.

На рисунку 2.5 показано, що на хості працюють сервіси DNS, SSH, HTTP та SMTP, кожен з яких надає специфічні мережеві функції.

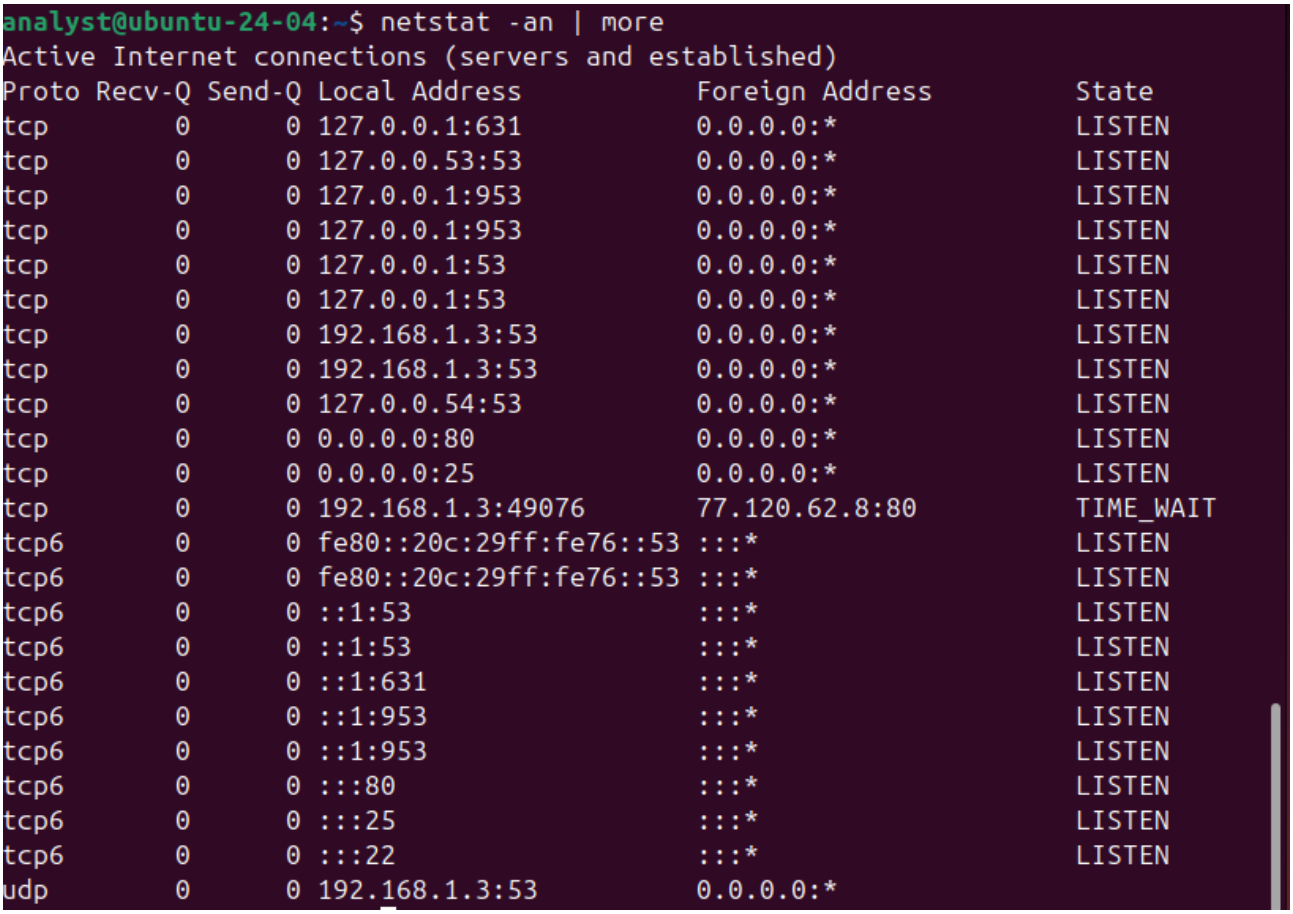


Рисунок 2.5 – Статус сервісів в Ubuntu Linux

Сервіс DNS працює на порту 53 для протоколів tcp і udp, і доступний як на локальному інтерфейсі 127.0.0.1, так і на внутрішньому інтерфейсі 192.168.1.3. Це дозволяє обробляти DNS-запити як з локальних процесів, так і з інших пристроїв у локальній мережі. Сервіс SSH, працює на порту 22. SSH дозволяє безпечний віддалений доступ до хоста для адміністрування та управління системою. Сервіс HTTP працює на порті 80 tcp. Порт 80 слухає на всіх інтерфейсах (0.0.0.0), що дає змогу обслуговувати HTTP-запити з будь-якої IP-адреси в мережі. Сервіс SMTP для надсилання електронної пошти використовує порт 25.

Використання цих сервісів у лабораторному середовищі надає можливість імітувати реальні умови для тестування різних типів атак.

2.2.4 Операційна система Parrot Security

Parrot Security — це спеціалізована операційна система на базі Debian GNU/Linux, розроблена для професіоналів у галузі кібербезпеки, цифрової криміналістики та тестування на проникнення [27]. Вона поєднує стабільність та надійність Debian з легким та ефективним робочим середовищем MATE, що забезпечує швидку та зручну роботу навіть на системах з обмеженими ресурсами. Parrot Security поставляється з великим набором попередньо встановлених інструментів, які охоплюють різні аспекти кібербезпеки. Серед них є засоби для аналізу мереж, виявлення вразливостей, експлуатації, зворотного інжинірингу, цифрової криміналістики та анонімного веб-серфінгу. Це робить систему універсальним інструментом для фахівців, які займаються оцінкою безпеки та розробкою захисних заходів.

Parrot Security активно підтримується та оновлюється спільнотою розробників і ентузіастів. Регулярні оновлення забезпечують актуальність інструментів та захист від новітніх загроз. Система має доступ до власних репозиторіїв програмного забезпечення, що містять спеціалізовані пакети для кібербезпеки, а також використовує репозиторії Debian для базових компонентів.

Серед інструментів, включених у Parrot Security, можна виділити такі:

- сканери вразливостей Nmap, OpenVAS, Nikto та інші для аналізу мереж та виявлення потенційних слабких місць;
- Metasploit Framework для запуску експлойтів;
- інструменти для зворотного інжинірингу Radare2, Ghidra для аналізу бінарних файлів та пошуку вразливостей у програмному забезпеченні;

Parrot Security також оптимізована для роботи у віртуальних середовищах, що робить її зручною для використання в лабораторіях та тестових стендах. Система підтримує різні платформи віртуалізації, що дозволяє легко інтегрувати її в існуючу інфраструктуру.

Parrot Security надає можливість відпрацьовувати практичні навички в безпечному та контрольованому середовищі, моделюючи різноманітні сценарії атак. Це сприяє глибшому розумінню принципів кібербезпеки та розвитку професійних компетенцій.

На рисунку 2.6 показано мережеві налаштування та таблицю маршрутизації в операційній системі Parrot Security Atacker 1.

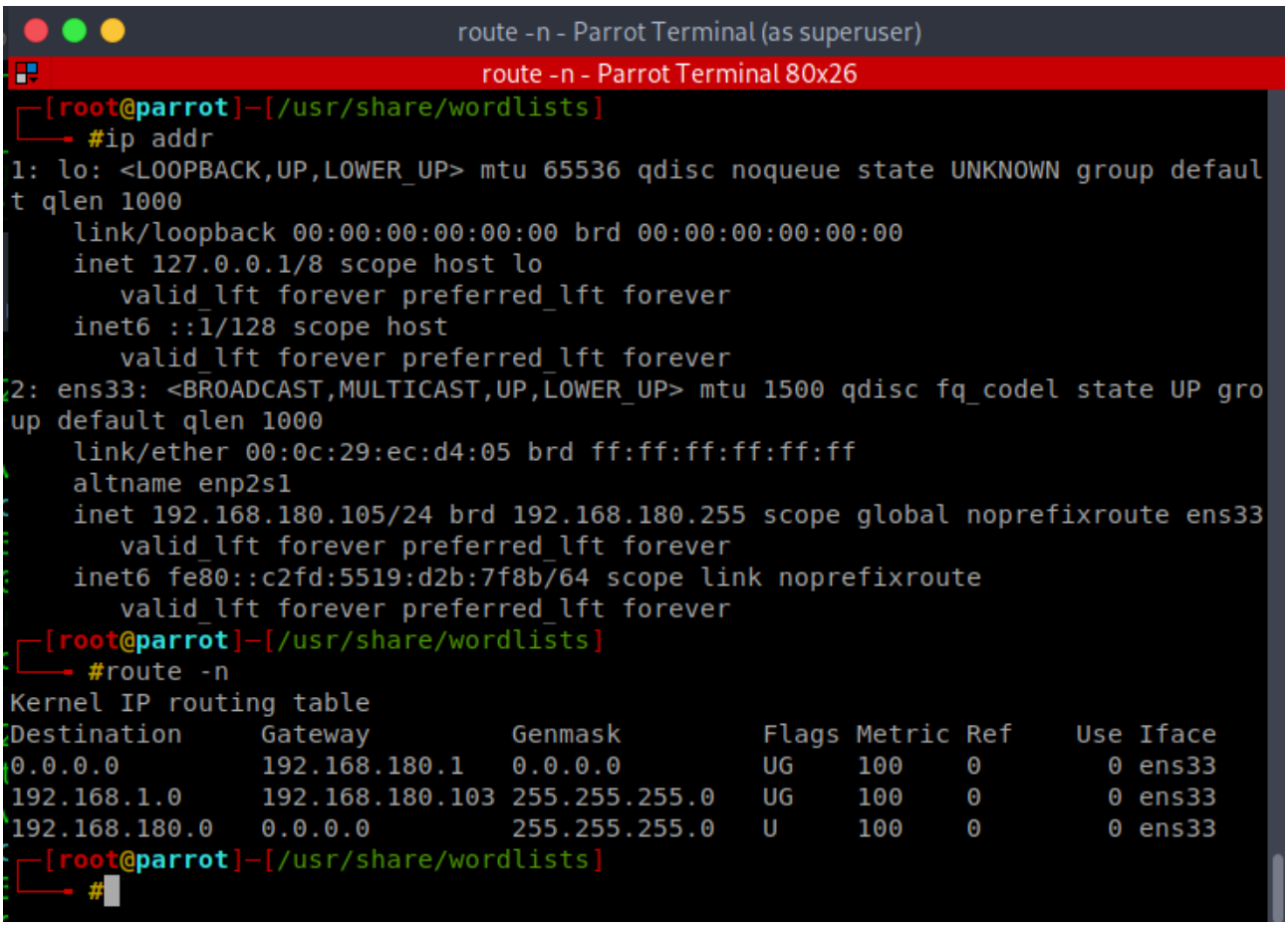


Рисунок 2.6 – Мережеві налаштування та таблицю маршрутизації в операційній системі Parrot Security Atacker 1

Аналогічні налаштування таблиці маршрутизації проведено на Atacker 2 та Atacker 3.

2.3 Тестування лабораторного середовища

Тестування лабораторного середовища є критичним етапом для забезпечення його коректної роботи та ефективності в моделюванні кіберзагроз і методів захисту. Воно дозволяє переконатися, що всі компоненти інфраструктури налаштовані правильно, взаємодіють між собою належним чином і готові до проведення експериментів та досліджень.

На рисунку 2.7 показано вивід команди `mtr` в операційній системи Ubuntu Linux, яка виконує трасування мережевого шляху від комп'ютера з IP-адресою 192.168.1.3 до цільового хоста з IP-адресою 192.168.180.105. Утиліта відображає кількість втрачених пакетів, затримку та статистику по кожному вузлу на шляху до цілі.

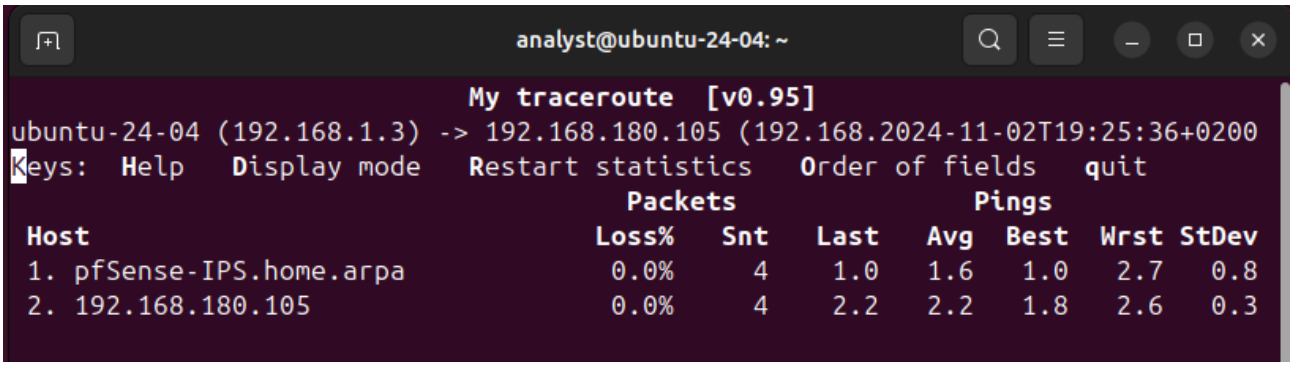


Рисунок 2.7 – Вивід команди `mtr` в операційній системи Ubuntu Linux

Перший вузол — це маршрутизатор pfSense-IPS.home.arpa, який віртуальним маршрутизатором. Втрати пакетів (Loss%) становлять 0%, що означає стабільне з'єднання через цей вузол. Середній час затримки (Avg) становить 1.6 мс, що вказує на швидке проходження трафіку через цей маршрутизатор. Другий вузол — це цільовий хост (Atacker1) із IP-адресою 192.168.180.105. Втрат пакетів також немає (0%), середня затримка становить 2.2 мс. Це вказує на стабільне з'єднання з цільовим хостом.

На рисунку 2.8 показано результат виконання команди `traceroute` до IP-адреси 192.168.1.3 в операційній системі Parrot Security Atacker 1. Трасування показує шлях пакетів від вихідної системи до цільового хоста через два вузли.

