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: «Проєкт підсистеми захисту клієнт– серверної мережі від атак на Active Directory ОС Windows Server 2019»

Виконав студент 4– го курсу групи КБ– 2
спеціальності 125 «Кібербезпека»
_____ Михайло Ульяніцький
Старший викладач кафедри КІ та КБ
_____ Єлизавета Байлюк
Старший викладач кафедри КІ та КБ
_____ Ігор Фальковський

Житомир – 2023

Державний університет «Житомирська політехніка»

Факультет інформаційно– комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та КБ,
к.т.н., доцент

Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Ульяніцький Михайло Анатолійович

Тема роботи: Проєкт підсистеми захисту клієнт– серверної мережі від атак на Active Directory ОС Windows Server 2019

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 23 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): вихідні дані для роботи;

Обладнання та програмне забезпечення:

1. Топологія мережі.
2. Windows Server 2019 (2)
3. Kali Linux.
4. Windows 10.
5. Windows 7.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О. С.	01.03.2023	01.03.2023
2	Головня О. С.	01.03.2023	01.03.2023
3	Головня О. С.	01.03.2023	01.03.2023

Студент _____ Михайло Ульяніцький

Керівник _____ Єлизавета Байлюк

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023-01.03.2023	Виконано
2	Аналіз теоретичний аспектів клієнт-серверної мережі	04.04.2023-10.03.2023	Виконано
3	Аналіз атак на AD	11.03.2023-18.03.2023	Виконано
4	Аналіз моделі загроз	19.03.2023-29.03.2023	Виконано
5	Проєктування топології клієнт-серверної мережі	01.04.2023-12.04.2023	Виконано
6	Розробка схеми IP-адресації	13.04.2023-17.04.2023	Виконано
7	Вибір мережевого обладення	18.04.2023-21.04.2023	Виконано
8	Налагодження мережевих пристроїв в мережі	22.04.2023-04.05.2023	Виконано
9	Перевірка роботи в мережі	05.05.2023-10.05.2023	Виконано
10	Написання пояснювальної записки	11.05.2023-20.06.2023	Виконано
11	Захист	23.06.2023	Виконано

Студент _____ Михайло Ульяніцький

Керівник _____ Єлизавета Байлюк

АНОТАЦІЯ

Кваліфікаційна робота дипломного проєкту на тему “Проєкт підсистеми захисту клієнт-серверної мережі від атак на Active Directory ОС Windows Server 2019” складається з вступу, трьох розділів, висновки, списку використаної літератури та додатків. Текстова частина викладена на 87 сторінках друкованого тексту. Пояснювальна записка має 9 сторінок додатків. Список використаних джерел містить 16 найменувань і займає 1 сторінку. В роботі наведено 102 рисунків та 4 таблиці. Загальний обсяг роботи – 96 сторінок.

Метою роботи є проведення різних атак на AD, та забезпечити захист від цих атак.

У роботі проаналізовано які є атаки та загрози на AD, як захищатися від цих загроз. Спроектовано загальну топологію мережі, розроблено схему адресації всіх пристроїв мережі з урахуванням розширення, здійснили вибір відповідного проєкту топології обладнання мережі. Побудовано модель загроз. Налаштовано мережу відповідно до проєкту та перевірено правильність функціювання налаштованих протоколів. Проведено Атаку з Kali Linuks на AD, після чого було налаштовано засоби захисту від атак на протоколи мережі.

Ключові слова: ЗАГРОЗА, АТАКА, МЕРЕЖА, КЛІЄНТ, КОРИСТУВАЧ, AD, МОДЕЛЬ, НАЛАГОДЖЕННЯ, ПРОТОКОЛ, KERBEROS.

					КІК.КР.Б – 125 – 15 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Ульяніцький М.А		20.06	Проєкт підсистеми захисту клієнт-серверної мережі від атак на Active Directory ОС Windows Server 2019	Літ.	Арк. 4 / Аркушів
Керівник		Байлюк Є.М.		20.06			
Реценз.		Фальковський І.Г.		20.06		ФІКТ, Гр. КБ-19-2	
Н. контр.							
Затверд.		Єфіменко А.А.		20.06.23			

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 6
ВСТУП 7
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ КЛІЄНТ– СЕРВЕРНОЇ МЕРЕЖІ ВІД АТАК НА ACTIVE DIRECTORY 8
1.1 Принципи роботи клієнт– серверної мережі та її ролі. 8
1.2 Теоретичні аспекти Windows Server 2019 та Active Directory 12
1.3 Різновид атак на AD та протоколи. 18
1.4 Захист AD від атак 26
РОЗДІЛ 2 ТОПОЛОГІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ 31
2.1 Побудова топології мережі 31
2.2 Вибір обладнання 33
2.3 Модель загроз спроєктованої мережі 35
2.4 Побудова моделі загроз клієнт– серверної мережі для атак на Active Directory ОС Windows Server 2019 44
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ КЛІЄНТ– СЕРВЕРНОЇ МЕРЕЖІ. 52
3.1 Налагодження комп'ютерної мережі. 52
3.2 Налагодження Acrive Directory, Windows server 2019 56
3.3 Реалізація атаки AS – REP Roasting на Active Directory та захист від неї. 72
3.4 Реалізація атаки DHCP starvation attack, та DHCP Spoofing на Active Directory та захист від них. 78
ВИСНОВКИ 85
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 86
ДОДАТКИ 87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК – Персональний комп’ютер

IP – Internet Protocol

AD – Active Directory

DHCP – Dynamic Host Configuration Protocol

SSH – Secure Shell

DFS – Distributed File System

SQL – Structured Query Language

СУБД – Система управління базами даних

LAN – Local Area Network

VPN – Virtual Private Network

ЦП – Центральний процесор

SSO – Single Sign– On" (одноразовий вхід)

OU – Organizational Unit" (організаційна одиниця)

KDC – Key Distribution Center" (центр розподілу ключів)

LSA – Local Security Authority" (локальний орган безпеки)

LDAP – Lightweight Directory Access Protocol" (протокол доступу до довідника)

TGS – Ticket– Granting Service" (служба видачі квитків)

SPN – Service Principal Name" (ім'я принципалу служби)

ВСТУП

Актуальність теми. Тема "Проєкт підсистеми захисту клієнт– серверної мережі від атак на Active Directory ОС Windows Server 2019" є дуже актуальною в сучасному світі інформаційних технологій. Active Directory є одним з основних компонентів сучасних корпоративних мереж, і важливо забезпечити його захист від різного роду атак, таких як злом паролів, використання недійсних логінів і багато інших. Коли будуть виконані успішні атаки на Active Directory права доступу до важливих ресурсів можуть порушитись, конфіденційні дані можуть бути викрадені або навіть мережа може бути повністю паралізована. Windows Server 2019 — це остання версія серверної ОС Microsoft, дуже популярна серед корпоративних користувачів. Таким чином, розробка підсистеми безпеки Active Directory на цій ОС є дуже актуальним завданням.

Тому я вважаю, що тема дуже актуальна і може бути корисною для організацій, які використовують Active Directory на базі Windows Server 2019 і хочуть забезпечити найвищий рівень захисту своєї мережі.

Метою кваліфікаційної роботи є розробка системи захисту, щоб забезпечити безпеку та цілісність Active Directory, тому що це одна з основних складових корпоративних мереж.

Встановлена мета створює наступні завдання:

- Виявлення та запобігання атакам на AD, таких як злам пароля, використання недійсних логінів та інші види атак.
- Аналіз діяльності AD, щоб знайти підозрілі дії та вчасно зреагувати на загрози безпеки
- Впровадити політики безпеки, щоб забезпечити високий рівень захисту AD

Об’єктом дослідження є процес налаштування захисту від атак на Active Directory

Предметом дослідження у кваліфікаційній роботі було використано такі методи: проведення атак на AD без захисту, проведення атак на AD з налаштованим захистом від атак.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ВІД АТАК НА ACTIVE DIRECTORY.

1.1 Принципи роботи клієнт– серверної мережі та її ролі.

Робота клієнт мережі

Мережа клієнт– сервер — це мережа, де пристрої є і клієнтами, і серверами. Комп'ютерів у клієнт– серверній мережі може бути так як і пару десятків, так і пару тисяч.

Клієнт– серверну мережу можна визначити, як концепцію комунікаційної інфаструктури, головна частина цих ресурсів, обслуговує своїх клієнтів та зосереджена на серверах. Ця архітектура буде визначати такі категорії елементів:

- асортимент серверів, що надають інформацію та послуги програмам, які звернені до них;
- асортимент клієнтів, що використовують сервіси, та надаються серверами;
- мережа, що забезпечує взаємодію між серверами та клієнтами.

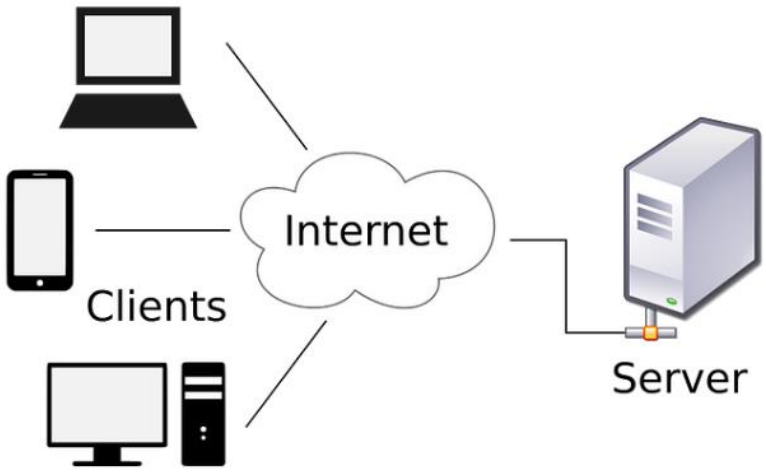


Рисунок 1.1 – Клієнт серверна мережа

Модель клієнт – серверної взаємодії унікальна завдяки підходу до розподілу завдань між серверами та клієнтами, його можна розбити на три рівні функціювання.

- рівень представлення даних, він може являти інтерфейс користувача і буде відповідати за відображення даних користувачем і треба буде вводити для нього керуючі команди;
- Прикладний рівень буде втілювати основну функціональність програмного додатка і виконуватиме саму необхідну обробку інформації.
- рівень управління даними, він буде гарантувати доступ до зберігання даних.

Дволанкова клієнт – серверна архітектура: Передбачається взаємодія двох компонентів програми: клієнтських та серверних модулів. Це може залежати від того, як між ними будуть розподілятися наведені вище функції, розрізняють:

- Модель тонкого клієнта – це модель, в якій вся логіка програми та управління даними централізована на сервері. Клієнтська програма забезпечує лише функціональність рівня представлення;
- Модель товстого клієнта – це модель, в якій сервер лише керує даними, тоді як обробка даними та інтерфейс користувача централізовані на стороні клієнта. Товстими клієнтами також можуть називатися пристрої з обмеженою потужністю, такі як кишенькові комп'ютери та мобільні телефони.

Трьохланкова клієнт – серверна мережа, розділяється інший програмний рівень, на якому створюється прикладна логіка програмного забезпечення. Застосунки проміжного рівня можуть функціонувати під керівництвом спеціальних серверів програмного забезпечення, проте запуск таких застосунків може бути здійснений і під керівництвом стандартного сервера вебдодатків, забезпечуючи гнучкість і альтернативні можливості управління. Тепер управління даними буде здійснюватися сервером даних.

Дволанкова мережа більш простіша, і всі запити забезпечуватимуся одним сервером, але вона буде не така надійна і висуватиме великі вимоги до продуктивності сервера.

Триланкова мережа пропонує більш складну структуру, де функції розподіляються між серверами других та третіх рівнів, що робить цю архітектуру особливо ефективною та прогресивною, вона буде проявляти:

- великий рівень адаптивності та масштабованості.
- висока безпека (такий захист можна вибирати для кожного сервісу та рівня).
- висока продуктивність (таке завдання розподіляють між серверами).

Ролі клієнт-серверної мережі.

Роль сервера визначає його функціональні можливості. Один сервер може виконувати не лише одну, але й декілька ролей одночасно, що надає йому гнучкість та ефективність в розподіленні завдань.

В залежності від ролі, сервісу який надається, будуть розрізнятися такі сервери:

Вебсервер (Web Server)

Сервери приймають HTTP – запити від клієнтів, переважно веббраузерів, і повертають їм відповіді, які часто охоплюють в себе HTML – сторінки, зображення, файли, медіапотоки та інші дані.

Під терміном "вебсервер" розуміють як програму, що забезпечує функціональність вебсервера, так і програмне забезпечення, на якому цей додаток працює.

Користувачі отримують доступ до вебсервера шляхом використання URL – адреси необхідної інтернет сторінки або іншого ресурсу.

*Сервер застосунків (*Application Server*)*

Сервер, який здійснює різні прикладні програми. Термін також відноситься і до програмного продукту, який встановлено на цьому сервері та створює роботу прикладного ПЗ.

Сервери баз даних

Сервери бази даних використовуються для створення запитів на мові SQL. При цьому СУБД буде знаходитись на сервері, до якого підключаються всі додатки клієнтів.

*Файловий сервер (*File Server*)*

Сервер який має доступ до інформації яку зберігає у вигляді файлів і показує користувачам тому файловий сервер здійснює і конкретний рівень захисту від неправомірного доступу.

Сервер друку (*Print Server*)

Сервери друку будуть виконуватися, щоб надати управління доступом до принтерів. Роль друку дає згоду управляти принтерами через інтернет оглядач, друкувати через URL адресу принтера, та використовувати протокол IPP, а також під'єднувати принтери, використовуючи Point and Print.

Поштовий сервер (*Mail Server*)

Поштовий сервер може обслуговувати основні поштові скриньки цих інтернет– користувачів і дозволятиме відправляти та приймати пошту зі сервера. Для того, щоб вхідна пошта могла бути збережена на поштовому сервері та отримана користувачем за допомогою протоколу POP3, вам необхідно мати наступні компоненти: активне підключення до Інтернету, зареєстроване домашнє ім'я та відповідний запис MX у провайдера для вашого поштового домену.

Термінальний сервер (*Terminal Server*)

Сервер, який дає користувачам ресурси для обчислювання (процесорний, пам’ять, простір для зберігання) щоб вирішити завдання. Термінальний сервер це потужний комп’ютер, цей комп’ютер буде під’єднаний до мережі з термінальними клієнтами – у яких є, зазвичай менш потужні або старіші робочі станції або головне рішення для доступу до проміжного сервера. Термінальний сервер надає робочий стіл та служить для віддаленого обслуговування користувача.

Remote Access/VPN Server

Сервери віддаленого управління та VPN забезпечують вхід в мережу для віддалених користувачів. Вибираючи роль Remote Access / VPN Server, ми можемо зробити механізми маршрутизації для середовищ LAN і WAN. Ця роль забезпечує можливість підключення через модем і VPN через інтернет.

DNS Server

Служба DNS забезпечує процес перетворення доменних імен на відповідні IP – адреси.

DHCP Server

Сервер DHCP дає дозвіл клієнтам, щоб вони отримували свій IP – адрес якщо їм це потрібно. Сервер DHCP також надаватиме додаткову інформацію для конфігурації мережі – адреса серверів DNS, WINS і інших

Streaming Media Server

Використовуються для керування та передачі мультимедійного змісту. потокового відео та аудіо – за допомогою локальної мережі або глобальної мережі.

Ігровий сервер (G*ame server*)

Сервер, що має зв'язок між різними клієнтами, дає їм можливість взаємодіяти між собою у межах програмного інтерфейсу конкретної гри.[1]

1.2 Теоретичні аспекти Windows Server 2019 та Active Directory

Windows Server 2019 – це серверна операційна система, розроблена корпорацією Майкрософт як частина сімейства операційних систем Windows NT. Ось деяка загальна інформація про Windows Server 2019:

Функції: Windows Server 2019 пропонує різноманітні функції та вдосконалення, зокрема покращену безпеку, покращену продуктивність, можливості гібридної хмари та розширені інструменти керування.

Параметри інсталяції: Windows Server 2019 пропонує різні варіанти інсталяції, як – от Server Core, Nano Server і Desktop Experience. Кожен варіант має свої переваги та підходить для конкретних сценаріїв.

Системні вимоги: Windows Server 2019 має певні системні вимоги, зокрема вимоги до ЦП, пам'яті, дискового простору та мережі. Важливо переконатися, що ваше обладнання відповідає цим вимогам для оптимальної продуктивності.

Версії: Windows Server 2019 доступна в різних версіях, зокрема Standard, Datacenter і Essentials. Кожен випуск має різні функції та варіанти ліцензування, щоб задовольнити потреби різних організацій.

Ролі та функції: Windows Server 2019 підтримує різні ролі та функції, які можна встановити та налаштувати відповідно до конкретних вимог до сервера. До них належать Active Directory, DNS, DHCP, служби файлів і зберігання, вебсервер (IIS), Hyper – V та багато інших.

Інструменти керування: Windows Server 2019 надає низку інструментів керування, таких як Windows Admin Center (раніше Project Honolulu), PowerShell і Server Manager, щоб спростити адміністрування сервера та завдання налаштування.

Сумісність: важливо перевірити сумісність ваших програм і апаратного забезпечення з Windows Server 2019 перед його оновленням або розгортанням. Деякі старі програми можуть вимагати оновлення або бути несумісними з останньою версією операційної системи.[10]

Що таке Active Directory і як він працює?

Active Directory (AD) – це власна служба каталогів Microsoft. Він працює на Windows Server і дозволяє адміністраторам керувати дозволами та доступом до мережевих ресурсів.

Active Directory зберігає дані як об’єкти. Об’єкт – це окремий елемент, наприклад користувач, група, програма або пристрій, наприклад принтер.

Зазвичай об’єкти визначаються як ресурси, наприклад принтери чи комп’ютери, або принципали безпеки, наприклад користувачі чи групи.

Active Directory класифікує об’єкти каталогу за назвою та атрибутами. Наприклад, ім’я користувача може включати рядок імені разом з інформацією, пов’язаною з користувачем, такою як паролі та ключі Secure Shell.

Основною службою в Active Directory є служби домену (AD DS), які зберігають інформацію каталогу та обробляють взаємодію користувача з доменом. AD DS перевіряє доступ, коли користувач входить на пристрій або намагається під’єднатися до сервера через мережу. AD DS контролює, які

користувачі мають доступ до кожного ресурсу, а також групові політики. Наприклад, адміністратор зазвичай має інший рівень доступу до даних, ніж кінцевий користувач.

Інші продукти операційної системи (ОС) Microsoft і Windows, такі як Exchange Server і SharePoint Server, покладаються на AD DS для надання доступу до ресурсів. Сервер, на якому розміщено AD DS, є контролером домену.



Рисунок 1.2 – Windows Server 2019

Служби Active Directory

До складу Active Directory входить кілька різних служб. Основною службою є служби домену, але Active Directory також включає служби полегшених каталогів (AD LDS), протокол доступу до спрощених каталогів (LDAP), служби сертифікатів або AD CS, служби федерації (AD FS) і служби керування правами (AD RMS). Кожна з цих інших служб розширює можливості продукту щодо керування такими каталогами:

- Полегшені служби каталогів мають ту саму кодову базу, що й AD DS, зі схожими функціями, як – от інтерфейс прикладної програми. Однак AD LDS може працювати в кількох екземплярах на одному сервері та зберігає дані каталогу в сховищі даних за допомогою полегшеного протоколу доступу до каталогу.
- Lightweight Directory Access Protocol – це прикладний протокол, який використовується для доступу та підтримки служб каталогів у мережі. LDAP

зберігає такі об’єкти, як імена користувачів і паролі, у службах каталогів, таких як Active Directory, і ділиться даними цих об’єктів у мережі.

- Служби сертифікації створюють, керують і надають спільний доступ до сертифікатів. Сертифікат використовує шифрування, щоб дозволити користувачеві безпечно обмінюватися інформацією через Інтернет за допомогою відкритого ключа.
- Служби об’єднання Active Directory автентифікують доступ користувачів до кількох програм – навіть у різних мережах – за допомогою єдиного входу (SSO). Як видно з назви, SSO вимагає від користувача лише одного входу, а не використання кількох спеціальних ключів автентифікації для кожної служби.
- Служби керування правами контролюють права на інформацію та керування нею. AD RMS шифрує вміст, наприклад електронну пошту або документи Microsoft Word, на сервері, щоб обмежити доступ

Основні функції доменних служб Active Directory

Доменні служби Active Directory використовують багаторівневу структуру макета, що складається з доменів, дерев і лісів для координації мережевих елементів.

Домени є найменшими з основних ярусів, тоді як ліси є найбільшими. Різні об’єкти, наприклад користувачі та пристрої, які спільно використовують ту саму базу даних, будуть в одному домені. Дерево – це один або кілька доменів, згрупованих разом за допомогою ієрархічних довірчих відносин. Ліс – це група з кількох дерев. Ліси забезпечують межі безпеки, тоді як доменами, які мають спільну базу даних, можна керувати такими параметрами, як автентифікація та шифрування.

