

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: "Моделювання кіберзагроз та оцінка ефективності системи IDS"

Виконав: студент VI курсу, групи СБм-61

Спеціальності:

125 «Кібербезпека та захист інформації»

(шифр і назва напрямку підготовки, спеціальності)

Пахода Владислав Юрійович

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.
(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 Паході Владиславу Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Моделювання кіберзагроз та оцінка ефективності системи IDS

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 включають тестове середовище на основі гіпервізора KVM, OPNsense, IDS Suricata, Metasploitable VM, Kali Linux та Ubuntu Linux.

4. Зміст роботи (перелік питань, які потрібно розробити)

Огляд існуючих типів атак та їх наслідків. Методи захисту від різних типів атак.

Аналіз функціональних можливостей OPNsense та IDS Suricata.

Провести налаштування системи IDS Suricata на базі OPNsense.

Здійснити моделювання кіберзагроз із використанням Metasploitable VM та Kali Linux.

Оцінити ефективність IDS Suricata за допомогою тестування реальних сценаріїв атак.

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.

Типи атак. Botnet мережі. Схема розташування NIDS.

Схема тестового лабораторного середовища.

Елементи тестового лабораторного середовища.

Тестування лабораторного середовища.

Активні правила IDS Suricata в OPNsense.

Моделювання кіберзагроз та оцінка ефективності правил IDS.

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 в галузі дослідження	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.	Моделювання кіберзагроз та оцінка ефективності системи IDS	25.10 - 30.10	Виконано
6.	Оформлення розділу «Огляд предметної області»	30.10 – 05.11	Виконано
7.	Оформлення розділу «Створення тестового середовища»	06.11 – 10.11	Виконано
8.	Оформлення розділу «Налаштування системи виявлення вторгнень та оцінка її ефективності»	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

(підпис)

Пахода В. Ю.

(прізвище та ініціали)

Керівник роботи

(підпис)

Оробчук О. Р.

(прізвище та ініціали)

АНОТАЦІЯ

Моделювання кіберзагроз та оцінка ефективності системи IDS // ОР «Магістр» // Пахода Владислав Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 80, рис. – 39, табл. – - , кресл. – 18, додат. – 1.

Ключові слова: DDoS, IDS, Suricata, OPNsense, Cybersecurity, Brute-force, SQL injection.

У кваліфікаційній роботі магістра проведено комплексне дослідження сучасних кіберзагроз та методів захисту від них. Основна увага була зосереджена на аналізі атак на доступність, конфіденційність та цілісність даних, а також на сучасних підходах до їх виявлення. Було створено тестове лабораторне середовище на базі гіпервізора KVM, яке включає віртуальні машини з операційними системами Kali Linux, Metasploitable VM та OPNsense. Це середовище дозволило моделювати різноманітні кіберзагрози в контрольованих умовах, що є критично важливим для дослідження та оцінки ефективності засобів захисту. Важливою частиною роботи була оптимізація наборів правил для підвищення ефективності роботи IDS Suricata. Вибір і активація специфічних правил для кожного типу атак, що відповідають вразливостям Metasploitable VM, дозволили покрити більшість можливих сценаріїв експлуатації в цьому середовищі. Загальна кількість активних правил становила 2602, що забезпечило комплексний захист від різних типів атак. Такий підхід до оптимізації дозволив зменшити кількість хибних спрацювань та підвищити ефективність системи.

Результати дослідження підтвердили високу ефективність налаштованої системи IDS Suricata у виявленні різних типів кіберзагроз. Це свідчить про доцільність використання таких систем у реальних мережах для підвищення рівня безпеки та оперативного реагування на потенційні загрози.

ABSTRACT

Cyber threat modeling and IDS efficiency evaluation // Thesis of educational level "Master"// Pakhoda Vladyslav // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group CBM-61 // Ternopil, 2024 // P. 80, figs. 39, tables -, drawings 18, added. 1.

Keywords: DDoS, IDS, Suricata, OPNsense, Cybersecurity, Brute-force, SQL injection.

In the master's thesis, a comprehensive study of modern cyber threats and methods of protection against them was conducted. The main focus was on analysing attacks on data availability, confidentiality and integrity, as well as on modern approaches to their detection. A test lab environment based on a KVM hypervisor was created, including virtual machines running Kali Linux, Metasploitable VM, and OPNsense operating systems. This environment made it possible to simulate various cyber threats under controlled conditions, which is critical for researching and evaluating the effectiveness of security tools. An important part of the work was the optimisation of rule sets to improve the efficiency of Suricata IDS. The selection and activation of specific rules for each type of attack corresponding to Metasploitable VM vulnerabilities allowed us to cover most possible exploitation scenarios in this environment. The total number of active rules was 2602, which provided comprehensive protection against various types of attacks. This approach to optimisation reduced the number of false positives and increased system efficiency.

The study results confirmed the high efficiency of the configured IDS Suricata system in detecting various types of cyber threats. This indicates the feasibility of using such systems in real networks to improve security and respond quickly to potential threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП.....	9
РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ	11
1.1 Огляд та класифікація сучасних кібератак.....	11
1.1.1 Атаки на доступність.....	11
1.1.2 Атаки на конфіденційність	21
1.1.3 Атаки на цілісність	23
1.2 Наслідки атак.....	24
1.3 Огляд існуючих підходів до захисту від атак	28
1.3 Висновки до розділу 1	31
РОЗДІЛ 2 СТВОРЕННЯ ТЕСТОВОГО СЕРЕДОВИЩА	33
2.1 Схема лабораторного тестового середовища.....	33
2.2 Налаштування компонентів тестового середовища	35
2.2.1 Гіпервізор KVM	35
2.2.2 Маршрутизатор OPNsense	37
2.2.3 Операційна системи Metasploitable VM	40
2.2.4 Операційна система Kali Linux.....	43
2.3 Тестування лабораторного середовища.....	45
2.4 Висновки до розділу 2	46
РОЗДІЛ 3 НАЛАШТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕННЯМ ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ.....	48
3.1 Налаштування IDS Suricata	48
3.2 Налаштування наборів правил для підвищення ефективності роботи IDS	53
3.3 Моделювання кіберзагроз та оцінка ефективності правил IDS	55
3.1.1 Сканування відкритих портів	56
3.1.2 Brute-force атаки.....	58
3.1.3 Атака типу SQL-ін'єкції.....	59
3.1.4 Атаки типу DDoS	63
3.4 Висновки до розділу 3	66
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	68
4.1 Охорона праці.....	68

4.2 Забезпечення захисту працівників суб'єкта господарювання від іонізуючого випромінювання	71
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	77
Додаток А Публікація	81

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS	—	Intrusion Detection System
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
OSI	—	Open Systems Interconnection
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ICMP	—	Internet Control Message Protocol
HTTP	—	Hypertext Transfer Protocol
DNS	—	Domain Name System
NTP	—	Network Time Protocol
MITM	—	Man-in-the-Middle
MFA	—	Multi-Factor Authentication
IoT	—	Internet of Things
HIDS	—	Host Intrusion Detection System
NIDS	—	Network Intrusion Detection System
IPS	—	Intrusion Prevention System
LAN	—	Local Area Network
WAN	—	Wide Area Network
KVM	—	Kernel-based Virtual Machine
DHCP	—	Dynamic Host Configuration Protocol
BM	—	Віртуальна машина
SSH	—	Secure Shell
DVWA	—	Damn Vulnerable Web Application
NAT	—	Network Address Translation

ВСТУП

Актуальність теми. З кожним роком кількість кіберзагроз зростає, а методи зловмисників стають усе більш витонченими. Захист інформаційних систем вимагає використання ефективних технологій виявлення та протидії атакам. Системи виявлення вторгнень (IDS) відіграють важливу роль у моніторингу та аналізі мережевої активності та виявленні потенційних загроз. Впровадження та тестування таких систем, як OPNsense з інтеграцією IDS Suricata, дозволяє оцінити їхню ефективність у реальних умовах. Це питання набуває особливої актуальності через необхідність надійного захисту мереж і швидкої реакції на кіберінциденти.

Мета і задачі дослідження. Метою роботи є моделювання кіберзагроз і оцінка ефективності системи IDS на основі OPNsense Suricata.

Для досягнення цієї мети необхідно вирішити такі задачі:

- провести аналіз існуючих типів атак та їхніх наслідків;
- описати методи захисту від різних типів атак;
- дослідити функціональні можливості OPNsense та IDS Suricata;
- встановити та налаштувати систему IDS Suricata на базі OPNsense;
- здійснити тестування системи за допомогою сценаріїв атак, створених за допомогою Metasploitable VM та Kali Linux;
- оцінити ефективність системи на основі результатів тестування.

Об'єкт дослідження. Системи виявлення та запобігання вторгненням у мережевих середовищах.

Предмет дослідження. Особливості роботи системи IDS Suricata на базі OPNsense при моделюванні кіберзагроз та оцінка її ефективності.

Наукова новизна одержаних результатів кваліфікаційної роботи. Удосконалено підхід до конфігурації системи IDS, що дозволяє підвищити рівень виявлення атак шляхом оптимізації правил Suricata. Дістало подальший розвиток практичне використання систем IDS для виявлення кіберзагроз у тестовому середовищі з реалістичними сценаріями атак за допомогою Metasploitable VM та Kali Linux.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані у сфері кібербезпеки для вдосконалення захисту мережевих інфраструктур. Запропоновані методики налаштування та тестування системи IDS можуть бути застосовані фахівцями з безпеки та адміністраторами мереж для підвищення рівня захисту від кіберзагроз.

Апробація результатів магістерської роботи. Основні результати дослідження були представлені на VIII Міжнародної науково-практичної конференції “ГЛОБАЛІЗАЦІЯ НАУКОВОГО ЗНАННЯ: МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ТА ІНТЕГРАЦІЯ НАУК” що проводилася 29.11.2024

Публікації. Основні результати кваліфікаційної роботи опубліковано в журналі “ГРААЛЬ НАУКИ” № 46 (листопад, 2024) (див. Додаток А).

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд та класифікація сучасних кібератак

Сучасні кіберзагрози можна класифікувати за кількома критеріями. За механізмом дії виділяють атаки на доступність, конфіденційність та цілісність даних [1].

1.1.1 Атаки на доступність

Атаки на доступність, відомі як атаки відмови в обслуговуванні (DoS) та розподілені атаки відмови в обслуговуванні (DDoS), спрямовані на те, щоб зробити мережеві ресурси або сервіси недоступними для легітимних користувачів [2]. Це досягається шляхом перевантаження цільової системи надмірною кількістю запитів або експлуатацією вразливостей, що призводять до збоїв у роботі системи.

Мережевий рівень (рівень 3) моделі OSI відповідає за маршрутизацію пакетів даних між вузлами мережі та забезпечує логічну адресацію [3]. Атаки на цьому рівні спрямовані на експлуатацію вразливостей протоколів і механізмів маршрутизації для перехоплення, модифікації або блокування трафіку. Ці атаки можуть призвести до уповільнення роботи мережі, втрати даних або повної відмови в обслуговуванні. Одним із поширених типів таких атак є ICMP Flood (Ping Flood), коли зловмисник надсилає велику кількість ICMP Echo Request (ping) пакетів до цільової системи, перевантажуючи її ресурси [4] (див. рисунок 1.1).

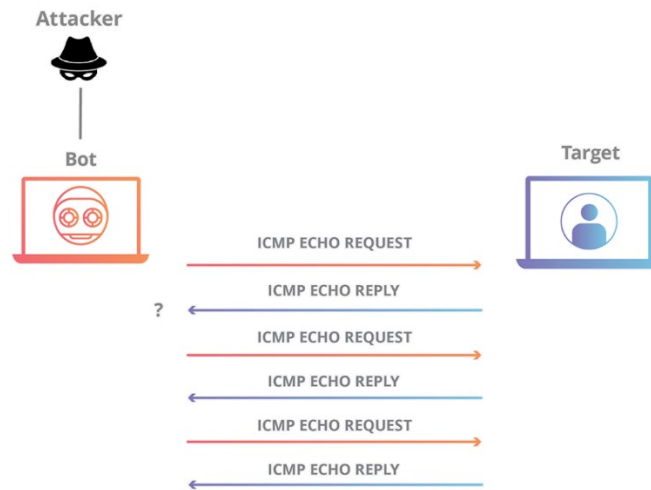


Рисунок 1.1 – Атака типу ICMP Flood (Ping Flood)

Система намагається відповісти на кожен запит, витрачаючи процесорний час та пропускну здатність мережі, що може призвести до відмови в обслуговуванні для легітимних користувачів. Іншим прикладом є Smurf Attack, яка використовує підроблені ICMP Echo Request пакети з IP-адресою джерела, встановленою на IP-адресу жертви, надсилаючи їх до широкомовних адрес [5]. Кожен пристрій, отримавши такий запит, відповідає на нього, спрямовуючи трафік до жертви, що призводить до перевантаження цільової системи відповідями від багатьох пристроїв у мережі. Атака Ping of Death – це тип мережевої атаки при якому надсилаються ICMP-пакети розміром, що перевищує максимальний дозволений розмір IP-пакету [6]. Стандартний розмір IP-пакету не повинен перевищувати 65,535 байтів, але при атаці Ping of Death зловмисник надсилає пакети, які після фрагментації та збирання на стороні цільової системи можуть перевищити цей ліміт. Коли така цільова система отримує та обробляє фрагментовані пакети, вони можуть зібратися у великий пакет, який перевищує максимальний дозволений розмір. Це може спричинити помилку переповнення буфера, що призводить до збою, перезавантаження або виходу з ладу операційної системи чи додатків (див. рисунок 1.2).

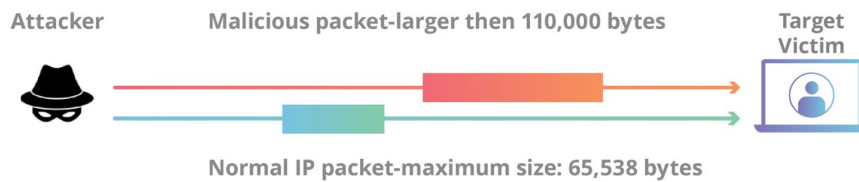


Рисунок 1.2 – Атака типу Ping of Death

Атака IP Spoofing полягає в тому, що зловмисник підробляє IP-адресу джерела в пакетах, видаючи себе за інший пристрій [7] (див. рисунок 1.3).

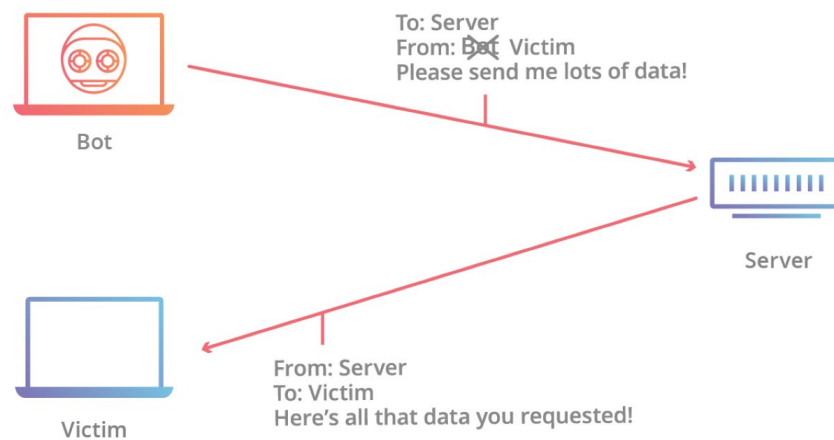


Рисунок 1.3 – Атака типу IP Spoofing

Це дозволяє обійти механізми аутентифікації або фільтрації за IP-адресами, надсилаючи підроблені пакети до цільової системи, що може призвести до несанкціонованого доступу або інших атак. Fragmentation Attacks експлуатують механізм фрагментації IP-пакетів для обходу систем захисту або викликання збоїв у цільовій системі. Зловмисник надсилає неправильно фрагментовані пакети, які система не може правильно зібрати, що призводить до збоїв або обходу брандмауерів та IDS/IPS систем.

Атаки на транспортному рівні (рівень 4) моделі OSI спрямовані на порушення роботи мережесервісів шляхом перевантаження їх ресурсів через експлуатацію протоколів TCP та UDP [8]. Ці атаки можуть призвести до недоступності сервісів для легітимних користувачів та значних фінансових втрат для організацій. Одним із найпоширеніших типів таких атак є SYN Flood.

Зловмисник надсилає велику кількість запитів на встановлення TCP-з'єднання (SYN-пакетів) до сервера, але не завершує трестороннє рукошискування (див. рисунок 1.4).

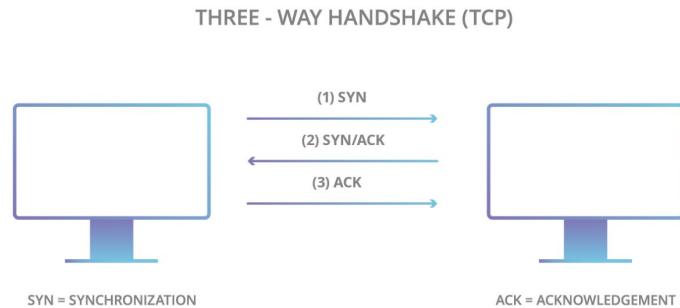


Рисунок 1.4 – Процедура коректної взаємодії

З'єднання залишаються напіввідкритими (див. рисунок 1.5).

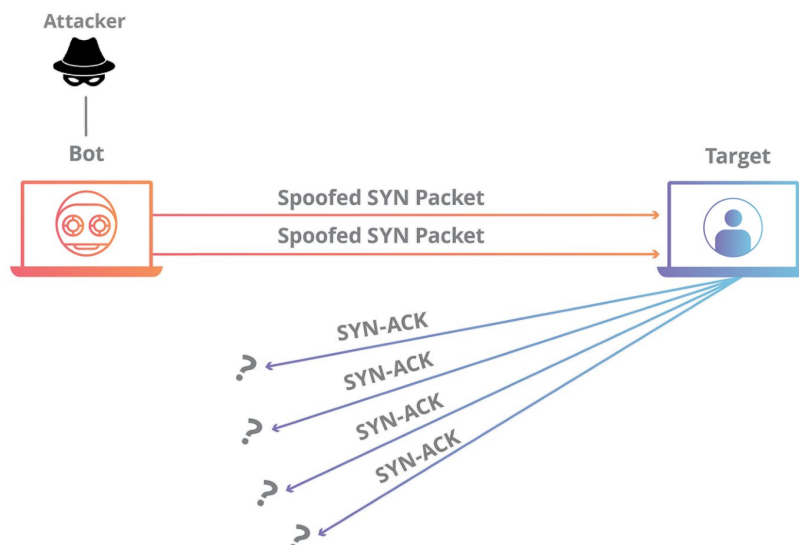


Рисунок 1.5 – Атака типу SYN Flood

Це призводить до перевантаження таблиці з'єднань сервера, що унеможлиблює обробку нових запитів від легітимних користувачів [9]. Іншим прикладом є UDP Flood, коли зловмисник надсилає велику кількість UDP-пакетів до випадкових або конкретних портів цільового сервера [10] (див. рисунок 1.6).

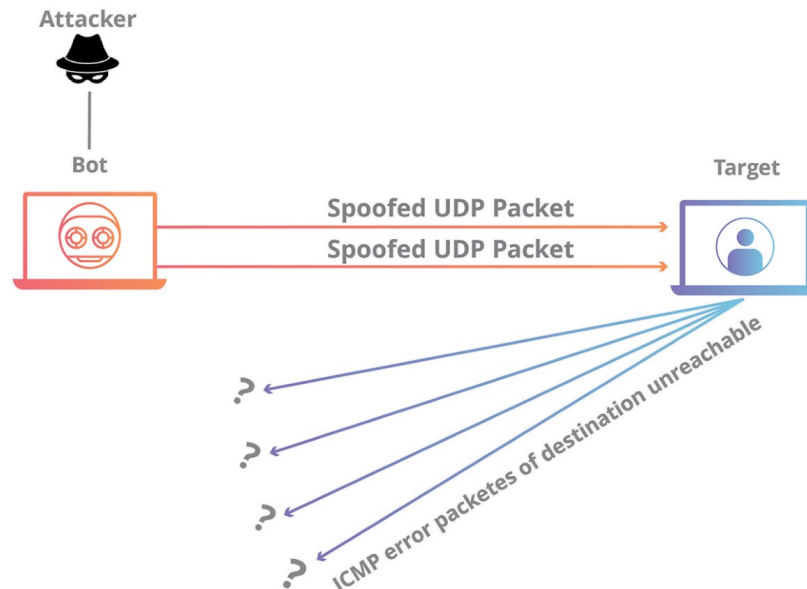


Рисунок 1.6 – Атака типу UDP Flood

Сервер намагається обробити кожен запит, що споживає його ресурси та може призвести до відмови в обслуговуванні. ACK Flood полягає в надсиланні великої кількості TCP ACK-пакетів без попереднього встановлення з'єднання [11]. Це перевантажує мережеву інфраструктуру та ресурси сервера, що може призвести до збоїв у роботі. RST Flood здійснюється шляхом надсилання великої кількості TCP RST-пакетів для розриву існуючих з'єднань. Це примусово закриває активні з'єднання, порушуючи роботу сервісів та додатків. Атаки з використанням фрагментованих пакетів (Fragmented Packet Attack) передбачають надсилання неправильно фрагментованих TCP або UDP-пакетів, які сервер не може правильно зібрати. Це перевантажує систему обробки пакетів та може спричинити збої в роботі сервера.

Атаки на прикладному рівні (рівень 7) моделі OSI спрямовані на порушення роботи конкретних додатків або сервісів, що функціонують на цільовому сервері [12]. На відміну від атак на нижчих рівнях, які націлені на мережеву інфраструктуру, атаки рівня 7 експлуатують вразливості в програмному забезпеченні, зокрема в веб-додатках, шляхом надсилання легітимних на вигляд запитів у великій кількості. Зловмисники генерують значний обсяг запитів до цільового додатка, імітуючи поведінку реальних користувачів. Ці запити можуть включати HTTP GET або POST-запити, запити до баз даних або інші операції, які вимагають значних ресурсів для обробки. Метою є перевантаження

серверних ресурсів, таких як процесор, пам'ять або дискова підсистема, що призводить до уповільнення роботи або повної недоступності сервісу для легітимних користувачів. Одним із поширених методів є HTTP Flood [13], коли зломисник надсилає велику кількість HTTP-запитів до веб-сервера з метою перевантаження його ресурсів (див. рисунок 1.7).

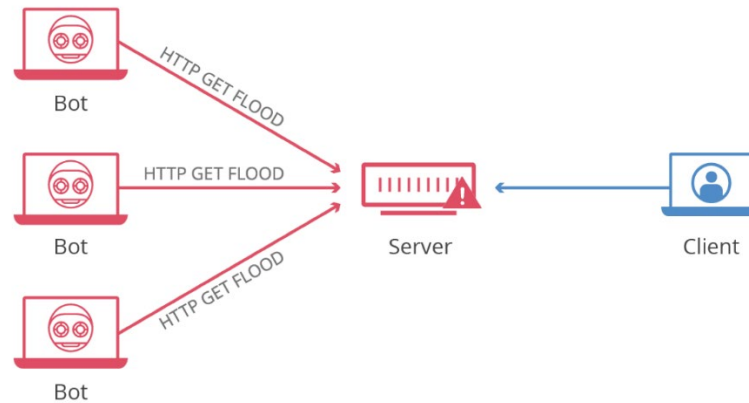


Рисунок 1.7 – Атака типу HTTP Flood

Ці запити можуть бути спрямовані на завантаження великих файлів, виконання складних пошукових запитів або доступ до ресурсомістких сторінок. Іншим прикладом є атака Slowloris, при якій зломисник встановлює велику кількість HTTP-з'єднань з сервером і підтримує їх відкритими якомога довше, надсилаючи неповні заголовки запитів [14] (див. рисунок 1.8).

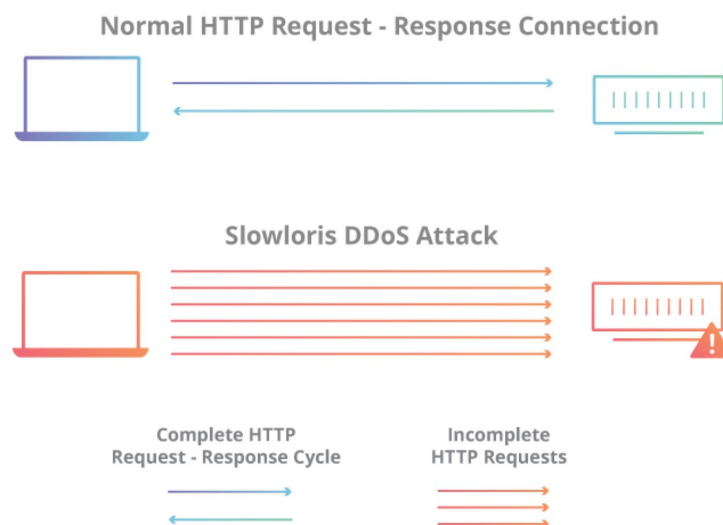


Рисунок 1.8 – Атака типу Slowloris

Це призводить до вичерпання доступних з'єднань і недоступності сервісу для інших користувачів. Атака RUDY (R-U-Dead-Yet) використовує повільні HTTP POST-запити з великим тілом, надсилаючи дані дуже повільно [15]. Сервер тримає з'єднання відкритим, очікуючи завершення передачі, що призводить до вичерпання ресурсів. DNS Flood – це тип атаки, при якій зловмисник намагається перевантажити сервер DNS великою кількістю запитів [16] (див. рисунок 1.9).