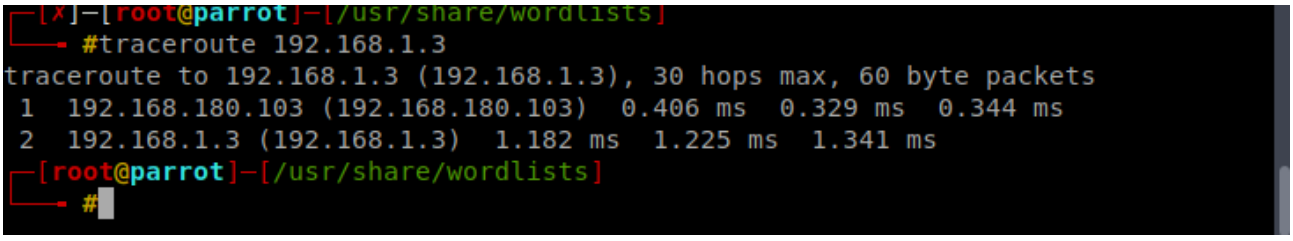


Рисунок 2.8 – Вивід команди `traceroute` в операційній системи Parrot Security Atacker 1

Перший вузол має IP-адресу 192.168.180.103. Це маршрутизатор pfSense, який пересилає пакети до цільової IP-адреси. Затримка для цього вузла коливається від 0.329 мс до 0.406 мс, що вказує на швидке та стабільне з'єднання.

Другий вузол — це цільовий хост Ubuntu Linux із IP-адресою 192.168.1.3. Затримка до цього вузла складає приблизно 1.182–1.341 мс, що також свідчить про хорошу швидкість з'єднання без значних затримок.

На рисунку 2.9 показано результат сканування портів хоста Ubuntu Linux, виконаного за допомогою команди `nmap` з операційній системи Parrot Security Atacker 1

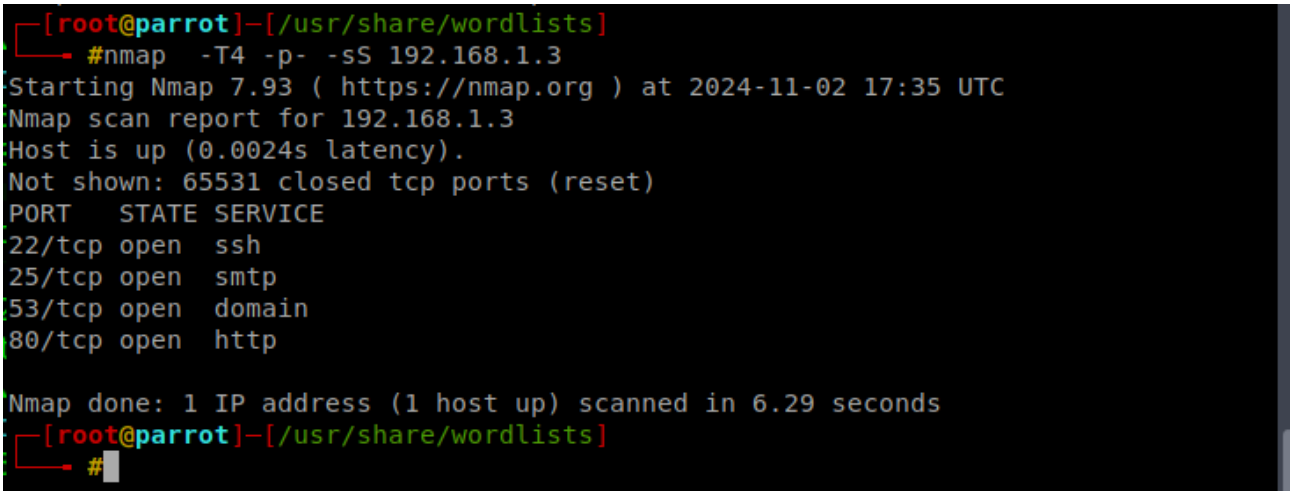


Рисунок 2.9 – Результат сканування портів хоста Ubuntu Linux з операційній системи Parrot Security Atacker 1

Сканування показало, що хост Ubuntu Linux має чотири відкриті порти, які відповідають основним мережевим сервісам: SSH, SMTP, DNS і HTTP.

Проведені тестування підтверджують, що лабораторне тестове середовище налаштоване коректно та готове до проведення експериментів і досліджень. Результати команди `mtr` в операційній системі Ubuntu Linux демонструють стабільне з'єднання між комп'ютером з IP-адресою 192.168.1.3 та цільовим хостом з IP-адресою 192.168.180.105. Відсутність втрат пакетів та низькі значення затримки свідчать про правильну конфігурацію мережі та ефективну маршрутизацію через маршрутизатор pfSense.

Виконання команди `traceroute` з операційної системи Parrot Security Atacker 1 показало, що пакети успішно проходять через маршрутизатор pfSense до цільового хоста Ubuntu Linux з мінімальними затримками. Це вказує на те, що маршрутизація налаштована правильно, і мережеві шляхи між зовнішньою та внутрішньою мережами функціонують безперебійно.

Результати сканування портів хоста Ubuntu Linux за допомогою команди `nmap` підтвердили доступність основних мережевих сервісів: SSH, SMTP, DNS і HTTP. Відкриті порти свідчать про те, що серверні служби запущені та працюють належним чином, що є критично важливим для моделювання реальних сценаріїв атак.

Таким чином, усі компоненти інфраструктури - гіпервізор VMware ESXi, маршрутизатор pfSense, атакуючі машини на базі Parrot Security OS та сервер Ubuntu Linux взаємодіють між собою коректно. Мережеві з'єднання стабільні, сервіси доступні та функціонують відповідно до очікувань. Лабораторне середовище повністю готове до моделювання кіберзагроз та тестування методів захисту, що дозволить проводити подальші експерименти з високою ефективністю та достовірністю результатів.

2.4 Висновки до розділу 2

В другому розділі було детально описано процес налаштування тестового лабораторного середовища для моделювання кіберзагроз та тестування методів захисту. Розглянуто схему лабораторного середовища, яке базується на гіпервізорі VMware ESXi і включає кілька компонентів, кожен з яких виконує специфічні функції для забезпечення реалістичного та ефективного тестування.

Було встановлено та налаштовано гіпервізор VMware ESXi, який забезпечує ізоляцію між віртуальними машинами та ефективне використання апаратних ресурсів. Детально проаналізовано його архітектуру, можливості апаратної віртуалізації та переваги використання у тестовому середовищі.

Маршрутизатор pfSense був налаштований як ключовий елемент безпеки мережі, виконуючи функції брандмауера та IPS. Описано його можливості щодо

маршрутизації трафіку між зовнішньою та внутрішньою мережами, фільтрації трафіку та використання додаткових модулів для підвищення рівня захисту. Сервер Ubuntu Linux налаштовано для виконання ролей DNS-сервера, веб-сервера, поштового сервера та SSH-сервера. Він виступає як ціль для моделювання реальних сценаріїв атак, що дозволяє тестувати ефективність захисних механізмів проти різних типів загроз. Також було налаштовано атакуючі машини на базі операційної системи Parrot Security, яка надає широкий набір інструментів для тестування на проникнення та аналізу безпеки. Це дозволяє моделювати різноманітні кіберзагрози в контрольованому середовищі.

Проведено тестування лабораторного середовища, включаючи перевірку мережевих з'єднань, доступності сервісів та ефективності маршрутизації. Результати тестування підтвердили, що всі компоненти інфраструктури налаштовані правильно та готові до проведення експериментів і досліджень.

РОЗДІЛ 3 ВПРОВАДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ

3.1 Моделювання кіберзагроз

Моделювання кіберзагроз є ключовим елементом у сучасній кібербезпеці, оскільки воно дозволяє дослідникам навчитись передбачати, виявляти та нейтралізувати потенційні атаки на інформаційні системи. Цей процес включає аналіз можливих вразливостей, сценаріїв атак та методів, які зловмисники можуть використовувати для компрометації систем. Моделювання допомагає зрозуміти, як зловмисники мислять і діють, що дозволяє розробляти ефективні стратегії захисту та реагування.

Одним із основних аспектів моделювання кіберзагроз є створення реалістичних сценаріїв атак, які відображають поточні та майбутні загрози. Це може включати моделювання різних типів атак, таких як DDoS, експлойти на основі вразливостей програмного забезпечення та інші. Використовуючи ці сценарії, організації можуть оцінити свою стійкість до атак, виявити слабкі місця в системах та процесах, а також розробити заходи для їх усунення.

Тестове лабораторне середовище є ідеальною платформою для моделювання кіберзагроз. Воно забезпечує контрольоване та безпечне середовище, де можна відтворювати мережеві топології, системи та сервіси. Це дозволяє фахівцям з безпеки проводити експерименти з різними типами атак, не ризикуючи поширити шкідливий код або спричинити реальні збитки. У такому середовищі можна точно налаштувати параметри систем, симулювати поведінку користувачів та зловмисників, а також оцінювати ефективність різних методів захисту.

3.1.1 DDoS атаки

DDoS-атаки є одним з найпоширеніших та найнебезпечніших видів кіберзагроз. Метою таких атак є порушення доступності сервісів шляхом

перевантаження мережевих ресурсів чи серверів великою кількістю запитів або спеціально сформованих пакетів. Зловмисники використовують ботнети або інші ресурси, щоб генерувати великий обсяг трафіку з численних джерел, що ускладнює виявлення і блокування атаки. DDoS-атаки можуть впливати на різні рівні моделі OSI — від мережевого рівня до рівня застосунків — і можуть приймати форми атак типу SYN Flood, UDP Flood, ICMP Flood, HTTP Flood тощо.

Одним із ефективних інструментів для моделювання DDoS-атак є hping3. Це консольна утиліта для генерації мережевого трафіку, яка дозволяє гнучко налаштовувати параметри пакетів і є корисною для тестування мережевих пристроїв і захисних механізмів. З hping3 можна моделювати такі атаки, як SYN Flood, UDP Flood, ICMP Flood та інші види мережевих атак, змінюючи параметри заголовків пакетів і встановлюючи потрібну частоту надсилання.

На рисунку 3.1 показано моделювання атаки типу SYN Flood за допомогою hping3 в Parrot Security Atacker 1.

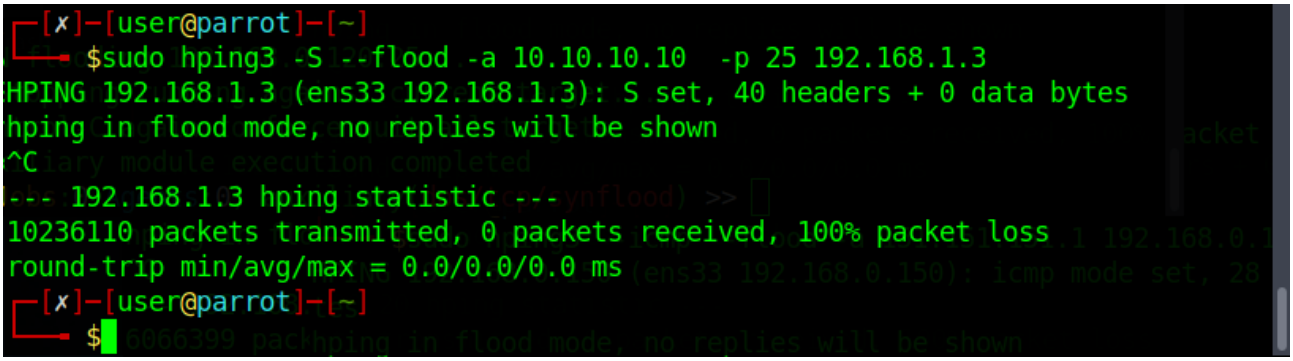


Рисунок 3.1 – SYN Flood атака на хост Ubuntu Linux з операційної системи Parrot Security Atacker 1

Використовується параметру `-S`, яка вказує на надсилання TCP SYN-пакетів, та `--flood`, яка активує режим безперервної передачі пакетів. Така атака перевантажує сервер великою кількістю запитів на встановлення з'єднань, що може призвести до виснаження ресурсів сервера через велику кількість незавершених з'єднань. SYN Flood є одним із найефективніших методів атак на

мережевому рівні, особливо якщо сервер не має відповідного захисту від таких запитів.

На рисунку 3.2 показано моделювання атаки типу UDP Flood за допомогою hping3 в Parrot Security Atacker 2.

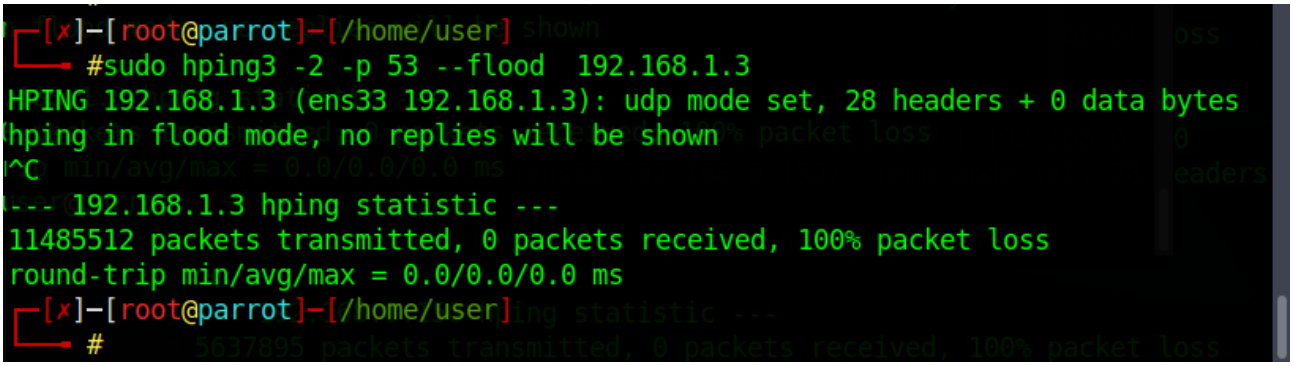


Рисунок 3.2 – UPD Flood атака на хост Ubuntu Linux з операційної системи Parrot Security Atacker 2

Ця команда надсилає UDP-пакети до 53 порту на цільовому хості, що може спричинити перевантаження мережевих ресурсів.

На рисунку 3.3 показано моделювання атаки типу ICMP Flood за допомогою hping3 в Parrot Security Atacker 3.