- Домен – це група об’єктів, наприклад користувачів або пристроїв, які спільно використовують ту саму базу даних AD. Домени мають систему доменних імен

- Дерево – це один або кілька доменів, згрупованих разом. Деревоподібна структура використовує безперервний простір імен, щоб зібрати колекцію доменів у логічну ієрархію. Дерева можна розглядати як довірчі відносини, де безпечне з'єднання, або довіра, поділяється між двома доменами. Декільком доменам можна довіряти, де один домен може довіряти другому, а другий – третьому. Через ієрархічний характер цієї настройки перший домен може неявно довіряти третьому домену, не потребуючи явної довіри.
- Ліс – це група з кількох дерев. Ліс складається зі спільних каталогів, схем каталогів, інформації про програми та конфігурацій домену. Схема визначає клас і атрибути об'єкта в лісі. Крім того, сервери глобального каталогу надають перелік усіх об'єктів у лісі. За словами Microsoft, ліс є кордоном безпеки Active Directory.
- Організаційні підрозділи (OU) організовують користувачів, групи та пристрої. Кожен домен може містити власний OU. Однак OU не можуть мати окремі простори імен, оскільки кожен користувач або об'єкт у домені має бути унікальним. Наприклад, не можна створити обліковий запис користувача з тим самим іменем користувача.
- Контейнери подібні до OU, але об'єкти групової політики не можна застосовувати або пов'язувати з об'єктами – контейнерами.

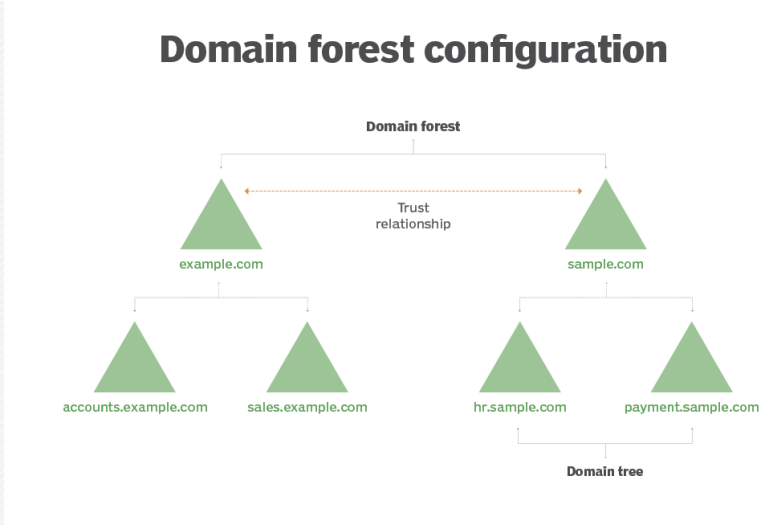


Рисунок 1.3 – Конфігурація лісу доменів

‘*Trusting terminology*

Active Directory покладається на довірі для модерування прав доступу до ресурсів між доменами. Існує кілька різних типів трастів:

- Одностороння довіра – це коли перший домен надає привілеї доступу користувачам другого домену. Однак другий домен не надає доступу користувачам першого домену.
- Двостороння довіра – це коли є два домени, і кожен домен надає доступ користувачам іншого домену.
- Довірений домен – це один домен, який надає користувачам доступ до іншого домену, який називається довірчим доменом.
- Перехідна довіра може виходити за межі двох доменів і надавати доступ до інших довірених доменів у лісі.
- Неперехідна довіра – це одностороння довіра, яка обмежена двома доменами.
- Явна довіра – це одностороння неперехідна довіра, створена адміністратором мережі.
- Перехресна довіра є типом явної довіри. Перехресні зв’язки довіри відбуваються між доменами в межах 1) одного дерева, без зв’язку «дочірньо – батьківський» між двома доменами, або 2) різних дерев.
- Довіра до лісу застосовується до доменів у всьому лісі та може бути односторонньою, двосторонньою або транзитивною.
- Ярлик поєднує два домени, які належать до окремих дерев. Ярлики можуть бути односторонніми, двосторонніми або транзитивними.
- Сфера – це транзитивний, неперехідний, односторонній або двосторонній траст.
- Зовнішня довіра – це довіра, яка зв’язує домени через окремі ліси або домени, які не є AD. Зовнішні трасти можуть бути нетранзитивними, односторонніми або двосторонніми.

- Довіра приватного керування доступом (PAM) – це одностороння довіра, створена Microsoft Identity Manager між виробничим лісом і бастіонним лісом.

Домени проти робочих груп

Робоча група – це термін Microsoft для машин Windows, підключених через однорангову мережу. Робочі групи є ще однією одиницею організації комп'ютерів Windows у мережах. Робочі групи дозволяють цим машинам обмінюватися файлами, доступом до Інтернету, принтерами та іншими ресурсами через мережу. Однорангова мережа усуває потребу в сервері для автентифікації. Існує кілька відмінностей між доменами та робочими групами:

Домени, на відміну від робочих груп, можуть розміщувати комп'ютери з різних локальних мереж.

Домени можна використовувати для розміщення набагато більшої кількості комп'ютерів, ніж робочих груп. Домени можуть включати тисячі комп'ютерів, на відміну від робочих груп, верхня межа яких зазвичай становить близько 20.

У доменах принаймні один сервер є комп'ютером, який використовується для керування дозволами та функціями безпеки для кожного комп'ютера в домені. У робочих групах немає сервера, і всі комп'ютери є рівноправними.

Користувачам домену зазвичай потрібні ідентифікатори безпеки, такі як логіни та паролі, на відміну від робочих груп.[2]

1.3 Різновид атак на AD та протоколи.

Протокол Kerberos:

Kerberos – це протокол мережевої автентифікації, який забезпечує безпечну автентифікацію для програм клієнт/сервер у розподіленому мережевому середовищі. Ось деяка інформація про протокол Kerberos:

- Автентифікація: Kerberos в основному використовується для автентифікації користувачів і служб у мережі. Це дозволяє клієнтам підтверджувати свою особу серверам, а серверам – автентифікувати себе клієнтам.

- Система на основі квитків: Kerberos використовує систему на основі квитків для автентифікації. Коли користувач входить у клієнтську машину, клієнт запитує квиток, відомий як Ticket Granting Ticket (TGT), у Центрі розповсюдження ключів Kerberos (KDC). Потім TGT використовується для запиту сервісних квитків для доступу до певних ресурсів.
- Центр розподілу ключів (KDC): KDC є центральним компонентом інфраструктури Kerberos. Він складається з двох основних частин: сервера автентифікації (AS) і сервера надання квитків (TGS). AS перевіряє особу користувача та видає TGT, тоді як TGS видає сервісні квитки для доступу до певних послуг.
- Процес автентифікації. Процес автентифікації Kerberos включає такі кроки:

a. Автентифікація користувача: користувач надає свої облікові дані клієнтській машині, яка пересилає запит до KDC для перевірки.

b. Запит TGT: KDC перевіряє облікові дані користувача та видає TGT, якщо автентифікація пройшла успішно.

c. Запит на квиток служби: коли користувач хоче отримати доступ до певної послуги, клієнт запитує квиток на послугу від KDC, надаючи TGT.

d. Перевірка сервісного квитка: KDC перевіряє TGT і видає сервісний квиток, зашифрований сеансовим ключем.

e. Автентифікація служби: клієнт представляє квиток служби сервера, який розшифровує його за допомогою ключа сеансу та перевіряє особу клієнта.

- Шифрування та ключі: Kerberos використовує симетричне шифрування для захисту зв’язку між клієнтами та серверами. Він покладається на спільні секретні ключі: пароль користувача (відомий лише користувачу) і секретні ключі, що зберігаються в KDC.
- Термін дії та поновлення квитка: квитки Kerberos мають обмежений термін дії. Клієнти та служби можуть подати запит на оновлення квитка або отримати нові квитки, використовуючи наявні квитки та KDC.

- Міждоменна автентифікація: Kerberos підтримує міждоменну автентифікацію, що дозволяє користувачам з різних областей (доменів) Kerberos автентифікуватись і отримувати доступ до ресурсів в інших сферах.
- Інтеграція з програмами: Kerberos можна інтегрувати в різні програми, такі як веббраузери, клієнти електронної пошти, файлові сервери та мережеві служби, щоб забезпечити безпечну автентифікацію та можливості єдиного входу.

Kerberos широко використовується в корпоративних середовищах для забезпечення безпечної автентифікації та захисту мережевих ресурсів. Він забезпечує надійну та надійну структуру для автентифікації користувачів і підтримує взаємодію між різними платформами та операційними системами.[3]

Види атак на Active Directory

1. Kerberoasting

Kerberos широко використовується в корпоративних середовищах для забезпечення безпечної автентифікації та захисту мережевих ресурсів. Він забезпечує надійну та надійну структуру для автентифікації користувачів і підтримує взаємодію між різними платформами та операційними системами



Рисунок 1.4 –Локотип Kerberos

2. Password Spraying (розпилення пароля)

Тут зловмисник використовує список раніше зламаних паролів і хешів, щоб грубою силою проникнути в обліковий запис. Оскільки більшість систем

автентифікації блокують користувачів після кількох невдалих спроб входу, зловмисник пробуватиме різні комбінації імен користувачів, доки не знайде збіг. Природно, доцільно переконатися, що співробітники використовують складні паролі, і, де це можливо, використовувати багатофакторну автентифікацію, щоб запобігти атакам з використанням пароля. Рішення, яке також зберігає список раніше зламаних паролів і хешів, також може бути ефективним у виявленні аномальних спроб входу.[15]



Рисунок 1.5 – Зловмисник пробує увійти в аккаунти

3. Local Loop Multicast Name Resolution (LLMNR) – це мережева функція Windows, яка ставить під загрозу Active Directory. LLMNR дозволяє розпізнавати імена без DNS – сервера. Багатоадресні пакети транслюються в мережу, запитуючи IP – адресу заданого імені хоста. Зловмисники можуть перехопити ці пакети та стверджувати, що IP – адреса пов’язана з іменем хоста. Ця функція не потрібна, якщо систему доменних імен (DNS) налаштовано належним чином. Таким чином, найкращим способом пом’якшити цю загрозу було б просто повністю вимкнути LLMNR.

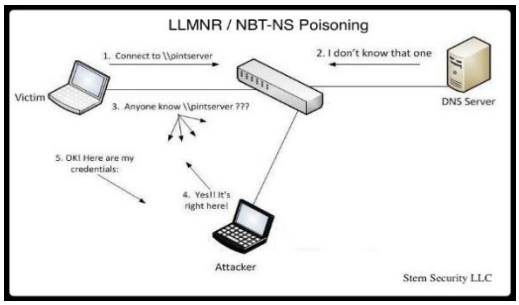


Рисунок 1.6 – Link– Local багатоадресна розсилка

4.Pass– the– hash with Mimikatz

Pass–the–hash – це техніка, яка використовується для викрадення облікових даних з Active Directory, а також сприяє боковому переміщенню в середовищі. Зловмисники використовують інструмент під назвою Mimikatz, який використовує протокол автентифікації NTLM, щоб видавати себе за користувача та скидати хеші облікових даних із пам'яті. Організації повинні гарантувати, що хеші привілейованих облікових записів не зберігаються в місці, де їх можна легко видобути. Їм також слід увімкнути захист LSA та використовувати режим обмеженого адміністратора для віддалених робочих столів.



Рисунок 1.7 – Pass The Hash

5. Default Credentials

Компанії часто забувають змінити стандартні паролі на пристроях/системах, і зловмисники шукатимуть ці пристрої/системи, щоб зламати вашу мережу. Організації повинні переконатися, що вони змінюють паролі за замовчуванням і ведуть актуальну інвентаризацію всього мережевого обладнання. Можливо, також варто прийняти рішення, яке створює випадкові паролі для бізнес – користувачів і пристроїв.



Рисунок 1.8 – Облікові дані за замовчуванням

6. Hard– coded Credentials

У деяких випадках розробники програмного забезпечення жорстко кодують облікові дані в сценарії, що, очевидно, становить загрозу безпеці, особливо якщо облікові дані надають привілейований доступ. Можливо, розробники жорстко закодували облікові дані, щоб перевірити функціональність сценарію, а потім забули їх видалити. Незалежно від причини зловмисники намагатимуться знайти сценарії, які містять жорстко закодовані облікові дані, якими вони можуть скористатися. Адміністратори повинні уважно стежити за всіма обліковими записами користувачів, щоб переконатися, що вони використовуються за призначенням.

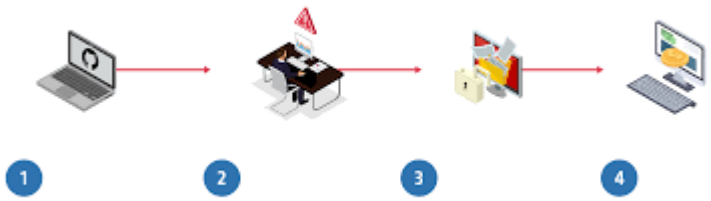


Рисунок 1.9 – Жорстко закодовані облікові дані

7. Privilege Escalation

Кіберзлочинці, як правило, намагаються отримати доступ до стандартного облікового запису користувача, використовуючи неправильні методи введення

пароля. Отримавши доступ, вони спробують підвищити свої привілеї за допомогою соціальної інженерії, використання вразливостей програмного/апаратного забезпечення, неправильних налаштувань, встановлення шкідливого програмного забезпечення тощо. Організації повинні підтримувати актуальну інвентаризацію того, які облікові записи мають доступ до ресурсів, особливо критичних. Облікові записи повинні мати найменші привілеї, необхідні для виконання своєї ролі, і вся діяльність привілейованого облікового запису повинна постійно контролюватися, надсилаючи сповіщення в режимі реального часу адміністратору.

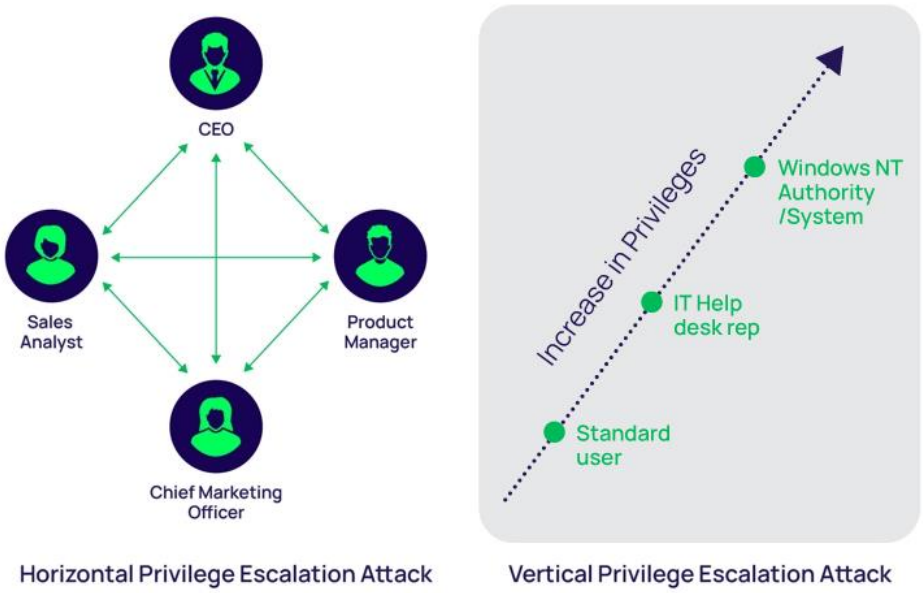


Рисунок 1.10 – Підвищення привілеїв

8. LDAP Reconnaissance

Зловмисники, які вже отримали доступ до вашого середовища Active Directory, можуть використовувати запити LDAP для збору додаткової інформації про середовище. Використовуючи цей метод, вони можуть виявити користувачів, групи та комп'ютери, що допоможе їм спланувати свій наступний крок. Запобігти розвідці LDAP складно, оскільки більшість інформації в Active Directory доступна всім користувачам за замовчуванням. Таким чином, вам

потрібно буде уважно стежити за трафіком LDAP на наявність аномалій і переконатися, що всім обліковим записам надано найменший доступ, необхідний для виконання своїх ролей.

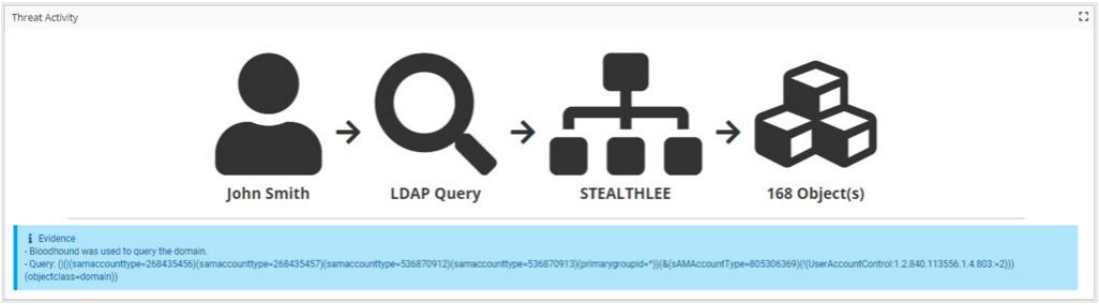


Рисунок 1.11 – Розвідка LDAP

9. BloodHound Reconnaissance

BloodHound – це інструмент, який допомагає зловмисникам ідентифікувати та візуалізувати шляхи атак у середовищах Active Directory. Інструмент працює, створюючи карту того, які комп'ютери доступні для яких користувачів, і які облікові дані користувача можна вкрасти з пам'яті. Організації також можуть використовувати BloodHound, щоб допомогти їм виявити та усунути вразливості у своєму середовищі, а також надати змістовну інформацію про те, як призначити належний рівень доступу для користувачів.[14]



Рисунок 1.12 – Розвідка BloodHound

10. NTDS.dit Extraction

Контролери домену зберігають усі дані Active Directory у файлі під назвою ntds.dit або «dit», як його називають деякі. За замовчуванням цей файл знаходиться за таким шляхом: C:\Windows\NTDS\. Якщо зловмисник отримує доступ до Active Directory, він може отримати доступ до файлу ntds.dit або скомпрометувати рішення організації для резервного копіювання та витягти файл ntds.dit із резервної копії. Щоб запобігти зловмисникам вилучення файлу ntds.dit, вам слід мінімізувати кількість облікових записів, які можуть входити до контролерів домену, контролювати доступ до фізичних комп'ютерів контролерів домену та вжити всіх необхідних заходів для посилення середовища Active Directory.[4]

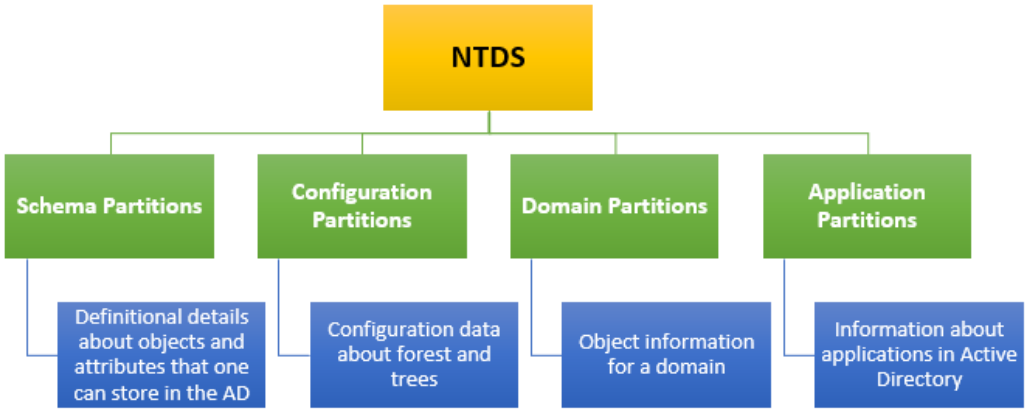


Рисунок 1.13 – Видобуток NTDS.dit

1.4 Захист AD від атак

Захист Active Directory від атак має вирішальне значення для підтримки безпеки та цілісності вашого мережевого середовища. Нижче наведено кілька ключових заходів для підвищення безпеки Active Directory:

- Регулярні виправлення та оновлення: оновлюйте сервери Active Directory і допоміжні системи за допомогою останніх виправлень безпеки та оновлень. Це допомагає усунути вразливості та захистити від відомих проблем безпеки.

- Політики безпечної автентифікації: впроваджуйте політики надійних паролів і багатофакторну автентифікацію (MFA) для облікових записів користувачів. Заохочуйте використання складних паролів і регулярно змінюйте їх. MFA додає додатковий рівень безпеки, вимагаючи додаткових кроків перевірки, окрім просто пароля.
- Керування привілейованим доступом (PAM): реалізуйте модель найменших привілеїв і обмежте адміністративний доступ лише авторизованим особам, яким це потрібно. Використовуйте такі інструменти, як модель адміністративного рівня Active Directory і робочі станції привілейованого доступу (PAW), щоб захистити привілейовані облікові записи та запобігти несанкціонованому доступу.
- Безпечні периметри мережі: захистіть периметр мережі за допомогою брандмауерів, систем виявлення та запобігання вторгненням (IDPS) і віртуальних приватних мереж (VPN). Ці заходи допомагають відстежувати та контролювати вхідний і вихідний трафік, гарантуючи, що надається лише авторизований доступ.
- Моніторинг і аудит безпеки: увімкніть аудит безпеки в Active Directory, щоб відстежувати та контролювати зміни, внесені в об’єкти, політики безпеки та дії користувачів. Регулярно переглядайте та аналізуйте журнали безпеки, щоб виявляти будь – які підозрілі дії чи потенційні порушення безпеки та реагувати на них.
- Регулярне резервне копіювання та відновлення: запровадьте комплексну стратегію резервного копіювання та відновлення для Active Directory. Регулярно створюйте резервні копії бази даних Active Directory, стану системи та важливої конфігураційної інформації. Періодично тестуйте процес відновлення, щоб переконатися в можливості відновлення в разі втрати даних або зламу системи.
- Безпечна реплікація та довірчі відносини: захистіть трафік реплікації між контролерами домену за допомогою таких технологій, як IPsec, і налаштуйте безпечні довірчі відносини із зовнішніми доменами або лісами.