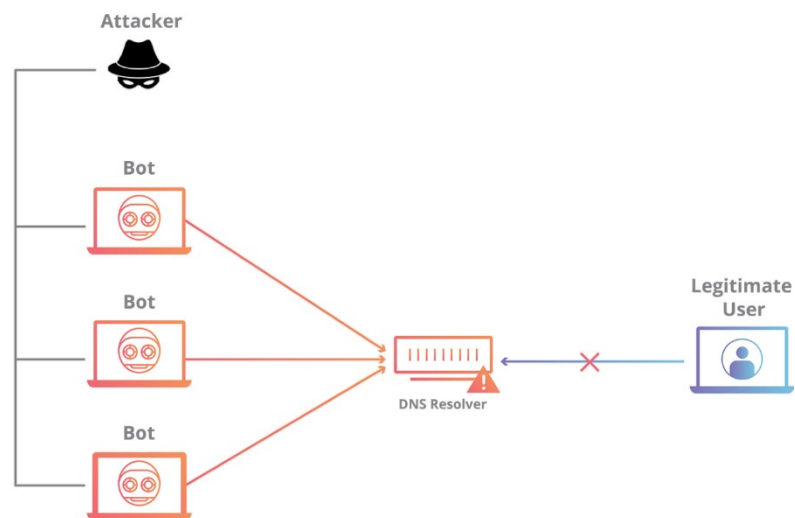


Рисунок 1.9 – Атака типу DNS Flood

Метою є вичерпання ресурсів сервера, що спричиняє його уповільнення або повну недоступність. Зловмисник може використовувати ботнет, що складається з великої кількості скомпрометованих пристроїв, для генерування масивного трафіку запитів. DNS Amplification – це вид DDoS атаки, при якій зловмисник використовує сервери DNS для підсилення трафіку [17] (див. рисунок 1.10).

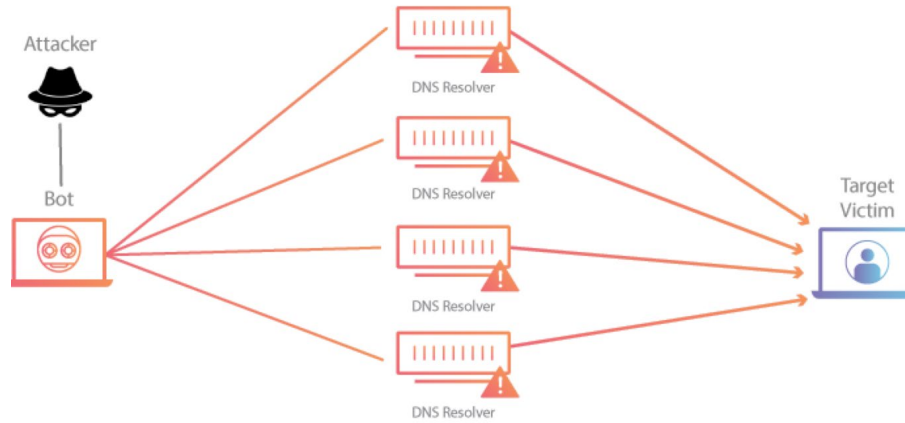


Рисунок 1.10 – Атака типу DNS Amplification

Механізм полягає в тому, що зловмисник надсилає DNS-запити до відкритих DNS із підробленою IP-адресою жертви. Сервери DNS відповідають на запити, надсилаючи великі обсяги даних на IP-адресу жертви, що перевищує обсяг початкового запиту. Це підсилює потік даних, і сервер жертви отримує значний обсяг трафіку, що призводить до перевантаження та відмови в обслуговуванні. Цей тип атаки також стосується прикладного рівня, адже використовує можливості протоколу DNS для створення посиленого навантаження. NTP Amplification – подібна атака, що використовує протокол NTP для підсилення трафіку [18] (див. рисунок 1.11).

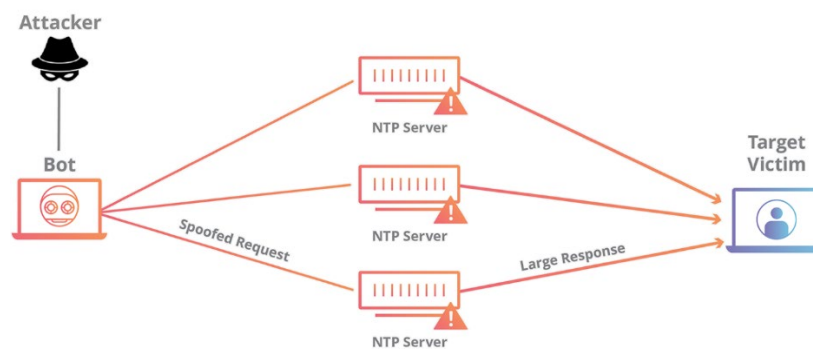


Рисунок 1.11 – Атака типу NTP Amplification

Зловмисник надсилає запити до серверів NTP, використовуючи команду monlist, яка повертає список останніх клієнтів, що зверталися до сервера. Ці запити надсилаються з підробленою IP-адресою жертви, і відповіді сервера NTP, які значно більші за розміром від початкового запиту, надходять до жертви. Як і

у випадку з DNS Amplification, це призводить до перевантаження цільової системи. Атака NTP Amplification також діє на прикладному рівні OSI, використовуючи специфіку протоколу NTP для створення об'ємного трафіку.

Використання ботнетів для здійснення DDoS-атак є поширеною та небезпечною практикою в кіберзлочинному середовищі [19]. Ботнет — це мережа скомпрометованих пристроїв, відомих як "боти", які зловмисник контролює дистанційно. Ці пристрої можуть включати комп'ютери, сервери, IoT-пристрої, такі як камери спостереження. Власники цих пристроїв часто навіть не підозрюють, що їхні пристрої використовуються для шкідливої діяльності.

Зловмисник, контролюючи ботнет, може одночасно активувати тисячі або навіть мільйони ботів для надсилання величезного обсягу трафіку на цільову систему або мережу. Це перевантажує ресурси жертви, спричиняючи збої, уповільнення роботи або повну відмову в обслуговуванні. Сила ботнету полягає в його розподіленій природі: трафік надходить із різних IP-адрес, що ускладнює його фільтрацію та блокування (див. рисунок 1.12).

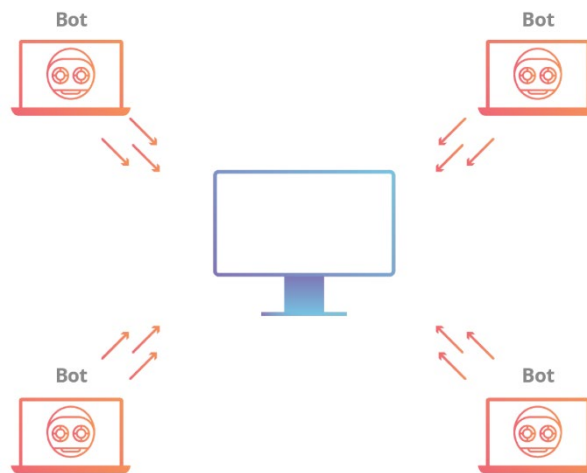


Рисунок 1.12 – Принцип використання ботнет мережі

Для створення ботнетів зловмисники використовують різні методи. Одним із найпоширеніших є розповсюдження шкідливого програмного забезпечення, яке інфікує пристрої, використовуючи вразливості в програмному забезпеченні або соціальну інженерію. Після встановлення шкідливого ПЗ надає зловмиснику можливість дистанційного контролю над зараженим пристроєм.

Використовуючи централізоване керування через командний центр CnC (див. рисунок 1.13) або децентралізовані P2P-мережі (див. рисунок 1.14), зловмисники можуть одночасно командувати великою кількістю пристроїв.

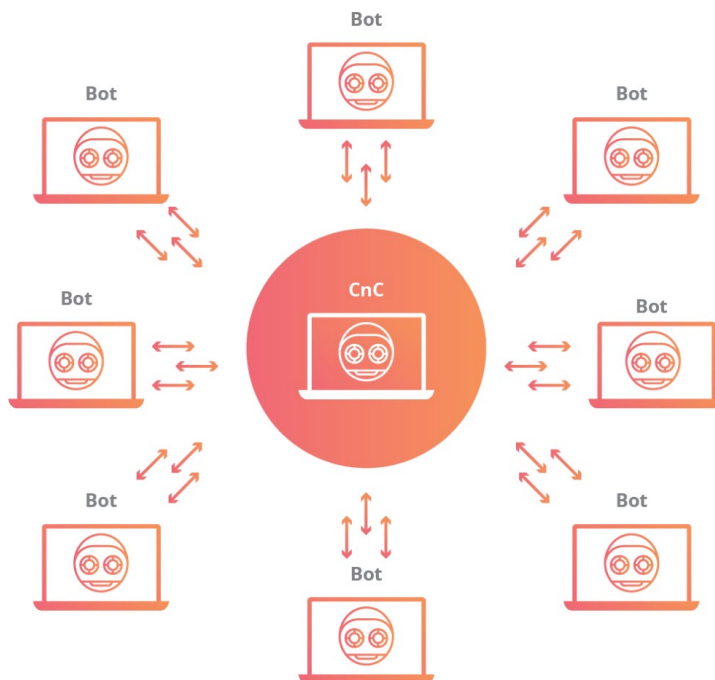


Рисунок 1.13 – Ботнет мережа типу CnC

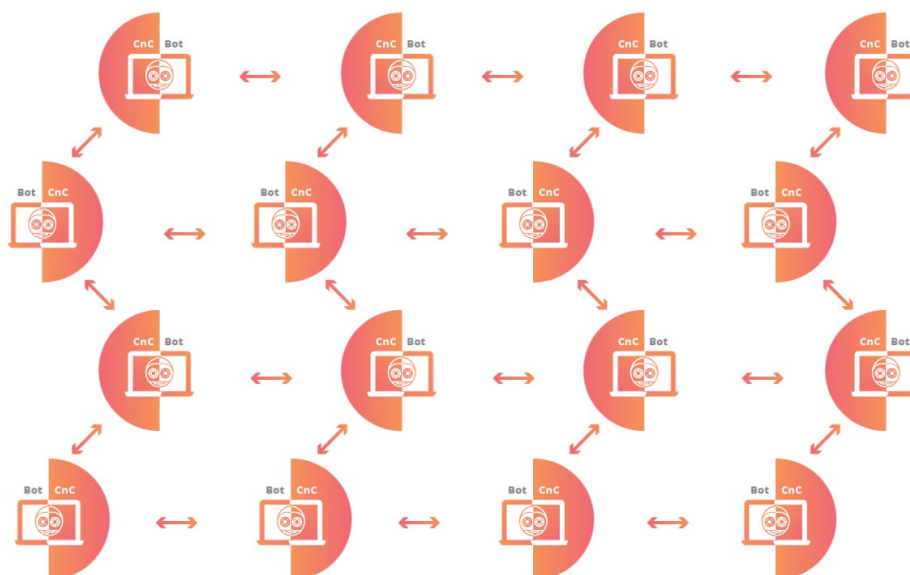


Рисунок 1.14 – Ботнет мережа типу P2P

Зазвичай DDoS-атаки з використанням ботнетів спрямовані на виведення з ладу веб-сайтів, серверів або мережевих інфраструктур великих компаній,

банків, урядових організацій або інших важливих установ. Мета таких атак може варіюватися від вимагання викупу (загроза продовження атаки до сплати певної суми) до політичних чи ідеологічних мотивів, а також конкурентних війн. Відомі випадки, коли ботнети використовувалися для здійснення атак на критичну інфраструктуру, що призводило до серйозних наслідків. Ботнети можуть складатися не лише з традиційних комп'ютерів, а й з численних пристроїв IoT. Зловмисники часто націлюються на такі пристрої через їх слабку безпеку: відсутність оновлень, слабкі або стандартні паролі та обмежені функції захисту. Масштабні ботнети, такі як Mirai, демонстрували, що навіть звичайні IoT-пристрої можуть бути об'єднані в потужні мережі для масових DDoS-атак, що досягають обсягів у сотні гігабіт на секунду.

Використання ботнетів робить DDoS-атаки більш ефективними та небезпечними, оскільки вони дозволяють значно збільшити обсяг трафіку та тривалість атаки.

1.1.2 Атаки на конфіденційність

Атаки на конфіденційність передбачають несанкціонований доступ до інформації. До них відносяться фішингові кампанії, перехоплення трафіку (атака MITM) [20], а також крадіжка облікових даних. Зловмисники можуть використовувати соціальну інженерію, щоб обманом отримати необхідну інформацію від користувачів.

Одним із найпоширеніших методів атак на конфіденційність є фішинг. Фішинг - це форма соціальної інженерії, при якій зловмисники видають себе за довірених осіб або організації, щоб обманом отримати конфіденційну інформацію, таку як паролі, номери кредитних карток або інші особисті дані. Зазвичай фішингові атаки здійснюються через електронну пошту, але можуть використовуватися й інші канали, такі як SMS або соціальні мережі. Зловмисник надсилає повідомлення, яке виглядає як офіційне звернення від відомої організації, наприклад, банку або популярного онлайн-сервісу. У повідомленні міститься посилання на підроблений веб-сайт, який візуально схожий на

справжній. Користувач, перейшовши за посиланням, вводить свої облікові дані, які потім потрапляють до зловмисника. Для захисту від фішингових атак рекомендується бути обережними з електронними листами від невідомих відправників або з підозрілим змістом, перевіряти URL-адреси перед введенням особистої інформації та використовувати багатофакторну аутентифікацію для додаткового захисту облікових записів. Шкідливе програмне забезпечення (Malware) також становить значну загрозу для конфіденційності [21]. Шкідливе ПЗ - це програми, розроблені для виконання зловмисних дій на комп'ютері жертви. Деякі види шкідливого ПЗ, такі як клавіатурні шпигуни (keyloggers) або трояни, спеціально створені для збору конфіденційної інформації. Шкідливе ПЗ може потрапити на комп'ютер через заражені вкладення в електронних листах, завантаження з ненадійних джерел або через вразливості в програмному забезпеченні. Після встановлення воно може записувати натискання клавіш, робити знімки екрану або передавати файли з комп'ютера жертви на сервер зловмисника. Для захисту від шкідливого ПЗ рекомендується встановлювати та регулярно оновлювати антивірусне програмне забезпечення, не відкривати підозрілі вкладення та не завантажувати файли з ненадійних джерел, а також оновлювати операційну систему та інше програмне забезпечення для усунення відомих вразливостей. Атаки типу MITM є ще одним методом порушення конфіденційності [20]. У таких атаках зловмисник перехоплює та, комунікацію між двома сторонами без їх відома. Це дозволяє отримати доступ до конфіденційної інформації, такої як облікові дані або фінансові дані. Зловмисник може використовувати підроблені Wi-Fi точки доступу або експлуатувати вразливості в мережевих протоколах для перехоплення трафіку. Наприклад, у публічних мережах Wi-Fi без шифрування зловмисник може легко перехоплювати незашифровані дані, що передаються між користувачем та веб-сайтом. Для захисту від таких атак рекомендується використовувати VPN при підключенні до публічних мереж Wi-Fi, переконуватися, що веб-сайти використовують HTTPS для шифрування трафіку, та уникати підключення до незахищених або підозрілих Wi-Fi мереж. Соціальна інженерія - це методи маніпуляції людьми з метою отримання конфіденційної інформації.

Зловмисники використовують психологічні прийоми, щоб змусити жертву розкрити паролі, фінансові дані або іншу чутливу інформацію. Зловмисник може зателефонувати, представившись співробітником технічної підтримки, та попросити надати пароль для вирішення "проблеми". Інший приклад - залишення зараженого USB-накопичувача в публічному місці з надією, що хтось підключить його до свого комп'ютера. Для захисту від таких атак рекомендується бути обережними з незнайомими людьми, які просять надати конфіденційну інформацію, навчати співробітників розпізнавати та реагувати на спроби соціальної інженерії, а також встановлювати чіткі політики безпеки щодо обробки конфіденційної інформації.

Приклади атак на конфіденційність включають SQL-ін'єкції [22], експлуатацію вразливості сервісів, перехоплення незашифрованих паролів, brute-force атаки [23].

1.1.3 Атаки на цілісність

Атаки на цілісність даних спрямовані на зміну, спотворення або знищення інформації, що може призвести до серйозних наслідків для користувачів та організацій. Одним із основних методів таких атак є впровадження шкідливого програмного забезпечення, яке може змінювати або пошкоджувати дані без відома власника. Віруси, троянські програми та інші види шкідливого ПЗ часто використовуються для реалізації атак, спрямованих на порушення цілісності інформації. Вони можуть бути розроблені для видалення файлів, внесення змін до документів або знищення важливих даних на комп'ютері жертви. Особливу загрозу становлять програми-вимагачі (ransomware), які шифрують дані на комп'ютері користувача та вимагають викуп за їх відновлення. Програми-вимагачі зазвичай проникають у системи через фішингові електронні листи, шкідливі веб-сайти або вразливості в програмному забезпеченні. Після шифрування даних користувач втрачає доступ до важливої інформації, і єдиним способом відновлення стає сплата викупу, що часто не гарантує повернення доступу. Відомі випадки, коли великі компанії та установи зазнавали значних

втрат через атаки програм-вимагачів, змушені були зупиняти свою роботу та відновлювати системи з резервних копій. Ще одним прикладом атак на цілісність є атаки з використанням програмних закладок (backdoors) або руткітів, які дозволяють зловмисникам отримувати прихований доступ до системи та вносити зміни в дані або конфігурацію системи без відома користувача. Такий доступ дає змогу зловмисникам поступово модифікувати дані, залишаючи їхню діяльність непомітною тривалий час. Соціальна інженерія також може використовуватися для атак на цілісність. Зловмисники, використовуючи психологічні методи впливу, можуть переконати користувача або співробітника організації внести зміни до важливих файлів або баз даних під виглядом офіційного запиту.

1.2 Наслідки атак

Атаки на доступність можуть мати серйозні наслідки для організацій, бізнесу та користувачів, оскільки вони спрямовані на порушення нормальної роботи систем і сервісів, що призводить до збоїв або повної недоступності послуг. Наслідки таких атак включають фінансові втрати, погіршення репутації, зниження рівня обслуговування клієнтів та додаткові витрати на відновлення інфраструктури та впровадження заходів безпеки.

Фінансові втрати від атак на доступність можуть бути значними, особливо для великих компаній та інтернет-платформ, які залежать від безперебійної роботи своїх онлайн-сервісів. Наприклад, тривала DDoS-атака може призвести до втрати доходу від продажів, збоїв у роботі електронної комерції та зриву бізнес-процесів. Для фінансових установ збої у роботі можуть означати переривання банківських операцій, що, у свою чергу, підриває довіру клієнтів і може призвести до відтоку користувачів.

Погіршення репутації також є одним із ключових наслідків атак на доступність. Якщо компанія не здатна забезпечити безперебійну роботу своїх сервісів або не має адекватних заходів захисту, це може призвести до втрати довіри клієнтів та партнерів. У конкурентному середовищі, де надійність є

критичною, навіть один випадок тривалої недоступності може мати тривалі наслідки для іміджу компанії.

Атаки на доступність можуть також призвести до значного збільшення операційних витрат. Організації змушені витрачати ресурси на усунення наслідків атаки, залучення спеціалістів із кібербезпеки, відновлення інфраструктури та впровадження нових заходів безпеки для запобігання подібним інцидентам у майбутньому. Це включає оновлення програмного забезпечення, закупівлю обладнання, яке може протидіяти атакам, та навчання персоналу.

Для державних установ і критичної інфраструктури атаки на доступність можуть призвести до набагато серйозніших наслідків. Наприклад, атаки на енергетичні системи, транспортні мережі або системи охорони здоров'я можуть порушити нормальну роботу цих секторів, що створює ризик для громадської безпеки. Недоступність систем може призвести до затримок у наданні медичних послуг, перебоїв у постачанні електроенергії або транспортного колапсу.

Крім цього, атаки на доступність можуть бути використані як відволікаючий маневр для проведення інших, більш небезпечних атак, таких як крадіжка даних або впровадження шкідливого програмного забезпечення. Поки організація займається відновленням роботи та протидією атаці, зловмисники можуть отримати доступ до конфіденційної інформації або впровадити троянські програми, які залишатимуться непоміченими. Наслідки атак на доступність можуть варіюватися від тимчасових незручностей до серйозних економічних і соціальних проблем, залежно від масштабу атаки та характеру постраждалої організації чи системи.

Атаки на конфіденційність мають широкий спектр негативних наслідків для фізичних осіб, бізнесу та державних установ. Вони спрямовані на несанкціонований доступ до чутливої інформації, її розголошення або використання зловмисниками. Наслідки таких атак можуть бути серйозними і мати довгострокові наслідки.

Перш за все, порушення конфіденційності може призвести до фінансових втрат. Якщо зловмисники отримують доступ до банківських рахунків, платіжних

даних або фінансової інформації, вони можуть здійснити шахрайські транзакції, що призводить до прямих збитків для жертви. У випадку бізнесу такі атаки можуть включати крадіжку комерційної інформації, зокрема фінансових звітів, планів розвитку чи секретних контрактів, що може поставити компанію в не вигідне конкурентне становище. Порухення конфіденційності часто супроводжується значним ударом по репутації. Для компаній та організацій витік даних може означати втрату довіри клієнтів та партнерів, оскільки люди стають обережнішими у взаємодії з організацією, яка не змогла забезпечити захист даних. Репутаційні втрати можуть вплинути на довгострокові партнерські відносини, призвести до зниження продажів і навіть відтоку клієнтів до конкурентів. Крім того, атаки на конфіденційність можуть створювати юридичні проблеми для компаній. У багатьох країнах існують суворі регуляційні правила щодо захисту даних, і витік конфіденційної інформації може призвести до штрафів та інших юридичних санкцій. Атаки на конфіденційність також можуть призвести до психологічних та емоційних наслідків для постраждалих. Коли йдеться про особисті дані, такі як медична історія, особисті листування або приватні фотографії, їх розголошення може завдати значної моральної шкоди та стресу. У випадку державних установ і агентств атаки на конфіденційність можуть мати ще серйозніші наслідки, оскільки вони можуть включати доступ до секретної інформації, що стосується національної безпеки, оборонних стратегій або дипломатичних переговорів. Розголошення таких даних може підірвати довіру до уряду, поставити під загрозу безпеку країни та викликати політичні кризи. Витоки даних також можуть використовуватись зловмисниками для подальших атак. Наприклад, інформація, отримана під час першого порушення конфіденційності, може використовуватись для фішингових атак, соціальної інженерії або шантажу. Отримані дані дозволяють зловмисникам більш точно націлювати свої атаки та створювати складніші схеми обману.

Наслідки атак на конфіденційність виходять за межі негайних збитків та включають довготривалі проблеми, які можуть вимагати значних зусиль для їх подолання.

Атаки на цілісність даних можуть мати далекосяжні та серйозні наслідки для організацій, державних установ, підприємств та окремих осіб. Цілісність даних означає, що інформація залишається незмінною та точною під час її зберігання, обробки чи передачі. Коли зловмисники здійснюють атаки на цілісність, вони змінюють, підробляють або видаляють дані, що може призвести до серйозних проблем, зокрема в критично важливих системах. Одним із найпомітніших наслідків атак на цілісність є спотворення інформації, яка використовується для прийняття рішень. У випадку підприємств, зміна даних у фінансових звітах, планах розвитку чи інших критичних документах може призвести до неправильних управлінських рішень, які вплинуть на стабільність та прибутковість компанії. Використання спотвореної інформації може завдати шкоди стратегіям розвитку та знищити конкурентні переваги, створюючи серйозні фінансові та репутаційні проблеми.

Для державних установ атаки на цілісність можуть призвести до спотворення або знищення інформації, яка використовується для забезпечення громадського порядку, управління кризовими ситуаціями або інших державних функцій. Наприклад, атака на бази даних, які зберігають інформацію про громадян чи планування оборонних стратегій, може призвести до серйозних національних криз і навіть загрози національній безпеці.

У сфері охорони здоров'я атаки на цілісність даних можуть мати катастрофічні наслідки. Зміна медичних записів може призвести до неправильного діагнозу або лікування пацієнтів, що може спричинити шкоду їхньому здоров'ю або навіть призвести до летальних випадків. Зловмисники, які змінюють або видаляють дані про медичні процедури чи рецепти, створюють серйозну загрозу для медичних установ та їхніх пацієнтів.

Важливим аспектом є також порушення довіри клієнтів та партнерів. Організації, які зазнають атак на цілісність, можуть втратити довіру своїх клієнтів, оскільки останні почнуть сумніватися у точності та достовірності інформації, що надається компанією. Це особливо важливо у фінансовому секторі, де довіра клієнтів до точності інформації є основою стабільності бізнесу.

