Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Назарчука Валерія Сергійовича

на здобуття ступеня вищої освіти Бакалавра

Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атак на кінцеві пристрої

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.2101022.20.01.15 ПЗ

Виконав студент 4 курсу група КБ-20-1 Валерій НАЗАРЧУК
Керівник канд. техн. наук, доцент Вікторія ОРЛЕНКО
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

10 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Назарчуку Валерію Сергійовичу

1 Тема роботи Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атак на кінцеві пристрої

Керівник роботи к.т.н. доцент Вікторія ОРЛЕНКО

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи Проаналізувати існуючі рішення організації кіберполігонів для навчання здобувачів та фахівців з кібербезпеки. Підібрати оптимальні варіанти апаратної складової. Прописати перелік ролей користувачів кіберполігону із переліком можливостей. Інсталювати та налаштувати програмні продукти, які потрібні для виконання різноманітних завдань при роботі. Проведення тестування кіберполігону задля перевірки наявності витоків атак із мережі полігону назовні.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Роль кіберполігону для дослідження кібердій. Огляд існуючих рішень полігонів. Постановка задачі. Параметри та налаштування кіберполігону. Опис апаратної складової. Опис програмної складової. Політики безпеки. Розгортання кіберполігону. Схема мережі. Операційні системи. Забезпечення відмовостійкості. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схеми з'єднання центральних комутуючих вузлів та підключення навчальних аудиторій до мережі. Схема підключення пристроїв в навчальній аудиторії до комп'ютерної мережі. Алгоритм роботи кіберполігону при імітації атак

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Валерій НАЗАРЧУК

Керівник кваліфікаційної роботи Вікторія ОРЛЕНКО

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої»

Автор роботи: студент групи КБ–20–1 Назарчук В.С.

Керівник роботи: к.т.н. доц. Орленко В.С.

Пояснювальна записка: 63с., 19 рисунки, 5 таблиць, 42 джерел, 3 креслення.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: КІБЕРПОЛІГОН, АТАКА, КОМП'ЮТЕРНА МЕРЕЖА, ПОЛІТИКА БЕЗПЕКИ, МОНІТОРИНГ МЕРЕЖЕВОГО ТРАФІКУ.

Завданням даної роботи є розробка кіберполігону для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої, який буде активно використовуватися для практичного навчання здобувачів спеціальності 125 Кібербезпека та захист інформації. Під час виконання завдання було: налаштовано апаратну складову та створено віртуальне середовище для імітації атак; налаштовано системи збору мережевого трафіку для реєстрації активності під час атак на кінцеві пристрої; інстальовано та налаштовано програмні продукти для аналізу мережевого трафіку та імітації атак, налаштування систем захисту; формування політики безпеки для користувачів кіберполігону. Також проведено дослідження для перевірки ефективності розроблених заходів захисту та алгоритмів виявлення атак без витоку зловмисного трафіку на зовні.

При розгортанні полігону було забезпечено контрольоване середовище кіберполігону для дослідження мережевого трафіку під час атаки чи захисту, що проводиться, та ізоляцію від інших комп'ютерних мереж.

10.06.2024

ABSTRACT

Topic of the qualification work: "Cyber polygon for network traffic research using monitoring tools during endpoint attacks"

Author: student of group KB-20-1, Nazarchuk V. S.

Supervisor: Ph.D., Associate Professor Orlenko V. S.

Explanatory note: 63 pages, 19 figures, 5 tables, 42 sources, 3 diagrams.

LIST OF KEYWORDS: CYBER RANGE, ATTACK, COMPUTER NETWORK, SECURITY POLICY, NETWORK TRAFFIC MONITORING.

The objective of this work is to develop a cyber polygon for network traffic research using monitoring tools during endpoint attacks, which will be actively utilized for practical training of students specializing in Cybersecurity and Information Protection (specialty 125). During the task execution, the following were accomplished: configuration of hardware components and creation of a virtual environment for simulating attacks; setup of systems for collecting network traffic to record activity during attacks on endpoint devices; installation and configuration of software products for analyzing network traffic, simulating attacks, and configuring security systems; formulation of a security policy for cyber range users. Additionally, research was conducted to verify the effectiveness of the developed protective measures and attack detection algorithms without the leakage of malicious traffic outside.

During the deployment of the cyber range, a controlled environment was ensured for studying network traffic during attacks or defensive measures being conducted, with isolation from other computer networks.

10.06.2024

ЗМІСТ

ВСТУП

Із зростанням кількості залучених людей та компаній до цифрових технологій збільшується також обсяг кіберзлочинності, а кіберзлочинці постійно шукають нові шляхи вторгнення в системи та використання вразливостей. Тенденція на використання IoT пристроїв призвела до суттєвого збільшення підключених IoT пристроїв до мережі, таких як роутери, камери спостереження, домашні асистенти тощо, що робить їх мішенню для несанкціонованого доступу. Кіберзлочинці все частіше використовують соціальну інженерію для отримання доступу до систем, використовуючи фішингові атаки, відправляючи шкідливі посилання через електронну пошту, соціальні мережі тощо. А використання штучного інтелекту і машинного навчання в кібератаках дає змогу автоматизувати атаки та коригувати їх відповідно до типу захисту, що робить їх складнішими для виявлення та відновлення.

Великі компанії та установи є потенційними жертвами кіберзлочинців через великий обсяг конфіденційної інформації, яку вони зберігають, та наявність комерційних чи державних таємниць. Проблеми захисту таких підприємств спричинені розмірами інфраструктури та її складністю в реалізації. До головних проблем забезпечення надійного захисту даних можна віднести:

- некоректне налаштування систем виявлення вразливостей та вторгнень;
- велика кількість різноманітного програмного забезпечення, яке може містити вразливості та потребує регулярних оновлень;
- велика кількість різних працівників полегшує реалізацію атак із використанням соціальної інженерії;
- велика кількість ролей може спричинити недостатній контроль над привілеями доступу, що в свою чергу може призвести до неправомірного використання або зловживання доступом, яке може бути використане хакерами;
- недостатній моніторинг систем та недостатність процедур для виявлення та реагування на кіберінциденти можуть призвести до того, що атаки залишаться непоміченими або не будуть вчасно зупинені.

Для боротьби з загрозами та запобіганню типових проблем, рекомендується використовувати комплексний підхід до кібербезпеки, який включає в себе застосування технологічних заходів безпеки, навчання персоналу, регулярне оновлення програмного забезпечення та захисту, а також регулярні аудити та тестування на проникнення.

Саме тому набуває актуальності питання створення спеціального середовища, яке буде використовуватися для тренування та тестування заходів кібербезпеки. Основна мета кіберполігону полягає в навчанні персоналу з питань кібербезпеки та вдосконаленні заходів захисту інформації. Деякі з основних призначень використання кіберполігону:

– дозволяє проводити тренувальні сесії для персоналу, включаючи адміністраторів мереж, аналітиків кібербезпеки та інших зацікавлених сторін. Персонал може вивчати реальні кібератаки та виконувати практичні вправи з виявлення та реагування на інциденти;

– дозволяють організаціям тестувати свої системи та заходи безпеки на відповідність, виявляти потенційні вразливості та оцінювати ефективність заходів захисту перед тим, як вони будуть впроваджені в реальному середовищі;

– можна моделювати різноманітні сценарії кібератак для вивчення їх впливу та розвитку стратегій для їх запобігання та виявлення;

– є середовищем для випробування нових технологій та інструментів в області кібербезпеки перед їх впровадженням у реальних умовах..

У загальному, кіберполігони відіграють важливу роль у підвищенні кібербезпеки шляхом підготовки персоналу, тестування заходів безпеки та вивчення реальних кіберзагроз. Тому метою даної роботи є розробка кіберполігону для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої, який буде активно використовуватися для практичного навчання здобувачів спеціальності 125 Кібербезпека, 125 Кібербезпека та захист інформації.

1 РОЛЬ КІБЕРПОЛІГОНУ ДЛЯ ДОСЛІДЖЕННЯ КІБЕРДІЙ

1.1 Роль кінцевих пристроїв у безпеці мережі

Для багатьох організацій різних сфер діяльності стає все актуальнішою проблема можливості зіткнення з цілеспрямованими атаками, які все частіше використовують комбінацію поширених загроз, вразливостей "нульового дня", унікальних схем без використання шкідливого програмного забезпечення, методів без файлів та інших. Використання рішень, що ґрунтуються на превентивних технологіях, а також систем, спрямованих лише на виявлення складних шкідливих активностей в мережевому трафіку, не може бути достатнім для захисту підприємства від складно структурних цілеспрямованих атак. Кінцеві точки, такі як робочі станції, ноутбуки, сервери та смартфони, також є критично важливими об'єктами контролю, оскільки вони залишаються досить простими та популярними точками проникнення для зловмисників, що підвищує значимість контролю за ними.

Кінцеві точки - це фізичні пристрої, що підключаються до комп'ютерної мережі та обмінюються з нею даними, такі як мобільні пристрої, настільні комп'ютери, вбудована техніка або сервери [1-2]. До них також відносяться пристрої Інтернету речей, наприклад, камери, світильники, холодильники, системи безпеки, розумні колонки та термостати. Кіберзлочинці обирають кінцеві точки для атак, оскільки вони дають доступ до корпоративних даних і за своєю природою вразливі.

З ростом мобільності робочих ресурсів організації стають все більш вразливими до атак на кінцеві точки. Нижче наведено деякі поширені загрози безпеці кінцевих точок:

– фішинг - вид атаки з використанням соціотехніки, метою якої є отримання від жертви конфіденційної інформації [3-4];

– програми-вимагачі - шкідливе програмне забезпечення, яке блокує доступ

до інформації жертви до сплати викупу [5];

– втрата пристроїв - одна з основних причин порушення безпеки корпоративних даних. Втрата та крадіжка пристроїв також може мати серйозні фінансові наслідки з боку регулюючих органів;

– застарілі патчі - через це в системах можуть виникати вразливості, через які зловмисники можуть отримати доступ до даних та їх вкрасти [6];

– шкідлива реклама - інтернет-оголошення, через які поширюються шкідливі програми та відбувається злом систем;

– приховане завантаження - автоматичне завантаження програм на пристрій без відома користувача;

– моніторинг активності користувачів;

– крадіжка облікових даних для входу;

– поширення програм-вимагачів та іншого шкідливого програмного забезпечення;

– отримання точки входу до мережі організації.

Виявлення та реагування на атаки на кінцеві точки (EDR) - це загальний термін для програмного рішення, яке постійно відслідковує кінцеві пристрої, такі як комп'ютери та ноутбуки користувачів, сервери, мобільні пристрої та пристрої Інтернету речей (IoT), для збору та аналізу даних про загрози та сповіщення фахівців з безпеки про порушення в реальному часі [7-8].

Оскільки термін EDR є досить широким, конкретні функції та можливості окремих рішень EDR значно відрізняються залежно від постачальників і навіть реалізацій. Загалом, засоби виявлення та реагування на атаки на кінцеві точки потрапляють в одну з наступних трьох категорій:

– спеціальна платформа EDR;

– набір інструментів, які спільно використовуються для виявлення та реагування на атаки на кінцеві точки;

– функціональність EDR, вбудована в інший продукт безпеки, наприклад, антивірусне програмне забезпечення нового покоління. Деякі постачальники рішень для управління інформаційною безпекою та подіями безпеки (SIEM)

пропонують EDR як частину своїх пакетів.

EDR допомагає виявляти загрози, які ухиляються від AV або NGAV. Під час моніторингу через платформу безпеки та аналітику, керовану штучним інтелектом, EDR може надавати дієві рекомендації щодо виправлення. Інструменти та рішення EDR спрямовані на забезпечення необхідної видимості для виявлення, дослідження та пом'якшення потенційних загроз.

Хоча технологія EDR допомагає виявити сліпі плями, вона потребує кваліфікованих аналітиків безпеки для інтерпретації вихідних даних та прийняття відповідних заходів.

Забезпечуючи огляд обладнання кінцевих точок, рішення EDR можуть допомогти виявити загрози, які інші заходи безпеки можуть пропустити. Ці загрози включають:

– зловмисне програмне забезпечення, яке може обійти застарілі антивіруси або нові покоління антивірусного ПЗ (NGAV). EDR може виявити ознаки зараження пристрою, якщо інші заходи безпеки його не помітили;

– безфайлові атаки, які уникають захисту від антивірусів (AV) або NGAV, тому що вони не записують файли на диск. Хоча EDR не може заборонити безфайлові атаки, він може допомогти виявити їх і сприяти розслідуванню та пом'якшенню їхніх наслідків;

– внутрішні загрози та порушення облікових записів. EDR може виявити аномальну поведінку користувачів, що може вказувати на компрометацію облікових записів.

Рішення EDR працюють, виявляючи інциденти безпеки та допомагаючи зменшити їх наслідки. Процес включає такі кроки:

– моніторинг кінцевих точок - постійний огляд всіх кінцевих пристроїв;

– використання поведінкового аналізу для виявлення аномалій - встановлення стандартів поведінки пристроїв і виявлення дій, які відрізняються від норми;

– ізоляція кінцевих точок та процесів - автоматичне відокремлення пристроїв та зупинка підозрілих процесів;

– відстеження початкової точки входу зловмисника - збір інформації про можливі точки входу для атаки;

– надання інформації про аномальність та ймовірне порушення - надання аналітикам необхідних даних для розслідування інциденту.

Платформа захисту кінцевих точок (EPP) призначена для запобігання атак на кінцеві точки, такі як шкідливе програмне забезпечення, вразливість нульового дня та безфайлові атаки. EPP інтегрує різні технології, включаючи антивірус, міжмережевий екран, контроль додатків, шифрування даних та управління пристроями. Ці технології працюють разом для забезпечення всебічного захисту кінцевих точок, запобігання втраті даних і забезпечення відповідності нормативним вимогам. Однією з ключових функцій EPP є можливість моніторингу та аналізу активності на кінцевих точках у реальному часі. Це дозволяє виявляти та блокувати підозрілу активність ще до того, як вона може завдати шкоди. Крім того, EPP забезпечує централізоване управління політиками безпеки, що дозволяє адміністраторам швидко реагувати на нові загрози та конфігурувати захист відповідно до потреб організації [9-10]. Сучасні EPP рішення також включають функції автоматичного відновлення систем після атак, що мінімізує час простою та знижує операційні ризики. Завдяки постійним оновленням сигнатур і використанню штучного інтелекту, EPP системи можуть ефективно адаптуватися до нових загроз і забезпечувати надійний захист навіть у складних і динамічних умовах кіберпростору. EPP виявляє атаки кількома способами:

– використання баз даних відомих сигнатур для визначення шкідливих програм та інших файлових загроз;

– блокування або дозвіл додатків, URL-адрес, портів та адрес за допомогою чорних або білих списків;

– створення "пісочниці" для перевірки можливих загроз, таких як виконувані файли;

– використання поведінкових аналітиків та машинного навчання для виявлення аномальної або підозрілої активності на кінцевій точці.

Хоча EPP розгортається на кінцевих точках, він зазвичай має хмарне рішення, що дозволяє збирати та аналізувати дані, а також забезпечує зручний доступ для аналітиків безпеки. Хоча ми порівнюємо EPP та EDR, більшість сучасних платформ EPP насправді містять рішення EDR, принаймні як додатковий компонент.

Розширене виявлення та реагування (XDR) — це передова інтегрована платформа безпеки, яка забезпечує комплексний огляд та аналіз кібербезпеки, зібравши дані з різноманітних джерел і систем у межах організації. Вона автоматично збирає та аналізує дані не тільки з кінцевих точок, але й із мереж, серверів, облікових записів користувачів, і навіть хмарних сервісів, що дозволяє здійснювати більш глибокий та точний аналіз загроз [11-13]. XDR інтегрується з існуючими системами безпеки, такими як системи управління інформацією та подіями безпеки (SIEM), рішеннями для виявлення та реагування на інциденти на кінцевих точках (EDR), інструментами мережевої аналітики, а також з інструментами управління ідентифікацією та доступом (IAM). Ця інтеграція сприяє збагаченню даних безпеки, оскільки вона об'єднує інформацію з різних джерел, що підвищує точність виявлення загроз та скорочує час на їх аналіз і реагування. Однією з ключових переваг XDR є її здатність до надання єдиної, уніфікованої панелі керування, що спрощує моніторинг, аналіз та реагування на загрози для команд безпеки. Це значно підвищує продуктивність команд безпеки завдяки швидкому доступу до інформації, необхідної для всебічного розслідування і вжиття відповідних заходів. Завдяки цим можливостям, платформи XDR є надзвичайно важливими в контексті сучасної кібербезпеки, забезпечуючи компаніям інструменти для ефективної боротьби з постійно змінюваними і складнішими кіберзагрозами.

1.2 Аналіз мережевого трафіку

Мережевий трафік - це потік даних, який передається по мережі між пристроями. Він включає в себе всі пакети даних, що передаються між

відправником та отримувачем.

Мережевий трафік може мати різні типи, включаючи передачу файлів, відправку електронної пошти, перегляд веб-сторінок, відео дзвінки та багато іншого. Кожен тип трафіку має свої особливості і вимагає певних протоколів та портів для передачі даних. Мережевий трафік може бути як внутрішнім, тобто передаватися всередині локальної мережі, так і зовнішнім, коли дані передаються через Інтернет або іншу публічну мережу. Аналіз мережевого трафіку дозволяє вивчати та розуміти, як дані передаються по мережі, і може бути корисним інструментом для виявлення та запобігання мережевим атакам, оптимізації мережевої інфраструктури та вирішення інших завдань у галузі інформаційної безпеки.

Завдання аналізу мережного трафіку стає все більш актуальним з розвитком та впровадженням нових технологій мережі, що веде до збільшення обсягу даних і появи нових мережевих протоколів на рівні застосування. Серед найбільш популярних областей практичного застосування можна виділити наступні: аналіз трафіку для виявлення проблем у мережі, відновлення потоків даних, запобігання різноманітним мережевим атакам, збір статистики.

При комплексному розв'язанні завдання аналізу мережного трафіку перш за все слід розглядати його етапи: перехоплення трафіку, його зберігання та аналіз.

Аналіз мережевого трафіку включає різноманітні методи і техніки, які дозволяють вивчати та аналізувати дані.

Сніфінг - це метод, при якому мережевий трафік перехоплюється та аналізується на певному вузлі мережі. Для цього використовуються спеціальні програми, що називаються сніферами. Сніфери можуть перехоплювати та аналізувати трафік на різних рівнях мережевої моделі OSI, починаючи з фізичного рівня та закінчуючи прикладним рівнем. Дана технологія має важливе значення як для адміністрування та забезпечення безпеки мереж, так і для потенційного зловживання в разі використання зловмисниками. Сніфінг може бути законним (для моніторингу та оптимізації мережевого трафіку) або незаконним (для перехоплення конфіденційних даних) [14-17].