- Виявлення та запобігання вторгненням: розгортайте системи виявлення та запобігання вторгненням (IDPS) для моніторингу мережевого трафіку, виявлення та запобігання спробам неавторизованого доступу та підозрілим діям, націленим на Active Directory.
- Навчання та обізнаність співробітників: навчайте співробітників найкращим методам безпеки, таким як уникнення підозрілих електронних листів, дотримання гігієни паролів і пильність проти атак соціальної інженерії. Регулярне навчання з питань безпеки допомагає посилити важливість безпеки та зменшує ймовірність успішних атак.

- Регулярні оцінки безпеки: проводите регулярні оцінки безпеки, сканування вразливостей і тести на проникнення, щоб виявити та усунути будь – які слабкі місця або вразливості в інфраструктурі Active Directory.

Важливо зазначити, що захист Active Directory – це постійний процес, який потребує поєднання технічних заходів, політик безпеки та обізнаності користувачів. Регулярний моніторинг, профілактичне обслуговування та своєчасне реагування на інциденти безпеки є ключовими для підтримки безпечного середовища Active Directory.[11]

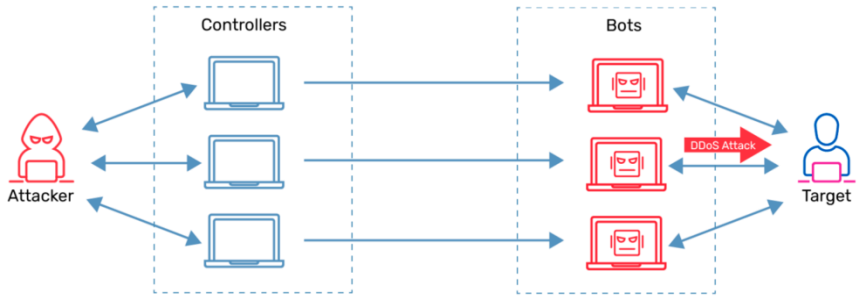


Рисунок 1.14 – Захист від атаки

Методи атак на Kerberos

Kerberos, як і будь – який інший протокол автентифікації, не захищений від атак. Зловмисники можуть спробувати різними способами використати вразливі місця в протоколі Kerberos і поставити під загрозу його безпеку. Ось деякі поширені методи атаки, націлені на Kerberos:

- Вгадування пароля/атаки грубою силою: зловмисники можуть намагатися вгадати або систематично пробувати різні паролі, щоб отримати неавторизований доступ до облікових записів користувачів. Слабкі паролі або паролі, які легко вгадати, більш сприйнятливі до таких атак. Застосування політики надійних паролів і механізмів блокування облікових записів може допомогти зменшити цей ризик.
- Перехоплення квитків Kerberos: зловмисники можуть перехоплювати квитки Kerberos, якими обмінюються клієнти та сервери, щоб виконувати офлайн – атаки. Вони можуть аналізувати захоплені квитки та намагатися зламати шифрування, яке використовується для отримання сеансового ключа квитка. Захист мережі від несанкціонованого перехоплення пакетів і впровадження механізмів шифрування можуть допомогти запобігти цій атаці.
- Підробка служби надання квитків Kerberos (TGS): ця атака передбачає перехоплення зв’язку між клієнтом і TGS для отримання неавторизованого доступу до ресурсів. Шляхом підробки або підробки відповіді TGS зловмисник може отримати сервісні квитки для доступу до захищених сервісів. Впровадження захищених каналів зв’язку та використання цифрових підписів або шифрування може допомогти виявити та запобігти такому типу атак.
- Атаки Pass– the– Hash: у цій атаці зловмисник захоплює хешований пароль із скомпрометованої системи та використовує його для автентифікації як законного користувача без необхідності знати справжній пароль. Впровадження надійних алгоритмів хешування паролів і регулярне оновлення систем може ускладнити зловмисникам використання хешованих паролів.
- Атаки Kerberos Golden Ticket/Silver Ticket: ці розширені атаки передбачають отримання та підробку квитків Kerberos із привілеями високого рівня. Зловмисники отримують доступ до бази даних центру розповсюдження ключів Kerberos (KDC) або використовують уразливості в контролері домену для створення шкідливих квитків. Впровадження суворого контролю доступу,

регулярний моніторинг і перевірка привілейованих облікових записів, а також виявлення незвичних запитів на квитки можуть допомогти запобігти цим атакам.

- Kerberoasting: під час цієї атаки зловмисник націлює на облікові записи служб з іменами учасників служб Kerberos (SPN) і намагається отримати зашифрований пароль облікового запису служби з квитка Kerberos. Слабкі паролі або паролі облікових записів, які легко зламати, особливо вразливі до цієї атаки. Застосування надійних паролів облікових записів служби та моніторинг незвичних запитів на квитки може допомогти зменшити цей ризик.
- Атаки на відмову в обслуговуванні (DoS): зловмисники можуть спробувати перевантажити інфраструктуру Kerberos потоком запитів, спричиняючи збої в обслуговуванні та відмову в обслуговуванні. Впровадження заходів безпеки мережі, моніторинг трафіку та обмеження швидкості може допомогти захистити від атак DoS.

Щоб пом’якшити ці атаки, важливо впровадити комплексну стратегію безпеки, яка включає надійні механізми автентифікації, захищену мережеву інфраструктуру, регулярний моніторинг і аудит, а також навчання для підвищення обізнаності користувачів. Регулярне оновлення та виправлення систем, а також дотримання найкращих практик і рекомендацій експертів з документації та безпеки Kerberos можуть значно підвищити безпеку вашого середовища Kerberos.[13]

Висновки до першого розділу

У цьому розділі було розглянуто як працює клієнт – серверна мережа, розглянуто що таке Windows server 2019 та як правильно працює Active Directory. Було розглянуто що таке протокол Kerberos, та проаналізовано які бувають атаки та методи на AD, також було розглянуто як захищатись від атак на Active Directory.

РОЗДІЛ 2 ТОПОЛОГІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Побудова топології мережі

У цій роботі було розглянуто клієнт– серверну мережу, в якій буде використано основний та резервний сервер Windows Server 2019 .Робочі станції будуть підключені до комутаторів SW – 1 і SW – 2, також в цій мережі підключений роутер та інтернет, на мережевих пристроях налаштований ntp server, та syslog, на Windows Server буде налаштовано AD, DHCP server, та DNS server, також буде налаштований захист від атак, також при проектуванні я використав трьохрівневу модель мережі. Ця модель має ієрархічну структуру і передбачає, що мережа ма є три залежних один від одного рівні, це рівень ядра, рівень розподілу та рівень доступу, ця мережа представлена на рисунку нижче.

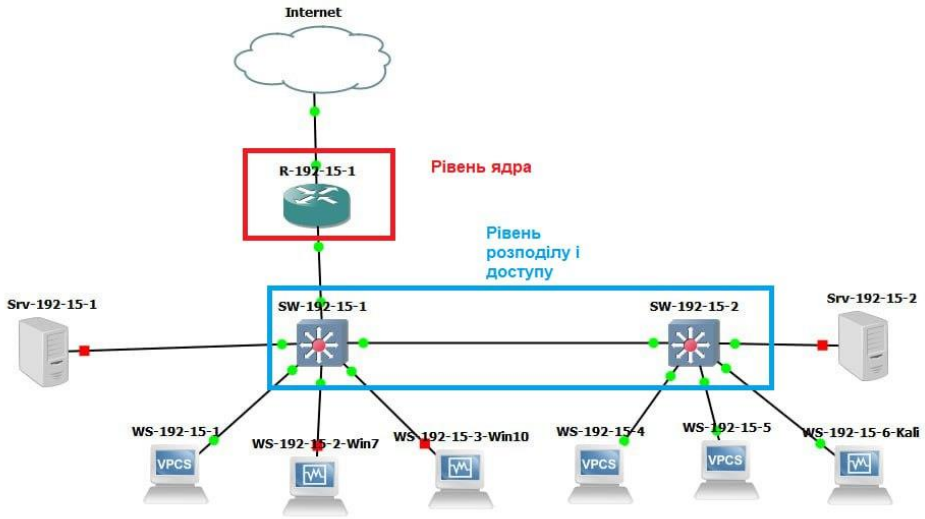


Рисунок 2.1 – Загальна топологія мережі

Рівень ядра складається з 1 маршрутизатора, він з'єднаний між собою канальними зв'язками технології Fast Ethernet.

Рівень розподілу та доступу має 2 комутатори, що під'єднані до ядра мережі. З'єднання до ядра використано за допомогою технології Ethernet.

У таблиці 2.1 буде наведено топологію підключень всієї топології мережі.

Для зв'язку між R – 1 та Intrnet було використано дві адреси з мережі: 202.192.15.0/30

Для локальної мережі буде залучено 1 адресу: 192.192.15.0/24

Таблиця 2.1 – Параметри підключення пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейса
Internet	Eth 1/0	Маршутизатор R– 192– 15– 1	Eth 1/0
R– 192– 15– 1	Eth 1/1	Комутатор SW– 192– 15– 1	Eth 0/1
SW– 192– 15– 1	Eth 0/0	Server Srv– 192– 15– 1	Eth 0
SW– 192– 15– 1	Eth 0/2	Комп’ютер WS– 192– 15– 1	Eth 0
SW– 192– 15– 1	Eth 0/3	Комп’ютер WS– 192– 15– 2– Win7	Eth 0
SW– 192– 15– 1	Eth 1/0	Комп’ютер WS– 192– 15– 3– Win10	Eth 0
SW– 192– 15– 1	Eth 1/1	Комутатор SW– 192– 15– 2	Eth 0/0
SW– 192– 15– 2	Eth 0/1	Комп’ютер WS– 192– 15– 4	Eth 0
SW– 192– 15– 2	Eth 0/2	Комп’ютер WS– 192– 15– 5	Eth 0
SW– 192– 15– 2	Eth 1/0	Комп’ютер WS– 192– 15– 6– Kali	Eth 0
SW– 192– 15– 2	Eth 0/3	Server Srv– 192– 15– 2	Eth 0

Здійсню розподіл адрес для локальних мереж. Для зручності результат наведений в таблиці 2.2.

Таблиця 2.2 – Адресація локальної мережі.

Призначення адрес	IP– address
Адреса мережі	192.192.15.0

Продовження табл. 2.2 – Адресація локальної мережі.

Призначення адрес	IP– address
Маска мережі	255.255.255.0(/24)
Мінімальна адреса	192.192.15.1
Шлюз за замовчуванню (1)	192.192.15.254
Призначені Windows Server (2)	192.192.15.250 – 192.192.15.251
Призначені комутаторам (2)	192.192.15.252 – 192.192.15.253
Діапазон адрес майбутніх пристроїв (40)	192.192.15.1 – 192.192.15.35
Діапазон вільних адрес (209)	192.192.15.36 – 192.192.15.243

2.2 Вибір обладнання

Мережа розроблена на обладнані Cisco. Нижче я навів характеристики обладання Cisco, що буде використано в мережі.

1. Високопродуктивний мережевий маршрутизатор Cisco C7200 із набором функцій adventerprisek9

Маршрутизатор Cisco C7200 із набором функцій adventerprisek9 – це високопродуктивний мережевий пристрій, розроблений для мереж корпоративного рівня та потреб у маршрутизації. Він належить до маршрутизаторів серії Cisco 7200, які відомі своєю масштабованістю та розширеними функціями.

Маршрутизатор Cisco C7200 adventerprisek9 пропонує надійні можливості маршрутизації та підтримує різні протоколи, такі як OSPF, BGP, EIGRP, MPLS тощо. Він оснащений вдосконаленими апаратними компонентами для обробки високого мережевого трафіку та забезпечення надійного підключення.

Завдяки набору функцій adventerprisek9 цей маршрутизатор включає розширені функції безпеки, такі як підтримка VPN, розширені можливості брандмауера та механізми шифрування для забезпечення конфіденційності та цілісності мережевого трафіку. Він також надає широкі можливості керування та

моніторингу, дозволяючи адміністраторам ефективно керувати мережею та усувати несправності.

Маршрутизатор Cisco C7200 adventerprisek9 зазвичай використовується у великих корпоративних мережах, середовищах постачальників послуг і центрах обробки даних, де висока продуктивність маршрутизації, масштабованість і безпека є важливими. Він розроблений відповідно до високих вимог сучасних мереж і може працювати з широким спектром мережевих програм і послуг.

Загалом маршрутизатор Cisco C7200 adventerprisek9 є надійним і потужним мережевим пристроєм, який пропонує розширені функції та продуктивність для мережевої інфраструктури корпоративного рівня.[5]



Рисунок 2.2 – Високопродуктивний мережевий маршутизатор Cisco C7200

Таблиця 2.3 – Харахтеристика маршутизатора cisco c7200 adventerpricek9

Інтерфейси	Загальна інформація
Стандартна пам'ять	1 Gb
Максимальна пам'ять:	2 Gb
Технологія пам'яті	SDRAM
Флеш– пам'ять	64 Mb
Підтримується карта пам'яті	CompactFlash (CF) Card

2. Комутатор cisco IBM2498– B40

IBM2498 – B40 – це модель комутатора IBM SAN (Storage Area Network). Він розроблений, щоб забезпечити підключення та можливості керування пристроями зберігання даних у середовищі SAN. Комутатор IBM2498 – B40 пропонує певну кількість портів, зазвичай 24 або 40, для підключення масивів зберігання, серверів та інших компонентів SAN.

Будучи комутатором SAN, IBM2498 – B40 забезпечує передачу даних між пристроями зберігання даних і серверами, забезпечуючи централізоване керування сховищем і покращений доступ до даних і доступність. Він підтримує різні протоколи, наприклад Fibre Channel, який зазвичай використовується в середовищах SAN.

Комутатор IBM2498 – B40 зазвичай розгортається в інфраструктурах зберігання корпоративного рівня, центрах обробки даних і середовищах, де потрібна високопродуктивна та надійна мережа зберігання даних. Він надає такі функції, як зонування, що дозволяє логічно розділити ресурси зберігання, і керування структурою для ефективної конфігурації та моніторингу SAN.[12]

SERVAK



Рисунок 2.3 – Комутатор IBM2498– B40

2.3 Модель загроз спроєктованої мережі

Вплив моделі загроз на клієнт – серверну мережу:

Моделі загроз впливають на клієнт– серверну мережу шляхом ідентифікації потенційних загроз і ризиків, які можуть виникнути в процесі

обміну даними між клієнтами та серверами. Такі моделі допомагають оцінити вразливості системи, ідентифікувати потенційні атаки та розробити відповідні заходи безпеки. Ось кілька способів, якими моделі загроз можуть впливати на клієнт – серверну мережу:

- Оцінка ризиків, загрози допомагають визначити потенційні ризики та вразливі місця в мережі клієнт – сервер. Аналізуючи різні вектори атак і потенційні загрози, організації можуть оцінити рівень ризику, пов'язаного з їх мережевою інфраструктурою, і відповідно визначити пріоритети заходів безпеки.
- Засоби керування безпекою: моделі загроз дають змогу зрозуміти потенційні точки входу та слабкі зв'язки в мережі клієнт – сервер. Ця інформація дозволяє організаціям впроваджувати відповідні засоби контролю безпеки та заходи для пом'якшення виявлених ризиків. Наприклад, впровадження надійних механізмів автентифікації, сегментації мережі, шифрування, систем виявлення вторгнень і брандмауерів може допомогти захистити мережу від різних загроз.
- Реагування на інциденти. Розуміючи потенційні загрози та вектори атак, організації можуть розробити ефективні плани реагування на інциденти. Це включає встановлення процедур для виявлення, реагування та відновлення після інцидентів безпеки в мережі клієнт – сервер. Наявність чітко визначеного плану реагування на інциденти може мінімізувати вплив порушень безпеки та забезпечити оперативні дії для пом'якшення ризиків.
- Відповідність вимогам і правилам, всі загрози допомагають організаціям узгодити свої методи безпеки з галузевими стандартами, найкращими практиками та нормативними вимогами. Розглядаючи потенційні загрози та вразливі місця, організації можуть запровадити заходи безпеки, які відповідають відповідним нормам і захистити конфіденційні дані.
- Постійне вдосконалення, моделювання загроз – це ітеративний процес, який розвивається в міру появи нових загроз і змін у мережевій інфраструктурі. Регулярно переглядаючи та оновлюючи моделі загроз,

організації можуть залишатися проактивними у вирішенні нових загроз і підвищенні безпеки клієнт – серверної мережі.

Існуючі моделі загроз

1. Модель STRIDE

Модель STRIDE – це широко використовувана структура в галузі кібербезпеки для ідентифікації та класифікації різних типів загроз. STRIDE – це абревіатура, яка представляє шість категорій загроз:

- Підробка: це означає, що зловмисник видає себе за когось іншого або фальсифікує свою особу, щоб отримати несанкціонований доступ або ввести користувачів в оману. Приклади включають підробку IP – адреси, підробку електронної пошти або домену.
- Втручання: це передбачає несанкціоновану модифікацію або зміну даних під час передачі чи зберігання. Зловмисники можуть маніпулювати даними, щоб отримати переваги або порушити нормальне функціонування системи. Приклади включають зміну мережевих пакетів, зміну вмісту бази даних або зміну файлів конфігурації.
- Відмова: це стосується відмови від певних дій або подій суб'єктом. Зловмисники можуть спробувати спростувати свої дії, щоб уникнути відповідальності або оскаржити автентичність транзакцій. Приклади включають відмову у виконанні транзакції, відмову від надісланих повідомлень або відхилення завершеної дії.
- Розголошення інформації: це стосується несанкціонованого доступу або доступу до конфіденційної інформації. Зловмисники можуть використовувати вразливості, щоб отримати доступ до конфіденційних даних або перехопити інформацію під час передачі. Приклади включають прослуховування мережевого трафіку, викрадення облікових даних або доступ до конфіденційних документів.
- Відмова в обслуговуванні (DoS): це передбачає порушення або погіршення доступності системи чи мережі, що робить їх недоступними для

законних користувачів. Зловмисники перевантажують ресурси, вичерпують місткість вихлопної системи або використовують уразливості, щоб викликати збої в роботі. Приклади включають переповнення мережі трафіком, запуск розподіленої DoS – атаки або використання вразливостей програмного забезпечення для збою системи.

- Підвищення привілеїв: це стосується неавторизованого підвищення привілеїв, що дозволяє зловмиснику отримати вищі рівні доступу або дозволів. Зловмисники використовують уразливості, щоб збільшити свої привілеї та отримати контроль над системами або даними за межами їх дозволеного обсягу. Приклади включають атаки на підвищення привілеїв, обхід засобів контролю доступу або використання вразливостей програмного забезпечення для отримання адміністративних привілеїв.

Розглядаючи ці шість категорій загроз, організації можуть розробити ефективні стратегії пом’якшення ризиків і захисту своїх систем і даних від потенційних атак.

Таблиця 2.4 – Модель загроз Stride

Загроза	Визначення	Власність	Приклад
Спуфінг	Прикидатися кимось іншим	Аутентифікація	Зламати електронну пошту жертви та використовувати для надсилання повідомлень від імені жертви

Продовження табл. 2.4 – Модель загроз Stride.

Загроза	Визначення	Власність	Приклад
Фальсифікація	Змінити дані або код	Цілісність	виконавчий файл програмного забезпечення підроблено хакерами
Відмова	Стверджувати, що не робити певної дії	Не відмова	я не надсилав електронного листа Алісі
Розкриття інформації	Витік конфіденційної інформації	Конфіденційність	Інформація про кредитну картку доступна в Інтернеті
Відмова в обслуговуванні	Відсутність послуги	Доступність	веб– програма не відповідає на запити користувачів
Підвищення привілеїв	Здатний здійснювати несанкціоновані дії	Авторизація	звичайний користувач може видалити обліковий запис адміністратора

2. Модель MITRE ATT&CK

MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це база знань і структура, яка надає детальну інформацію про реальну поведінку та методи супротивника. Це вичерпний каталог тактик і прийомів, які використовують суб'єкти загрози на різних етапах кібератаки.

MITRE ATT&CK складається з таких компонентів:

- Тактика: високорівневі цілі, яких загрозливі особи прагнуть досягти під час атаки. Є 12 тактик, включаючи початковий доступ, виконання, постійність, ескалацію привілеїв, ухилення від захисту, доступ до облікових

даних, виявлення, бічний рух, збір, ексфільтрацію, командування та контроль і вплив.

- Техніки: конкретні методи та дії, які використовують супротивники для досягнення своїх цілей у межах кожної тактики. Існують сотні методів, задокументованих у рамках MITER ATT&CK, таких як фішинг, віддалене виконання коду, скидання облікових даних, латеральне переміщення за допомогою WMI, викрадання даних через DNS тощо.
- Під методи: подальше вдосконалення методів, які надають більш конкретні відомості про поведінку зловмисників. Допоміжні методи дозволяють більш детально аналізувати та виявляти дії супротивника.
- Засоби пом’якшення: рекомендовані оборонні стратегії та контрзаходи для запобігання або пом’якшення впливу певних методів або тактик. Це практичні кроки, які організації можуть зробити, щоб підвищити рівень безпеки та зменшити ризик успішних атак.
- Групи: групи супротивників, також відомі як суб’єкти загрози або групи APT (Advanced Persistent Threat), класифікуються та описуються в MITRE ATT&CK. Кожна група пов’язана з відомими тактиками, техніками та процедурами (TTP), які вона використовує.