Втрата довіри може призвести до масового відтоку клієнтів, падіння акцій компанії та зниження її ринкової вартості.

Атаки на цілісність також можуть використовуватися зловмисниками для створення хаосу або саботажу. Наприклад, у промислових системах зловмисники можуть змінювати дані про контроль процесів, що призводить до порушень у виробничих процесах, аварій або пошкодження обладнання. Це створює не лише фінансові збитки, а й загрозу для безпеки працівників та навколишнього середовища. Зміна даних у логістичних системах може призвести до дезорганізації ланцюгів постачання, що вплине на своєчасну доставку товарів і послуг. Це, у свою чергу, знижує рівень обслуговування клієнтів та призводить до втрат доходу.

Відновлення після атак на цілісність може бути надзвичайно складним процесом. Організації повинні ретельно перевіряти резервні копії, щоб переконатися в їхній точності, та здійснювати відновлення даних із надійних джерел. Це вимагає значних фінансових і часових ресурсів, а також залучення експертів з кібербезпеки для аналізу інциденту, виявлення слабких місць та впровадження заходів для запобігання майбутнім атакам.

Атаки на цілісність також мають далекосяжні наслідки, що охоплюють фінансові втрати, втрату довіри клієнтів, юридичні проблеми, фізичну небезпеку для людей та збитки для навколишнього середовища.

1.3 Огляд існуючих підходів до захисту від атак

Захист від атак є багатошаровим процесом, що поєднує організаційні, технічні та адміністративні заходи для забезпечення стійкості систем до зловмисних дій.

Одним із найважливіших підходів є використання брандмауерів [24] та систем виявлення та запобігання вторгненням (IDS/IPS). Брандмауери забезпечують фільтрацію трафіку, блокуючи підозрілі пакети, які можуть бути частиною атаки. IDS/IPS системи дозволяють виявляти підозрілі дії в мережі та автоматично реагувати на них, щоб запобігти потенційним загрозам [26,27].

Шифрування даних є одним із найефективніших способів захисту конфіденційної інформації. Використання сучасних криптографічних алгоритмів дозволяє забезпечити захист даних під час їх передачі та зберігання. Це унеможливлює доступ до даних для зломисників навіть у разі перехоплення інформації або несанкціонованого доступу до системи.

Аутентифікація та контроль доступу є важливими елементами захисту від атак. Впровадження багатофакторної аутентифікації (MFA) значно підвищує рівень безпеки, оскільки вимагає використання кількох способів підтвердження особи користувача. Системи контролю доступу обмежують можливості користувачів у межах їхніх прав і дозволяють запобігти несанкціонованому доступу до критичних систем.

Оновлення та патчі програмного забезпечення є ключовими для забезпечення безпеки, оскільки вони дозволяють усунути відомі вразливості, які можуть бути використані зломисниками для проникнення в систему. Регулярне оновлення систем та програм зменшує ризик атак, спрямованих на експлуатацію відомих недоліків у ПЗ.

Навчання та підвищення обізнаності користувачів є важливим елементом захисту від соціальної інженерії та фішингових атак. Працівники організацій повинні бути обізнані про можливі загрози та навчатися правильно реагувати на підозрілі дії, такі як фішингові листи чи спроби обману через телефонні дзвінки.

Системи резервного копіювання дозволяють захиститися від атак, таких як програми-вимагачі (ransomware). Регулярне створення резервних копій важливих даних і збереження їх у захищених середовищах допомагає швидко відновити інформацію у разі її пошкодження або втрати.

Моніторинг та аналіз трафіку у реальному часі дозволяють виявляти аномальні дії, які можуть свідчити про початок атаки. Використання систем моніторингу та аналізу мережевої активності допомагає запобігти атакам на ранніх стадіях і мінімізувати їх вплив на систему.

Сегментація мережі також є важливим підходом до захисту. Розділення мережі на ізольовані сегменти обмежує можливість поширення атаки в межах

організації. Це дозволяє захистити критично важливі ресурси навіть у разі компрометації окремих ділянок мережі.

Антивірусне програмне забезпечення та інші засоби захисту від шкідливого ПЗ допомагають виявляти та видаляти шкідливі програми, які можуть бути використані для атак на конфіденційність, цілісність і доступність даних.

Хмарні рішення для захисту від DDoS-атак дозволяють розподілити навантаження та забезпечити стійкість до об'ємних атак. Використання захищених хмарних платформ із вбудованими засобами безпеки може допомогти організаціям забезпечити безперебійну роботу навіть у разі великих мережесих атак.

Як вже було сказано вище IDS є важливим елементом сучасної стратегії кібербезпеки, оскільки дозволяють виявляти та аналізувати потенційно шкідливу активність у мережах та на пристроях. Основна функція IDS — моніторинг трафіку, виявлення підозрілих дій і попередження адміністраторів про можливі вторгнення, щоб запобігти або мінімізувати шкоду від атак.

IDS можуть бути двох основних типів: мережева системи виявлення вторгнень (NIDS) і системи виявлення вторгнень на основі хоста (HIDS). NIDS розміщуються на критичних точках мережі для аналізу трафіку, що проходить через них, виявлення аномалій або шаблонів атак і попередження про них. HIDS працюють безпосередньо на кінцевих пристроях, аналізуючи журнали системних подій, файли та інші ознаки несанкціонованих дій [25].

На рисунку 1.15 показано схему розташування NIDS.

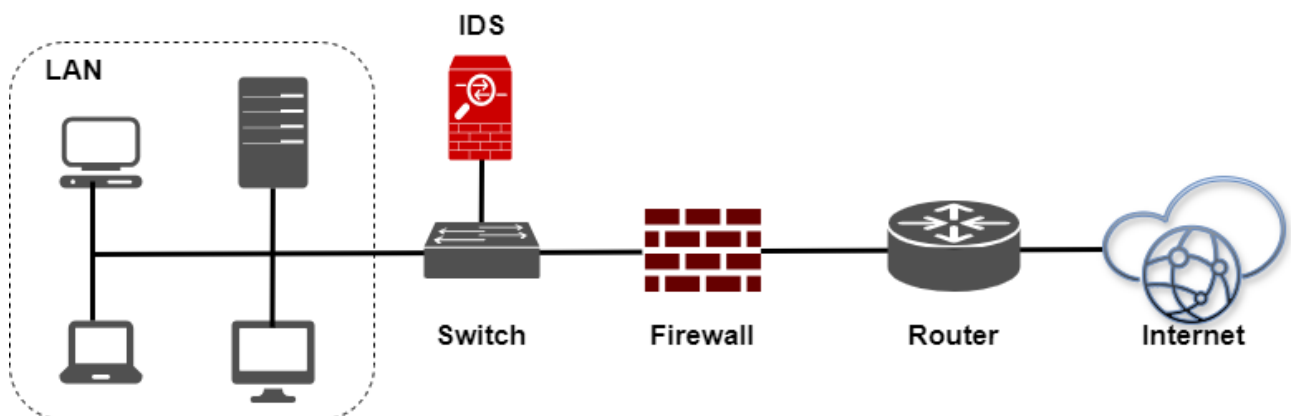


Рисунок 1.15 – Схема розташування NIDS

Одним із головних підходів до роботи IDS є використання сигнатурного аналізу, при якому система порівнює мережевий трафік або дії з базою даних відомих сигнатур атак. Якщо знайдено збіг, система попереджає про потенційну загрозу. Такий підхід дозволяє ефективно виявляти відомі атаки, але може бути менш ефективним проти нових або модифікованих загроз, для яких ще не існує сигнатур.

Іншим підходом є аналіз поведінки або аномалій. IDS з використанням цього методу навчаються на основі звичайного, очікуваного рівня активності та сигналізують, коли виявляють відхилення від цієї норми. Такий підхід є корисним для виявлення нових або складних атак, які не мають характерних сигнатур. Проте він може генерувати більше хибнопозитивних спрацювань, що вимагає додаткового аналізу та налаштування.

Використання IDS забезпечує ряд переваг. IDS дозволяють оперативно виявляти вторгнення та реагувати на них, що допомагає запобігти поширенню загрози та зменшити потенційну шкоду. Вони також надають докладні журнали подій і дій, що можуть бути використані для подальшого аналізу та вдосконалення політик безпеки. Це особливо важливо для проведення розслідувань та збору доказів у разі інцидентів безпеки.

IDS є важливим компонентом загальної архітектури безпеки, який допомагає організаціям залишатися обізнаними про події в мережі та на кінцевих пристроях. Їх використання в поєднанні з іншими засобами захисту, такими як брандмауери, антивірусне програмне забезпечення та системи резервного копіювання, допомагає забезпечити багаторівневий захист від сучасних кіберзагроз.

1.3 Висновки до розділу 1

В першому розділі було розглянуто основні аспекти сучасних кіберзагроз, зокрема класифікацію атак на доступність, конфіденційність та цілісність даних. Детально проаналізовано різні типи атак, їхні механізми та вплив на

інформаційні системи та мережі. Було описано атаки на мережевому, транспортному та прикладному рівнях моделі OSI, серед яких виділяються такі поширені атаки як ICMP Flood, SYN Flood, UDP Flood, DNS та NTP Amplification, а також атаки на конфіденційність і цілісність даних, що включають фішинг, атаки типу "людина посередині", шкідливе програмне забезпечення та програми-вимагачі.

Проведено аналіз наслідків кожного типу атак, які можуть варіюватися від фінансових втрат і репутаційних збитків до серйозних соціальних і національних проблем. Окремо підкреслено важливість захисту даних у різних секторах, зокрема у фінансовій сфері, охороні здоров'я та державних установах, де порушення цілісності та конфіденційності може призвести до катастрофічних наслідків.

Також було зроблено огляд сучасних підходів до захисту від атак, серед яких виділяються використання брандмауерів, систем IDS/IPS, шифрування, багатофакторна аутентифікація, регулярне оновлення програмного забезпечення. Описано важливість навчання персоналу для підвищення обізнаності про загрози та створення ефективної політики безпеки в організації.

РОЗДІЛ 2 СТВОРЕННЯ ТЕСТОВОГО СЕРЕДОВИЩА

2.1 Схема лабораторного тестового середовища

Використання тестового лабораторного середовища для дослідження кіберзагроз та методів захисту є критично важливим для підготовки фахівців до роботи з реальними загрозами. Лабораторні середовища дозволяють моделювати різноманітні сценарії атак у контрольованих умовах, що забезпечує можливість безпечного дослідження поведінки шкідливого програмного забезпечення, аналізу вразливостей та вивчення методів їх експлуатації. Це дозволяє кіберфахівцям розвивати навички та отримувати практичний досвід, що надзвичайно важливо для швидкого виявлення та реагування на загрози у реальних ситуаціях.

Лабораторні середовища надають змогу тестувати та впроваджувати новітні методи захисту, оцінювати їхню ефективність та адаптувати відповідно до конкретних вимог мережі або організації. Такі середовища можуть бути використані для відпрацювання сценаріїв реагування на інциденти та підготовки планів безперервності бізнесу у разі кібератак. Крім того, лабораторні дослідження дозволяють краще розуміти механізми роботи сучасних засобів захисту, таких як системи IDS/IPS, брандмауери та антивірусне програмне забезпечення, шляхом спостереження за їхньою роботою під час атак.

Використання тестових середовищ є також важливим для розробників та інженерів, які створюють нові рішення у сфері кібербезпеки. Це дозволяє виявляти потенційні вразливості на ранніх етапах розробки та мінімізувати ризики перед впровадженням у виробничі середовища. Окрім цього, лабораторні дослідження допомагають навчати співробітників розпізнавати та запобігати кіберзагрозам, створюючи симуляції атак та аналізуючи їхні наслідки.

На рисунку 2.1 показано лабораторне середовище базою якого є гіпервізор KVM.

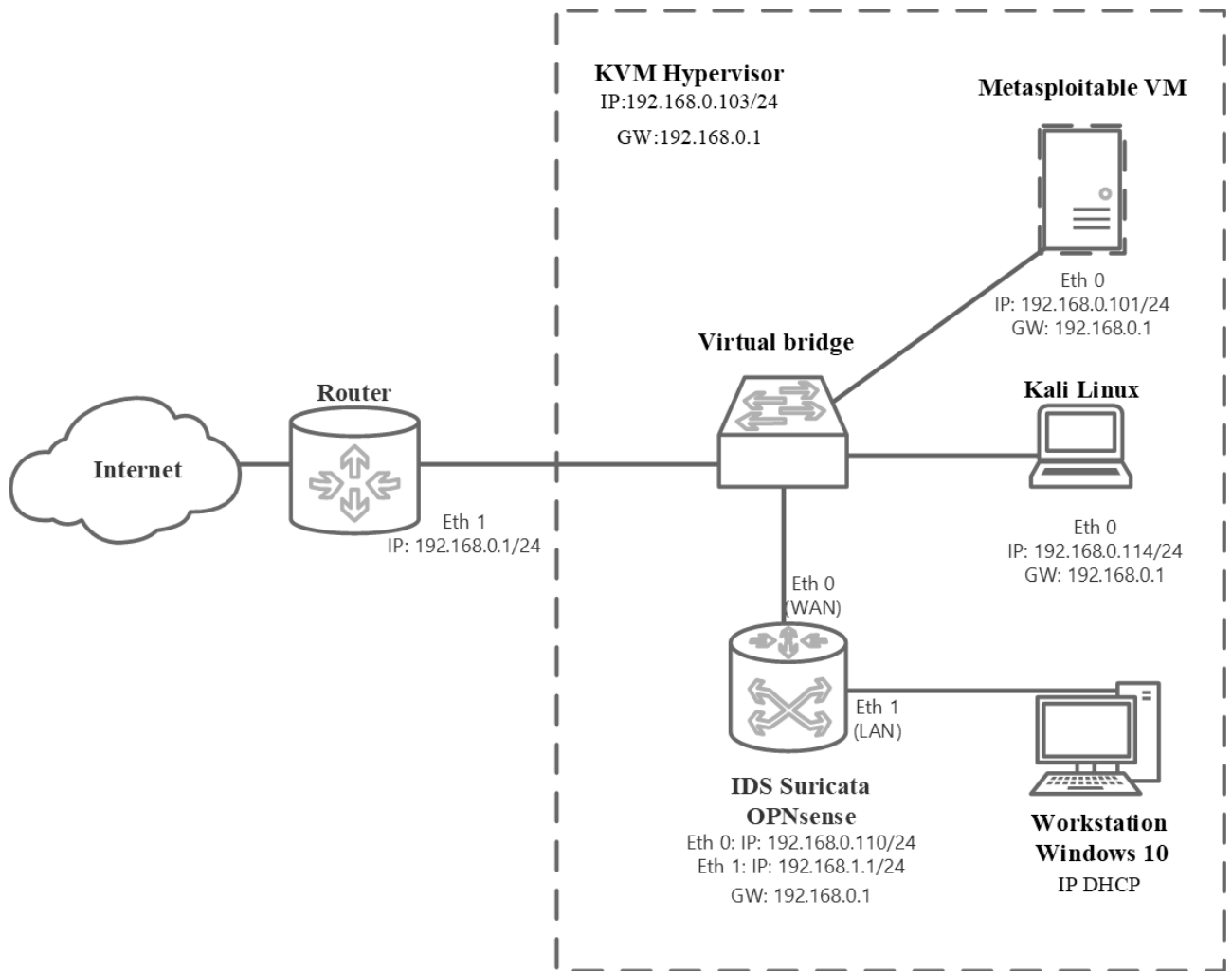


Рисунок 2.1 – Схема тестового лабораторного середовища

Схема тестового лабораторного середовища складається з декількох компонентів для дослідження кіберзагроз та методів захисту. Основним елементом є гіпервізор KVM, який використовується для запуску віртуальних машин, включаючи Metasploitable VM та Kali Linux. Гіпервізор має IP-адресу 192.168.0.103/24.

До віртуального моста підключено IDS Suricata, яка розгорнута на платформі OPNsense. Ця система має два мережеві інтерфейси: Eth 0 (WAN) з IP-адресою 192.168.0.110/24 та Eth 1 (LAN) з IP-адресою 192.168.1.1/24. IDS Suricata використовується для моніторингу мережевого трафіку та виявлення потенційних вторгнень. Також до віртуального моста підключено три віртуальні машини: Metasploitable VM, Kali Linux та робоча станція Windows 10. Metasploitable VM використовується як вразлива система для моделювання різних атак і має IP-адресу 192.168.0.101/24. Kali Linux, яка використовується для

проведення тестувань і атак, має IP-адресу 192.168.0.114/24. Робоча станція Windows 10 отримує IP-адресу через DHCP та використовується для управління IDS в умовах реального користування.

Мережевий маршрутизатор з IP-адресою 192.168.0.1/24 забезпечує зв'язок тестового середовища з інтернетом через інтерфейс Eth 1.

Загальна архітектура тестового середовища забезпечує комплексну інфраструктуру для дослідження різних типів кіберзагроз, включаючи мережеві атаки, атаки на операційні системи та вразливі програми.

2.2 Налаштування компонентів тестового середовища

2.2.1 Гіпервізор KVM

Гіпервізор KVM є одним із найпопулярніших рішень для віртуалізації в середовищі з відкритим вихідним кодом [27]. KVM інтегрується безпосередньо в ядро Linux, що забезпечує високу ефективність, надійність і гнучкість. Він перетворює ядро Linux на повноцінний гіпервізор, який може запускати декілька ізольованих VM, використовуючи ресурси хост-системи. Це робить KVM одним із найкращих рішень для серверної віртуалізації в середовищах на основі Linux.

Основна особливість KVM полягає в тому, що кожна віртуальна машина працює як процес користувача в хостовій операційній системі, використовуючи власний виділений обсяг оперативної пам'яті та процесорних ресурсів. Завдяки такій архітектурі KVM забезпечує високу продуктивність і мінімальне використання системних ресурсів хоста. Окрім цього, KVM підтримує апаратну віртуалізацію, використовуючи технології Intel VT-x і AMD-V, що дозволяє ефективно використовувати апаратні ресурси для прискорення роботи віртуальних машин.

Кожна VM, створена за допомогою KVM, має власну віртуалізовану апаратну інфраструктуру, включаючи процесори, оперативну пам'ять, мережеві інтерфейси та сховища. Це забезпечує можливість запуску на хост-системі різних операційних систем, таких як Linux, Windows та інші. Гіпервізор також

дозволяє створювати та використовувати віртуальні диски для кожної VM, підтримуючи формати образів, як-от qcow2, raw та інші, що надає користувачам гнучкість у налаштуванні та використанні сховищ.

Керування віртуальними машинами на KVM здійснюється за допомогою різних інструментів, зокрема libvirt, яка є бібліотекою для управління віртуалізацією та забезпечує API для інтеграції з іншими програмами, такими як virt-manager, virsh та OpenStack. Virt-manager – це графічний інтерфейс для управління віртуальними машинами, що дозволяє легко створювати, конфігурувати та запускати VM, а virsh – інструмент командного рядка для управління віртуальними машинами, який підходить для скриптування та автоматизації.

KVM забезпечує високу безпеку завдяки можливості використання розширених функцій захисту, таких як sVirt, яка інтегрує SELinux для ізоляції віртуальних машин одна від одної, зменшуючи ризик потенційних атак. Також KVM підтримує функцію живої міграції, яка дозволяє переносити запущені віртуальні машини з одного фізичного хоста на інший без переривання роботи, що є важливою функцією для забезпечення високої доступності та безперервності бізнес-процесів.

На рисунку 2.2 представлено інтерфейс управління гіпервізором KVM, який працює на базі Oracle Linux.

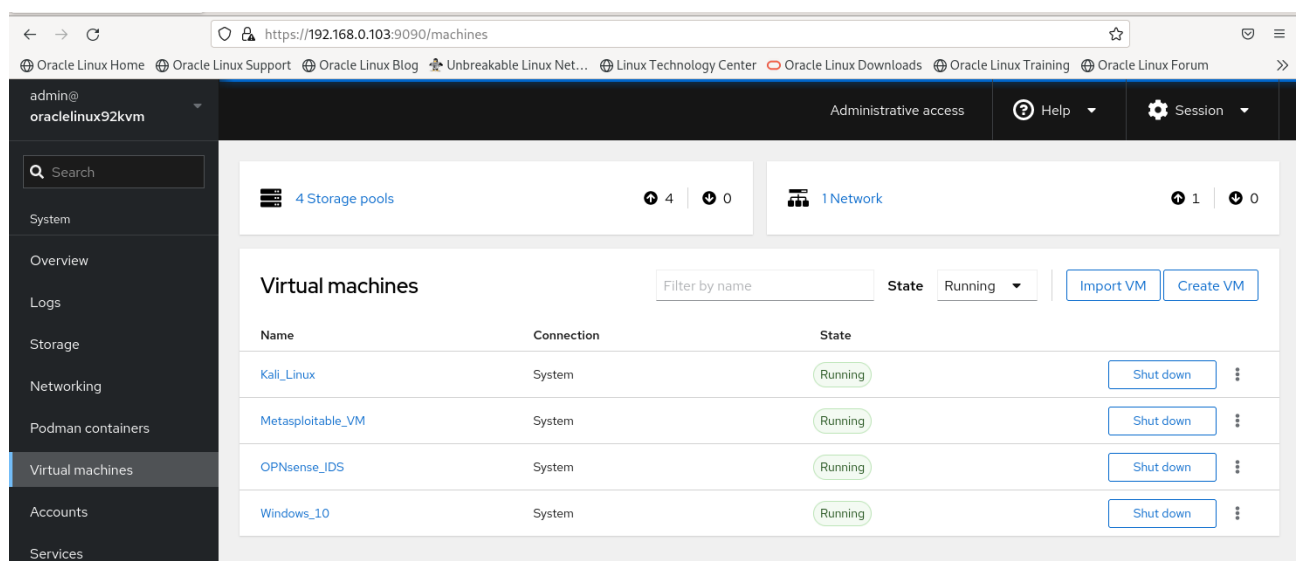


Рисунок 2.2 – Вебінтерфейс керування гіпервізором KVM

Інтерфейс забезпечує просте та ефективне управління віртуалізацією на базі KVM, дозволяючи адміністраторам контролювати віртуальні машини, стежити за їхнім станом, створювати нові та зупиняти роботу існуючих.

2.2.2 Маршрутизатор OPNsense

OPNsense - це операційна система з функціями маршрутизатора та брандмауера, заснована на операційній системі FreeBSD [28]. Вона розроблена як відкрите програмне забезпечення, що дозволяє створювати надійні та безпечні мережеві рішення. OPNsense вирізняється гнучкістю налаштування, широким спектром функцій та зручним інтерфейсом користувача, що дозволяє адміністраторам легко налаштовувати і керувати мережею.

Маршрутизатор OPNsense може виконувати різні функції, включаючи маршрутизацію мережевого трафіку, фільтрацію пакетів, налаштування політик безпеки та управління пропускнуою здатністю. Його основою є ядро FreeBSD, яке забезпечує високу стабільність і надійність роботи, а також підтримку широкого спектру мережевих протоколів і функцій.

OPNsense підтримує сучасні методи забезпечення безпеки, включаючи брандмауер на основі правил, VPN для забезпечення безпечного підключення віддалених користувачів, та систему виявлення вторгнень IDS Suricata. Завдяки цим функціям OPNsense може виявляти підозрілий трафік у реальному часі, повідомляти про можливі загрози.

Однією з основних переваг OPNsense є його інтуїтивно зрозумілий веб-інтерфейс, який надає можливість керувати маршрутизатором через браузер. Інтерфейс включає різноманітні інструменти для моніторингу трафіку, управління користувачами, налаштування VPN та інших функцій. Завдяки цьому адміністратори можуть легко створювати правила для фільтрації трафіку, контролювати активні з'єднання, налаштовувати балансування навантаження і забезпечувати резервування з'єднань для підвищення надійності мережі.

OPNsense підтримує інтеграцію з розширеннями та модулями, що дозволяє адаптувати його до конкретних потреб організації. Це включає налаштування функцій, таких як портал для автентифікації користувачів, підтримка Captive Portal для управління доступом до гостьової мережі, а також налаштування QoS (якість обслуговування) для управління пріоритетами трафіку.

У OPNsense реалізована підтримка VPN-технологій, зокрема IPSec та OpenVPN, що дозволяє організаціям забезпечувати безпечний доступ до внутрішніх ресурсів для віддалених працівників. Це забезпечує конфіденційність і захист даних, що передаються через мережу. Крім того, система має можливість створювати резервні копії конфігурації та автоматизовані оновлення для підтримання актуального стану безпеки.

Інтеграція з системами виявлення вторгнень Suricata дозволяє OPNsense виявляти і реагувати на аномалії у трафіку та потенційні загрози. Suricata підтримує глибокий аналіз пакетів, що дозволяє виявляти складні атаки та порушення безпеки, забезпечуючи захист мережі від широкого спектра загроз, включаючи DDoS-атаки та експлуатацію вразливостей.

