

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

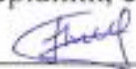
до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект підсистеми захисту локальної мережі підприємства від
атак різних типів»

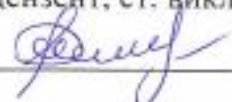
Виконав студент 4-го курсу, групи КБ-І
спеціальності 125 «Кібербезпека»

 Савчук А.В.

Керівник, ст. викладач кафедри КІ та КБ

 Покотило О.А.

Рецензент, ст. викладач кафедри КІ та КБ

 Байлюк Є.М.

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Савчука Андрія Васильовича

Тема роботи: **Проект підсистеми захисту локальної мережі підприємства від атак різних типів**

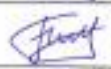
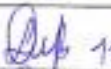
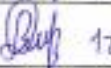
затверджена Наказом по університету від «12» Квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «23» Червня 2021р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Комутатори Cisco
5. Операційні системи Cisco IOS, Windows XP, Windows 7, Kali Linux
6. Графічний симулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	 12.04.2021	 12.04.2021
2	Покотило О.А.	 12.04.2021	 12.04.2021
3	Покотило О.А.	 12.04.2021	 12.04.2021

Керівник  Покотило О.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз технологій захисту мережі за допомогою налаштувань на маршрутизаторах та комутаторах CISCO	12 квітня 2021 – 16 квітня 2021	Виконано
4	Аналіз можливостей мережного обладнання Cisco для локальної мережі	17 квітня 2021 – 19 квітня 2021	Виконано
5	Розробка загального проекту мережі підприємства	20 квітня 2021 – 24 квітня 2021	Виконано
6	Проектування мережі та вибір обладнання для її реалізації	25 квітня 2021 – 30 квітня 2021	Виконано
7	Проектування таблиці маршрутизації	1 травня 2021 – 4 травня 2021	Виконано
8	Проектування сценарію тестування мережі	5 травня 2021 – 9 травня 2021	Виконано
9	Базове налагодження пристроїв мережі	10 травня 2021 – 13 травня 2021	Виконано
10	Налагодження локальної мережі	14 травня 2021 – 18 травня 2021	Виконано
11	Тестування роботи локальної мережі	19 травня 2021 – 22 травня 2021	Виконано
12	Аналіз результатів тестування	23 травня 2021 – 24 травня 2021	Виконано
13	Написання пояснювальної записки	25 травня 2021 – 29 травня 2021	Виконано
14	Підготовка презентації та виступу	30 травня 2021 – 31 травня 2021	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2021 – 8 червня 2021	Виконано
16	Захист	22 червня 2021	Виконано

Студент  Савчук А.В.

Керівник  Покотило О.А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми захищеної локальної мережі підприємства від різних типів атак на неї та пояснювальної записки до нього. Пояснювальна записка містить 60 сторінок, 75 ілюстрацій та 2 таблиці.

Проект присвячений захисту локальної мережі підприємства від різних типів атак. Метою проекту буде налаштування захисту мережі для того, щоб мережа безперервно працювала, і зловмисники не мали змоги її атакувати. Також буде перевірка мережі на захист способом тестування мережі різними типами атак. Додатково буде налаштовано віддалений доступ до пристроїв мережі.

Пояснювальна записка складатиметься з трьох розділів, в які входять теоретична розробка мережі, вибір програмного-апаратного забезпечення, базове налагодження мережі, тестування мережі, налагодження захисту мережі та його перевірка за допомогою виконання різних типів атак.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖА ПІДПРИЄМСТВА, АТАКА, CISCO, KALI LINUX.

					КБ.КВ.Б – 125 -21 -ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту локальної мережі підприємства від атак різних типів Пояснювальна записка	Лист	Арк.	Архів
Розроб.		Савчук А. В.		22.06.21				
Керівник		Покошило О. А.		22.06.21			4	61
Рецензент		Байлок С. М.		22.06.21		Державний університет «Житомирська політехніка», група КБ-1		
Зав. каф.		Ефіменко А. А.		22.06.21				

ABSTRACT

Qualification work consists of a project of the local network of the enterprise and attacks on this network with the help of different types of attacks and an explanatory note to it. The explanatory note contains 60 pages, 75 illustrations and 2 tables.

The project is dedicated to protecting the local network of the enterprise from various types of attacks. The goal of the project will be to configure network security so that the network runs continuously and intruders cannot attack the network. There will also be a network security check by testing the network with different types of attacks. Remote access to network devices will also be set up.

The explanatory note will consist of three sections, which include theoretical network development, software and hardware selection, basic network debugging, network testing, network security debugging and verification by performing various types of attacks. KEY WORDS: DEFENSE, LOCAL NETWORK, ENTERPRISE NETWORK, ATTACK, CISCO, KALI LINUX.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ	Ошибка! Закладка не определена.
ABSTRACT	5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА. РІЗНОВИДИ АТАК НА МЕРЕЖУ ТА СПОСОБИ ЗАХИСТУ	10
1.1 Особливості побудови локальної мережі підприємства	10
1.2 Різновиди атак	12
1.3 Захист системи	16
1.4 Загальні технічні відомості та вимоги до програмного та апаратного забезпечення мережі.	18
РОЗДІЛ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА	20
2.1 Проект локальної мережі підприємства	20
2.2 Розробка структури мережі.....	22
2.3 Вибір обладнання та програмного забезпечення.....	25
РОЗДІЛ 3 НАЛАШТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ТА ЗАХИСТ ЇЇ ВІД РІЗНИХ ТИПІВ АТАК	29
3.1 Базове налаштування мережі	29
3.2 Перевірка базових налаштувань мережі та проведення атак на неї	38
3.3 Налаштування захисту та перевірка роботи мережі	46
3.4 Аналіз результатів тестування.....	55
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	59
ДОДАТКИ.....	61

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОС – Операційна система

DHCP – Dynamic Host Configuration Protocol

OSFP – Open Shortest Path First

DIA – Dynamic ARP Inspection

ARP – Address Resolution Protocol

MAC – Media Access Control

IP – Internet Protocol

DOS – Denial of Service

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В наш час інтернет став невід'ємною частиною життя. З кожним днем в мережі з'являється все більше і більше користувачів, проте не кожен з них задумується про свою інформаційну безпеку. Існує багато способів для того, щоб дізнатися інформацію про ту чи іншу людину. Найчастіше це соціальні мережі та електронні пошти. Відсутність захисту чи необдуманно введена інформація дає хакерам змогу отримати доступ до персональної інформації людини. Небезпека заключається в тому, що злочинці можуть використовувати облікові записи для розповсюдження спаму та шкідливих посилань, які в свою чергу збільшують кількість постраждалих. Не рідкі випадки, коли злочинці знаходять на електронній пошті логіни та паролі від платіжних сервісів та використовують це з метою свого збагачення.

Проте не тільки люди потребують інформаційного захисту. Багато підприємств також потребують захисту від різних типів атак. Більшість компаній не можна уявити без доступу до глобальної мережі Інтернет, оскільки вони працюють з великим обсягом інформації з різної точки світу. Візьмемо, наприклад, мережу банку: вона працює з інформацією робітників та клієнтів. Оскільки це банк, майже вся інформація являється персональною та конфіденційною та потребує захисту.

В такому випадку страждають не сотні чи тисячі людей, а набагато більше. Тому великі підприємства потребують постійного захисту на мережевому рівні.

Не рідкі випадки, коли кіберзлочини здійснюються з метою позбутися конкурентів чи нанести шкоду бізнесу конкурентів. В таких випадках бізнеси людей, тобто онлайн магазини, форуми, сайти і тому подібне несуть великі втрати.

Стрімкий зріст кіберзлочинності обумовлюється тим, що злочинці можуть швидко отримати незаконний дохід, тому потрібно задуматися про свою інформаційну безпеку, адже однією обережністю себе не захистити.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

Метою кваліфікаційної роботи є розробка підсистеми захисту локальної мережі підприємства.

Встановлена мета створює наступні завдання:

- вибір та аналіз сучасних приладів;
- вибір засобів для реалізації підмережі;
- вибір засобів для атаки на мережу;
- тестування та реакція мережі на атаку;
- розробка системи захисту для мережі.

Об’єктом дослідження є процес захисту локальної підмережі від різних типів атак.

Предметом дослідження є методи і засоби для розробки захисту в локальній підмережі.

В процесі розробки кваліфікаційної роботи був розроблений проект підсистеми захисту локальної мережі від різних типів атак. При цьому для виконання атак було використано операційну систему Kali Linux.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА. РІЗНОВИДИ АТАК НА МЕРЕЖУ ТА СПОСОБИ ЗАХИСТУ

1.1 Особливості побудови локальної мережі підприємства

Локальна мережа – це мережа з обмеженою кількістю користувачів, що об'єднує всю систему в одне підприємство. Тобто, локальна мережа створюється для того, щоб об'єднати всі пристрої в одне ціле, із загальним чи обмеженим доступом до файлів, папок і тому подібне[1]. Головною складовою локальної мережі є:

- маршрутизатори;
- комутатори;
- робочі станції.

При розробці локальної мережі потрібно вибрати правильну топологію. Існує 3 найпопулярніших топології:

- шина;
- кільцева;
- зірка.

Топологія шина складається з кабелю, до якого під'єднані всі робочі станції. До переваг даної топології відносять:

- проста для адміністрування;
- низька вартість.

Основний недолік те, що в випадку пошкодження кабелю вся мережа виходить з ладу.

Кільцева топологія складається з вузлів, які з'єднуються між собою по колу. Основні переваги даної топології: її легко створювати та налаштовувати. До недоліків відносять те, що пошкодження одного вузла приводить до несправності всієї мережі.

В топології зірка всі робочі станції під'єднуються до комутатора. Основні переваги даної топології:

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

- висока працездатність;
- якщо пошкоджена одна робоча станція, це не впливає на роботу мережі;
- швидкий пошук несправностей;
- легко додавати нові робочі станції.

Серед недоліків виділяють наступні:

- кількість робочих станцій обмежена портами комутатора;
- несправність комутатора призводить до несправності мережі чи підмережі.

Тобто, основним недоліком перших двох топологій є те, що в випадку коли кабель буде пошкоджено, вся мережа виходить з ладу, що дуже погано відзначиться на працездатності мережі. Тобто кожна із них має як свої плюси так мінуси, і на це потрібно звертати увагу при виборі[2].

При створенні мережі підприємства слід взяти до уваги, що це мережа конкретного підприємства, користувачами якого є співробітники даної мережі. Прийнято вважати, що мережа підприємства працює на протоколі ТСП/ІР. Часто така мережа працює на «приватних» адресах, в зв'язку з тим що ІР адрес з часом стало не достатньо. Також в мережах підприємства використовується динамічна видача адрес, ДНСР. Даний протокол використовується для того, щоб різні робочі станції отримали свою адресу і не було повторів, через які не зможе працювати співробітник підприємства.

Також, як і будь-яка мережа, мережа підприємства потребує захисту. В наш час не можна уявити підприємство, яке не має доступу до глобальної мережі Інтернет. Підключивши мережу до Інтернету, підприємство наражає себе на небезпеку. Хакери намагаються дізнатися інформацію будь-якими методами, тому потрібно мати достатньо надійний захист від:

- спроб злому;
- спаму;
- завантаження та установки вірусних програм;
- несанкціонованому доступу до персональних даних.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

При цьому, необхідно налагодити захист так, щоб це не заважало співробітникам мати змогу безперешкодно користуватися мережею підприємства.

1.2 Різновиди атак

Розвиток технологій не стоїть на місці і стрімко йде вгору. Не кожна людина в даний період розвитку встигає дізнатися та вивчити інформацію про свою безпеку в мережі. Проте зловмисники не стоять на місці, а також вигадують, знаходять помилки в обладнаннях чи коді, і користуються цим в своїх цілях. На сьогоднішній день існує дуже багато різних атак, які здійснюють хакери для того, щоб дізнатися ту чи іншу інформацію, зламати сайти, заволодіти мережею і тому подібне. Для того, щоб захиститися від різних типів атак, потрібно знати, як вони працюють. На великих підприємствах захистом мережі займаються адміністратори. Розберемо деякі типи атак, щоб знати як правильно і надійно від них захищатися.

Rogue DHCP Server - це атака, яка спрямована на DHCP сервера. Порушник вичерпує всі адреси, які пропонує справжній сервер, а далі видає себе за сервер і пропонує всім іншим користувачам в мережі IP-адреси та інші мережеві налаштування. Тобто зловмисник впроваджує в мережі свій несправжній сервер (рис.1.1).

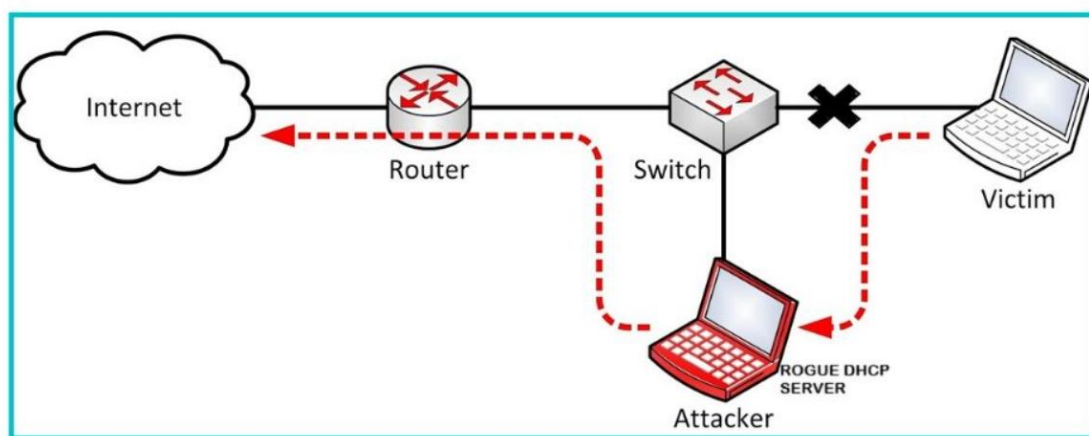


Рис. 1.1. Принцип роботи Rogue DHCP Server

Цей сервер має змогу відповідати на запити клієнтів на виявлення DHCP. У випадку, коли користувач отримує дані зловмисного сервера, це може порушити доступ до мережі, спричиняючи DoS. У результаті, зловмисник отримує весь трафік від клієнта і перенаправляє на шлюз по замовчуванню. Такі атаки залишаються впродовж довгого часу непомітними, тому що клієнт вважає, що працює правильно. Зловмисник за допомогою даних маніпуляцій намагається отримати дані користувачів мережі[3].

DHCP starvation - це атака, за допомогою якої порушники посилають багато підроблених пакетів DISCOVER, доки DHCP сервер не втратить всі IP-адреси. Тобто, якщо клієнт захоче отримати IP-адресу, в нього нічого не вийде, так як буде відмовлено в доступі. Крім того, порушник може створити свій DHCP сервер для того, щоб надавати свої IP-адреси для перехоплення трафіку клієнта. Для того, щоб перехопити всі IP-адреси, порушник надсилає сотні пакетів DHCP DISCOVER, використовуючи підроблені MAC-адреси (рис.1.2)[4].

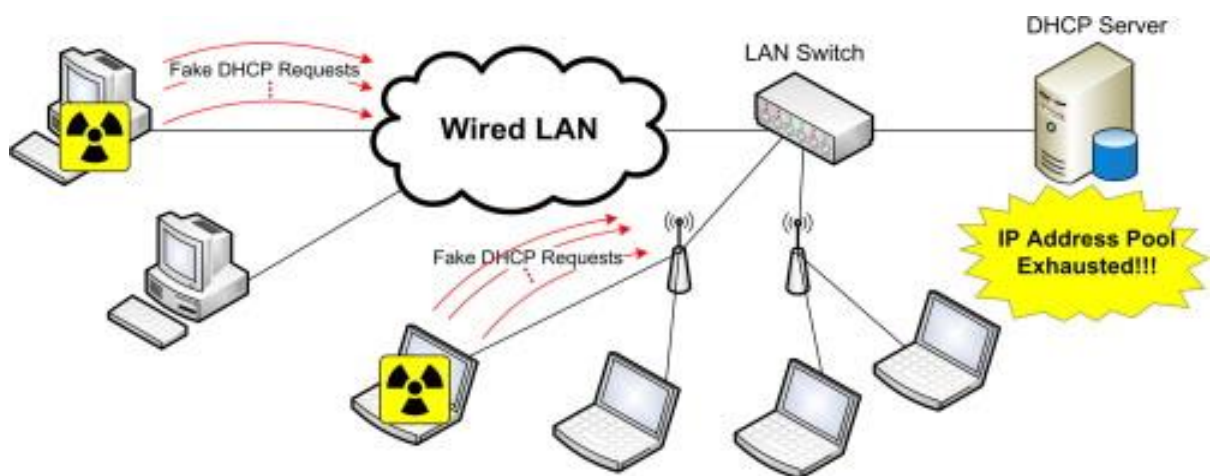


Рис. 1.2. Принцип роботи DHCP starvation

MAC-spoofing - це атака, при якій порушник обходить перевірку автентифікації для порушення працездатності мережі [5]. Використовується для того, щоб дізнатися про дані, програми, паролі та IP-адреси кінцевого хоста. Принцип роботи MAC-spoofing зображено на рисунку 1.3.

Крок 1 на рисунку 1.3 демонструє три виявлені пристрої (А, В і С) в таблиці САМ. Пристрій С – зловмисник. Після підміни MAC-адреси пристрою

А (початковий кадр, коли таблиця CAM пуста, відправляється на всі порти, крім вихідного), пристрій С відправляє кадр з вихідною MAC-адресою А з новою підrobною IP-адресою. Комутатор повторно дізнається MAC-адресу і змінює записи таблиці CAM на кроці 2 атаки. Тепер, коли пристрій В хоче зв'язатися з легітимним пристроєм А, комутатор відправляє пакет у відповідності з таблицею CAM, на порт 3, тобто зломиснику. Поки пристрій А не відправить пакети повторно, потік даних залишиться, і зломисник буде отримувати і проглядати активні дані.