Пакетний аналіз - це метод детального вивчення мережевого трафіку шляхом розбивання цього трафіку на окремі пакети даних для аналізу. Кожен пакет містить важливу інформацію, таку як ідентифікатори відправника та отримувача, використовувані протоколи, порти та інші важливі метадані. Аналізуючи ці пакети, можна отримати детальне уявлення про те, як дані передаються в мережі, і виявити можливі зловмисні дії, такі як вірусні атаки, шпигунське програмне забезпечення, або спроби несанкціонованого доступу. Пакетний аналіз також дозволяє виявляти і усувати проблеми з продуктивністю мережі. Завдяки аналізу тривалості затримок, втрати пакетів та інших параметрів ефективності мережі можна вжити заходів для оптимізації роботи мережі. Цей метод використовується також для перевірки дотримання політик безпеки та стандартів, особливо у великих корпоративних та громадських мережах. Додатково, пакетний аналіз включає в себе можливість аналізувати пропускну здатність мережі, вивчати і відстежувати тренди у використанні мережі, а також виявляти неоптимальне використання ресурсів мережі. Ці дані можуть бути критично важливими для планування мережевої інфраструктури та її масштабування відповідно до зростаючих потреб організації [18-20].

Візуалізація трафіку — це метод, за допомогою якого мережевий трафік подається у вигляді графіків, діаграм або інших візуальних елементів, що значно спрощує сприйняття та аналіз великих обсягів даних. Використання візуалізації дозволяє легше ідентифікувати патерни, тренди та аномалії у мережевому трафіку, що може бути особливо корисним для моніторингу та управління безпекою мереж [21-22].

Статистичний аналіз - це метод, який використовується для збору та аналізу статистичних даних про мережевий трафік. Цей метод охоплює аналіз таких параметрів, як кількість переданих пакетів, обсяг переданих даних, середня пропускна здатність, час відклику та інші показники. Завдяки статистичному аналізу можна виявляти аномалії, тренди та потенційні проблеми в мережевій інфраструктурі, що допомагає в проведенні оптимізації та забезпеченні стабільності роботи мережі.

Виявлення атак - це метод, при якому аналізується мережевий трафік з метою виявлення та запобігання мережевим атакам. Цей процес зазвичай включає аналіз пакетів даних на наявність підозрілих або шкідливих дій, таких як сканування портів, атаки на протоколи, або спроби несанкціонованого доступу. Аналізування трафіку допомагає виявити не лише відкриті атаки, але й складніші загрози, такі як мережеві черв'яки, троянські коні, або віруси.

Таблиця 1.1 демонструє порівняння методів аналізу мережевого трафіку демонструє лише деякі з методів аналізу мережевого трафіку, де кожен із методів має свої переваги та недоліки. Слід зазначити, що вибір методу залежить від конкретних завдань та поставлених вимог до аналізу.

Таблиця 1.1 – Порівняння методів аналізу мережевого трафіку

Метод	Опис	Переваги	Недоліки
1	2	3	4
Пакетний аналіз	Аналіз окремих пакетів даних у мережі	Дозволяє отримати детальну інформацію про кожен пакет та виявити аномалії чи атаки.	Потребує великих обчислювальних ресурсів і складний для інтерпретації результатів.
Потоковий аналіз	Аналіз потоків даних у мережі	Дозволяє виявляти аномалії та атаки на основі поведінки потоків при меншому навантаженні обчислювальних ресурсів.	Може пропустити деталі кожного пакета і складний для інтерпретації результатів.

Кінець таблиці 1.1

1	2	3	4
Сигнатурний аналіз	Аналіз мережевого трафіку на наявність співпадінь з відомими сигнатурами атак	Дозволяє виявити відомі атаки при меншому навантаженні обчислювальних ресурсів.	Може пропустити невідомі сигнатури, оскільки не виявляє нові або змінені атаки.
Машинне навчання	Застосування алгоритмів машинного навчання для аналізу мережевого трафіку	Дозволяє виявляти нові та невідомі атаки. Може адаптуватися до мережевого середовища, котре змінюється.	Потребує великих обчислювальних ресурсів. Може вимагати великого обсягу навчальних даних.

Для аналізу трафіку можна використовувати складні спеціалізовані рішення з інформаційної безпеки, такі як системи IPS/IDS (система запобігання вторгненням та система виявлення вторгнення). У цьому сегменті існує широкий вибір продуктів, які можуть бути як відкритими розробками, так і комерційними продуктами. Вони дозволяють переглядати вміст трафіку як у ручному, так і в автоматичному режимі. Особливість таких рішень полягає у можливості глибокого аналізу, під час якого розглядаються навіть не пакети, а окремі сигнатури до кожного байта переданої інформації для кожного використаного протоколу. Це дозволяє виявити шкідливе програмне забезпечення на рівні коду, яке передається по мережі.

Під час аналізу трафіку використовуване рішення визначає параметри даних, що відстежуються, і на їхній основі формує "ідеальну" модель мережі (яка в подальшому може змінюватися в залежності від зміни обраних параметрів). Потім йде етап аналізу, коли модель порівнюється з реальними подіями, а

виявлені відхилення відзначаються як аномалії.

IPS/IDS - це комплексне рішення, використання якого відображає два принципи контролю мережевих аномалій. Вони можуть працювати як в межах інфраструктури, наприклад, на пристроях користувача, так і на периметрі. Виявлення аномалій відбувається за рахунок розбору мережевих пакетів і пошуку шкідливих сигнатур, а також завдяки правилам контролю трафіку [23-25].

1.3 Огляд існуючих рішень полігонів

RangeForce – це хмарна платформа для кібернавчання, що містить реальну IT-інфраструктуру, справжні інструменти безпеки та реальні кіберзагрози. Вона пропонує практичні, інтерактивні модулі навчання, які охоплюють такі теми, як етичний злом, реагування на інциденти, безпечне програмування та інші. RangeForce створює віртуальне середовище, де користувачі можуть вправлятися у реальних сценаріях і симуляціях для поліпшення їх розуміння концепцій та технік кібербезпеки. Ця платформа використовується як початківцями, які вступають у галузь кібербезпеки, так і досвідченими фахівцями, які бажають покращити свої навички та триматися в курсі останніх тенденцій і технологій. Крім того, RangeForce пропонує адаптивне навчання, яке підлаштовується під індивідуальні потреби та рівень знань кожного користувача. Платформа також підтримує командні тренування, що дозволяє організаціям покращувати колективні навички реагування на кіберзагрози та підвищувати загальний рівень кібербезпеки [26]. Завдяки детальним звітам та аналітиці, користувачі можуть відстежувати свій прогрес, визначати слабкі місця та отримувати рекомендації щодо подальшого навчання. Таким чином, RangeForce допомагає створювати висококваліфікованих спеціалістів з кібербезпеки, готових ефективно захищати IT-інфраструктуру від сучасних загроз.

Unit Range – це кіберполігон, призначений для практичного навчання фахівців з кібербезпеки в умовах, які максимально наближені до реальних. У системі наявні понад 150 сценаріїв. Засновником полігону є експерт з

кібербезпеки Єгор Аушев. Unit Range є хмарним рішенням, яке працює на віртуальних машинах (Amazon Web Services), де виконуються сценарії, які розроблено експертами з кібербезпеки. Створені сценарії максимально реалістично імітують атаки хакерів або системи, що підлягають атакам [27-28]. Unit Range також надає інформаційну панель даних у реальному часі, де вимірюється ефективність та ризиковий профіль для всіх членів команди, від керівників до звичайного IT-персоналу. Інтерфейс ресурсу відображено на рисунку 1.1.

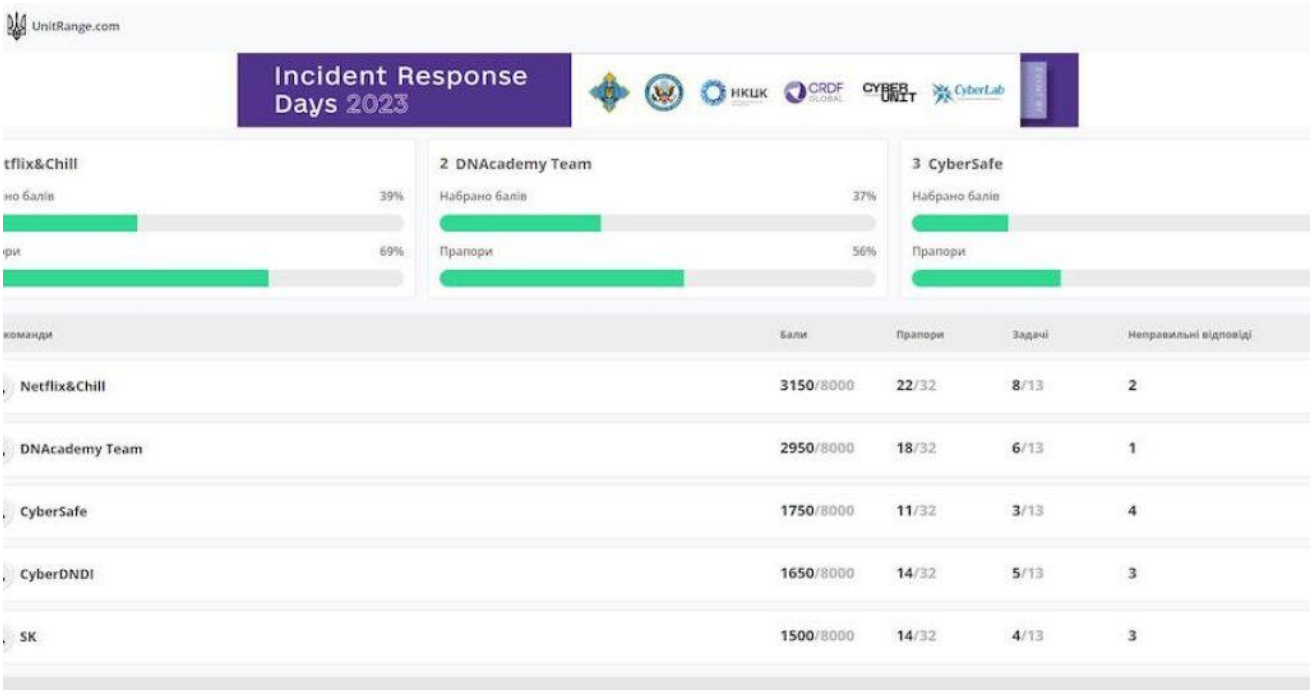


Рисунок 1.1 – Інтерфейс Unit Range

На базі Житомирського військового інституту імені С. П. Корольова успішно діє навчально-тренувальний комплекс «Кіберполігон», який використовується для проведення науково-практичних досліджень, вдосконалення навчальних заходів з протидії гібридним впливам у кіберпросторі та якісної підготовки фахівців з кібербезпеки. Кіберполігон складається з чотирьох функціонально пов’язаних компонентів (рисунок 1.2): комплекту кібероборони (забезпечення кібербезпеки та кіберзахисту) та кіберрозвідки (проведення тестування на кіберзахищеність), серверної інфраструктури для

створення мережевої моделі, моніторингу та аналізу усіх виконуваних дій. Програмне ядро представлене новітнім дистрибутивом операційної системи Kali Linux [29-30].

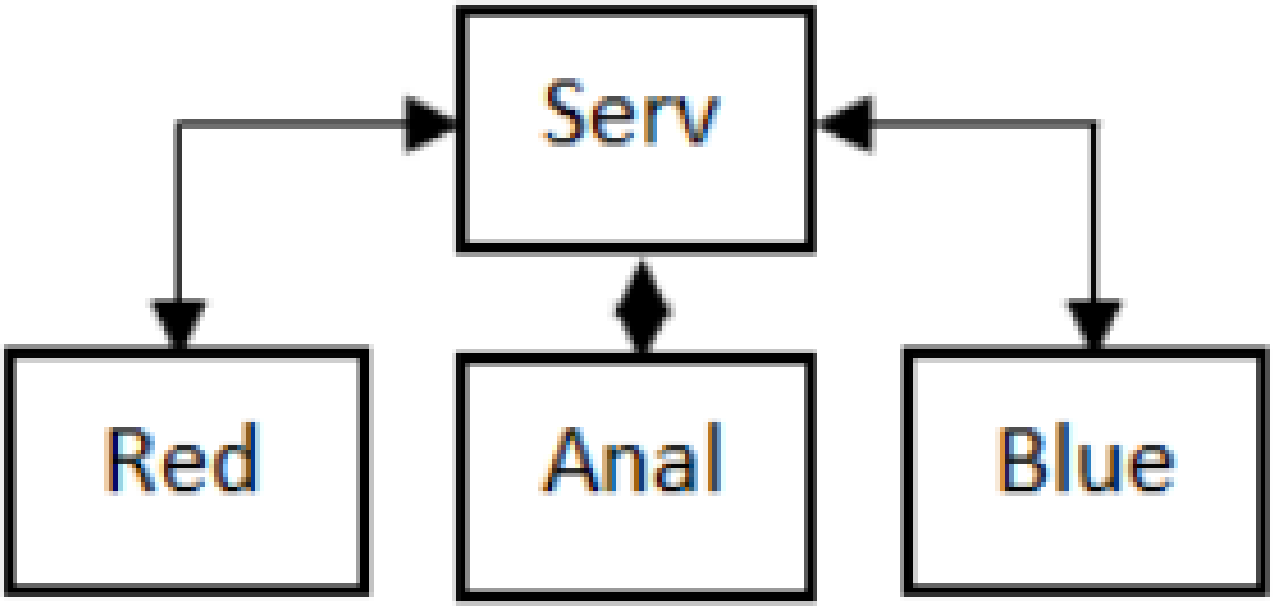


Рисунок 1.2 – Топологія навчально-тренувального комплексу «Кіберполігон»

Функціональне призначення програмних та апаратних компонентів визначається конкретними класами задач та характеристиками кожного з компонентів Кіберполігону. Використання Кіберполігону у навчанні надає можливість тренування фахівців з інформаційної безпеки у умовах, які якомога більше наближені до реальних. Це сприяє покращенню практичних навичок студентів через командні змагання, такі як національні змагання з кібербезпеки UA30CTF, Національний оборонний хакатон та інші подібні заходи.

Західноукраїнський національний університет у ході практичної підготовки фахівців з кібербезпеки використовує кіберполігон, що реалізований на одноплатових комп'ютерах Raspberry Pi з встановленими операційними системами, що мають певні вразливості [31]. Студенти можуть проводити тестування на проникнення, зокрема виявляти та використовувати наявні уразливості. Зображення кіберполігону показано на рисунку 1.3.

Рисунок 1.3 – Кіберполігон з реалізацією на одноплатових комп’ютерах Raspberry Pi

На кафедрі кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут діє навчально-тренувальний комплекс кібербезпеки (рисунок 1.4). Його метою є виявлення, реагування, протидії та запобігання кіберзагрозам. Комплекс включає в себе програмно-технічні засоби, ситуаційний центр та комплекс технічних засобів, який містить 80 автоматизованих робочих місць для курсантів та слухачів, що навчаються за спеціальністю «Кібербезпека» Кіберполігон забезпечує постійне функціонування програмно-апаратного ядра та дає можливість створення, модифікації та реалізації сценаріїв, а також контролю за проведенням навчальних занять та тренувань з кібербезпеки. Оперативне управління інфраструктурою кіберполігону здійснюється через ситуаційний центр, який відповідає за підготовку та проведення навчальних заходів та тренувань, а також реагування на кібератаки під час їх здійснення. Доступ до ресурсів комплексу здійснюється через

захищений віртуальний канал з використанням двофакторної автентифікації. Брандмауер та антивірусне програмне забезпечення забезпечує захист внутрішньої інфраструктури від зовнішніх загроз [32].

Рисунок 1.4 – Навчально-тренувальний комплекс кібербезпеки

Харківський національний економічний університет імені Семена Кузнеця має для відпрацювання кібердій віртуальне середовище, яке не має доступу до Інтернету. Основним компонентом кіберполігону є програмне забезпечення та системи віртуалізації (рисунок 1.5), які використовуються для моделювання кібератак на комп'ютерні мережі [33]. Це дозволяє зменшити або навіть уникнути витрат на придбання ресурсів хмарних обчислень та непотрібного використання пропускної здатності загальних комунікаційних каналів для виконання завдань кіберполігону.

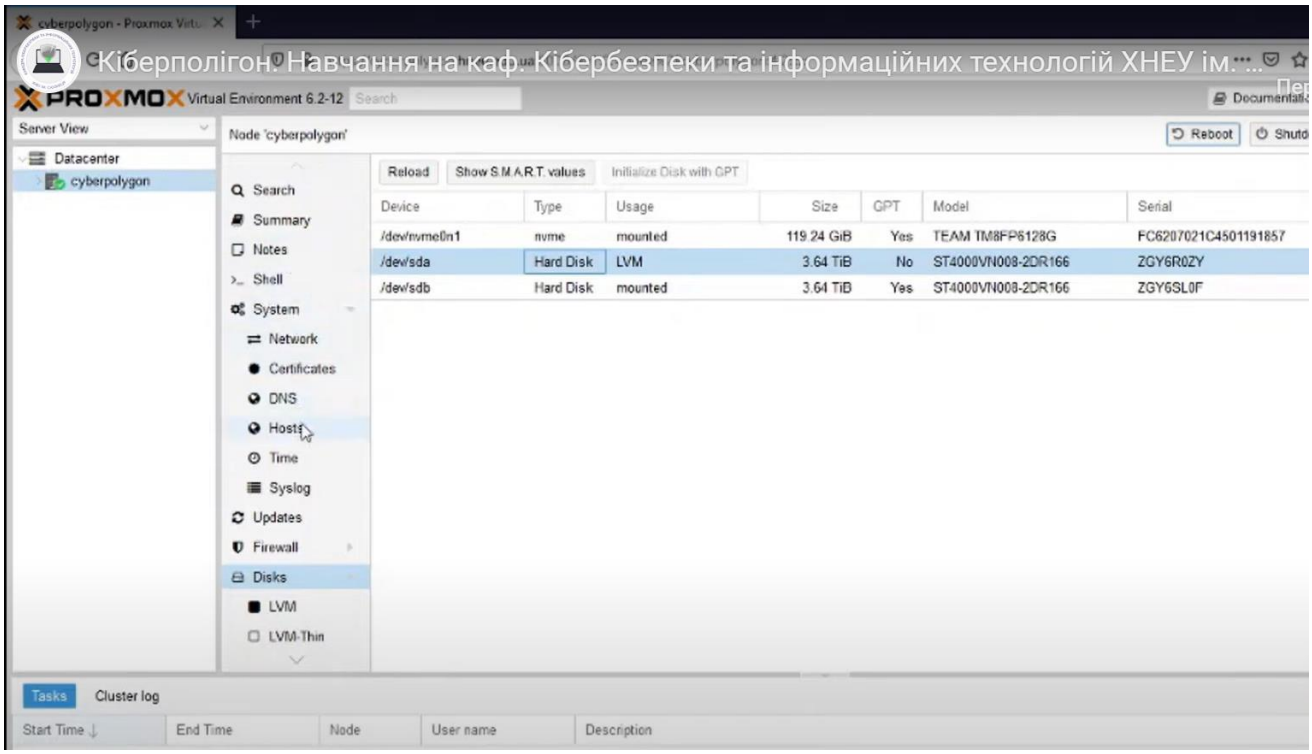


Рисунок 1.5 – Віртуальне середовище кіберполігону

Харківський національний університет радіоелектроніки кафедра Інфокомунікаційної інженерії ім. В.В. Поповського за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» реалізувала CTF платформу (рисунок 1.6).