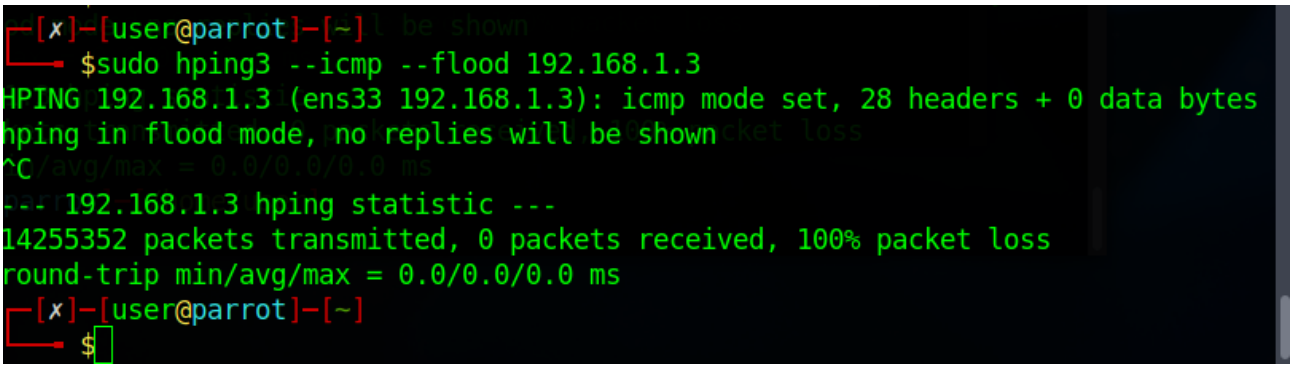


Рисунок 3.3 – ICMP Flood атака на хост Ubuntu Linux з операційної системи Parrot Security Atacker 3

Ця команда надсилає безперервний потік ICMP-пакетів (echo request) до цілі, що може швидко виснажити пропускну здатність мережі або серверні ресурси, особливо якщо ICMP-пакети надходять із високою частотою.

Утиліта hping3 дозволяє гнучко налаштовувати параметри заголовків, зокрема IP-адреси, порти, прапорці TCP та частоту надсилання. Завдяки цьому можна імітувати широкий спектр атак, які будуть дуже схожими на реальні загрози. Це дозволяє тестувати здатність захисних механізмів, таких як брандмауери або системи виявлення та IPS, виявляти і блокувати DDoS-трафік.

DDoS-атаки, спрямовані на веб-сервіси, є одним із найпоширеніших способів виведення серверів з ладу шляхом перевантаження їхнього процесора, пам’яті або пропускної здатності мережі. Один із видів таких атак, відомий як HTTP Flood, використовує велике число запитів на рівні застосунків, що імітують справжні HTTP-запити від користувачів. Мета таких атак — виснажити ресурси веб-сервера, змусивши його обробляти надмірну кількість запитів до веб-сторінок, що може призвести до недоступності сервісу для легітимних користувачів.

Apache Benchmark (ab) — це утиліта для тестування продуктивності веб-серверів, яка дозволяє генерувати великий обсяг HTTP-запитів до певного URL. Хоча вона спочатку розроблялася для вимірювання продуктивності, ab також можна використовувати для моделювання атак на веб-сервери, оскільки вона здатна генерувати великий обсяг запитів за короткий проміжок часу. Це робить ab корисним інструментом для імітації HTTP Flood атак, що дозволяє тестувати здатність серверів обробляти великий обсяг одночасного трафіку.

Для моделювання атаки на веб-сервер із використанням ab, можна використати таку команду:

На рисунку 3.4 показано моделювання атаки типу HTTP Flood за допомогою ab в Parrot Security Atacker 1.

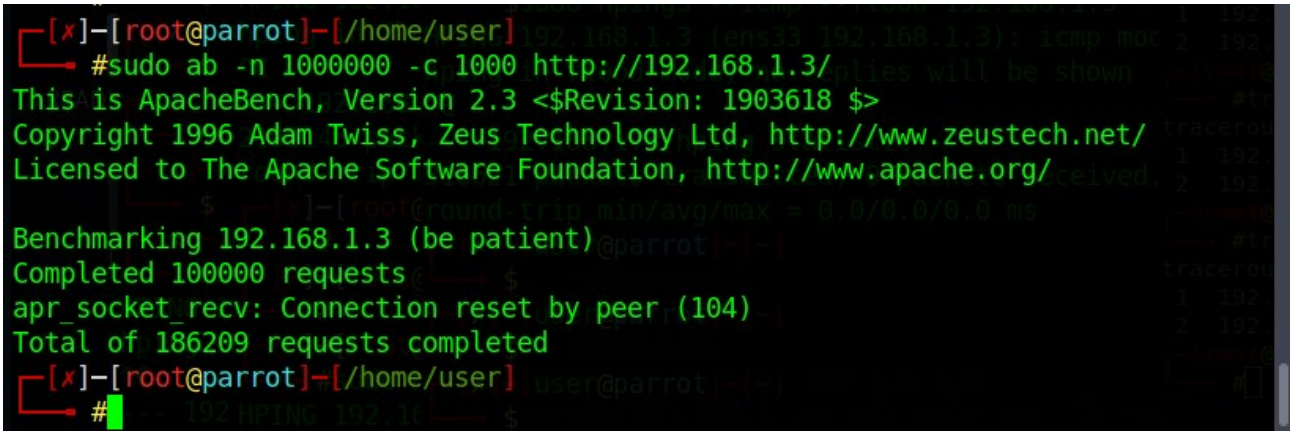


Рисунок 3.4 – HTTP Flood атака на хост Ubuntu Linux з операційної системи Parrot Security Atacker 1

Ця команда ініціює великий потік запитів до сервера, що дозволяє оцінити, наскільки ефективно він може справлятися з подібним навантаженням.

Параметри `-n` задає загальну кількість запитів, які будуть надіслані до сервера, `-c` встановлює кількість одночасних запитів, що надсилаються паралельно.

Під час моделювання DDoS-атак важливо забезпечувати ізоляцію тестового середовища від реальних мереж, щоб уникнути ненавмисного поширення шкідливого трафіку. Тестове середовище повинно бути налаштоване так, щоб захисні механізми (брандмауери та IPS) могли відслідковувати і реагувати на шкідливу активність, забезпечуючи надійний аналіз захисних заходів.

3.1.2 Brute-force атака

Атаки типу Brute-Force є одним із класичних способів отримання несанкціонованого доступу до систем або облікових записів. У таких атаках зловмисники намагаються підібрати правильну комбінацію логіна та пароля, перебираючи всі можливі варіанти. Ці атаки часто застосовуються проти служб із слабким захистом, таких як SSH, FTP, HTTP, RDP та інші. Brute-Force атаки можуть бути надзвичайно ресурсомісткими і з часом блокуються сучасними системами захисту, але вони все ще є актуальною загрозою, особливо для систем, що не мають належного рівня захисту.

Hydra — це популярний інструмент для проведення атак типу Brute-Force, який підтримує широкий спектр протоколів, включаючи SSH, FTP, HTTP, MySQL, SMTP, Telnet, і багато інших. Використовуючи hydra, можна моделювати атаки Brute-force на тестових серверах, щоб перевірити їхню стійкість до підбору паролів, а також оцінити ефективність механізмів захисту, таких як блокування облікових записів після кількох невдалих спроб, обмеження швидкості запитів та двофакторна автентифікація.

На рисунку 3.5 показано використання інструменту hydra для brute-force атаки на SSH-сервер.

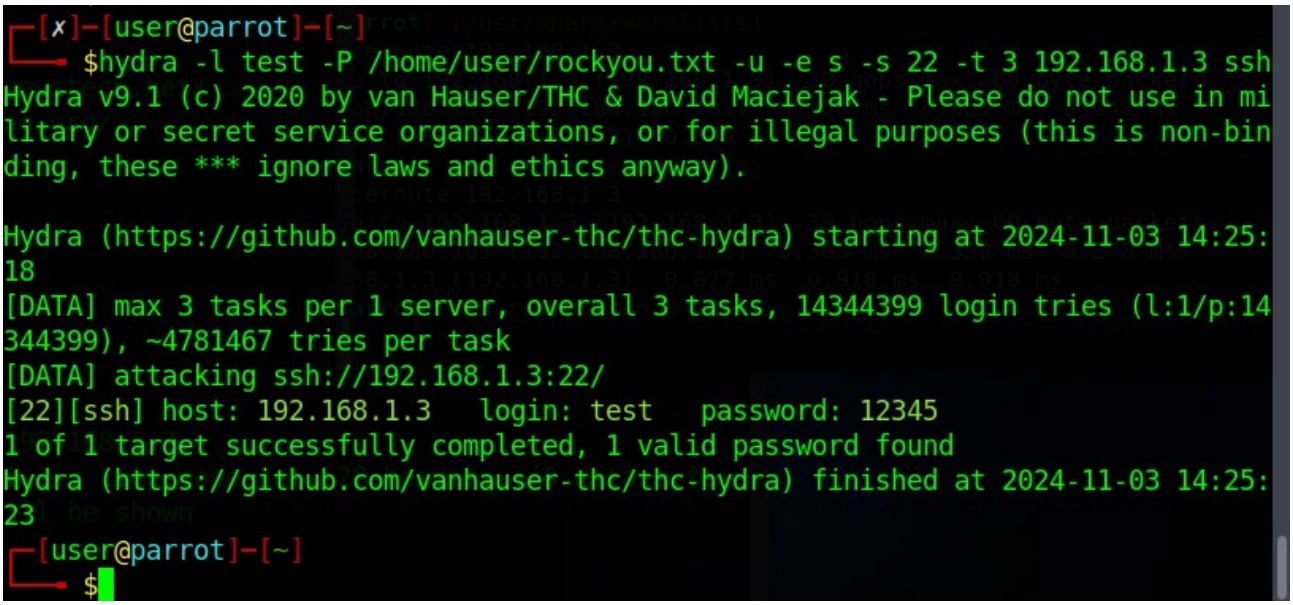


Рисунок 3.5 – Brute-force атака на хост Ubuntu Linux з операційної системи Parrot Security Atacker 1

Результат показує, що пароль 12345 користувача test було підібрано. Це свідчить про успішне завершення атаки.

3.1.3 Результат багатовекторної атаки

Багатовекторна атака, яка об’єднує кілька типів атак, спрямованих на різні вразливості та ресурси, має на меті досягти максимально максимального деструктивного ефекту. Скомбіноване використання SYN Flood, UDP Flood, ICMP Flood, HTTP Flood та Brute-force атак може викликати серйозні наслідки

для цільової інфраструктури, особливо якщо захисні механізми недостатньо налаштовані для комплексного захисту. SYN Flood генерує велику кількість запитів на встановлення з'єднання (SYN-запитів) без завершення процесу рукостискання TCP. У результаті сервер резервує ресурси для кожного запиту, що може швидко виснажити доступні ресурси. Сервер починає втрачати здатність встановлювати нові з'єднання, що призводить до зниження доступності для легітимних користувачів і значного зниження продуктивності, що може призвести до повної недоступності. UDP Flood надсилає великий обсяг UDP-пакетів до випадкових або конкретних портів на сервері. Оскільки UDP є протоколом без єднання, сервер змушений обробляти кожен пакет, що створює значне навантаження на мережу і процесор. Це призводить до перевантаження мережі, зниження пропускної здатності та створення черг у маршрутизаторах і комутаторах, а також до зниження якості сервісу для інших користувачів мережі через високий рівень затримок і втрат пакетів. ICMP Flood, або Ping Flood, створює великий потік ICMP-запитів (типу Echo Request) до цільового сервера. Цей тип атаки спрямований на вичерпання пропускної здатності мережі та ресурсів процесора сервера, необхідних для обробки запитів. Це призводить до затримки обробки або повної втрати доступності, а також до виснаження пропускної здатності та значних затримок, які можуть вплинути не тільки на цільовий сервер, але й на інші служби, що працюють у тій самій мережі. HTTP Flood генерує великий обсяг HTTP-запитів до веб-сервера. Ці запити можуть імітувати звичайні користувацькі запити, наприклад, до веб-сторінок, але надходять у надмірній кількості. Оскільки веб-сервер обробляє кожен запит, це може швидко виснажити ресурси сервера, викликаючи недоступність веб-сервісів для легітимних користувачів і значне навантаження на процесор і пам'ять сервера, яке може призвести до аварійних зупинок або зниження продуктивності інших сервісів. Brute-force атака є додатковим елементом багатовекторної атаки, спрямованим на підбір паролів для доступу до облікових записів. Це підвищує ризик несанкціонованого доступу до облікових записів у разі успішного підбору пароля і призводить до блокування легітимних облікових записів через активацію механізмів захисту, таких як блокування після кількох

невдалих спроб входу. Також це створює додаткове навантаження на систему автентифікації, що може уповільнити процес обробки запитів для інших користувачів. Поєднання SYN Flood, UDP Flood, ICMP Flood, HTTP Flood та Brute-force атак створює комплексний багатовекторний тиск на сервер і мережу, що значно ускладнює процес виявлення та нейтралізації. Цільова система зазнає навантаження на декількох рівнях одночасно: мережевому, транспортному та рівні застосунків. Основні наслідки такої багатовекторної атаки включають зниження або повну втрату доступності сервісів для легітимних користувачів, що призводить до фінансових втрат, втрати репутації та довіри користувачів, виснаження пропускної здатності мережі, що впливає не тільки на цільовий сервер, але й на інші сервіси та користувачів у тій самій інфраструктурі. Це також призводить до перевантаження процесора та пам'яті сервера, що може викликати аварійне завершення роботи або серйозне уповільнення обробки запитів, а також до збоїв у роботі системи автентифікації та захисних механізмів, що може спричинити блокування облікових записів, зниження продуктивності та порушення доступу.

На рисунку 3.6 можна побачити мережеву статистику зібрану за допомогою iptraf-ng в Ubuntu Linux.