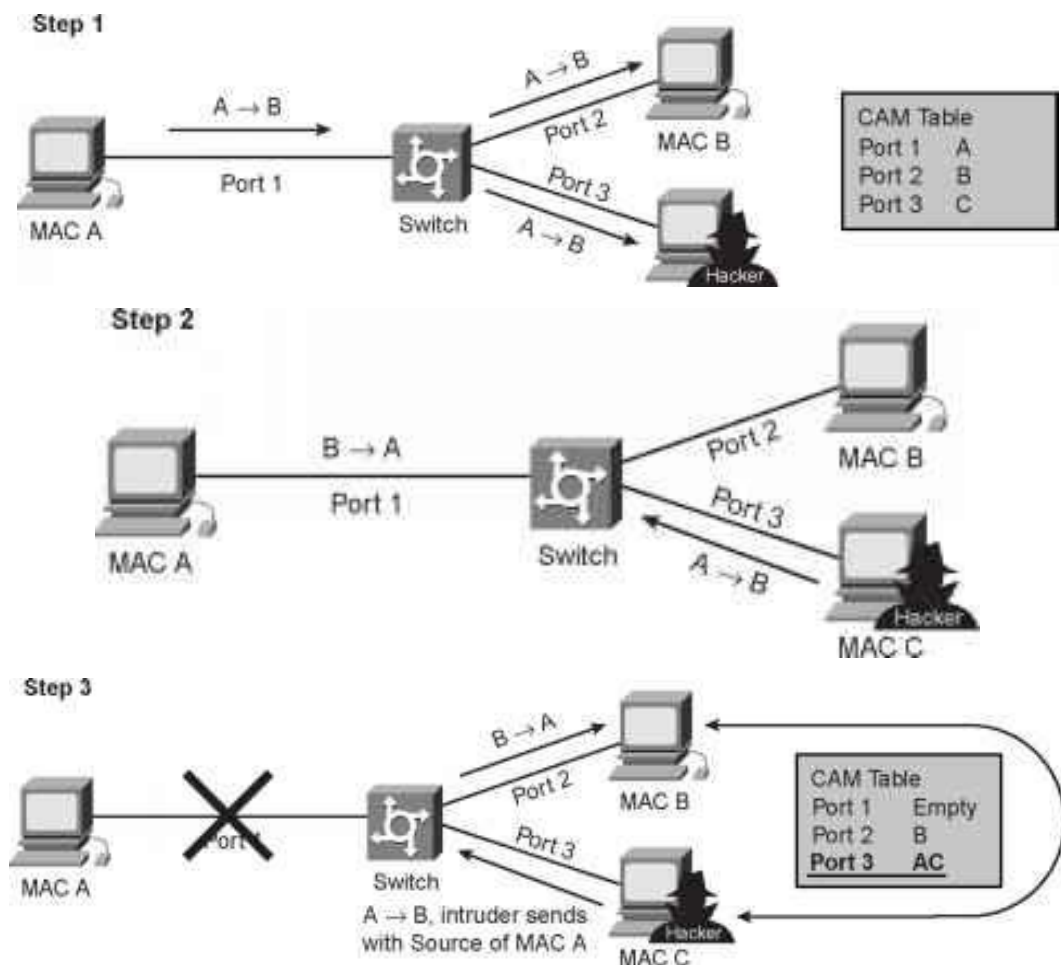


Рис.1.3. Принцип роботи MAC-spoofing

ARP Spoofing - це атака, при якій зломисник надсилає підrobленні ARP пакети через локальну мережу для того, щоб зв'язати свою MAC адресу з IP-адресою справжнього користувача мережі. Коли зв'язок налаштовується, зломисник починає отримувати, а також модифікувати передачу даних. ARP атаки відбуваються лише в локальних мережах (рис.1.4).

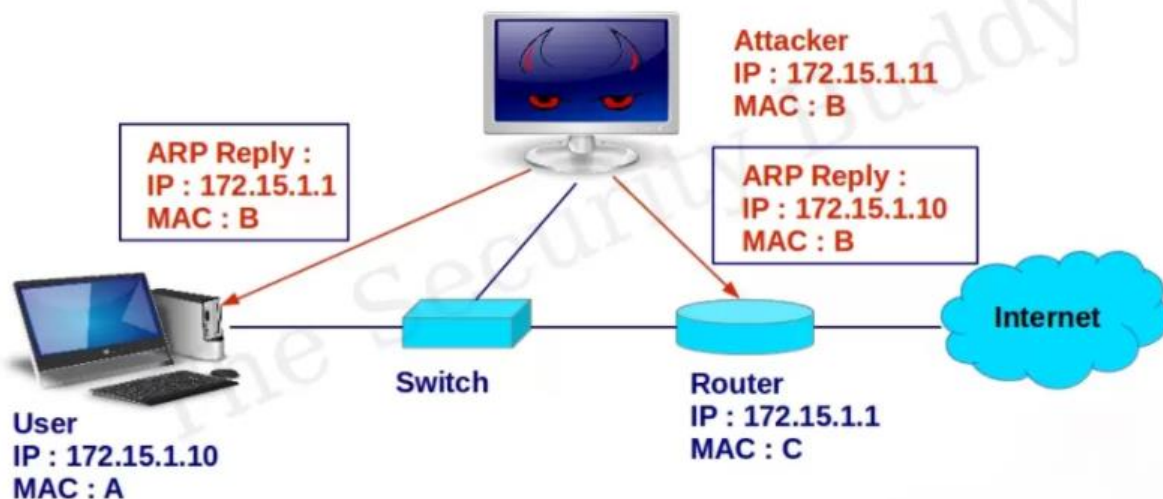


Рис.1.4. Принцип роботи ARP Spoofing

DOS - це атака, за допомогою якої злочинець намагається зробити цільовий пристрій недоступним для користувачів, перезавантажуючи або заповнюючи пристрій запитами, поки неможливо буде обробити звичайний трафік, що призводить до відмови в обслуговуванні інших користувачів. Основною різницею DOS і DDOS атаки є те, що перша виконується з використанням одного комп'ютера, а друга – із залученням великої кількості робочих станцій (рис.1.5-1.6) [6].

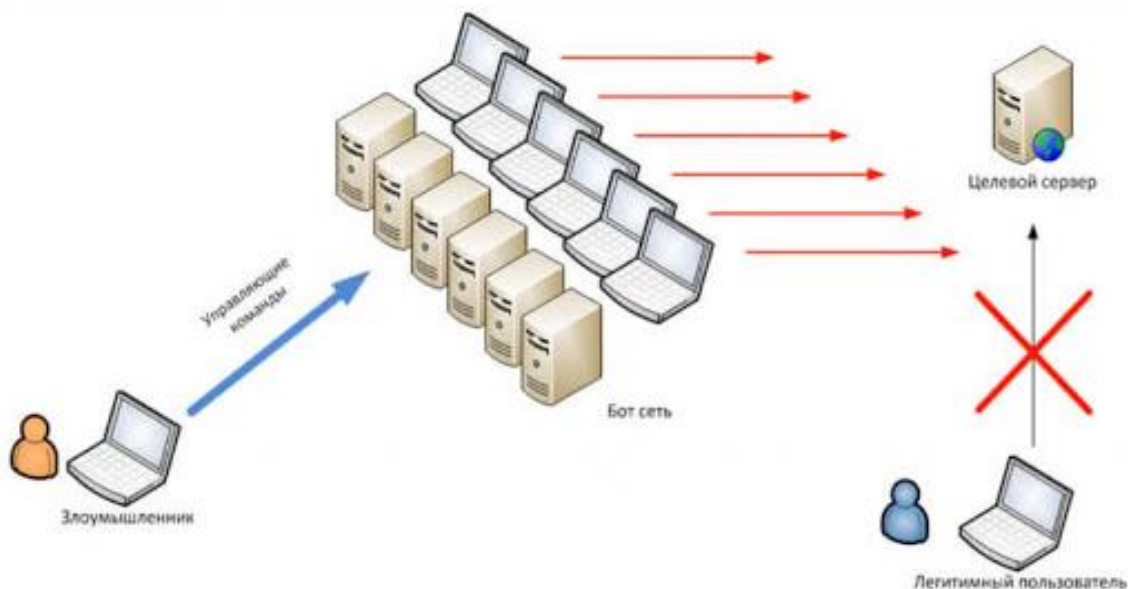


Рис.1.5. Принцип роботи DOS атаки

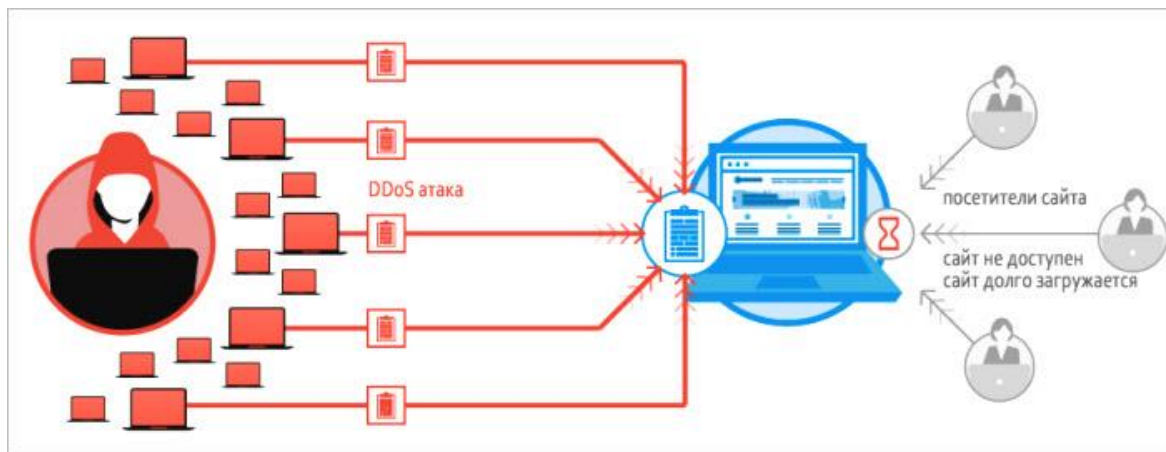


Рис.1.6. Принцип роботи DDOS атаки

Отже, як бачимо, в сучасному світі існує багато атак на робочі станції, пристрої та на мережі, які тим чи іншим чином впливають на її працездатність. Тобто для того, щоб налагодити робочу мережу та налаштувати її працездатність, потрібно її захищати від порушників, які будуть намагатися заволодіти інформацією.

1.3 Захист системи

Із розвитком атак розвивався і захист мереж. Більшість атак, які здійснювали порушники, мали пагубний характер, так як могли виводити мережі з ладу на достатньо довгий термін, красти інформацію і тому подібне. На великих підприємствах на даний час досить розвинена система захисту. Майже всі атаки відбиваються і не мають великого впливу на мережі. Проте кожний день зловмисники розвивають свої способи атаки і тому потрібно також розробляти нові методи захисту від них. Розглянемо способи захисту від атак, які були вказані в попередньому розділі.

Rogue DHCP Server: простим та ефективним способом захисту є вмикання DHCP snooping на комутаторах. Існує 2 типи портів: довірений (до якого підключається DHCP сервер) та недовірені (порти для всіх інших підключень, за якими DHCP сервера не може бути і за яким може бути зловмисник, який намагається атакувати даний сервер). Топологія налаштування захисту від цієї атаки зображена на рисунку 1.7 [7].

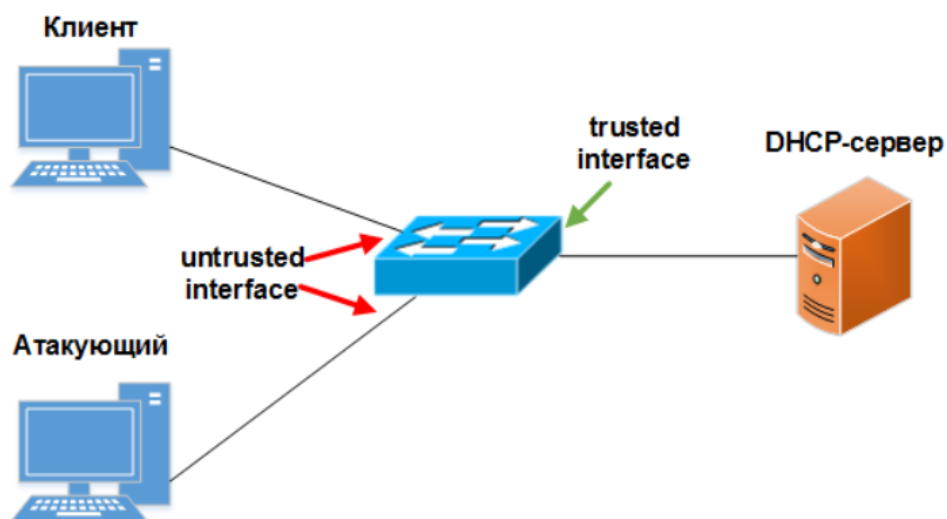


Рис. 1.7. Топологія налаштування захисту від атаки типу Rogue DHCP Server.

Налаштування DHCP snooping необхідно, щоб показати, що пакети DHCP offer та acknowledgment повинні проходити через довірений порт (trusted), і не допускати проходження даних пакетів через недостовірні (untrusted) порти. Після налаштування запити від справжніх клієнтів будуть перенаправлятися на довірені порти.

DHCP starvation: кращим способом захисту від даної атаки буде обмеження кількості доступних IP адрес, які може дати DHCP сервер. Також необхідно налаштувати збереження в комутаторі MAC адреси в конфігураційному файлі. Це необхідно для того, щоб DHCP сервер міг видавати користувачу мережі IP адресу, прив'язану до MAC адреси користувача. Якщо це мережа чи підмережа якогось підприємства, до якого не мають доступу інші користувачі, то необхідно налаштувати кількість безпечних MAC адрес, налаштувати кількість DHCP пакетів на порт, і в випадку їх перевищення автоматично виключати його на деякий час.

MAC-spoofing: кращим захистом від даної атаки є запис в таблицю комутатора MAC адресу користувача, який підключений за даним портом. Тобто, якщо MAC адреса за даним портом зміниться, то користувач буде недоступний.

ARP Spoofing: у випадку цієї атаки потрібно використовувати інструмент Dynamic ARP Inspection. Суть його роботи полягає в тому, що він

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

вибирає, які пакети пропускати, а які відкинути, тобто повністю захищає мережу від атаки[8].

DOS: від даної атаки існує ряд захистів. Можна налаштовувати комутатори так, щоб вони визначали тип невідомого трафіку і не пропускали його. Також можна обмежити пропускну швидкість до сервера. І можна виділити сервер, який зможе обробляти інформацію і буде працювати.

Отже, як можна побачити, що як розвиваються атаки, так розвивається і захист. В наш час будь-яка мережа повинна бути захищена, щоб працювати[9].

1.4 Загальні технічні відомості та вимоги до програмного та апаратного забезпечення мережі.

Мережа буде розроблятися і складатися з декількох підмереж та віртуальної машини з операційною системою Kali Linux, за допомогою якою будуть здійснюватися атаки на мережу.

В мережі буде створено:

- різні підмережі з спеціальною підмережею, із якої будуть здійснюватися атаки на всю мережу;
- різні операційні системи;
- налаштування DHCP серверів;
- налаштування захисту мережі;
- створення сайту, на який буде здійснено атаку.

Роблячи висновок з цього, до програмно-апаратного забезпечення будуть такі вимоги:

- використання Windows 7 як серверу для сайту;
- використання Kali Linux, за допомогою якою буде здійснено атаки;
- надійність мережі;
- наявність DHCP серверів;
- захист мережі від різних типів атак.

Тобто в мережі буде розроблено буде розроблено декілька DHCP серверів за які будуть відповідати комутатори для подальшої її розширення. В

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows 7 буде розроблено сайт для локальної мережі. Кожне підприємство повинно мати свій сайт на який зазвичай викладають інформацію для співробітників.

За допомогою операційної системи Kali Linux, а саме за допомогою інструментів, до яких надає доступ ця операційна система, буде здійснено тестування мережі на її захищеність. Буде додано віртуальну машину з операційною системою Kali Linux, на яку необхідно буде встановити додаткові інструменти, а саме GoldenEye, Yersenia, Ettercap.

Після проведення тестування мережі необхідно буде розробити аналіз проведених атак для того, щоб розробити оптимальний захист мережі.

Також необхідно буде налаштувати захист даної мережі для нормального її функціонування. Захист буде налаштовано за допомогою команд на комутаторі та маршрутизаторі.

Висновок до розділу 1

В результаті розглянутої інформації в першому розділі було визначено основні характеристики локальної мережі підприємства, топологію створення такої мережі.

Було розглянуто різні типи атаки на дану мережу та способи захисту від цих атак.

З ОС було вибрано Kali Linux, так як вона має багато різних програм для створення атак на підмережу та всю мережу. Було встановлено додаткові інструменти для проведення тестування мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

2.1 Проект локальної мережі підприємства

Розробляючи проект мережі потрібно звернути увагу, що це мережа підприємства. Тобто буде складатися з багатьох підмереж. Також будуть використовуватися різні операційні системи. Так як проект складається з підмереж, доцільно буде використання DHCP протоколу для розподілу IP адрес. Тобто з легкістю можна буде додавати нові робочі станції чи видаляти старі у випадку несправності. Було розроблено чотири підмережі з DHCP серверами.

Топологію з'єднань буде наведено в таблиці 2.1

Таблиця 2.1

Параметри з'єднань мережі

Пристрої	Інтерфейси	Підключення	Підключення до інтерфейсів
R_Central	E0/1	R_Admin	E0/0
	E0/2	R_1	E0/0
	E0/3	R_2	E0/0
	E1/0	R_3	E0/0
R_Admin	E0/0	R_Central	E0/1
	E0/1	SW_Admin	E0/0
SW_Amin	E0/0	R_ADMIN	E0/1
	E0/1	Win XP	E0
	E0/2	WS_N	E0
R_1	E0/0	R_Central	E0/2
	E0/1	SW_1	E0/0
SW_1	E0/0	R_1	E0/1
	E0/1	SW1	E0

Продовження таблиці 2.1

R_2	E0/0	R_Central	E0/3
	E0/1	SW_2	E0/0
SW_2	E0/0	R_2	E0/1
	E0/1	SW2	E0
R_3	E0/0	R_Central	E1/0
	E0/1	SW_3	E0/0
SW_3	E0/0	R_3	E0/1
	E0/1	SW3	E0

Для даної мережі також необхідно розробити IP адресацію (табл.2.2).

Таблиця 2.2

Параметри адресації мережі

Підмережа	Інтерфейс	IP-адреса	Маска	Префікс
R_Central	E0/1	192.168.2.1	255.255.255.252	/30
	E0/2	192.168.3.1	255.255.255.252	/30
	E0/3	192.168.4.1	255.255.255.252	/30
	E1/0	192.168.5.1	255.255.255.252	/30
R_Admin	E0/0	192.168.2.2	255.255.255.252	/30
	E0/1	193.168.4.1	255.255.255.0	/24
SW_Admin	VLAN 1	193.168.4.2	255.255.255.0	/24
R_1	E0/0	192.168.3.2	255.255.255.252	/30
	E0/1	193.168.3.1	255.255.255.0	/24
SW_1	VLAN 1 (E0/0)	193.168.3.2	255.255.255.0	/24
	VLAN 1 (E0/1)	DHCP		

Продовження таблиці 2.2

R_1	E0/0	192.168.4.2	255.255.255.252	/30
	E0/1	193.168.2.1	255.255.255.0	/24
SW_1	VLAN 1 (E0/0)	193.168.3.2	255.255.255.0	/24
	VLAN 1 (E0/1)	DHCP		
R_2	E0/0	192.168.4.2	255.255.255.252	/30
	E0/1	193.168.2.1	255.255.255.0	/24
SW_2	VLAN 1 (E0/0)	193.168.2.2	255.255.255.0	/24
	VLAN 1 (E0/1)	DHCP		
R_3	E0/0	192.168.5.2	255.255.255.252	/30
	E0/1	193.168.1.1	255.255.255.0	/24
SW_3	VLAN 1 (E0/0)	193.168.2.2	255.255.255.0	/24
	VLAN 1 (E0/1)	DHCP		

2.2 Розробка структури мережі

В даній мережі було використано трирівневу ієрархічну структуру мережі[10], тому що це дає змогу легко розширювати мережу, полегшує усунення неполадок та забезпечує ефективне управління. Тобто мережа буде складатися з рівня ядра, рівня розподілу та рівня доступу (рис.2.1).

Розглянемо кожний рівень детальніше:

1. Рівень ядра: є головним рівнем в ієрархії, так як відповідає за транспортування даних між підмережами. В зв'язку з тим, що це центральний

рівень мережі, він повинен бути захищений, і у випадку якоїсь несправності мати змогу швидко відновитися для того, щоб не втрачати зв'язку в мережі.

Основні характеристики рівня:

- продуктивність та надійність;
- масштабованість.

2. Розподільчий рівень: забезпечує зв'язок між рівнем ядра та рівнями доступу. Тобто даний рівень служить для маршрутизації по мережі і розподілу навантаження. Крім того, зменшує витрати за рахунок щільності портів.

Основні характеристики рівня:

- розподіл навантаження;
- маршрутизація між підмережами.