OPNsense також підтримує сегментацію мережі завдяки використанню VLAN, що дозволяє розділяти мережевий трафік між різними сегментами для підвищення безпеки та управління трафіком. Ця функція особливо корисна для організацій, що хочуть ізолювати певні частини своєї мережі для запобігання несанкціонованому доступу та потенційним загрозам.

На рисунку 2.3 показано панель управління OPNsense. Панель управління це веб-інтерфейс, до якого можна підключитися за допомогою браузера через IP-адресу 192.168.1.1.

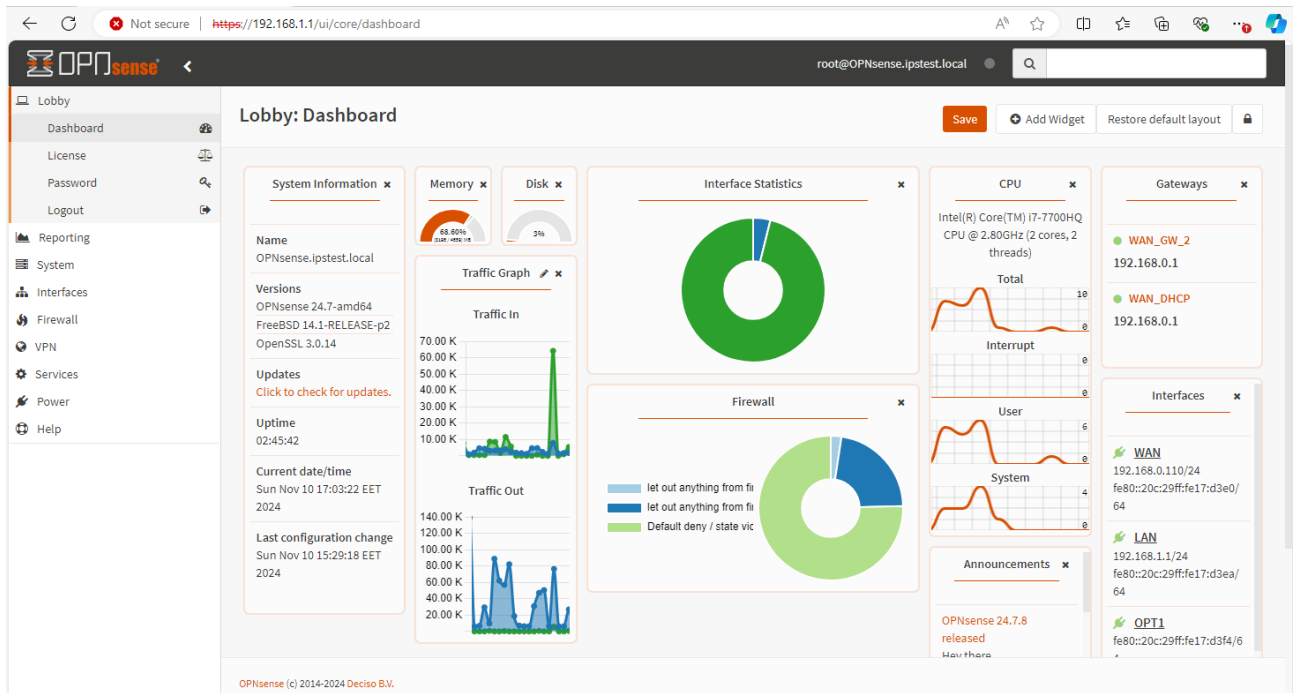


Рисунок 2.3 – Панель адміністрування OPNsense

Головне меню надає доступ до всіх основних функцій та налаштувань системи. Це меню дозволяє адміністраторам швидко перемикатися між різними розділами для управління мережею та конфігурацією брандмауера. Першим розділом є "Lobby", який є головним екраном і включає панель приладів, що надає загальний огляд системи та її стану, використання ресурсів і статистику мережевого трафіку. Розділ "Dashboard" відображає детальний огляд системної інформації та статистики у вигляді віджетів, які адміністратор може налаштовувати відповідно до своїх потреб. Розділ "Reporting" містить звіти та аналітику, пов'язані з мережею та активністю брандмауера, допомагаючи моніторити трафік та роботу системи IDS/IPS. У розділі "System" адміністратори можуть керувати загальними налаштуваннями системи, такими як оновлення, резервне копіювання конфігурацій та управління користувачами. "Interfaces" дозволяє налаштовувати мережеві інтерфейси, змінювати IP-адреси та інші мережеві параметри. У розділі "Firewall" адміністратори створюють та налаштовують правила фільтрації трафіку та керують політиками NAT, що є ключовими аспектами захисту мережі. Розділ "VPN" дозволяє налаштовувати та керувати віртуальними приватними мережами, забезпечуючи безпечний віддалений доступ до мережі. У розділі "Services" адміністратори можуть

керувати додатковими мережевими сервісами, такими як DHCP, DNS, IDS та Captive Portal, що доповнюють функціональність мережевої інфраструктури.

2.2.3 Операційна системи Metasploitable VM

Metasploitable VM версії 2 – це віртуальна машина, створена спеціально для навчання та тестування у сфері кібербезпеки [29]. Вона побудована на базі операційної системи Ubuntu Linux і призначена для використання у контрольованому середовищі. Її основне призначення – бути навчальною платформою для практичних занять з виявлення вразливостей, тестування на проникнення та демонстрації різноманітних кіберзагроз. Ця віртуальна машина містить цілий набір навмисно незахищених або вразливих до експлуатації сервісів і додатків, що дозволяє фахівцям з кібербезпеки навчатися та проводити експерименти без ризику завдання шкоди реальним системам.

Операційна система Metasploitable 2 включає в себе кілька відомих вразливих служб і додатків. Наприклад, на ній зазвичай працюють сервіси, такі як старі версії Apache Tomcat, FTP-сервери, старі версії баз даних MySQL, ненадійні веб-додатки на PHP і інші інструменти, які мають відомі вразливості. Це дозволяє дослідникам використовувати Metasploitable для проведення атак різного рівня складності, включаючи сканування портів, експлуатацію помилок в конфігурації та слабких місць у програмному забезпеченні.

Однією з ключових особливостей Metasploitable 2 є її інтеграція з Metasploit Framework, популярною платформою для тестування на проникнення та розробки експлойтів. Використовуючи Metasploit, фахівці можуть легко запускати експерименти на виявлення та використання вразливостей, перевіряючи, як вони можуть впливати на систему. Ця комбінація дозволяє проводити навчання не тільки на рівні виявлення вразливостей, але й на рівні розробки стратегій захисту та аналізу результатів атак.

Metasploitable 2 також включає веб-додаток під назвою DVWA, який створений для навчання основам веб-безпеки. DVWA містить різні типи вразливостей, включаючи SQL-ін'єкції, XSS (міжсайтовий скриптинг), CSRF

(підробка міжсайтових запитів) та інші [30]. Це дозволяє користувачам вивчати та практикувати методи атак і захисту у веб-середовищі.

Інша популярна вразливість у Metasploitable 2 – це стара версія сервера FTP, яка може бути використана для отримання віддаленого доступу до системи через експлуатацію відомих експлойтів. Крім того, система містить застарілі версії SSH-серверів, які можуть бути піддані атакам, таким як атаки на слабкі паролі та інші методи аутентифікації.

Metasploitable 2 також надає можливість вивчати атаки MITM, аналізувати трафік і тренуватися в використанні мережевих сканерів, таких як Nmap та Wireshark. Ця система є ідеальною для проведення практичних лабораторних занять, де користувачі можуть досліджувати реальні сценарії атак, не завдаючи шкоди продуктивному середовищу.

Mutillidae — це веб-додаток, спеціально створений для навчання та відпрацювання навичок тестування на проникнення, який входить до складу Metasploitable VM версії 2. Він є одним із ключових компонентів, що дозволяють досліджувати та практикувати різні аспекти веб-безпеки. Mutillidae розроблений для того, щоб забезпечити легкий доступ до багатьох поширених веб-вразливостей, що зустрічаються у реальних додатках, і таким чином слугує важливим навчальним інструментом для кібербезпеки.

Mutillidae побудований на основі PHP та працює на веб-сервері, що зазвичай вже налаштований у середовищі Metasploitable 2. Це означає, що користувачі можуть відразу після запуску віртуальної машини почати працювати з цим додатком, не потребуючи додаткових налаштувань.

Mutillidae підтримує безліч вразливостей, які можна використовувати для тренування, таких як SQL-ін'єкції, XSS, CSRF, а також різні атаки, пов'язані з управлінням сесіями та аутентифікацією [31].

Додаток має простий інтерфейс, у якому користувачі можуть обирати різні рівні складності та типи вразливостей для відпрацювання (див. рисунок 2.4).

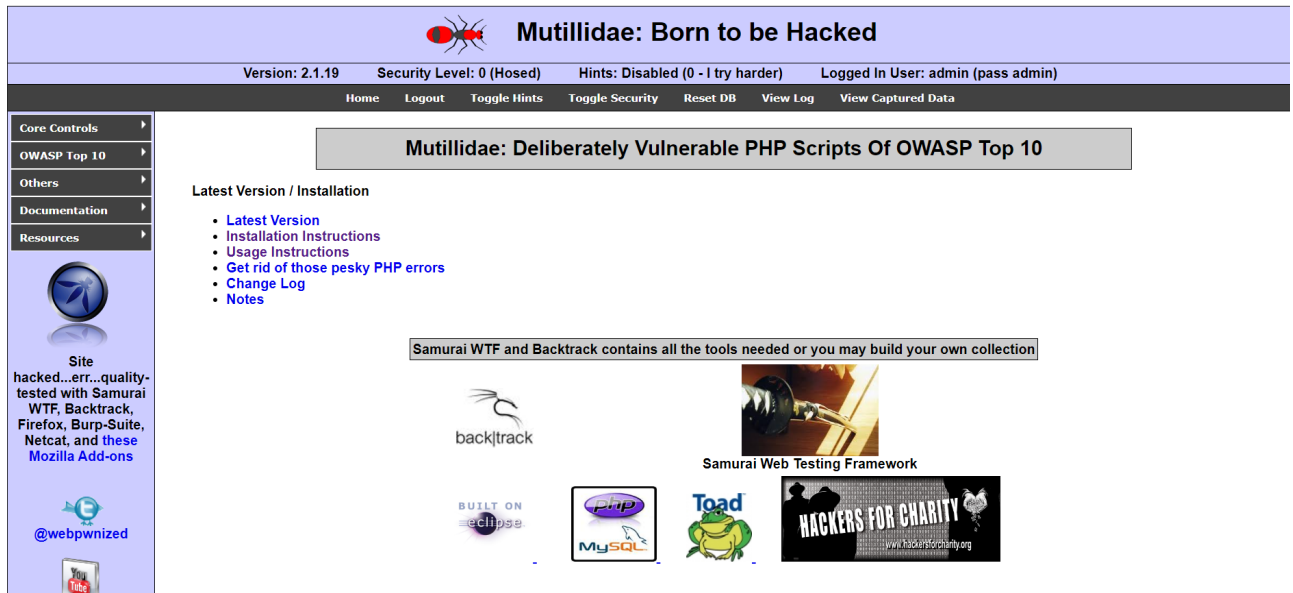


Рисунок 2.4 – Вебінтерфейс керування Mutillidae

Це дозволяє як новачкам, так і досвідченим фахівцям з кібербезпеки поступово підвищувати свої навички, вивчаючи основи атак і переходячи до більш складних сценаріїв. Користувачі можуть вивчати, як знайти та експлуатувати ці вразливості, використовуючи різні інструменти, такі як Burp Suite, OWASP ZAP, або навіть ручне введення кодів у поля вводу, щоб зрозуміти, як відбувається експлуатація вразливостей.

Mutillidae також має освітню функцію, оскільки кожна вразливість забезпечена поясненням, що вона собою являє та як її можна експлуатувати. Після проведення атаки користувачі можуть вивчати рекомендації щодо захисту, які допомагають зрозуміти, як виправити або запобігти подібним уразливостям у реальних веб-додатках. Це робить Mutillidae не тільки інструментом для атак, але й ресурсом для вивчення методів захисту та зміцнення безпеки веб-додатків.

Однією з ключових вразливостей, які можна досліджувати за допомогою Mutillidae, є SQL-ін'єкції, що дозволяють зловмисникам виконувати довільні SQL-запити до бази даних, отримуючи доступ до конфіденційної інформації або змінюючи дані. Також додаток дозволяє вивчати XSS-атаки, коли зловмисники вставляють шкідливі скрипти у веб-сторінки, що викликаються на стороні клієнта, або CSRF, що дозволяють здійснювати дії від імені користувача без його відома.

Mutillidae є надзвичайно корисним для підготовки фахівців із кібербезпеки, оскільки дозволяє відтворювати реалістичні сценарії атак у безпечному середовищі. Це не тільки допомагає розуміти, як працюють певні вразливості, але й показує важливість належного захисту веб-додатків у реальному світі. За допомогою цього додатку користувачі отримують можливість на практиці перевіряти методи захисту, навчатися розробляти більш безпечний код і використовувати різні інструменти для тестування безпеки.

2.2.4 Операційна система Kali Linux

Kali Linux - це операційна система на основі Debian, спеціально створена для тестування на проникнення та дослідження в сфері інформаційної безпеки [32]. Вона розроблена і підтримується компанією Offensive Security, відомою своєю діяльністю у сфері кібербезпеки та навчанням етичних хакерів. Kali Linux є однією з найбільш популярних платформ для тестування на проникнення завдяки її потужним вбудованим інструментам, гнучкості та широкій підтримці спільноти.

Операційна система містить більше 600 попередньо встановлених інструментів для тестування безпеки, що дозволяє фахівцям проводити аналіз уразливостей, оцінку безпеки, тестування проникнення та дослідження мережових і системних загроз. Інструменти в Kali Linux включають різні категорії, такі як сканування портів, експлуатація вразливостей, аналіз трафіку, тестування веб-додатків, парсинг даних та інші методи перевірки безпеки. Серед найпопулярніших інструментів - Nmap для сканування мереж, Metasploit Framework для створення та використання експлойтів, Burp Suite для тестування безпеки веб-додатків та Aircrack-ng для аналізу та тестування безпеки Wi-Fi мереж.

Однією з особливостей Kali Linux є можливість працювати як з інсталяційною версією, так і з Live-середовищем. Це дозволяє користувачам завантажувати систему з USB-накопичувача або DVD без необхідності встановлення її на жорсткий диск. Це забезпечує гнучкість і зручність

використання для тих, хто бажає проводити тестування безпеки без змін у налаштуваннях основної системи.

Kali Linux підтримує безліч архітектур, включаючи x86, x64 та ARM, що дозволяє запускати систему на різних пристроях, включаючи Raspberry Pi та інші платформи з низьким енергоспоживанням. Це робить систему дуже універсальною і зручною для використання у різних сценаріях, від тестування безпеки корпоративних мереж до дослідження IoT-пристроїв.

Операційна система має інтуїтивно зрозумілий графічний інтерфейс, побудований на базі середовища робочого столу Xfce за замовчуванням, що робить її легкою у використанні, навіть для новачків у сфері кібербезпеки. Однак більш досвідчені користувачі також можуть працювати через командний рядок.

На рисунку 2.5 показано мережеві налаштування та таблицю маршрутизації в операційній системі Kali Linux.