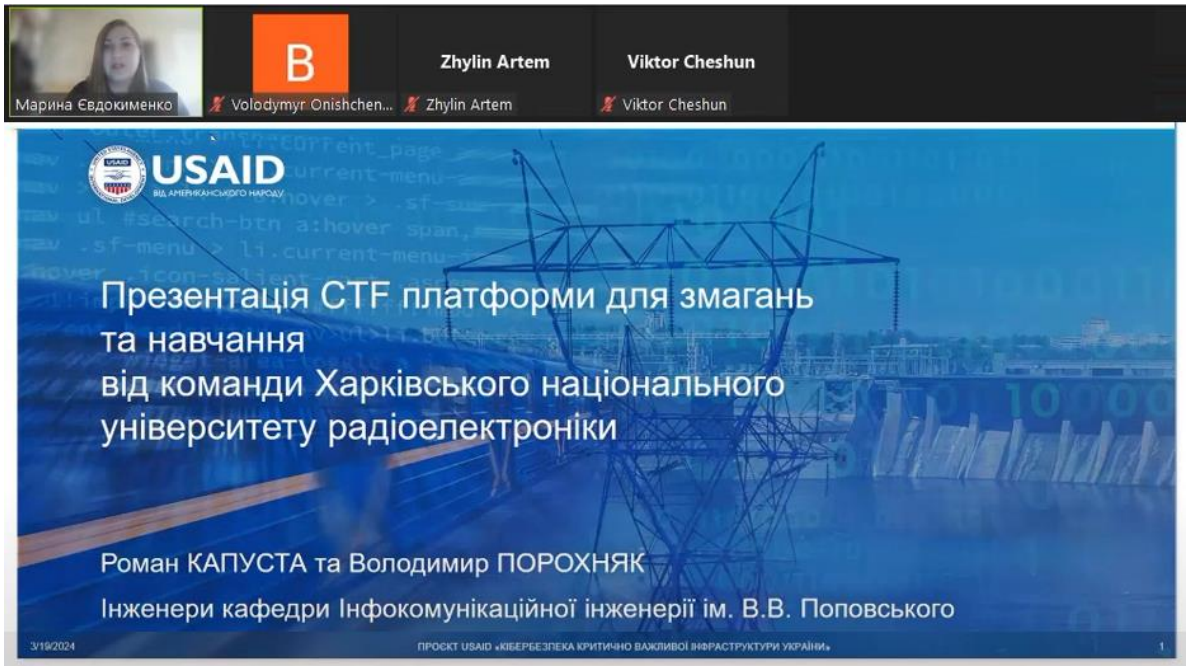


Рисунок 1.6 – CTF платформа

Дана платформа призначена для групових вирішень тих чи інших завдань, які попередньо були внесені до бази завдань із відповідними налаштуваннями. Перевагою платформи є можливість командної роботи. Проте база має обмежену кількість завдань, а для добавлення нових потрібно детально готувати всі етапи виконання (які не передбачають альтернативних рішень) та призначені для застосування комплексних рішень. Відпрацьовувати окремі технології чи засоби буде не можливо.

1.4 Призначення кіберполігону

Призначення кіберполігону полягає у створенні віртуального середовища, яке імітує реальні умови роботи мережі та інформаційних систем з метою тренування персоналу та проведення вправ з кібербезпеки. Кіберполігон дозволяє організаціям тестувати свої заходи захисту, виявляти вразливості та реагувати на кібератаки в контрольованому середовищі, що допомагає підвищити рівень готовності та навички персоналу у вирішенні кібербезпекових викликів. Також кіберполігон може використовуватися для проведення симуляційних вправ, тренувань та навчання з метою підготовки до реальних ситуацій та підвищення ефективності заходів захисту інформації.

Підходи до створення кіберполігонів для тестування інноваційних інструментів та заходів забезпечення інформаційної та кібербезпеки в умовах гібридних конфліктів різної інтенсивності та характеру базуються на проведенні комплексу наукових досліджень, які охоплюють як фундаментальний, так і практичний аспекти, і включають в себе наступні елементи:

– постійне вдосконалення науково-прикладних та технологічних принципів розробки та впровадження програмно-апаратних засобів для моніторингу, захисту та впливу в кіберпросторі, а також їх практичне тестування;

– розробка фундаментальних та прикладних методів створення математичного забезпечення для програмно-апаратних засобів, що забезпечують моніторинг, аналітичну обробку даних, прогнозування, планування та реалізацію

заходів протидії інформаційним і кібер загрозам в кіберпросторі;

– розробка та практичне впровадження в середовищі кіберполігонів програмних засобів для моніторингу, аналітичної обробки даних, прогнозування, планування та виконання заходів протидії інформаційним і кібер загрозам в кіберпросторі;

– розвиток новітніх методів та засобів протидії кібер загрозам, включаючи захист критичних інфраструктур, суб'єктів та об'єктів управління державної безпеки і оборони, а також громадянського суспільства в умовах гібридних конфліктів різної інтенсивності;

– розробка методичних основ класифікації, стандартизації та сертифікації кіберполігонів, а також створення системи класифікації і стандартів для цих полігонів.

На кіберполігоні можна робити наступне:

– проводити симуляції кібератак та тренувати персонал у виявленні, аналізі та реагуванні на них;

– тестувати заходи захисту, зокрема перевіряти ефективність захисних заходів, таких як файерволи, антивіруси, системи виявлення вторгнень тощо;

– моделювати сценарії реальних кіберзагроз, які можуть виникнути в реальному світі від зовнішнього чи внутрішнього порушника, для оцінки готовності та реакції організації на них;

– тестувати та вдосконалювати стратегії кібербезпеки, в тому числі розробляти та перевіряти стратегії та процедури реагування на кіберподії для підвищення ефективності та швидкості реагування;

– проводити оцінку вразливостей, ідентифікувати та аналізувати вразливості в мережі та системах, щоб вжити заходів для їх усунення;

– навчати студентів, спеціалістів та інших зацікавлених осіб з питань кібербезпеки, використовуючи реалістичні сценарії та вправи.

Користувачі кіберполігону можуть бути поділені на п’ять груп.

До першої групи слід віднести адміністраторів полігону, які відповідають за безпосереднє налаштування та підтримку роботоздатності, резервне копіювання

та відновлення роботоздатності віртуальних машин полігону.

До другої групи слід віднести облікові записи викладачів, котрі відповідають за проведення лабораторних чи практичних занять, керують студентським конструкторським бюро, керують дослідженнями тощо. Вони матимуть можливість створення, редагування та видалення профілів учасників (студентів, учасників конструкторського бюро), включатиме їх до наступних груп.

Третьою має бути група моніторингу, яка має стежити за подіями інформаційної безпеки, створювати картки інцидентів, підтверджувати інциденти, зареєстровані автоматичними стандартними засобами.

Наступною буде група реагування, котра матиме доступ до вбудованих у шаблон засобів виявлення комп'ютерних атак та додаткових систем захисту інформації, характерних для обраного завдання.

Останньою буде група порушників. Їх завданням буде здійснювати атаки та зловмисні дії у залежності від розробленого сценарію.

Загалом, кіберполігон є важливим інструментом для підготовки та вдосконалення заходів кібербезпеки в організаціях будь-якого рівня.

1.5 Постановка задачі

Завданням даної кваліфікаційної роботи є розробка кіберполігону для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої.

Основними кроками для виконання поставленого завдання є:

– налаштування апаратної складової та створення віртуальних середовищ для імітації атак, тобто підготовка інфраструктури;

– налаштування системи збору мережевого трафіку для реєстрації активності під час атак на кінцеві пристрої;

– інсталяція та налаштування програмних продуктів для аналізу мережевого трафіку;

– налаштування системи розпізнавання та класифікація типів атак на основі зібраної інформації (аналізу мережевого трафіку);

– формування політики безпеки для користувачів кіберполігону;

– проведення експериментів для перевірки ефективності розроблених заходів захисту та алгоритмів виявлення атак.

При розгортанні полігону слід враховувати наступні умови:

– дослідження мережевого трафіку під час атаки проводиться у контрольованому середовищі кіберполігону;

– кіберполігон є ізольованим від інших мереж та не зашкодить іншим мережам при зловмисній діяльності;

– збір та аналіз мережевого трафіку має проводитися з дотриманням вимог щодо конфіденційності та приватності даних;

– результати дослідження використовуються виключно для наукових цілей та розробки кібербезпечних заходів.

2 ПАРАМЕТРИ ТА НАЛАШТУВАННЯ КІБЕРПОЛІГОНУ

2.1 Опис апаратної складової

Для реалізації кіберполігону потрібні сервери, які дозволять розгорнути достатню кількість віртуальних машин та будуть підтримувати одночасно велику кількість віддалених користувачів.

Сервер HPE ProLiant ML350 Gen10 може працювати з двома масштабованими процесорами Intel Xeon, починаючи з рівня Bronze і закінчуючи Platinum. Кількість ядер процесорів може бути розширена з 4 до 28, що гарантує високу продуктивність. Має до 24 слотів для модулів DIMM, які підтримують пам'ять HPE DDR4 SmartMemory3 з швидкістю 2933 млн транзакцій/с або 2600 млн транзакцій/с [34]. Функція швидкого відновлення після збоїв, ліцензована за технологією HPE Gen10, сприяє не лише зменшенню втрат даних і часу простою, а й підвищує продуктивність праці та ефективність енергоспоживання. Окрім стандартних операційних систем, підтримуються різноманітні рішення від Azure до Docker. З можливостями розширення графічних процесорів можна додати до чотирьох модулів для підвищення продуктивності застосунків у сфері фінансів, відеоспостереження, освіти, наукових досліджень та інших галузях. Підтримка нових графічних процесорів NVIDIA Tesla T4 і NVIDIA Quadro RTX8000/6000/4000 перетворює його в ще потужніший сервер AI Tower з швидким підключенням графічного процесора, трасуванням променів і штучним інтелектом [35-36]. Основні характеристики сервера відображено у таблиці 2.1.

Таблиця 2.1- Основні характеристики сервера HP ML350 Gen10

Назва параметру	Значення
1	2
Серія	HP ML350

Кінець таблиці 2.1

1	2
Форм-фактор	Tower
Тип охолодження	Повітряне
Процесор (модель)	Intel Xeon Silver 4214 (Cascade Lake)
Процесор (тактова частота - turbo), ГГц	2,2 - 3,2
Процесор (к-сть ядер /потоків)	12 ядер / 24 потоків
Кількість процесорів	2 шт
Система охолодження	BOX
Оперативна пам’ять (тип)	DDR4-2933 МГц
Оперативна пам’ять (об’єм)	128 ГБ
Вбудований накопичувач (тип)	SSD 2x1 TB
Вбудований накопичувач (об’єм), ГБ	SSD 2x1 TB
Вбудований накопичувач (HDD)	HDD 2x4 TB
Оптичний привід	Пристрій без дисководу
Передбачена ОС	Windows Server 2019 (With interface)
Мережеве підключення (LAN RJ-45), шт	4 x RJ-45
Мережеве підключення (LAN RJ-45), Мбіт/с	10/100/1000 Ethernet
Блок живлення	800 Вт

Сервер ProLiant ML350 Gen10 забезпечує можливість розширення та гнучкість завдяки наявності корзин для накопичувачів різних форм-факторів (великих та малих). Він підтримує від 8 до 24 накопичувачів малого форм-фактора або 16 накопичувачів малого форм-фактора при встановленні 8 твердотільних накопичувачів NVMe PCIe, від 4 до 12 накопичувачів великого форм-фактора з можливістю гарячої заміни або без неї. Ці можливості сприяють захисту вашого інвестиційного капіталу у гібридному середовищі. Є багато варіантів розширення:

вісім слотів PCIe, шість портів USB, підтримка перетворення в 5U стійку та додаткові блоки живлення. Сервер має чотири вбудовані мережеві адаптери 1GbE, додаткові вертикальні адаптери PCIe (1GbE, 10GbE, 25GbE або 100GbE) і плати Infiniband забезпечують гнучкість у виборі пропускної здатності та комутаційних можливостей мережі. Це дозволяє адаптувати та розширювати систему у міру необхідності.

Візуальний вигляд сервера показано на рисунку 2.1.

Рисунок 2.1 - Сервер HPE ProLiant ML350 Gen10

Проте для того, щоб можна було відслідковувати поведінку реальних пристроїв, а не лише віртуальних машин до кіберполігону також буде під’єднано сервер Cisco UCS C220 M4. Основні характеристики сервера Cisco UCS C220 M4 відображено у таблиці 2.2 [37].

Таблиця 2.2 - Основні характеристики сервера Cisco UCS C220 M4

Назва параметру	Значення
1	2
Процесор	2 ЦП сімейства Intel Xeon E5-2600 v3

Продовження таблиці 2.2

1	2
З’єднання	2 канала з’вязку Intel Quick Path Interconnect (QPI) швидкістю 6.4, 8.0 і 9.6 ГТ/с
Набір мікросхем	Intel C610
Пам’ять	128 ГБ
Слоти PCIe	2 слоти PCIe третього покоління
RAID-контролер	Модульний контролер Cisco 12 Гбіт/с RAID. Вбудований програмний RAID-масив підтримує рівні RAID 0, 1, 5 і 10 на 4 дисководи SATA. Адаптер головної шини Cisco 9300-8E 12 Гбіт/с SAS забезпечує можливість зовнішнього підключення SAS і підтримує масиви JBOD/enclosures.
Накопичувачі	2 SSD 100 і 120 Гб 6 HDD по 1ТБ
Вбудована плата NIC	Два порта 1 Гбіт/с Intel i350 Ethernet
Модульний вбудований мережевий адаптер (mLOM)	Слот адаптера mLOM забезпечує адаптери з швидкістю 1,10 або 40 Гбіт/с
Блоки живлення	2 блоки живлення потужністю 770 Вт, які можна використовувати в «гарячому режимі»
Внутрішній USB-накопичувач	Сервер підтримує один внутрішній USB флеш-накопичувач.
Роз’єм на передні панелі	1 роз’єм для KVM-перемикача (включає 2 USB-роз’єма, 1 порт відеоадаптера (VGA) і 1 послідовний порт)
Світодіодний індикатор стану на передні панелі	Індикатор, який дозволяє адміністраторам слідкувати за конкретними серверами в крупних середовищах дата-центрів.

Кінець таблиці 2.2

1	2
Вбудований контролер управління Cisco IMC	Вбудований контролер управління материнською платою (BMC).Сумісний з IPMI 2.0 для забезпечення управління і контролю. Один інтерфейс 10/100/1000 Ethernet для управління. Інструмент управління з інтерфейсом командного рядка і графічним веб-інтерфейсом для забезпечення автоматизованого автономного управління. KVM-перемикач
Додаткові роз'єми зв'язку	Додаткові інтерфейс порти: VGA-порт відеоадаптера, 2 порта USB 3.0, послідовний порт RJ45, порт управління 1 Gigabit Ethernet і два порта 1 Gigabit Ethernet.

Слід відмітити, що на двох фізичних серверах налаштовано віртуальні комутатори, які взаємодіють між собою.

2.2 Опис програмної складової

Для швидкої інсталяції програмних продуктів та операційної системи, потрібної кількості віртуальних машин відповідно до поставлених завдань на лабораторних чи практичних заняттях попередньо було підготовлено образи різних віртуальних машин. Для віртуальної машини із операційною системою Kali Linux буде оновлено чи інстальовано наступне програмне забезпечення: Medusa, Hydra, Wireshark, Angry IP Scanner, Nikto, Zaproxy, Tcpdump, Spiderfoot, Nmap, Enum4linux, Nessus, Metasploit, Burpsuite Community Edition. Для віртуальної машини із операційною системою Windows 10 інстальовано наступне програмне забезпечення: Wireshark, Angry IP Scanner, Zaproxy. У разі необхідності додаткове програмне забезпечення можна інсталювати на віртуальну машину.

Medusa - це швидкий, паралельний та віддалений інструмент для грубої

сили при вході. Метою програми є підтримка якнайбільшої кількості служб, які дозволяють подальшу аутентифікацію. За допомогою програми стає доступним паралельне тестування на основі потоків. А тестування грубої сили може проводитися одночасно проти різних хостів, користувачів або паролів. Забезпечено гнучкий вхід користувача. Інформація про ціль (хост/користувач/пароль) може бути вказана різними способами [38]. Наприклад, кожен елемент може бути або окремим записом, або файлом, що містить різні розділи. Крім того, формат файлу комбінації дозволяє користувачеві уточнити свій цільовий список. Модульна конструкція. Кожний модуль служби існує як самостійний файл .mod. Це означає, що жодні зміни в основному додатку не потрібні для розширення підтримуваного списку служб для грубої сили. Medusa підтримує основні протоколи та різні служби (наприклад, SMB, HTTP, POP3, MS-SQL, SSHv2 та інші).

Hydra - це популярний відкритий інструмент, призначений для здійснення атак грубої сили на різні типи систем входу. Зазвичай його використовують фахівці з безпеки та хакери, щоб перевірити надійність паролів або отримати несанкційний доступ до систем. Hydra відомий своєю швидкістю та ефективністю при здійсненні таких атак, що робить його цінним інструментом. Цей інструмент дає змогу дослідникам та фахівцям з безпеки показати, наскільки легко можна отримати несанкційний доступ до системи віддалено. Він був протестований і компілюється на Linux, Windows/Cygwin, Solaris, FreeBSD/OpenBSD, QNX (Blackberry 10) та MacOS. Наразі цей інструмент підтримує наступні протоколи: Маркер, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MEMCACHED, MONGODB, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, Radmin, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 та v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC та XMPP [39].

Підтримувані платформи:

– Всі UNIX-платформи (Linux, *BSD, Solaris, тощо)

– MacOS (переважно клон BSD)

– Windows з Cygwin (IPv4 і IPv6)

– Мобільні системи на базі Linux, MacOS або QNX (наприклад, Android, iPhone, Blackberry 10, Zaurus, iPaq)

Wireshark є аналізатором мережевих пакетів. Аналізатор пакетів мережі надає детальні дані про з'єднання (рисунок 2.2). Wireshark доступний безкоштовно, є відкритим джерелом та є одним з найкращих аналізаторів пакетів, доступних сьогодні. Wireshark - це проект з відкритим кодом і випускається під ліцензією GNU General Public License (GPL) [41].