3. Рівень доступу: рівень складається з комутаторів та точок доступу, до яких підключаються ПК та інші пристрої мережі. Комутатори цього рівня забезпечують надходження пакетів між різними кінцевими пристроями мережі. Основні характеристики рівня:

- висока доступність;
- безпека;
- списки контролю доступу.

Проектування такої мережі займає досить багато часу і ресурсів. Для того, щоб спростити процес адресації, в таких мережах зазвичай використовуються DHCP сервера[11]. Це дозволяє робочим станція швидко отримувати собі адресу і підключатися до мережі. А в випадку якоїсь несправності легко її знаходити і відновлювати роботу.

Для того, щоб різні підмережі мали між собою зв'язок, було використано протокол маршрутизації OSPF, так як даний протокол дозволяє збалансувати навантаження, здійснювати автентифікацію, що забезпечує захист мережі, а також зміни в маршрутизації поширюються миттєво[12].

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

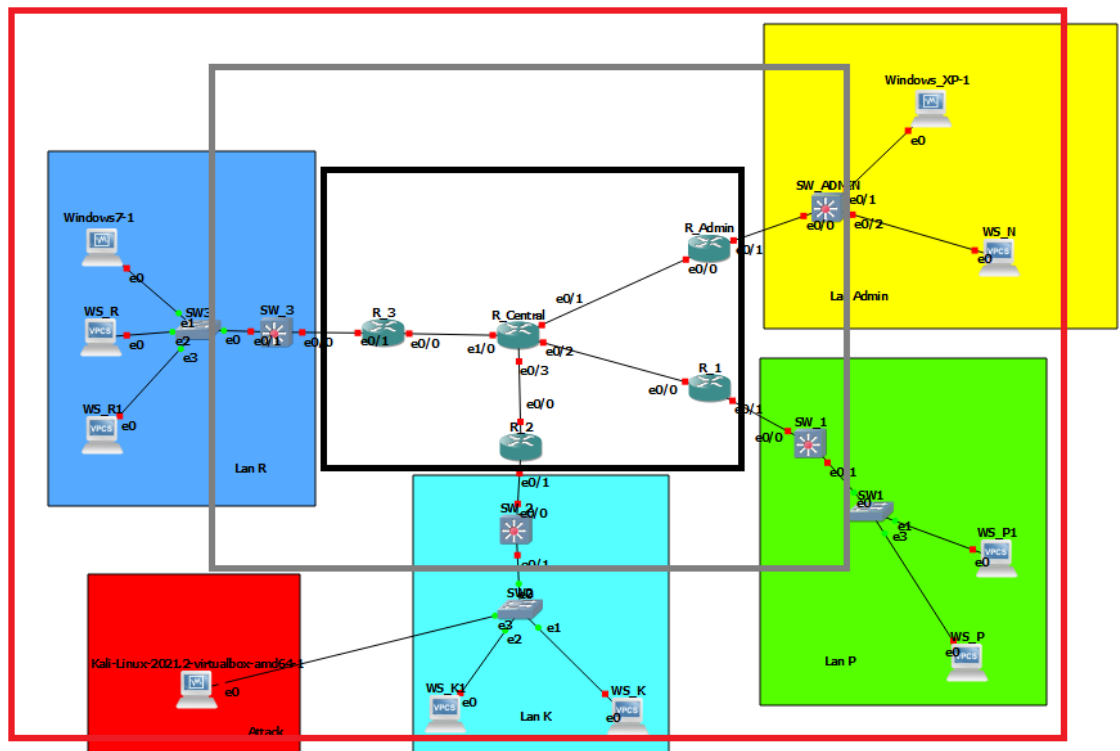


Рис. 2.1. Трирівнева модель мережі.

На рисунку 2.1 можна побачити побачити розроблену трирівневу структуру мережі. Розглянемо кожний рівень окремо.

Рівень ядра складається з п'яти маршрутизаторів, чотири з яких, а саме R_Admin, R_1, R_2, R_3, з'єднуються між собою центральним R_Central. Тобто саме в цьому рівні з'єднуються між собою всі підмережі в мережі.

Розподільчий рівень складається з чотирьох комутаторів, які виступають в ролі DHCP серверів. За допомогою налаштувань на даних комутаторах зручно додавати нових користувачів.

Рівень доступу складається з десяти віртуальних машин, серед яких Windows 7 в Lan R слугує сервером для сайту.

Окремо виділимо рівень доступу, так як на цьому рівні працюють DHCP сервера, тобто до цього рівня можна під'єднувати нові робочі станції, якщо того потребує мережа, або поки не закінчаться порти в комутаторах. На рисунку 2.1 можна побачити що було під'єднано віртуальну машину Kali

Linux[13], яка виступає в ролі зловмисника, який намагається атакувати схему.

Сама мережа складається з чотирьох підмереж.

Lan R складається з двох влаштованих в GNS3 робочих станцій та Windows 7, яка слугує як сервер для локального сайту, і з комутатора, який виступає в ролі DHCP сервера.

Lan K складається з двох влаштованих в GNS3 робочих станцій та Kali Linux, яка виступає в ролі як порушника. Саме за допомогою її буде проведено тестування мережі. Також наявний комутатор, який виступає в ролі DHCP сервера.

Lan P складається з двох влаштованих в GNS3 робочих станцій і комутатора, який виступає в ролі DHCP сервера.

Lan Admin складається з двох влаштованих в GNS3 робочих станцій та Windows XP, яка слугує як адміністратор мережі. Також є комутатор, який виступає в ролі DHCP сервера.

2.3 Вибір обладнання та програмного забезпечення.

При розробці будь-якої мережі необхідно вибрати правильне обладнання та програмне забезпечення, адже від кожного вибору буде залежати працездатність всієї мережі, її надійність та захист. Опираючись на ці потреби, можна зробити список програмно-апаратного забезпечення, що включатиме в себе:

1. Використання Windows 7, яка буде виступати як сервер, на якому буде налаштовано локальний сайт.
2. Використання ОС Windows 7 та Windows XP.
3. Налаштування захисту та надійності роботи системи.
4. Використання операційної системи Kali Linux, за допомогою якої будуть здійснені атаки
5. Використання віддаленого доступу до пристроїв за допомогою SSH

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

Для проектування схеми було вибрано обладнання від фірми Cisco. Чому саме обладнання від цієї фірми? Тому що воно має ряд таких переваг:

- Cisco – це одна із небагатьох компаній, яка є лідером серед розробки мережевих приладів. Дана компанія розробляє прилади для всього світу і відповідає за якість своєї продукції;
- прилади компанії розробляються так, щоб вони мали змогу якнайдовше працювати. Це саме те, що потрібно для великих підприємств та компаній;
- налаштування мережевих приладів від компанії Cisco максимально просте і зрозуміле. Прилади підтримують можливість графічного інтерфейсу користувача. Також можна керувати мережею і одночасно налаштувати прилади;
- комутатори Cisco мають вбудовану систему безпеки, за допомогою якої вони бачать, які прилади підключаються до мережі задля запобігання атак;
- компанія має велику кількість обладнання, яке підходить як для великих підприємств та компаній, так і для малих, що дозволяє підібрати такі прилади, що будуть оптимальні як і для роботи, так і для бюджету цих самих компаній та підприємств[14].

Роблячи висновки із вище сказаного, мережеве обладнання від компанії Cisco ідеально підходить для розробки мереж, тому буде використано і в даній мережі, зокрема комутатор Cisco 2960-X (рис. 2.2), а також маршрутизатор Cisco 2800 (рис. 2.3).



Рис.2.2. Комутатор Cisco 2960-X



Рис.2.3. Маршрутизатор Cisco 2800

Для розробки самої мережі буде використано GNS3. GNS3 (Graphical Network Simulator) – це безкоштовне програмне забезпечення, яке дає можливість створювати топологію від маленької, яка складається з декількох пристроїв, так і до великих, які складаються з багатьох пристроїв, віртуальних машин і тому подібне [15]. Для цього не потрібне реальне обладнання, адже GNS використовує емулятори того самого обладнання, що дає змогу максимально наблизитися до реального. Основна перевага GNS заключається в тому, що він дозволяє використовувати віртуальні машини операційних систем. Тобто це дозволяє нам створювати майже реальну мережу якогось підприємства чи компанії. Все ж таки будь-яке програмне забезпечення має свої недоліки, і GNS не виключення. Для того, щоб зручно і безперешкодно працювати в GNS, потрібно мати достатньо потужний ПК, адже розробка мереж це ресурсозатратний процес. Тому не на всіх ПК є можливість працювати в даному симуляторі.

Для того, щоб додавати та використовувати різні операційні системи, буде використано Virtual Box. Virtual Box – це програмне забезпечення, яке дозволяє додавати, використовувати, видаляти та працювати в різних операційних системах, при цьому не змінюючи своєї [16]. До основних переваг програми можна віднести:

- зручний та простий інтерфейс;
- тестування різних ОП не змінюючи своєї основної;
- налаштування ресурсо-затратності різних ОП.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Також, для слідкування та виявлення атак, в GNS буде використано програму Wireshark. Wireshark – це програма для аналізу трафіку в мережі. Вона допоможе нам відстежувати атаки на мережу та розробляти план захисту від них[17].

Ну і сама операційна система, за допомогою якою будуть здійснено атаки, це Kali Linux. Дана операційна система розроблялась для того, щоб тестувати мережі та знаходити слабкі місця. Тобто за допомогою даної системи можна проводити атаки на мережу. Kali Linux має такі переваги:

- зручний інтерфейс.
- безкоштовна;
- має багато утиліт, за допомогою яких можна тестувати мережі на захищеність.

Висновок до розділу 2

В даному розділі було розглянуто поняття трирівневої ієрархічної моделі мережі. Сформовано необхідність її використання в даній роботі.

Також було вибрано правильне обладнання для того, щоб мережа працювала надійно та мала захист. Було вибрано програмне забезпечення, в якому буде створено саму мережу, а також операційну систему, за допомогою якої зможемо перевірити дану мережу на її недоліки в захисті та налаштувати сам захист даної мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТА ТА ЗАХИСТ ЇЇ ВІД РІЗНИХ ТИПІВ АТАК

3.1 Базове налаштування мережі

В цьому підрозділі буде розроблено схему мережі та проведено базове налаштування пристроїв мережі. Загальна схема мережі, що розробляється, зображена на рисунку 3.1.

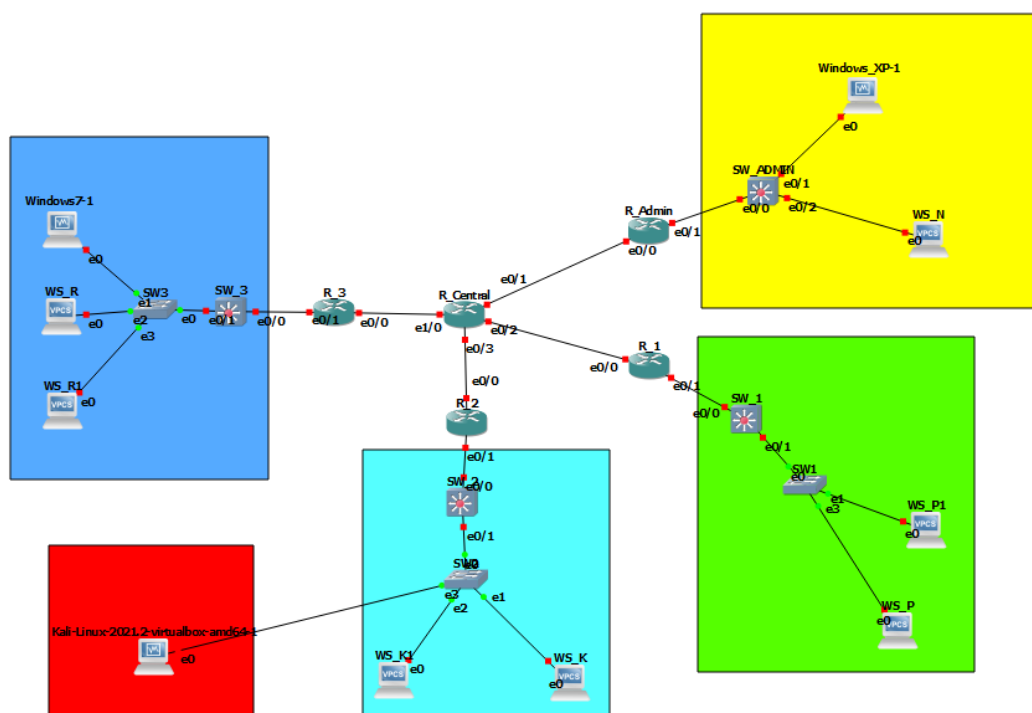


Рис. 3.1. Схема мережі

Далі потрібно налаштувати адресацію мережі. На рисунку 3.2 можна побачити налаштування адресації. Аналогічно налаштовуємо інші маршрутизатори мережі.

Також за DHCP сервера в даній мережі будуть відповідати комутатори, тому потрібно їх налаштувати.

На рисунку 3.3 було налаштовано DHCP адресацію на комутаторі. Аналогічно налаштовуємо інші комутатори мережі.

```

R_Central(config)#int e0/1
*May 27 13:34:09.915: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May 27 13:34:10.920: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R_Central(config)#int e0/1
R_Central(config-if)#ip add 192.168.2.1 255.255.255.252
R_Central(config-if)#no sh
R_Central(config-if)#ex
R_Central(config)#int
*May 27 13:34:25.258: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*May 27 13:34:26.260: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
R_Central(config)#int e0/2
R_Central(config-if)#ip add 192.168.3.1 255.255.255.252
R_Central(config-if)#no sh
R_Central(config-if)#ex
R_Central(config)#
*May 27 13:34:44.529: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*May 27 13:34:45.529: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
R_Central(config)#int e0/3
R_Central(config-if)#ip add 192.168.4.1 255.255.255.252
R_Central(config-if)#no sh
R_Central(config-if)#ex
R_Central(config)#
*May 27 13:35:06.730: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*May 27 13:35:07.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
R_Central(config)#int e1/0
R_Central(config-if)#ip add 192.168.5.1 255.255.255.252
R_Central(config-if)#no sh
R_Central(config-if)#ex
R_Central(config)#
*May 27 13:35:26.779: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*May 27 13:35:27.782: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
R_Central(config)#

```

Рис. 3.2. Налаштування IP адресації на маршрутизаторі R_Central

```

SW_2(config)#int vlan 1
SW_2(config-if)#ip add 193.168.2.2 255.255.255.0
SW_2(config-if)#no sh
SW_2(config-if)#ex
SW_2(config)#ip dhc
*Jun 7 17:06:52.715: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 7 17:06:53.720: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW_2(config)#ip dhcp ex
SW_2(config)#ip dhcp excluded-address 193.168.2.1 193.168.2.2
^
% Invalid input detected at '^' marker.
SW_2(config)#ip dhcp excluded-address 193.168.2.1 193.168.2.2
SW_2(config)#ip dhcp pool K
SW_2(dhcp-config)#network 193.168.2.0 255.255.255.0
SW_2(dhcp-config)#def
SW_2(dhcp-config)#default-router 193.168.2.1
SW_2(dhcp-config)#exit
SW_2(config)#
*Jun 7 17:07:39.331: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 193.168.2.3.
SW_2(config)#

```

Рис. 3.3. Налаштування комутатора SW_2

Для того, щоб був зв'язок між усіма приладами мережі, потрібно налаштувати протокол маршрутизації. В моєму випадку це протокол OSPF. На рисунку 3.4 видно як проводиться налаштування.

```

R_Central(config)#router ospf 1
R_Central(config-router)#network 192.168.2.0 0.0.0.3 area 0
R_Central(config-router)#network 192.168.3.0 0.0.0.3 area 0
R_Central(config-router)#network 192.168.4.0 0.0.0.3 area 0
R_Central(config-router)#network 192.168.5.0 0.0.0.3 area 0
R_Central(config-router)#exit
R_Central(config)#

```

Рис. 3.4. Налаштування протоколу OSPF на маршрутизаторі R_Central

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі необхідно створити локальний сайт, який буде слугувати як сайт для робітників, на який буде здійсненна атака далі. Для того, щоб створити сайт, було використана функція спільної папки в VirtualBox та програма Denwer[18]. Сервером для сайта буде слугувати Windows 7.

Як можна побачити на рисунку 3.5, спільну папку було створено. Тепер, за її допомогою туди можна завантажити Denwer та використовувати уже на віртуальній машині.

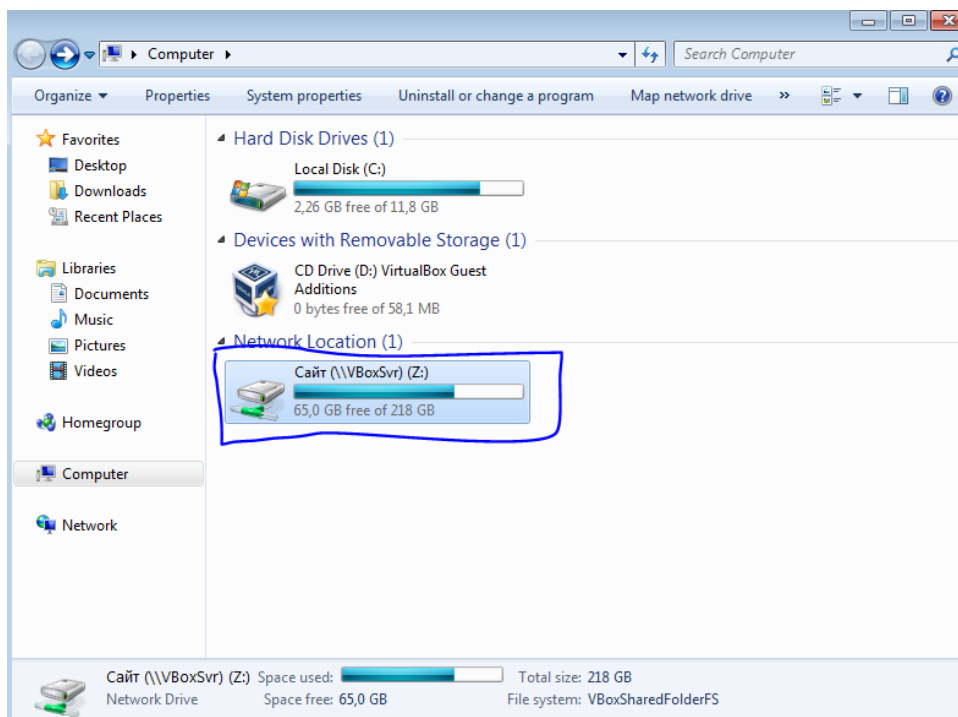


Рис. 3.5. Створення спільної папки на Windows 7

Далі необхідно встановити програму та створити сам сайт. Процес встановлення буде наведено на рисунках 3.6-3.7