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280
    inet 192.168.0.114 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::ff66:d595:e0f3:ce0c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:be:79:0d txqueuelen 1000 (Ethernet)
    RX packets 169258859 bytes 20684542430 (19.2 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 887799443 bytes 53459867692 (49.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 15068082 bytes 2054580877 (1.9 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15068082 bytes 2054580877 (1.9 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 100 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
```

Рисунок 2.5 – Мережеві налаштування та таблицю маршрутизації в Kali Linux

2.3 Тестування лабораторного середовища

Тестування лабораторного середовища є важливим етапом забезпечення його функціональності, ефективності та безпеки перед початком досліджень і моделювання кіберзагроз. Тестування лабораторного середовища включає перевірку всіх компонентів інфраструктури, налаштування мережевих підключень, функціонування віртуальних машин.

Процес тестування починається з перевірки базових функцій гіпервізора KVM, який повинен забезпечувати стабільну роботу всіх віртуальних машин. Потрібно переконатися, що всі віртуальні машини, включаючи Kali Linux, Metasploitable VM та OPNsense, правильно налаштовані, мають коректні мережеві параметри і взаємодіють між собою через віртуальні інтерфейси.

Важливим етапом є тестування внутрішніх мережевих зв'язків між компонентами середовища.

На рисунку 2.6 показано результати сканування мережі за допомогою Zenmap, графічної оболонки для популярного мережевого сканера Nmap з операційної системи Windows 10.

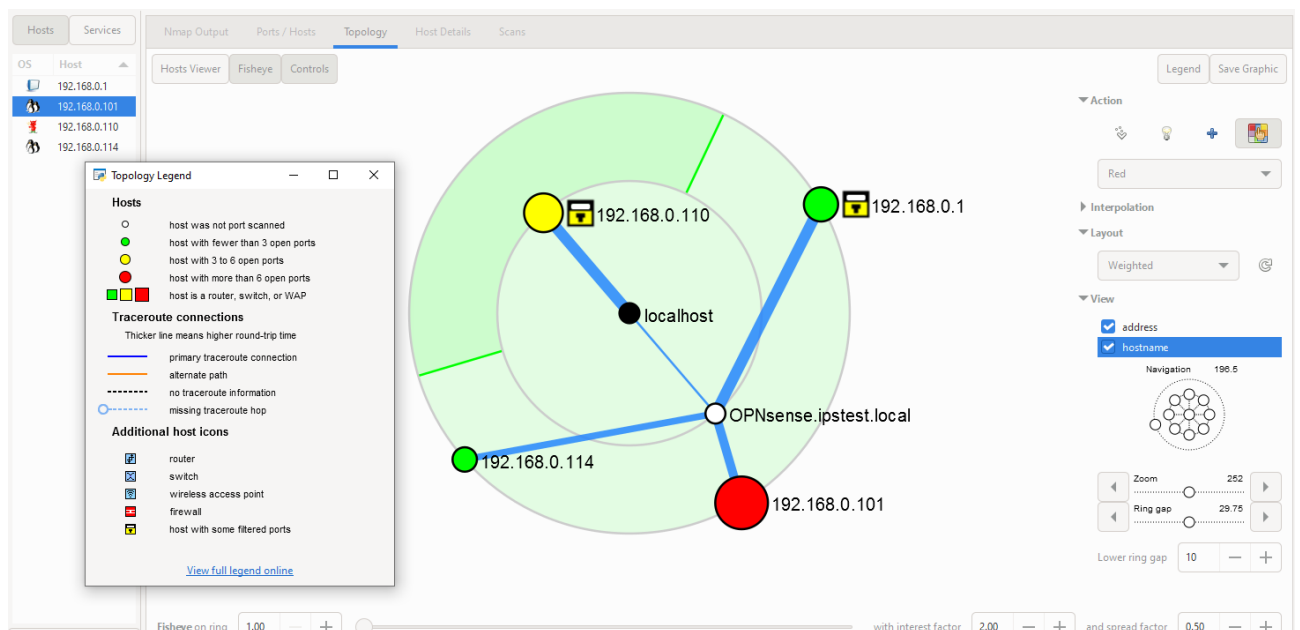


Рисунок 2.6 – Тестування доступності хостів та сервісів лабораторного середовища

Всі хости, представлені у мережі, є доступними, оскільки вони були виявлені під час сканування, і їхній стан відображається у вигляді кольорових позначок. Доступність хостів підтверджується тим, що кожен із них має принаймні кілька відкритих портів або відповідає на мережеві запити, що дозволило Zenmap створити їхню візуалізацію та відобразити зв'язки між ними.

Отже, всі хости, відображені на діаграмі, є доступними, що підтверджується їхньою присутністю у мережевій топології Zenmap. Кольорові позначки вказують на кількість відкритих портів.

2.4 Висновки до розділу 2

В другому розділі було створено тестове лабораторне середовище для дослідження кіберзагроз. Середовище включало гіпервізор KVM, що забезпечує надійну віртуалізацію для розгортання віртуальних машин, таких як Kali Linux, Metasploitable VM та OPNsense. Гіпервізор KVM показав свою ефективність та гнучкість завдяки підтримці апаратної віртуалізації та інтеграції з ядром Linux. Було детально описано OPNsense, що слугує маршрутизатором і системою виявлення вторгнень, а також його можливості, що включають брандмауер, VPN, IDS Suricata та інші функції безпеки. Було проаналізовано використання операційних систем Metasploitable VM та Kali Linux, які слугують навчальними платформами для дослідження вразливостей та проведення тестувань.

Процес тестування лабораторного середовища включав перевірку працездатності гіпервізора KVM, налаштування та взаємодію віртуальних машин, а також зв'язки між ними. Для оцінки доступності хостів та сервісів було проведено сканування мережі за допомогою Zenmap, що підтвердило доступність усіх компонентів середовища. Результати сканування та діаграми мережевої топології показали, що всі хости коректно налаштовані та можуть взаємодіяти один з одним, що свідчить про правильну конфігурацію тестового середовища. Таким чином, створене лабораторне середовище є готовим до використання для подальших досліджень.

РОЗДІЛ 3 НАЛАШТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕННЯМ ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ

3.1 Налаштування IDS Suricata

Suricata - це передова система IDS/IPS з відкритим вихідним кодом, яка підтримується та розробляється організацією Open Information Security Foundation (OISF). Suricata створена для забезпечення ефективного виявлення загроз у мережевому середовищі та може працювати в режимі IDS та IPS [33].

Режим IDS виконує аналіз трафіку, що проходить через мережу, і виявляє підозрілі дії без втручання у потік даних. Виявлені загрози реєструються у журналах, що дозволяє адміністраторам аналізувати події та вживати необхідних заходів. Режим IPS не тільки виявляє загрози, але й може активно блокувати небажаний трафік у реальному часі. Цей режим вимагає більш складних налаштувань і глибокої інтеграції з мережевою інфраструктурою.

Suricata має низку унікальних особливостей, які роблять її популярною серед фахівців з кібербезпеки. Однією з головних переваг є підтримка багатопотоковості, що дозволяє використовувати всі ядра процесора для обробки трафіку та забезпечує високу продуктивність навіть в умовах великих обсягів даних. Suricata використовує різні механізми для аналізу трафіку, включаючи сигнатурний аналіз, аналіз на основі аномалій.

Система підтримує різні протоколи, такі як IP, TCP, UDP, HTTP, DNS, TLS та багато інших, що дозволяє виконувати глибокий аналіз пакетів на рівні додатків. Suricata може визначати різні типи атак і загроз, включаючи сканування портів, DDoS-атаки, спроби експлуатації вразливостей у додатках і мережевих протоколах, а також інші небажані дії. Окрім цього, Suricata може відслідковувати поведінку мережевого трафіку, ідентифікувати додатки та протоколи, а також виконувати аналіз файлів, що передаються через мережу.

Однією з важливих можливостей Suricata є підтримка роботи з правилами, що дозволяє налаштовувати поведінку системи залежно від потреб. Suricata

використовує правила для виявлення атак, де кожне правило описує шаблон або сигнатуру, за якою система визначає підозрілі пакети (див. рисунок 3.1).

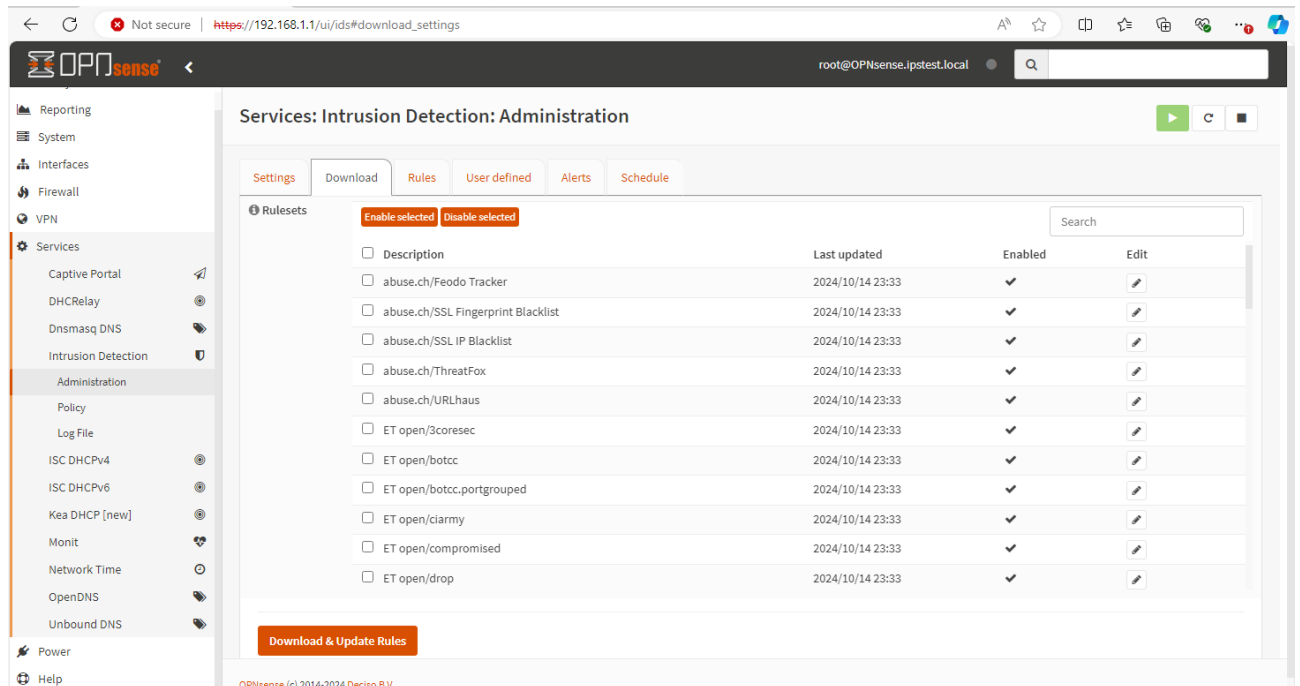


Рисунок 3.1 – Розділ для завантаження правил в OPNsense

У OPNsense доступні різні набори правил для налаштування Suricata. Emerging Threats (ET) - це популярний набір правил IDS/IPS, який включає як безкоштовну версію з ліцензією BSD, так і комерційну версію. Безкоштовний набір ET Open інтегрований в OPNsense і надає базове покриття для виявлення загроз. Однак варто зазначити, що ETOpen не є повним і всебічним набором правил і може бути недостатнім для використання в середовищах із жорсткими регуляторними вимогами, тому його не рекомендується використовувати як єдиний захисний інструмент. ETPro Telemetry - безкоштовна альтернатива комерційній версії ET Pro, яку пропонує Proofpoint. Abuse.ch - це проєкт, що пропонує кілька чорних списків для захисту від підозрілих мережевих ресурсів. Одним з ключових компонентів є SSL Blacklist (SSLBL), який забезпечує список шкідливих SSL-сертифікатів, пов'язаних із діяльністю ботнетів або шкідливим програмним забезпеченням. Ці списки використовують SHA1-хеші для ідентифікації шкідливих сертифікатів. Feodo Tracker - це інструмент, який відстежує діяльність троянів сімейства Feodo (відомі також як Cridex або Bugat),

що використовуються для шахрайства в електронному банкінгу і крадіжки конфіденційної інформації, такої як дані кредитних карток і облікові дані. Tracker відстежує кілька версій Feodo, кожна з яких має свої особливості:

- версія А використовує скомпрометовані веб-сервери з проксі-сервером nginx на порту 8080 TCP;
- версія В розміщується на серверах, орендованих кіберзлочинцями, з використанням доменних імен із ccTLD.ru;
- версія С, відома як Geodo або Emotet, використовує ту саму інфраструктуру, що й версія А, але з іншою структурою URL;
- версія D, яка є наступником Cridex, відома як Dridex.

URLHaus List - ще один проєкт від abuse.ch, доданий у OPNsense з версії 18.1.7, який збирає інформацію про скомпрометовані веб-сайти, що поширюють шкідливе ПЗ. App detection rules - набір правил, доданий у версії 18.1.11, що дозволяє виявляти та блокувати веб-сервіси і пов'язані з ними URL. Це корисно, оскільки близько 80% мережевого трафіку становлять веб-додатки.

Адміністратори можуть використовувати вже готові набори правил, такі як Emerging Threats (ET Open) та інші комерційні джерела, або створювати власні правила, щоб адаптувати систему під специфічні вимоги.

Suricata підтримує інтеграцію з іншими засобами моніторингу та управління безпекою, включаючи системи збору логів і SIEM (Security Information and Event Management) платформи. Це дозволяє фахівцям з кібербезпеки централізовано контролювати та аналізувати дані про події у мережі, швидко реагувати на загрози та проводити розслідування інцидентів безпеки.

Система також має функцію відображення файлів і аналізу потоку даних, що дозволяє збирати інформацію про файли, передані через мережу, і виконувати їх аналіз для виявлення шкідливого коду. Крім цього, Suricata підтримує HTTP-логування, що дозволяє відстежувати запити та відповіді HTTP, аналізуючи заголовки, URL і тіла запитів.

Налаштування Suricata в OPNsense в режимі IDS є важливим етапом для забезпечення безпеки мережі, оскільки Suricata дозволяє виявляти та реагувати на потенційні загрози у реальному часі. Вибір інтерфейсу для моніторингу є

важливим кроком у налаштуванні Suricata. Часто постає питання, який інтерфейс обрати для аналізу трафіку. Зокрема, при захопленні трафіку на інтерфейсі WAN ви побачите тільки трафік після NAT, що означає, що весь трафік виглядатиме так, ніби він походить від брандмауера, а не від фактичної машини, яка його ініціює. Це може стати проблемою, оскільки для коректного спрацювання правил IDS необхідно розуміти внутрішню мережу, і ця інформація може бути втрачена при використанні NAT.

Загальні налаштування системи включають кілька важливих опцій, які допомагають налаштувати Suricata для роботи в мережі:

Promiscuous mode дозволяє Suricata прослуховувати весь трафік, що проходить через інтерфейс, а не лише той, який адресовано цьому інтерфейсу (див. рисунок 3.2).

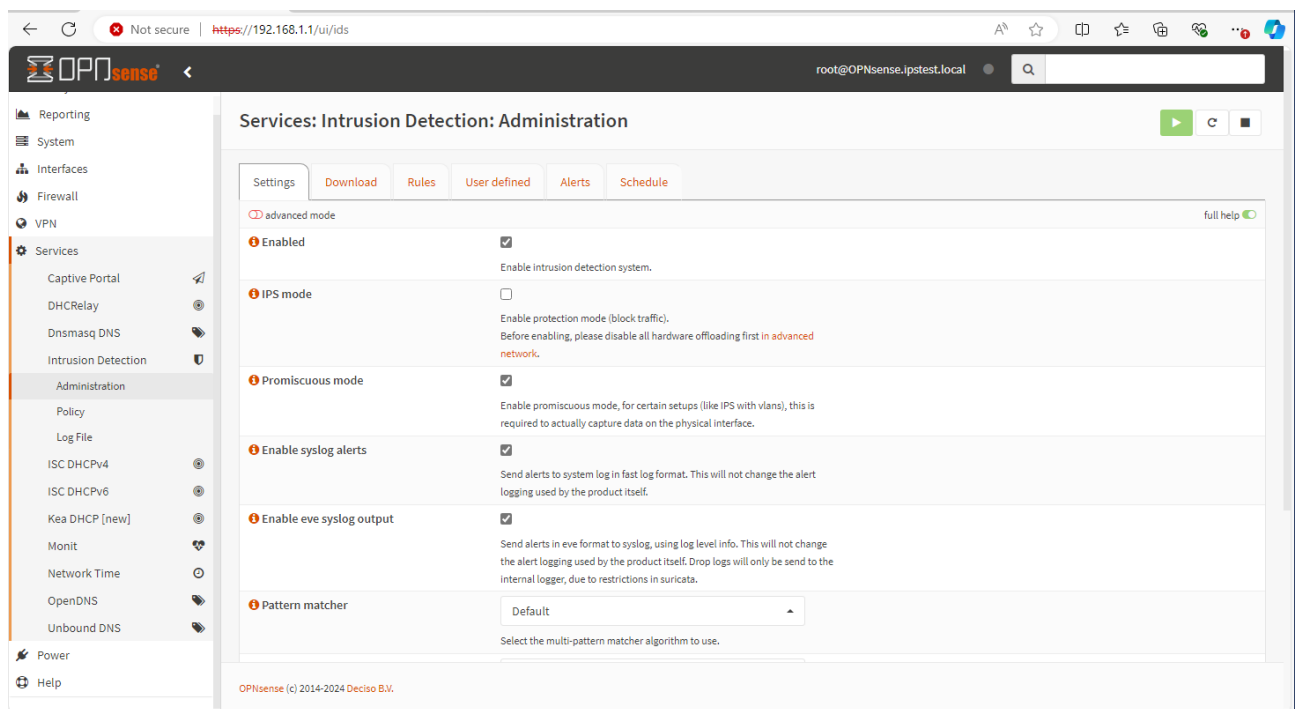


Рисунок 3.2 – Розділ IDS в OPNsense

Налаштування політик і пріоритетів допомагає керувати діями Suricata при виявленні загроз. Журнали та оповіщення є важливою частиною роботи Suricata, оскільки вони дозволяють адміністраторам отримувати інформацію про виявлені загрози та аналізувати їх для подальших дій. У розділі Alerts можна переглядати

всі сповіщення, що були згенеровані системою, і отримувати детальну інформацію про кожен інцидент (див. рисунок 3.3).

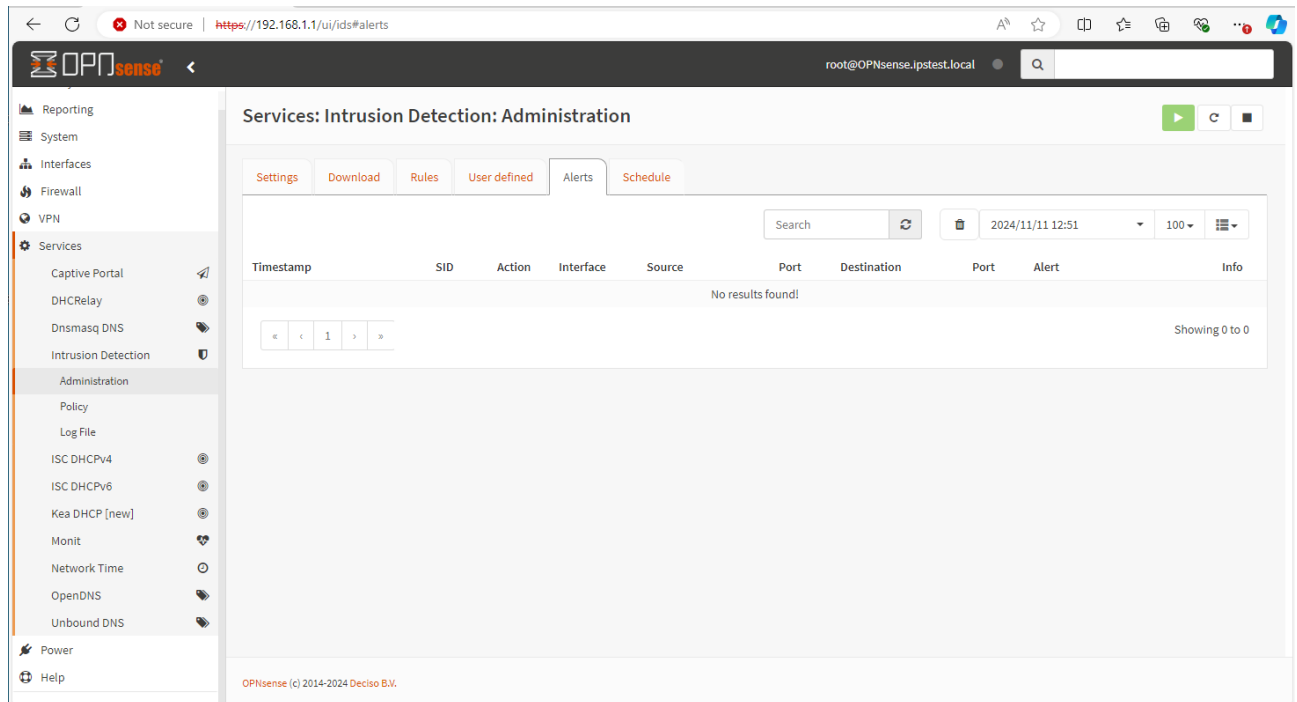


Рисунок 3.3 – Розділ Alerts в IDS OPNsense

Оповіщення можна налаштувати для відправки в syslog, що дозволяє передавати їх до зовнішніх інструментів моніторингу та аналізу. Додаткові налаштування включають можливість вказати домашні мережі (Home Networks), щоб Suricata знала, які IP-адреси вважати внутрішніми. Це важливо для правил, які залежать від розрізнення між внутрішнім та зовнішнім трафіком. Також можна налаштувати розмір пакетів і частоту ротації журналів, щоб оптимізувати продуктивність та зберігання даних.

Налаштування користувацьких правил дозволяє створювати власні правила для Suricata у випадках, коли готові правила не відповідають потребам мережі. Це робиться через вкладку User defined, де адміністратори можуть додавати правила з використанням специфікації Suricata.

Розширене налаштування Suricata в OPNsense дозволяє користувачам створювати спеціальні конфігураційні файли у форматі `suricata.yaml` для додавання додаткових опцій, що не підтримуються у веб-інтерфейсі за замовчуванням. Ці файли можна розміщувати в каталозі

/usr/local/opnsense/service/templates/OPNsense/IDS/ і використовувати шаблони Jinja2 для додаткової гнучкості налаштування.

3.2 Налаштування наборів правил для підвищення ефективності роботи IDS

Налаштування наборів правил для підвищення ефективності роботи IDS є важливим етапом для забезпечення точного та своєчасного виявлення загроз. Для цього необхідно уважно підходити до вибору і налаштування правил, щоб мінімізувати кількість хибнопозитивних спрацювань та підвищити ефективність системи.

Для виявлення DDoS атак, сканування портів, SQL ін'єкцій та brute-force атак необхідно ретельно налаштувати конкретні набори правил та вибрати окремі правила, які найбільш точно відповідають вашій мережевій інфраструктурі.

Для виявлення DDoS було використано набір правил Emerging Threats. У цьому наборі є правила, що дозволяють виявляти аномалії трафіку, характерні для DDoS атак. Зокрема, правила, які відстежують високий обсяг однотипних запитів від одного джерела або до одного порту, можуть сигналізувати про можливу атаку на доступність. Правила такого типу були налаштовані для режиму Alert. Прикладом може бути правило ET з підписом "ET DOS Possible DDoS Attempt".

Для виявлення сканування портів було увімкнено правила, які відстежують множинні запити до різних портів від одного джерела за короткий проміжок часу. У наборах ET Open та Abuse.ch містяться такі правила, як "ET SCAN Potential Port Scan" та інші подібні сигнатури. Ці правила були налаштовані для створення сповіщень (режим Alert), щоб адміністратори могли вчасно реагувати та приймати рішення про блокування.

Для виявлення SQL ін'єкцій було використано правила з наборів ET Open та спеціалізованих правил для веб-додатків. Такі правила містять сигнатури, що відстежують специфічні запити до серверів, які мають вказівки на ін'єкційні атаки. Прикладом може бути правило з підписом "ET WEB_SPECIFIC_APPS

Possible SQL Injection Attempt". Ці правила були налаштовані для режиму Alert, щоб забезпечити моніторинг та аналіз без негайного блокування.

Для виявлення brute-force атак було використано правила, які відстежують багаторазові спроби підключення до одного й того ж сервісу з різними обліковими даними або паролями. Було застосовано набір ET Open з правилами "ET ATTACK Multiple Login Attempts" або "ET POLICY Brute Force Login Attempt Detected". Такі правила можуть сигналізувати про підозрілі дії з боку IP-адреси, яка намагається отримати доступ до системи шляхом підбору паролів..

Загальна кількість правил IDS Suricata становить 177613. Активізація всіх доступних правил дозволяє системі здійснювати детальну перевірку трафіку на наявність потенційних загроз, включаючи DDoS-атаки, сканування портів, SQL-ін'єкції, brute-force атаки та інші види шкідливої активності.

Але активне використання такої великої кількості призводить до високого навантаження на систему. Це може вплинути на продуктивність та ефективність аналізу мережевого трафіку. Тому для підтримання оптимальної роботи системи потрібно ретельно підходити до вибору активних правил і використовувати тільки ті, які відповідають специфіці їхньої мережі або можливих загроз.

Крім того, активізація всіх правил може призвести до збільшення кількості помилкових спрацьовувань, що ускладнює аналіз і моніторинг подій, оскільки кожне спрацювання потребує уваги для визначення його реальної загрози.

Вибір і активація специфічних правил для кожного типу атак, що відповідають вразливостям Metasploitable VM, дозволила покрити більшість можливих сценаріїв експлуатації в цьому середовищі. Загальна кількість активних правил становить 2602, що враховую комплексний захист від різних типів атак.

На рисунку 3.4 показано список активних правил з джерелами, типами класів та короткими описами.

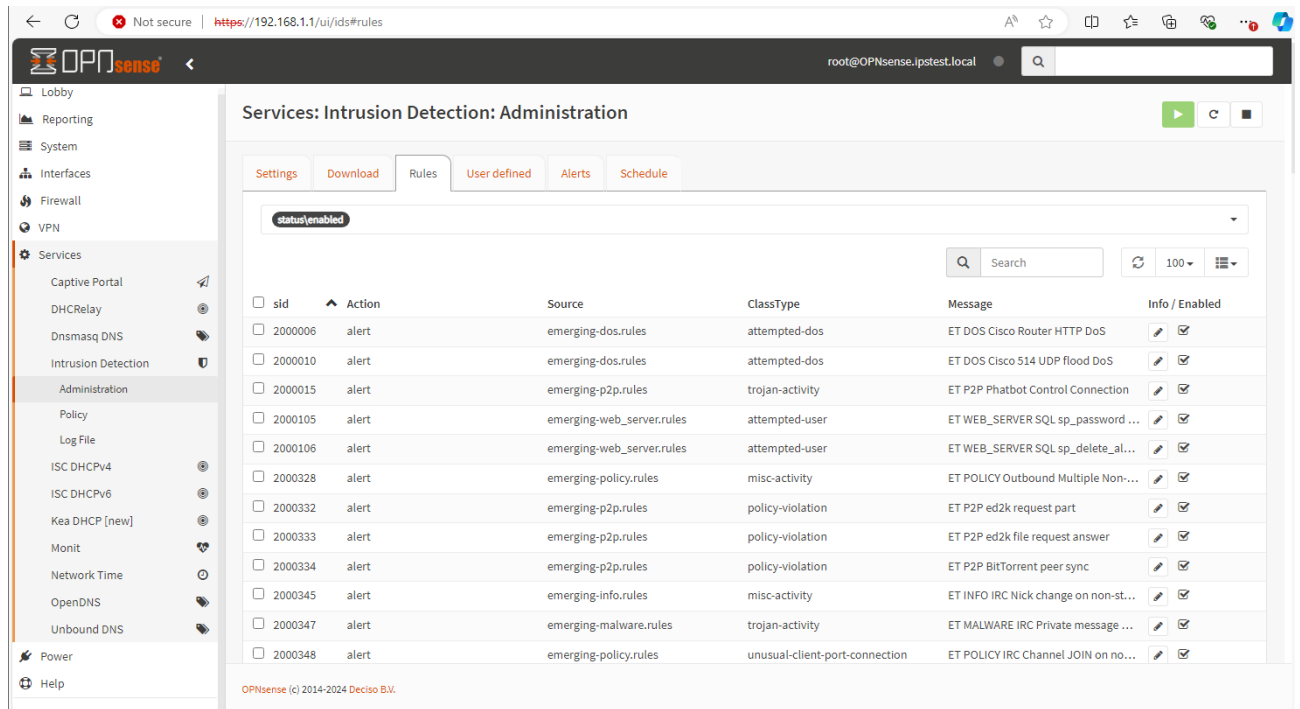


Рисунок 3.4 – Активні правила в IDS OPNsense

Оптимізація цих правил також передбачає регулярне оновлення наборів правил та аналіз сповіщень для налаштування фільтрів і політик, які мінімізують хибні спрацювання. Використання налаштувань на основі пріоритетів дозволило визначати, які правила мають першочергове значення, що допомогло швидше виявляти найнебезпечніші загрози та знижувати навантаження на систему.

3.3 Моделювання кіберзагроз та оцінка ефективності правил IDS

Моделювання кіберзагроз у тестовому середовищі, яке включає Metasploitable VM версії 2 та Kali Linux, є важливим етапом для оцінки ефективності налаштованих правил виявлення вторгнень та роботи систем IDS. Це середовище дозволяє проводити різні сценарії атак та аналізувати, наскільки якісно правила реагують на потенційні загрози. Оцінка ефективності правил IDS відбувається через запуск моделювання атак, моніторинг спрацювань у системі IDS та аналіз результатів. Перевіряється, чи були загрози виявлені та чи відображаються вони як попередження або активні дії, а також аналізуються помилкові спрацювання для забезпечення точності роботи системи. Результати тестування продемонструють, наскільки добре правила виявляють та

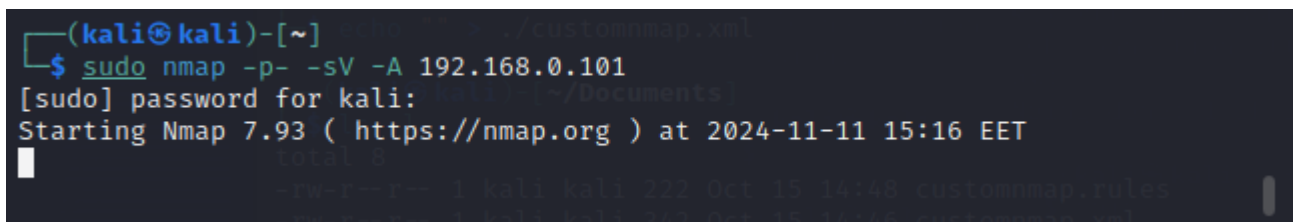
блокують атаки на різні служби Metasploitable VM, допомагаючи оцінити ефективність вибраних правил.

3.1.1 Сканування відкритих портів

Сканування відкритих портів на Metasploitable VM за допомогою інструмента nmap у середовищі Kali Linux є важливим етапом дослідження безпеки та аналізу можливих вразливостей. Kali Linux, відома своїм багатим набором інструментів для тестування на проникнення, дозволяє проводити різноманітні види сканування мережі, включаючи виявлення відкритих портів та визначення служб, що на них працюють.

Metasploitable VM створена спеціально для моделювання кіберзагроз. Вона містить різні сервіси, серед яких FTP, SSH, Telnet, SMTP, HTTP, MySQL, що є вразливими до атак. Використання nmap для сканування портів дозволяє перевірити доступність цих служб, виявити потенційні вразливості та оцінити можливості для їхньої експлуатації.

На рисунку 3.5 показано виконання команди nmap в Kali Linux для сканування всіх портів на Metasploitable VM.