MITRE ATT&CK є цінним ресурсом для організацій і фахівців з кібербезпеки, щоб зрозуміти тактику та методи, які використовують суб’єкти загроз. Він допомагає покращити розвідку про загрози, реагування на інциденти та загальний стан безпеки, надаючи інформацію про поведінку зловмисників у реальному світі та ефективні стратегії пом’якшення.[16]

3. Модель DREAD

Модель загроз DREAD – це структура оцінки ризиків, яка допомагає ідентифікувати потенційні загрози системі чи програмі та визначати пріоритети. Він позначає такі п'ять компонентів:

- Потенційна шкода: оцінка потенційної шкоди або впливу, які може спричинити загроза, якщо її використовувати. Допомагає оцінити тяжкість наслідків.
- Відтворюваність: оцінка легкості, з якою загроза може бути відтворена або використана багаторазово. Цей фактор враховує, чи є загроза разовою подією, чи її можна використовувати постійно.
- Можливість використання: визначення рівня зусиль і досвіду, необхідних для використання вразливості. Він оцінює легкість, з якою зловмисник може скористатися вразливістю.
- Постраждалі користувачі: визначення кількості користувачів або систем, які можуть постраждати від загрози. Цей фактор допомагає оцінити масштаби впливу.
- Виявленість: оцінка того, наскільки легко зловмисник може виявити вразливість або загрозу. Цей фактор враховує ймовірність того, що зловмисник знайде та скористається вразливістю.

Оцінюючи кожен із цих компонентів, модель загроз DREAD забезпечує систематичний підхід до встановлення пріоритетів і усунення найбільш критичних загроз для системи чи програми. Це допомагає організаціям ефективно розподіляти ресурси та зосереджуватися на пом'якшенні найбільш значних ризиків.

4. Модель Kill Chain

Модель загроз Kill Chain – це структура, розроблена компанією Lockheed Martin для опису різних етапів кібератаки. Це допомагає організаціям зрозуміти та пом'якшити загрози, розділивши життєвий цикл атаки на окремі етапи. Ось огляд етапів у моделі ланцюга вбивств:

- Розвідка: зловмисник збирає інформацію про ціль, таку як виявлення вразливостей, топології мережі та потенційних точок входу.
- Вепонізація: зловмисник розробляє або отримує інструменти та методи, необхідні для використання виявлених вразливостей.

- Доставка: зловмисник доставляє озброєне корисне навантаження в цільову систему, часто використовуючи такі методи, як фішингові електронні листи, шкідливі вебсайти або скомпрометоване програмне забезпечення.
- Експлуатація: зловмисник виконує корисне навантаження, щоб використовувати вразливості в цільовій системі, отримуючи неавторизований доступ або контроль.
- Встановлення: зловмисник установлює постійну присутність у скомпрометованій системі чи мережі, забезпечуючи постійний доступ і контроль.
- Командування та контроль: зловмисник встановлює канали зв'язку та інфраструктуру для віддаленого управління та контролю скомпрометованих систем.
- Цільові дії: зловмисник виконує заплановані зловмисні дії, які можуть включати крадіжку даних, несанкціонований доступ, маніпулювання системою або інші цілі.

Розуміючи та аналізуючи кожну стадію ланцюга несправності, організації можуть виявити потенційні слабкі місця, запровадити відповідні засоби контролю безпеки та розробити стратегії виявлення, реагування на атаки та пом'якшення атак на різних етапах життєвого циклу. Ця модель допомагає командам безпеки прийняти проактивний підхід до запобігання загрозам і реагування на інциденти.



Рисунок 2.5 – Ланцюг Кіберубивст

5. Модель CIA.

Модель загроз CIA, також відома як тріада CIA, є фундаментальною концепцією інформаційної безпеки, яка зосереджена на трьох основних принципах: конфіденційність, цілісність і доступність. Він забезпечує основу для розуміння та усунення ризиків безпеки та допомагає організаціям захистити свої інформаційні активи. Ось розбивка кожного елемента моделі загроз CIA:

- Конфіденційність: Конфіденційність гарантує, що інформація доступна лише уповноваженим особам або організаціям. Це передбачає захист конфіденційних даних від несанкціонованого розголошення, наприклад, за допомогою шифрування, контролю доступу та безпечних каналів зв'язку.
- Цілісність: цілісність гарантує, що інформація залишається точною, повною та незмінною протягом усього життєвого циклу. Це передбачає запобігання неавторизованим змінам, додаванням або видаленням даних. Такі методи, як перевірка даних, контрольні суми та цифрові підписи, допомагають підтримувати цілісність даних.
- Доступність: доступність гарантує, що інформація та ресурси доступні та придатні для використання, коли це необхідно. Він передбачає захист від збоїв або несанкціонованих атак на відмову в обслуговуванні, які можуть вплинути на доступність систем, мереж або даних. Резервування, резервне копіювання та надійна інфраструктура є прикладами заходів, вжитих для підтримки доступності.

Модель загроз CIA розроблена, щоб забезпечити комплексний підхід до інформаційної безпеки, розглядаючи різні аспекти ризику. Це допомагає організаціям визначати потенційні вразливості, оцінювати вплив загроз і впроваджувати відповідні засоби контролю безпеки та контрзаходи для захисту своїх критично важливих активів. Розглядаючи разом конфіденційність, цілісність і доступність, організації можуть створити збалансовану та ефективну систему безпеки.

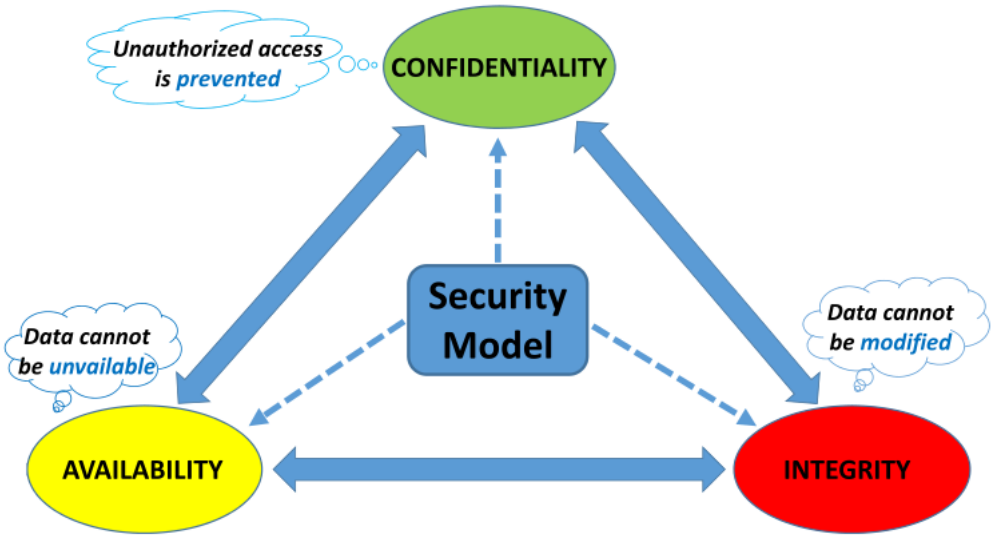


Рисунок 2.6 – модель загроз CIA

Я використав модель загроз STRIDE для аналізу безпеки корпоративної мережної інфраструктури з відкритим вебдодатком в домені Active Directory. Ця модель дозволила ідентифікувати та категоризувати найчастіші або найбільш небезпечні загрози, які можуть виникнути в такому середовищі.[6]

2.4 Побудова моделі загроз клієнт– серверної мережі для атак на Active Directory ОС Windows Server 2019

В цьому підрозділі я визначу конкретні загрози клієнт – серверної мережі, критичні елементи своєї підсистеми, визначу різні потоки даних в системі, побудую діаграму загроз для системи.

Елементи клієнт – серверної мережі:

1. Мережеве обладнання
2. Сервери
3. Клієнти
4. Активний каталог (Active Directory)
5. Аутентифікація та авторизація
6. Захист мережі
7. Клієнтські пристрої

Потоки даних в межах клієнт – серверної мережі:

1. Клієнтські запити до сервера

2. Передача даних від клієнта до сервера

3. Відповіді сервера до клієнта

4. Передача даних між серверами

Потоки даних між користувачем та системою клієнт – сервурної мережі

1. Веб – перегляд

2. Електронна пошта

3. Файловий доступ

4. Бази даних

Потоки даних між користувачем та пристроями клієнт – серверної мережі

1.Запит на аутентифікацію

2.Запити від користувача

Критичними елементами, що є з відкритими загрозами, у моїй клієнт – серверній мережі це сервери, та мережеві маршрутизатори та комутатори, Якщо перестануть працювати сервери може відбутися перерва в роботі системи, і це призведе до зупинки робочих процесів та будуть недоступні важливі функції. В разі неполадок в роботі комутаторів будуть виникати проблеми з підключенням до мережі, це призведе до втрати даних та зниження продуктивності мережевих додатків.

Загрози для DHCP spoofing:

Загроза перехоплення мережевого трафіку

Тип загрози: "Sniffing" або "Packet Sniffing"

Рівень загрози: середній – високий

Опис загрози: зловмисники перехоплюють та аналізують мережевий трафік, що передається через мережі

Спосіб пом’якшення: використовувати шифрування, використовувати протоколи безпеки, встановлення фаєрволу, моніторинг мережі, оновлювати програмне забезпечення.

Загроза підробка IP – адрес

Тип загрози: IP Spoofing

Рівень загрози: середній

Опис загрози: зловмисники можуть намагатися використовувати підроблені IP – адреси для введення в оману систем і мереж

Спосіб пом’якшення: використовувати аутентифікацію на основі мережевих протоколів, використовувати захищені протоколи, встановити фільтрацію вхідного трафіку

Загрози для DHCP starvation attack:

Загроза втрата мережевого з'єднання

Тип загрози: DoS (Denial of Service) атак.

Рівень загрози: низький

Опис загрози: під час атаки зловмисники намагаються витратити або зайняти всі доступні IP – адреси в пулі DHCP – сервера

Спосіб пом’якшення: резервне живлення, резервні мережеві шляхи, резервне обладнання, регулярне обслуговування та моніторинг.

Загроза перерозподіл IP – адрес

Тип загрози: в мережі відбувається неправильне або несанкціоноване присвоєння або зміна IP – адреси пристрою

Рівень загрози: середній

Опис загрози: це призведе до різних проблем у мережі, таких як конфлікти адрес, втрата зв'язку з мережевими ресурсами або некоректна робота мережевих служб.

Спосіб пом’якшення: використовувати статичні IP – адреси, використовувати DHCP Snooping, використання DHCP аудиту, заборона фізичного доступу.[7]

Загрози AS – REP Roasting на Active Directory:

Загроза ризик підбору пароля

Тип загрози: загрози безпеки

Рівень загрози: високий

Опис загрози: зловмисники намагаються зламати або вгадати пароль користувача, щоб отримати несанкціонований доступ до облікового запису або конфіденційної інформації

Спосіб пом’якшення: треба використовувати складні паролі, уникати використання загальнопоширених паролів, використовувати двофакторну аутентифікацію, регулярно змінювати паролі.

Загроза несанкціонований доступ до систем та ресурсів

Тип загрози: несанкційований доступ

Рівень загрози: високий

Опис загрози: зловмисники намагаються отримати несанкціонований доступ до комп'ютерних систем, мереж, баз даних або інших цифрових ресурсів

Спосіб пом’якшення: сильна аутентифікація, складні паролі, регулярне оновлення паролів, права доступу, використання мережевих заходів безпеки.[9]

Відповідно створили діаграму загроз у програмному додатку OWASP Threat – Dgragon.[8]

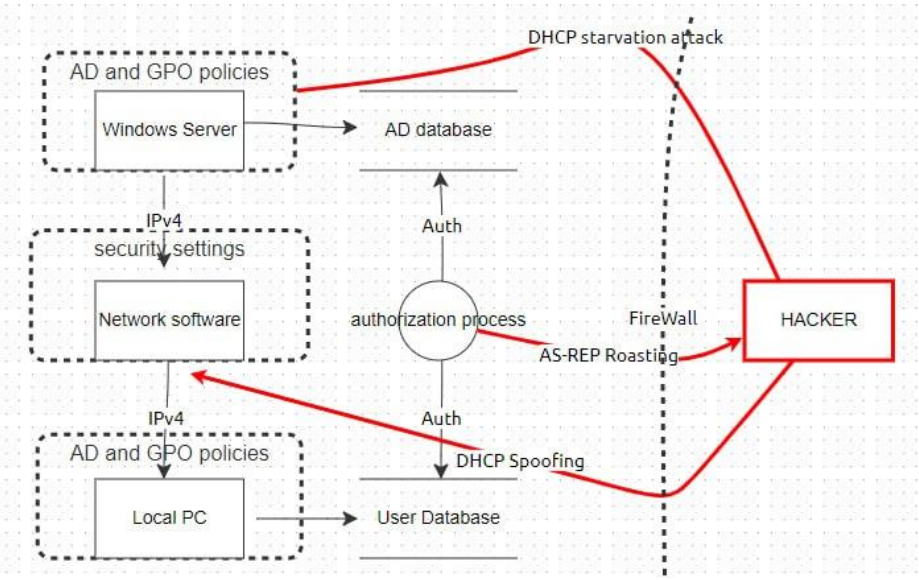


Рисунок 2.7 – Діаграма моделі загроз клієнт– серверної мережі на базі Active director

Нижче описано головні зовнішні фактори, які своєю дією можуть вплинути на клієнт– серверну мережу, також я представив загрози, які будуть описувати, та запроваджуватимуть для пом'якшення цих загроз.