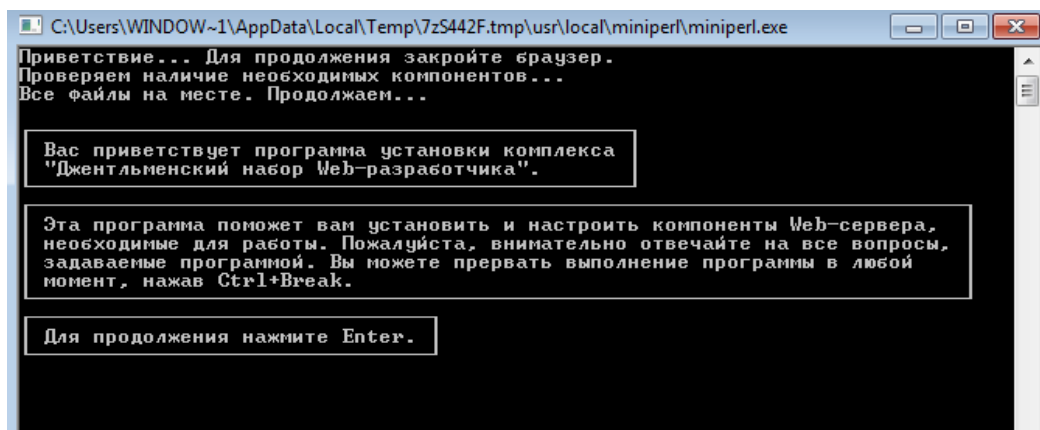


Рис. 3.6. Встановлення Denwer на віртуальну машину Windows 7

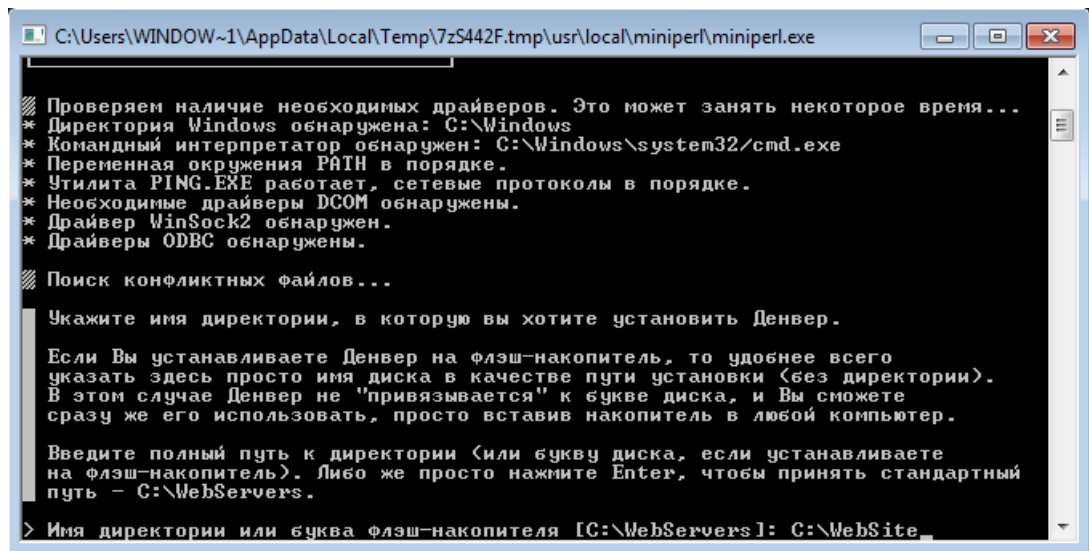


Рис. 3.7. Встановлення Denwer на віртуальну машину Windows 7

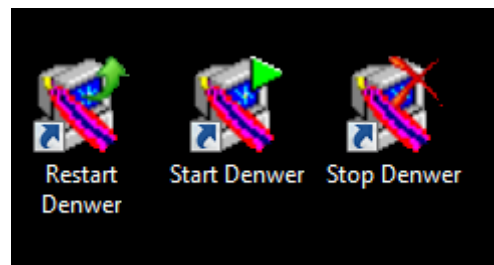


Рис. 3.8. Встановлення Denwer на віртуальну машину Windows 7

Як можна побачити на рисунку 3.8, програму було встановлено. Тепер, за допомогою її можна створити та налаштувати локальний сайт (рис. 3.9-3.11).

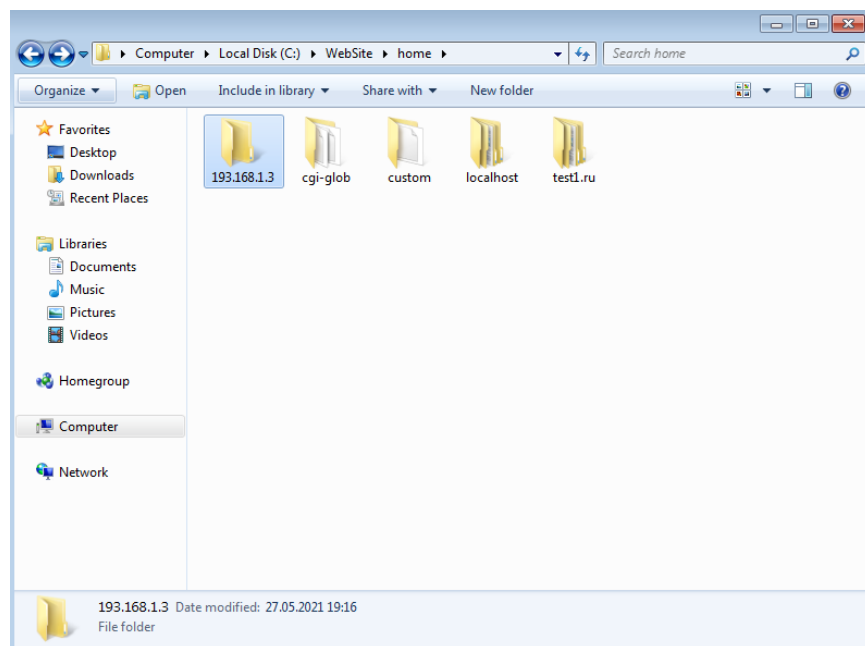


Рис. 3.9. Створення локального сайту на віртуальній машині Windows 7

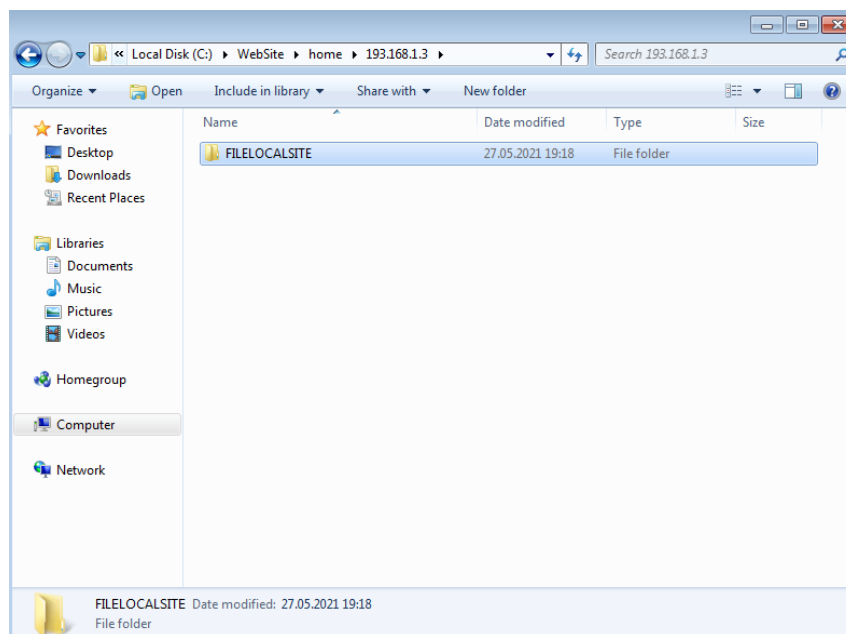


Рис. 3.10. Створення локального сайту на віртуальній машині Windows

7

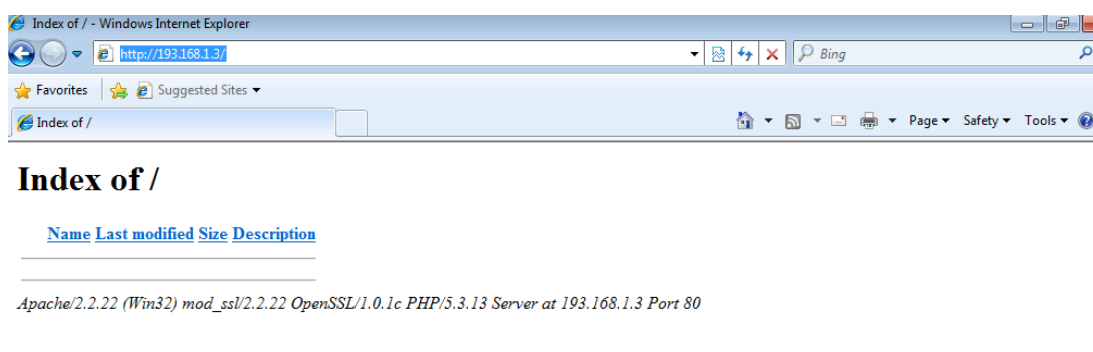


Рис. 3.11. Створений локальний сайт на віртуальній машині Windows 7

Як можна побачити на рисунку 3.11, сайт було успішно створено.

Далі необхідно налаштувати операційну систему Kali Linux, за допомогою якої буде виконуватися атаки на мережу, а саме необхідно встановити інструменти, які будуть нам в цьому допомагати. Було вибрано 3 основних інструменти: це GoldenEye[19], Yersinia[20], Ettercap[21]. Останній, в свою чергу, вбудований в операційну систему, перші два необхідно встановити.

Для встановлення GoldenEye потрібно також налаштувати спільну папку, проте спосіб налаштування в Linux відрізняється від Windows.

На рисунках 3.12-3.13 наведено принцип створення спільної папки в Kali Linux.

```
kali@kali:~$ sudo usermod -aG vboxsf kali

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
kali@kali:~$
```

Рис. 3.12. Налаштування спільної папки на віртуальній машині Kali Linux

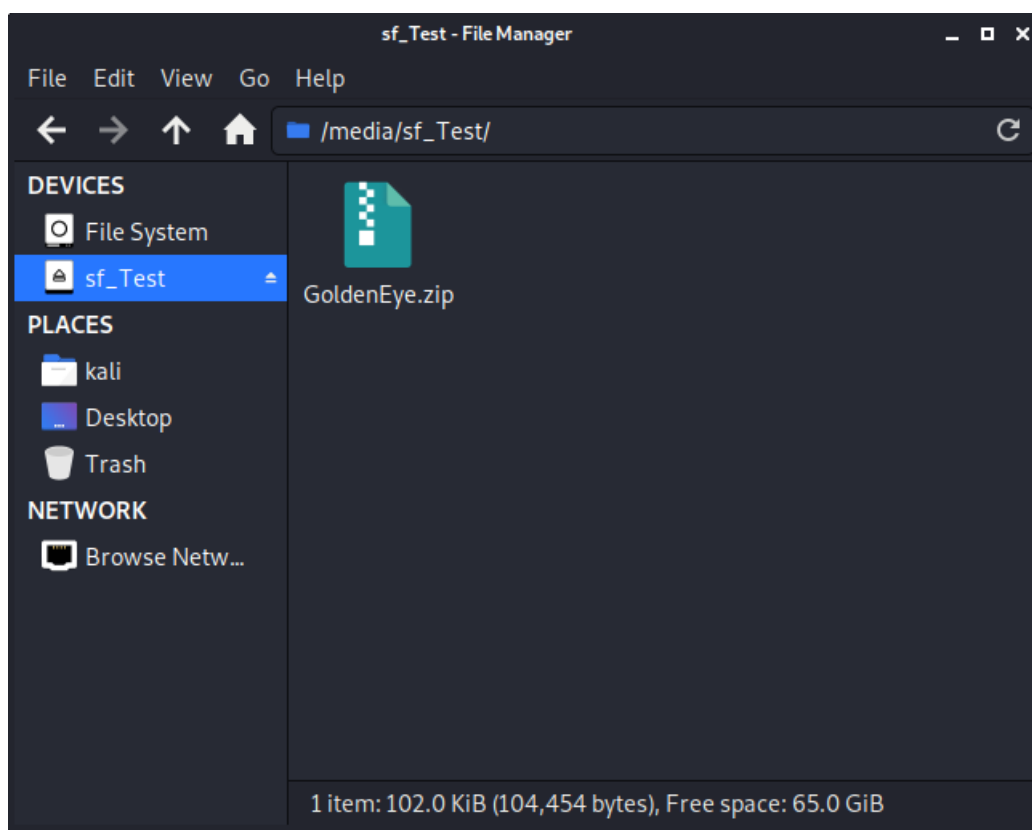


Рис. 3.13. Налаштування спільної папки на віртуальній машині Kali Linux

Після налаштувань папки необхідно встановити саму програму. На рисунках 3.14-3.17 показано процес встановлення GoldenEye.

```

kali@kali:~$ mkdir GoldenEye
kali@kali:~$ cd GoldenEye
kali@kali:~/GoldenEye$ cd
kali@kali:~$ cd /media/sf_Test/
kali@kali:/media/sf_Test$ unzip GoldenEye.zip
Archive:  GoldenEye.zip
792862f5c8cb98f9ffcb9fab245e2c663e3a1026
  creating: GoldenEye-master/
  inflating: GoldenEye-master/README.md
  inflating: GoldenEye-master/goldeneye.py
  creating: GoldenEye-master/res/
  creating: GoldenEye-master/res/lists/
  creating: GoldenEye-master/res/lists/useragents/
  inflating: GoldenEye-master/res/lists/useragents/android.txt
  inflating: GoldenEye-master/res/lists/useragents/browsers.txt
  inflating: GoldenEye-master/res/lists/useragents/cloudplatforms.txt
  inflating: GoldenEye-master/res/lists/useragents/crawlers.txt
  inflating: GoldenEye-master/res/lists/useragents/feedreaders.txt
  inflating: GoldenEye-master/res/lists/useragents/ipad.txt
  inflating: GoldenEye-master/res/lists/useragents/iphone.txt
  inflating: GoldenEye-master/res/lists/useragents/libraries.txt
  inflating: GoldenEye-master/res/lists/useragents/linkcheckers.txt
  inflating: GoldenEye-master/res/lists/useragents/others.txt
  inflating: GoldenEye-master/res/lists/useragents/validators.txt
  inflating: GoldenEye-master/res/lists/useragents/zytrax-browserid.txt
  creating: GoldenEye-master/util/
  inflating: GoldenEye-master/util/getuas.py
kali@kali:/media/sf_Test$ cd
kali@kali:~$

```

Рис. 3.14. Налаштування GoldenEye на віртуальній машині Kali Linux

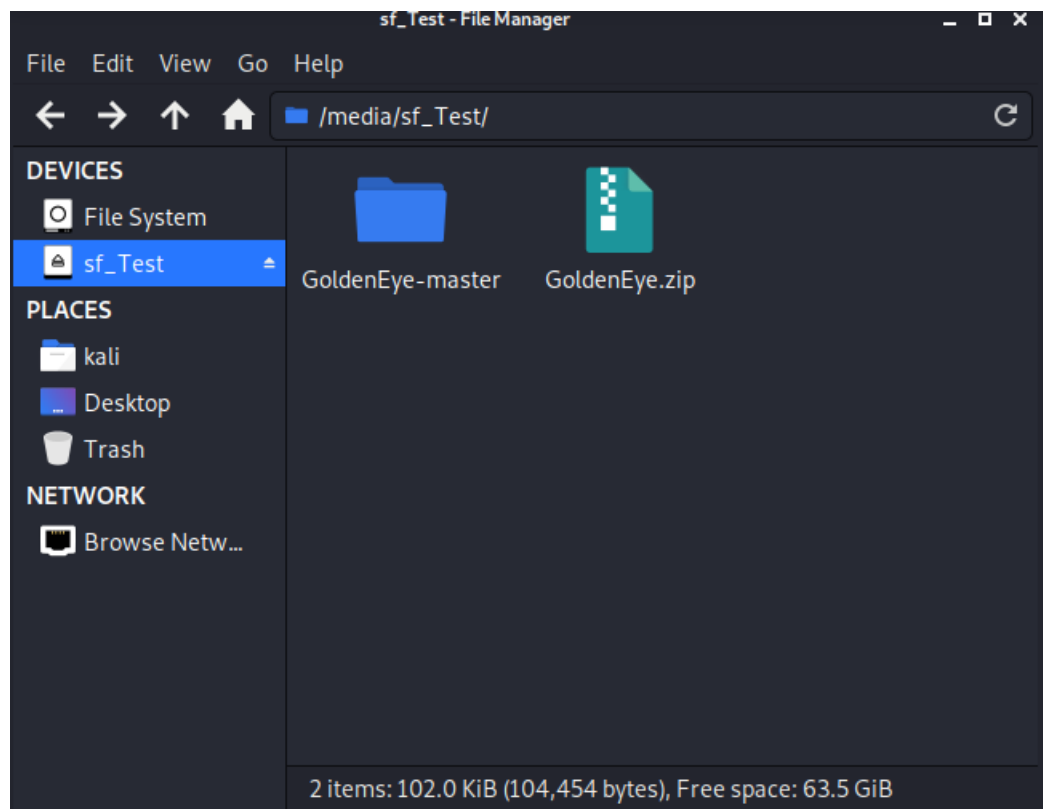


Рис. 3.15. Налаштування GoldenEye на віртуальній машині Kali Linux

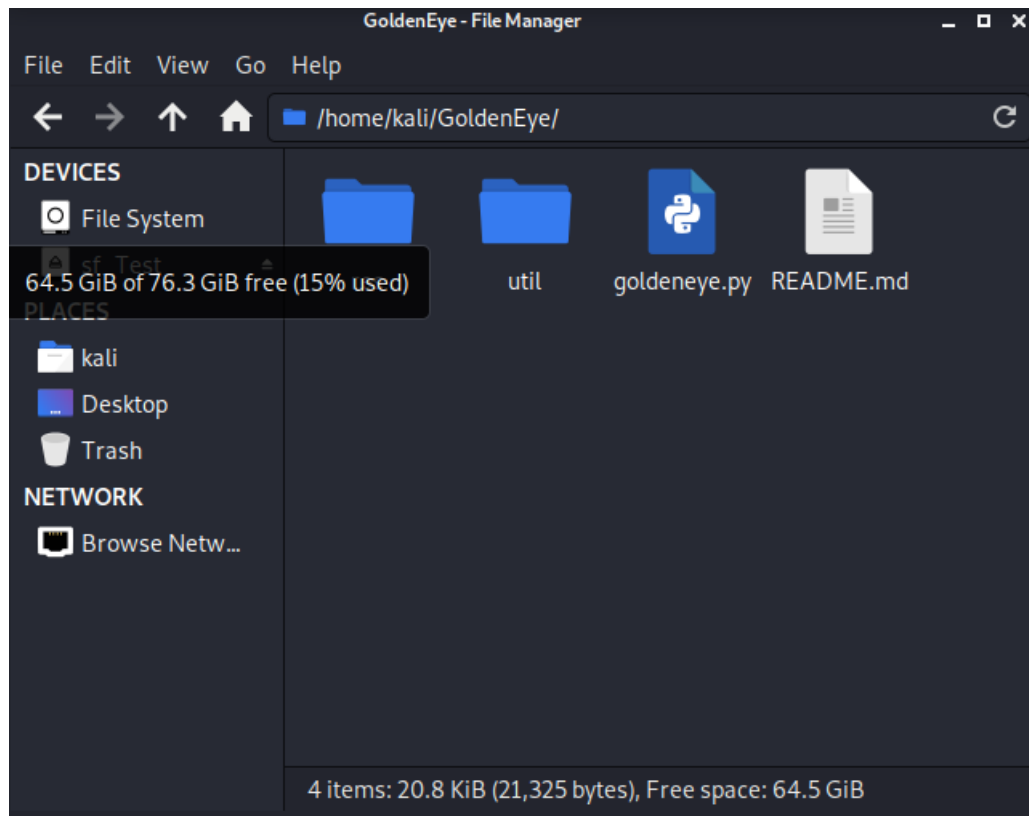


Рис. 3.16. Налаштування GoldenEye на віртуальній машині Kali Linux

```
kali@kali:~$ cd GoldenEye
kali@kali:~/GoldenEye$ ./goldeneye.py
Please supply at least the URL

-----
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

USAGE: ./goldeneye.py <url> [OPTIONS]

OPTIONS:
Flag                                Description                                Default
-u, --useragents                    File with user-agents to use              (default: randomly genera
ted)
-w, --workers                        Number of concurrent workers              (default: 10)
-s, --sockets                       Number of concurrent sockets              (default: 500)
-m, --method                        HTTP Method to use 'get' or 'post' or 'random' (default: get)
-n, --noSSLcheck                    Do not verify SSL Certificate              (default: True)
-d, --debug                          Enable Debug Mode [more verbose output]    (default: False)
-h, --help                          Shows this help

-----
kali@kali:~/GoldenEye$
```

Рис. 3.17. Перевірка роботи програми GoldenEye на віртуальній машині Kali Linux

Як можна побачити, програма працює. Тепер за допомогою неї можна виконувати DoS атаки на локальний сайт мережі.