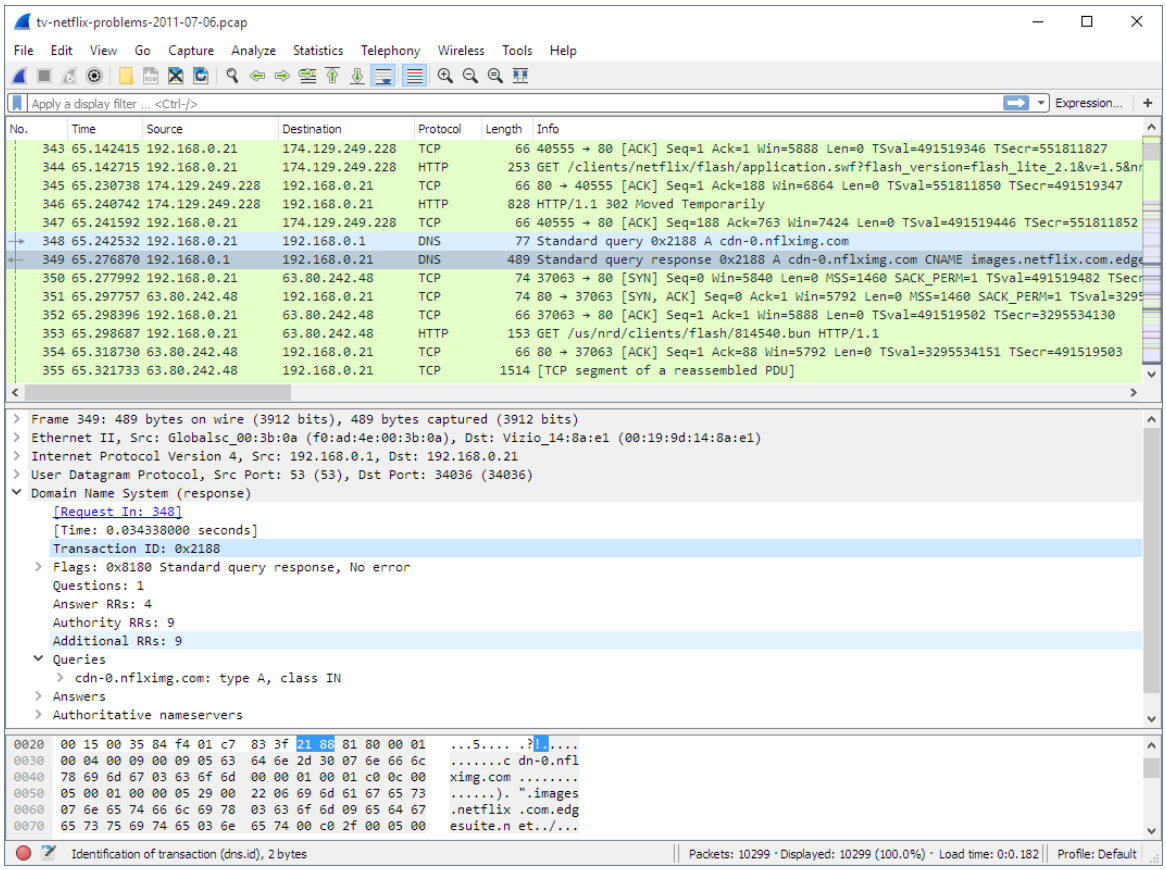


Рисунок 2.2 – Аналізатор мережевих пакетів Wireshark

Приклади використання Wireshark наступні:

– системні адміністратори використовують його для усунення неполадок в

мережі;

– фахівці з безпеки мережі використовують Wireshark для виявлення проблем з безпекою;

– QA-інженери застосовують для перевірки мережевих додатків;

– розробники використовують Wireshark для аналізу реалізації протоколів;

– інші люди використовують його для вивчення внутрішніх протоколів мережі.

Проте Wireshark також може бути корисним в багатьох інших ситуаціях. Wireshark може захоплювати трафік з багатьох різних типів мереж, включаючи Ethernet, бездротову LAN, Bluetooth, USB та інше. Конкретні типи медіа, які підтримуються, можуть бути обмежені кількома факторами, включаючи обладнання та операційну систему. Wireshark може відкривати захоплені пакети з великої кількості програм захоплення. Wireshark може зберігати захоплені пакети у багатьох форматах, зокрема pcap, pcapng, Ethereal, cap, csv, txt, json, psml, pdml та інші. Однак є кілька речей, які Wireshark не може замінити чи зробити:

– Wireshark не є системою виявлення вторгнень;

– Wireshark не керує об’єктами в мережі, а лише збирає дані з неї.

Angry IP Scanner - це широко використовуваний відкритий програмний сканер мережі, що підтримується на різних платформах. Зазвичай такі програми є відкритими, оскільки вони розробляються за участю багатьох людей без комерційних цілей. Ліцензія, обрана для Angry IP Scanner, - це популярна GPL (GNU General Public License), яка надає користувачам максимальну свободу, але обмежує використання відкритого коду для пропрієтарного програмного забезпечення [41]. Іншими словами, метою GPL є збереження вільного програмного забезпечення назавжди. Це також уникає можливості того, що автор або будь-який з спонсорів відкличуть будь-які права, надані ліцензією. Безпечні системи можливі лише завдяки використанню відкритих систем та інструментів, які можуть бути переглянуті тисячами незалежних експертів і хакерів. Основна аудиторія програми - це мережеві адміністратори, фахівці та розробники, які використовують інструмент щодня і, отже, мають високі вимоги до зручності

використання, налаштовуваності та розширюваності. Проте IP Scanner прагне бути зрозумілим і для початківців. Angry IP Scanner - це відкритий комп'ютерний програмний засіб, який можна використовувати, поширювати та модифікувати. Кросплатформенність можна розглядати як ще одну можливість, яку повинні мати користувачі - можливість вибирати свою платформу, не відмовляючись від улюбленого програмного забезпечення та не базуючись на тому, чи працює певна програма на іншій платформі чи ні. Сьогодні настає нова хвиля переміщення між платформами: Apple, за повідомленнями, відроджується через збільшення продажів та популярності їх комп'ютерів, Linux набуває все більшої популярності на ринку персональних комп'ютерів (окрім домінування у світі серверів). Світ буде набагато різноманітнішим у відношенні до різних програмних та апаратних платформ у наступні роки, ніж раніше. І це дуже добре: конкуренція стимулює розвиток; більше вибору означає більше свободи. Проте кросплатформенність ставить перед розробниками програмного забезпечення багато викликів. Незалежно від того, яку технологію виберуть, завжди буде деяка робота, специфічна для платформи, щоб зробити користувачів на кожній з них задоволеними, дотримуючись правил і конвенцій кожної з них. Це особливо важливо для графічних настільних додатків, таких як Angry IP Scanner. Існує безліч причин, чому Angry IP Scanner повинен бути кросплатформовим. Одна з них полягає в тому, що більшість користувачів все ще використовують Microsoft Windows, хоча це найгірша платформа для фільтрації мережі, тому Angry IP Scanner має підтримувати як відомі платформи, так і більш корисні, але менш популярні. Внутрішня структура Angry IP Scanner має бути модульною, наскільки це можливо, щоб мати можливість встановлювати ще більше внутрішніх розширень або зовнішніх плагінів пізніше. Сканувальний компонент сам по собі дуже унікальний - він не знає нічого про те, які дані збираються. Інформація збирається за допомогою додатків, які вибирає клієнт. Angry IP Scanner містить кілька вбудованих додатків (як було сказано вище), але додаткові додатки сторонніх розробників можна використовувати за допомогою плагінів. Це гарантує дуже велику гнучкість та розширюваність сканування програми - кожен

клієнт може мати дуже різноманітні та нестандартні потреби, особливо якщо клієнт є адміністратором великої мережі. Під час сканування компонент фільтрації керує станами. У стані фільтрації він повторює IP-адреси, надані додатком, та передає управління додаткам, щоб здійснити справжню фільтрацію.

Nikto - це інструмент для сканування веб-серверів з відкритим кодом (GPL), який проводить оцінки проти веб-серверів на кілька об'єктів, таких як понад 6700 потенційно небезпечних файлів/програм, перевіряє на старі версії понад 1250 серверів та проблеми, що відносяться до конкретних версій понад 270 серверів. Також він перевіряє об'єкти конфігурації сервера, такі як наявність кількох індексних файлів, функції веб-сервера HTTP, і може спробувати визначити встановлені веб-сервери та програмне забезпечення. Об'єкти сканування та плагіни регулярно оновлюються і можуть бути автоматично оновлені. Nikto не призначений для тих, хто хоче діяти приховано. Не кожен тест - це проблема безпеки. Є деякі об'єкти, які є тільки "інформаційними" тестами, що шукають речі, які можуть не мати дефектів безпеки, але вони можуть бути невідомі тестувальнику сервера. Ці об'єкти, як правило, правильно позначаються у відповідних повідомленнях. Є також деякі тести для невідомих об'єктів, які були помічені під час сканування в файлів журналу. Метою проекту є дослідження веб-сервера для виявлення можливих проблем та уразливостей безпеки, таких як:

- неправильна конфігурація сервера та програмного забезпечення;
- стандартні файли та програми;
- небезпечні файли та програми;
- застарілі сервери та програми;
- підказки для тестувальника щодо кращої підтримки тестування.

Nikto побудований на основі LibWhisker2 (створений Rain Forest Puppy) і може працювати на будь-якій платформі, яка має середовище Perl. Він підтримує SSL, проксі, аутентифікацію хоста, кодування атак та багато іншого.Zed Attack Proxy (ZAP) - це безкоштовний інструмент для тестування веб-додатків на наявність вразливостей у їхній безпеці. Цей інструмент розроблений спільнотою і випускається в рамках проекту OWASP (Open Web Application Security Project).

Завдяки ZAP користувачі можуть проводити різноманітні види тестів безпеки, такі як сканування вразливостей, тестування введення з відомими атаками, аналіз параметрів запитів та відповідей, перехоплення трафіку для вручного аналізу та багато іншого (рисунок 2.3).

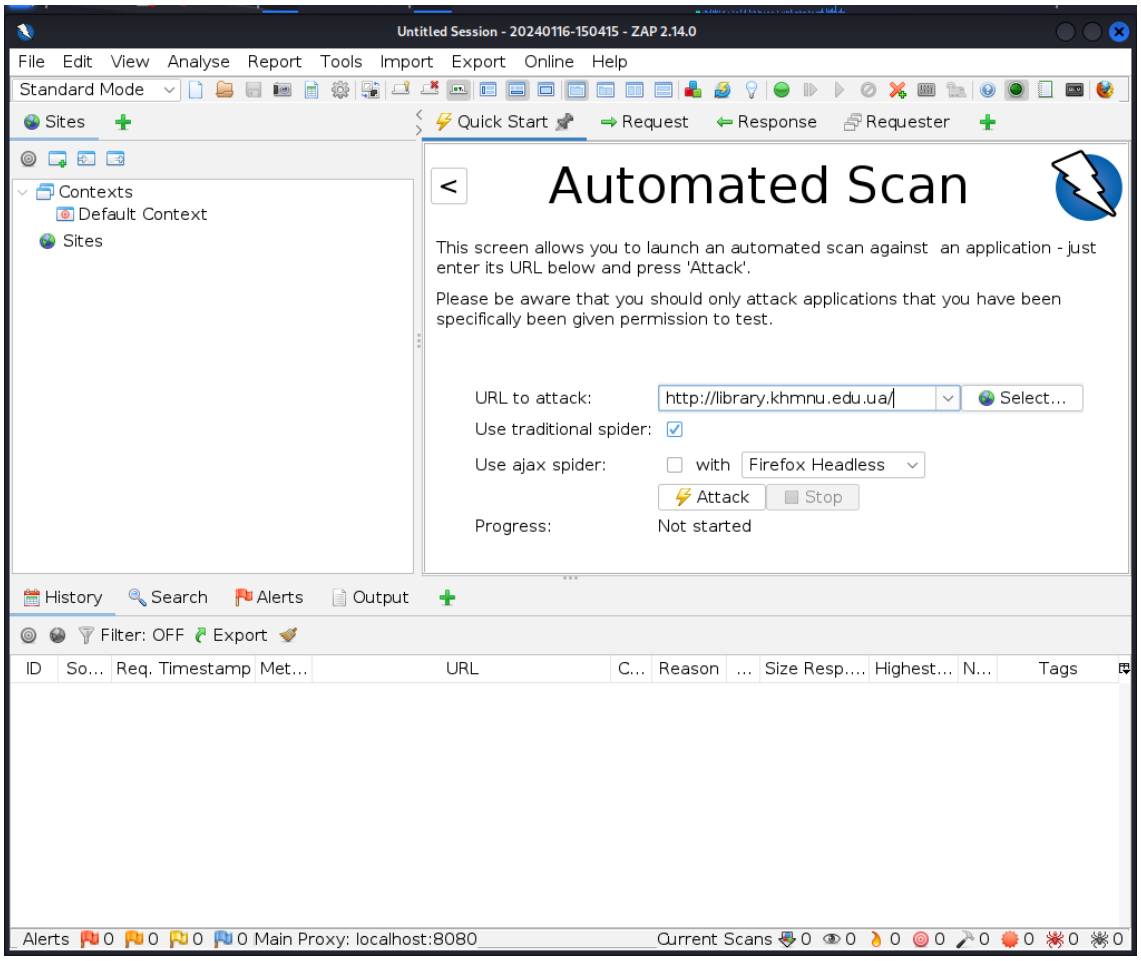


Рисунок 2.3 - Zed Attack Proxy

ZAP надає розширені можливості налаштування тестів та відображення результатів у зручному для аналізу форматі. В основі ZAP лежить так званий «проксі-сервер людини посередині». Він розташований між браузером тестувальника та веб-додатком, перехоплює та перевіряє повідомлення, що надсилаються між браузером і веб-додатком, за необхідності змінює вміст і пересилає ці пакети до місця призначення. Може використовуватися як окрема програма або процес демона. ZAP пропонує функції для широкого діапазону кваліфікаційних рівнів, від розробників до тестувальників, які новачки в

тестуванні безпеки, до експертів з тестування безпеки. ZAP має версії для всіх основних операційних систем і Docker, тому не потрібно бути прив’язаним до однієї операційної системи. Додаткові функції доступні безкоштовно через різні додатки ZAP Marketplace, доступні через клієнт ZAP. ZAP надає двох павуків для сканування веб-додатків. Пасивне сканування чудово підходить для виявлення вразливостей, а також як спосіб зрозуміти базовий рівень безпеки ваших веб-додатків і визначити, де потрібне подальше дослідження. Однак активне сканування використовує відомі атаки на вибрані цілі, щоб спробувати знайти інші вразливості. Активне сканування є справжнім нападом на цілі та може поставити їх під загрозу [42].

tcpdump - це інструмент командного рядка для аналізу мережевого трафіку в реальному часі. Він дозволяє користувачам перехоплювати та відображати пакети, які надсилаються та отримуються через мережевий інтерфейс. tcpdump здатний аналізувати різноманітні аспекти мережевого трафіку, такі як джерело та призначення пакетів, типи протоколів, розмір пакетів та багато іншого. tcpdump може аналізувати пакети різних типів, включаючи IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS, BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS та інші. Цей інструмент широко використовується для розв'язання проблем з мережевим зв'язком, відладки мережевих протоколів та аналізу безпеки мережі. Крім того, tcpdump підтримує фільтрацію трафіку за допомогою потужного синтаксису фільтрів, що дозволяє користувачам відфільтровувати лише потрібні пакети для аналізу, що значно полегшує роботу з великими обсягами даних. Інструмент також може зберігати перехоплені пакети в файл для подальшого аналізу за допомогою інших програм, таких як Wireshark. Завдяки своїй гнучкості та потужності, tcpdump є невід'ємним інструментом для мережевих адміністраторів, інженерів з безпеки та розробників, які займаються моніторингом, аналізом та оптимізацією мережевого трафіку.

Spiderfoot - це безкоштовний та відкритий програмний інструмент. Цей фреймворк написаний мовою програмування Python. Для використання потрібно мати встановлену Python на операційній системі Kali Linux. Spiderfoot

використовується для розвідки. Spiderfoot використовує різні модулі для збору даних. Spiderfoot здатний збирати інформацію про цільовий хост за допомогою активних та пасивних опцій сканування (рисунок 2.4). У фреймворку Spiderfoot доступні різні опції сканування та модулі для налаштування та перевірки цільового хосту.

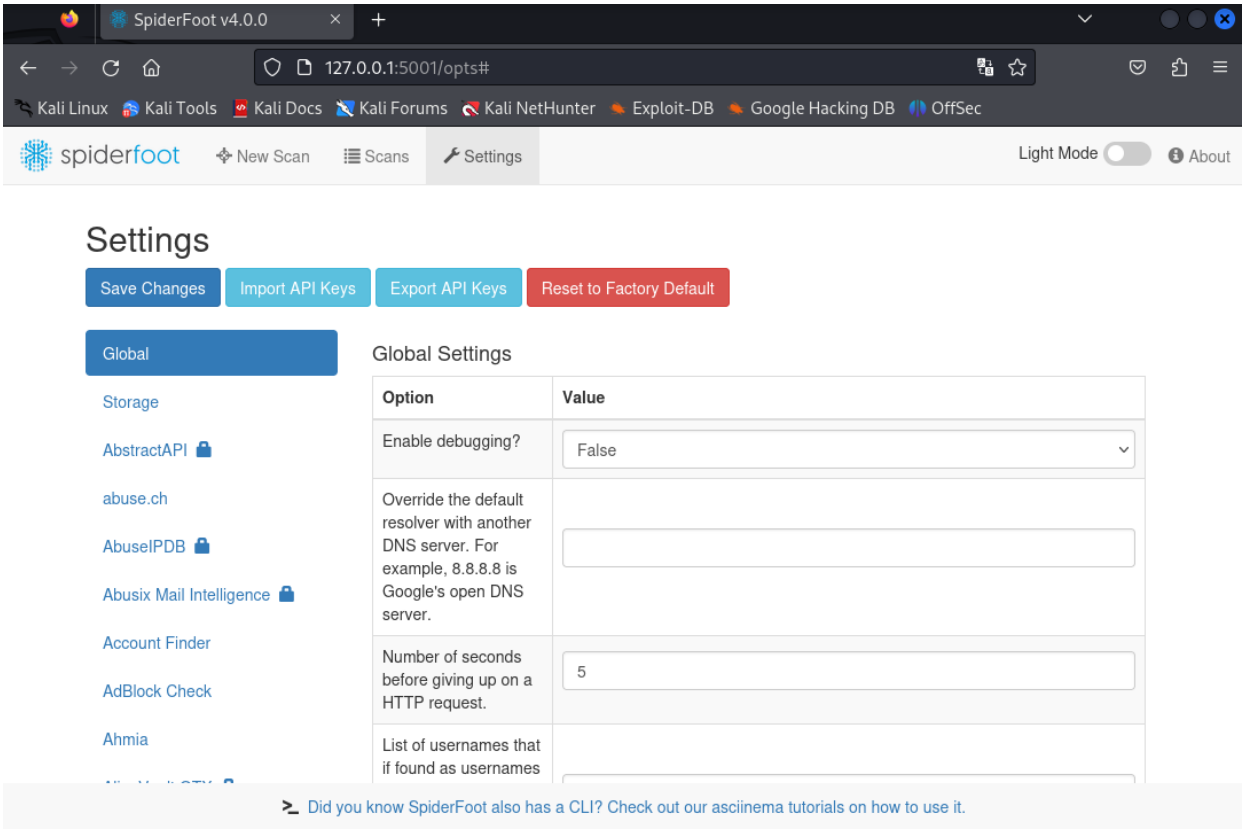


Рисунок 2.4 – Фреймворк Spiderfoot

Spiderfoot - це інструмент для збору відкритої інформації та розвідки. Spiderfoot здатний виконувати майже все, що потрібно для розвідки, відповідно потреб. Spiderfoot інтегрується з майже кожним джерелом даних і використовує різноманітні методи для аналізу даних, зробивши ці дані легкими для навігації. Spiderfoot має вбудований веб-сервер для надання інтуїтивного веб-інтерфейсу, але також можна використовувати той самий функціонал за допомогою командного рядка.