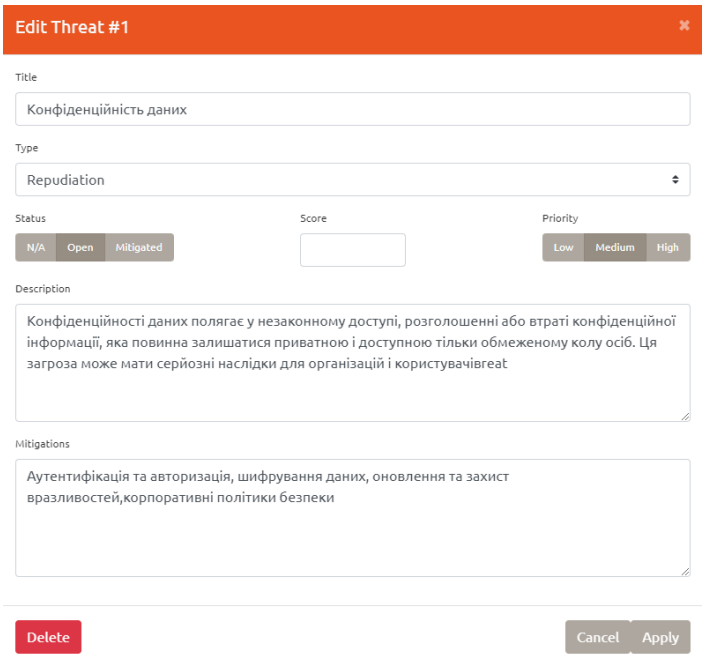


Рисунок 2.8 – Опис загрози конфіденційність даних

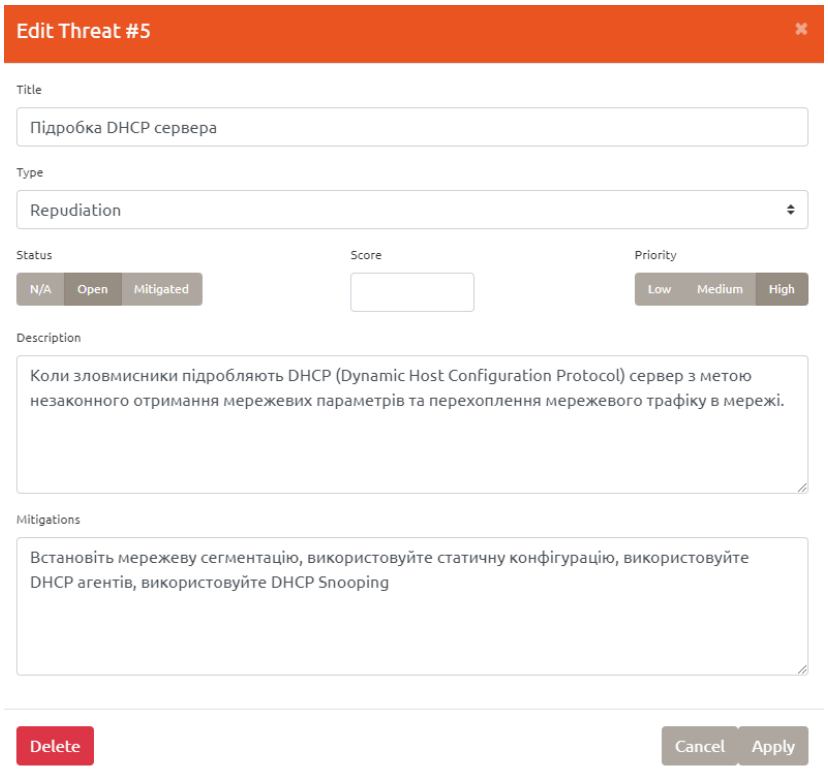


Рисунок 2.9 – Опис загрози підробка DHCP сервера

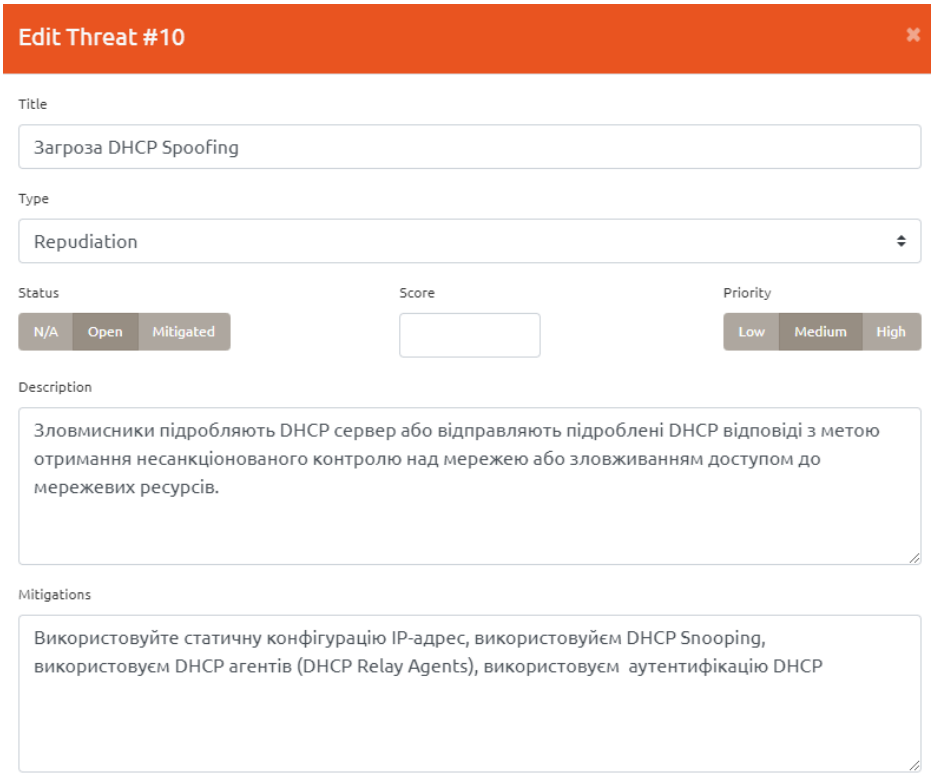


Рисунок 2.10 – Опис загрози DHCP spoofing

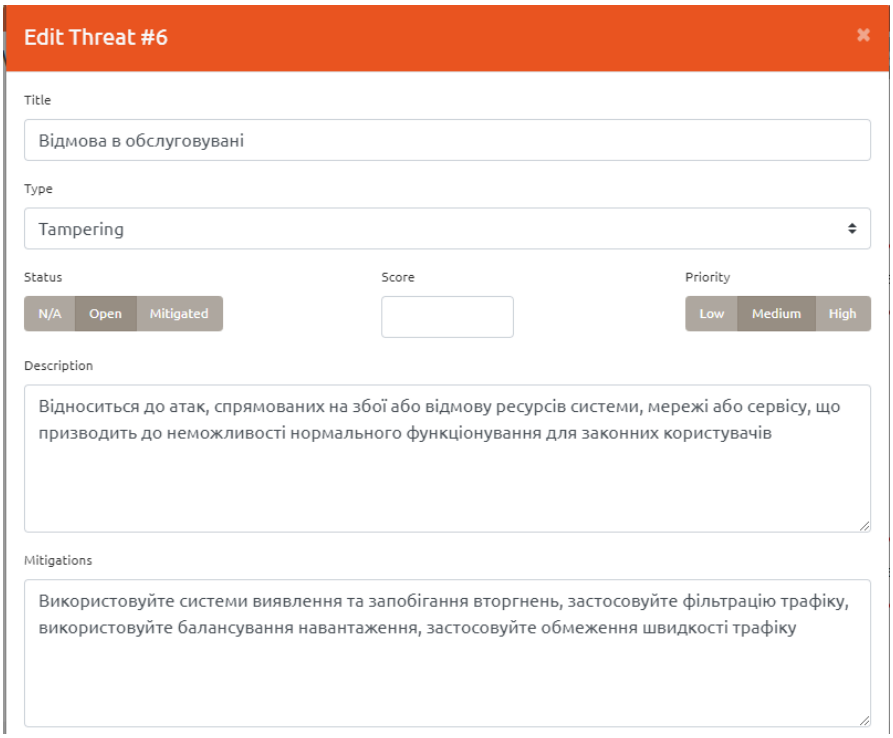


Рисунок 2.11 – Опис загрози відмова в обслуговувані

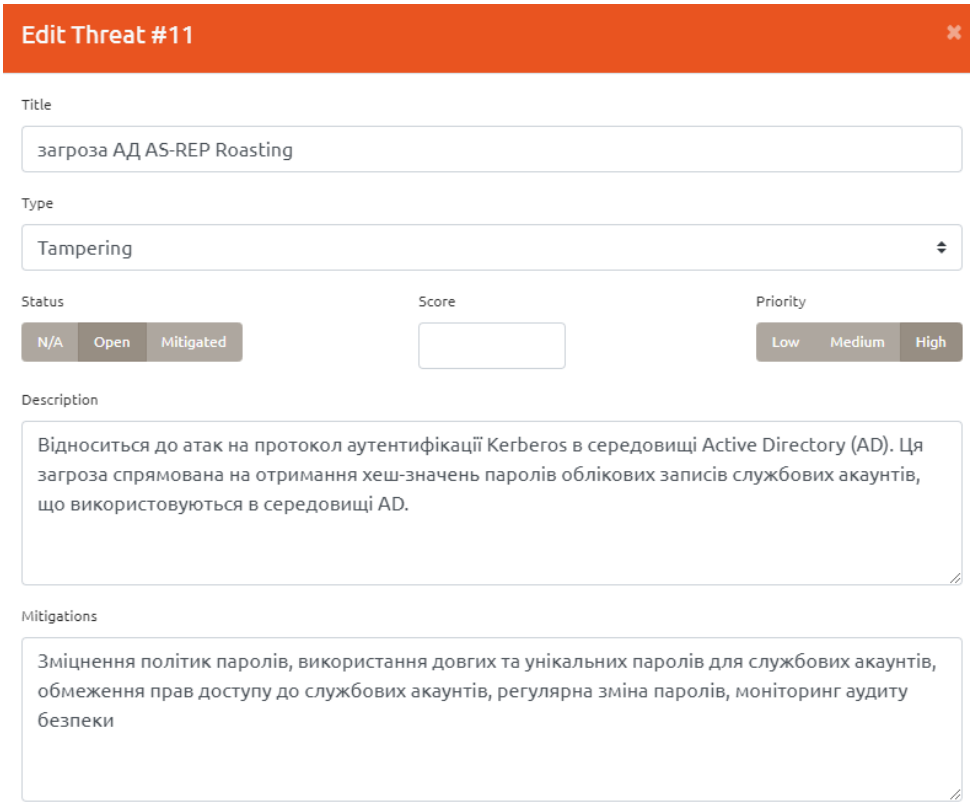


Рисунок 2.12 – Опис загрози AS– REP Roasting

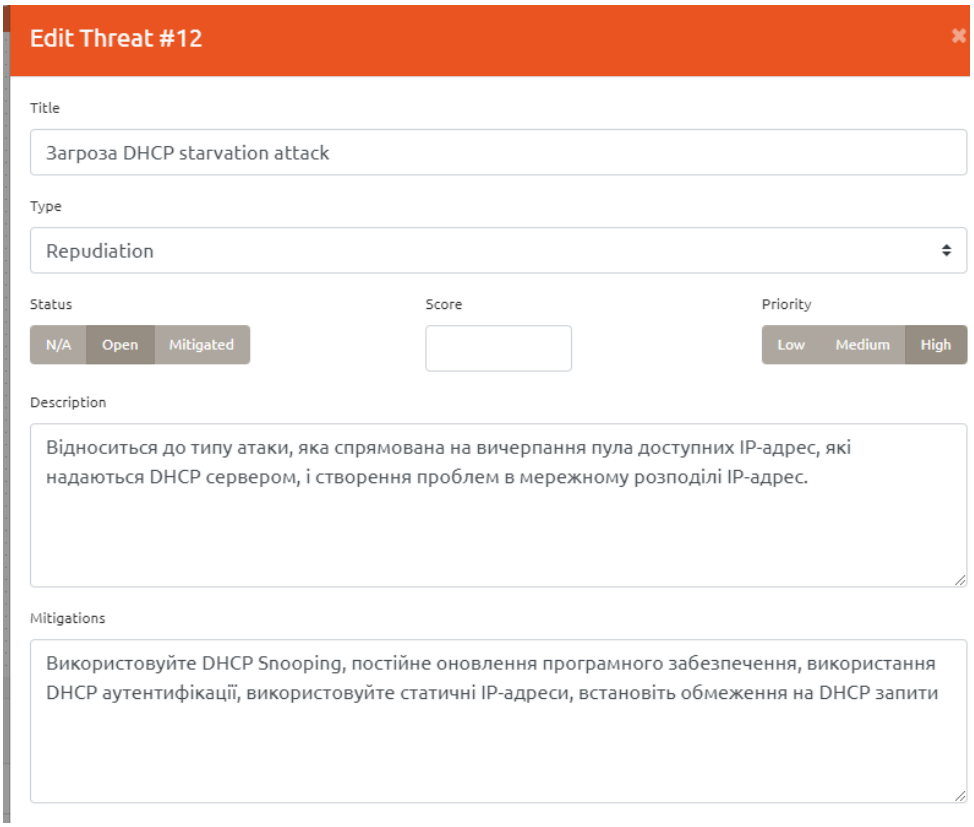


Рисунок 2.13 – Опис загрози DHCP starvation attack

Висновки до другого розділу

В даному розділі була описана клієнт – серверна мережа. Складена таблиця параметрів підключень мережевих пристроїв. Описані пристрої мережі та їх характеристика. Описані різні моделі загроз та визначені конкретні загрози клієнт-серверної мережі, критичні елементи підсистеми, визначено різні потоки даних в системі, побудована діаграма загроз.

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ КЛІЄНТ– СЕРВЕРНОЇ МЕРЕЖІ.

3.1 Налагодження комп'ютерної мережі.

Для того, щоб мережа правильно працювала, потрібно налаштовувати все у правильному порядку, та ви користовувати правильні параметри.

Початок налагодження я почав з налаштування ip адрес на Internet, R– 192– 15 – 1, Sw – 192 – 15 – 1 та SW – 192 – 15 – 2, також задав ip адреси комп'ютерам.

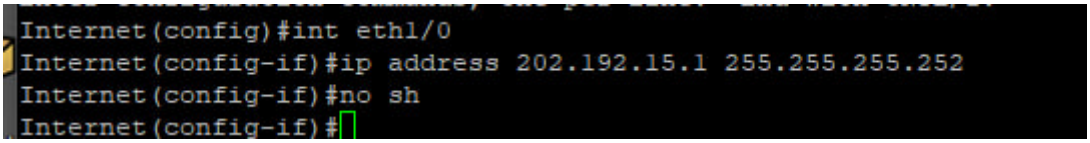


Рисунок 3.1 – Задана адреса Internet

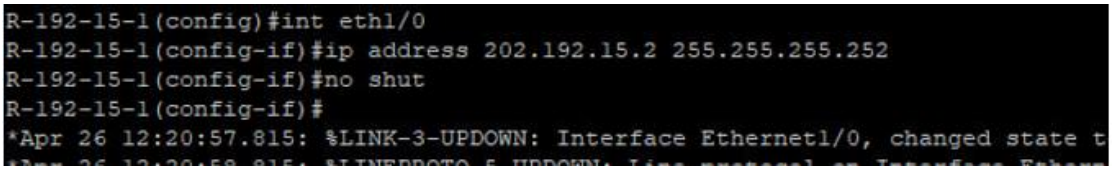


Рисунок 3.2 – Задана адреса R– 192– 15– 1

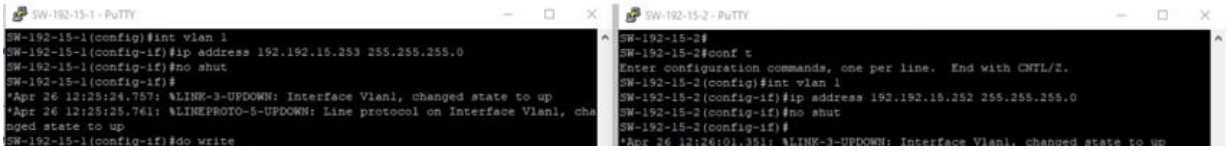


Рисунок 3.3 – Задана адреса SW– 192– 15– 1, SW– 192– 15– 2

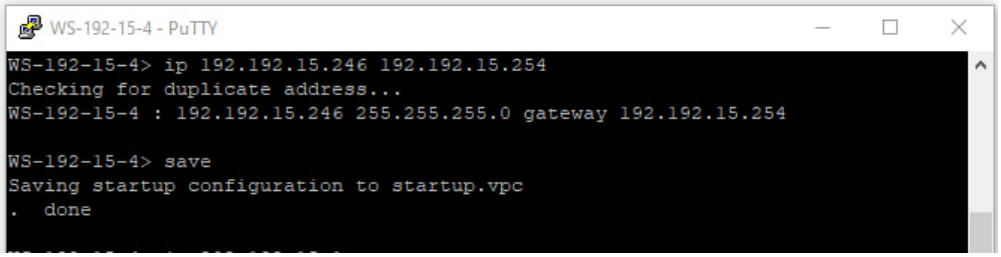


Рисунок 3.4 – Налаштовані адреси на комп'ютерах

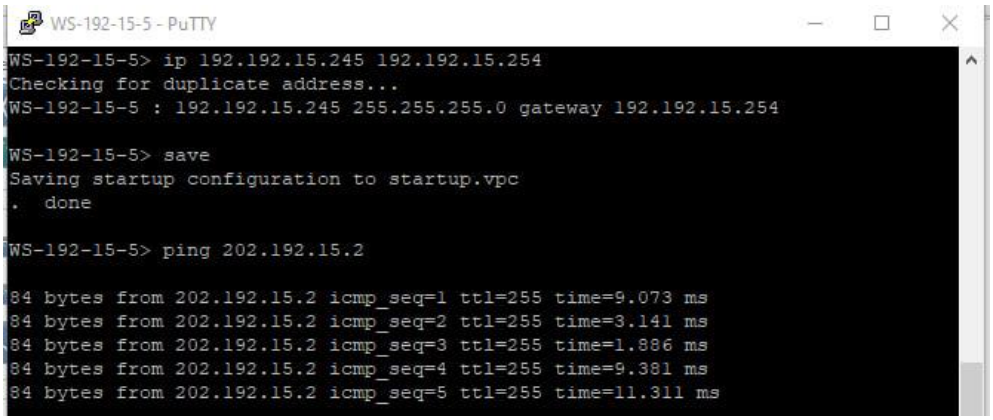


Рисунок 3.5 – Всі адреси на комп’ютері пінгують

Далі ми почали налаштовувати динамічну аутентифікацію OSPF на R – 1, та Ineternet, налаштували ntp, щоб синхронізовувася автоматично час та syslog, щоб збирати журнали подій з різних пристроїв і систем, таких як сервери, мережеві пристрої, додатки та інші компоненти мережі на мережевих пристроях, використали налаштування ssh, щоб використовувати віддалений безпечний доступ до комп’ютерних систем і передачі файлів через незахищену мережу.