Далі необхідно провести базове налаштування адресації робочих станцій та віртуальних машин (рисунки 3.18-3.21).

```

C:\Users\Windows 7>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::805b:6aca:ac17:e202%11
    IPv4 Address. . . . . : 192.168.10.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.{BBF602A0-E711-45F8-BFF5-280DA50978B3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Windows 7>

```

Рис. 3.18. Налаштування адресації на віртуальній машині Windows 7

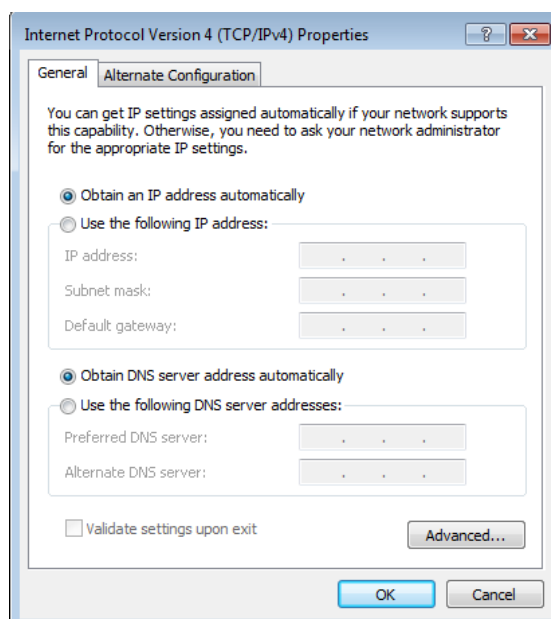


Рис. 3.19. Налаштування адресації на віртуальній машині Windows 7

```

C:\Windows\system32\cmd.exe
C:\Users\Windows 7>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::805b:6aca:ac17:e202%11
    IPv4 Address. . . . . : 193.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 193.168.1.1

Tunnel adapter isatap.{BBF602A0-E711-45F8-BFF5-280DA50978B3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:c1a8:103::c1a8:103
    Default Gateway . . . . . : 

C:\Users\Windows 7>

```

Рис. 3.20. Налаштування адресації на віртуальній машині Windows 7

```
kali@kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 193.168.2.3 netmask 255.255.255.0 broadcast 193.168.2.255
    inet6 fe80::a00:27ff:fe1f:3076 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 542 (542.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 2314 (2.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 3.21. Налаштування адресації на віртуальній машині Kali Linux

3.2 Перевірка базових налаштувань мережі та проведення атак на неї

Перевіримо зв'язок між віддаленими робочими станціями мережі (рис.3.22 – 3.23).

```
kali@kali:~$ ping 193.168.1.3 facebook wikipedia red
PING 193.168.1.3 (193.168.1.3) 56(84) bytes of data.
 64 bytes from 193.168.1.3: icmp_seq=1 ttl=125 time=3.53 ms
 64 bytes from 193.168.1.3: icmp_seq=2 ttl=125 time=2.15 ms
 64 bytes from 193.168.1.3: icmp_seq=3 ttl=125 time=1.46 ms
 64 bytes from 193.168.1.3: icmp_seq=4 ttl=125 time=1.41 ms
 64 bytes from 193.168.1.3: icmp_seq=5 ttl=125 time=2.30 ms
^C
--- 193.168.1.3 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4015ms
 rtt min/avg/max/mdev = 1.414/2.170/3.532/0.766 ms
kali@kali:~$
```

Рис. 3.22. Перевірка зв'язку між робочою станцією Kali Linux та Windows 7

```
Admin> ping 193.168.2.3
84 bytes from 193.168.2.3 icmp_seq=1 ttl=61 time=1.952 ms
84 bytes from 193.168.2.3 icmp_seq=2 ttl=61 time=1.241 ms
84 bytes from 193.168.2.3 icmp_seq=3 ttl=61 time=1.930 ms
84 bytes from 193.168.2.3 icmp_seq=4 ttl=61 time=1.602 ms
84 bytes from 193.168.2.3 icmp_seq=5 ttl=61 time=1.906 ms
Admin>
```

Рис. 3.23. Перевірка зв'язку між робочою станцією Admin та WS_K

Тепер можемо перейти до проведення атак на мережу. Спочатку проведемо атаку на протокол ARP, а саме ARP-Spoofing. Виконувати її будемо за допомогою Ettercap (рис. 3.24 – 3.29).



Рис. 3.24. Виконання атаки ARP-Spoofing.

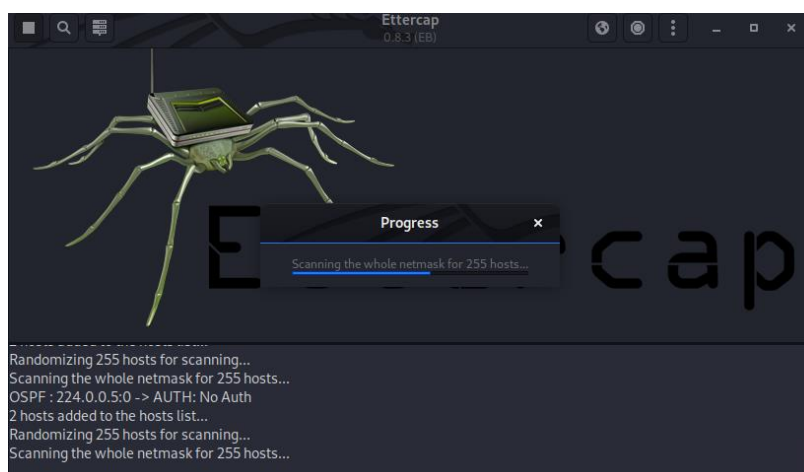


Рис. 3.25. Виконання атаки ARP-Spoofing.

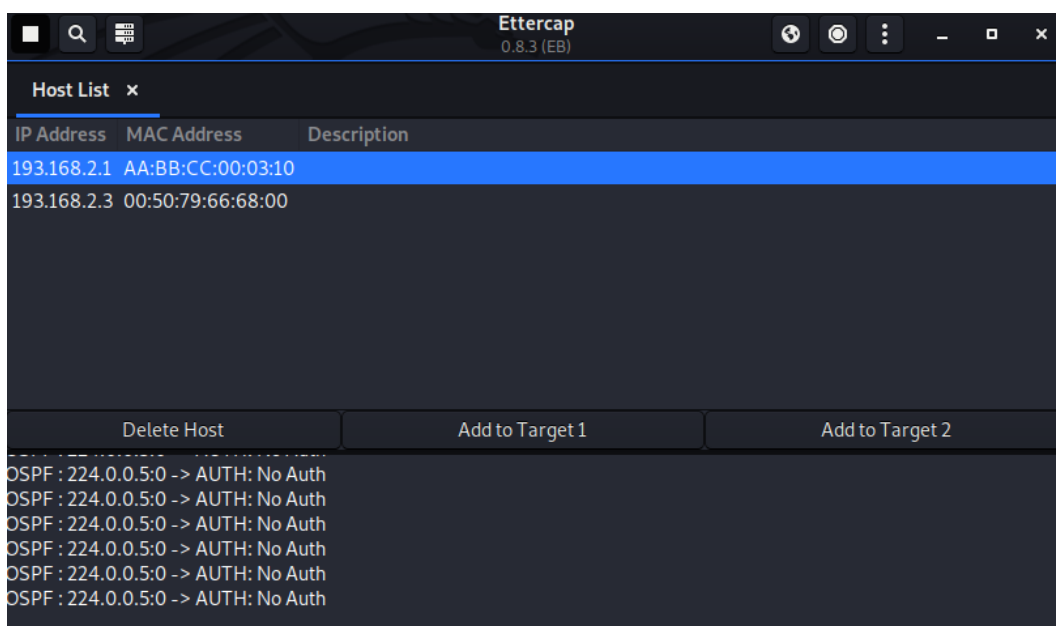


Рис. 3.26. Виконання атаки ARP-Spoofing.

Як можна переглянути на рисунку 3.26, програма бачить шлюз по замовчуванню, тобто маршрутизатор з IP-адресою 193.168.2.1, а також користувача з IP-адресою 193.168.2.3. Далі необхідно виконати саму атаку за допомогою даного інструменту.

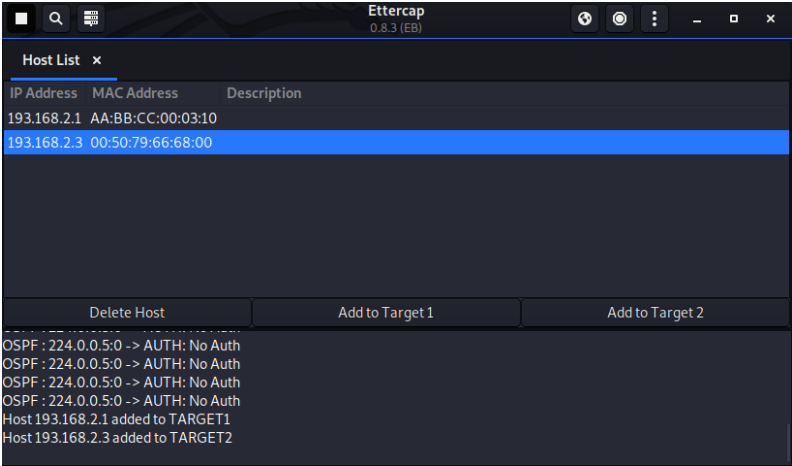


Рис. 3.27. Виконання атаки ARP-Spoofing

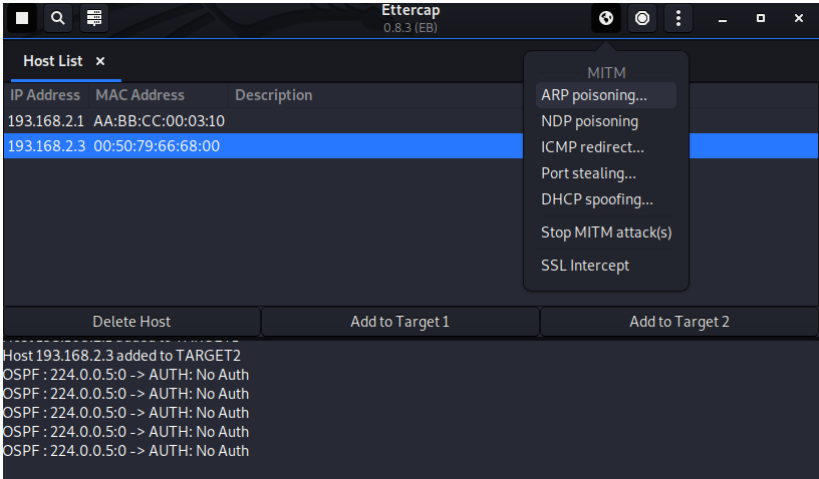


Рис. 3.28. Виконання атаки ARP-Spoofing

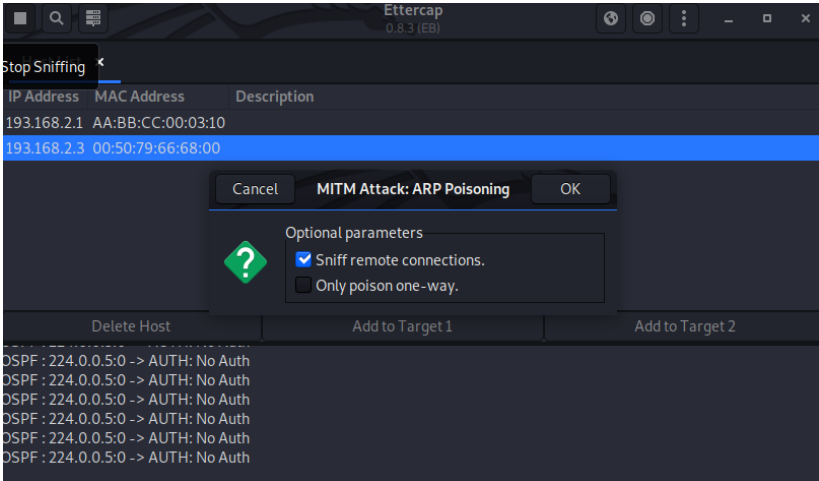


Рис. 3.29. Виконання атаки ARP-Spoofing

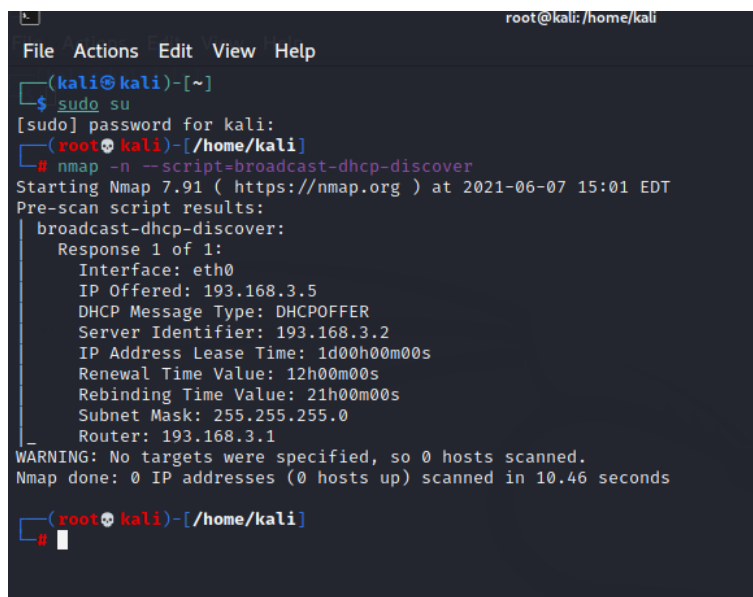
Далі перевіряємо зв'язок між віддаленою робочою станцією та робочою станцією, на яку здійснено атаку.

```
Admin> ping 193.168.2.3
84 bytes from 193.168.2.3 icmp_seq=1 ttl=61 time=11.803 ms
84 bytes from 193.168.2.3 icmp_seq=2 ttl=61 time=17.530 ms
84 bytes from 193.168.2.3 icmp_seq=3 ttl=61 time=14.375 ms
84 bytes from 193.168.2.3 icmp_seq=4 ttl=61 time=13.573 ms
84 bytes from 193.168.2.3 icmp_seq=5 ttl=61 time=15.211 ms
Admin>
```

Рис. 3.30. Виконання атаки ARP-Spoofing

Як можна побачити на рисунку 3.30, пакети надходять, проте з великою затримкою, що вже показує, що з підмережею щось не так.

Далі будемо виконувати атаку на DHCP сервер, а саме DHCP starvation. Атаку будемо виконувати за допомогою програми Kali Linux Yersinia (рис. 3.31 – 3.35).



```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -n --script=broadcast-dhcp-discover
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 15:01 EDT
Pre-scan script results:
broadcast-dhcp-discover:
Response 1 of 1:
Interface: eth0
IP Offered: 193.168.3.5
DHCP Message Type: DHCPOFFER
Server Identifier: 193.168.3.2
IP Address Lease Time: 1d00h00m00s
Renewal Time Value: 12h00m00s
Rebinding Time Value: 21h00m00s
Subnet Mask: 255.255.255.0
Router: 193.168.3.1
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.46 seconds
(root@kali)-[/home/kali]
#
```

Рис. 3.31. Пошук доступних DHCP серверів.

На рисунку 3.31 можна побачити, що було знайдено доступний DHCP сервер. Тобто на нього будемо здійснювати атаку. Перед атакою перевіримо список виданих адрес за допомогою команди show dhcp binding.

За допомогою інструмента нам необхідно виловити DHCP пакет з підмережі. Це необхідно для того, щоб ми мали переслати цей пакет в підмережу стільки раз, скільки потрібно, для того щоб забрати всі доступні адреси, які може видати DHCP сервер. На рисунку 3.36 можна буде побачити, як виглядає виловлений DHCP пакет.