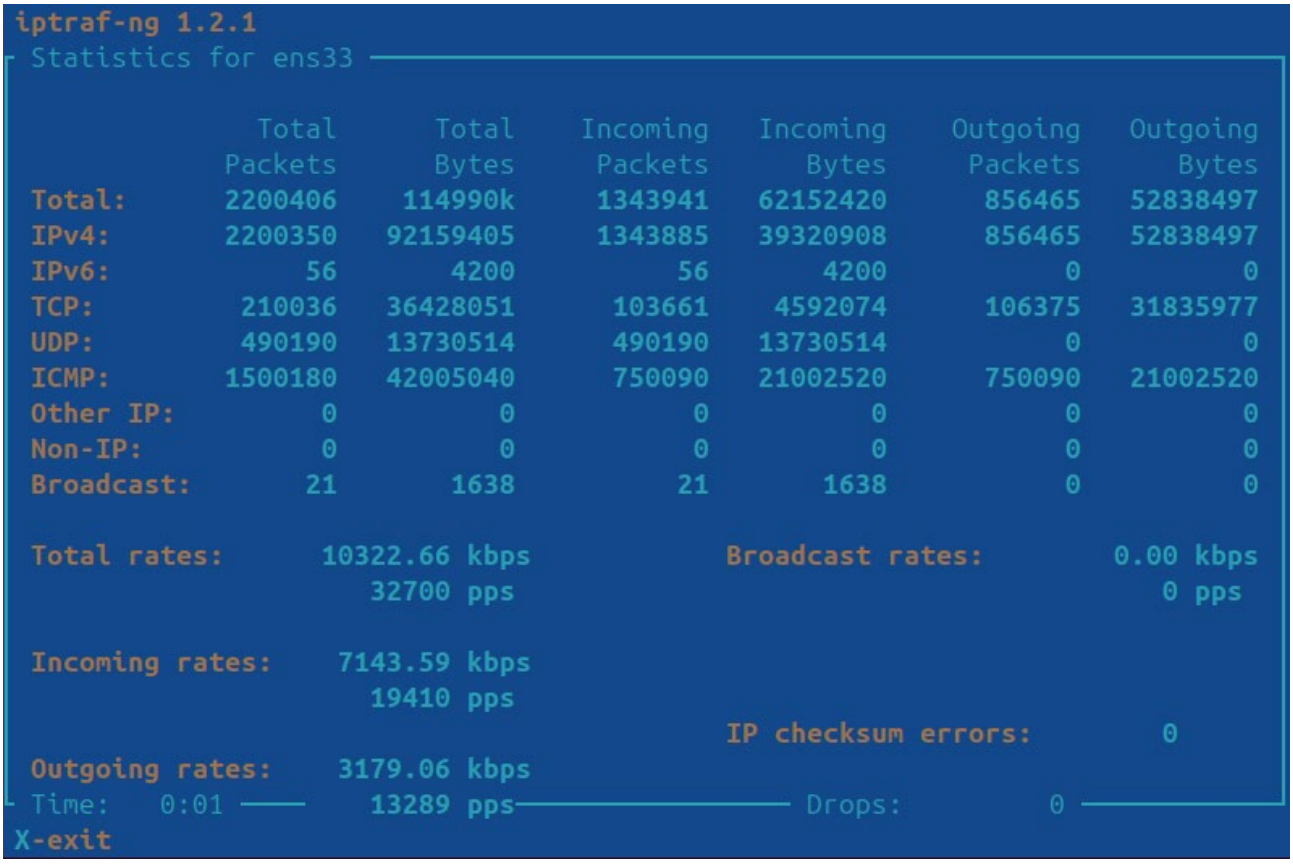


Рисунок 3.6 – Мережева статистика під час багатовекторної атаки на хост Ubuntu Linux

Мережевий інтерфейс ens33 обробляє значний обсяг вхідного трафіку з високою швидкістю — 19,410 пакетів за секунду (pps). Це значення є досить високим і є ознакою багатовекторної атаки.

Багатовекторна атака такого масштабу вимагає комплексних захисних заходів, включаючи брандмауери, системи виявлення та запобігання вторгненням, блокування IP-адрес з великою кількістю запитів.

3.2 Маршрутизатор pfSense та система IPS

Маршрутизатор pfSense є потужним програмним рішенням з відкритим вихідним кодом, розробленим на основі операційної системи FreeBSD, що виконує функції брандмауера, маршрутизатора та системи IPS. Маршрутизатор pfSense підтримує додаткові пакети, серед яких одним із найважливіших є Snort — популярна система виявлення та запобігання вторгненням [28]. Snort розроблена як система для аналізу мережевого трафіку та виявлення підозрілих

активностей, дозволяє ідентифікувати різні типи загроз, такі як DDoS-атаки та спроби експлуатації вразливостей. Snort працює на основі сигнатурного аналізу, який порівнює вхідний трафік із відомими шаблонами загроз, а також підтримує поведінковий аналіз для виявлення аномалій.

Комбінація pfSense та Snort забезпечує багаторівневий захист мережі. pfSense здійснює фільтрацію на рівні брандмауера, контролюючи доступ до мережі за IP-адресами, портами та протоколами, а Snort додає додатковий рівень захисту, моніторячи трафік у реальному часі та блокуючи підозрілі активності. У випадку виявлення аномалій або шкідливих з'єднань Snort здатний автоматично блокувати ці загрози до їхнього потрапляння в локальну мережу. Це забезпечує активний захист мережевих ресурсів, що дозволяє не тільки фільтрувати вхідний трафік, але й запобігати вторгненням, зберігаючи доступність та безпеку внутрішніх ресурсів.

Інтеграція Snort у pfSense також дозволяє налаштовувати детальні правила IPS для певних типів трафіку, що надає адміністраторам контроль над тим, які з’єднання можуть вважатися потенційно шкідливими. Snort може використовувати спеціалізовані бази даних сигнатур, оновлювані спільнотою або постачальником, що дозволяє миттєво реагувати на нові загрози. pfSense надає зручний веб-інтерфейс для керування налаштуваннями Snort, що дозволяє гнучко налаштовувати IPS, а також переглядати журнали подій та аналітику трафіку для оперативного реагування на кіберзагрози (див. рисунок 3.7).

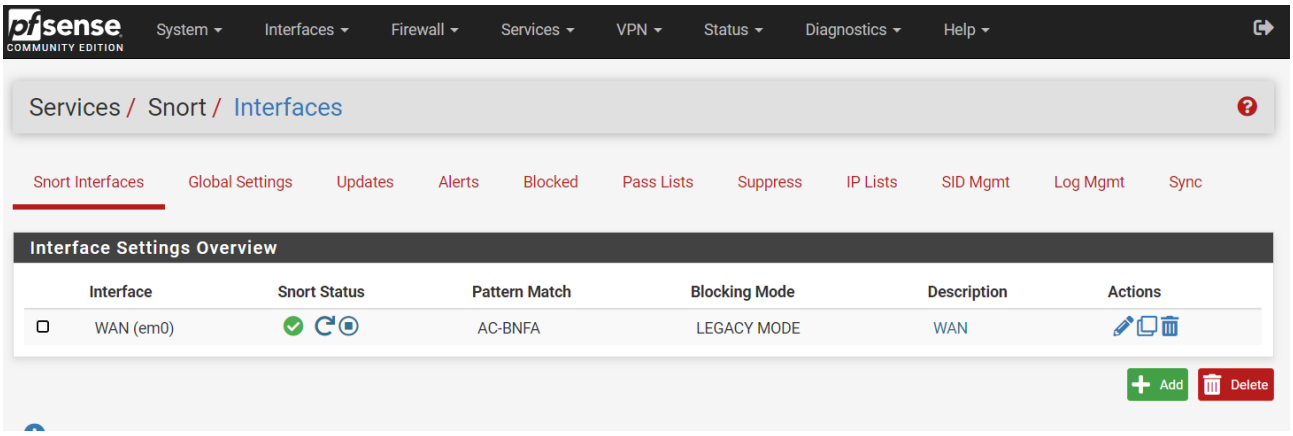


Рисунок 3.7 – Інтерфейс налаштування Snort в pfSense

Завдяки такій комбінації pfSense та Snort забезпечують надійну та ефективну платформу для захисту від вторгнень, яка є особливо корисною в умовах зростаючого обсягу мережевого трафіку та поширення складних загроз.

Snort був розроблений компанією Sourcefire (нині частина Cisco). Snort виконує функції аналізатора мережевого трафіку і здатен виявляти, класифікувати та запобігати широкому спектру кіберзагроз. Однією з основних особливостей Snort є його сигнатурний аналіз, який працює на основі бази правил, що визначають шаблони атак та підозрілих активностей. Сигнатури включають опис загрози або її поведінки в мережі, зокрема структуру пакетів, типи протоколів, порти та інші специфічні параметри. Коли Snort порівнює вхідний трафік з цими правилами, він виявляє відповідності між трафіком та відомими шаблонами атак і може генерувати сповіщення про загрозу або автоматично блокувати шкідливі з'єднання. Цей підхід дозволяє ефективно ідентифікувати відомі загрози, такі як DDoS-атаки, спроби експлуатації вразливостей, шкідливе програмне забезпечення та сканування портів.

Snort також підтримує поведінковий аналіз, що дозволяє виявляти аномалії в мережевій активності, не прив’язані до конкретної сигнатури. Це особливо корисно для виявлення нових загроз, які не мають відомих шаблонів, але їхня поведінка відрізняється від нормальної мережевої активності. Наприклад, незвично високий обсяг трафіку на певному порту або раптове збільшення ICMP-запитів можуть бути ознаками атаки. Таким чином, поведінковий аналіз доповнює сигнатурний і дозволяє Snort виявляти широкий спектр загроз.

У pfSense система Snort може працювати в різних режимах, кожен з яких має своє призначення та особливості. У pfSense ці режими дозволяють ефективно використовувати Snort для моніторингу та захисту мережевого трафіку.

Перший режим, режим виявлення вторгнень (IDS Mode), є основним і найпоширенішим. У цьому режимі Snort аналізує трафік у реальному часі, порівнюючи його з набором правил і сигнатур для виявлення підозрілої активності. Коли Snort виявляє збіг із відомими шаблонами атак або аномальною поведінкою, він генерує попередження (alert), яке може бути записане в журнал або відправлене адміністратору. Проте в цьому режимі Snort не блокує трафік

автоматично. Його основна функція полягає у спостереженні та інформуванні про можливі загрози. Цей режим є ідеальним для тестування та налаштування системи, оскільки дозволяє адміністраторам вивчити характер трафіку і визначити, які правила потрібно налаштувати або відкоригувати перед переходом до активних заходів блокування.

Другий режим, режим запобігання вторгненням (IPS Mode), додає функціонал активного блокування до системи Snort. У цьому режимі Snort не тільки аналізує трафік, але й здатен автоматично блокувати шкідливі пакети до того, як вони потраплять у внутрішню мережу. Це відбувається за рахунок встановлення Snort на мережевий інтерфейс pfSense у режимі «inline», що дозволяє йому перехоплювати трафік у режимі реального часу. При виявленні підозрілої активності або атаки, Snort може миттєво відкинути шкідливі пакети, забезпечуючи активний захист мережі. Цей режим вимагає ретельного налаштування, оскільки неправильні правила можуть призвести до блокування легітимного трафіку, що є небажаним у продуктивних середовищах.

Snort підтримує гнучкі правила для налаштування IDS/IPS, що дозволяє адаптувати його до специфічних вимог мережі та додавати власні сигнатури. Правила можуть бути налаштовані для моніторингу трафіку на певних портах, протоколах або IP-адресах, а також для виявлення специфічних шаблонів, наприклад, за ключовими словами в заголовках HTTP або FTP. Кожне правило в Snort визначає умову, при виконанні якої активується відповідна дія, наприклад, генерація попередження або блокування трафіку. Snort також забезпечує гнучку систему звітності, яка дозволяє генерувати різні види сповіщень про загрози, зокрема запис до журналу, надсилання повідомлення електронною поштою або відправлення сповіщення до зовнішньої системи моніторингу. Це забезпечує швидке реагування на інциденти безпеки, а також дозволяє інтегрувати Snort у комплексну систему керування подіями безпеки (SIEM), що надає адміністраторам повну картину мережевої активності та загроз у реальному часі.

3.3 Розробка оптимізованих правил IPS

Розробка оптимізованих правил для IPS Snort на платформі pfSense є критично важливим кроком для забезпечення ефективного та продуктивного захисту мережі. Правильне налаштування та оптимізація правил дозволяють знизити кількість хибних спрацьовувань, зменшити навантаження на систему та підвищити точність виявлення реальних загроз.

Перш ніж приступати до розробки правил, важливо глибоко розуміти архітектуру мережі, типи трафіку, використовувані протоколи та сервіси, а також потенційні загрози, характерні для конкретного середовища. Це дозволить налаштувати правила таким чином, щоб вони відповідали реальним потребам та мінімізували кількість непотрібних спрацьовувань.

Snort використовує базу правил, яка складається з тисяч сигнатур для виявлення відомих загроз. Рекомендується використовувати актуальні бази правил, такі як Snort Community Rules (безкоштовний набір правил, підтримуваний спільнотою), Emerging Threats (ET) Rules (набір правил з відкритим вихідним кодом, що оновлюється регулярно) та VRT Rules (Snort Subscriber Ruleset) (платний набір правил від Cisco Talos, що містить найновіші сигнатури). Важливо регулярно оновлювати базу правил, щоб бути захищеним від нових загроз. Не всі правила є релевантними для кожного середовища. Активування всіх доступних правил може призвести до надмірного навантаження на систему та великої кількості хибних спрацьовувань. Рекомендується вимкнути нерелевантні правила, які не стосуються використовуваних сервісів або протоколів у мережі, та фокусуватися на критичних загрозах, приділяючи особливу увагу правилам, що стосуються відомих вразливостей у використовуваних системах та додатках.

Кожне правило має свій рівень пріоритету та дію, наприклад, оповіщення або блокування. Для оптимізації варто встановити відповідні пріоритети, призначаючи високий пріоритет для критичних загроз та низький для менш важливих, а також визначити дії для кожного правила, наприклад, блокування для серйозних загроз та оповіщення для менш критичних.

Після початкового налаштування потрібно провести тестування та моніторинг. Оптимізація правил включає використання змінних для IP-адрес та

портів, що дозволяє робити правила більш гнучкими та легше керованими; злиття подібних правил для зменшення їхньої кількості та спрощення обробки; оптимізацію регулярних виразів у правилах для зменшення навантаження на процесор.

Стандартні правила є недостатніми. Доцільним є створення власних правила, які відповідають специфічним вимогам мережі або виявленим загрозам. Врахування продуктивності також є важливим аспектом. Налаштуйте обмеження на розмір пакетів або сесій, які аналізуються, щоб зменшити навантаження; використовуйте багатопоточність, якщо апаратне забезпечення дозволяє, налаштувавши Snort на використання кількох ядер процесора; виключіть певний трафік, який не потребує аналізу, наприклад, внутрішній трафік між довіреними серверами.