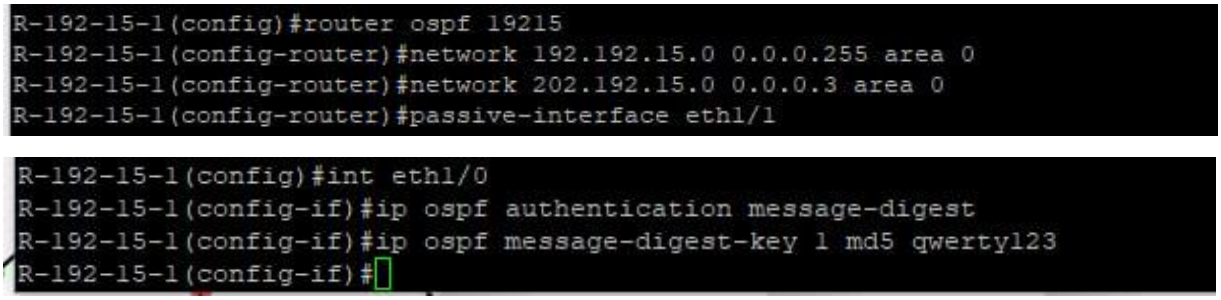


Рисунок 3.6 – Налаштування OSPF на R– 192– 15– 1

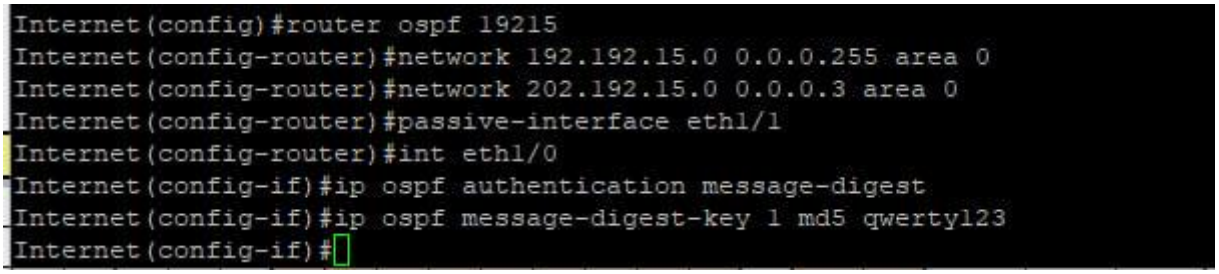


Рисунок 3.7 – Налаштування OSPF на Internet

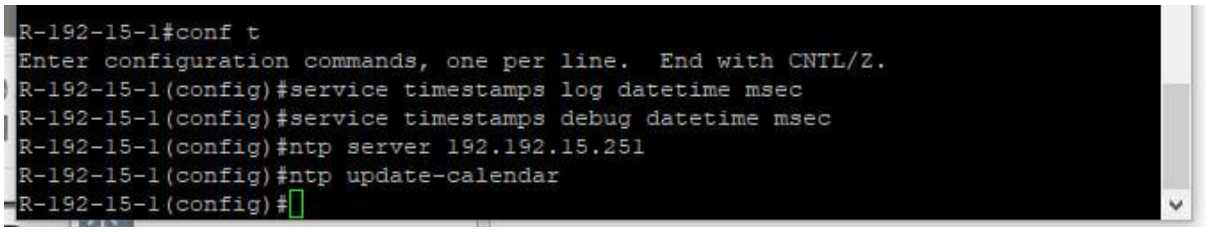


Рисунок 3.8 – Налаштування ntp

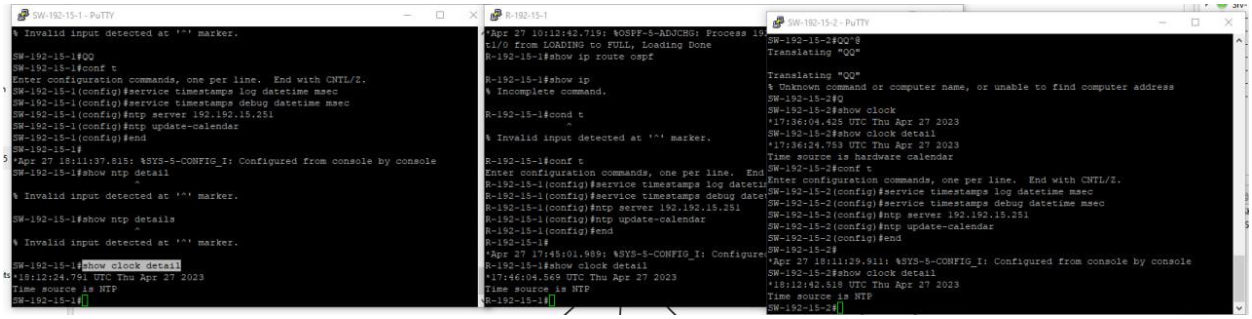


Рисунок 3.9 – Показано що ntp працює

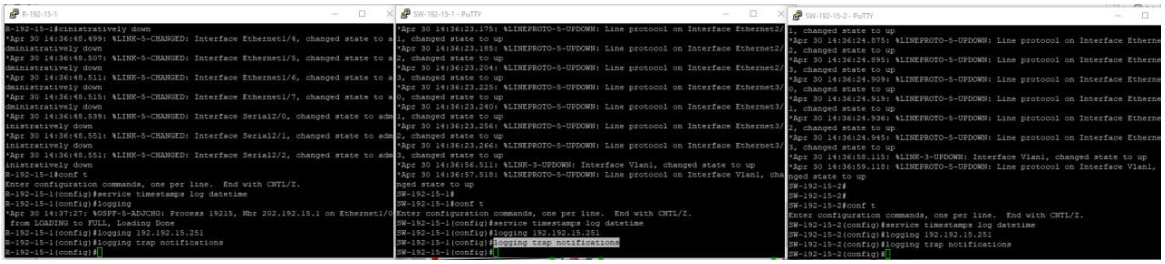


Рисунок 3.10 – Налаштування syslog

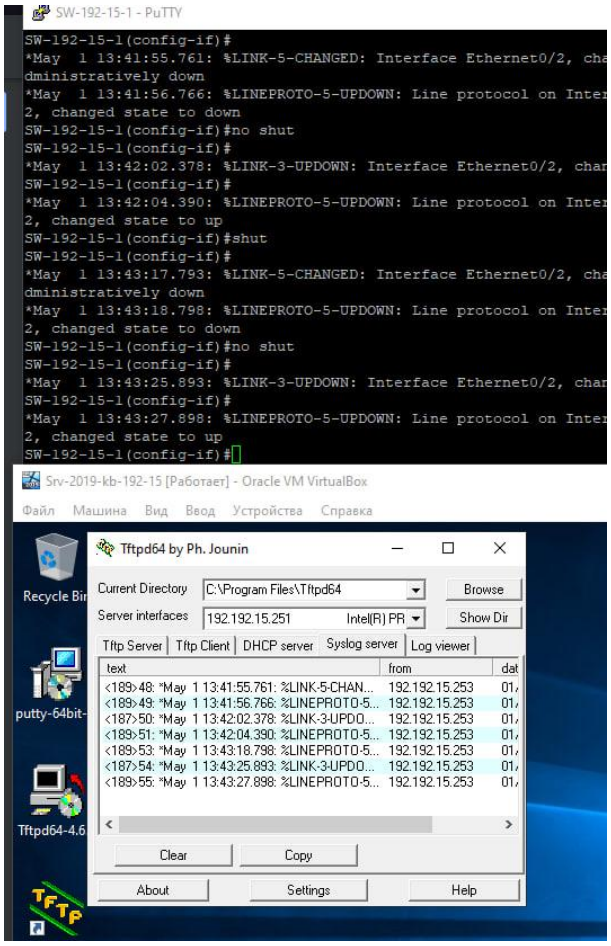


Рисунок 3.11 – Syslog працює

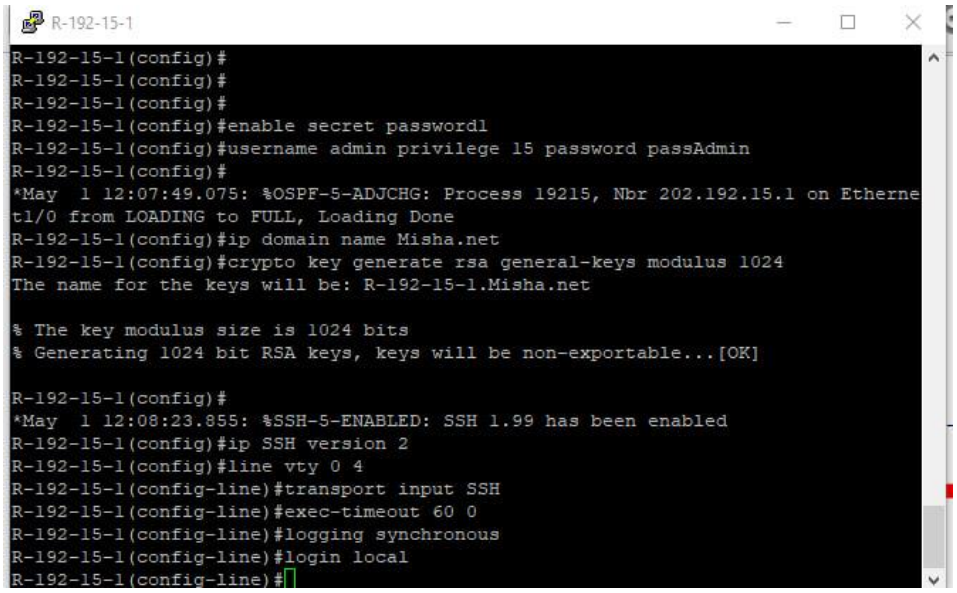


Рисунок 3.12 – Налаштований ssh на R– 192– 15– 1

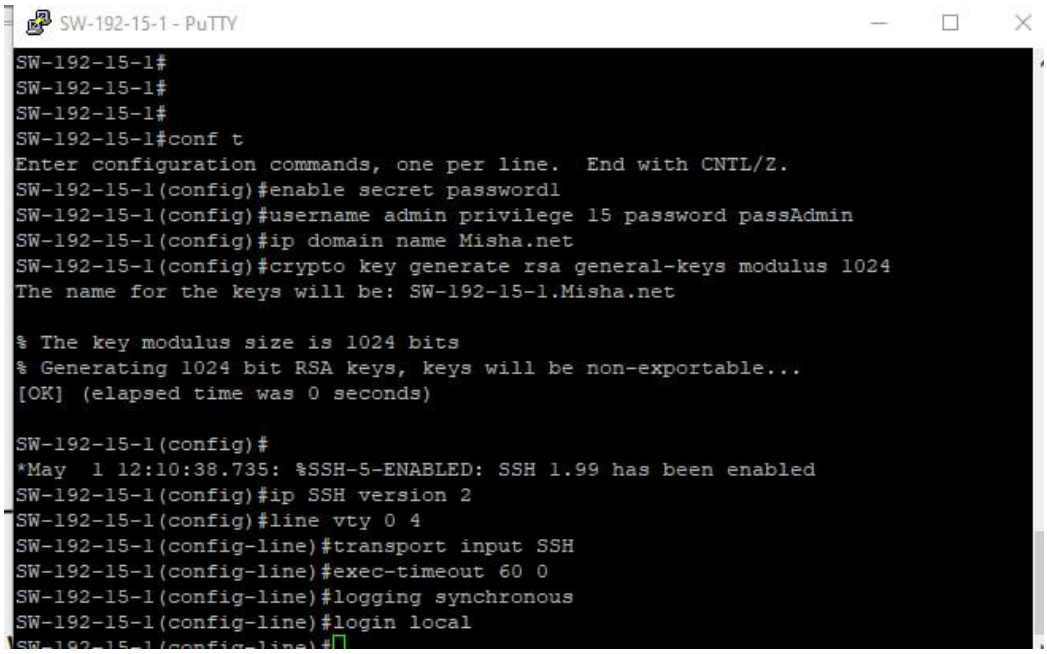


Рисунок 3.13 – Налаштований ssh на SW– 192– 15– 1

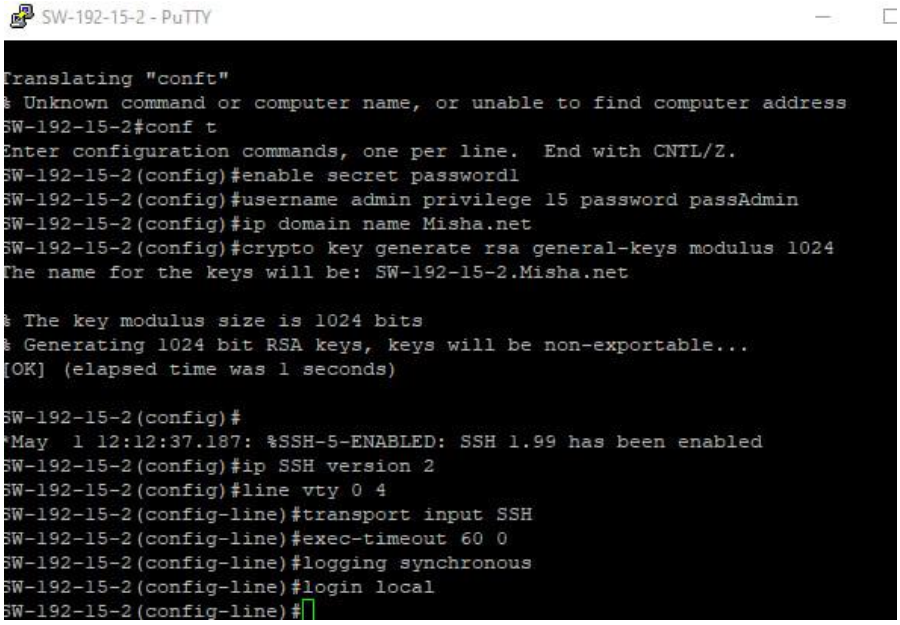


Рисунок 3.14 – Налаштований ssh на SW– 192– 15– 2

3.2 Налагодження Acrive Directory, Windows server 2019

В цьому підрозділі покажемо налаштування основного контролера домену Serv192 – 15 – 1(Windows Server 2019). На даному сервері задається адресація, рисунок 3.14, та створюється домен Misha.net, рис. 3.15. Також на всіх ОС Windows налаштували адресацію. Також надамо спільний доступ до файлів.