```
SW_1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration        Type      State
  Interface      Hardware address/
                  User name
193.168.3.3     0100.5079.6668.03    Jun 08 2021 06:59 PM    Automatic  Activ
e      Vlan1
193.168.3.4     0108.0027.0e34.8d    Jun 08 2021 07:00 PM    Automatic  Activ
e      Vlan1
193.168.3.5     dead.c0de.cafe       Jun 07 2021 07:06 PM    Automatic  Selec
ting Vlan1
SW_1#
```

Рис.3.32. Перевірка виданих DHCP адрес.

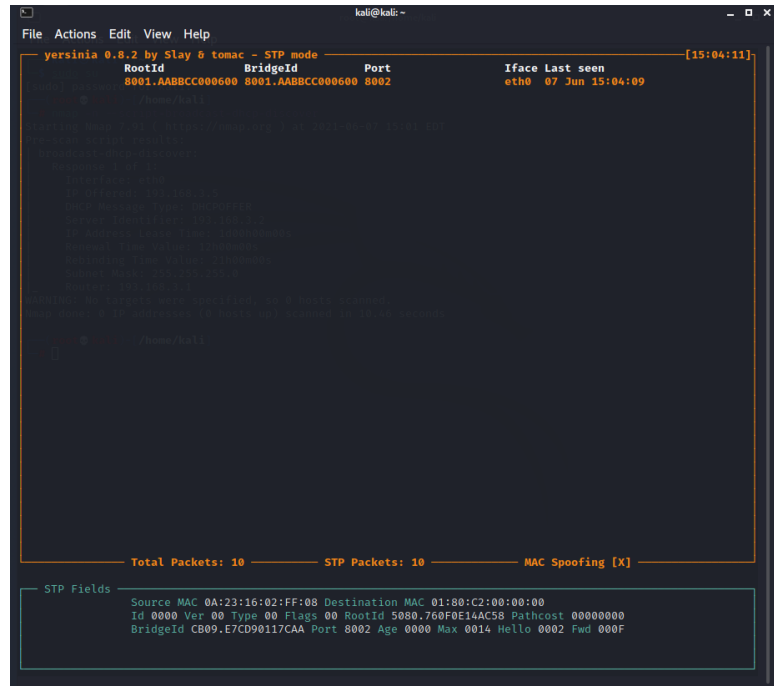


Рис.3.33. Виконання атаки DHCP Starvation

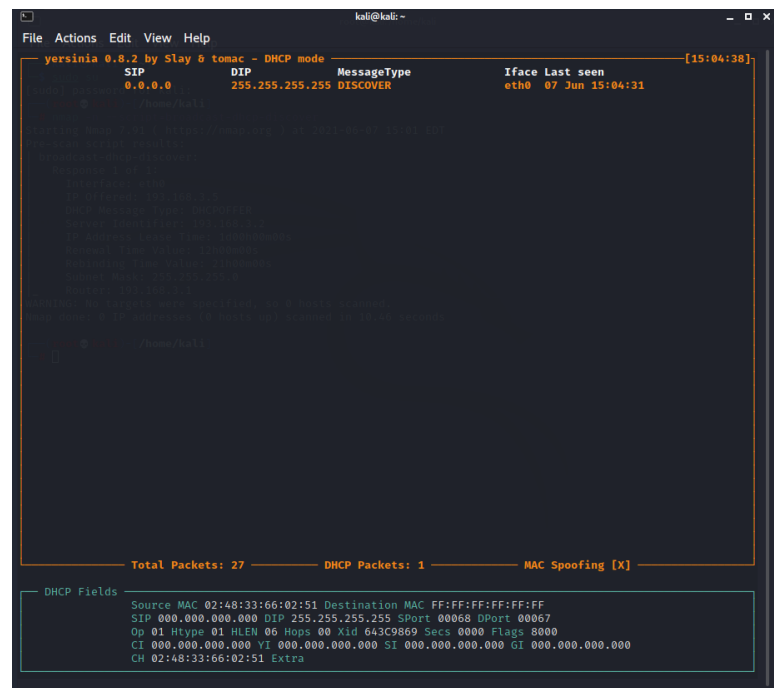


Рис.3.34. Виконання атаки DHCP Starvation

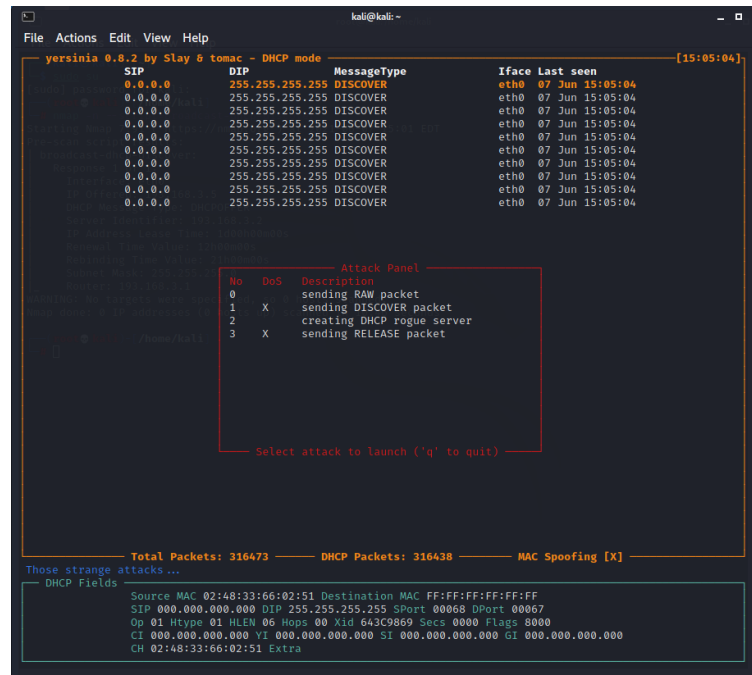


Рис.3.35. Виконання атаки DHCP Starvation

Як можна побачити на рисунку 3.35, програма починає посилати дуже багато DHCP пакетів, для того щоб швидко виснажити DHCP сервер і забрати всі доступні DHCP адреси.



Рис.3.36. Перевірка роботи DHCP сервера.

Тобто на рисунку 3.36 можна побачити, що DHCP сервер вийшов з ладу а це значить, що атаку виконано успішно.

SW_1#show ip dhcp binding						
Bindings from all pools not associated with VRF:						
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type	State	Interface	
193.168.3.3	0100.5079.6668.03	Jun 08 2021 07:04 PM	Automatic	Active	Vlan1	
193.168.3.4	0108.0027.0e34.8d	Jun 08 2021 07:00 PM	Automatic	Active	Vlan1	
193.168.3.5	dead.c0de.cafe	Jun 07 2021 07:14 PM	Automatic	Selecting	Vlan1	
193.168.3.6	0942.f04e.45e4	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.7	c7e7.8e05.75e5	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.8	6a6d.be66.7807	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.9	c712.506f.797a	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.10	bef9.4925.528c	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.11	a6d8.a207.6571	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.12	0d79.ac00.90a5	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.13	f5c1.ea73.6849	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.14	2c90.2a07.c562	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.15	bd57.df45.c11f	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.16	882f.493f.366a	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.17	2dd1.cc6c.f11a	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.18	6ad1.562c.d408	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.19	bc45.3865.1512	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.20	522f.e309.8fe5	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.21	105c.6224.2fca	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.22	5d49.7900.c86d	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.23	3b56.6a59.ff1d	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	
193.168.3.24	54f1.eb03.bcb1	Jun 07 2021 07:10 PM	Automatic	Selecting	Vlan1	

Рис. 3.37. Перевірка виданих IP адрес DHCP сервером

На рисунку 3.37 ми бачимо, що DHCP сервер видав всі можливі та доступні адреси, тобто нові користувачі уже не зможуть підключитися до підмережі.

Далі виконаємо DoS атаку на створений раніше сайт. Виконувати атаку будемо за допомогою GoldenEye. Спочатку потрібно перевірити, чи працює наш локальний сайт (рис. 3.38).

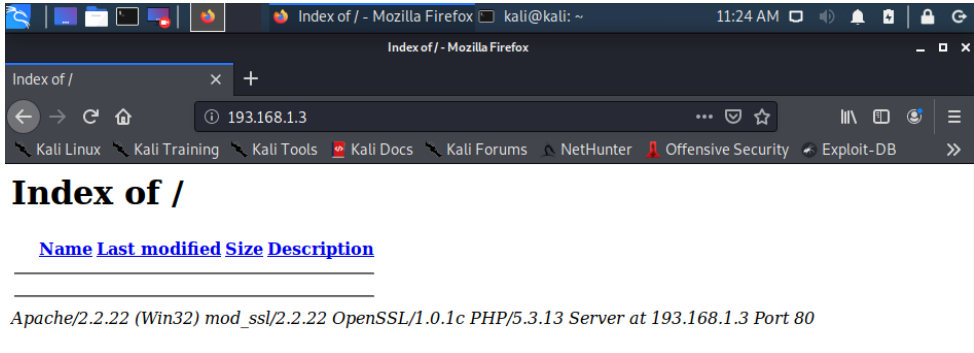


Рис.3.38. Перевірка працездатності сайту

Як бачимо, цей сайт працює, тобто на нього можна спробувати виконати атаку (рим 3.39-3.42).

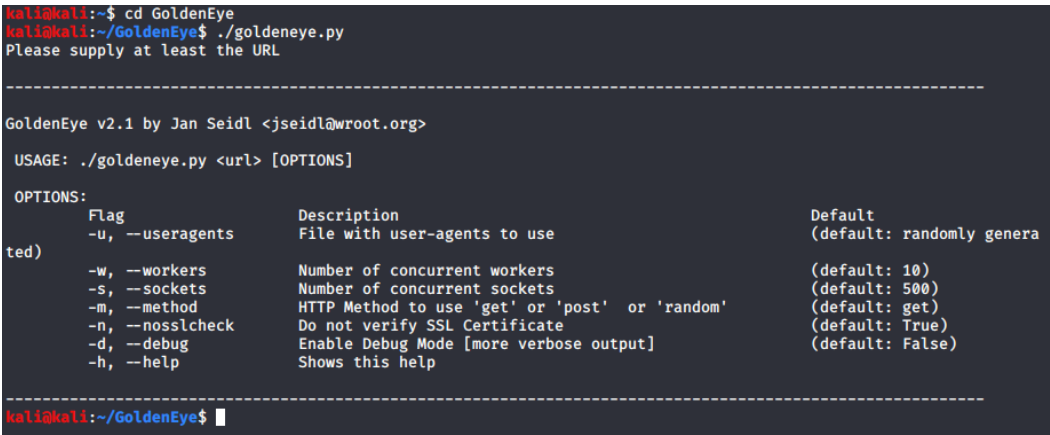


Рис. 3.39. Виконання атаки DoS

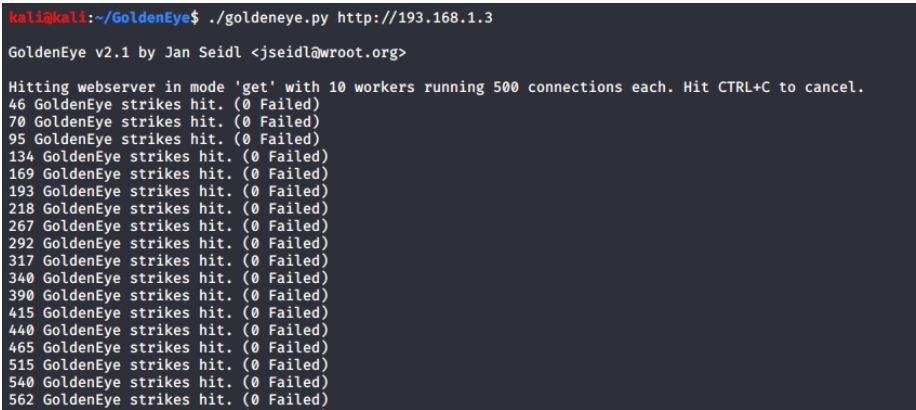


Рис. 3.40. Виконання атаки DoS

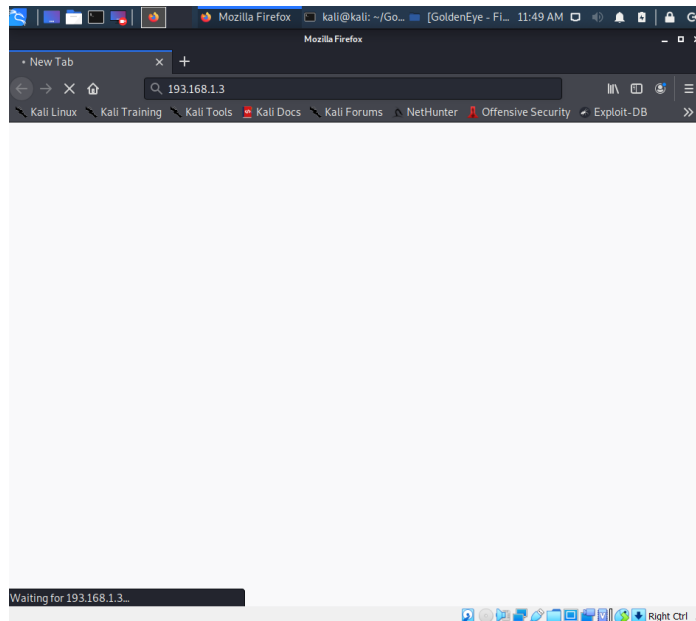


Рис. 3.41. Виконання атаки DoS

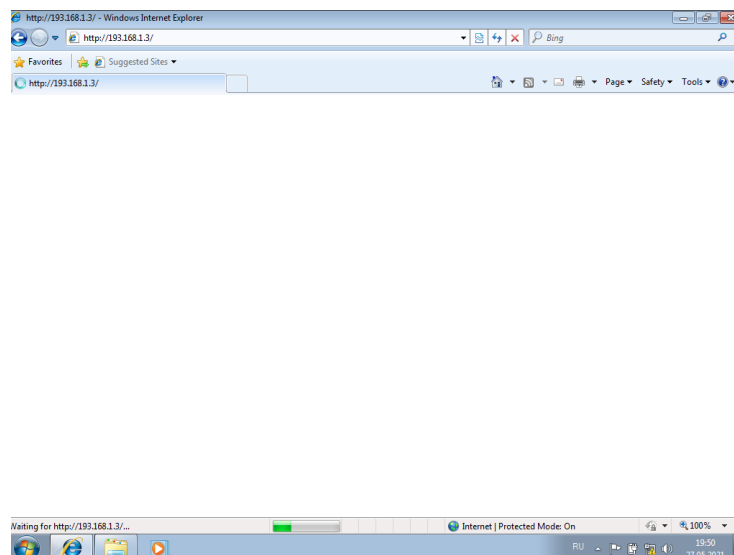


Рис.3.42. Виконання атаки DoS

Як можна побачити на рисунках 3.41-3.42, сайт уже перестав працювати, тобто атака була виконана успішно.

Захват из - [R_Central Ethernet1/0 to R_3 Ethernet0/0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
26529	1186.290809	193.168.2.3	193.168.1.3	TCP	66	37596 → 80 [ACK] Seq=1 Ac
26530	1186.290924	193.168.2.3	193.168.1.3	HTTP	540	GET /?GTdwuij8xT=aHbTABCE
26531	1186.290973	193.168.1.3	193.168.2.3	TCP	78	80 → 37182 [ACK] Seq=1 Ac
26532	1186.291060	193.168.1.3	193.168.2.3	TCP	78	80 → 37166 [ACK] Seq=1 Ac
26533	1186.291258	193.168.1.3	193.168.2.3	TCP	78	80 → 37184 [ACK] Seq=1 Ac
26534	1186.291471	193.168.2.3	193.168.1.3	TCP	74	37618 → 80 [SYN] Seq=0 Wi
26535	1186.291520	193.168.1.3	193.168.2.3	TCP	78	80 → 37178 [ACK] Seq=1 Ac
26536	1186.291661	193.168.1.3	193.168.2.3	TCP	74	80 → 37598 [SYN, ACK] Seq
26537	1186.291845	193.168.1.3	193.168.2.3	TCP	74	80 → 37600 [SYN, ACK] Seq
26538	1186.292017	193.168.1.3	193.168.2.3	TCP	74	80 → 37602 [SYN, ACK] Seq

Рис. 3.43. Кількість відправлених пакетів при виконанні атаки

На рисунку 3.43 можна побачити, що програма надсилає велику кількість TCP пакетів, які сервер не встигає обробляти і виходить із ладу.

3.3 Налаштування захисту та перевірка роботи мережі

Для нормальної роботи мережі потрібно налаштувати захист мережі, щоб порушники не мали змогу атакувати мережу. Спочатку налаштуємо захист проти DHCP starvation. В цьому нам допоможе port-security (рис.3.45).

```
SW_2(config)#int e0/1
SW_2(config-if)#swit
SW_2(config-if)#switchport mode ac
SW_2(config-if)#switchport mode access
SW_2(config-if)#switchport port-s
SW_2(config-if)#switchport port-security
SW_2(config-if)#switchport port-security ma
SW_2(config-if)#switchport port-security maximum 10
SW_2(config-if)#switchport port-security mac-address sticky
SW_2(config-if)#switchport port-security violation protect
SW_2(config-if)#exit
SW_2(config)#int e0/1
SW_2(config-if)#ip dhc
SW_2(config-if)#ip dhcp snooping limit rate 50
SW_2(config-if)#exit
SW_2(config)#
```

Рис.3.44. Налаштування захисту

За допомогою даних команд було зроблено захист, а саме встановлено максимальну кількість MAC-адрес на порту – 10. Всі MAC-адреси записуються, і тепер по записам в комутаторі кожній MAC-адресі присвоюється своя IP-адреса. У випадку, коли йде переповнення пакетів, всі вони відкидаються, а також максимальна кількість DHCP-пакетів не перевищує 50.

Тепер можна повторно здійснити атаку і перевірити, як працює захист (рис. 3.45 – 3.46).

Як можна побачити на рисунку 3.47, захист пройшов успішно. Тобто порушники тепер не зможуть отримувати безліч IP-адрес і виводи з ладу DHCP-сервер.

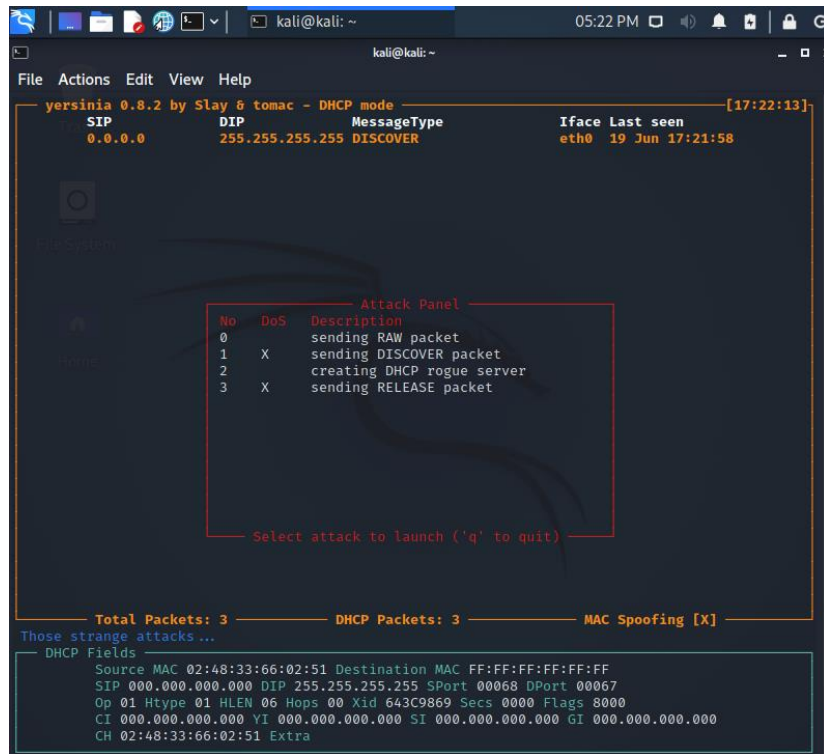


Рис. 3.45. Проведення повторної атаки DHCP starvation.

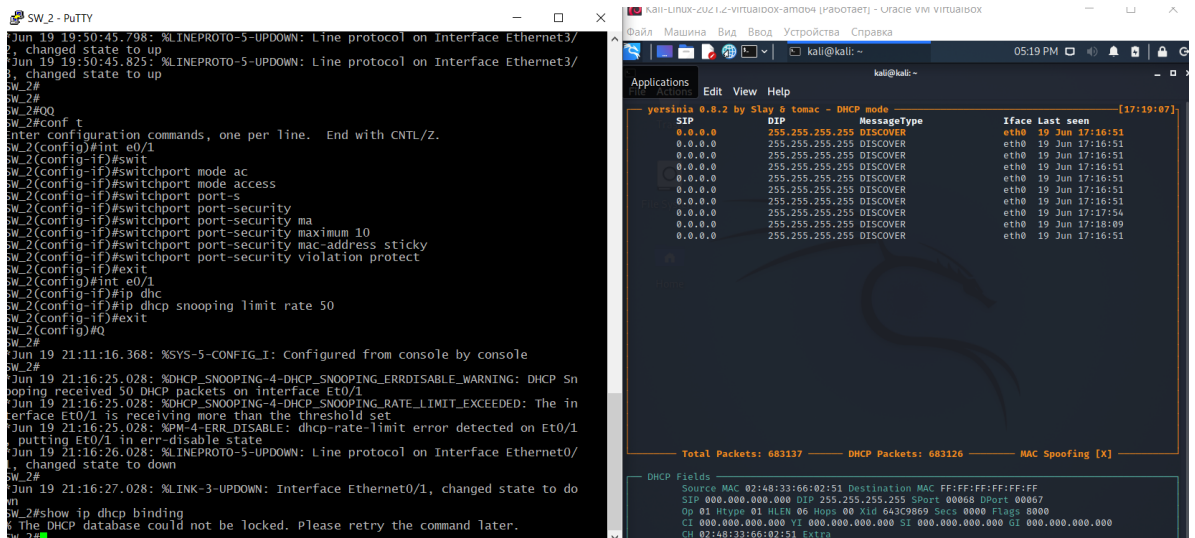


Рис.3.46. Реакція комутатора на атаку DHCP starvation

SW_2#sh ip dhcp binding						
Bindings from all pools not associated with VRF:						
IP address	Client-ID/	Lease expiration	Type	State	Inter	
face						
	Hardware address/					
	User name					
193.168.2.3	0100.5079.6668.00	Jun 20 2021 09:29 PM	Automatic	Active	Vlan1	
SW_2#						

Рис. 3.47. Кількість виданих IP-адрес після атаки.

Тепер потрібно також налаштувати захист проти атаки на протокол ARP. А саме налаштуємо захист проти атаки ARP-spoofing. Для того, щоб захистити підмережу від таких типів атак, необхідно використовувати Dynamic ARP Inspection. Тобто DAI буде вирішувати, які запити пропускати, які відкидати. Для того, що DAI працював, спочатку необхідно налаштувати DHCP snooping (рис. 3.48 – 3.50).