На рисунку 3.8 показано правило для IDS Snort, яке використовується для виявлення атак SYN Flood. Це правило призначене для виявлення спроби DDoS-атаки шляхом перенавантаження цільового сервера великою кількістю SYN-пакетів.

```
alert tcp $EXTERNAL_NET any -> $SERVER any (msg:"SYN Flood Attack Detected";
    flags:S; dsize:0; flow:stateless; ttl:<64;
    detection_filter:track by_dst, count 100, seconds 1; priority:1;
    reference:url,https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/;
    classtype:attempted-dos; sid:1000001; rev:2;)
```

Рисунок 3.8 – Правило для IPS Snort для виявлення SYN Flood атаки

де:

- `alert` вказує, що при виконанні умов правила має бути створено сповіщення;
- `tcp` вказує, що правило застосовується до TCP-трафіку;
- `$EXTERNAL_NET` змінна, що представляє зовнішню мережу;
- `any` вказує, що правило застосовується до будь-якого порту;
- `$SERVER` змінна, що представляє цільовий сервер;
- `msg` визначає повідомлення, яке буде створене при спрацьовуванні правила. В даному випадку це "SYN Flood Attack Detected;

- `flags` вказує, що правило спрацьовує на пакети з встановленим прапором SYN. Це характерно для SYN Flood атаки, де зловмисник надсилає багато SYN-запитів для встановлення з'єднань, не завершуючи їх;
- `dsize` визначає розмір корисного навантаження (payload) в байтах. У цьому випадку розмір має бути 0, що відповідає типовим SYN-запитам, які зазвичай не містять даних;
- `flow:stateless` вказує, що правило не враховує стан з'єднання. Це важливо, оскільки SYN Flood атаки не мають встановленого стану (вони спрямовані на відправку великої кількості початкових запитів);
- `detection_filter` встановлює фільтр для виявлення аномальної активності за частотою трафіку;
- `priority` пріоритет правила встановлено на 1, що означає високий рівень важливості;
- `reference` це посилання на додаткову інформацію про атаку SYN Flood. У даному випадку, це стаття на сайті Cloudflare, що пояснює, як працює SYN Flood атака.
- `classtype` це класифікація типу атаки. В даному випадку це "attempted-dos", що означає спробу атаки типу відмова в обслуговуванні (DoS);
- `sid` це унікальний ідентифікатор правила (Snort ID). В даному випадку це 1000001;
- `rev` це номер ревізії правила.

Це правило Snort використовується для виявлення спроб SYN Flood атаки на сервер, коли відбувається надмірна кількість SYN-запитів за короткий час. Якщо система IDS виявить більше ніж 100 SYN-пакетів за секунду на один і той самий сервер, буде створено сповіщення "SYN Flood Attack Detected" та IP-адреса атакуючого буде заблокована.

На рисунку 3.9 показано правило, яке використовується для виявлення ICMP Flood атаки.

```
alert icmp $EXTERNAL_NET any -> $SERVER any (msg:"ICMP Flood Detected";
    itype:8; dsize:0<>1024; ttl:<64; flow:stateless; detection_filter:track by_dst,
    count 50, seconds 1; priority:1;
    reference:url,https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/;
    classtype:attempted-dos; sid:1000002; rev:2;)
```

Рисунок 3.9 – Правило для IPS Snort для виявлення ICMP Flood атаки

Якщо система IPS виявить атаку буде створено сповіщення "ICMP Flood Detected" та IP-адреса атакуючого буде заблокована.

На рисунку 3.10 показано правило, яке використовується для виявлення UDP Flood атаки.

```
alert udp $EXTERNAL_NET any -> $SERVER any (msg:"UDP Flood Attack Detected";
    dsize:>1000; ttl:<64; flow:stateless; detection_filter:track by_dst,
    count 50, seconds 1; priority:1;
    reference:url,https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/;
    classtype:attempted-dos; sid:1000003; rev:2;)
```

Рисунок 3.10 – Правило для IPS Snort для виявлення UDP Flood атаки

Якщо система IPS виявить атаку буде створено сповіщення "UDP Flood Attack Detected" та IP-адреса атакуючого буде заблокована.

На рисунку 3.11 показано правило, яке використовується для виявлення UDP Flood атаки.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"HTTP Flood Attack Detected";
    flow:to_server,established; content:"GET"; http_method; content:"/"; http_uri; nocase;
    dsize:0<>500; detection_filter:track by_dst, count 100, seconds 1; priority:1;
    reference:url,https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/;
    classtype:attempted-dos; sid:1000004; rev:2;)
```

Рисунок 3.11 – Правило для IPS Snort для виявлення HTTP Flood атаки

де:

- `$HTTP_SERVERS` змінна, що представляє IP-адресу HTTP-сервера.
- `content:"GET"; http_method` шукає вміст "GET" у запиті, що відповідає HTTP GET-запиту. Більшість HTTP Flood атак використовують GET-запити для завантаження ресурсу сервера;

- `content:"/"; http_uri; nocase` шукає символ "/" у запиті URI, що вказує на запит кореневого ресурсу, nocase означає, що пошук нечутливий до регістру;
- `dsize:0<>500` вказує на розмір корисного навантаження (payload) пакета. У цьому випадку розмір повинен бути від 0 до 500 байтів, що охоплює типові невеликі GET-запити, які часто використовуються в атаках HTTP Flood.

Якщо система IDS виявить атаку буде створено сповіщення "HTTP Flood Attack Detected" та IP-адреса атакуючого буде заблокована.

На рисунку 3.12 показано правило, яке використовується для виявлення спроби підбору пароля до SSH-сервера з метою несанкціонованого доступу до нього.