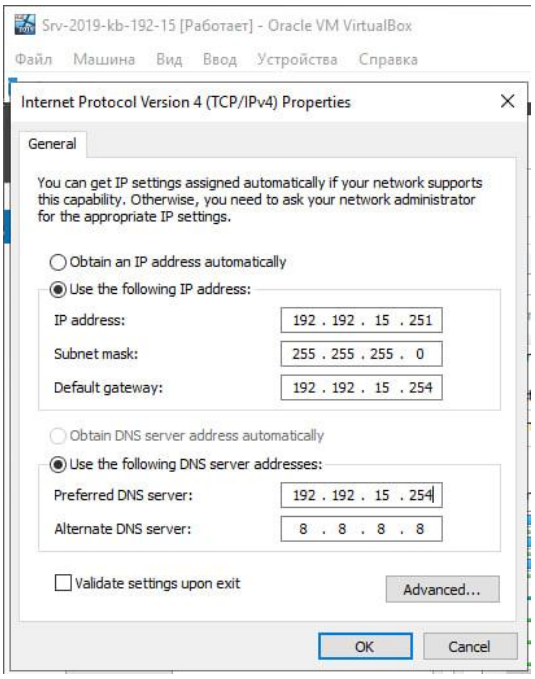


Рисунок 3.15 – Налаштування адресації на Serv – 192 – 15 – 1

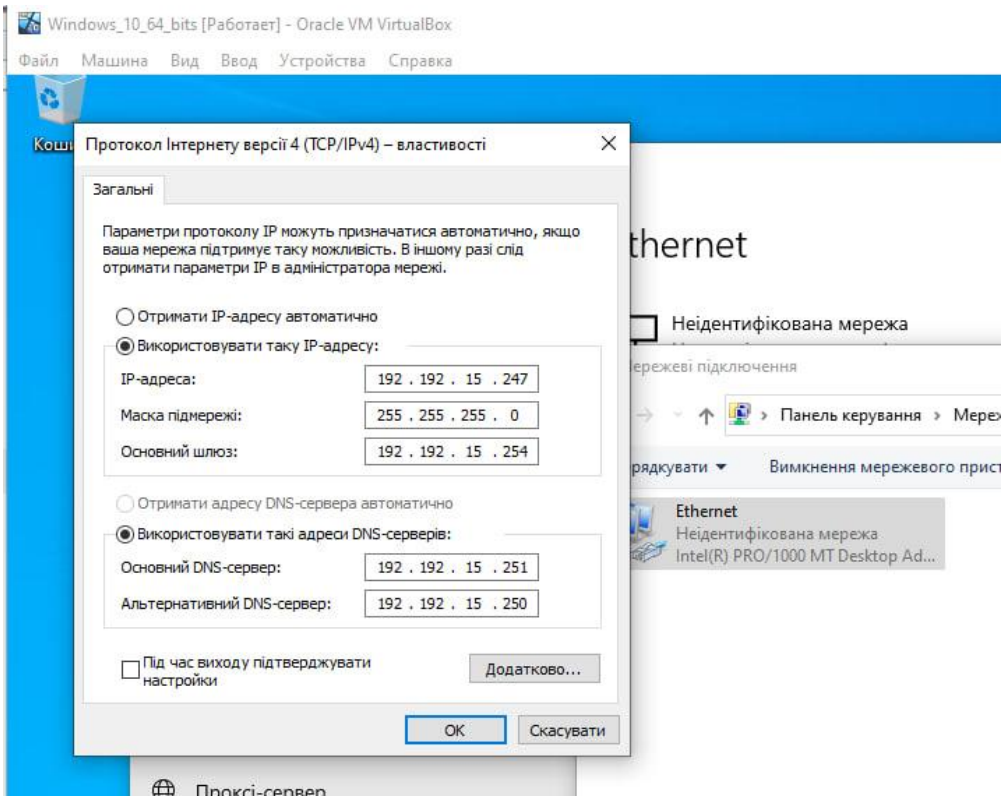


Рисунок 3.15 – Налаштування адресації на Windows 10

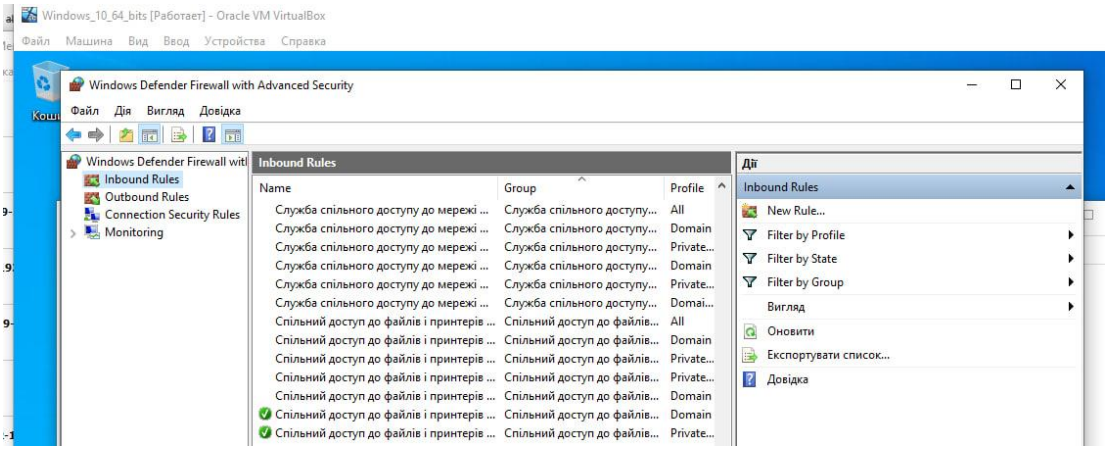


Рисунок 3.16 – Надали спільний доступ

```
C:\Users\Administrator>ping 192.192.15.254

Pinging 192.192.15.254 with 32 bytes of data:
Reply from 192.192.15.254: bytes=32 time=8ms TTL=255
Reply from 192.192.15.254: bytes=32 time=8ms TTL=255
Reply from 192.192.15.254: bytes=32 time=3ms TTL=255
Reply from 192.192.15.254: bytes=32 time=4ms TTL=255

Ping statistics for 192.192.15.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 8ms, Average = 5ms

C:\Users\Administrator>ping 192.192.15.251

Pinging 192.192.15.251 with 32 bytes of data:
Reply from 192.192.15.251: bytes=32 time<1ms TTL=128
Reply from 192.192.15.251: bytes=32 time<1ms TTL=128
Reply from 192.192.15.251: bytes=32 time<1ms TTL=128
Reply from 192.192.15.251: bytes=32 time<1ms TTL=128

Ping statistics for 192.192.15.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.17 – Всі станції пінгують

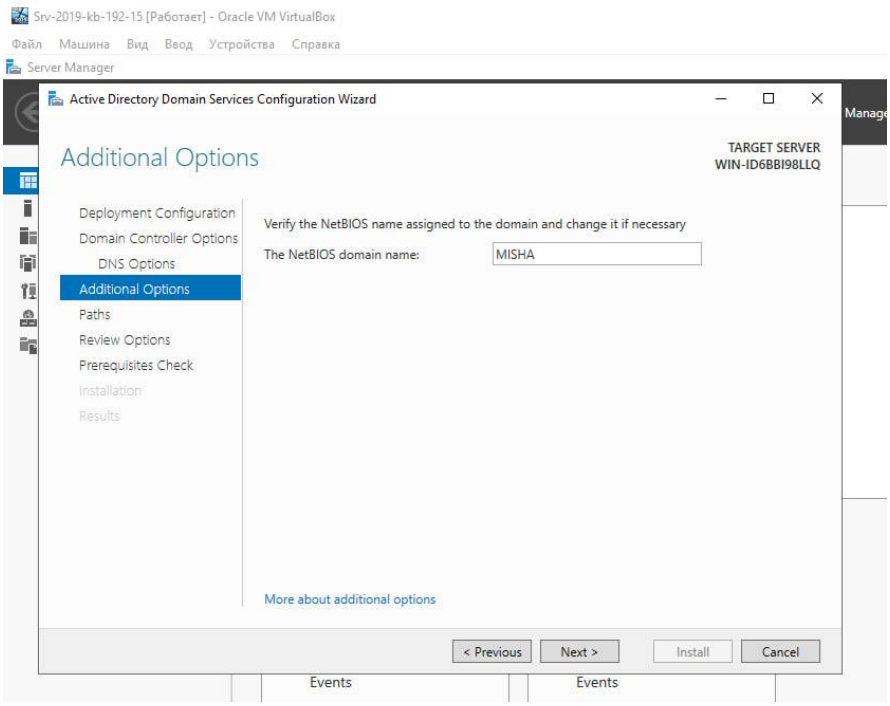


Рисунок 3.18 – Створення домену Misha.net на Serv – 192 – 15 – 1

На цьому ж сервері слід створити та налаштувати DHCP сервер, аби робочі станції мали змогу динамічно отримувати адреси. Тому створюємо область Misha_scope, рис. 3.21 і визначаємо діапазон роздачі адрес, рис. 3.22. Також ми покажемо що ми змогли під’єднатися до домену ОС 7 рис. 3.19 та ОС 10 рис. 3.20.

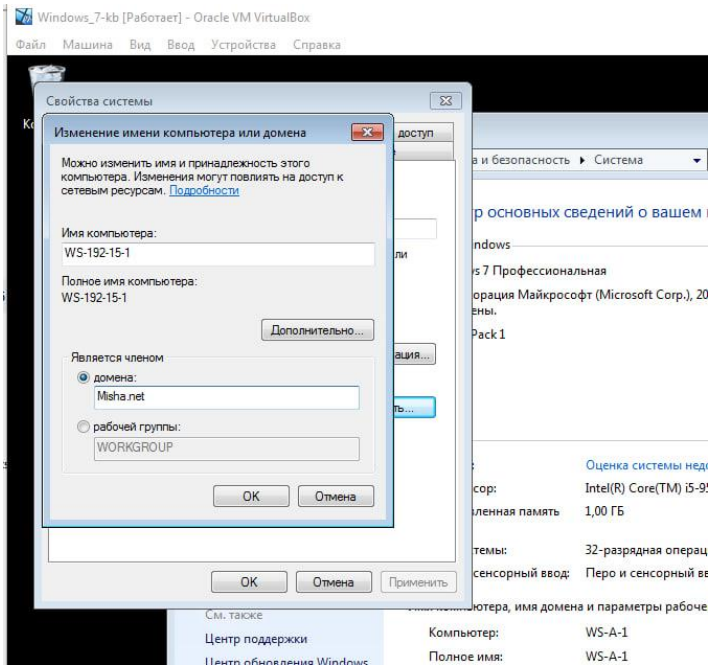


Рисунок 3.19 – Підключення до домену ОС 7

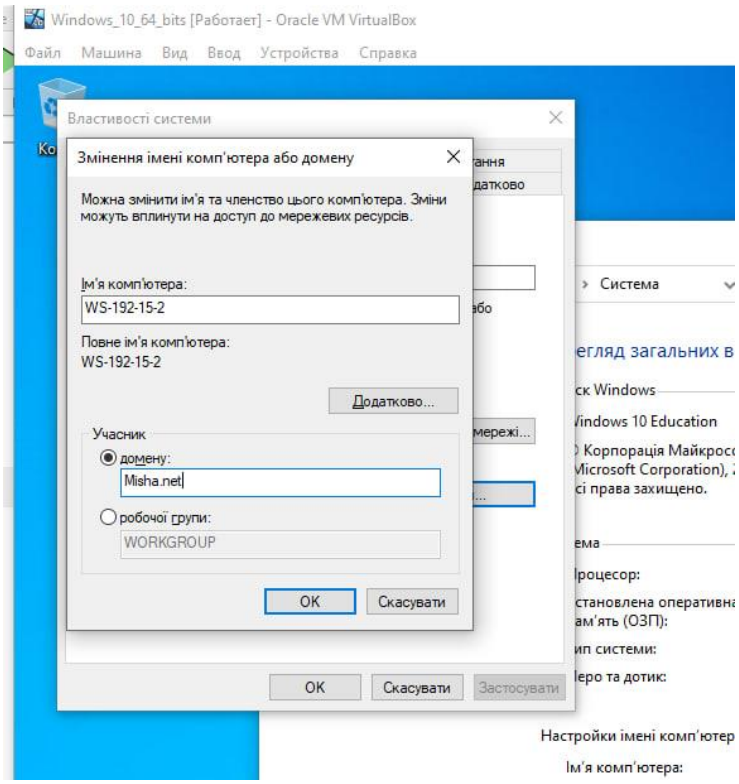


Рисунок 3.20 – Підключення до домену ОС 10

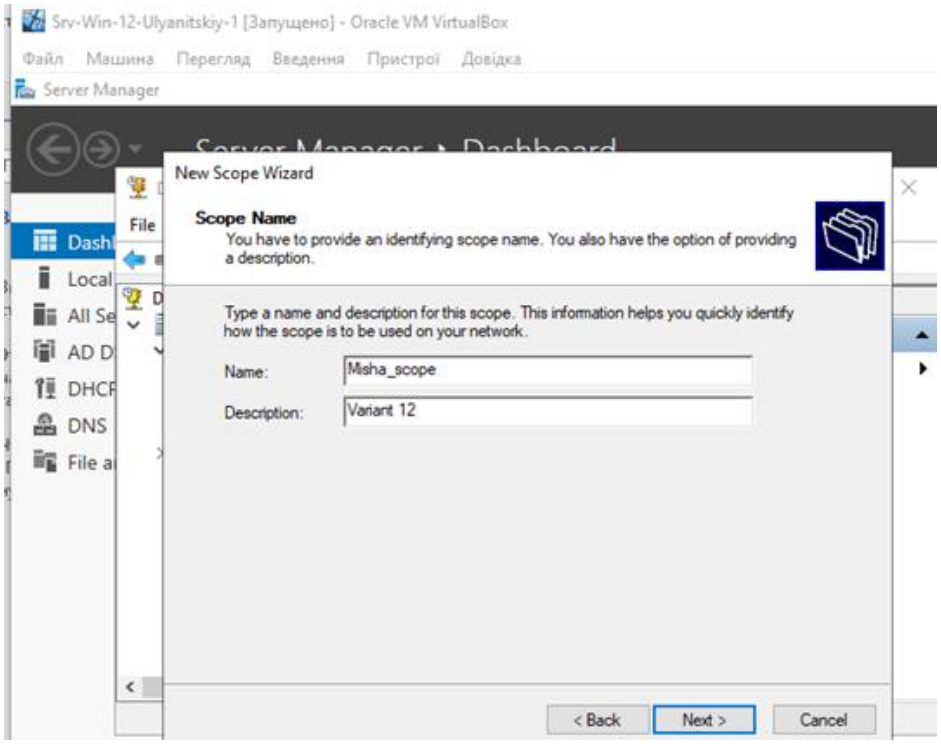


Рисунок 3.21 – Створення області Misha_scope

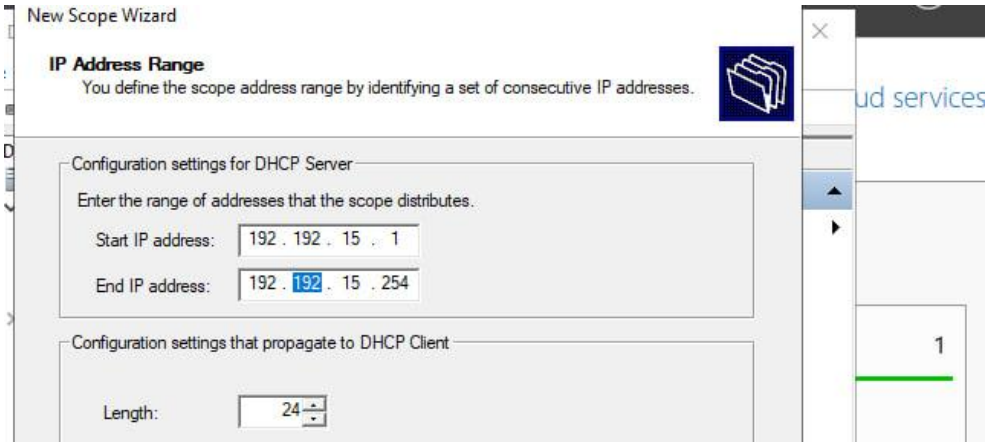


Рисунок 3.22 – Визначення діапазону роздачі адрес

З діапазону роздачі виключаю адреси, які будуть статично призначені іншим пристроям, рис. 3.23.

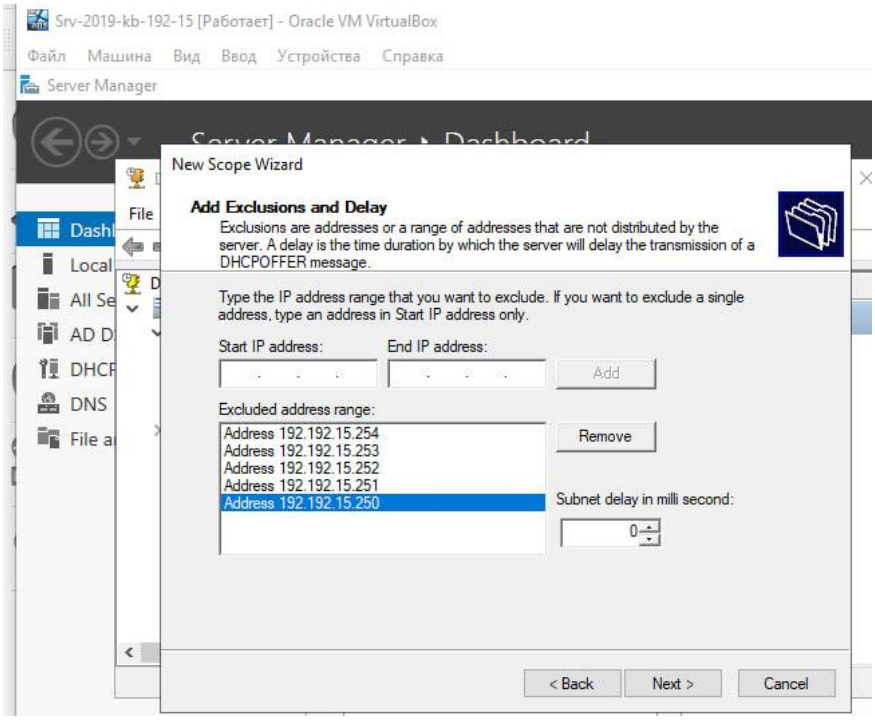


Рисунок 3.23 – Виключення статичних адрес з діапазону роздачі

Вказуємо, що робоча станція отримуватиме адреси автоматично, рис. 3.24.

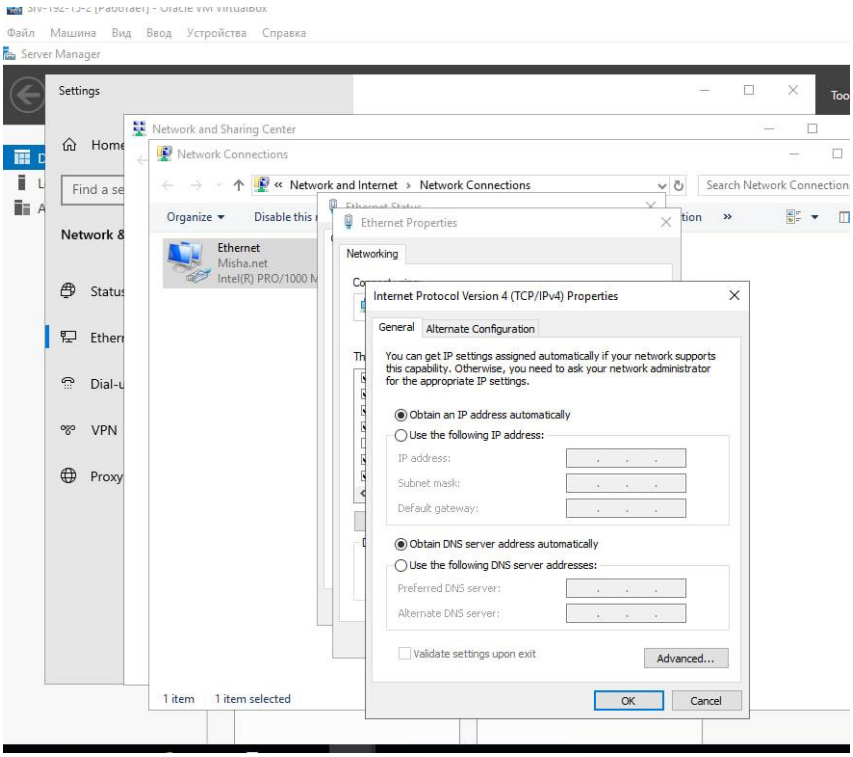


Рисунок 3.24 – Налаштування станції на автоматичне отримання адрес

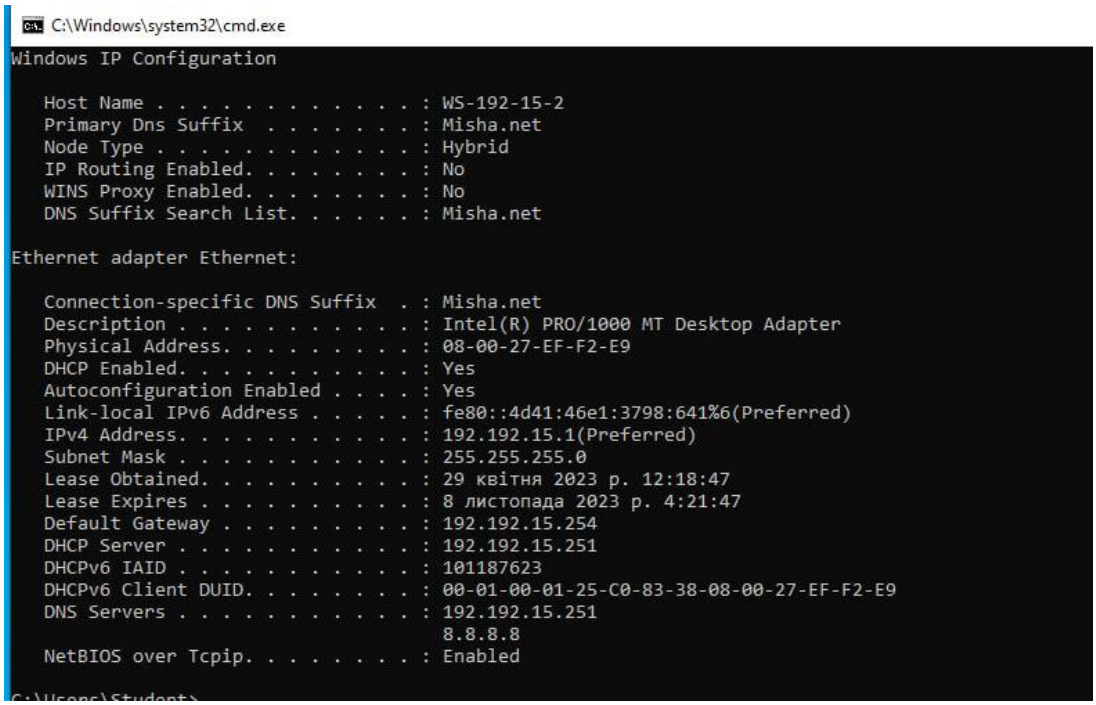


Рисунок 3.25 – Показано, що DHCP працює

Далі налаштовуємо віддалений доступ на Srv2019, щоб дозволити користувачам підключатися та працювати з комп'ютерами або системами, що