```
SW_2(config)#ip dhcp snooping vlan 1
SW_2(config)#ip dhcp snooping database disk0
SW_2(config)#ip dhcp snooping
SW_2(config)#int e0/0
SW_2(config-if)#ip dhcp snooping trust
SW_2(config-if)#exit
SW_2(config)#
```

Рис. 3.48. Налаштування DHCP snooping

```
SW_2#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0100 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes       yes             unlimited
Custom circuit-ids:
SW_2#
```

Рис. 3.49. Перевірка налаштувань DHCP snooping

```
SW_2#sh ip dhcp snooping binding
MacAddress                IpAddress        Lease(sec)  Type           VLAN  Interface
-----
00:50:79:66:68:01        193.168.2.3      86268      dhcp-snooping  1     Ethernet0/1
08:00:27:0E:34:8D        193.168.2.5      86320      dhcp-snooping  1     Ethernet0/1
Total number of bindings: 2
SW_2#
```

Рис. 3.50. Перевірка налаштувань DHCP snooping

Тепер порушник не зможе стати DHCP сервером. Якщо він спробує, то комутатор буде відкидати його запити. На основі таблиці, де зберігаються всі записи MAC та IP адрес, буде працювати механізм DAI.

Далі вже можна переходити до налаштування DAI (рис. 3.51 – 3.52)

```

SW_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_2(config)#ip arp inspection vlan 1
SW_2(config)#int e0/0
SW_2(config-if)#ip arp inspection trust
SW_2(config-if)#exit
SW_2(config)#errdisable recovery cause arp-inspection
SW_2(config)#

```

Рис. 3.51. Налаштування DAI

Даними командами включили DAI, також дали функцію довіреного порта, який йде до маршрутизатора, а також включили функцію відновлення порта, якщо MAC та IP адреси відповідають.

```

SW_2#show ip arp inspection int

```

Interface	Trust State	Rate (pps)	Burst Interval
Et0/0	Trusted	None	N/A
Et0/1	Untrusted	15	1
Et0/2	Untrusted	15	1
Et0/3	Untrusted	15	1
Et1/0	Untrusted	15	1
Et1/1	Untrusted	15	1
Et1/2	Untrusted	15	1
Et1/3	Untrusted	15	1
Et2/0	Untrusted	15	1
Et2/1	Untrusted	15	1
Et2/2	Untrusted	15	1
Et2/3	Untrusted	15	1
Et3/0	Untrusted	15	1
Et3/1	Untrusted	15	1
Et3/2	Untrusted	15	1
Et3/3	Untrusted	15	1

```

SW_2#

```

Рис. 3.52. Перевірка налаштувань.

Тепер можна повторно здійснити атаку і перевірити захист, який було налаштовано (рис.3.53 – 3.54).

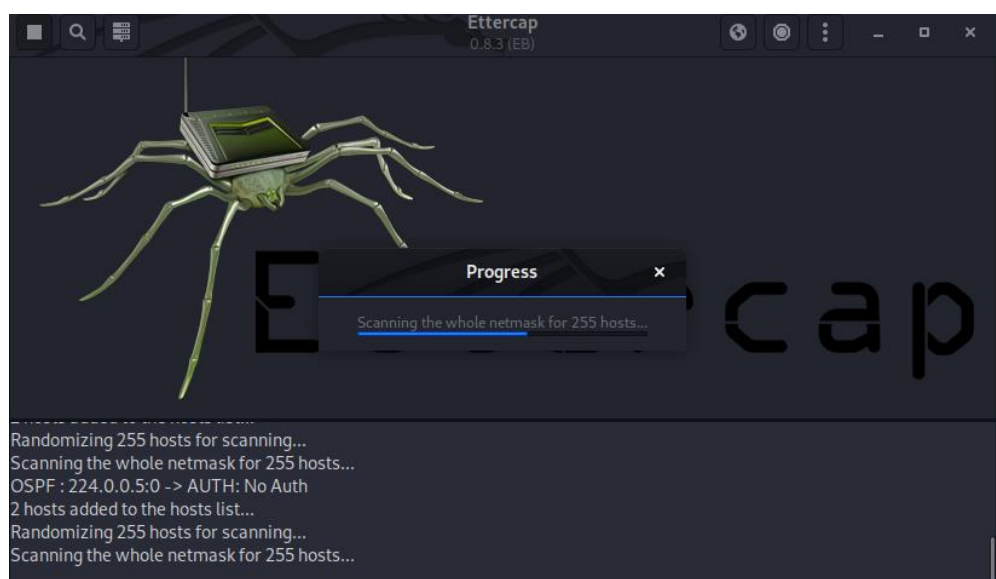


Рис. 3.53. Виконання повторної атаки ARP-spoofing



Рис. 3.54. Реакція комутатора на атаку ARP-spoofing

На рисунку 3.54 можна побачити, що комутатор реагує на атаку і захищає, тобто відкидає пакети.

Далі потрібно налаштувати захист проти DoS атаки. Для цього спочатку необхідно дізнатися, звідки йде атака. Так як в нас локальна мережа, то на допомогу приходить Wireshark (рис.3.55).

26572	1186.297529	193.168.1.3	193.168.2.3	TCP	66 80 → 37238 [ACK] Seq=1 Ac
26573	1186.297656	193.168.1.3	193.168.2.3	TCP	78 [TCP Dup ACK 26550#1] 80
26574	1186.299028	193.168.1.3	193.168.2.3	TCP	78 [TCP Dup ACK 26561#1] 80
26575	1186.299649	193.168.1.3	193.168.2.3	TCP	78 [TCP Dup ACK 26562#1] 80
26576	1186.299845	193.168.1.3	193.168.2.3	TCP	78 [TCP Dup ACK 26551#1] 80
26577	1186.300067	193.168.1.3	193.168.2.3	TCP	74 80 → 37604 [SYN, ACK] Sec

Рис. 3.55. Перевірка за допомогою Wireshark

Тобто ми дізналися, що атака йде з IP-адреси 193.168.2.3. Так як це локальна мережа, то атака йде з підмережі 193.168.2.0. Для запобігання атаки ми можемо просто обмежити пропускну здатність від даної мережі (рис.3.56 – 3.58).

```
R_Central#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Central(config)#int e0/3
R_Central(config-if)#rate-limit output 8000 1500 2000 conf
R_Central(config-if)#$output 8000 1500 2000 conform-action transmit ex
R_Central(config-if)#$0 1500 2000 conform-action transmit exceed-action drop
R_Central(config-if)#
```

Рис. 3.56. Обмеження пропускну здатності на порту комутатора

R_Central

Тепер повторно проведемо атаку і перевіримо, чи спрацював захист (рис.3.57).

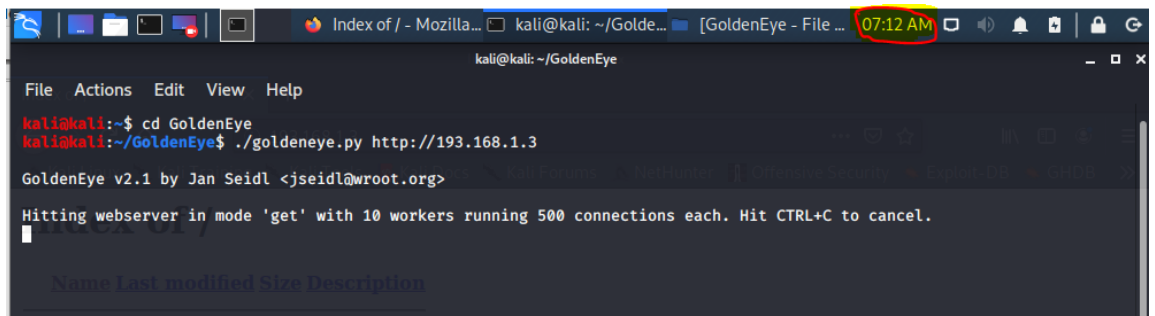


Рис. 3.57. Проведення повторної DoS атаки

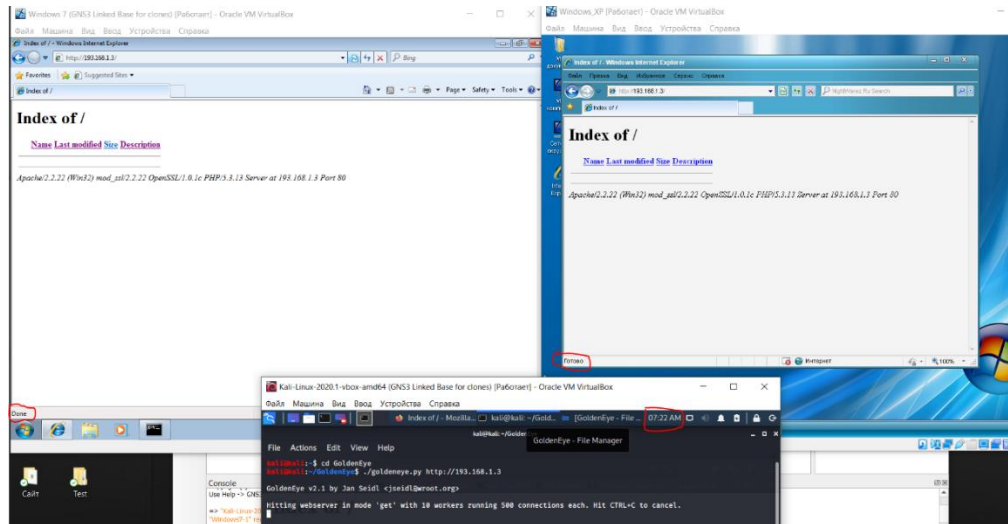


Рис. 3.58. Перевірка працездатності сайту.

Як можна побачити на рисунку 3.58, сайт працює, значить захист спрацював.

Також для додаткового захисту було налаштовано хешування MD5 та протокол віддаленого доступу SSH (рис. 3.59 – 3.61).

No.	Time	Source	Destination	Protocol	Length	Info
64	140.877636	192.168.3.2	224.0.0.5	OSPF	94	Hello Packet
65	141.495812	aa:bb:cc:00:05:20	aa:bb:cc:00:05:20	LOOP	60	Reply
66	142.942824	192.168.3.1	224.0.0.5	OSPF	94	Hello Packet
67	150.054386	aa:bb:cc:00:04:00	aa:bb:cc:00:04:00	LOOP	60	Reply
68	150.583920	192.168.3.2	224.0.0.5	OSPF	94	Hello Packet
69	150.946776	aa:bb:cc:00:04:00	aa:bb:cc:00:04:00	CDP/VTP/DTP/PagP/UDL	315	Device ID: R_1 Port ID: Ethernet0/0
70	151.501404	aa:bb:cc:00:05:20	aa:bb:cc:00:05:20	LOOP	60	Reply
71	152.238216	192.168.3.1	224.0.0.5	OSPF	94	Hello Packet
72	160.056134	aa:bb:cc:00:04:00	aa:bb:cc:00:04:00	LOOP	60	Reply
73	160.416319	192.168.3.2	224.0.0.5	OSPF	94	Hello Packet
74	161.506108	aa:bb:cc:00:05:20	aa:bb:cc:00:05:20	LOOP	60	Reply
75	161.859018	192.168.3.1	224.0.0.5	OSPF	94	Hello Packet
76	169.751121	192.168.3.2	224.0.0.5	OSPF	94	Hello Packet
77	170.063765	aa:bb:cc:00:04:00	aa:bb:cc:00:04:00	LOOP	60	Reply
78	171.510408	aa:bb:cc:00:05:20	aa:bb:cc:00:05:20	LOOP	60	Reply
79	171.844134	192.168.3.1	224.0.0.5	OSPF	94	Hello Packet
80	179.124406	192.168.3.2	224.0.0.5	OSPF	94	Hello Packet
81	180.068086	aa:bb:cc:00:04:00	aa:bb:cc:00:04:00	LOOP	60	Reply
82	181.514548	aa:bb:cc:00:05:20	aa:bb:cc:00:05:20	LOOP	60	Reply
83	181.598490	192.168.3.1	224.0.0.5	OSPF	94	Hello Packet

Packet Length: 48	
Source OSPF Router: 193.168.3.1	
Area ID: 0.0.0.0 (Backbone)	
Checksum: 0xd9f6 [correct]	
Auth Type: Null (0)	
Auth Data (none): 0000000000000000	
> OSPF Hello Packet	
> OSPF LLS Data Block	

0010	00 50 00 27 00 00 01 59	14 bf c0 a8 03 02 e0 00	..P...Y.....
0020	00 05 02 01 00 30 c1 a8	03 01 00 00 00 d9 f6	...0.....
0030	00 00 00 00 00 00 00 00	00 00 ff ff ff fc 00 0a	
0040	12 01 00 00 28 c0 a8	03 02 c0 a8 03 01 c0 a8	
0050	05 01 ff f6 00 03 00 01	00 04 00 00 00 01	

Рис. 3.59. Вигляд аутентифікації протокола OSPF до налаштувань.

```

R_Central(config)#int e0/1
R_Central(config-if)#ip ospf mes
R_Central(config-if)#ip ospf message-digest-key 13 md5 cisco
R_Central(config-if)#router ospf 1
R_Central(config-router)#area 0 aut
R_Central(config-router)#area 0 authentication me
R_Central(config-router)#area 0 authentication message-digest
R_Central(config-router)#exit
R_Central(config)#
*Jun  6 13:23:45.473: %OSPF-5-ADJCHG: Process 1, Nbr 193.168.2.1 on Ethernet0/3
from FULL to DOWN, Neighbor Down: Dead timer expired
*Jun  6 13:23:45.627: %OSPF-5-ADJCHG: Process 1, Nbr 193.168.3.1 on Ethernet0/2
from FULL to DOWN, Neighbor Down: Dead timer expired
R_Central(config)#
*Jun  6 13:23:50.649: %OSPF-5-ADJCHG: Process 1, Nbr 193.168.4.1 on Ethernet0/1
from FULL to DOWN, Neighbor Down: Dead timer expired
*Jun  6 13:23:51.318: %OSPF-5-ADJCHG: Process 1, Nbr 193.168.1.1 on Ethernet1/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R_Central(config)#int e0/2
R_Central(config-if)#ip ospf me
R_Central(config-if)#ip ospf message-digest-key 13 md5 cisco
R_Central(config-if)#router ospf 1
R_Central(config-router)#area 0 au
R_Central(config-router)#area 0 authentication me
R_Central(config-router)#area 0 authentication message-digest
R_Central(config-router)#exit
R_Central(config)#int e0/3
R_Central(config-if)#ip ospf me
R_Central(config-if)#ip ospf message-digest-key 13 md5 cisco
R_Central(config-if)#router ospf 1
R_Central(config-router)#area 0 au
R_Central(config-router)#area 0 authentication me
R_Central(config-router)#area 0 authentication message-digest
R_Central(config-router)#exit
R_Central(config)#int e1/0
R_Central(config-if)#ip ospf me
R_Central(config-if)#ip ospf message-digest-key 13 md5 cisco
R_Central(config-if)#router ospf 1
R_Central(config-router)#area 0 au
R_Central(config-router)#area 0 authentication me
R_Central(config-router)#area 0 authentication message-digest
R_Central(config-router)#exit
R_Central(config)#

```

Рис. 3.60. Налаштування MD5 на маршрутизаторі R_Central

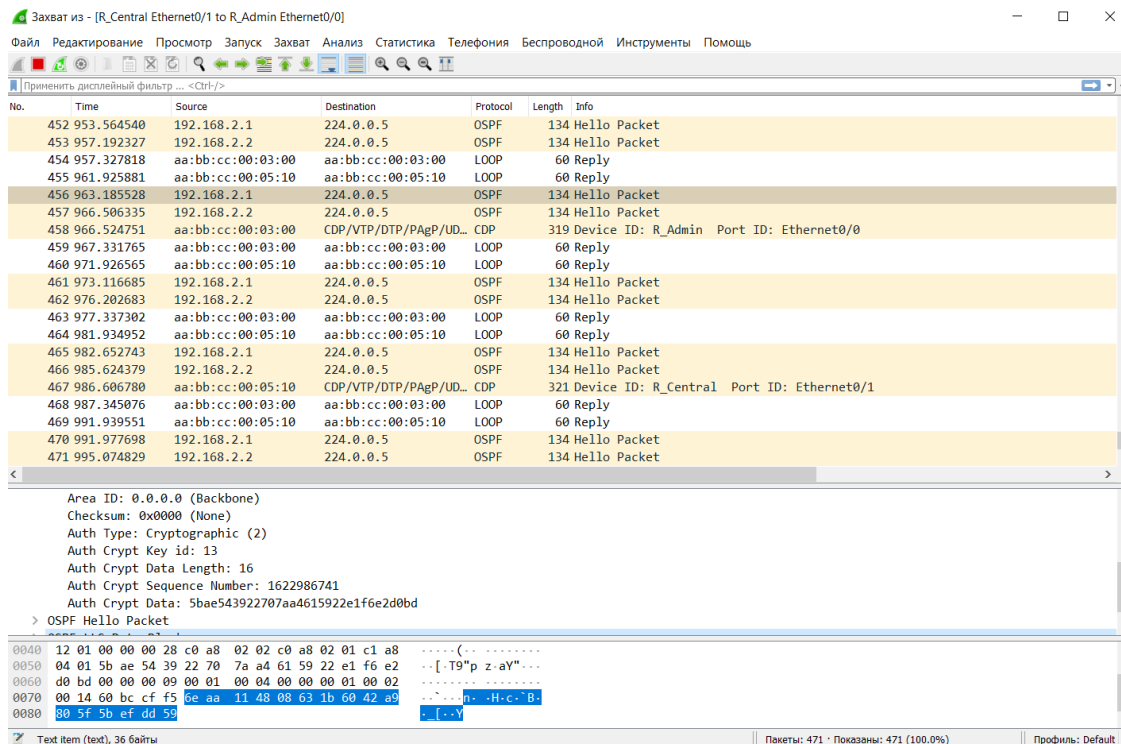


Рис. 3.61. Вигляд аутентифікації протокола OSPF після налаштувань.

					Арк.
					52
Змн.	Арк.	№ докум.	Підпис	Дата	

Налаштування пройшло успішно. Далі налаштуємо SSH з різними типами користувачами для різного доступу (рис. 3.62 – 3.64).

```
R_Central#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Central(config)#ip domain-name mylan.local
R_Central(config)#crypto key generate rsa
The name for the keys will be: R_Central.mylan.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R_Central(config)#
*Jun  6 14:11:38.409: %SSH-5-ENABLED: SSH 1.99 has been enabled
R_Central(config)#username admin privi
R_Central(config)#username admin privilege 15 password cisco
R_Central(config)#enable secret ciscocisco
R_Central(config)#service pasw
R_Central(config)#service passw
R_Central(config)#service password-encryption
R_Central(config)#line vty 0 4
R_Central(config-line)#login local
R_Central(config-line)#transport input ssh
R_Central(config-line)#exec-timeout 60 0
R_Central(config-line)#logging sy
R_Central(config-line)#logging synchronous
R_Central(config-line)#exit
R_Central(config)#line console 0
R_Central(config-line)#logging local
^
% Invalid input detected at '^' marker.