Особливості Spiderfoot:

– - це безкоштовний та відкритий програмний інструмент;

– - працює як фреймворк та інструмент;

– - написаний мовою Python;

– - може використовуватися для розвідки;

– - містить багато модулів;

– - працює на принципах OSINT;

– - це автоматизований фреймворк OSINT;

– - автоматизує процеси розвідки.

Використання Spiderfoot:

– для розвідки;

– для збору даних;

– як сканер для активного та пасивного сканування цільового об'єкту;

– для футпринтингу домену;

– для пошуку номерів телефонів, електронних адрес цільового об'єкту;

– для пошуку адрес біткоїнів;

– для збереження усього зібраного краткого опису даних;

– для створення графіків сканування, проведеного за допомогою Spiderfoot;

– для автоматизації всіх процесів збору даних.

Nmap («Network Mapper») — це інструмент з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Він призначений для швидкого сканування великих мереж, але найкраще працює на окремих хостах. Nmap використовує необроблені IP-пакети по-іншому, щоб визначити, які хости доступні у мережі, які послуги вони пропонують (назви та версії програм), які операційні системи (і версії ОС) вони використовують, а також тип фільтра пакетів/брандмауера (рисунок 2.5). У наявності є й багато інших функцій. Nmap часто використовується для аудиту безпеки, але багато системних і мережевих адміністраторів також знаходять його корисним для повсякденних завдань, таких як інвентаризація мережі, керування розкладами оновлення служб і моніторинг доступності хостів і служб. Nmap створює детальний звіт про всі цілі, які були просканові, включаючи різноманітну інформацію про кожну з них в залежності

від параметрів, що були використані. Ключем до цієї інформації є «Таблиця портів». У цій таблиці наведено номери портів і протоколи, назви служб і статус. Стан може бути відкритим, відфільтрованим, закритим або нефільтрованим. «Відкритий» означає, що програма на цільовому комп'ютері прослуховує з'єднання/пакети на цьому порту. Відфільтрований означає, що брандмауер, фільтр або інша мережева перешкода блокує порт, тому Nmap не може визначити, відкритий чи закритий порт. Закриті порти не контролюються програмою, але їх можна відкрити в будь-який час. Порт класифікується як нефільтрований, якщо він відповідає на перевірку Nmap, але Nmap не може визначити, відкритий чи закритий порт. Якщо Nmap не може визначити, який із двох станів відповідає порту, він повідомляє про комбінацію станів «відкрито|відфільтровано» та «закрито|відфільтровано». Також можна включити деталі версії програмного забезпечення в таблицю портів, коли отримано запит на версію. Коли Nmap запитують пошук IP-протоколу, тр Nmap надає інформацію про підтримувані IP-протоколи, а не порти прослуховування.

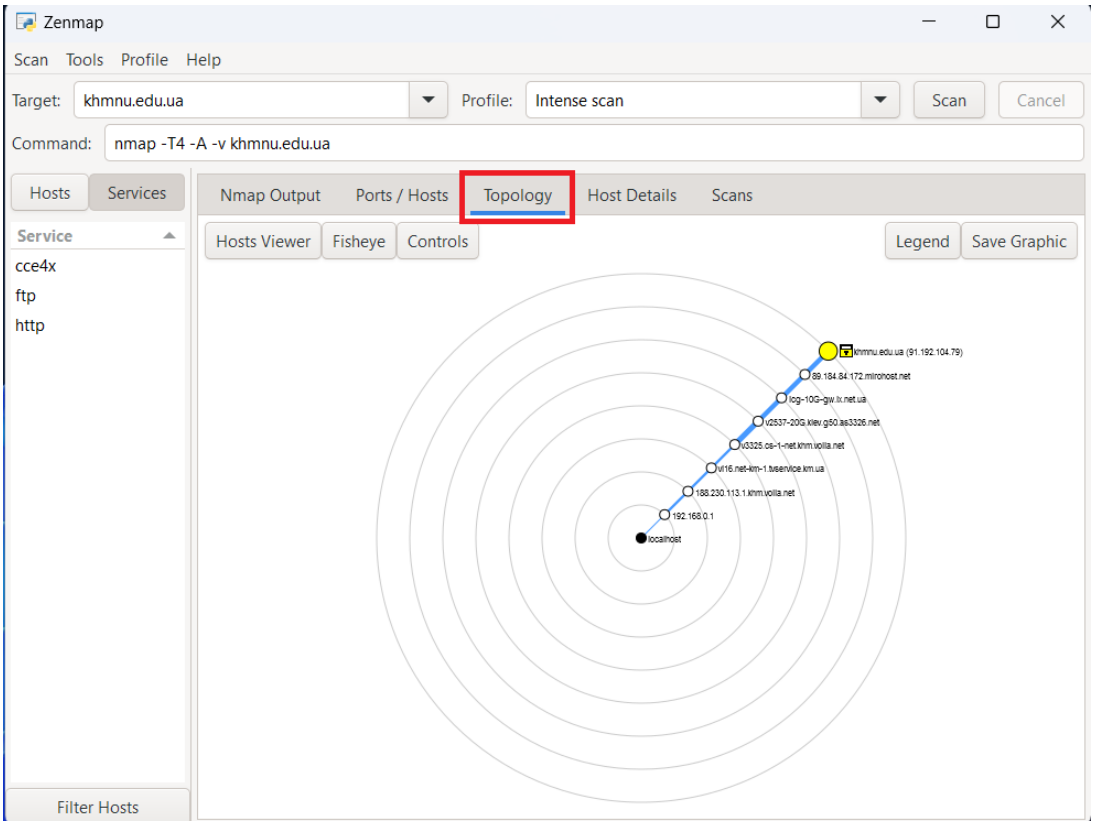


Рисунок 2.5 - Nmap

Nessus Community - це безкоштовна версія популярної системи виявлення вразливостей Nessus, призначена для використання спільнотою користувачів та малими комерційними організаціями. Вона забезпечує базові можливості сканування безпеки, дозволяючи виявляти вразливості та надавати звіти про їхню відповідність. Nessus Community підтримує одночасне сканування до 16 IP-адрес та має обмежений функціонал порівняно з комерційними версіями (рисунок 2.6). Проте ця версія є ефективним інструментом для базового аналізу безпеки мережі та виявлення потенційних загроз. Корпоративні мережі можуть відрізнятися за продуктивністю, ємністю, протоколами та загальною активністю.

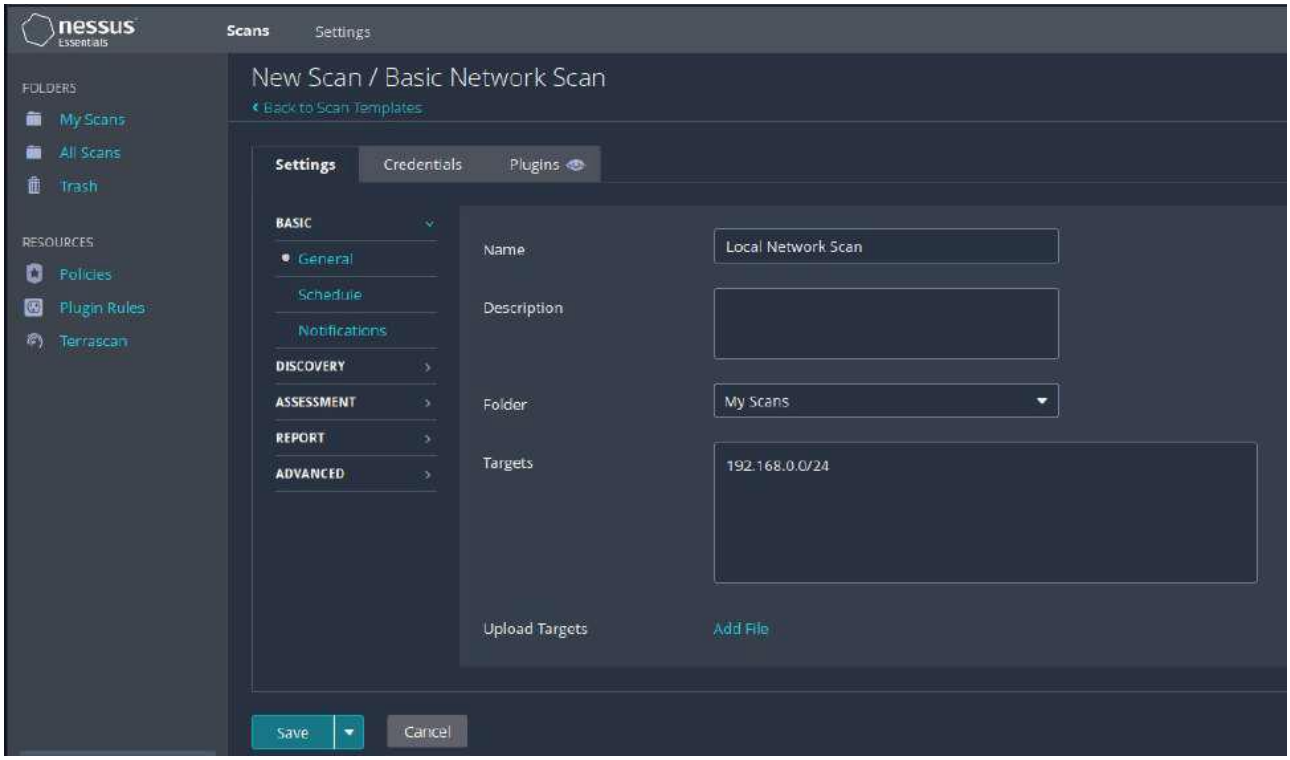


Рисунок 2.6 - Nessus Community

Для розгортання Tenable Nessus необхідно враховувати вимоги до ресурсів, такі як вихідна швидкість мережі, розмір мережі та конфігурація. Наступні рекомендації стосуються мінімального розподілу обладнання. Деякі типи сканування потребують більше ресурсів. Якщо буде виконуватися складне сканування, особливо з обліковими даними, то може знадобитися більше місця на диску, пам'яті та процесорної потужності. Щодо сканування до 50 000 хостів за

одну операцію, рекомендовано мати 4 ядра процесора з тактовою частотою 2 ГГц, 4 ГБ оперативної пам'яті (рекомендовано 8 ГБ) та мінімум 30 ГБ вільного місця на диску. Nessus Manager з 0-10 000 агентів потребує 4 ядра процесора з тактовою частотою 2 ГГц, 16 ГБ оперативної пам'яті та мінімум 5 ГБ на 5000 агентів.

Nessus підтримує лише конфігурації мереж зберігання (SAN) або мережевого сховища (NAS), якщо він встановлений на віртуальну машину, яка керується гіпервізором корпоративного класу. У віртуалізованій інфраструктурі, такій як Hyper-V або Docker, можуть виникати проблеми з ресурсами, особливо якщо потрібно запустити декілька віртуалізованих сканерів Nessus одночасно. Тому варто ретельно розглянути оптимізацію розподілу ресурсів віртуальної інфраструктури. Наступне, що слід зауважити, - це інтенсивне використання процесора програмою Nessus.

Metasploit Framework, розроблений компанією Rapid7, є модульною платформою для тестування на проникнення, заснованою на Ruby. Вона дозволяє спеціалістам з безпеки писати, тестувати та виконувати код експлойту. Фреймворк використовується для виявлення вразливостей, виконання коду експлойту та запуску корисних навантажень для компрометації цільових систем. Metasploit доступний на всіх основних операційних системах, таких як macOS, Windows та різних дистрибутивах Linux. Він пропонує широкий спектр інструментів для тестування безпеки, сканування мережі, виконання атак та ухилення від виявлення.

Однією з головних переваг Metasploit є те, що він має відкритий вихідний код і активно розробляється. На відміну від багатьох інших інструментів для тестування на проникнення, Metasploit надає глибокі можливості налаштування, дозволяючи користувачам мати повний доступ до вихідного коду та можливість додавати власні модулі. Metasploit Framework містить велику кількість інструментів, які дозволяють тестувальникам на проникнення виявляти вразливості, здійснювати атаки та уникати виявлення. Багато з цих інструментів організовані у вигляді модулів, серед яких особливо важливі:

- консоль MSF, яка є основним інтерфейсом командного рядка Metasploit,

який дозволяє тестувальникам сканувати системи на наявність вразливостей, проводити розвідку мережі, запускати експлойти тощо;

- модулі експлойтів, які дозволяють націлюватися на відомі вразливості систем. Metasploit має широкий асортимент таких модулів, включаючи ті, що стосуються переповнення буфера та ін'єкції SQL;

- допоміжні модулі, які виконують додаткові дії, необхідні під час тестування на проникнення, такі як фаззінг, сканування портів та DoS-атаки;

- модулі після експлуатації, що дозволяють розширити доступ до скомпрометованої системи та підключених систем, включаючи нумератори програм та хеш-дампи;

- модулі корисних навантажень, котрі забезпечують код оболонки, який виконується після успішного використання. Корисні навантаження можуть бути статичними сценаріями або використовувати Meterpreter - розширений метод, що дозволяє тестувальникам писати власні бібліотеки DLL або створювати нові можливості використання.

Metasploit дозволяє проводити тестування на проникнення, досліджувати вразливості, навчати персонал служби безпеки та реагувати на кібератаки, що робить його незамінним інструментом для сучасних організацій у галузі кібербезпеки.

Burp Suite може бути етапом тестування веб-додатків, створеним PortSwigger. Burp служить проксі-сервером для спроб захоплення веб-активності, може перехоплювати та коригувати вимоги http, переглядати інформацію про реакцію та комп’ютеризувати послідовні вимоги (рисунок 2.7).

Burp дає можливість контролювати надіслані вимоги та робить вступне тестування менш вимогливим і швидшим. Burp надає повний контроль, дозволяючи поєднувати прогресивні ручні процедури з найсучаснішою комп’ютеризацією, щоб робота була швидшою, цікавішою та продуктивнішою.

Інструменти, які пропонує BurpSuite:

– Spider. Веб-павук/сканер, який використовується для відображення цільової веб-програми. Мета відображення полягає в тому, щоб створити список

кінцевих точок, щоб можна було спостерігати за їх корисністю та знаходити потенційні вразливості. Спайдерінг виконується з простої причини: чим більше кінцевих точок ви збираєте під час підготовки до розвідки, тим більше поверхонь для нападу у вас є під час справжнього тестування.

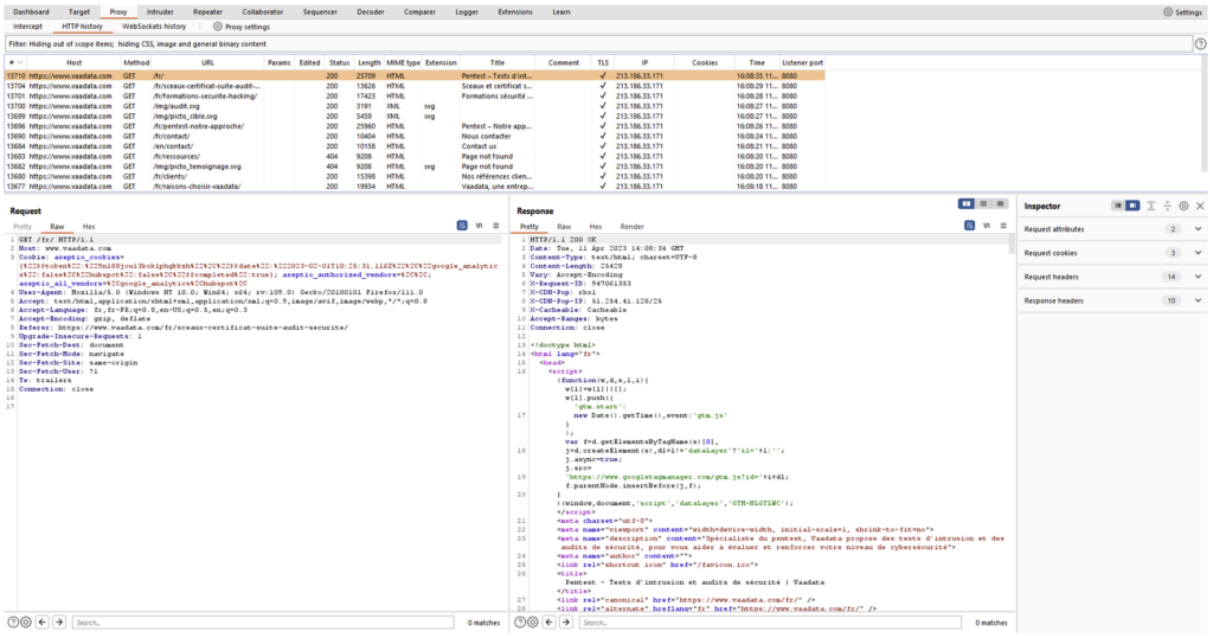


Рисунок 2.7 - BurpSuite

– Proxy. BurpSuite містить посередника, який дозволяє клієнту бачити та змінювати суть вимог і реакцій, коли вони перебувають у подорожі. Це також дозволяє клієнту надсилати запит/відповідь під спостереженням на інший важливий пристрій у BurpSuite. Проміжний сервер може бути збалансований для роботи на певному IP-адресі та порті. Крім того, посередник може бути організований для каналізації певних типів наборів запитів-відповідей.

– Intruder. Це може бути fuzzer. Часто використовується для запуску набору значень через точку введення. Значення запускаються, і вивід перевіряється на успіх/невдачу та довжину відповіді. Найчастіше аномалія призводить до зміни коду реакції або тривалості повідомлення. BurpSuite допускає грубу силу, запис посилання на слово та окремі значення для позиції корисного навантаження. Слово-посилання атакує форми ключового слова, області, які, як підозрюють, є беззахисними для введення XSS або SQL. Обмеження рівня тестування та нападу

на веб-додаток.

– Repeater. Повторювач дозволяє клієнту надсилати вимоги більше одного разу за допомогою ручних налаштувань.