```
(kali@kali)-[~]  
$ sudo nmap -p- -sV -A 192.168.0.101  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-11 15:16 EET  
[...]
```

Рисунок 3.5 – Сканування всіх портів на Metasploitable VM

Сканування допомагає отримати детальну інформацію про відкриті порти, працюючі сервіси та їх версії, а також дозволяє зробити попередній аналіз можливих вразливостей, що може бути використане для планування подальших дій з безпеки або тестування на проникнення.

IDS Suricata розпізнала сканування портів. На рисунку 3.6 показано повідомлення, створені IDS Suricata в OPNsense під час виявлення активності сканування портів.

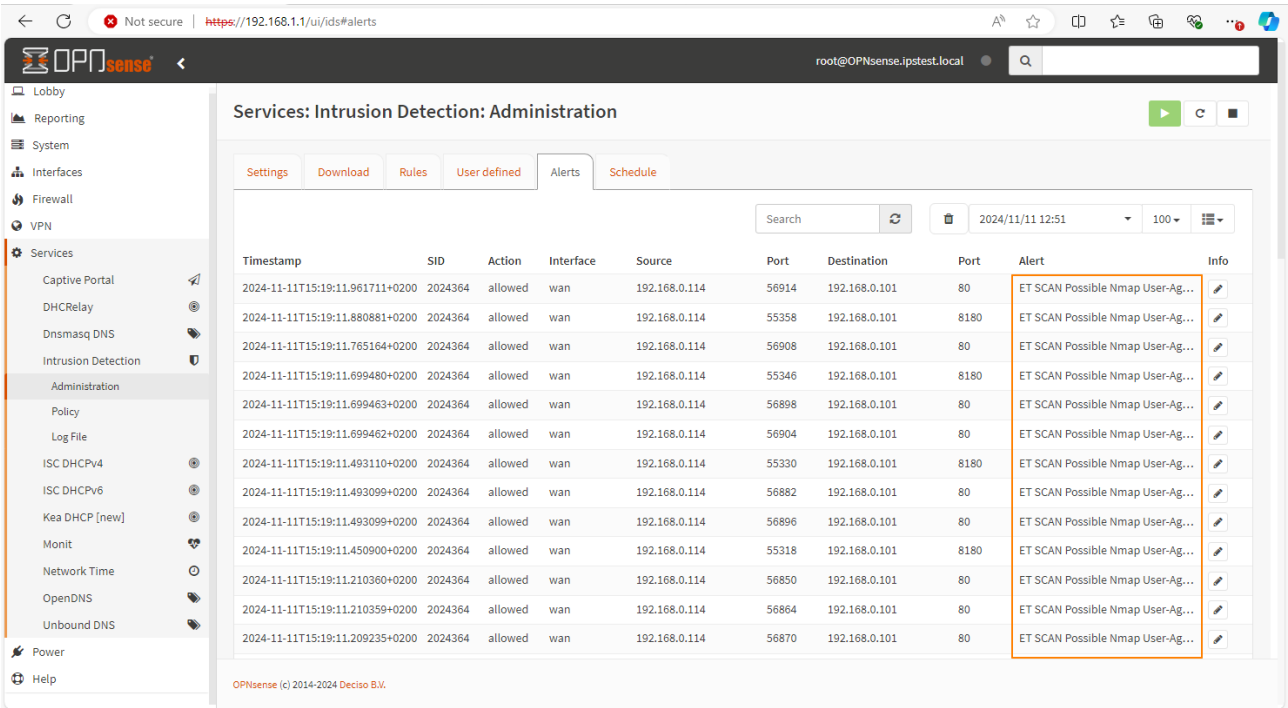


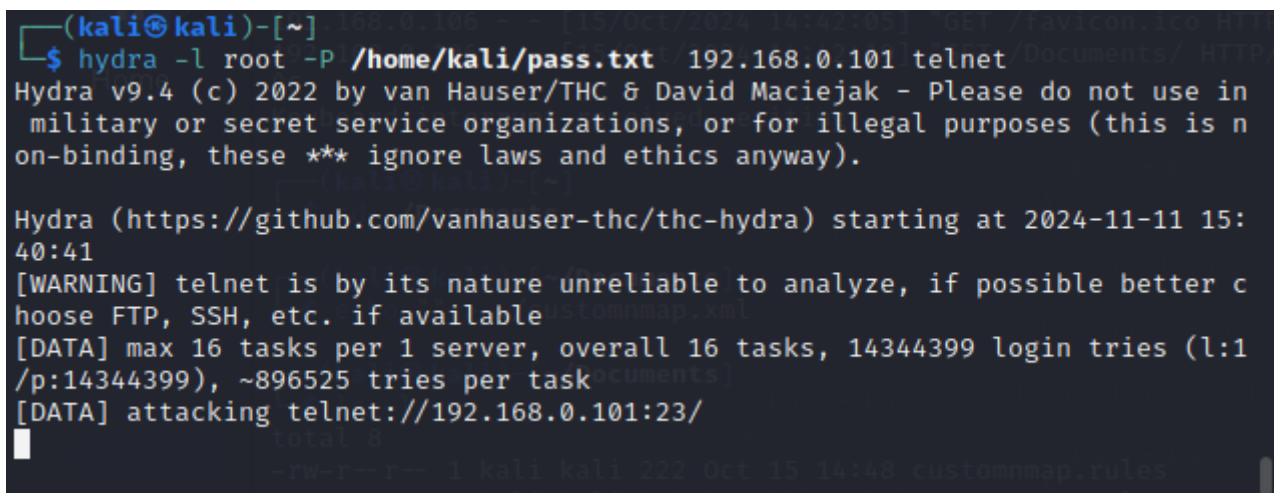
Рисунок 3.6 – Сповіщення IDS Suricata під час сканування портів

Усі сповіщення мають один і той самий SID – 2024364, що вказує на активоване правило в наборі правил IDS, яке відповідає за виявлення спроб сканування портів за допомогою відомих інструментів, таких як Nmap. Джерелом є IP-адреса 192.168.0.114, що відповідає Kali Linux, з якої здійснювалось сканування портів. Призначенням сканування була IP-адреса 192.168.0.101, що належить Metasploitable VM. Сповіщення "ET SCAN Possible Nmap User-Agent Detected" вказує на можливість використання Nmap для сканування, активувавши відповідне правило Emerging Threats для попередження про потенційну небезпеку. Таке сповіщення є важливим для адміністраторів мережі, оскільки швидко повідомляє про підозрілу активність, що може свідчити про підготовку до атаки або збір інформації про систему, попереджаючи про можливу спробу знайти слабкі місця в мережі.

3.1.2 Brute-force атаки

Для моделювання brute-force атак на віртуальну машину Metasploitable VM з використанням Kali Linux можна скористатися інструментом hydra. Hydra – це потужний інструмент для атак підбору паролів, який підтримує різні протоколи, такі як FTP, SSH, HTTP, Telnet та інші. Metasploitable VM спеціально налаштована для того, щоб бути вразливою до таких атак, оскільки містить декілька служб з відомими слабкими обліковими даними.

На рисунку 3.7 відображено процес запуску brute-force атаки за допомогою інструменту hydra в операційній системі Kali Linux. У цьому прикладі виконується спроба підбору паролю для доступу до сервісу Telnet на вразливій машині Metasploitable VM.



```
(kali㉿kali)-[~]
└─$ hydra -l root -P /home/kali/pass.txt 192.168.0.101 telnet
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
  military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-11 15:
40:41
[WARNING] telnet is by its nature unreliable to analyze, if possible better c
hoose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking telnet://192.168.0.101:23/
```

Рисунок 3.7 – Brute-force атака на сервіс telnet

Hydra використовується для тестування паролів з файлу /home/kali/pass.txt для імені користувача root. Аналогічна brute-force атаки була проведена для FTP сервісу.

IDS Suricata розпізнала brute-force атаки. На рисунку 3.8 показано повідомлення, створені IDS Suricata в OPNsense під час виявлення brute-force атаки.

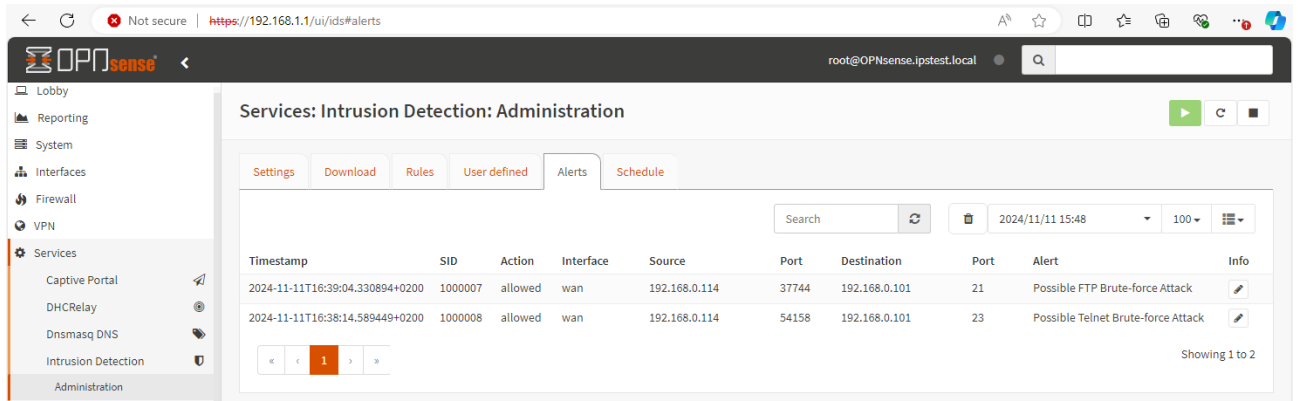


Рисунок 3.8 – Сповіщення IDS Suricata під час brute-force атаки

Зафіксовано дві події, кожна з яких відповідає спробам brute-force атаки на різні сервіси. Перший запис з ідентифікатором SID 1000007 вказує на можливу brute-force атаку на FTP (порт 21), а другий запис з SID 1000008 — на спробу brute-force атаки на Telnet (порт 23). В обох випадках атакуюча система з IP-адресою 192.168.0.114 (Kali Linux) намагається отримати доступ до сервісів на хості Metasploitable VM з IP-адресою 192.168.0.101.

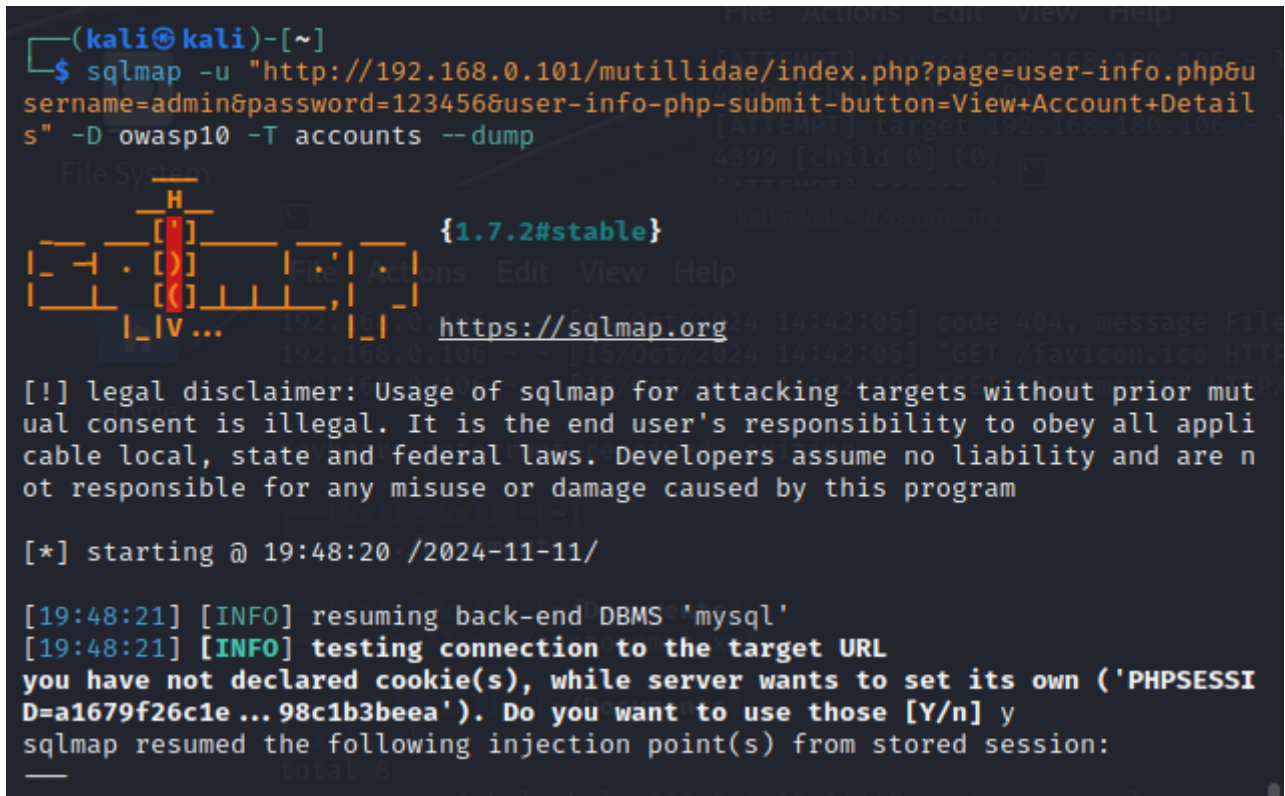
Suricata ідентифікувала ці спроби як можливі brute-force атаки завдяки частим підключенням до цільових портів у короткий проміжок часу, що характерно для автоматизованих атак типу brute-force.

3.1.3 Атака типу SQL-ін'єкції

Атака типу SQL-ін'єкції з використанням інструменту sqlmap спрямована на виявлення і використання вразливостей у веб-додатках, які обробляють SQL-запити, наприклад, Mutillidae, що встановлений на віртуальній машині Metasploitable VM. У цьому сценарії Kali Linux використовується як атакуюча система, де запускається sqlmap для автоматизованого виявлення та експлуатації SQL-ін'єкцій у веб-додатку. SQLmap сканує вхідні точки веб-додатку, аналізуючи відповіді сервера і шукаючи можливості для ін'єкцій з метою несанкціонованого доступу до бази даних. Інструмент намагається вставити шкідливі SQL-запити, що можуть дозволити отримати доступ до конфіденційних даних, видалити, змінити або додати записи в базі даних, а також виконати інші шкідливі дії. Після визначення вразливої точки sqlmap може автоматично

виконати ін'єкцію SQL-коду для отримання інформації, такої як структура бази даних, імена таблиць, записи користувачів та інші дані, що можуть бути збережені у базі.

На рисунку 3.8 показано процес запуску інструменту sqlmap в системі Kali Linux для виконання SQL-ін'єкції на веб-додатку Mutillidae, що працює на вразливій віртуальній машині Metasploitable VM.



```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.0.101/mutillidae/index.php?page=user-info.php&username=admin&password=123456&user-info-php-submit-button=View+Account+Details" -D owasp10 -T accounts --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:48:20 /2024-11-11/

[19:48:21] [INFO] resuming back-end DBMS 'mysql'
[19:48:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a1679f26c1e...98c1b3beea'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
```

Рисунок 3.9 – Атака типу SQL-ін'єкції

У команді sqlmap зазначено URL-адресу вразливої сторінки, яка може бути потенційно вразливими до SQL-ін'єкцій. Команда також включає параметри для визначення бази даних -D owasp10, вказівки на конкретну таблицю -T accounts та дії --dump, яка наказує sqlmap отримати та показати дані з таблиці.

При запуску sqlmap, система спочатку тестує з'єднання з цільовим URL і перевіряє, чи існує потреба в куках для продовження атаки. Після того, як sqlmap встановлює, що ціль підтримує сесію через куки, користувачу пропонується використати ці куки для більш точного тестування.

Інструмент автоматично відновлює точку ін'єкції, раніше збережену з сеансу, що дозволяє sqlmap проводити наступні ін'єкції більш ефективно. Після

підтвердження цієї інформації sqlmap продовжує ін'єкцію для вилучення даних з таблиці accounts та читає конфіденційну інформацію (див. рисунок 3.10).

```
[19:48:23] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[19:48:24] [WARNING] reflective value(s) found and filtering out
[19:48:24] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[17 entries]
```

cid	is_admin	password	username	mysignature
1	TRUE	adminpass	admin	Monkey!
2	TRUE	someword	adrian	Zombie Films Rock!
3	FALSE	monkey	john	I like the smell of confunk
4	FALSE	password	jeremy	d1373 1337 speak
5	FALSE	password	bryce	I Love SANS
6	FALSE	samurai	samurai	Carving Fools
7	FALSE	password	jim	Jim Rome is Burning
8	FALSE	password	bobby	Hank is my dad
9	FALSE	password	simba	I am a cat
10	FALSE	password	dreveil	Preparation H
11	FALSE	password	scotty	Scotty Do
12	FALSE	password	cal	Go Wildcats
13	FALSE	password	john	Do the Duggie!
14	FALSE	42	kevin	Doug Adams rocks
15	FALSE	set	dave	Bet on S.E.T. FTW
16	FALSE	pentest	ed	Commandline KungFu anyone?
17	NULL	admin	admin	pass admin

Рисунок 3.10 – Результат SQL-ін'єкції

Після виявлення уразливих точок sqlmap отримує доступ до бази даних owasp10, до таблиці accounts, і завантажує дані. Серед вилучених даних - ідентифікатори користувачів (cid), статус адміністратора (is_admin), паролі (password), імена користувачів (username) і підписи (mysignature). Дані показують приклади облікових записів із вразливостями, зокрема облікові записи з простими паролями, такими як "password", що є типовою проблемою безпеки.

Цей результат підтверджує наявність уразливостей SQL-ін'єкції в додатку Mutillidae, а sqlmap демонструє свою здатність автоматично виявляти та експлуатувати ці вразливості.

IDS Suricata розпізнала атаку типу SQL-ін'єкції. На рисунку 3.11 показано повідомлення, створені IDS Suricata в OPNsense під час виявлення SQL-ін'єкції.

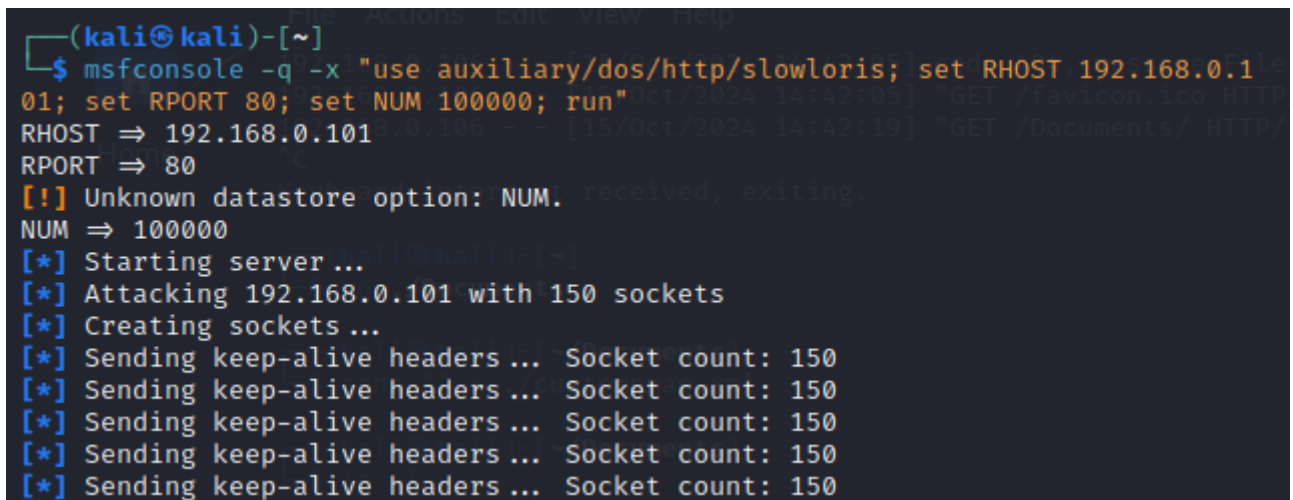
Рисунок 3.12 – Детальна інформацію зафіксована IDS Suricata під час SQL-ін'єкції

Система IDS змогла виявити активність, характерну для SQL-ін'єкцій, які здійснювалися через HTTP-запити до веб-сервера, що підтверджує спроби несанкціонованого доступу або вилучення даних через SQL-ін'єкцію.

3.1.4 Атаки типу DDoS

Атаки типу DDoS - це атаки на інформаційні системи, які мають на меті зробити ресурси (сервери, мережі, веб-додатки) недоступними для користувачів.

На рисунку 3.13 показано використання команди для запуску DDoS-атаки типу Slowloris за допомогою Metasploit Framework (msfconsole).



```
(kali㉿kali)-[~]
$ msfconsole -q -x "use auxiliary/dos/http/slowloris; set RHOST 192.168.0.101; set RPORT 80; set NUM 100000; run"
RHOST => 192.168.0.101
RPORT => 80
[!] Unknown datastore option: NUM.
NUM => 100000
[*] Starting server ...
[*] Attacking 192.168.0.101 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
```

Рисунок 3.13 – Атака типу Slowloris

До цільового сервера надсилаються заголовки keep-alive, щоб зберегти з'єднання відкритим. Таким чином, атакуючий продовжує тримати сокети відкритими, що може призвести до вичерпання ресурсів веб-сервера і його недоступності для інших користувачів.

IDS Suricata розпізнала атаку типу Slowloris. На рисунку 3.14 показано повідомлення, створені IDS Suricata в OPNsense під час виявлення Slowloris атаки.

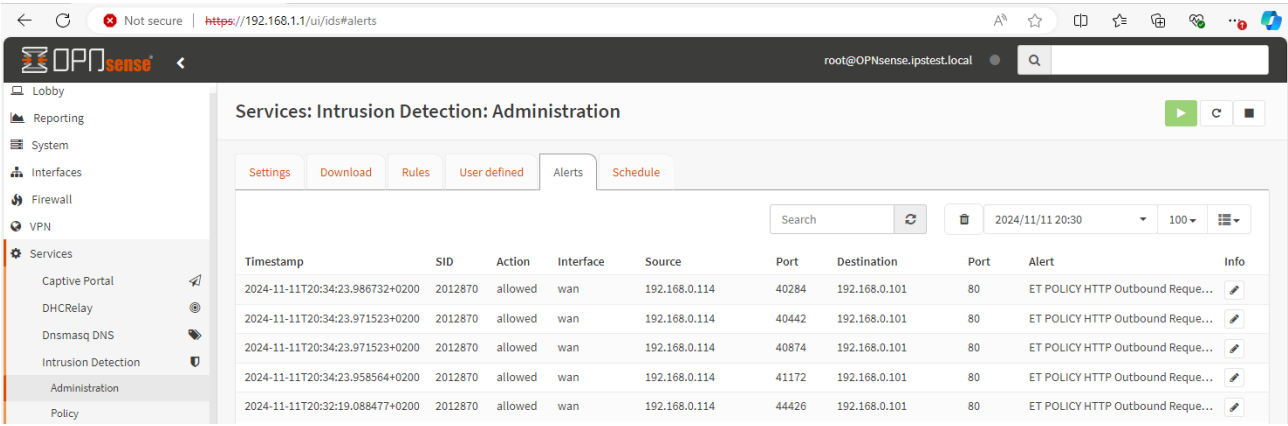


Рисунок 3.14 – Сповіщення IDS Suricata під час Slowloris атаки

На рисунку 3.15 показано запуск команди `hping3` для здійснення DDoS-атаки типу ICMP Flood на цільовий сервер з IP-адресою 192.168.0.101.

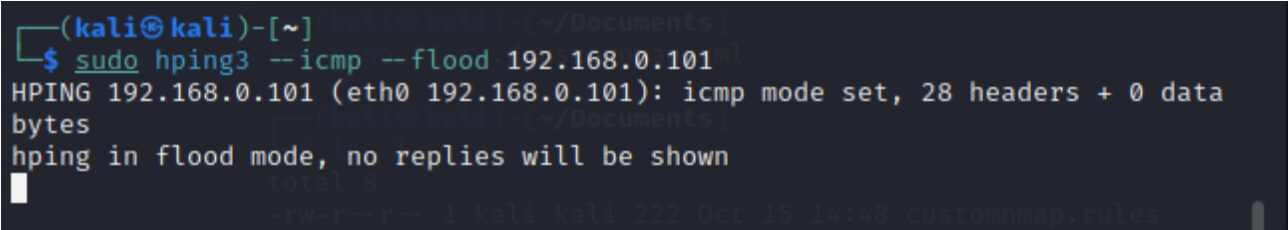


Рисунок 3.15 – Атака типу ICMP Flood

На рисунку 3.16 показано журнал сповіщень у системі виявлення вторгнень Suricata в середовищі OPNsense. Відображаються декілька сповіщень, що вказують на виявлення ICMP-запитів типу "PING".

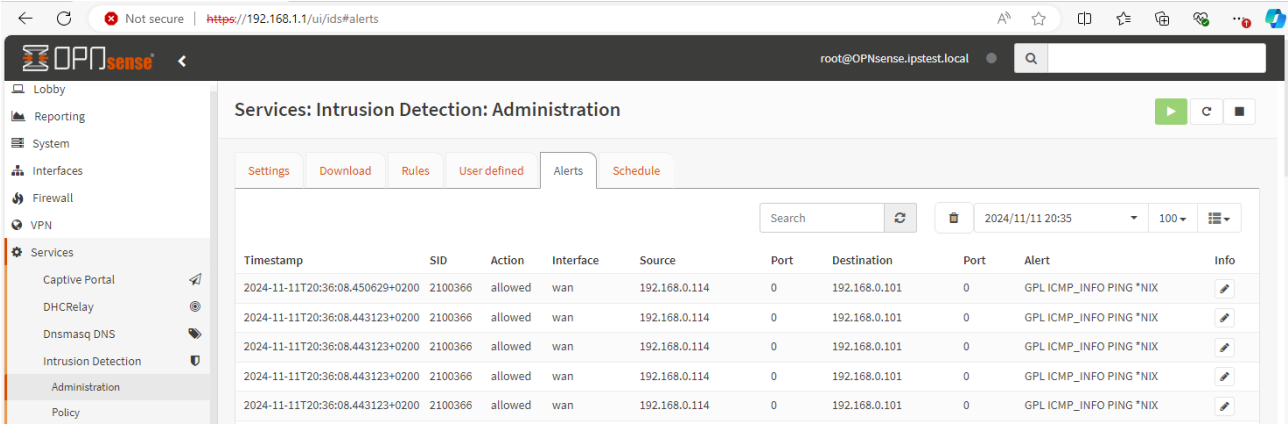
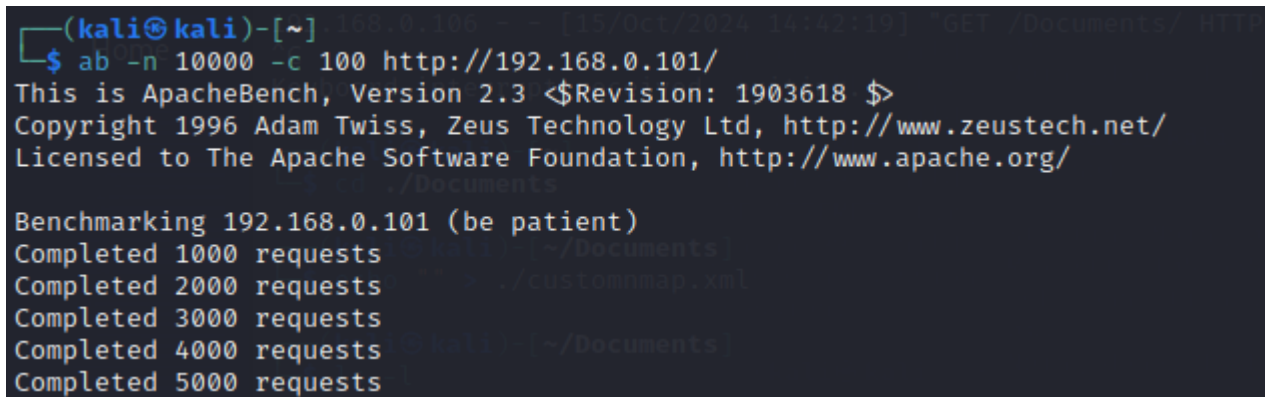


Рисунок 3.16 – Сповіщення IDS Suricata під час ICMP Flood атаки

Ці сповіщення є результатом активної ICMP Flood атаки, виконаної за допомогою hping3. Suricata розпізнала високий потік ICMP-запитів від джерела до цілі, що свідчить про DDoS-атаку типу ICMP Flood.

На рисунку 3.17 показано використання інструменту ab (Apache Benchmark) для симулювання HTTP Flood атаки на сервер за IP-адресою 192.168.0.101.