```
alert tcp $EXTERNAL_NET any -> $SERVER 22 (msg:"SSH Brute-Force Attack Detected";
    flow:to_server,established; flags:S; content:"SSH-"; depth:4;
    detection_filter:track by_src, count 5, seconds 30; priority:1;
    reference:url,https://www.cloudflare.com/learning/bots/brute-force-attack/;
    classtype:attempted-recon; sid:1000005; rev:2;)
```

Рисунок 3.12 – Правило для IPS Snort для виявлення SSH Brute-force атаки

Якщо система IPS виявить атаку буде створено сповіщення " SSH Brute-Force Attack Detected" та IP-адреса атакуючого буде заблокована.

3.4 Тестування розроблених правил IPS

Тестування розроблених правил IPS Snort є важливим етапом для перевірки їхньої ефективності та впевненості в тому, що вони правильно виявляють та блокують відповідні загрози без створення хибних спрацьовувань. Для цього необхідно провести кілька кроків, які включають моделювання атак, спостереження за поведінкою системи та аналіз журналів подій.

Моделювання атак здійснюється за допомогою утиліт hping3, ab та hydra, що дозволяє імітувати реальні сценарії загроз та оцінити реакцію системи безпеки аналогічно, як в пункті 3.1.

Для початку, необхідно переконатися, що лабораторне середовище налаштоване відповідно до вимог. Маршрутизатор pfSense з встановленим та налаштованим Snort має бути розгорнутий між зовнішньою мережею та внутрішньою мережею, де розташований цільовий сервер Ubuntu Linux з активними сервісами SSH, HTTP, DNS та іншими. Атакуючі машини на базі Parrot Security OS використовуються для ініціації атак з метою перевірки спрацьовування правил Snort.

На рисунку 3.13 показано сторінку Alerts інтерфейсу Snort у системі pfSense, яка містить журнал сповіщень про атаки.

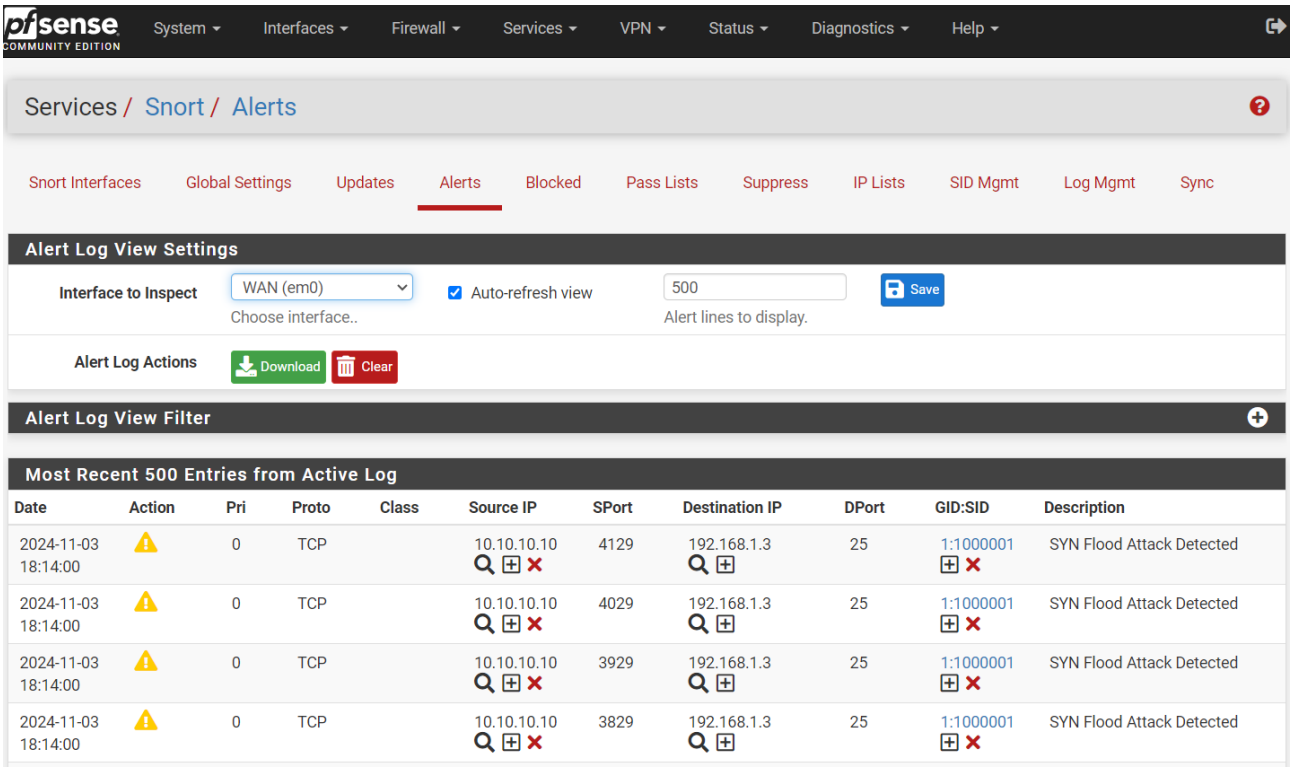


Рисунок 3.13 – Повідомлення про виявлення SYN Flood атаки

Зокрема, у цьому журналі зафіксовано виявлення атак типу SYN Flood на порт 25 (SMTP) сервера з IP-адресою 192.168.1.3 з IP-адреси 10.10.10.10.

На рисунку 3.14 показано сторінку Alerts інтерфейсу Snort у системі pfSense, яка містить журнал сповіщень про UDP Flood атаку.

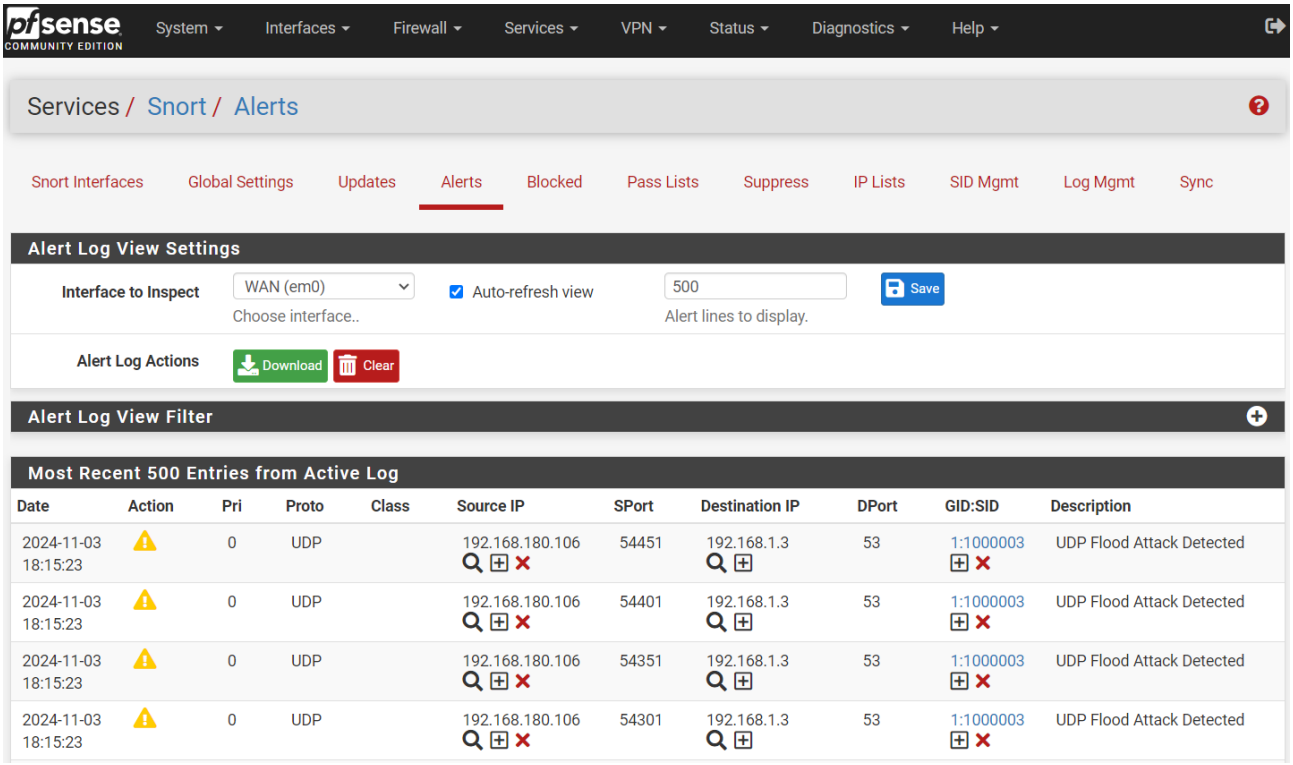


Рисунок 3.14 – Повідомлення про виявлення UDP Flood атаки

У цьому випадку журнал показує зафіксовані сповіщення про UDP Flood атаку на сервер з IP-адресою 192.168.1.3 на порт 53 (DNS) з IP-адреси 192.168.180.106.

На рисунку 3.15 показано сторінку Alerts інтерфейсу Snort у системі pfSense, яка містить журнал сповіщень про ICMP Flood атаку.

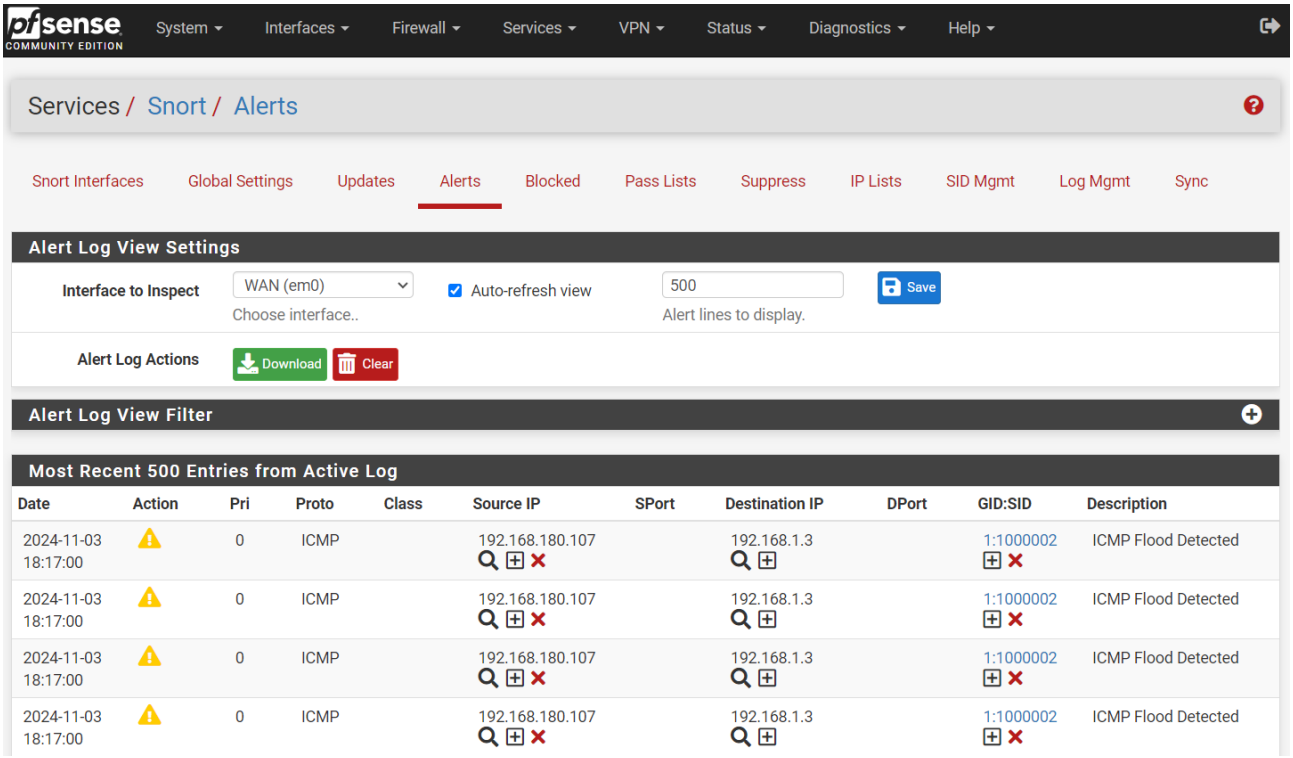


Рисунок 3.15 – Повідомлення про виявлення ICMP Flood атаки

Ця послідовність сповіщень вказує на спробу ICMP Flood атаки з адреси 192.168.180.107 на IP-адресу сервера 192.168.1.3.

На рисунку 3.16 показано сторінку Alerts інтерфейсу Snort у системі pfSense, яка містить журнал сповіщень про HTTP Flood атаку.

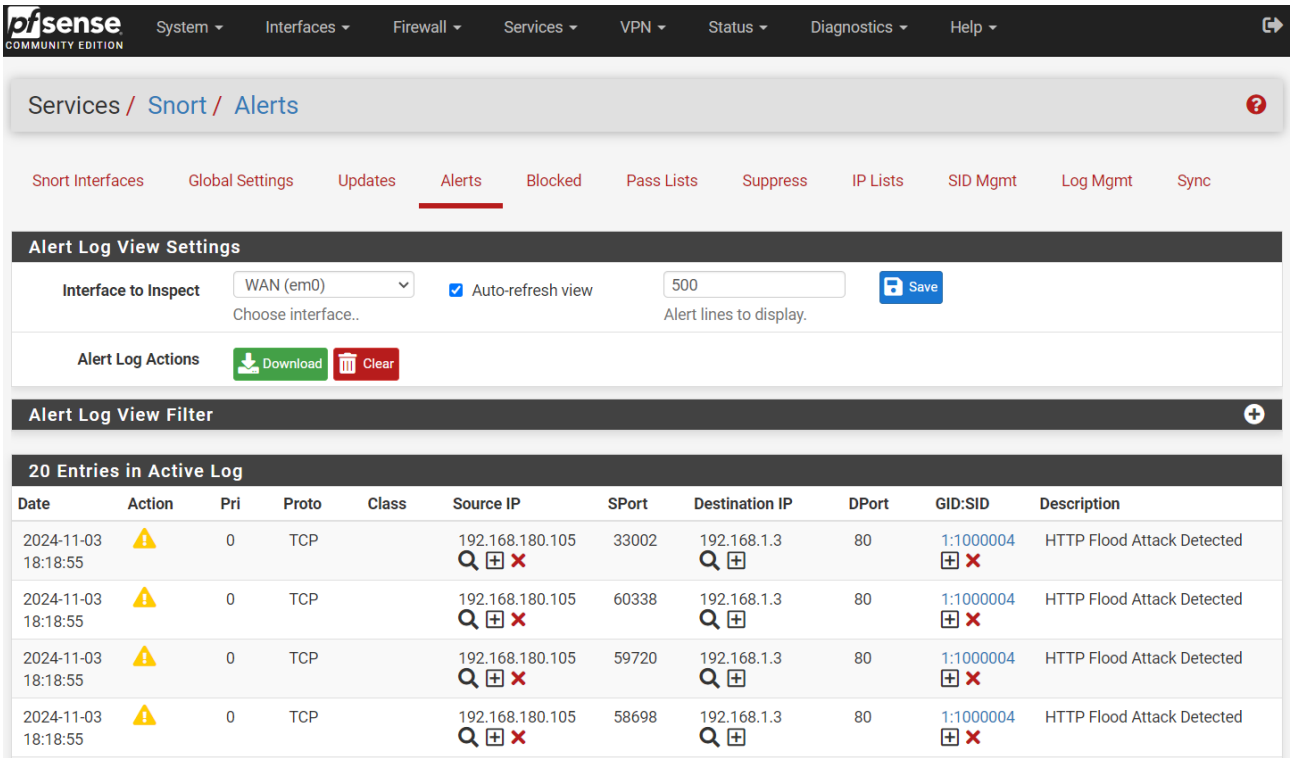


Рисунок 3.16 – Повідомлення про виявлення HTTP Flood атаки

Ця серія сповіщень вказує на активну HTTP Flood атаку з IP-адреси 192.168.180.105 на вебсервер із адресою 192.168.1.3. Велика кількість одночасних HTTP-запитів на порт 80 спрямована на перевантаження сервера, що може призвести до відмови в обслуговуванні для легітимних користувачів.

На рисунку 3.17 показано сторінку Alerts інтерфейсу Snort у системі pfSense, яка містить журнал сповіщень про SSH Brute-force атаку.

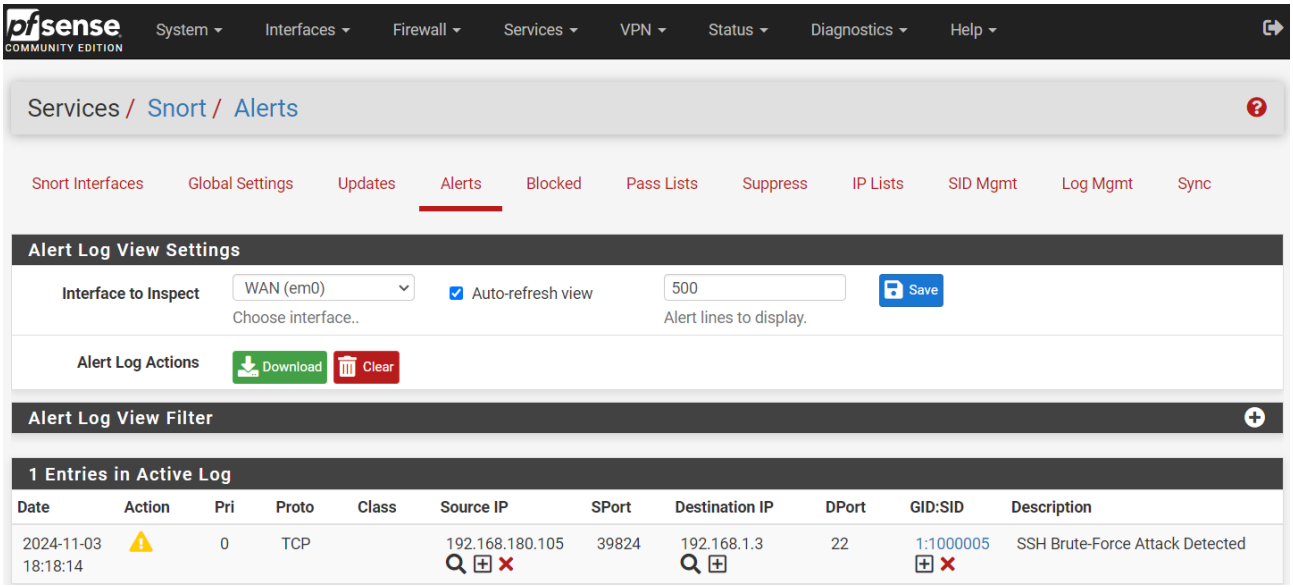


Рисунок 3.17 – Повідомлення про виявлення SSH Brute-force атаки

Ця подія вказує на спробу SSH Brute-force атаки з IP-адреси 192.168.180.105 на сервер з IP-адресою 192.168.1.3 порт 22. Така атака спрямована на підбір облікових даних з метою отримання несанкціонованого доступу.

На рисунку 3.18 показано сторінку Blocked Hosts інтерфейсу Snort у системі pfSense, де відображено заблоковані IP-адреси, які були визначені як джерела атак. Система автоматично заблокувала ці IP-адреси для запобігання подальших загроз.

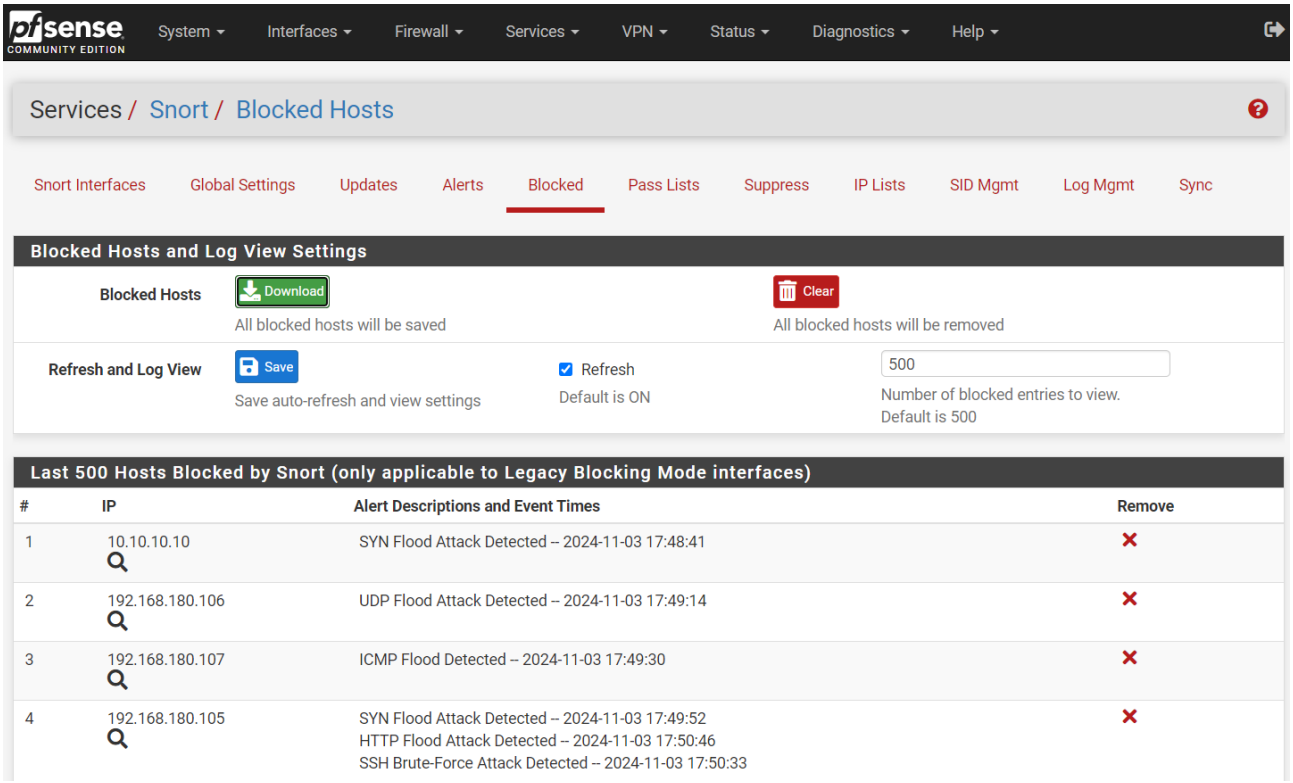


Рисунок 3.18 – Зблоковані IP-адреси системою IPS

Цей журнал демонструє, що система Snort у pfSense ефективно виявляє та блокує підозрілу активність з різних IP-адрес. Усі заблоковані адреси були визначені як джерела атак типу Flood (SYN, UDP, ICMP, HTTP) або Brute-force, що свідчить про спроби перевантаження сервера або підбору облікових даних.

3.5 Висновки до розділу 3

В третьому розділі було проведено комплексне дослідження впровадження системи виявлення та запобігання вторгненням (IPS) з використанням маршрутизатора pfSense та системи Snort. Було змодельовано різні типи кіберзагроз у лабораторному середовищі, включаючи DDoS-атаки типів SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, а також атаку типу Brute-force. Для цього використовувалися інструменти hping3, ab та hydra, що дозволило імітувати реальні сценарії атак та оцінити їхній вплив на цільову інфраструктуру.

Також було детально розглянуто можливості маршрутизатора pfSense та інтегрованої в нього системи Snort. Описано режими роботи Snort у pfSense, зокрема режим виявлення вторгнень (IDS) та режим запобігання вторгненням

(IPS). Особлива увага приділялася розробці оптимізованих правил для Snort, які були спрямовані на ефективне виявлення конкретних типів атак з мінімізацією хибних спрацьовувань та навантаження на систему.

Розроблені правила IPS були протестовані в лабораторному середовищі шляхом моделювання атак за допомогою зазначених інструментів. Тестування підтвердило ефективність правил та здатність системи Snort виявляти та блокувати різні типи загроз, включаючи багатовекторні атаки. Також було проаналізовано журнали подій та сповіщень, що підтвердило правильність налаштувань та ефективність захисту.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою даної кваліфікаційної роботи є розробка та впровадження оптимізованих правил для системи IPS на базі pfSense з метою ефективного виявлення багатовекторних DDoS-атак. При створенні подібних засобів потрібно дотримуватись основні правила і норми експлуатації комп’ютерів та периферійних пристроїв під час проведення дослідження.

В загальному, поняття охорона праці в комп’ютерних системах являє собою дотримання всіх вимог і нормативів, що присутні в законодавчих актах про охорону праці. Закони цієї області спрямовані на якісну і безпечну експлуатацію робочих приладів і приміщень, дотримання санітарно-гігієнічних умов праці і захист від інших небезпечних чинників на підприємстві. Ці засоби є складовими дослідження математичного і програмного забезпечення автоматизованої системи підбору команди розробників комп’ютерних систем. В основних законодавчих актах про охорону праці приділяється велика увага поліпшенню умов праці в усіх галузях господарства, впровадженню сучасних засобів техніки безпеки і забезпечення санітарно-гігієнічних умов, що запобігають виробничому травматизму і професійним захворюванням.

Охорона життя і здоров’я людини є пріоритетним напрямком соціальної політики держави. В Україні прийнято закон прямої дії «Про охорону праці», який регламентує захист конституційного права працівників на безпечні умови праці. Законодавство України про охорону праці складається із загальних законів України та спеціальних законодавчих актів. Загальними законами України, що визначають основні положення з охорони праці є Конституція України, Закон України «Про охорону праці», Кодекс законів про працю (КЗпП), Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності».

Виконання досліджень кваліфікаційної роботи передбачали використання ПК, де площа та об'єм для одного робочого місця оператора визначається згідно вимог НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями», зокрема площа повинна становити не менше 6,0 квадратних метрів, об'єм - не менше 20,0 кубічних метрів.

Згідно вимог охорони праці та державних санітарних правил, стіни, стеля та підлога приміщень, в яких розміщені ЕОМ, повинні бути виготовлені з матеріалів, дозволених для оформлення приміщень органами державного санітарно-епідеміологічного нагляду.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), повинні бути надійно захищені діелектричними щитками та сітками з метою недопущення потрапляння працівника під напругу.

Організація робочого місця оператора повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам. У приміщенні, де одночасно експлуатуються понад п'ять електронно-обчислювальних машин (ЕОМ), на помітному та доступному місці мають бути встановленні аварійні резервні вимикачі, які можуть повністю вимкнути електричне живлення приміщення, крім освітлення [29].

Дотримання правил значно знижує наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відео-дисплейними терміналами, зокрема можливість зорових, нервово-емоційних переживань, серцево-судинних захворювань. Виходячи з цього, роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації електронно-обчислювальних машин (ЕОМ) з ВДТ, робочого середовища, робочих місць з ЕОМ, режиму праці і відпочинку при роботі з ЕОМ тощо, які викладені у нормах НПАОП 0.00-7.15-18. Відповідно до встановлених гігієнічно-санітарних вимог роботодавець зобов'язаний забезпечити в приміщеннях з ЕОМ оптимальні параметри виробничого середовища [29].

Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски з поверхні екранів персонального комп’ютера і клавіатури повинні бути передбачені сонцезахисні пристрої, вікна повинні мати жалюзі або штори.

Основні задачі охорони праці при використанні комп'ютерної техніки:

- аналіз впливу факторів виробничого середовища на здоров'я і працездатність користувачів персональних комп’ютерів;

- вдосконалювання методів оцінки працездатності і стану здоров'я користувачів ПК;

- розробка і впровадження організаційно-технічних, гігієнічних і соціально-економічних заходів щодо раціоналізації виробничого середовища;

- розробка і впровадження профілактичних і оздоровчих заходів, що дозволяють зберігати здоров'я людини і підвищувати її працездатність;

- вдосконалення методик навчання користувачів ПК питанням охорони праці.

Вимогам нормативних актів з охорони праці мають відповідати:

- умови праці на кожному робочому місці;

- безпека технологічних процесів, машин, механізмів, обладнання й інших засобів виробництва;

- стан засобів колективного та індивідуального захисту;

- санітарно-побутові умови.

При дослідженні методів і засобів створення програмних систем та проектуванні системи захисту від атак на сервери важливо було проаналізовати та враховати необхідні вимоги щодо охорони праці при використанні електронно-обчислювальної техніки і забезпечити умови для зручної та ефективної роботи працівників.

4.2 Підвищення стійкості роботи комп’ютеризованих систем в умовах дії ЕМІ ядерних вибухів

Інтенсивний сучасний технічний розвиток несе комфорт і процвітання в усі сфери людської діяльності, проте поряд з цим зростає ймовірність техногенної

небезпеки. Техногенні небезпеки можуть носити механічний, енергетичний та хімічний характер. Однією з найпотужніших енергетичних небезпек є ядерний вибух. Ядерний вибух – це вибух, який утворюється при виділенні внутрішньої енергії при розпаді важких ядер урану-235, 233, 238, плутонію-239 та ін.