– Sequencer. Секвенсор - це засіб перевірки ентропії, який перевіряє випадковість токенів, створених веб-сервером. Ці токени здебільшого використовуються для перевірки в конфіденційних операціях: випадками таких токенів є файли cookie та анти-CSRF-токени. В ідеалі ці маркери повинні створюватися абсолютно нерегулярним способом, щоб імовірність появи кожного мислимого персонажа на позиції поширювалася послідовно. Це має бути виконано як побітово, так і посимвольно. Ентропійний аналізатор перевіряє цю теорію на справжність. Це працює так: спочатку очікується, що токени будуть нерегулярними. У цей момент токени перевіряються на певні параметри для певних характеристик. Рівень заслуговує на увагу терміну характеризується як найменша оцінка ймовірності того, що токен продемонструє характеристику, так що у випадку, якщо токен включає ймовірність характеристики нижче рівня центральності, гіпотезу про те, що токен є довільним, буде відхилено. Цей апарат можна використовувати, щоб виявити безсильні токени та скласти список їх розвитку.

– Decoder. Містить перелік поширених методів кодування, таких як URL, HTML, Base64, HEX тощо. Цей пристрій стане в нагоді під час пошуку фрагментів даних у значеннях параметрів або заголовків. Він додатково використовується для розробки корисного навантаження для різних класів уразливості. Використовується для виявлення істотних випадків IDOR і захоплення сесії.

– Extender. BurpSuite підтримує зовнішні компоненти, які повинні бути координатами в набір пристроїв, щоб покращити його можливості. Ці зовнішні компоненти називаються BApps. Вони працюють схоже на розширення браузера. Їх можна побачити, налаштувати, ввести та видалити у вікні Extender. Деякі з них базуються на адаптації спільноти, але деякі вимагають платної професійної форми.

2.3 Політика безпеки

Всі облікові записи буде поділено на групи із власними правами та можливостями. Проте при етичному хакінгу їх поділ буде наступним (рисунок 8):

- адміністратор, який контролює роботу усіх користувачів та дії в середовищі;
- викладач, котрий видає завдання та здійснює підготовку робочого середовища;
- порушник, що ініціалізує атаки, сканування чи інші зловмисні/несанкціоновані дії у межах виконання поставленого завдання;
- реагування, яке має протидіяти та/або виявляти порушника в залежності від поставленого завдання;
- моніторинг, до якого можуть належати всі інші користувачі з метою аналізу дій та спостереження.

Загальний алгоритм роботи з кіберполігоном наведено у Додатку Б.

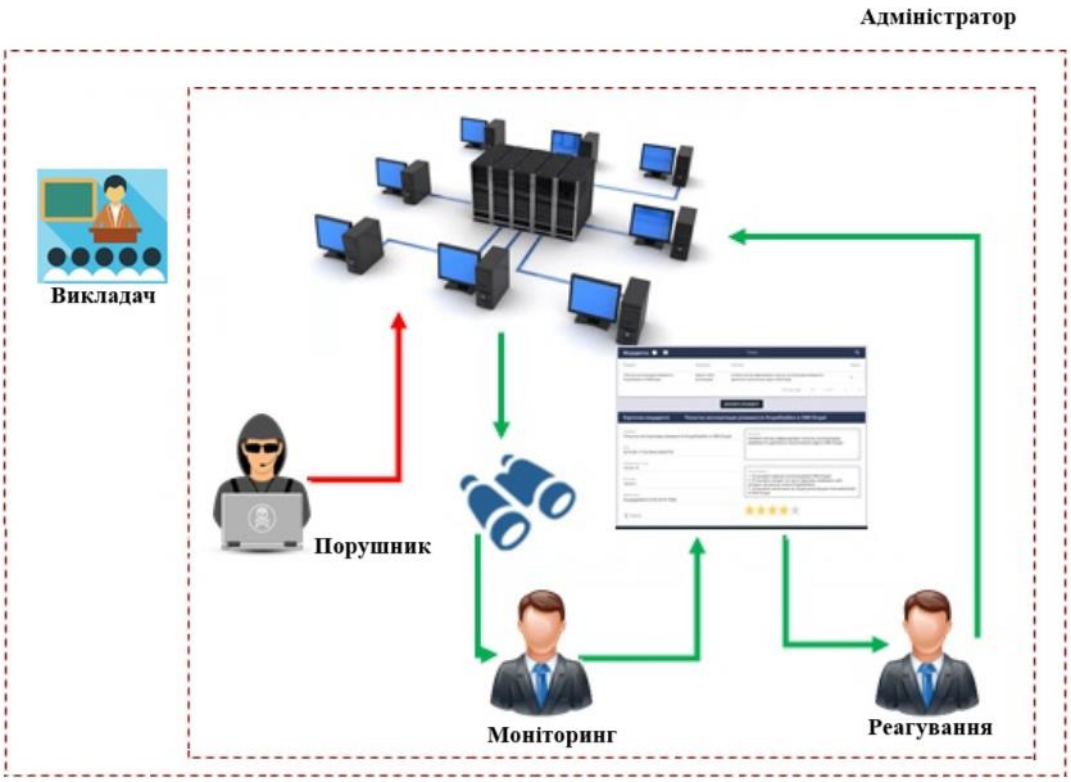


Рисунок 2.8 – Поділ користувачів на ролі

Адміністратори домену — це вбудована група служб Microsoft Active Directory, яка зазвичай використовується в мережах на базі Windows для керування обліковими записами користувачів, комп'ютерами та іншими ресурсами в межах домену. Члени групи адміністраторів домену мають широкі права та дозволи в домені та можуть виконувати різноманітні адміністративні завдання, зокрема:

- адміністратори домену можуть створювати, змінювати та видаляти облікові записи користувачів і груп у домені;

- створювати та керувати об'єктами групової політики (GPO), які визначають параметри безпеки та конфігурації для користувачів і комп'ютерів у вашому домені;

- керувати спільними папками, принтерами та іншими мережевими ресурсами в межах домену;

- налаштовувати контролери домену, DNS-сервери та інші важливі компоненти інфраструктури;

- призначати дозволи, керувати політиками безпеки та виконувати перевірки безпеки, щоб забезпечити цілісність і конфіденційність ресурсів домену.

Важливо зазначити, що членство в групі адміністраторів домену надає значні привілеї та контроль над інфраструктурою домену. Таким чином, членство повинно бути обмежено адміністраторами, яким потрібні ці привілеї для виконання адміністративних функцій. Несанкціонований доступ до групи адміністраторів домену може становити серйозну загрозу безпеці всього домену. Як найкраща практика, потрібно дотримуватися принципу найменших привілеїв. Тобто користувачам надаються лише повноваження, необхідні для виконання конкретного завдання. Саме тому адміністратор домену – це системний адміністратор кафедри, який відповідає за роботоздатність полігону.

Локальні адміністратори сервера - це користувачі, які мають повний доступ і контроль над конкретним сервером. Вони мають права адміністратора на цьому конкретному сервері, але не мають автоматичного доступу до інших серверів у

домені. Важливо розрізняти між локальними адміністраторами і доменними адміністраторами. Локальні адміністратори сервера:

– мають повний доступ до всіх ресурсів і функцій сервера, включаючи встановлення програмного забезпечення, налаштування системи, керування користувачами та групами тощо;

– можуть створювати, видаляти і керувати обліковими записами користувачів та групами на цьому сервері;

– вести журнал дій, щоб відстежувати активності користувачів і системні події;

– відповідають за забезпечення безпеки сервера, встановлення необхідних заходів захисту, виявлення і виправлення потенційних загроз;

– можуть налаштовувати параметри системи, служб та програм, щоб забезпечити оптимальну продуктивність і безпеку.

Важливо враховувати, що локальні адміністратори мають обмежений обсяг контролю та повноважень, які обмежені лише цим конкретним сервером. Для керування всією інфраструктурою мережі зазвичай використовують доменних адміністраторів, які мають повний доступ до всіх серверів у домені.

Локальними адміністраторами доцільно робити наукових чи науково-педагогічних працівників, які безпосередньо розробляють завдання, налаштовують програмні продукти та контролюють хід виконання здобувачами.

Доменні користувачі у Windows Server - це користувачі, які мають облікові записи, керовані централізованою службою домену.

Коли користувач створюється в домені, він має можливість входити в систему на будь-якому комп'ютері в цьому домені з використанням одного і того ж облікового запису користувача та пароля. Це дозволяє легко керувати доступом користувачів до різних ресурсів у мережі, а також централізовано встановлювати правила безпеки та політики.

Доменні користувачі мають доступ до різних ресурсів, таких як файли та принтери, які можуть бути спільно використані в рамках цього домену. Крім того, адміністратори можуть налаштовувати права доступу для кожного користувача

окремо або у групах користувачів.

Створені облікові записи (доменні користувачі) будуть надаватися для здобувачів під час виконання завдань. Політика безпеки для доменних користувачів у Windows Server може бути налаштована адміністратором домену з метою забезпечення безпеки мережі. Нижче наведено базові налаштування політики безпеки, які можуть бути застосовані:

– вимога до складних паролів, періодична зміна паролів, обмеження повторного використання паролів і блокування облікових записів після декількох невдалих спроб входу;

– налаштування двофакторної аутентифікації, обмеження часу сесії для захисту від несанкціонованого доступу;

– налаштування прав доступу до файлів, папок та інших ресурсів з врахуванням принципу найменших привілеїв (Least Privilege);

– включення аудиту подій для відстеження дій користувачів та виявлення можливих загроз безпеці;

– використання антивірусного програмного забезпечення, блокування небезпечних веб-сайтів та прикріплених файлів електронної пошти;

– вимога до шифрування даних при їх передачі по мережі або зберіганні на пристроях.

Фактичний набір правил і налаштувань буде залежати від конкретних потреб, який потрібно забезпечити.

2.4 Висновки до розділу

Основні параметри та налаштування кіберполігону, описані у даному розділі, ретельно розкривають складові необхідні для створення ефективної платформи для навчання та тестування у сфері кібербезпеки. Кіберполігон забезпечений високопродуктивними серверами, такими як HPE ProLiant ML350 Gen10 та Cisco UCS C220 M4, які оснащені потужними процесорами, значною кількістю оперативної пам'яті та різноманітними можливостями зберігання даних,

що дозволяє налаштувати велику кількість віртуальних машин для імітації різних мережевих середовищ.

Програмне забезпечення, що використовується на полігоні, включає спеціалізовані інструменти для пенетраційного тестування та моніторингу мережі, такі як Nessus для аудиту вразливостей, Wireshark для аналізу мережевого трафіку, а також Metasploit для виконання експлойтів. Це забезпечує комплексний підхід до навчання, де користувачі можуть вивчати реальні загрози та методи їх нейтралізації.

Кіберполігон підтримує розширення функціональності через можливість додавання нового обладнання та оновлення програмного забезпечення, що дозволяє адаптувати навчальний процес під актуальні потреби у сфері кібербезпеки. Підтримка різних операційних систем і програмних середовищ сприяє більш ефективному та гнучкому використанню ресурсів полігону.

Враховуючи наявність різноманітних засобів для тестування та розробки, кіберполігон не лише виконує функцію навчального центру, але й служить платформою для проведення досліджень в галузі розробки та тестування нових методологій і технологій у сфері кібербезпеки. Такий комплексний підхід сприяє підготовці кваліфікованих спеціалістів, здатних ефективно протидіяти сучасним і майбутнім кіберзагрозам.

3 РОЗГОРТАННЯ ПОЛІГОНУ

3.1 Схема мережі

Доцільно сервери розташовувати у спеціально підготовлених приміщеннях – серверних, де забезпечено кілька ліній електроживлення та забезпечено відповідний температурний режим, звукоізоляцію.

Для доступу до мережі сервери під’єднано до наявного мережевого обладнання, яке знаходиться у серверній. А саме до маршрутизатора MikroTik CCR2116-12G-4S+ (рисунок 3.1).

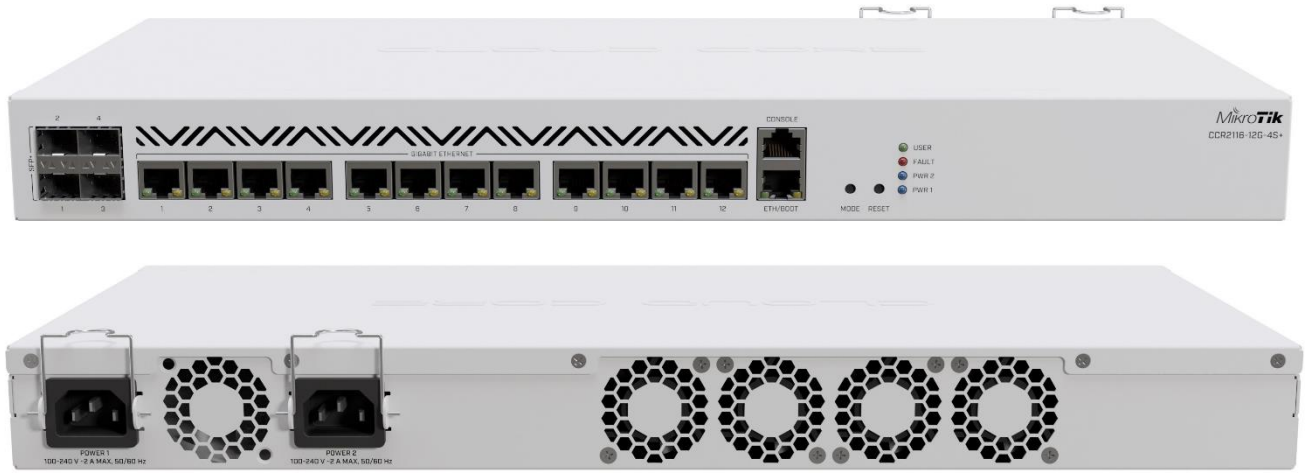


Рисунок 3.1 – MikroTik CCR2116-12G-4S+

Маршрутизатор оснащений потужним процесором Amazon Annapurna Labs Alpine CPU. Є чотири порти 10G SFP+, які мають окремі повнодуплексні лінії, що підключені до чіпу перемикача сімейства Marvell Amethyst. Є порти Gigabit Ethernet. 12 з них працюють через чіп Marvel. Також є ще один порт Gigabit, підключений безпосередньо до CPU. Кожна група з 4 портів має окреме повнодуплексне підключення до чіпу перемикача. Також є слот M.2 PCIe. Він підтримує SSD об'ємом до 8 терабайт. Це може бути надзвичайно корисним для різних контейнерних додатків. Інші параметри наведено у таблиці 3.1. Крім того,

маршрутизатор підтримує передові функції безпеки, такі як апаратне прискорення шифрування для VPN з'єднань та захист від DDoS-атак. Завдяки вбудованому механізму апаратного шифрування, він може забезпечувати високу продуктивність при обробці зашифрованого трафіку, що є важливим для забезпечення безпеки мережевих з'єднань. Маршрутизатор також оснащений вбудованою підтримкою для віртуальних локальних мереж (VLAN) та розширеними можливостями керування трафіком, що дозволяє ефективно розподіляти навантаження та підвищувати продуктивність мережі. Інтерфейс керування маршрутизатором є інтуїтивно зрозумілим і пропонує широкий набір інструментів для моніторингу та конфігурації мережевих параметрів. Підтримка стандартів SNMP, syslog та NetFlow дозволяє легко інтегрувати маршрутизатор у існуючі системи моніторингу та управління мережею. Завдяки своїй високій продуктивності, розширеним функціям безпеки та гнучким можливостям підключення, цей маршрутизатор є ідеальним вибором для підприємств, які прагнуть забезпечити надійну та безпечну роботу своєї мережевої інфраструктури.

Таблиця 3.1 – Параметри маршрутизатора MikroTik CCR2116-12G-4S+

Параметр	Значення
Кількість портів	13
Швидкість LAN-портів (RJ-45), Мб/сек	10/100/1000 Gigabit Ethernet
Інтерфейси	13xRJ-45, 1xRJ-45 (консольний порт), 4xSFP
Процесор	AL7400
Номінальна частота процесора, ГГц	2
Пам'ять	Flash 128 МБ

Комутатор MikroTik CRS326-24G-2S+RM (рисунок 3.2) приєднаний в порт маршрутизатора MikroTik CCR2116-12G-4S+. До комутатора приєднано комп’ютерні класи, які використовуються для освітнього процесу здобувачами

кафедри кібербезпеки, які безпосередньо будуть використовувати кіберполігон для навчальних цілей. Дана реалізація мережі дозволяє адміністраторам мережі швидко реагувати на несанкціоновані дії користувачів мережі, які виходять із сегменту.

Рисунок 3.2 - CRS326-24G-2S+RM

Параметри комутатора MikroTik CRS326-24G-2S+RM наведено у таблиці 3.2.

Таблиця 3.2 - Параметри комутатора MikroTik CRS326-24G-2S+RM

Параметр	Значення
Процесор	98DX3236A1
Номінальна частота процесора	800 MHz
Кількість ядер процесора	1
Об'єм оперативної пам'яті	512 MB
Розмір сховища даних	16 MB
Тип сховища даних	FLASH
Інтерфейси	(24) 10/100/1000 Ethernet порт; (2) SFP+ порт; (1) серійний порт RJ45
Обмінна здатність	88 Gbps
Операційна система	RouterOS
Джерело живлення	24V 1.2A адаптер; PoE in Passive PoE
Роз'єм живлення	2 (PoE-IN, DC jack)

Умовно схему підключення всіх пристроїв комп'ютерної мережі можна поділити на три компоненти, які зображені на рисунках 3.3-3.5.

На рисунку 3.3 зображено фрагмент мережі приєднання серверів до інтернету. Маршрутизатор MikroTik CCR2116 є центральним комутуючим вузлом у корпусі. До нього під'єднано сервери HPE ProLiant ML350 Gen10 (USAID) та Cisco UCS C220 M4 (Cisco), які використовуються для розгортання кіберполігону. Також підключено комутатор MikroTik CRS 326.

Рисунок 3.3 – З'єднання центральних комутуючих вузлів

Він забезпечуватиме роботу окремого сегменту мережі, до якого буде підключено обладнання кафедри і у разі несанкціонованих дій чи в разі виникнення позаштатних ситуацій можна буде швидко локалізувати зловмисні дії без втрати роботоздатності інших сегментів мережі. Для додаткового підвищення надійності та безпеки мережі, до комутатора MikroTik CRS 326 підключено резервний канал зв'язку, що дозволяє забезпечити безперебійний доступ до критичних сервісів навіть у разі виходу з ладу основного маршрутизатора. Сервери HPE ProLiant ML350 Gen10 та Cisco UCS C220 M4 підключені через високошвидкісні інтерфейси 10G SFP+, що забезпечує швидкий обмін даними та

мінімізує затримки при виконанні критично важливих завдань. Додатково, кожен сегмент мережі оснащено власною системою моніторингу трафіку і засобами для автоматичного виявлення та реагування на аномалії, що дозволяє оперативно виявляти і нейтралізувати потенційні загрози. Система резервного копіювання даних забезпечує збереження важливої інформації та швидке відновлення у разі збоїв або атак.

До комутатора MikroTik CRS 326 під'єднано навчальні аудиторії кафедри: 4-232, 4-233, 4-235, 4-237, 4-201, 4-203 та 4-205, як показано на рисунку 3.4.