```
(kali㉿kali)-[~]  
$ ab -n 10000 -c 100 http://192.168.0.101/  
This is ApacheBench, Version 2.3 <$Revision: 1903618 $>  
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/  
Licensed to The Apache Software Foundation, http://www.apache.org/  
  
Benchmarking 192.168.0.101 (be patient)  
Completed 1000 requests  
Completed 2000 requests  
Completed 3000 requests  
Completed 4000 requests  
Completed 5000 requests
```

Рисунок 3.17 – Атака типу HTTP Flood

Це програмне забезпечення створює велику кількість HTTP-запитів до сервера в короткий проміжок часу, що імітує DDoS-атаку типу HTTP Flood. Метою такої атаки є перевантаження сервера HTTP-запитами, що може призвести до зниження його продуктивності або навіть відмови в обслуговуванні.

На рисунку 3.18 показано журнал сповіщень IDS Suricata в OPNsense, де було виявлено HTTP Flood атаку, симульовану інструментом ab. В полі Alert видно попередження "ET POLICY ApacheBenchmark Tool Usage," що вказує на те, що Suricata розпізнала використання ab як потенційне джерело небезпечної активності.

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2024-11-11T21:01:07.515635+0200	2010725	allowed	wan	192.168.0.114	41642	192.168.0.101	80	ET POLICY ApacheBenchmark Too...	
2024-11-11T21:00:07.501820+0200	2010725	allowed	wan	192.168.0.114	41670	192.168.0.101	80	ET POLICY ApacheBenchmark Too...	

Рисунок 3.18 – Сповіщення IDS Suricata під час HTTP Flood атаки за допомогою ab

IDS зафіксувала декілька сповіщень з однаковим типом попередження, що підтверджує надмірну кількість запитів до порту 80 на сервері за IP-адресою 192.168.0.101. Це типовий приклад DDoS атаки типу HTTP Flood, коли сервер перевантажується великою кількістю HTTP-запитів, що може призвести до зниження продуктивності або відмови у відповідях. Suricata змогла успішно ідентифікувати цей тип атаки та відобразити відповідні попередження у журналі подій.

3.4 Висновки до розділу 3

В третьому розділі було розглянуто процес налаштування системи виявлення вторгнень IDS Suricata в середовищі OPNsense, а також детально проаналізовано її ефективність у виявленні різних типів кіберзагроз. Було показано основні аспекти налаштування IDS, описано процес завантаження та активації правил, які дозволяють налаштувати систему на виявлення специфічних загроз, таких як DDoS атаки, сканування портів, SQL-ін'єкції та brute-force атаки. Здійснено налаштування правил із використанням готових наборів, таких як Emerging Threats і Abuse.ch.

Проведено детальне моделювання різних кіберзагроз на віртуальному тестовому середовищі, що включає Metasploitable VM та Kali Linux, з метою оцінки можливостей IDS Suricata щодо виявлення та фіксації потенційних атак. Сканування відкритих портів за допомогою nmap показало, що Suricata вміє своєчасно розпізнавати ознаки сканування та попереджати про можливі

підготовчі дії до атак. Також було успішно ідентифіковано спроби brute-force атак на різні сервіси Metasploitable, а саме FTP та Telnet, що свідчить про здатність системи швидко реагувати на підозрілу активність, пов'язану зі спробами несанкціонованого доступу.

Крім цього, було проведено атаку SQL-ін'єкції з використанням sqlmap, під час якої Suricata розпізнала характерні параметри запиту, що використовуються для експлуатації вразливості на веб-додатку, та зафіксувала потенційно шкідливі дії. Також було змодельовано кілька DDoS атак, таких як Slowloris, ICMP Flood та HTTP Flood, що дозволило оцінити здатність Suricata до виявлення надмірного трафіку та попередження про можливе порушення доступності ресурсів мережі.

Важливою частиною роботи була оптимізація наборів правил для підвищення ефективності роботи IDS. Вибір і активація специфічних правил для кожного типу атак, що відповідають вразливостям Metasploitable VM, дозволила покрити більшість можливих сценаріїв експлуатації в цьому середовищі. Загальна кількість активних правил становила 2602, що враховує комплексний захист від різних типів атак. Такий підхід до оптимізації дозволив зменшити кількість хибних спрацювань та підвищити ефективність системи.

Проведений аналіз та тестування продемонстрували високу ефективність системи IDS Suricata на базі OPNsense у виявленні різного типу кіберзагроз. Завдяки широким можливостям налаштування правил та підтримці багатопотоковості, Suricata виявилася здатною ефективно ідентифікувати як базові, так і складні атаки. Це дозволяє адміністраторам мережі вчасно отримувати інформацію про загрози та приймати відповідні заходи, підвищуючи рівень безпеки мережі.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою даної кваліфікаційної роботи є моделювання кіберзагроз та оцінка ефективності системи IDS. Дані системи встановлюються на серверному обладнанні, яке розміщене в приміщенні спеціального типу. Пожежна безпека в серверних кімнатах є важливим завданням збереження матеріальних цінностей та життя людей.

Небезпечними чинниками, які впливають на людей під час пожежі, може бути відкритий вогонь чи іскри, підвищена температура повітря, предметів, токсичні продукти горіння, дим, знижена концентрація кисню. Тому пожежну безпеку вважають за невід'ємну частину охорони праці.

Пожежна безпека – це стан об'єкта, за якого із встановленою ймовірністю виключається можливість виникнення та розвитку пожежі, а також забезпечується захист матеріальних цінностей. У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються різні елементи, дроти, комутаційні кабелі. При протіканні електричного струму відходить значна кількість теплоти, що може призвести до підвищення температури окремих вузлів до 80-100°C. З іншого боку, робоча температура силових транзисторів сягає 120°C. Все це може викликати оплавлення ізоляції з'єднувальних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих температурних навантажень елементів схем, їх згоряння з виділенням диму [34].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступень вогнестійкості. Приміщення для обслуговування, ремонту та налагодження ЕОМ повинні належати до категорії В за безпекою щодо пожеж та вибухів, а за класом приміщення - до П за ПБЕ.

Неприпустимим є розташування приміщень категорій А і Б, а також виробництв з мокрими технологічними процесами поряд з приміщеннями, де

розташовуються ЕОМ, виконується їх обслуговування, налагодження і ремонт, а також над такими приміщеннями або під ними.

Стіни кабін мають бути виготовлені з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій. У кабіні мусить бути оглядове вікно (вікна). Висота оглядового вікна має бути не менше 1,5 м, а відстань від підлоги не більше 0,8 м.

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог правил пожежної безпеки в Україні. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, в яких розміщуються великі ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до правил пожежної безпеки в Україні та вимог нормативно-технічної та експлуатаційної документації заводу-виробника [34].

Підходи до засобів пожежогасіння повинні бути вільними. Будівлі та приміщення, в яких експлуатуються ПК та виконується їх обслуговування, налагодження і ремонт, повинні відповідати вимогам пожежної безпеки об'єктів будівництва, експлуатаційної документації заводу-виробника ПК, чинним санітарним нормам у сфері охорони праці.

Не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог, в інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення, мають бути оснащені вогнегасниками.

Приміщення, в яких розміщуються робочі місця операторів великих ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння

Система вентиляції обчислювальних центрів та приміщень з ЕОМ повинна бути обладнана блокувальним пристроєм, який забезпечує її відключення на випадок пожежі.

Пожежна безпека приміщень забезпечується такими засобами:

- справність електропроводки;
- наявність засобів пожежогасіння;
- наявність пожежної сигналізації.

До первинних засобів пожежогасіння у приміщеннях з ЕОМ відносяться різні вуглекислотні, аерозольні, порошкові вогнегасники, призначені для гасіння загорянь та пожеж у початковій стадії їх розвитку.

Вуглекислотні вогнегасники (ВВ-2, ВВ-5, ВВ-8) призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники містять вуглекислоту, яка при відкритті крана розширюється та викидається через розтруб у вигляді вуглекислого снігу температурою -55°C . Тривалість роботи вогнегасників 25-40 секунд, довжина струменя, що викидається, 1,5-2 м (ВВ-2, ВВ-5).

Аерозольні вогнегасники закачувального типу містять або тільки вогнегасний засіб, або ще й додатковий (робочий) газ (наприклад, азот, хладон). Вони призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники малогабаритні, спрощені (з об'ємом заряду від 0,25 до 1,0 літра).

Порошкові вогнегасники (ВП-1, Момент, ВП-2А, ВП-10А) застосовуються для гасіння лужних металів, що горять, горючих рідин, а також обладнання з напругою до 5000 В. Дані вогнегасники містять вогнегасний порошок і балон з газом. Порошок з корпусу вогнегасника виштовхується стисненим газом (азот, повітря) приблизно за 30 секунд.

Автоматичні засоби пожежогасіння розраховані на подачу вогнегасної речовини у разі виникнення пожежі незалежно від того, перебувають у

приміщенні люди або відсутні. Останнім часом знаходять широке застосування автономних автоматичних установок порошкового пожежогасіння.

Проведені дослідження в кваліфікаційній роботі вимагали взаємодії людини з серверним обладнанням. Тому важливим є забезпечити безпечні умови праці інженерів комп'ютерних систем при встановленні, налаштуванні та подальшому обслуговуванні систем захисту сервісів.

4.2 Забезпечення захисту працівників суб'єкта господарювання від іонізуючого випромінювання

Працівники, які виконують роботи з радіоактивними речовинами, повинні перебувати під постійним медичним наглядом, використовувати засоби індивідуального захисту від радіації та прилади індивідуального дозиметричного контролю (універсальні радіометри) для своєчасного виявлення і вимірювання рівня випромінювання [35].

Захищаючись від зовнішнього іонізуючого опромінювання при роботах із закритими джерелами випромінювання, тобто такими, які виключають можливість потрапляння радіоактивних речовин у навколишнє середовище, перш за все необхідно не допустити переопромінення працівників.

Основним способами захисту від цього є:

- зменшення активності джерела, з яким контактують працівники під час конкретного технологічного процесу – досягається шляхом використання речовин із меншою активністю;
- зменшення часу контакту з джерелом випромінювання – досягається шляхом вдосконалення організації робіт і технологічного виробничого процесу та проведення попередніх тренінгів працівників;
- збільшення відстані між людиною і джерелом – використовується, як правило, при контакті з точковим джерелом випромінювання шляхом використання дистанційних універсальних маніпуляторів та інших автоматизованих пристроїв;

- розташування між людиною і джерелом захисного екрану (стаціонарного, пересувного, розбірного, настільного тощо), тобто пристрою, який зменшує інтенсивність випромінювання до безпечного рівня [35].

Для виготовлення екранів, а також для захисту працівників в стаціонарних спорудах, використовується бетон, чавун, сталь, алюміній, скло, свинець та інші матеріали. Від дії рентгенівських променів застосовують екрани зі сталевого листа товщиною 0,5-1 мм або алюмінію товщиною 3 мм, спеціальної гуми. Оглядові вікна виконують з плексигласу товщиною 30 мм або з покритого оловом скла товщиною 9 мм.

Для захисту шкіри від забруднень радіоактивними речовинами та запобігання їх попаданню всередину організму, захисту від альфа і бета-випромінювання передусім застосовуються засоби індивідуального захисту (ЗІЗ) від радіації.

Отже, засоби захисту від радіації використовуються у тих випадках, коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення.

З урахуванням зазначеного прогнозу на території області може виникнути складна радіаційна обстановка наслідки якої вимагатимуть від органів виконавчої влади, органів місцевого самоврядування, суб'єктів господарювання, на які покладено виконання завдань щодо захисту населення і територій від надзвичайних ситуацій, оперативного реагування та дій [35].

Місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання здійснюють для забезпечення захисту людей від впливу іонізуючих випромінювань наступні заходи:

- приймають згідно з законодавством України рішення щодо застосування на підвідомчій території заходів втручання у разі радіаційних аварій;

- організовують проведення в установленому порядку щорічні обстеження з метою оцінки стану захисту людини від впливу іонізуючих випромінювань та ведення екологічного паспорта підвідомчої території;

- здійснюють організаційне керівництво системою обліку та контролю доз опромінення населення на підвідомчій території;
- організовують контроль за виконанням заходів щодо захисту людини від впливу радіонуклідів, що містяться у будівельних матеріалах;
- затверджують відповідні плани щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують постійну готовність засобів оповіщення населення на підвідомчій території про виникнення радіаційної аварії;
- організовують контроль за виконанням заходів щодо захисту населення від радіаційних аварій та їх наслідків;
- забезпечують населення, в місцях його проживання, інформацією щодо рівнів опромінення людини та заходів захисту від впливу іонізуючих випромінювань, що виконуються на підвідомчій території;
- розробляють та впроваджують програми захисту людей від впливу іонізуючих випромінювання;
- здійснюють оповіщення населення у разі виникнення радіаційної аварії та інформування про рятувальні та профілактичні заходи у зв'язку з цим.

Для виконання вищезазначених заходів залучаються органи управління, сили і засоби обласної територіальної та функціональних підсистем єдиної державної системи цивільного захисту (далі – ЄДС ЦЗ), порядок дій яких визначено Планом реагування на надзвичайні ситуації, пов'язаних з викидом радіоактивних речовин.

Режими захисту робітників і службовців на суб'єктах господарювання вводяться в дію рішенням керівників об'єктів. Незалежно від місця розміщення суб'єкту господарювання (в населеному пункті або за його межами) на його території вводиться в дію свій режим захисту з урахуванням рівнів радіації, виміряних на об'єкті, і реального ступеню захисту працівників і службовців.

При виникненні комунальної радіаційної аварії окрім термінових робіт щодо стабілізації радіаційного стану (включаючи відновлення контролю над джерелом) місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання одночасно здійснюють заходи, спрямовані на:

- зведення до мінімуму кількості осіб з населення, які зазнають аварійного опромінення;
- запобігання чи зниження індивідуальних і колективних доз опромінення населення;
- запобігання чи зниження рівнів радіоактивного забруднення продуктів харчування, питної води, сільськогосподарської сировини і сільгоспугідь, об'єктів довкілля (повітря, води, ґрунту, рослин тощо), а також будівель і споруд.

Для населення, робітників та службовців суб'єктів господарювання, які можуть потрапити в зону випадіння радіоактивних опадів, доцільно завчасно, виходячи з конкретних місцевих умов, розрахувати варіанти режимів радіаційного захисту [36].

З урахуванням вищезазначеного, режими радіаційного захисту вводяться в дію місцевими органами виконавчої влади, органами місцевого самоврядування, суб'єктами господарювання з метою захисту людей від впливу іонізуючого випромінювання у разі загрози або виникнення надзвичайних ситуацій, пов'язаних з радіаційними аваріями.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра було проведено комплексне дослідження сучасних кіберзагроз та методів захисту від них. Основна увага була зосереджена на атаках на доступність, конфіденційність та цілісність даних, а також на сучасних підходах до їх виявлення.

Було створено тестове лабораторне середовище, яке включало гіпервізор KVM для розгортання віртуальних машин, таких як Kali Linux, Metasploitable VM та OPNsense. Це середовище дозволило моделювати різноманітні кіберзагрози в контрольованих умовах, що є критично важливим для дослідження та оцінки ефективності засобів захисту.

Було налаштовано систему виявлення вторгнень IDS Suricata на базі OPNsense, яка дозволила виявляти та аналізувати різні типи атак, зокрема DDoS-атаки, сканування портів, SQL-ін'єкції та brute-force атаки.

У процесі моделювання кіберзагроз було проведено серію атак на віртуальну машину Metasploitable VM з використанням інструментів Kali Linux. IDS Suricata успішно виявила та зафіксувала спроби сканування портів, brute-force атаки на сервіси FTP та Telnet, SQL-ін'єкції на веб-додаток Mutillidae, а також різні типи DDoS-атак, такі як Slowloris, ICMP Flood та HTTP Flood.

Важливою частиною роботи була оптимізація наборів правил для підвищення ефективності роботи IDS. Вибір і активація специфічних правил для кожного типу атак, що відповідають вразливостям Metasploitable VM, дозволила покрити більшість можливих сценаріїв експлуатації в цьому середовищі. Загальна кількість активних правил становила 2602, що враховує комплексний захист від різних типів атак. Такий підхід до оптимізації дозволив зменшити кількість хибних спрацювань та підвищити ефективність системи.

Результати дослідження підтвердили високу ефективність налаштованої системи IDS Suricata у виявленні та фіксації різних типів кіберзагроз. Це свідчить про доцільність використання таких систем у реальних мережах для підвищення рівня безпеки та оперативного реагування на потенційні загрози.

Таким чином, поставлені завдання були успішно виконані. Створене лабораторне середовище та налаштована система виявлення вторгнень можуть служити основою для подальших досліджень та впровадження передових методів захисту інформаційних систем та мереж. Отримані результати сприятимуть підвищенню рівня підготовки фахівців у сфері кібербезпеки та вдосконаленню існуючих засобів протидії сучасним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Types of network attacks against confidentiality, integrity and availability. Free Networking tutorials, System Administration Tutorials and Security Tutorials - omniseu.com. URL: <https://www.omniseu.com/ccna-security/types-of-network-attacks.php> (date of access: 12.11.2024).
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. 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.
4. Лупа, В., Горын, І., Zagorodna, N., Tymoshchuk, D., Lechachenko Т., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
5. Smurf DDoS attack. Cloudflare. URL: <https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/> (date of access: 12.11.2024).
6. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.
7. What is IP spoofing? URL: <https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/> (date of access: 12.11.2024).
8. MazeBolt | the IT guide to ddos: layer 4 – what you need to know (part 2). MazeBolt Technologies. URL: <https://mazebolt.com/blog/the-it-guide-to-ddos-layer-4-everything-you-need-to-know-part-2/> (date of access: 04.11.2024).
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. Іваночко, Н., Тимошук, В., Букатка, С., & Тимошук, 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.
11. 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).
12. Application layer DDoS attack. Cloudflare. URL: <https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/> (date of access: 04.11.2024).
13. HTTP flood attack. Cloudflare. URL: <https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/> (date of access: 04.11.2024).
14. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΟΓΟΣ», (August 16, 2024; Oxford, UK), 171-176.
15. R U Dead Yet? (R.U.D.Y.) attack. URL: <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/r-u-dead-yet-rudy/> (date of access: 04.11.2024).
16. Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. In CITI (pp. 250-256).
17. DNS amplification attack. URL: <https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/> (date of access: 04.11.2024).
18. Bomba, A., Lechachenko, T., & Nazaruk, M. (2021). Modeling the Dynamics of “Knowledge Potentials” of Agents Including the Stakeholder Requests. In Advances in Computer Science for Engineering and Education IV (pp. 75-88). Springer International Publishing.

19. What is a DDoS botnet? Cloudflare. URL: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/> (date of access: 04.11.2024).
20. Lindemulder G., Kosinski M. What Is a Man-in-the-Middle (MITM) Attack? | IBM. IBM - United States. URL: <https://www.ibm.com/think/topics/man-in-the-middle> (date of access: 12.11.2024).
21. 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 «ΛΟΓΟΣ», (December 13, 2024; Zurich, Switzerland), 232-237.
22. SQL injection | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-community/attacks/SQL_Injection (date of access: 12.11.2024).
23. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА ІМАР СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276
24. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
25. 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.
26. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. <https://doi.org/10.36074/grail-of-science.29.11.2024.081>

27. 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.
28. OPNsense documentation. URL: <https://docs.opnsense.org/> (date of access: 12.11.2024).
29. Metasploitable 2 | metasploit documentation. Docs @ Rapid7. URL: <https://docs.rapid7.com/metasploit/metasploitable-2> (date of access: 12.11.2024).
30. Derkach, M., Lysak, V., Skarga-Bandurova, I., & Kotsiuba, I. (2019, September). Parking Guide Service for Large Urban Areas. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 567-571). IEEE.
31. OWASP mutillidae II | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: <https://owasp.org/www-project-mutillidae-ii/> (date of access: 12.11.2024).
32. Kali docs | kali linux documentation. Kali Linux. URL: <https://www.kali.org/docs/> (date of access: 12.11.2024).
33. Suricata User Guide – Suricata 8.0.0-dev documentation. Suricata User Guide – Suricata 8.0.0-dev documentation. URL: <https://docs.suricata.io/en/latest/> (date of access: 12.11.2024).
34. Основи охорони праці: навчальний посібник / М. П. Купчі та ін. Київ: Основа, 2000. 416 с.
35. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.: ЕКОМЕН. 2011. 200 с.
36. Депутат О. П., Коваленко І. В., Мужик І. С. Цивільна оборона. Навчальний посібник. За редакцією полковника В.С. Франчука. Львів: Афіша. 2000. 336 с.

INDEX COPERNICUS
INTERNATIONAL

The issue of journal contains:

Proceedings of the VIII Correspondence
International Scientific and Practical Conference

GLOBALIZATION OF SCIENTIFIC KNOWLEDGE: INTERNATIONAL COOPERATION AND INTEGRATION OF SCIENCES

held on November 29th, 2024 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

№46
NOVEMBER, 2024

ISSN 2710-3056



**GRAIL OF
SCIENCE**

PERIODICAL SCIENTIFIC JOURNAL

INTERNATIONAL SCIENTIFIC JOURNAL

GRAIL OF SCIENCE

№ **46** (November, 2024)

with the proceedings of the:

VIII Correspondence International
Scientific and Practical Conference

**GLOBALIZATION OF SCIENTIFIC
KNOWLEDGE: INTERNATIONAL
COOPERATION AND INTEGRATION
OF SCIENCES**

held on November 29th, 2024 by

NGO European Scientific Platform
(Vinnytsia, Ukraine)
LLC International Centre Corporative
Management (Vienna, Austria)

МІЖНАРОДНИЙ НАУКОВИЙ ЖУРНАЛ

ГРААЛЬ НАУКИ

№ **46** (листопад, 2024)

за матеріалами:

VIII Міжнародної науково-
практичної конференції

**ГЛОБАЛІЗАЦІЯ НАУКОВОГО
ЗНАННЯ: МІЖНАРОДНЕ
СПІВРОБІТНИЦТВО ТА
ІНТЕГРАЦІЯ НАУК**

що проводилася 29.11.2024

ГО «Європейська наукова
платформа» (Вінниця, Україна)
ТОВ «International Centre Corporative
Management» (Відень, Австрія)



Вінниця – Відень, 2024

DOI 10.36074/grail-of-science.29.11.2024

ГРААЛЬ НАУКИ : міжнар. наук. журнал. – Вінниця : ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2024. – No 46. – 1036 с.

Видання розраховане на науковців, викладачів, аспірантів, студентів, усіх, хто прагне отримати ґрунтовні знання теоретичного і прикладного характеру.

**Рекомендовано до видання Вченою Радою Наукової установи
«Інститут науково-технічної інтеграції та співпраці». Протокол № 64 від 28.11.2024.**

Головний редактор: Танасійчук Альона Миколаївна, д-р. екон. наук, доцент (Україна)
Заступник головного редактора: Ємельянов Олександр Юрійович, д-р. екон. наук, професор (Україна)
Голова оргкомітету конференції: Голденблат Марія (Україна)
Заступник голови оргкомітету конференції: Рейчел Апаро (Австрійська Республіка)
Відповідальний секретар: Рабей Настасія Романівна (Україна)

ЧЛЕНИ РЕДАКЦІЙНОЇ КОЛЕГІЇ:

Квасницька Раїса Степанівна - д-р. екон. наук, професор (Україна); Jakhongir Shaturaev - канд. екон. наук, доцент (Республіка Узбекистан); Бойко Світлана Василівна - канд. екон. наук, доцент (Україна); Заднепровська Ганна Ігорівна - канд. екон. наук (Україна); Занора Володимир Олександрович - канд. екон. наук, доцент (Україна); Маркович Ірина Богданівна - канд. екон. наук, доцент (Україна); Яковенко Роман Валерійович - канд. екон. наук, доцент (Україна); Поливана Людмила Анатоліївна - канд. екон. наук, доцент (Україна); Гевчук Анна Вікторівна - д-р. екон. наук, професор (Україна); Маслій Олександра Анатоліївна - канд. екон. наук, доцент (Україна); Євтушенко Наталія Миколаївна - канд. екон. наук, доцент (Україна); Москвічова Олена Сергіївна - канд. екон. наук, доцент (Україна); Ясишена Валентина Валеріївна - д-р. екон. наук, професор (Україна); Михайлишин Лілія Іванівна - д-р. екон. наук, професор (Україна); Гавриленко Наталія Вікторівна - канд. екон. наук, доцент (Україна); Гіулі Гігуашвілі - д-р. екон. наук, професор (Грузія).

НАУКОВІ КОНСУЛЬТАНТИ:

Онїкієнко Сергій Володимирович - д-р. екон. наук, професор (Україна); Marko Timchev - д-р. екон. наук, доцент (Республіка Болгарія); Khatuna Tabagari - д-р. екон. наук, професор (Сакартвело); Грень Лариса Миколаївна - д-р. наук з держ. управління, професор (Україна); Михаліцька Наталія Ярославівна - канд. наук з держ. управління, доцент (Україна); Ткаченко Павло Ігорович - аспірант (Україна); Купріянова Дарина Сергіївна - практикуючий юрист (Польща); Губаль Галина Миколаївна - канд. фіз.-мат. наук, доцент (Україна); Козуб Галина Олександрівна - канд. техн. наук, доцент (Україна); Козьма Антон Антонович - канд. хім. наук (Україна); Морозова Тетяна Василівна - канд. біол. наук, доцент (Україна); Купріянова Лариса Сергіївна - канд. мед. наук, доцент (Україна); Лисенко Дмитро Андрійович - канд. мед. наук, доцент (Україна); Цубанова Наталія Анатоліївна - д-р. фарм. наук, професор (Україна); Олійник Світлана Валентинівна - канд. фарм. наук, доцент (Україна); Полежаєв Юрій Григорович - канд. наук із соц. ком., доцент (Україна); Mikhabbat Khakimova - д-р. пед. наук, професор (Республіка Узбекистан); Куліченко Алла Костянтинівна - д-р. пед. наук, доцент (Україна); Фурман Тарас Юрійович - канд. пед. наук, доцент (Україна); Бажан Станіслав Миколайович - д-р. філософії (Україна); Ямполь Юрій Віталійович - аспірант (Україна); Антипова Жанна Ігорівна - старший викладач (Україна); Яцик Мар'яна Романівна - канд. пед. наук, доцент (Україна); Корбозерова Ніна Миколаївна - д-р. філол. наук, професор (Україна); Ковальська Наталія Аркадіївна - канд. філол. наук, доцент (Україна); Мелех Галина Богданівна - канд. філол. наук, доцент (Україна); Присяжнюк Оксана Ярославівна - канд. філол. наук, доцент (Україна); Фомін Андрій Володимирович - канд. іст. наук, доцент (Україна); Гірна Наталія Мирославівна - канд. іст. наук, доцент (Україна); Устїнова Ірина Ігорівна - д-р. арх., професор (Україна); Катерина Діденко - канд. арх. (Україна); Воскобойнікова Юлія Василівна - д-р. мист. (Україна); Крипчук Микола Володимирович - канд. мист., доцент (Україна); Лугова Тетяна Анатоліївна - канд. мист., доцент (Україна)

Верстальник: Білоус Тетяна (Україна). **Дизайнер:** Казьміна Надія (Україна). **Коректор:** Дудник Григорій (Україна).

«Грааль науки» є офіційно зареєстрованим мультидисциплінарним науковим виданням з міжнародною сферою поширення, що підтримує політику відкритого доступу. **Ідентифікатор медіа R30-02704** (рішення № 430 від 22.02.2024 Національної Ради України з питань телебачення і радіомовлення).

Наказом МОН України № 582 від 24.04.2024 виданню «Грааль науки» присвоєно Категорію Б фахових видань України з питань економіки (051 «Економіка»).

«Грааль науки» індексується в міжнародних реферативних та наукометричних базах даних: Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

Конференція зареєстрована УкрІНТЕІ (Посвідчення № 371 від 12.06.2024) та сертифікована Euro Science Certification Group (Сертифікат № 22689 від 21.10.2024).

За точність викладених фактів та коректність цитування відповідальність несе автор.



© Автори статей, 2024
© ГО «Європейська наукова платформа», 2024
© НУ «Інститут науково-технічної інтеграції та співпраці», 2024
© LLC «International Centre Corporative Management», 2024

DOI 10.36074/grail-of-science.29.11.2024

GRAIL OF SCIENCE : inter. scientific journal. – Vinnytsia : NGO «European Scientific Platform»; SI «Institute of Scientific and Technical Integration and Cooperation», 2024. – No 46. – 1036 p.

The publication is intended for scientists, teachers, graduate students, students, all those who seek to obtain thorough knowledge of a theoretical and applied nature.

Recommended for publication by the Academic Council of the Institute of Scientific and Technical Integration and Cooperation. Protocol № 64 from November 28, 2024.

Editor-in-chief: Alona Tanasiichuk, D.Sc. in Economics, Associate professor (Ukraine)
Deputy editor-in-chief: Olexandr Yemelyanov, D.Sc. in Economics, Professor (Ukraine)
Chairman of the Organizing Committee: Miriam Goldenblat (Ukraine)
Deputy Chairman of the Organizing Committee: Rachael Aparo (Austria)
Responsible secretary: Nastasiia Rabei (Ukraine)

EDITORIAL BOARD:

Raisa Kvasnytska - D.Sc. in Economics, Professor (Ukraine); **Jakhongir Shaturaev** - Ph.D. in Economics, Associate professor (Republic of Uzbekistan); **Svitlana Boiko** - Ph.D. in Economics, Associate professor (Ukraine); **Hanna Zadnieprovskia** - Ph.D. in Economics (Ukraine); **Volodymyr Zanora** - Ph.D. in Economics, Associate professor (Ukraine); **Iryna Markovych** - Ph.D. in Economics, Associate professor (Ukraine); **Roman Yakovenko** - Ph.D. in Economics, Associate professor (Ukraine); **Liudmyla Polyvana** - Ph.D. in Economics, Associate professor (Ukraine); **Anna Hevchuk** - D.Sc. in Economics, Professor (Ukraine); **Oleksandra Maslii** - Ph.D. in Economics, Associate professor (Ukraine); **Nataliia Yevtushenko** - Ph.D. in Economics, Associate professor (Ukraine); **Olena Moskvichova** - Ph.D. in Economics, Associate professor (Ukraine); **Valentyna Yasyshena** - D.Sc. in Economics, Professor (Ukraine); **Liliia Mykhailyshyn** - D.Sc. in Economics, Professor (Ukraine); **Nataliia Havrylenko** - Ph.D. in Economics, Associate professor (Ukraine); **Giuli Giguashvili** - D.Sc. in Economics, Professor (Georgia).

EDITORIAL CONSULTANTS:

Serhii Onikiienko - D.Sc. in Economics, Professor (Ukraine); **Khatuna Tabagari** - D.Sc. in Economics, Professor (Georgia); **Marko Timchev** - D.Sc. in Economics, Associate professor (Republic of Bulgaria); **Larysa Hren** - D.Sc. in Public administration, Professor (Ukraine); **Nataliia Mykhalitska** - Ph.D. in Public administration, Associate professor (Ukraine); **Pavlo Tkachenko** - Ph.D. student (Ukraine); **Daryna Kupriianova** - lawyer (Republic of Poland); **Halyna Hubal** - Ph.D. in Physics and Maths, Associate professor (Ukraine); **Halyna Kozub** - Ph.D. in Technical sciences, Associate professor (Ukraine); **Anton Kozma** - Ph.D. in Chemistry (Ukraine); **Tetiana Morozova** - Ph.D. in Biology, Associate professor (Ukraine); **Larysa Kupriianova** - Ph.D. in Medicine, Associate professor (Ukraine); **Dmytro Lysenko** - Ph.D. in Medicine, Associate professor (Ukraine); **Natalia Tsubanova** - D.Sc. in Pharmacy, Professor (Ukraine); **Svitlana Oliinyk** - Ph.D. in Pharmacy, Associate professor (Ukraine); **Yuriy Polyzhahayev** - Ph.D. in Social Communications, Associate professor (Ukraine); **Mukhabbat Khakimova** - D.Sc. in Pedagogy, Professor (Republic of Uzbekistan); **Alla Kulichenko** - D.Sc. in Pedagogy, Associate professor (Ukraine); **Taras Furman** - Ph.D. in Pedagogy, Associate professor (Ukraine); **Stanislav Bazhan** - Doctor of Philosophy (Ukraine); **Yurii Yampol** - Ph.D. student (Ukraine); **Zhanna Antypova** - Senior Lecturer (Ukraine); **Yatsyk Mariana** - Ph.D. in Pedagogy, Associate professor (Ukraine); **Nina Korbozerova** - D.Sc. in Philology, Professor (Ukraine); **Natalia Kovalska** - Ph.D. in Philology, Associate professor (Ukraine); **Oksana Prysiazhniuk** - Ph.D. in Philology, Associate professor (Ukraine); **Melekh Halyna** - Ph.D. in Philology, Associate professor (Ukraine); **Anatolii Kornus** - Ph.D. in Geography, Associate professor (Ukraine); **Andrii Fomin** - Ph.D. in History, Associate professor (Ukraine); **Nataliia Hirna** - Ph.D. in History, Associate professor (Ukraine); **Iryna Ustinova** - D.Sc. in Architecture, Professor (Ukraine); **Kateryna Didenko** - Ph.D. in Architecture (Ukraine); **Yuliia Voskoboinikova** - D.Sc. in Arts (Ukraine); **Mykola Krypchuk** - Ph.D. in Arts, Associate professor (Ukraine); **Tetiana Luhova** - Ph.D. in Arts, Associate professor (Ukraine)

Responsible for e-layout: Tetiana Bilous (Ukraine). **Designer:** Nadiia Kazmina (Ukraine). **Proofreader:** Hryhorii Dudnyk (Ukraine).

The journal «Grail of Science» is an officially registered in Ukraine multidisciplinary and internationally disseminated scientific edition that supports the policy of open access for scientific publications. **Media identifier R30-02704** (decision № 430 dated 22.02.2024 of the National Council of Ukraine on Television and Radio Broadcasting).

By order of the Ministry of Education and Culture of Ukraine № 582 of April 24, 2024, the journal «Grail of Science» was assigned Category B of specialized publications of Ukraine on economics (051 «Economics»).

The journal «Grail of Science» is indexed in international reference and scientometric databases:

Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

The conference is approved by UKRISTEI (Certificate № 371 dated June 12th, 2024) and certified by Euro Science Certification Group (Certificate № 22689 dated October 21st, 2024).

The author is responsible for the accuracy of the facts presented and the correctness of citations.



© Authors of articles, 2024
 © NGO «European Scientific Platform», 2024
 © SI «Institute of Scientific and Technical Integration and Cooperation», 2024
 © LLC «International Centre Corporative Management», 2024



DOI 10.36074/grail-of-science.29.11.2024.081

MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS

SCIENTIFIC RESEARCH GROUP:

Vitaliy Tymoshchuk 

First-level student of higher education

Faculty of Applied Information Technologies and Electrical Engineering

Ternopil Ivan Puluj National Technical University, Ukraine

Vladyslav Pakhoda

Second-level student of higher education

Faculty of Computer Information Systems and Software Engineering

Ternopil Ivan Puluj National Technical University, Ukraine

Andrii Dolinskyi 

Third-level student of higher education

Faculty of Computer Information Systems and Software Engineering

Ternopil Ivan Puluj National Technical University, Ukraine

Andrii Karnaukhov 

Third-level student of higher education

Faculty of Computer Information Systems and Software Engineering

Ternopil Ivan Puluj National Technical University, Ukraine

Dmytro Tymoshchuk 

Senior lecturer at the Department of Cyber Security

Ternopil Ivan Puluj National Technical University, Ukraine

Summary. Cyber threats are becoming increasingly complex and diverse, which requires improved approaches to their detection. This article is devoted to modelling cyber threats, optimising the number of rules of an IDS system, and evaluating its effectiveness. The classification of modern cyberattacks, their implementation features and consequences are considered. A test environment for modelling attacks is created. The IDS Suricata was configured and the number of active rules was optimised, which reduced the load on the system and minimised false positives. The effectiveness of IDS Suricata in detecting various types of attacks was evaluated. The study results demonstrated the high efficiency of IDS Suricata in detecting cyber threats.

Keywords: Cyber threats; IDS; Suricata; attack modelling; cybersecurity.

Introduction. With the development of information technology, cyber threats are becoming more complex and diverse, posing serious challenges to the security of



information systems and networks. Cybercriminals are using the latest methods and tools to carry out attacks aimed at compromising the confidentiality, integrity and availability of data. This requires continuous improvement of threat detection tools.

Cyber threats are classified according to various criteria, including the mechanism of action: denial of service (DoS/DDoS) attacks, which are aimed at disabling services; privacy attacks, such as phishing, traffic interception and data theft; and integrity attacks, which include the alteration or destruction of information through the introduction of malware or ransomware [1].

Intrusion detection systems (IDS) play a key role in ensuring the security of network infrastructures [2]. They allow us to monitor network traffic, detect anomalies and potential attacks in real time, which is critical for timely response to threats. One of the most popular open source IDSs is Suricata, which supports multi-threaded processing and has advanced traffic analysis capabilities [3]. Previous studies show that proper configuration and optimisation of IDS rules are critical to improving their effectiveness. For example, using specific rules to detect certain types of attacks can significantly reduce the number of false positives and increase detection accuracy. Simulating cyber threats in a controlled environment allows us to evaluate the effectiveness of an IDS and improve protection strategies.

The aim of this study is to model different types of cyber threats and evaluate the effectiveness of IDS systems with an optimised number of rules.

Methodology. To achieve the research goal, a comprehensive approach was developed, including the creation of a test laboratory environment, setting up the IDS Suricata intrusion detection system with an optimised number of rules, and modelling various types of cyber threats to assess the effectiveness of the IDS. The research methodology was based on the practical application of cybersecurity tools and analysis of their interaction in a controlled environment.

First, we created a test laboratory environment based on the KVM hypervisor, which is one of the most popular open source virtualisation tools [4,5] (Fig. 1).

The KVM hypervisor allowed the deployment of multiple virtual machines on a single physical platform, ensuring the isolation and independence of each system [6]. The virtual machines were configured to simulate a real network infrastructure with the ability to model various types of attacks.

One of the key components of the environment was the Metasploitable VM, a vulnerable virtual machine specially designed for training and penetration testing purposes [7]. It contains intentionally vulnerable services and applications, such as old versions of FTP servers, SSH, web servers with known vulnerabilities, and other components that allow for research and exploitation. This makes it possible to realistically simulate attacks and analyse their impact on the system. Using Metasploitable VM provides a platform for testing the effectiveness of IDS in detecting known vulnerabilities and exploits.

To simulate the actions of a potential attacker, we used the Kali Linux operating system, which is specially designed for penetration testing and security assessment [8]. Kali Linux contains a wide range of pre-installed tools, including nmap, hydra, sqlmap, and many others, which are used by cybersecurity professionals to identify vulnerabilities, conduct attacks, and analyse network traffic. Kali Linux was used in the

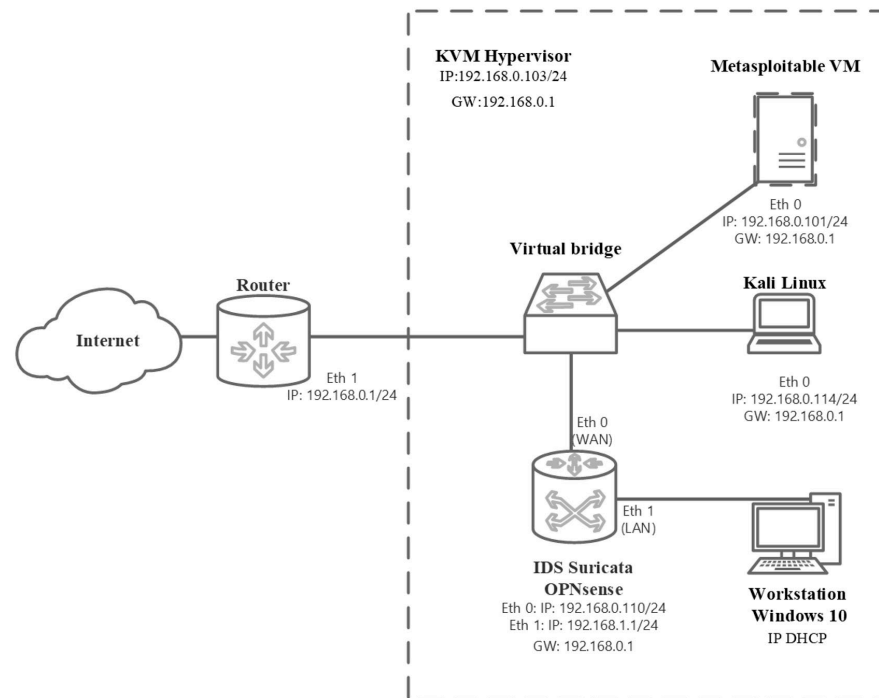


Fig. 1. Scheme of the laboratory environment

study to simulate various types of attacks on the Metasploitable VM and evaluate the response of the intrusion detection system. This contributed to the creation of realistic scenarios that reflect the actions of attackers in real life.

The OPNsense platform with integrated Suricata IDS was used to monitor network traffic and identify potential threats. OPNsense is an open-source firewall and network security platform that provides routing, traffic filtering, and other security features [9]. The integration of Suricata IDS into OPNsense allowed us to monitor network traffic, detect anomalies and potential threats in real time.

The network environment was configured in such a way as to ensure interaction between all components. All virtual machines were placed on the same subnet with corresponding IP addresses, which simplified the configuration and monitoring process. This allowed Kali Linux to launch attacks on the Metasploitable VM, and Suricata IDS to analyse traffic between these machines and identify potential threats. This configuration created conditions that were as close as possible to real network environments where cyber threats can occur.

After setting up the environment, the Suricata IDS was configured. We downloaded the current rule sets, which contained rules for detecting various types of attacks. Particular attention was paid to selecting specific rules that corresponded to the types of attacks that were planned for modelling. Rules were activated to detect DDoS attacks [10,11,12], port scanning, SQL injections [13], and brute-force attacks [14]. This allowed us to focus the IDS on the most relevant threats for a given environment and increase detection efficiency. The number of active rules was optimised to 2602, which reduced the system load and minimised the number of



false positives. The next step was to model cyber threats. Using the Kali Linux tools, a number of attacks were carried out on the Metasploitable VM, including port scans, brute-force attacks, SQL injections, and DDoS attacks. The port scan with nmap collected information about open ports and active services on the Metasploitable VM, which is a typical preparatory step for further attacks. Brute-force attacks on FTP and Telnet services using hydra were aimed at guessing passwords and gaining unauthorised access to the system. The use of sqlmap to perform SQL injections on the Mutillidae web application allowed to exploit vulnerabilities and attempt to gain access to confidential database data. DDoS attacks such as Slowloris, ICMP Flood, and HTTP Flood were aimed at overloading the system and testing the ability of Suricata IDS to detect availability attacks.

During the attacks, Suricata IDS analysed network traffic, applying activated rules to detect suspicious activity. In the process of simulating attacks, we closely monitored the IDS response, alert registration, and their accuracy. This allowed us to assess how effectively the system detects different types of attacks and whether it provides enough information to respond. To evaluate the effectiveness of Suricata's IDS, criteria were established that included the ability to detect and record an attack, the accuracy of alerts, the absence of false positives, and the speed of response. The IDS event logs were analysed to check whether attacks were correctly identified and whether the system provided sufficiently detailed information about incidents. Particular attention was paid to analysing alerts to ensure that they corresponded to real events and that they allowed for quick decision-making based on the information received.

Discussion. The results of the study demonstrate the high efficiency of the IDS Suricata system in detecting various cyber threats in the test environment. When simulating attacks on a vulnerable Metasploitable VM system using Kali Linux, IDS Suricata was able to detect port scans, brute-force attacks, SQL injections, and various types of DDoS attacks in a timely manner. This proves that with proper configuration and rule optimisation, Suricata can be an effective tool for network security.

One of the key factors in the successful detection of attacks was the correct configuration of the IDS system and careful selection of active rules. Activation of specific rules that correspond to potential threats in a particular environment helped reduce the number of false positives and improve detection accuracy. For example, to detect SQL injections, rules were activated that analyse HTTP traffic for the presence of characteristic signs of this attack. This ensured timely notification of attempts to exploit web application vulnerabilities. Additionally, using up-to-date rule sets such as Emerging Threats helped to identify the latest threats and exploits that are constantly emerging in cyberspace. Regularly updating these rules is critical, as it allows the IDS to keep abreast of the latest attack methods and respond to them effectively.

Modelling cyber threats in a controlled environment has confirmed the need for regular testing and evaluation of security measures. This approach helps to identify potential weaknesses in the security system, as well as to check the effectiveness of existing mechanisms for detecting and responding to threats. In addition, it enables network administrators to better understand the behaviour of the IDS system and optimise its settings for the specifics of their own network.

It is important to note that Suricata IDS has demonstrated the ability to efficiently handle large volumes of traffic and detect attacks that use multi-threaded



methods, such as DDoS attacks. This is especially true in today's environment, when attackers are increasingly using distributed botnet networks to launch massive attacks on resources. Suricata, thanks to its multi-threaded architecture, can scale and provide a high level of performance even under heavy load.

However, it should be borne in mind that the results obtained in the test environment may differ from real-world conditions. In real-world networks, network traffic is much more complex and heterogeneous, with encrypted data, VPNs, and other factors that make traffic analysis more difficult. In addition, attackers are constantly evolving their methods, using zero-day attacks and other techniques that can be difficult to detect with traditional IDS. Another limitation is the possibility of false positives, which can lead to an administrator being overwhelmed by a large number of alerts and, as a result, missing important events. Therefore, it is important not only to configure IDS rules, but also to regularly analyse event logs, train staff, and implement additional means of correlating and filtering alerts.

Conclusions. The study confirms the high efficiency of the Suricata IDS system in detecting various types of cyber threats. Attack simulations have shown that Suricata is able to identify threats in a timely manner and warn administrators of potential dangers. To maintain effective IDS operation, it is recommended to:

- regularly update the rule sets and adapt them to the specifics of the network, which will help identify new threats and reduce the number of false positives;
- periodically test and simulate attacks in a controlled environment to evaluate the effectiveness of security measures and identify possible vulnerabilities;
- improve IDS settings based on network characteristics and typical threats, which will increase system performance and detection accuracy.

Given the growing sophistication of cyber threats, the use of effective IDS is essential to ensure the security of information systems and networks.

References:

- [1] Types of network attacks against confidentiality, integrity and availability. (n.d.). Free Networking tutorials, System Administration Tutorials and Security Tutorials - omniseu.com. <https://www.omniseu.com/ccna-security/types-of-network-attacks.php>
- [2] What is intrusion detection systems (IDS)? How does it work? | fortinet. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system>
- [3] Suricata User Guide — Suricata 8.0.0-dev documentation. (n.d.). Suricata User Guide — Suricata 8.0.0-dev documentation. <https://docs.suricata.io/en/latest/>
- [4] 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>
- [5] Тимошук, В., Долінський, А., & Тимошук, 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>
- [6] KVM user's guide. (2020, 19 june). Oracle Help Center. <https://docs.oracle.com/en/operating-systems/oracle-linux/kvm-user/kvm-AboutOracleLinuxKVM.html>
- [7] Metasploitable 2 | metasploit documentation. (n.d.). Docs @ Rapid7. <https://docs.rapid7.com/metasploit/metasploitable-2>
- [8] Kali docs | kali linux documentation. (n.d.). Kali Linux. <https://www.kali.org/docs/>



[9] OPNsense documentation. (n.d.). <https://docs.opnsense.org/>

[10] Іваночко, Н., Тимошук, В., Букатка, С., & Тимошук, 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.

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

[12] Tymoshchuk, D., & Yatskiv, V. (2024). SLOWLORIS DDOS DETECTION AND PREVENTION IN REAL-TIME. Collection of scientific papers «ΛΟΓΟΣ», (August 16, 2024; Oxford, UK), 171-176. <https://doi.org/10.36074/logos-16.08.2024.036>

[13] SQL injection | OWASP foundation. (n.d.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-community/attacks/SQL_Injection

[14] What is a brute force attack? | definition, types & how it works. (n.d.).Fortinet. <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>

МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ ВІЯВЛЕННЯ ВТОРГНЕНЬ

НАУКОВО-ДОСЛІДНА ГРУПА:

Тимошук Віталій Дмитрович

здобувач першого рівня вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Пахода Владислав Юрійович

здобувач другого рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Долінський Андрій Михайлович

здобувач третього рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Карнаухов Андрій Костянтинович

здобувач третього рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Тимошук Дмитро Іванович

старший викладач кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Анотація. Кіберзагрози набувають усе більшої складності та різноманітності, що вимагає вдосконалення підходів до їх виявлення. Ця стаття присвячена моделюванню кіберзагроз, оптимізації кількості правил системи IDS та оцінці її ефективності. Розглянуто класифікацію сучасних кібератак, особливості їх реалізації та наслідки. Створено тестове середовище для моделювання атак, проведено налаштування IDS Suricata, здійснено оптимізацію кількості активних правил, що зменшило навантаження на систему та мінімізувало хибні спрацювання. Оцінено ефективність IDS Suricata у виявленні різних типів атак. Результати дослідження продемонстрували високу ефективність IDS Suricata у виявленні кіберзагроз.

Ключові слова: Кіберзагрози; IDS; Suricata; моделювання атак; кібербезпека.