R_Central(config-line)#login local
R_Central(config-line)#log
R_Central(config-line)#loggin
R_Central(config-line)#logging sy
R_Central(config-line)#logging synchronous
R_Central(config-line)#exec-timeout 60 0
R_Central(config-line)#exit
R_Central(config)#
```

Рис. 3.62. Налаштування користувача admin та протоколу SSH

```
R_Central(config)#username user privilege 3 password cisco
R_Central(config)#privilege exec level 3 configure terminal
R_Central(config)#privilege exec level 3 show int
R_Central(config)#privilege exec level 3 show ip route
R_Central(config)#line vty 0 4
R_Central(config-line)#login local
R_Central(config-line)#log
R_Central(config-line)#logg
R_Central(config-line)#logging syn
R_Central(config-line)#logging synchronous
R_Central(config-line)#ex
% Ambiguous command: "ex"
R_Central(config-line)#exit
R_Central(config)#line console 0
R_Central(config-line)#login local
R_Central(config-line)#logging synchronous
R_Central(config-line)#exit
R_Central(config)#
```

Рис. 3.63. Налаштування користувача user

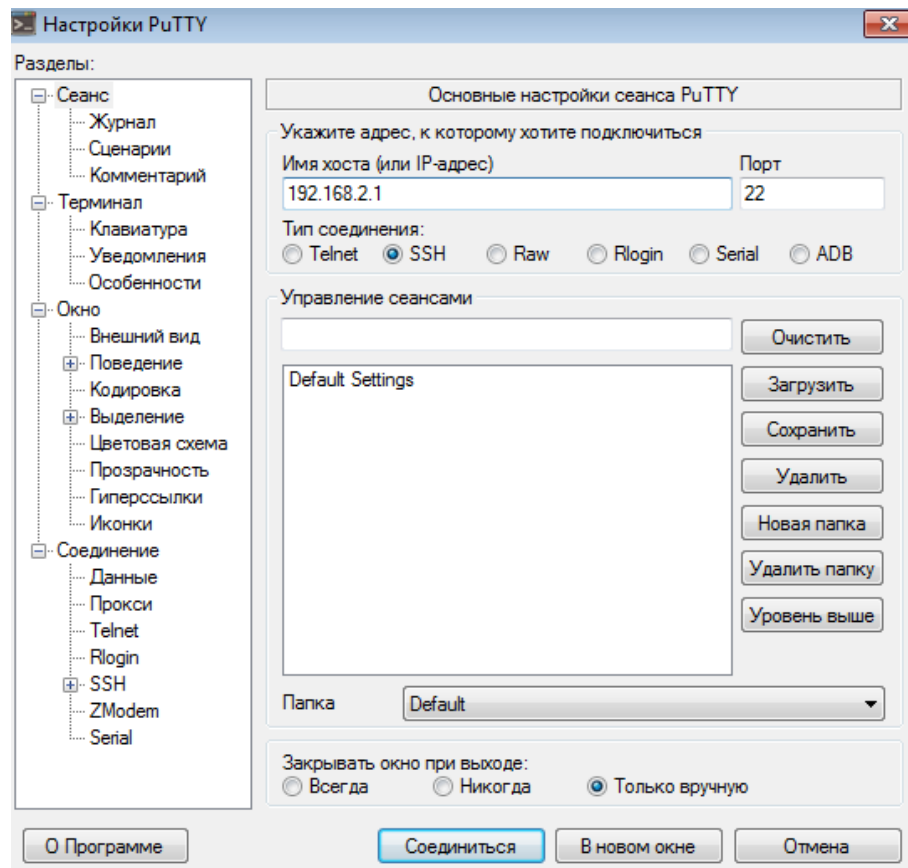


Рис. 3.64. Перевірка працездатності SSH

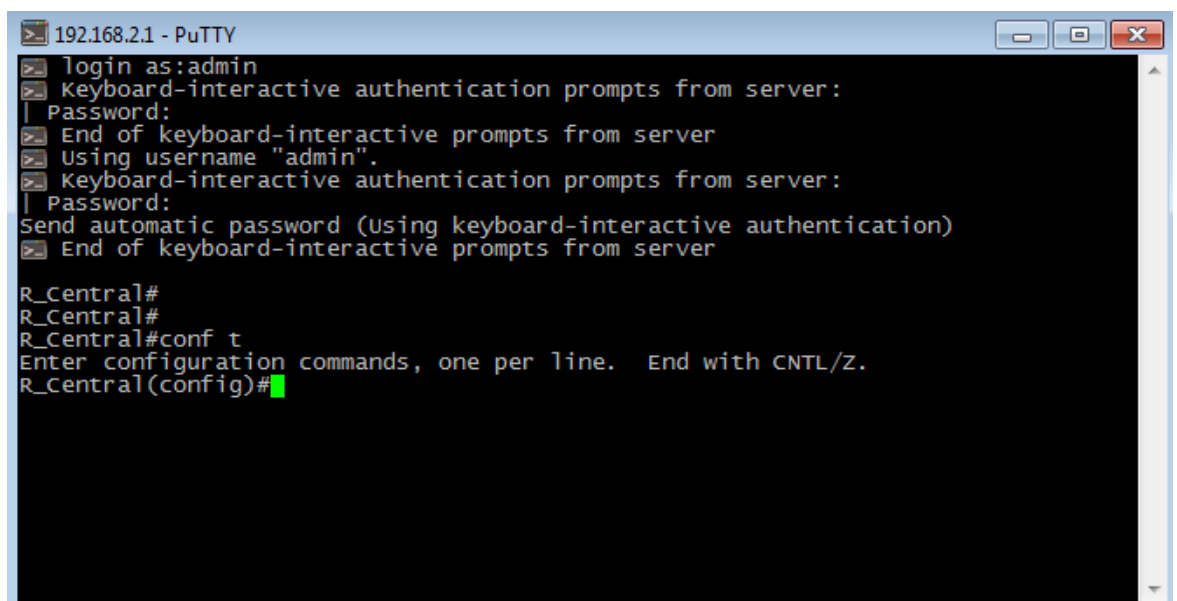


Рис. 3.65. Перевірка працездатності SSH

Як можна побачити на рисунку 3.65 SSH працює.

Всі налаштування необхідно зробити також і на інших пристроях мережі, для того щоб мережа мала захист.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

3.4 Аналіз результатів тестування

Всі поставлені завдання були виконані успішно. В подальшому дана мережа може бути розширена. Для цього було налаштовано DHCP маршрутизацію, що дасть змогу в подальшому додавати нових користувачів. В рівні ядра було використано прилади від компанії Cisco, що в подальшому можна використати і в розробці реальної мережі, так як можна підібрати пристрій, який саме буде підходити для тих чи інших задач.

В мережі було налаштовано захист комутаторів за допомогою захисту портів, що не дасть змогу порушникам виводити з ладу DHCP адресацію і забезпечить захист між мережею та користувачем. Також було налаштовано захист проти підміни MAC адреси для того, щоб за кожним користувачем був закріплений свій адрес. Було додатково налаштовано протокол віддаленого доступу SSH з різними користувачами. Дане налаштування в майбутньому допоможе адміністратору віддалено налаштовувати пристрої.

Якщо дивитися на подальше розширення мережі, то найкраще для цього буде підходити підмережа Lan K. Основною причиною такого рішення є те, що дана підмережа знаходиться якнайдалі від підмережі, де знаходиться сервер з локальним сайтом. Тобто в випадку, якщо під'єднається порушник, буде легко виявити його та знешкодити так, щоб він не наніс великої шкоди і мережа могла і далі працювати.

Також в даній підмережі нові користувачі під'єднуються не напряму до комутатора, що також в подальшому допоможе ефективніше захищати мережу від атак та різних порушників.

Щодо недоліків в даній мережі, виділимо те що, всі підмережі з'єднані між собою всього за допомогою одного маршрутизатора. Тобто якщо даний маршрутизатор вийде з ладу, то і вся мережа перестане коректно працювати. В подальшому при розширенні мережі необхідно використовувати декілька маршрутизаторів, з'єднаних між собою, щоб в випадку коли один виходить з ладу, інші могли знайти додаткові маршрути і підтримувати мережу

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

працездатною. Адже на великих підприємствах, коли мережа виходить з ладу навіть на декілька годин, це уже призводить до великих збитків.

Висновок до розділу 3

В даному розділі було проведено розробку мережі та базові налаштування пристроїв мережі. Було налаштовано декілька комутаторів, які виступали в ролі DHCP серверів для зручності і, в подальшому, для розвитку мережі.

В мережу було додано операційну систему Kali Linux, яка виступала як зловмисник. За допомогою інструментів даної операційної системи було проведено такі атаки як DoS, DHCP starvation та ARP-Spoofing на не захищену мережу, та розглядалась реакція пристроїв та самої мережі на дані атаки.

Було налаштовано захист від таких атак як DoS, DHCP starvation, ARP-Spoofing, Rogue DHCP Server, MAC-Spoofing. Додатково було налаштовано хешування MD5 та протокол віддаленого доступу SSH. Було проведено повторні атаки вже на захищену мережу та перевірено реакцію пристроїв та мережі на дані атаки. Також було проведено аналіз здійснених налаштувань і отриманих результатів із зазначенням недоліків мережі, варіантами їх вирішення та перспективами покращення,

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В кваліфікаційній роботі було розглянуто основні положення про локальну мережу та основні принципи розробки самої локальної мережі. Також було розглянуто можливість створення мереж підприємств, основні технології розробки та обрано найбільш підходящі. Було обґрунтовано необхідність використання для великих мереж динамічної (DHCP) маршрутизації в зв'язку з великою кількістю співробітників та користувачів.

Було розглянуто основні типи атак, які використовують зловмисники для того, щоб порушити працездатність мережі та отримати інформацію для свого користування, що може призвести до неполадок в мережі. Також було розглянуто захист від даних атак для того, щоб убезпечити мережу, і в подальшому забезпечити нормальне функціонування пристроїв та безпечне підключення користувачів, щоб їх інформація залишалась конфіденційною.

Для розробки мережі було проведено аналіз для того, щоб розробити оптимальний варіант з'єднання пристроїв в мережі між собою та розроблено таблицю з'єднань для подальшого використання в розширенні мережі. Також було розроблено IP-адресацію мережі. Для зручності підключення нових користувачів в деяких підмережах було налаштовано динамічну маршрутизацію.

Далі було вибрано програмне та апаратне забезпечення мережі, яке дає змогу зручно розробляти та працювати в мережі. Саму мережу було розроблено в трирівневій ієрархічній структурі що в подальшому дозволяє легко розширювати мережу, дозволяє швидко знаходити якісь неполадки та також швидко їх усувати. Тобто сама мережа складається з трьох рівнів, а саме: рівня ядра, рівня розподілу та рівня доступу. Кожен з рівнів має свої переваги, що в цілому дуже добре позначається на мережі і дає цілий комплекс переваг в подальшій роботі над мережею.

З самого обладнання було вибрано обладнання від компанії Cisco, тому що саме воно має дуже багато переваг та підходить в розробці мереж, як

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

великих так і малих. Саме маршрутизатори та комутатори від цієї компанії мають дуже велику кількість можливостей в подальшій розробці мережі.

Також було обрано програмне забезпечення для розробки мережі, а саме симулятор GNS3, що дозволяє розробляти мережі, які максимально схожі з реальними, а також за допомогою VirtualBox додавати віртуальні машини, що дає змогу працювати з реальними операційними системами. Для того, щоб слідкувати за пакетами в мережі, було використано програму WireShark.

За допомогою VirtualBox було додано віртуальну машину Kali Linux. Саме за допомогою цієї операційної системи було проведено атаки на мережу, так як вона має багато інструментів, які дозволяють тестувати мережі на захищеність. Також за допомогою віртуальної машини Windows 7 та програми Denwer було створено локальний сайт. Тобто комплекс цих програм дозволяє зручно розроблювати мережі.

В результаті було створено локальну мережу підприємства, яка складається з:

- робочої станції Windows 7, яка відповідає за роботу локального сайту;
- робочої станції Windows XP;
- робочої станції Kali Linux, за допомогою якої було здійснено тестування мережі.

Було проведено базове налаштування мережі, налаштування IP-адресації та налаштування протоколу OSPF для зв'язку між віддаленими підмережами. Також було проведено атаки на мережу до налаштування захисту, для перевірки реакції пристроїв та перевірки працездатності мережі в такому випадку. Було налаштовано захист та проведення повторних атак для перевірки роботи захисту. Додатково було налаштовано хешування MD5 та протокол віддаленого доступу SSH.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Local area network [Електронний ресурс] - [Local area network - Wikipedia](#)
2. ТОПОЛОГИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ [Електронний ресурс] - <http://kom-seti.narod.ru/index.files/4.htm?clk2398502361292193773143=1>
3. Rogue DHCP Server Attack [Електронний ресурс] - [Rogue DHCP Server Attack | Rogue DHCP | Info-savvy.com](#)
4. What is a DHCP Starvation Attack? [Електронний ресурс] - [What is a DHCP Starvation Attack? | CBT Nuggets](#)
5. MAC Spoofing Attack: All You Need to Know in 6 Important points [Електронний ресурс] - [MAC Spoofing Attack: All You Need to Know in 6 Important points \(jigsawacademy.com\)](#)
6. What is a denial of service attack [Електронний ресурс] - [What is a denial of service attack \(DoS\) ? - Palo Alto Networks](#)
7. Защищаем сеть L2 коммутаторами [Електронний ресурс] - [Защищаем сеть L2 коммутаторами / Хабр \(habr.com\)](#)
8. Атака канального уровня ARP-spoofing и как защитить коммутатор Cisco [Електронний ресурс] - [Атака канального уровня ARP-spoofing и как защитить коммутатор Cisco / Хабр \(habr.com\)](#)
9. The Three Elements of Defense Against Denial-of-Service Attacks [Електронний ресурс] - [The Three Elements of Defense Against Denial-of-Service Attacks | BizTech Magazine](#)
10. Трёхуровневая модель сети и технологии VLAN, DHCP, OSPF, STP, SNMP, ACL, NTP на Cisco и D-link [Електронний ресурс] - [Трёхуровневая модель сети и технологии VLAN, DHCP, OSPF, STP, SNMP, ACL, NTP на Cisco и D-link / Хабр \(habr.com\)](#)
11. Принципы работы протокола DHCP [Електронний ресурс] - [Протокол DHCP - назначение, настройки и принципы работы \(smart-soft.ru\)](#)
12. Протокол маршрутизации OSPF [Електронний ресурс] - [Протокол маршрутизации ospf - что такое, принцип работы \(smart-soft.ru\)](#)

13. Kali Linux [Электронный ресурс] - [Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution](#)
14. 10 Reasons to Choose Cisco Switching [Электронный ресурс] - [Singapore AAG flyer \(cisco.com\)](#)
15. GNS3 – Графический Сетевой Симулятор [Электронный ресурс] - [GNS3 - Графический Сетевой Симулятор » CiscoLab - Лаборатория Сетей](#)
16. Oracle VM VirtualBox что это за программа и нужна ли она? [Электронный ресурс] - [Oracle VM VirtualBox что это за программа и нужна ли она? \(virtmachine.ru\)](#)
17. Что такое WireShark? Для чего нужна эта программа? [Электронный ресурс] - [Что такое WireShark? Для чего нужна эта программа? \(nordd.ru\)](#)
18. Денвер (программа) [Электронный ресурс] - [Денвер \(программа\) — Википедия \(wikipedia.org\)](#)
19. СТРЕСС-ТЕСТ СЕТИ: DOS ВЕБ-САЙТА В KALI LINUX С GOLDENEYE [Электронный ресурс] - [Стресс-тест сети: DoS веб-сайта в Kali Linux с GoldenEye \(biglan.ru\)](#)
20. Атаки на сетевое оборудование с Kali Linux [Электронный ресурс] - [Атаки на сетевое оборудование с Kali Linux / Хабр \(habr.com\)](#)
21. Ettercap [Электронный ресурс] - [Ettercap - Инструменты Kali Linux](#)

ДОДАТКИ

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор R_Central

R_Central

version 15.2	ip domain name mylan.local
service timestamps debug datetime msec	ip cef
service timestamps log datetime msec	no ipv6 cef
service password-encryption	!
!	multilink bundle-name authenticated
hostname R_Central	!
!	!
boot-start-marker	!
boot-end-marker	!
!	!
!	!
enable secret 5	crypto pki token default removal timeout 0
\$1\$WVjI\$49g7mp1ITgKrGqvpSY5ra1	!
!	!
no aaa new-model	username admin privilege 15 password 7
!	104D000A0618
mmi polling-interval 60	username user privilege 3 password 7
no mmi auto-configure	094F471A1A0A
no mmi pvc	!
mmi snmp-timeout 180	redundancy
no ip icmp rate-limit unreachable	!
ip auth-proxy max-login-attempts 5	!
ip admission max-login-attempts 5	ip tcp synwait-time 5
!	!
!	!
!	!
!	!
!	!
!	!
no ip domain lookup	!

!	shutdown
!	!
!	interface Ethernet1/3
!	no ip address
!	shutdown
interface Ethernet0/0	!
ip address 192.168.1.1 255.255.255.252	interface Serial2/0
!	no ip address
interface Ethernet0/1	shutdown
ip address 192.168.2.1 255.255.255.252	serial restart-delay 0
ip ospf message-digest-key 13 md5 7 02050D480809	!
!	interface Serial2/1
interface Ethernet0/2	no ip address
ip address 192.168.3.1 255.255.255.252	shutdown
ip ospf message-digest-key 13 md5 7 121A0C041104	serial restart-delay 0
!	!
interface Ethernet0/3	interface Serial2/2
ip address 192.168.4.1 255.255.255.252	no ip address
ip ospf message-digest-key 13 md5 7 13061E010803	shutdown
!	serial restart-delay 0
interface Ethernet1/0	!
ip address 192.168.5.1 255.255.255.252	interface Serial2/3
ip ospf message-digest-key 13 md5 7 0822455D0A16	no ip address
!	shutdown
interface Ethernet1/1	serial restart-delay 0
no ip address	!
shutdown	interface Serial3/0
!	no ip address
interface Ethernet1/2	shutdown
no ip address	serial restart-delay 0
	!
	interface Serial3/1

no ip address	!
shutdown	!
serial restart-delay 0	!
!	!
interface Serial3/2	!
no ip address	privilege exec level 3 configure terminal
shutdown	privilege exec level 3 configure
serial restart-delay 0	privilege exec level 3 show ip route
!	privilege exec level 3 show ip
interface Serial3/3	privilege exec level 3 show interfaces
no ip address	privilege exec level 3 show
shutdown	!
serial restart-delay 0	line con 0
!	exec-timeout 60 0
router ospf 1	privilege level 15
area 0 authentication message-digest	logging synchronous
network 192.168.2.0 0.0.0.3 area 0	login local
network 192.168.3.0 0.0.0.3 area 0	line aux 0
network 192.168.4.0 0.0.0.3 area 0	exec-timeout 0 0
network 192.168.5.0 0.0.0.3 area 0	privilege level 15
!	logging synchronous
ip forward-protocol nd	line vty 0 4
!	exec-timeout 60 0
!	logging synchronous
no ip http server	login local
no ip http secure-server	transport input ssh
!	!
!	!
!	end
!	
control-plane	
!	

Комутатор SW_2

SW_2

SW_2#show run

Building configuration...

Current configuration : 1704 bytes

!

! Last configuration change at 14:28:14 UTC Sun

Jun 20 2021

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname SW_2

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6

msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

!

!

!

!

!

ip arp inspection vlan 1

no ip icmp rate-limit unreachable

!

ip dhcp excluded-address 193.168.2.1

193.168.2.2

!

ip dhcp pool K

network 193.168.2.0 255.255.255.0

default-router 193.168.2.1

!

!

ip dhcp snooping vlan 1

ip dhcp snooping database disk0_00001_00007

ip dhcp snooping

no ip domain-lookup

ip cef

no ipv6 cef

!

!

errdisable recovery cause arp-inspection

!

spanning-tree mode rapid-pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						65
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
interface Ethernet0/0
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 193.168.2.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