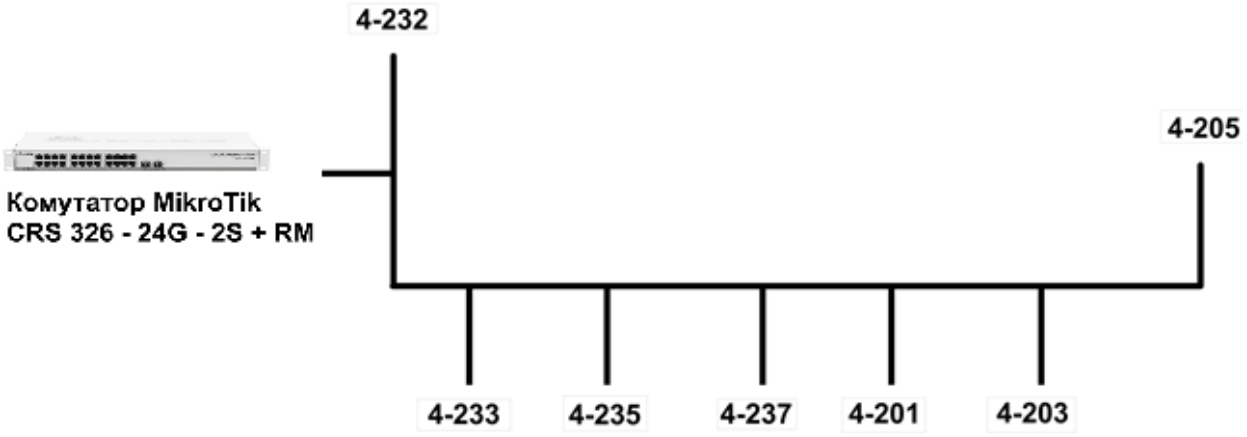


Рисунок 3.4 – Схема підключення навчальних аудиторій до мережі

Це забезпечить локалізацію несанкціонованих дій у разі їх появи до одного комп'ютерного класу. Також полегшить адміністрування комп'ютерної мережі. Кожна з навчальних аудиторій оснащена високошвидкісними Ethernet-підключеннями, що забезпечує стабільну та швидку передачу даних між комп'ютерами та сервером. Це дозволяє ефективно використовувати мережеві ресурси для навчання, тестування та проведення практичних занять з кібербезпеки. Крім того, мережеве обладнання підтримує віртуальні локальні мережі (VLAN), що дозволяє створювати ізольовані сегменти для різних груп користувачів або типів діяльності. Це підвищує безпеку мережі та дозволяє швидко реагувати на будь-які інциденти, ізолюючи їх від основної мережі. Адміністратори мережі мають доступ до централізованої консолі управління, що надає змогу віддалено моніторити стан мережі, здійснювати її налаштування та

вирішувати проблеми. Використання сучасних систем моніторингу та аналізу трафіку дозволяє виявляти підозрілу активність в реальному часі та оперативно вживати заходів для її усунення.

В кожній аудиторії розміщено комутатор D-Link для приєднання персональних комп'ютерів, ноутбуків та інших кінцевих пристроїв, як продемонстровано на рисунку 3.5.

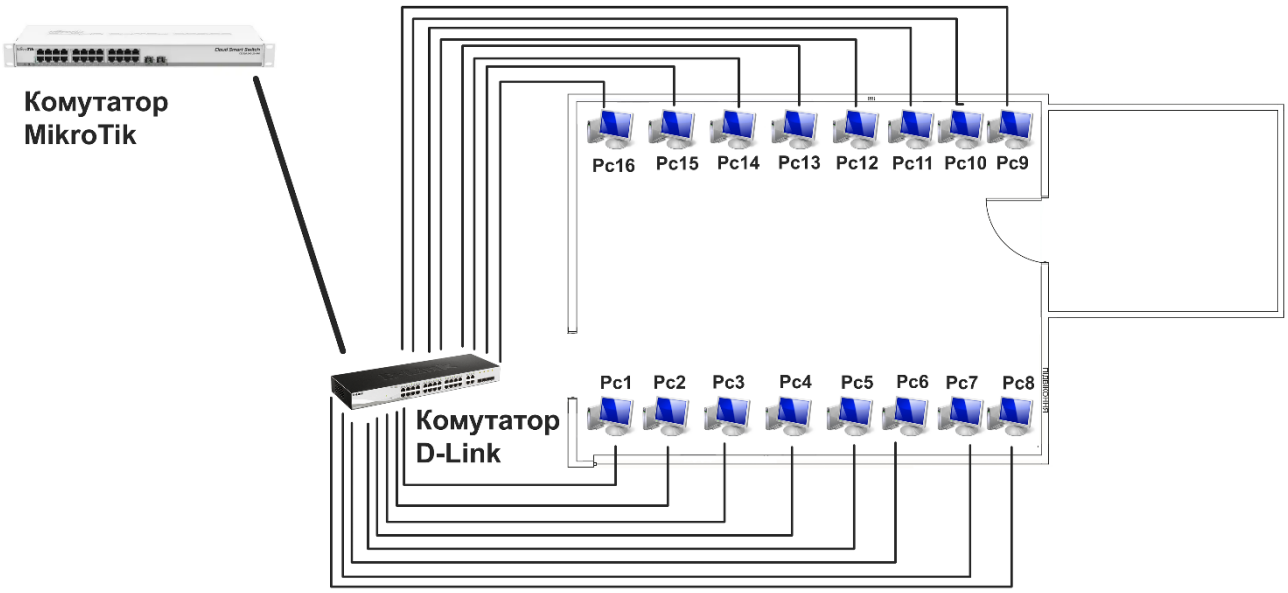


Рисунок 3.5 - Схема підключення пристроїв в навчальній аудиторії до мережі

Ці комутатори забезпечують надійне та швидке підключення всіх кінцевих пристроїв, дозволяючи студентам та викладачам ефективно використовувати мережеві ресурси для навчання та досліджень. Кожен комутатор D-Link підтримує високошвидкісні Ethernet-з'єднання та оснащений достатньою кількістю портів для підключення всіх необхідних пристроїв у класі. Це забезпечує стабільну мережеву взаємодію та мінімізує затримки при передачі даних. Комутатори D-Link також мають функції керування, які дозволяють адміністраторам віддалено контролювати та налаштовувати мережеві параметри кожного класу. Це полегшує процес управління мережею, дозволяє швидко виявляти та усувати проблеми, а також забезпечує належний рівень безпеки. Для підвищення безпеки та продуктивності, комутатори D-Link підтримують функції якості обслуговування

(QoS), що дозволяє пріоритезувати трафік важливих додатків і сервісів. Це особливо корисно під час проведення онлайн-занять, відеоконференцій та інших заходів, що потребують високої якості зв'язку. Загалом, розміщення комутаторів D-Link у кожній аудиторії створює надійну, гнучку та легко керовану мережеву інфраструктуру, що сприяє покращенню навчального процесу та підтримці високих стандартів кібербезпеки.

3.2 Операційні системи

На сервери, які включено до домену, інстальовано ОС Windows Server 2019.

Windows Server 2019 — це серверна операційна система, яка розроблена корпорацією Майкрософт. Є частиною сімейства ОС Windows NT.

До головних функцій та аспектів Windows Server 2019 можна віднести наступне:

– розроблено для інтеграції з Azure, платформою хмарних обчислень Microsoft, оскільки пропонує розширені гібридні можливості, що дозволяє організаціям легко підключати свої локальні середовища до служб Azure;

– питанню безпеки приділено значну увагу в Windows Server 2019. Він включає такі функції, як Windows Defender Advanced Threat Protection (ATP), який допомагає виявляти розширені загрози безпеці та реагувати на них. Крім того, такі функції, як екрановані віртуальні машини та зашифровані мережі, забезпечують покращений захист віртуалізованих робочих навантажень;

– Windows Admin Center — це веб-інтерфейс керування, вперше представлений у Windows Server 2019. Він надає централізовану інформаційну панель для керування серверами, кластерами, гіперконвергентною інфраструктурою та ПК з Windows 10;

– Windows Server 2019 включає вдосконалення підтримки контейнерів і мікросервісів. Він має кращу сумісність із Kubernetes у порівнянні із попередніми версіями, що дозволяє ефективніше розгортати та керувати контейнерними програмами;

– Storage Spaces Direct дозволяє створювати високодоступні та масштабовані програмно-визначені рішення для зберігання, використовуючи стандартні сервери з локально підключеними дисками;

– Windows Server 2019 містить оновлення Hyper-V, платформи віртуалізації Microsoft. Ці вдосконалення покращують масштабованість, продуктивність і безпеку для віртуалізованих робочих навантажень;

– Windows Server 2019 пропонує покращену підтримку віртуальних машин Linux, що спрощує запуск середовищ зі змішаними ОС.

Загалом, Windows Server 2019 розроблено, щоб забезпечити надійну, масштабовану та безпечну платформу для виконання широкого діапазону серверних навантажень, від традиційних локальних додатків до хмарних служб.

3.3 Забезпечення відмовостійкості

Забезпечення стабільної роботи сервера - це важливий фактор для ефективного використання за призначенням. Для стабільної роботи кіберполігону виконано та передбачено наступні дії:

– доменний адміністратор відповідає за регулярне оновлення програмного забезпечення, а саме встановлення оновлень і патчів безпеки для ОС, додатків і програмного забезпечення;.

– передбачено автоматичне резервне копіювання цінних даних за допомогою NAC;

– встановлено програмне забезпечення для моніторингу серверів, щоб виявляти проблеми, такі як перевантаження процесора чи проблеми з мережею, та реагувати на них до того, як вони призведуть до відмови сервера;

– із правом на читання для локальних користувачів на сервері розміщено підготовлені образи віртуальних машин, які мають різні ОС та набори програмного забезпечення, тому можна обирати відповідно до поставленого завдання і у разі краху віртуальної машини можна буде за лічені хвилини повторно розгорнути віртуальну машину;

– налаштовано управління доступом, адже передбачено обмеження доступу до серверів за типом користувача, встановлено права доступу відповідно до ролей та обов'язків користувачів;

– заплановано систематичну перевірку використаних ресурсів задля видалення користувачів чи віртуальних машин, які не використовуються протягом тривалого часу.

Задля того, щоб сервери працювали безперебійно при відсутності електроживлення розроблено ряд заходів, зокрема сервери мають дві лінії електроживлення (у разі аварійного вимкнення однієї інша автоматично вмикається), передбачено живлення від генератора. Дані заходи забезпечать роботу серверів та доступ до них віддалено.

3.5 Висновки до розділу

Схема мережі кіберполігону ретельно спланована для оптимального розміщення та підключення обладнання, що включає маршрутизатор MikroTik CCR2116-12G-4S+ і комутатор MikroTik CRS326-24G-2S+RM для забезпечення надійного та високопродуктивного мережевого з'єднання. Це дозволяє ефективно керувати мережевими потоками і забезпечити швидке реагування на несанкціоновані дії у мережі. Система використовує відповідно підібрані оперативні системи, зокрема Windows Server 2019, що забезпечує розширені гібридні можливості та вдосконалену безпеку з використанням функцій, як Windows Defender ATP. Таке обладнання і програмне забезпечення сприяє створенню стабільної та безпечної платформи для виконання навчальних та дослідницьких завдань у сфері кібербезпеки. Також забезпечення відмовостійкості кіберполігону є пріоритетним, що включає налаштування резервного копіювання даних, систем моніторингу серверів та регулярне оновлення програмного забезпечення. Ретельне планування використання ресурсів і управління доступом допомагає запобігати простоям і забезпечує високий рівень оперативності та безпеки кіберполігону.

ВИСНОВКИ

Дана кваліфікаційна робота зосереджена на розробці кіберполігону, який є симулятивним середовищем для дослідження мережевого трафіку та моніторингу поведінки систем під час кібератак на кінцеві пристрої. Для досягнення цієї мети визначено наступні етапи: підготовка апаратної складової, налаштування систем збору даних, встановлення та конфігурація програмного забезпечення для аналізу мережевого трафіку, а також розробка методів класифікації атак та формування політики безпеки.

В основу технічного забезпечення полігону лягли високопродуктивні сервери з потужними процесорами та великим обсягом пам'яті, що дозволяє емулювати різноманітні мережеві середовища. Використання таких інструментів як Nessus, Wireshark, та Metasploit забезпечує комплексний підхід до аналізу вразливостей та тестування захисних механізмів.

Кіберполігон розроблено з можливістю легкої інтеграції нового обладнання та оновлення програмного забезпечення, що робить його адаптивним до змінних умов і вимог сучасного цифрового світу. Розгортання полігону включає налаштування надійної мережевої інфраструктури з використанням сучасних маршрутизаторів та комутаторів, забезпечуючи високу пропускну здатність та швидке реагування на мережеві інциденти.

Важливу роль відіграє забезпечення відмовостійкості та безперебійної роботи полігону, що досягається за рахунок систем резервного копіювання, моніторингу стану серверів та регулярного оновлення безпеки. Робота полігону максимально ізольована від зовнішніх мереж, що забезпечує безпеку проведених досліджень та мінімізує ризик негативного впливу на інші системи.

Таким чином, розроблений кіберполігон є комплексною платформою, що забезпечує ефективне навчання та вдосконалення навичок з кібербезпеки, розробку та тестування новітніх методологій захисту, а також проведення наукових досліджень в цій важливій області.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Комп’ютерні мережі. Частина 1. Моделювання комп’ютерних мереж: Лабораторний практикум. / Укладачі: О. С. Яценко, О. І. Яценко. – Житомир: Вид-во ЖДУ ім. І. Франка, 2022. – 76 с.

2. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. – Київ, 2021. – 84 с.

3. Що таке фішинг? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 5.02.2024).

4. Головко Д.Ю. Бепек в цифровому просторі : електронний навчальний курс / Д.Ю. Головко. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2024. – 54 с.

5. The Evolution of Ransomware: Victims, Threat Actors, and What to Expect in 2022. URL: https://cdn2.assets-servd.host/giftedzorilla/production/files/Ransomware-Trends-Victims-Threat-Actors.pdf (дата звернення: 07.02.2024).

6. Є. Богданова, Т. Чорна, С. Малахов. Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп’ютерні науки та кібербезпека*. 2022. Випуск 2. ст.35-40. DOI: 10.26565/2519-2310-2022-2-04.

7. С. Легомінова, Г. Гайдур. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. Випуск 2. с.54–67. DOI: 10.28925/2663-4023.2023.22.5467.

8. Nitesh Kumar, Gaurav S. Kasbekar, D. Manjunath. Application of Data Collected by Endpoint Detection and Response Systems for Implementation of a Network Security System based on Zero Trust Principles and the EigenTrust Algorithm. *SIGMETRICS Perform*. 2023. Vol. 4. PP.5–7. DOI: 10.1145/3595244.3595247.

9. Siji FG, Uche OP. An improved model for comparing different endpoint detection and response tools for mitigating insider threat. *Indian Journal of Engineering*. 2023. Vol. 20. DOI: 10.54905/disssi/v20i53/e22ije1651.

10. P. J. Divya, R. S. George, G. Madhusudhan, S. Padmasree. Organization-

wide IOC Monitoring and Security Compliance in Endpoints using Open Source Tools. *IEEE 3rd Global Conference for Advancement in Technology (GCAT)*. 2022. PP. 1-6. DOI: 10.1109/GCAT55367.2022.9971999.

11. A. Shaji George, S. Sagayarajan, Dr. T. Baskar, A. S. Hovan George. Extending Detection and Response: How MXDR Evolves Cybersecurity. *Partners Universal International Innovation Journal*. 2023. Vol. 1, No 4, PP. 268–285. DOI: 10.5281/zenodo.8284342.

12. D. L. Pissanidis, K. Demertzis. Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and its Application in Intrusion Detection and System Log Management. *Preprints*. 2023. DOI: 10.20944/preprints202312.0205.v2.

13. L.F. Ilca, O.P. Lucian, T.C. Balan. Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. *Sensors*. 2023. Vol. 23, P. 6757. DOI: 10.3390/s23156757.

14. R. Shaw, S. Parveen. Literature Review on Packet Sniffing: Essential for Cybersecurity & Network Security. *5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2024. PP. 715-719. DOI: 10.1109/ICICV62344.2024.00119.

15. Топ 10 кращих програм для моніторингу мереж у 2024. URL: https://www.softinventive.com.ua/best-network-monitoring-tools (дата звернення: 23.02.2024).

16. K. M. Majidha Fathima, N. Santhiyakumari. A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap. *International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. 2021. PP. 1136-1141. DOI: 10.1109/ICAIS50930.2021.9395852.

17. P. S. Vijaya, N. Neelima, S. Shahin, Y. G. Krishna. Ethical Hacking and Demonstrating Network Exploits using Wireshark. *2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*. 2023. PP. 1058-1063. DOI: 10.1109/ICACRS58579.2023.10404948.

18. N. Kunhare, R. Tiwari, J. Dhar. Network Packet Analysis in Real Time Traffic and Study of Snort IDS During the Variants of DoS Attacks. *Hybrid Intelligent*

Systems. HIS 2019. Advances in Intelligent Systems and Computing. 2021. Vol 1179. DOI: 10.1007/978-3-030-49336-3_36.

19. A. Shahraki, M. Abbasi, A. Taherkordi, A.D. Jurcut. Active Learning for Network Traffic Classification: A Technical Study. *IEEE Transactions on Cognitive Communications and Networking*. 2022. Vol. 8, No 1, PP. 422-439. DOI: 10.1109/TCCN.2021.3119062.

20. A. Azab, M. Khasawneh, S. Alrabaee, K.-K. R. Choo, M. Sarsour. Network traffic classification: Techniques, datasets, and challenges. *Digital Communications and Networks*. 2022. DOI: 10.1016/j.dcan.2022.09.009.

21. T. Subbulakshmi, R.A. and other. Real-time Visualization and Classification of DDoS Attack using Supervised Learning Algorithms. *Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS 2023*. 23-25 November 2023, Lavasa, Pune, India.

22. C. Bachechi, L. Po, F. Rollo. Big Data Analytics and Visualization in Traffic Monitoring. *Big Data Research.* 2022. Vol. 27. DOI: 10.1016/j.bdr.2021.100292.

23. N. Gupta, V. Jindal, P. Bedi. A Survey on Intrusion Detection and Prevention Systems. *SN COMPUT. SCI.* 2023. Vol. 4, P. 439. DOI: 10.1007/s42979-023-01926-7.

24. R. Abhijith, B. J. Santhosh Kumar. First Level Security System for Intrusion Detection and Prevention in LAN. *2nd International Conference for Emerging Technology (INCET)*. 2021. PP. 1-5. DOI: 10.1109/INCET51464.2021.9456259.

25. W. Zegeye, M. Odejobi. Telemetry Networks Cyber Security Architecture. *International Telemetering Conference Proceedings*. 2022. P. 57.

26. Rangeforce. URL: https://www.rangeforce.com/ (дата звернення: 23.02.2024).

27. В Україні запустили кіберполігон UNIT Range. URL: https://ain.ua/2023/06/14/v-ukrayini-zapustyly-kiberpoligon-unit-range/ (дата звернення: 25.02.2024).