Внаслідок дії своїх вражаючих факторів ядерні вибухи призводять до масштабних небезпек та таких негативних наслідків як загибель людей, тварин і рослин, потрапляння радіоактивних речовин в навколишнє середовище, руйнування будівель, затоплення територій, пожеж.

Електромагнітне поле – це особлива форма матерії, яка виникає в результаті виробничої діяльності людей. Електромагнітні хвилі можуть існувати у вигляді випромінювань, що переміщуються в просторі зі швидкістю світла (с).

Вплив ЕМП на здоровий організм людини досліджений ще в наш час недостатньо. Існує ймовірність, що ЕМП призводить до розщеплення атомів і молекул організму на іони, а це може бути причиною утворення іонних струмів, які в результаті сприяють підвищенню температури тіла людини. Дослідження показали, що ЕМП може призводити до гальмування рефлексів, гіпотонії, збільшення лейкоцитів в крові людини, погіршення зору та ін. Певну небезпеку представляють для людини лінії електропередачі, поблизу яких визначається дуже значна напруженість електричного поля (до 15 КВ/м) [30].

При ядерному вибуху утворюється сильне електромагнітне випромінювання в широкому діапазоні хвиль з максимумом спектральної щільності в області 15-30 кГц. Це випромінювання триває кілька мікросекунд, тому його прийнято називати електромагнітним імпульсом.

ЕМІ характеризується великою напруженістю електричного та магнітного полів. Ці параметри є основним вражаючим фактором для струмопровідних елементів, хоча значного впливу на людину не мають. Імпульс струму, що з’являється на момент вибуху і високий потенціал можуть вивести з ладу трансформатор, пошкодити напівпровідникові елементи в приладах, розплавити ізоляційний матеріал на кабелях, спричинити вигорання запобіжників та розрядників. Особливу увагу слід приділити пунктам управління, де працюють

люди, оскільки існує загроза ураження персоналу внаслідок виведення з ладу техніки та розгортання аварійної ситуації.

Для захисту необхідно здійснити екранування ліній зв'язку, пунктів управління, окремих вузлів та блоків, електро та радіоапаратури, використовувати спеціальні захисні пристрої [31].

Поряд з цим слід зазначити, оскільки час ЕМІ в кілька мільярдних часток секунд настільки мізерний, що його зовсім недостатньо, щоб спрацювали більшість електронних систем захисту. Тому чутливе комп’ютерне обладнання не завжди зможе уникнути потужного перенавантаження. Комп’ютерні системи містять багато напівпровідникових елементів (цифрові процесори, діоди, транзистори, випрямлячі та ін.), які є дуже вразливими до дії ЕМІ.

У випадку, коли ядерний вибух відбувся неподалік лінії електропостачання, то наведені в них напруги можуть проходити через провідники впродовж багатьох кілометрів, а також псувати апаратуру та становити загрозу людям, які перебувають на безпечній відстані від вибуху.

Отже, основні критерії, які слід враховувати під час підвищення стійкості роботи електричних та комп’ютеризованих систем при дії ЕМІ - це максимальна напруга та максимальна енергія. Зокрема напруга, що наводиться у струмопровідних елементах та кабельних лініях передач, при якій ще не виходять з ладу системи.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра було проведено комплексне дослідження методів захисту мережевої інфраструктури від багатовекторних DDoS-атак та інших кіберзагроз шляхом впровадження системи виявлення та запобігання вторгненням (IPS) на основі маршрутизатора pfSense та системи Snort.

У першому розділі було здійснено аналіз предметної області, зокрема різних типів DDoS-атак, їхніх характеристик та наслідків для організацій. Особлива увага приділялася багатовекторним DDoS-атакам, які поєднують кілька методів для максимізації впливу на цільову систему. Розглянуто також існуючі підходи до захисту від таких атак, що заклало теоретичну основу для подальших досліджень.

У другому розділі було розроблено та налаштовано тестове лабораторне середовище на базі гіпервізора VMware ESXi. Це середовище включало маршрутизатор pfSense, сервер Ubuntu Linux та атакуючі машини на базі Parrot Security OS. Лабораторне середовище дозволило безпечно моделювати різні сценарії атак та оцінювати ефективність захисних механізмів у контрольованих умовах.

У третьому розділі було змодельовано різні типи кіберзагроз, включаючи DDoS-атаки типів SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, а також атаки типу Brute-force. Використовуючи інструменти hping3, ab та hydra, було проведено симуляцію реальних сценаріїв атак та оцінено їхній вплив на цільову інфраструктуру.

Особлива увага було приділено розробці та оптимізації правил для системи Snort, спрямованих на ефективне виявлення та блокування цих загроз з мінімізацією хибних спрацьовувань. Тестування розроблених правил IPS підтвердило їхню ефективність у виявленні та блокуванні різних типів атак, включаючи багатовекторні. Аналіз журналів подій та сповіщень засвідчив правильність налаштувань та надійність захисту, забезпеченого системою Snort у поєднанні з pfSense.

У результаті виконаної роботи було досягнуто наступних основних результатів:

- детально досліджено різні типи DDoS-атак та їхні характеристики, що дозволило зрозуміти механізми їхнього впливу на мережеву інфраструктуру;
- створено реалістичне тестове лабораторне середовище, яке дозволяє моделювати та аналізувати різні сценарії кіберзагроз у безпечних умовах;
- успішно налаштовано систему виявлення та запобігання вторгненням на основі pfSense та Snort, з оптимізованими правилами для ефективного виявлення конкретних типів атак;
- проведено комплексне тестування розроблених правил IPS, яке підтвердило їхню здатність ефективно виявляти та блокувати різні типи атак, забезпечуючи високий рівень захисту мережі.

Таким чином, проведене дослідження підтвердило доцільність використання комбінованого підходу з використанням pfSense та Snort для захисту мережевих інфраструктур від сучасних кіберзагроз. Розроблені методики та правила можуть бути застосовані в реальних умовах для підвищення рівня кібербезпеки організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a ddos attack? Ddos meaning, definition & types | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/ddos-attack (date of access: 04.11.2024).
2. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
3. Ping (ICMP) flood DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ (date of access: 04.11.2024).
4. Smurf DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/ (date of access: 04.11.2024).
5. Ping of death DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/ (date of access: 04.11.2024).
6. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
7. SYN flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/ (date of access: 04.11.2024).
8. UDP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (date of access: 04.11.2024).
9. What is an ACK flood DDoS attack? | Types of DDoS attacks. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/what-is-an-ack-flood/ (date of access: 04.11.2024).

10. Application layer DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/ (date of access: 04.11.2024).
11. HTTP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/ (date of access: 04.11.2024).
12. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
13. What is a DNS flood? | DNS flood DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/ (date of access: 04.11.2024).
14. MAC Flooding attack. Trustline. URL: https://www.trustline.sa/blog/MAC-Flooding-attack (date of access: 04.11.2024).
15. What is a DDoS botnet? Cloudflare. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (date of access: 04.11.2024).
16. What is the Internet of Things (IoT)? Cloudflare. URL: https://www.cloudflare.com/learning/ddos/glossary/internet-of-things-iot/ (date of access: 04.11.2024).
17. What is the Mirai Botnet? Cloudflare. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (date of access: 04.11.2024).
18. DNS amplification attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (date of access: 04.11.2024).
19. 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.

20. 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.
21. What is a content delivery network (CDN)? | How do CDNs work. Cloudflare. URL: https://www.cloudflare.com/learning/cdn/what-is-a-cdn/ (date of access: 04.11.2024).
22. 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.
23. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
24. 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.
25. PfSense documentation | pfsense documentation. Netgate Documentation | Netgate Documentation. URL: https://docs.netgate.com/pfsense/en/latest/ (date of access: 04.11.2024).
26. Lupenko, S., Orobchuk, O., Kateryniuk, I., Kozak, R., & Lypak, H. (2023). Secure information system for Chinese Image medicine knowledge consolidation.
27. ParrotOS documentation | parrotos documentation. Parrot Security. URL: https://parrotsec.org/docs/ (date of access: 04.11.2024).
28. Documents | Snort. Snort. URL: https://www.snort.org/documents (date of access: 04.11.2024).
29. Жидецький В.Ц. Охорона праці користувачів комп´ютерів. Львів: Афіша, 2011. 176 с.

30. В.В.Зацарний, Н.А.Праховнік, О.В.Землянська Безпека життєдіяльності: Конспект лекцій для студентів усіх спеціальностей за освітньокваліфікаційним рівнем «бакалавр» . Київ: НТУУ «КПІ», 2016. 92 с.
31. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник / В.С. Стручок, – Тернопіль: ТНТУ ім. І.Пулюя, 2022. – 150 с.

Додаток А Публікація

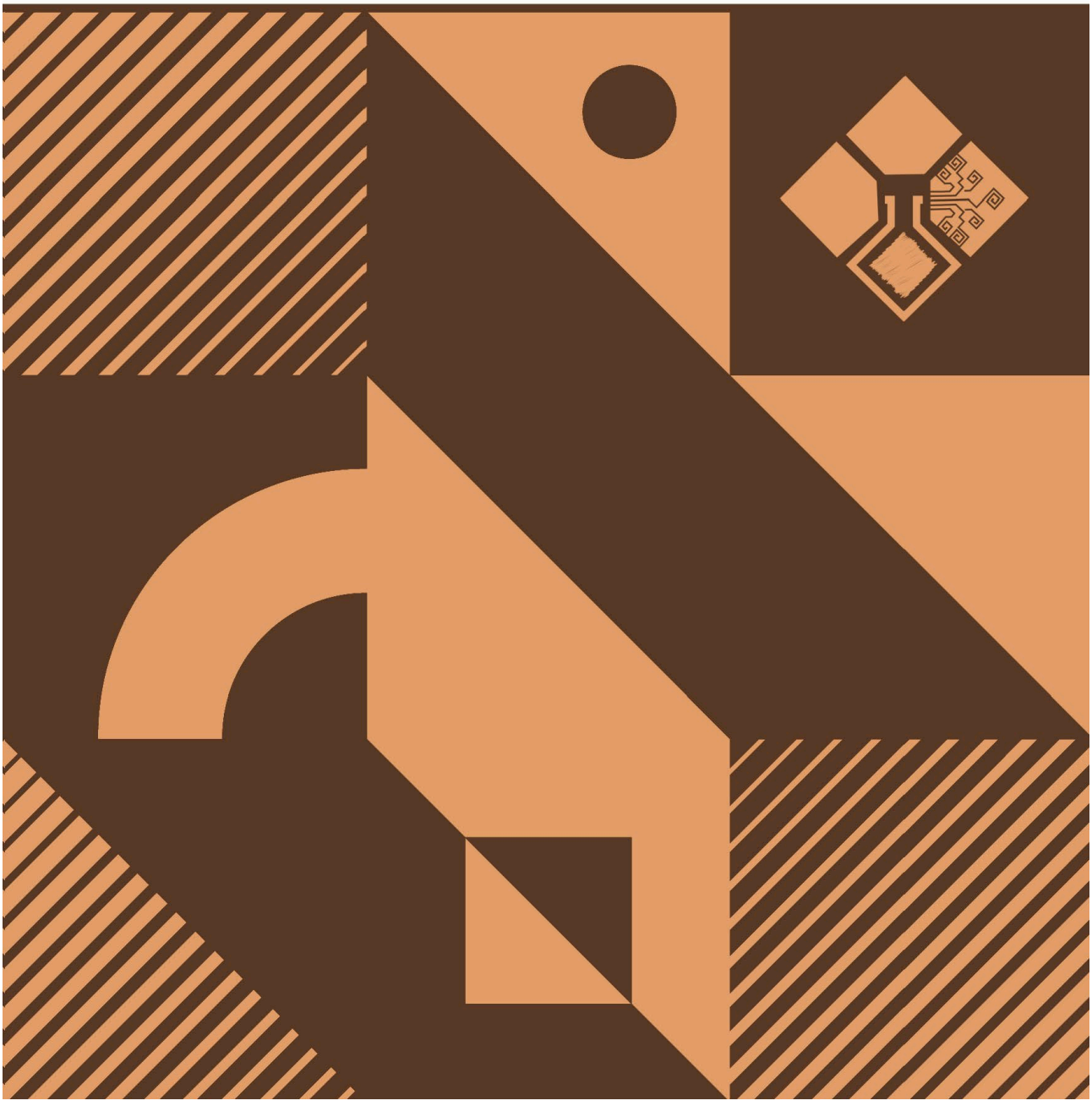
ЗБІРНИК НАУКОВИХ ПРАЦЬ

З МАТЕРІАЛАМИ VIII МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

22 ЛИСТОПАДА 2024 РІК

М. БІЛА ЦЕРКВА, УКРАЇНА

«ЗДОБУТКИ ТА ДОСЯГНЕННЯ ПРИКЛАДНИХ ТА ФУНДАМЕНТАЛЬНИХ НАУК XXI СТОЛІТТЯ»



ЗБІРНИК НАУКОВИХ
ПРАЦЬ З МАТЕРІАЛАМИ
VIII МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

ЗДОБУТКИ ТА ДОСЯГНЕННЯ ПРИКЛАДНИХ ТА ФУНДАМЕНТАЛЬНИХ НАУК XXI СТОЛІТТЯ

22 листопада 2024 рік
м. Біла Церква, Україна

Вінниця, Україна
«UKRLOGOS Group»
2024

СЕКЦІЯ XVII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

DOI 10.62731/mcnd-22.11.2024.002

OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS

SCIENTIFIC RESEARCH GROUP:

Vitaliy Tymoshchuk
ORCID ID: 0009-0007-2858-9434
First-level student of higher education
Faculty of Applied Information Technologies and Electrical Engineering
Ternopil Ivan Puluj National Technical University, Ukraine

Oleksandr Mykhailovskyi
Second-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, Ukraine

Andrii Dolinskyi
ORCID ID: 0009-0003-4230-0183
Third-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, Ukraine

Anastasiia Orlovska
ORCID ID: 0009-0001-0286-0691
First-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, Ukraine

Scientific supervisor: Dmytro Tymoshchuk
ORCID ID: 0000-0003-0246-2236
Senior lecturer at the Department of Cyber Security
Ternopil Ivan Puluj National Technical University, Ukraine