28. UNIT Range. URL: https://www.unitrange.com/ (дата звернення:

25.02.2024).

29. Роль навчальних кіберполігонів у підготовці фахівців у сфері кібербезпеки. URL: https://conf.ztu.edu.ua/wp-content/uploads/2023/06/36-1.pdf (дата звернення: 2.03.2024).

30. Навчальний кіберполігон відкрили в Житомирському військовому інституті. URL: https://censor.net/ua/photo_news/3222663/navchalnyyi_kiberpoligon_vidkryly_v_jytomyrskomu_viyiskovomu_instytuti_fotoreportaj (дата звернення: 2.03.2024).

31. Віртуальний полігон – Кібербезпека. URL: http://cs.tneu.edu.ua/?p=364 (дата звернення: 4.03.2024).

32. У ЗСУ функціонуватиме надсучасний кіберполігон VITIsecurity: на кафедрі кібербезпеки розгорнуто навчально-тренувальний комплек. URL: https://www.facebook.com/271060753242247/posts/1588909041457405 (дата звернення: 5.03.2024).

33. Кіберполігон - Кафедра кібербезпеки та інформаційних технологій. URL: https://www.kafcbit.hneu.edu.ua/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D0%B3%D0%BE%D0%BD/ (дата звернення: 11.03.2024).

34. Сервер hpe proliant ml350 gen10 (877623-421). URL: https://server-store.com.ua/ua/p811668789-server-hpe-proliant.html (дата звернення: 15.04.2024).

35. Сервер HP ProLiant ML350 Gen10 (877621-421). URL: https://hotline.ua/ua/computer-servery/hp-proliant-ml350-gen10-877621-421 (дата звернення: 15.04.2024).

36. Сервер HPE ML350 Gen10 (P11050-421). URL: https://e-server.com.ua/uk/server_hpe-ml350-gen10-p11050-421 (дата звернення: 16.04.2024).

37. Cisco UCS C220 M4 Rack Server. URL: https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c220-m4-rack-server/model.html (дата звернення: 21.04.2024).

38. Medusa. URL: https://www.kali.org/tools/medusa/ (дата звернення:

22.04.2024).

39. Hydra. URL: https://www.kali.org/tools/hydra/ (дата звернення: 22.04.2024).

40. Wireshark Documentation. URL: https://www.wireshark.org/docs/ (дата звернення: 23.04.2024).

41. Angry IP Scanner. URL: https://angryip.org/ (дата звернення: 25.04.2024).

42. ZAP (Zed Attack Proxy). URL: https://www.zaproxy.org/docs/ (дата звернення: 25.04.2024).

ДОДАТОК А

(обов'язковий)

Копія графічної частини

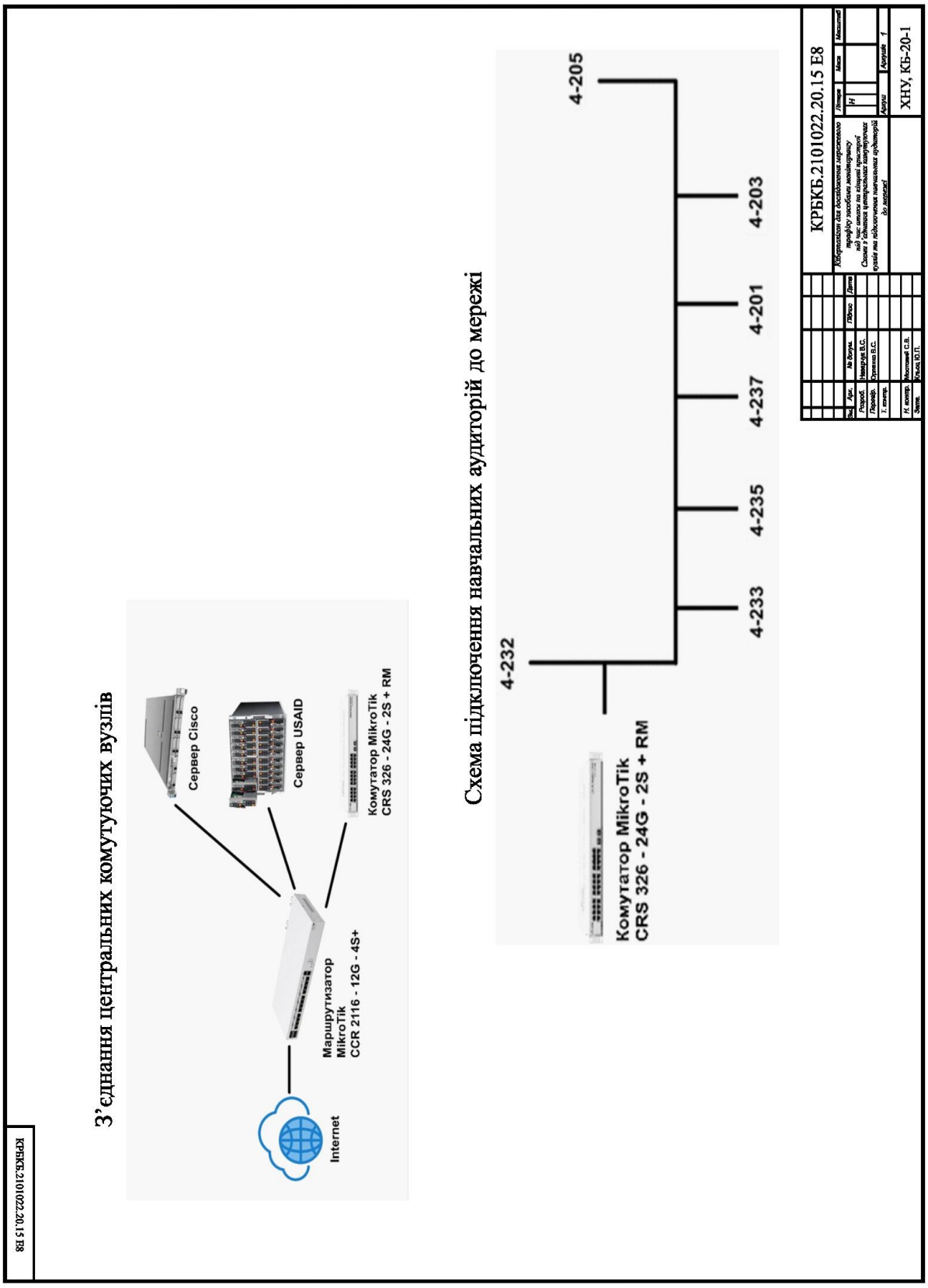
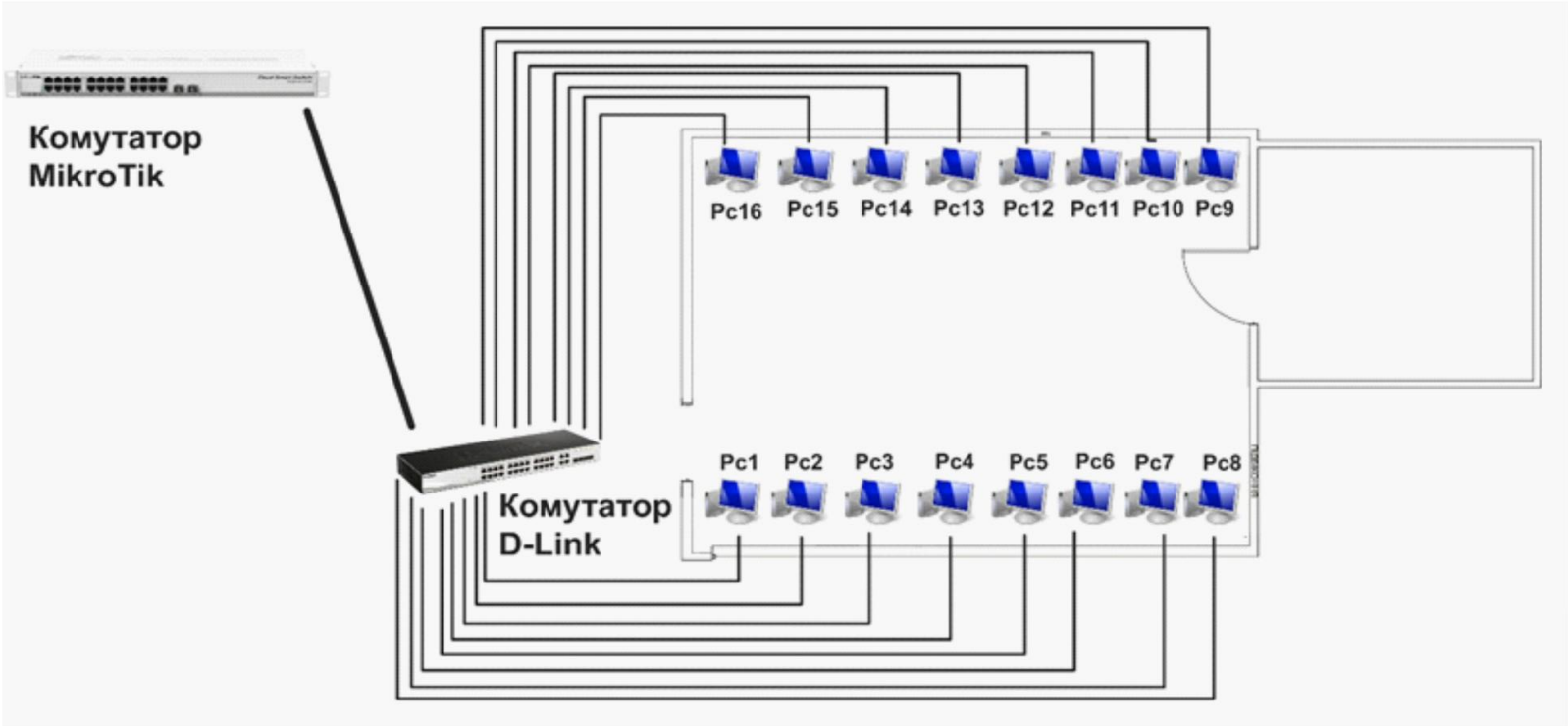
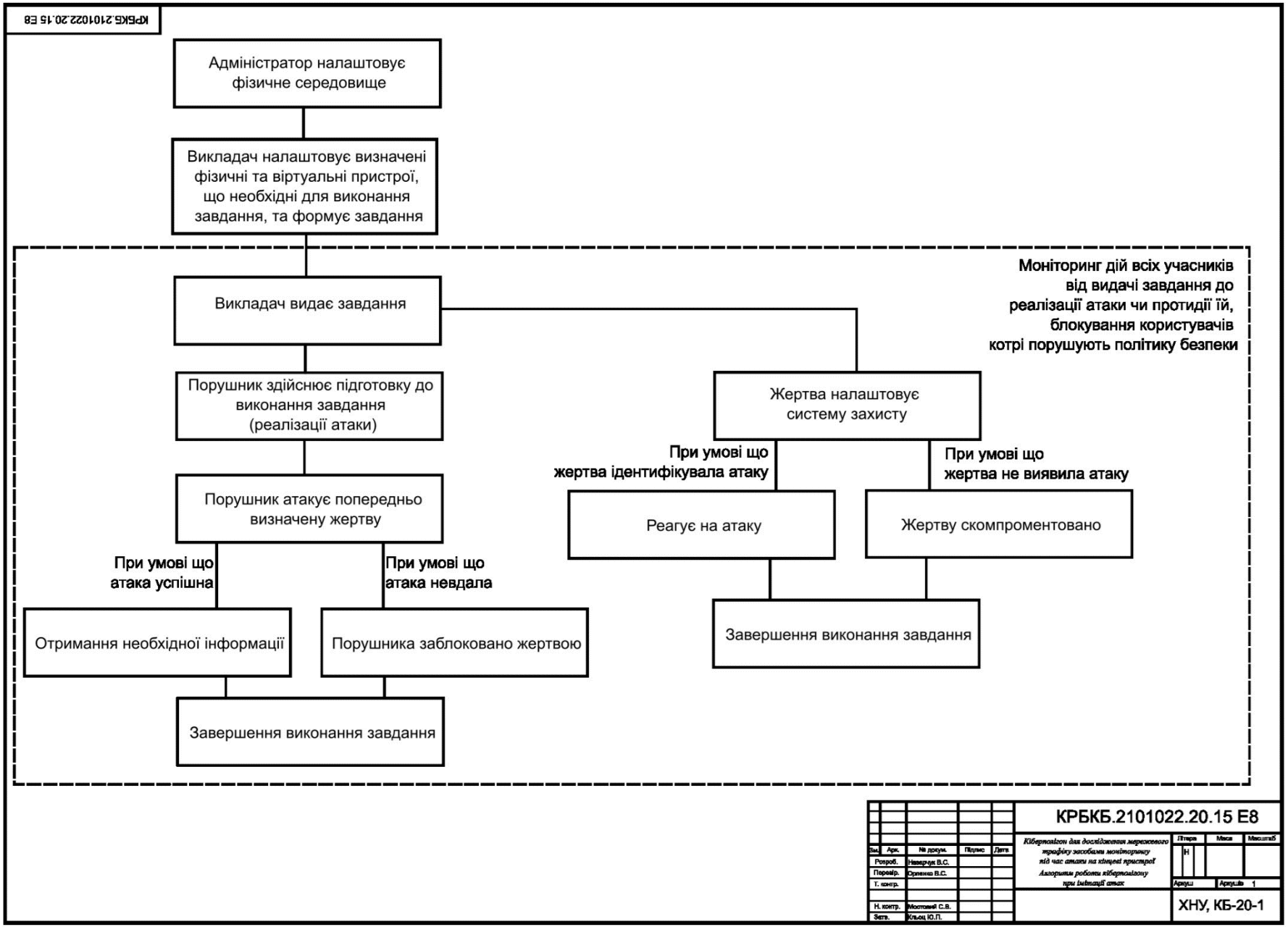


Схема підключення пристроїв в навчальній аудиторії до комп'ютерної мережі



					КРБКБ.2101022.20.15 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої. Схема підключення пристроїв в навчальній аудиторії до комп'ютерної мережі	Літера: Н; Маса; Масштаб
Розроб.		Навернук В.С.				Аркуш 1; Аркушів
Перевір.		Орленко В.С.				
Т. контр.						
Н. контр.		Мостовий С.В.			ХНУ, КБ-20-1	
Затв.		Кільоц Ю.П.				


КРБКБ.2101022.20.15 Е8
Адміністратор налаштовує фізичне середовище
Викладач налаштовує визначені фізичні та віртуальні пристрої, що необхідні для виконання завдання, та формує завдання
Моніторинг дій всіх учасників від видачі завдання до реалізації атаки чи протидії їй, блокування користувачів котрі порушують політику безпеки
Викладач видає завдання
Порушник здійснює підготовку до виконання завдання (реалізації атаки)
Порушник атакує попередньо визначену жертву
При умові що атака успішна
При умові що атака невдала
Отримання необхідної інформації
Порушника заблоковано жертвою
Завершення виконання завдання
Жертва налаштовує систему захисту
При умові що жертва ідентифікувала атаку
При умові що жертва не виявила атаку
Реагує на атаку
Жертву скомпрометовано
Завершення виконання завдання
КРБКБ.2101022.20.15 Е8
Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої
Алгоритм роботи кіберполігону при імітації атак
Літера
Маса
Масштаб
Аркуш
Аркушів 1
ХНУ, КБ-20-1

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Назарчука Валерія Сергійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.06.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

ID: 129877 Назва: Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атак на кінцеві пристрої Додано в БД: 2024-06-12 Автора: Назарчук В.С. Керівники: Орленко В.С. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	81090	624	502 (1%)	5 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016351570

Дата перевірки:
12.06.2024 11:28:18 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.06.2024 11:34:20 EEST

ID користувача:
100008300

Назва документа: **Назарчук_записка плагіат**

Кількість сторінок: **58** **Кількість слів:** **11193** **Кількість символів:** **89273** **Розмір файлу:** **3.68 MB** **ID файлу:** **1016155234**

3.82%
Схожість

Найбільша схожість: **0.87%** з Інтернет-джерелом (https://rstforums.com/forum/topic/111130-thc-hydra-90)

3.32% Джерела з Інтернету	201	Сторінка 60
0.88% Джерела з Бібліотеки	41	Сторінка 61

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	3

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атак на кінцеві пристрої

Автор: Назарчук Валерій Сергійович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Орленко Вікторія Сергіївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 96,18%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Вікторія ОРЛЕНКО

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Назарчук Валерій Сергійович

Тема Кіберполігон для дослідження мережевого трафіку засобами моніторингу під час атак на кінцеві пристрої

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 63.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі було розроблено кіберполігон для дослідження мережевого трафіку під час атак на кінцеві пристрої. Основна мета полягає у створенні спеціального середовища для тренування та тестування заходів кібербезпеки. Для цього було виконано такі завдання: розроблено та налаштовано апаратну і програмну складові кіберполігону, впроваджено політику безпеки, розгорнуто та протестовано систему, включаючи забезпечення відмовостійкості. Крім того, було створено схему мережі та описано процес розгортання операційних систем. Проведено оцінку ефективності розробленого кіберполігону, що забезпечує реалістичні умови для навчання та підготовки фахівців з кібербезпеки.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи наведена загальна характеристика проблеми кібербезпеки, визначені об'єкт, предмет та методи дослідження, а також сформульована мета роботи. Розглянуто актуальність створення кіберполігонів для тренування та тестування заходів кібербезпеки. У першому розділі розглядається роль кіберполігону для дослідження кібератак, а також роль кінцевих пристроїв у безпеці мережі. Проведено огляд існуючих рішень полігонів, визначено їх призначення та постановку задачі. У другому розділі описуються параметри та налаштування кіберполігону. Наведено деталі апаратної та програмної складових, а також політику безпеки, яка забезпечує захист даних та систем. У третьому розділі розглянуто процес розгортання кіберполігону. Описано схему мережі, налаштування операційних систем та заходи для забезпечення відмовостійкості. Проведено тестування системи та оцінку її ефективності у виявленні та реагуванні на кібератаки.

4. Позитивні сторони Розробка кіберполігону має практичну цінність. Він створений для дослідження мережевого трафіку засобами моніторингу під час атаки на кінцеві пристрої, що активно використовуватиметься для практичного навчання студентів. Кіберполігон дозволяє організаціям тестувати свої заходи захисту, виявляти вразливості та реагувати на кібератаки в контрольованому середовищі. Це сприяє підвищенню рівня готовності та навичок персоналу у вирішенні кібербезпекових викликів, підвищуючи загальний рівень безпеки інформаційних систем. Завдяки цьому організації можуть ефективніше протидіяти кіберзагрозам та мінімізувати ризики фінансових втрат і втрати конфіденційної інформації

5. Негативні сторони роботи Підготовка та налаштування кіберполігону потребує детального планування і значного часу на підготовку етапів виконання завдань, які не передбачають альтернативних рішень. Це може обмежити гнучкість у навчальному процесі та потребуватиме постійного оновлення бази завдань для забезпечення актуальності навчання.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович,
завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор

« 12 » червня 2024 _____ (підпис)