Abstract. *DDoS attacks have been and remain one of the biggest threats to information systems and networks. Multi-vector DDoS attacks, which combine several types of attacks*

simultaneously, are becoming increasingly common, making them difficult to neutralise. This article explores the use of optimised rules for a Snort-based intrusion detection and prevention system (IPS) in the pfSense environment. The methodology for developing and testing rules is presented, as well as experimental results that demonstrate an increase in detection efficiency and a decrease in false positives.

Introduction. Ensuring the security of information systems is becoming an increasingly difficult task. DDoS (Distributed Denial of Service) attacks are one of the most serious threats aimed at disrupting the availability of services by overloading them with an excessive number of requests [1]. Attackers use a variety of methods and tools to carry out such attacks, and over time, they are becoming more sophisticated and effective.

Particular attention should be paid to multi-vector DDoS attacks, which combine several types of attacks simultaneously. This allows attackers to bypass traditional defences and complicates the process of detecting and neutralising them. Traditional defence systems, such as firewalls and standard intrusion detection and prevention systems (IDS/IPS), are often not effective enough against such complex threats. In this regard, there is a need to develop new approaches and methods to effectively detect and prevent multi-vector DDoS attacks. One of the most promising areas is the optimisation of rules for intrusion detection and prevention systems (IPS), which allows to increase their sensitivity and accuracy, reducing the number of false positives.

Methodology. To achieve this goal, we created a test laboratory environment that allows simulating various attack scenarios under controlled conditions [2] (Fig. 1).

The basis of the environment was the VMware ESXi hypervisor, which provided the ability to deploy the necessary virtual machines and networks [3]. This made it possible to isolate the test environment from the real network, ensuring the security and controllability of the experiments [4]. A pfSense router with integrated Snort was used to implement the IPS functions. pfSense is a powerful open source tool that provides extensive network and security configuration options [5]. This allowed us to flexibly configure firewall and IPS rules, adapting them to the specific requirements of the study. Snort, in turn, is one of the most popular intrusion detection and prevention systems that supports flexible rule configuration [6]. The Ubuntu Linux-based server acted as a DNS server, web server, and SSH server, which allowed us to model real services that are often targeted by DDoS attacks. This ensured that the

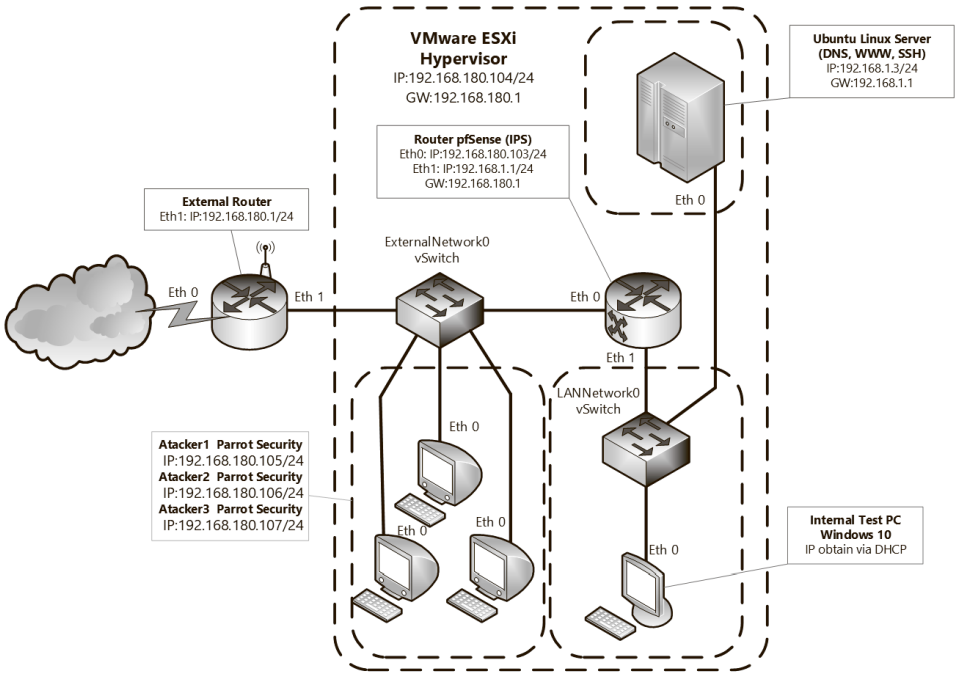


Fig. 1. **Scheme of the test environment**

experiments were realistic and allowed us to assess the impact of attacks on different types of services. Attack machines based on Parrot Security OS were used to generate malicious traffic and simulate various types of attacks. Parrot Security OS contains a wide range of tools for penetration testing and security analysis, which made it an ideal choice for our purposes [7].

To simulate the attacks, specialised tools were used to generate different types of malicious traffic. One of the main tools was hping3, which allows us to generate network traffic with the required parameters. SYN Flood, UDP Flood, and ICMP Flood attacks were modelled using hping3 [8,9,10]. This tool allows us to flexibly configure packet headers, frequency, and traffic volume, which allowed us to accurately model the behaviour of attackers. To simulate HTTP Flood attacks, we used the Apache Benchmark (ab) tool, which is commonly used to test the performance of web servers. Ab allows us to generate a large volume of HTTP requests to the server, which simulates high-load activity and allows us to assess the server's resistance to overload. A multi-vector attack was modelled by simultaneously launching several types of attacks from different attacking machines. This created a complex load on the target server and network infrastructure, which brought the conditions as close as possible

to real cyber threats. The simultaneous effect of several attacks with different vectors allowed us to test the ability of the IPS system to respond effectively to complex scenarios.

Development of optimised IPS rules. One of the key stages of the study was the development of optimised rules for the Snort system. When developing the rules, we took into account the features of each type of attack and the specifics of network traffic in the test environment. The goal was to create rules that would effectively detect threats while minimising false positives and not creating an excessive load on the system.

To detect SYN Flood attacks, a rule was created that triggers when an excessive number of SYN packets are detected in a short period of time. A threshold was defined for the number of packets that exceeds normal activity and indicates a possible attack. This made it possible to distinguish legitimate traffic from malicious traffic based on statistical traffic characteristics. Similarly, for UDP Flood and ICMP Flood attacks, rules were developed that respond to an abnormally high frequency of the corresponding packets. Particular attention was paid to setting thresholds and time intervals to avoid false positives during peak legitimate traffic loads. This required analysing normal network activity and setting adequate limits. To detect HTTP Flood attacks, we used the analysis of HTTP requests. The rule was triggered when an excessive number of requests of the same type to a web server was detected, exceeding the set thresholds. Additionally, request parameters, such as URIs and HTTP methods, were analysed to more accurately identify malicious activity.

When developing the rules, special attention was paid to optimisation to reduce the load on the system and minimise false positives. Variables for IP addresses and ports were used to make the rules more flexible and easier to manage. This ensured that the rules could be quickly adapted to changes in the network environment without having to rewrite them from scratch. Regular expressions and other rule parameters were also optimised to improve system performance. For example, efficient search and filtering algorithms were used to minimise latency and impact on network bandwidth.

Testing and results. After implementing the developed rules, a series of tests were conducted to evaluate their effectiveness. Attacking machines generated multi-vector DDoS attacks against the target server, and Snort in pfSense analysed the traffic and responded according to the configured rules.

The test results showed that the system effectively detects and blocks various types of attacks. All planned attacks were successfully detected, and

malicious traffic was blocked before entering the network. This confirms the effectiveness of the developed rules and their ability to protect the network from complex threats. Snort's event logs confirmed that the rules were triggered correctly and provided detailed information about the detected threats. Administrators could view the details of each incident, including source and destination IP addresses, attack type, and trigger time. This allowed them not only to detect attacks but also to analyse them to further improve the security system. The number of false positives was minimal, which indicates that the rules were successfully optimised. The system did not block legitimate traffic, which ensured uninterrupted operation of services for legitimate users. This is critical, as excessive sensitivity of the system can lead to a negative impact on business processes.

It was also noted that the load on the system did not exceed the permissible values, which indicates the effectiveness of the optimisation and the possibility of applying the developed rules in real environments with high traffic levels. This means that the system can be scaled up for use in large networks without significant additional costs.

Discussion. The results of the study confirmed that the use of optimised rules for the Snort system in pfSense allows to effectively detect and block multi-vector DDoS attacks. The flexibility and customisability of the rules make it possible to adapt the system to specific network requirements and traffic patterns. An important success factor is a deep understanding of the nature of attacks and network traffic in a particular environment. This allows us to develop rules that respond as accurately as possible to real threats, while reducing the number of false positives. Analysing normal network activity and defining thresholds are key elements of this process.

However, it should be borne in mind that with the development of technology and the emergence of new attack methods, it is necessary to regularly update the rule base and adapt it to new threats. Attackers are constantly looking for new ways to circumvent security, so the IPS system must be dynamic and capable of rapid adaptation. It is also advisable to combine signature analysis with behavioural analysis to detect unknown or modified attacks.

Conclusions. In this paper, we have demonstrated that optimising rules for an intrusion detection and prevention system is an effective approach to increasing the level of protection against multi-vector DDoS attacks. The developed and tested rules allowed the Snort system in pfSense to effectively

detect and block various types of attacks, ensuring the security of information systems and networks.

References:

1. What is a ddos attack? Ddos meaning, definition & types | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/ddos-attack
2. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56. https://doi.org/10.31891/2219-9365-2024-79-7
3. 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. https://doi.org/10.62731/mcnd-24.05.2024.001
4. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології "Тернопільського національного технічного університету імені Івана Пулюя, 95-95.
5. PfSense documentation | pfsense documentation. (n.d.). Netgate Documentation | Netgate Documentation. https://docs.netgate.com/pfsense/en/latest/
6. Documents | Snort. Snort. (n.d.). https://www.snort.org/documents.
7. ParrotOS documentation | parrotos documentation. (n.d.). Parrot Security. https://parrotsec.org/docs/
8. 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.
9. 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.
10. Tymoshchuk, D., & Yatskiv, V. (2024). SLOWLORIS DDOS DETECTION AND PREVENTION IN REAL-TIME. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176. https://doi.org/10.36074/logos-16.08.2024.036