знаходяться в іншому місці або віддаленому мережевому середовищі. Це показано на Рис. 3.26– 3.27

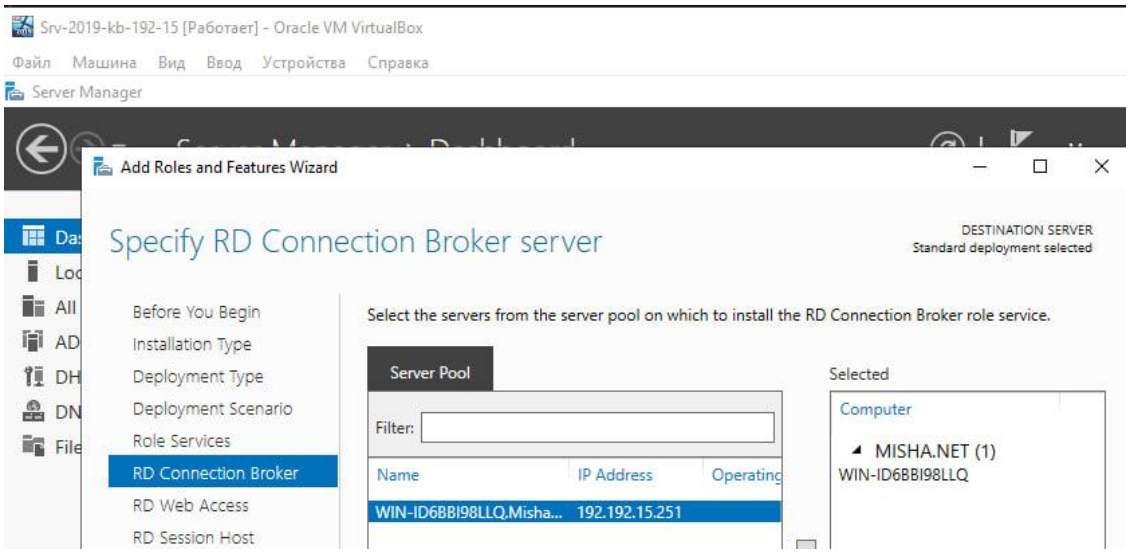


Рисунок 3.26 – Під’єднання до віддаленого доступу на сервері

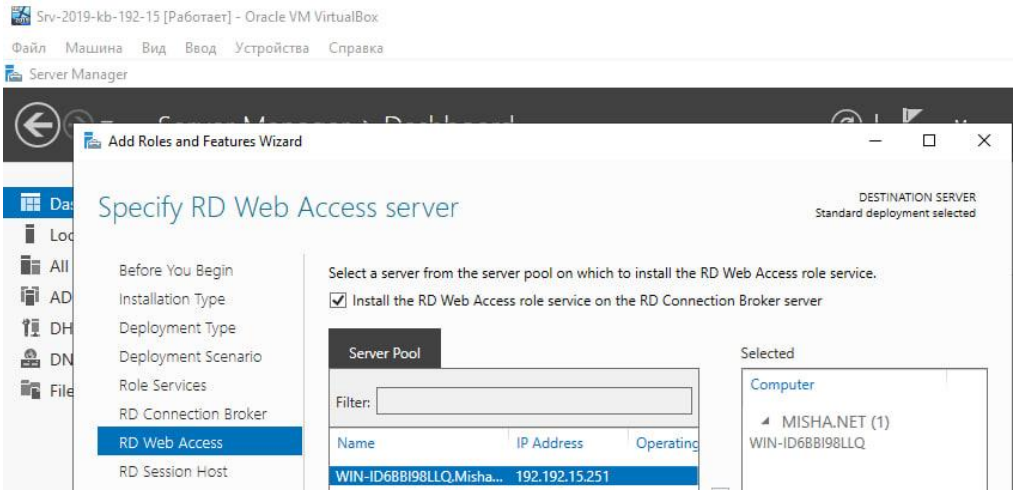


Рисунок 3.27 – Віддаленний доступ

Переходимо до налаштування часу, будем підключати ntp, потрібно перейти до групових політик.

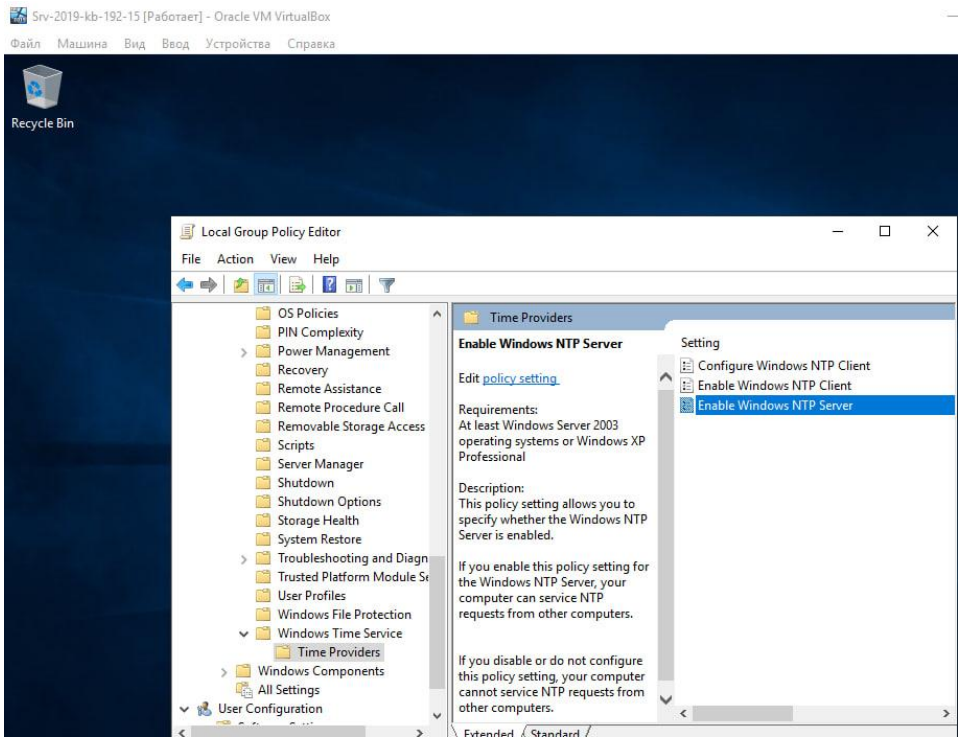


Рисунок 3.28 – Включили налаштування нтп сервера

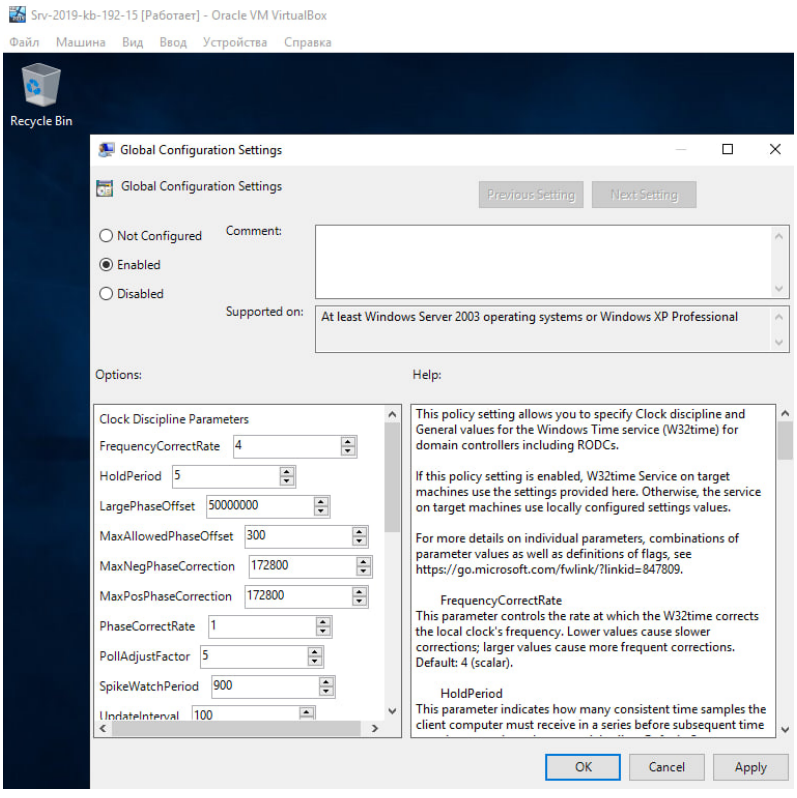


Рисунок 3.29 – Підключили глобальні налаштування нтп сервера

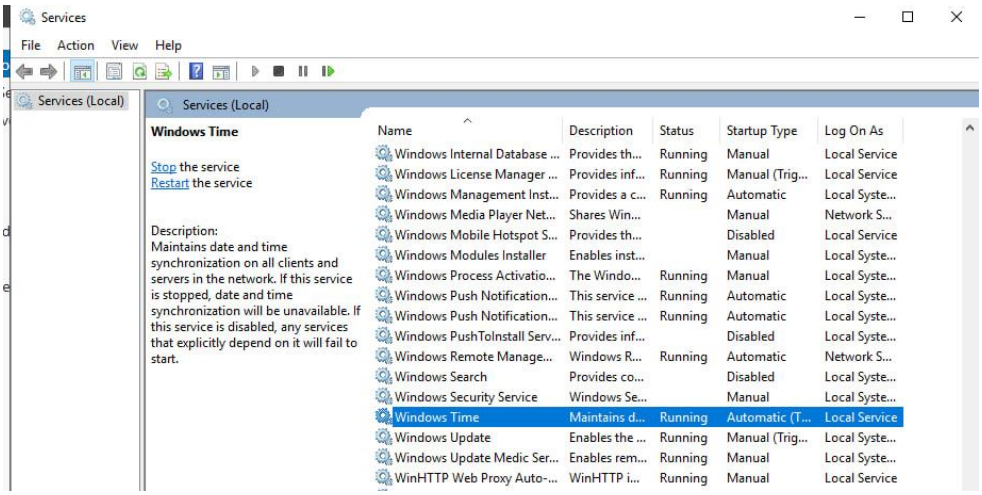


Рисунок 3.30 – NTP виконується

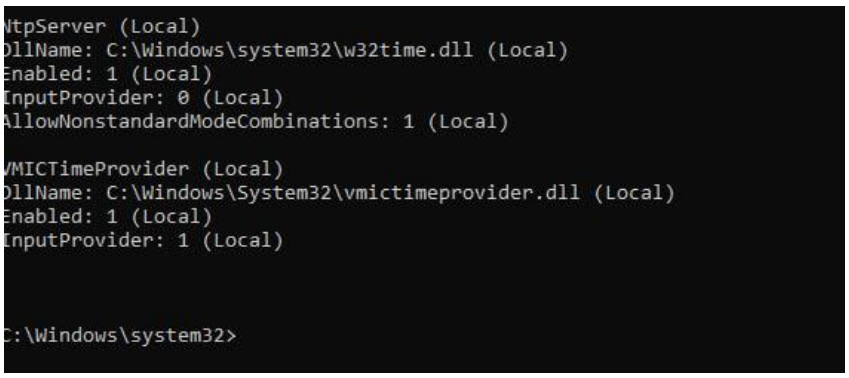


Рисунок 3.31 – На рисунку показано що NTP працює

В наступному кроці ми налаштуємо SSH для віддаленого управління комп’ютером.

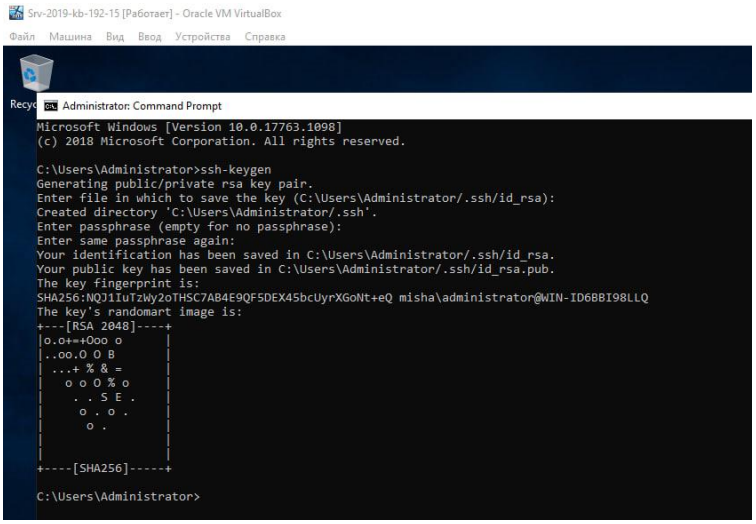


Рисунок 3.32 – Налаштування в cmd

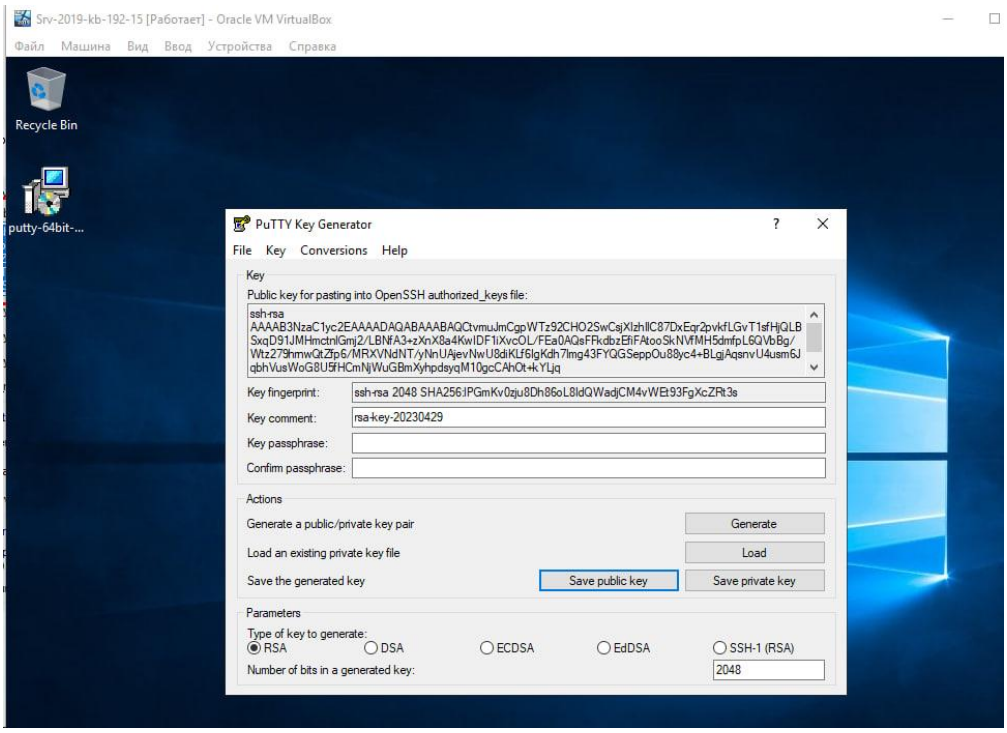


Рисунок 3.33 – Згенерували ключ

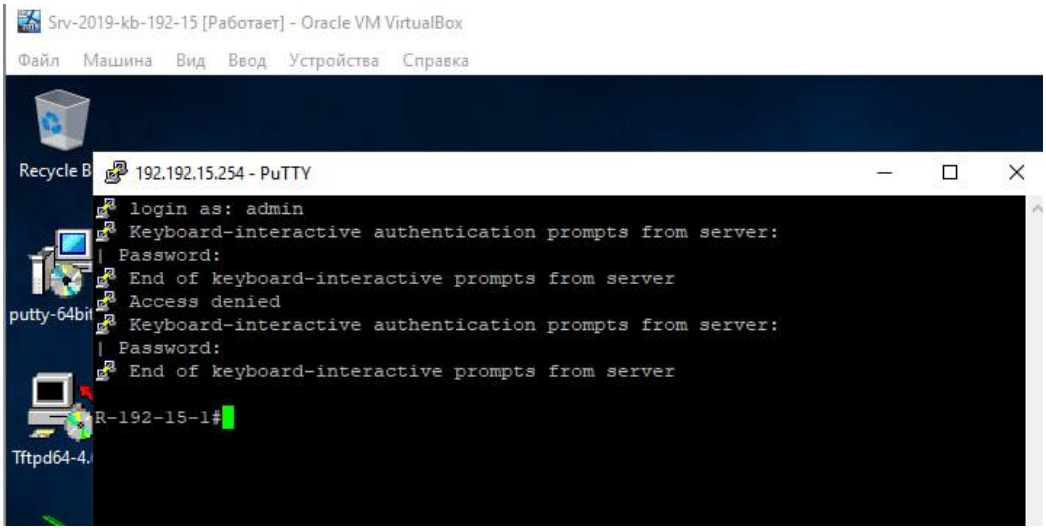


Рисунок 3.34 – На рисунку показано, що SSH під’єднався до маршутизатора

Далі ми виконаємо реплікацію між серверами, на випадок якщо один з серверів не буде працювати рис. 3.35– 3.36.

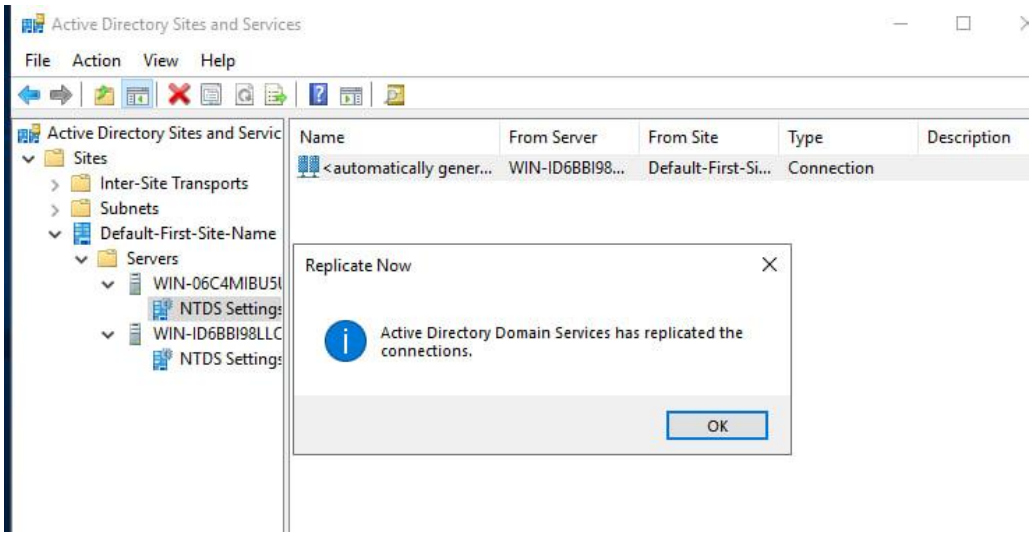


Рисунок 3.35 – Виконали реплікацію на одному із серверів

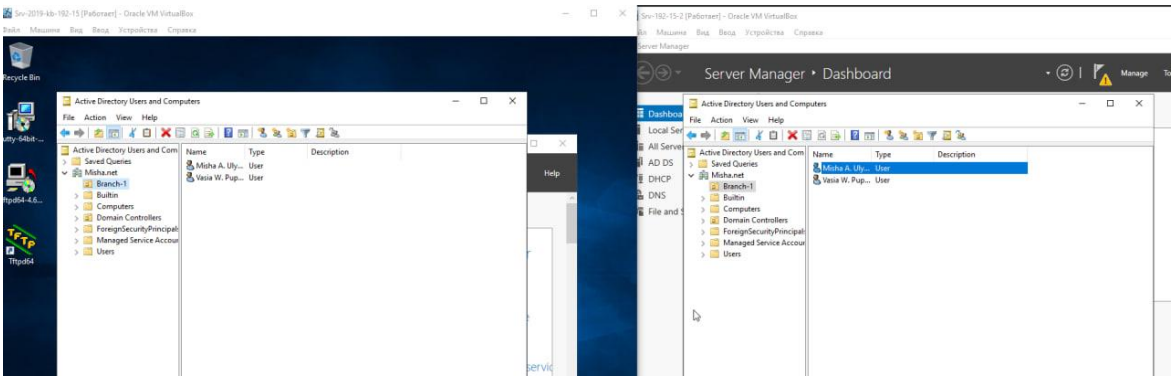


Рисунок 3.36 – Показано що реплікація працює

Далі налаштуємо Syslog server. На рисунку буде відразу показано що Syslog server працює.

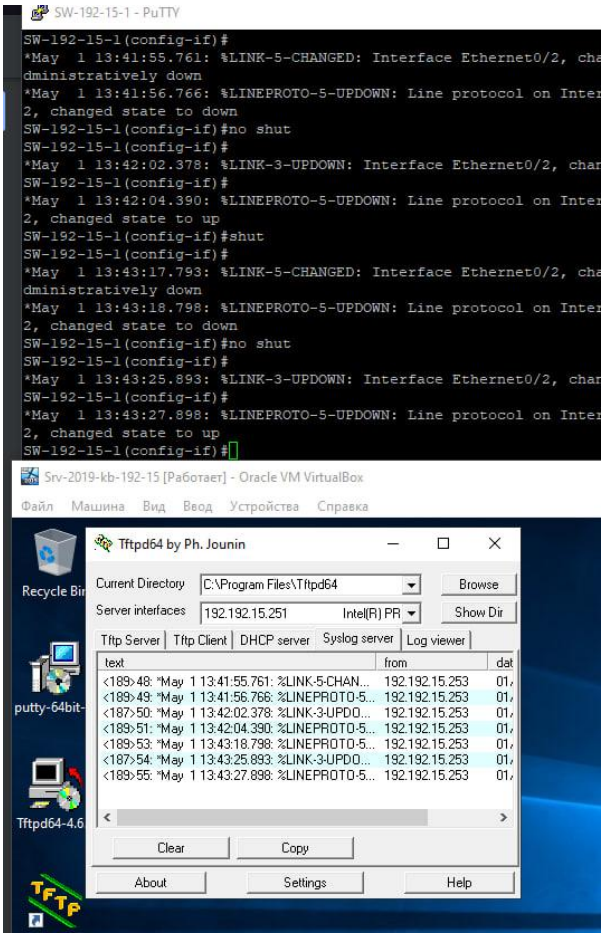


Рисунок 3.37 – Syslog проходить

Налаштовуємо kali linuks задаємо ip – address та входимо в домен, та добавляємо dns.

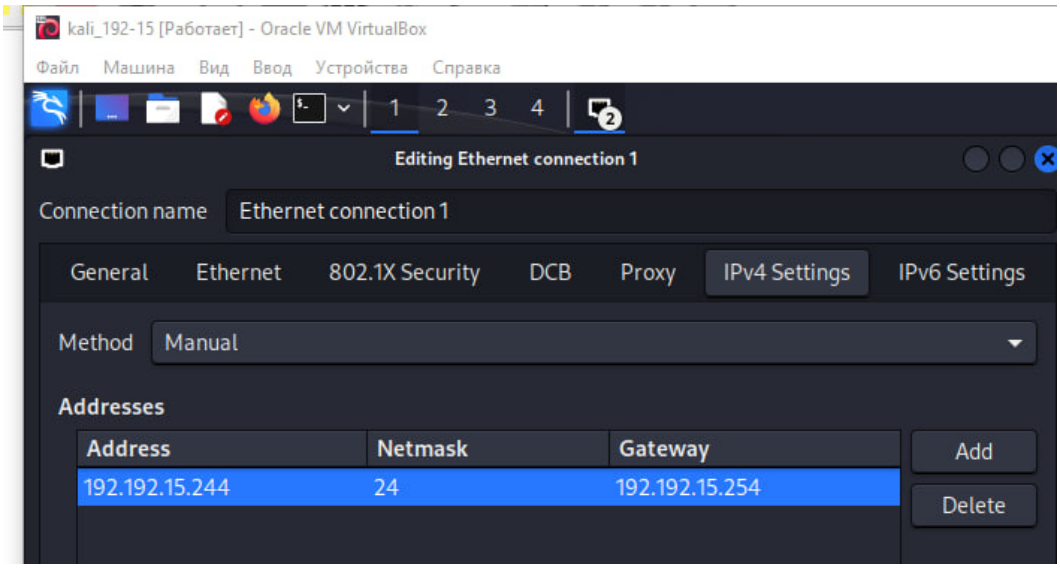


Рисунок 3.38 – Налаштований ip– addres

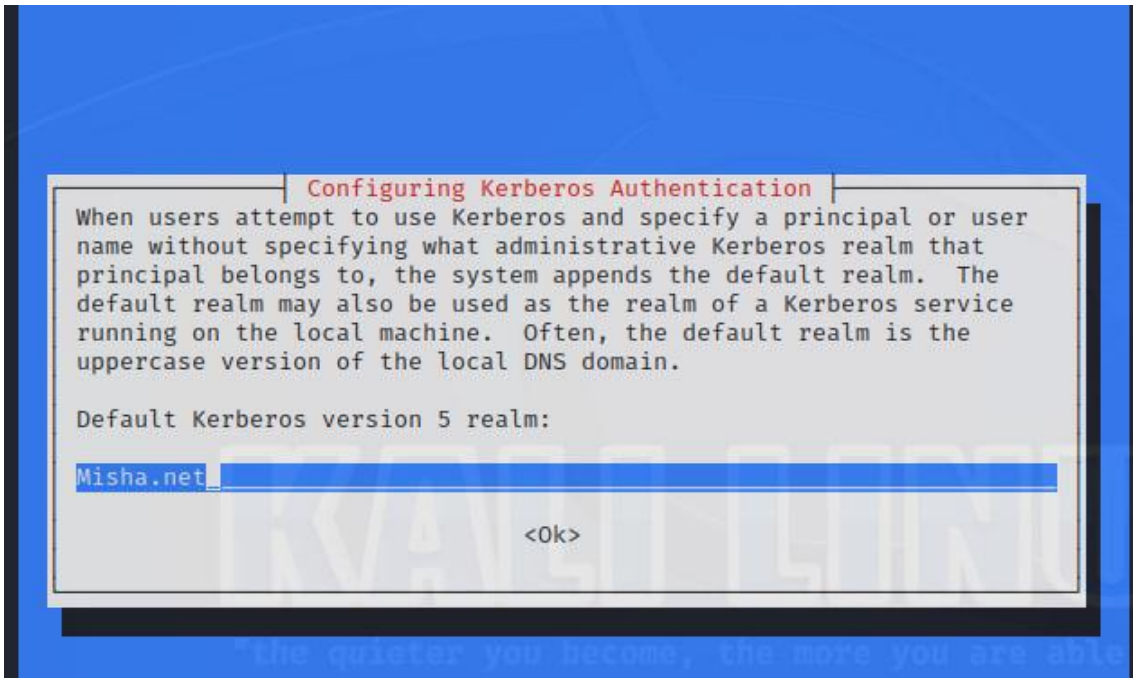


Рисунок 3.39 – Увійшли до домену



Рисунок 3.40 – У Windows Server 2019 створили зону DNS

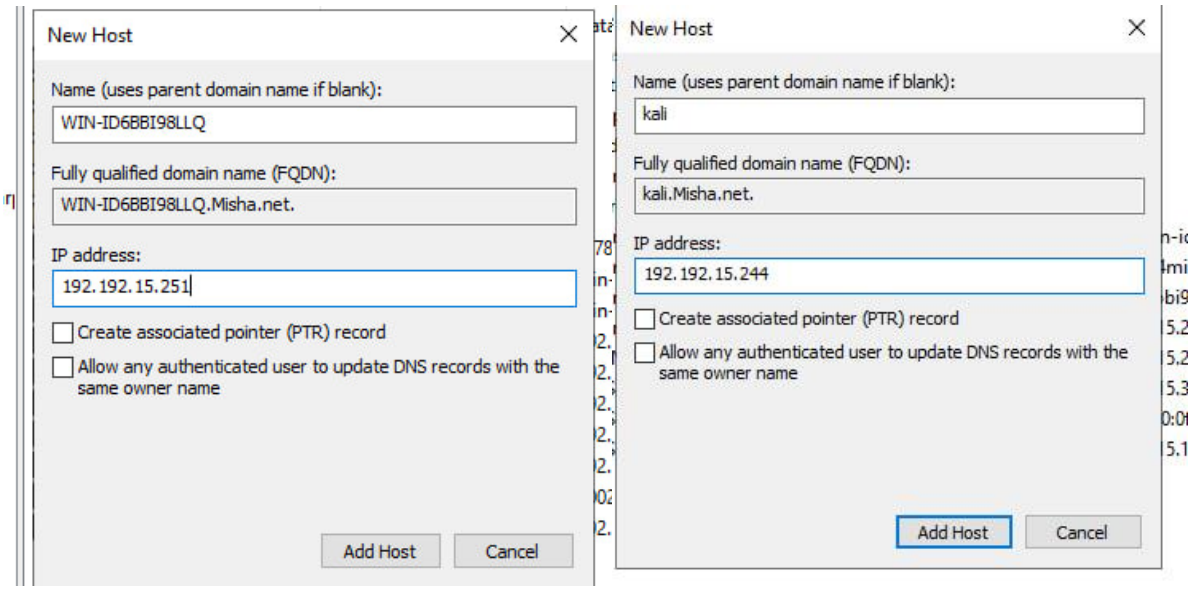


Рисунок 3.41 – Добавили хост

Тепер налаштуємо файловий сервер на Windows server, щоб виконувати роль централізованої системи зберігання, управління та надання доступу до файлів і папок у мережевому середовищі, спеціально налаштованому для Windows – платформи.

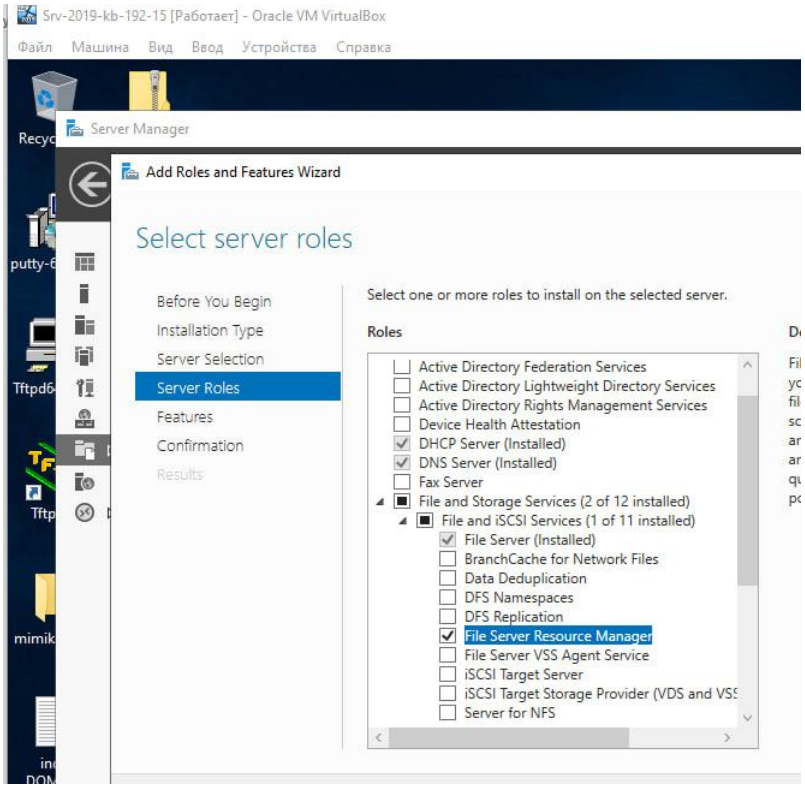


Рисунок 3.42 – Додали диспетчер ресурсів, у файловому сервісі

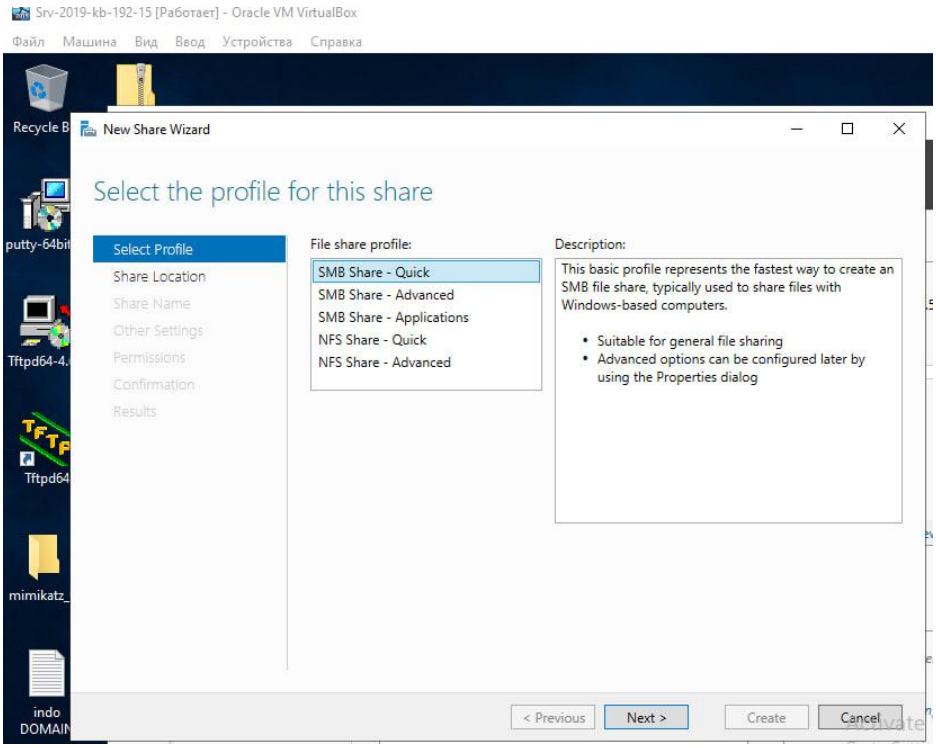


Рисунок 3.43 – Вибираємо швидкий профіль

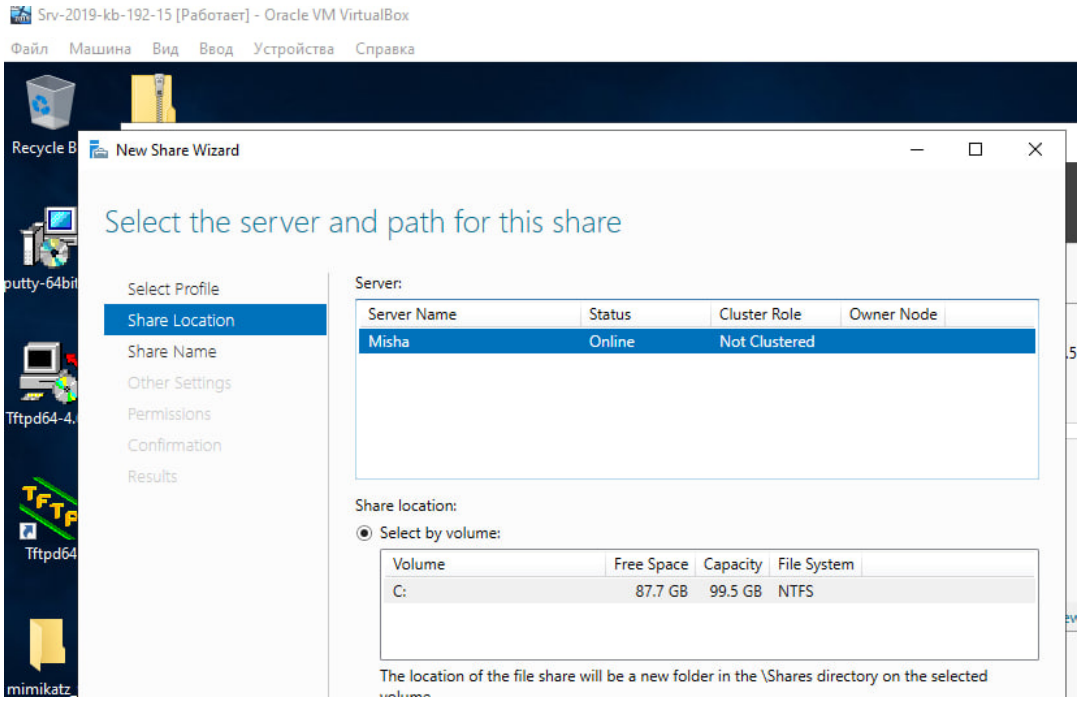


Рисунок 3.44 – Зберігаємо на диску С

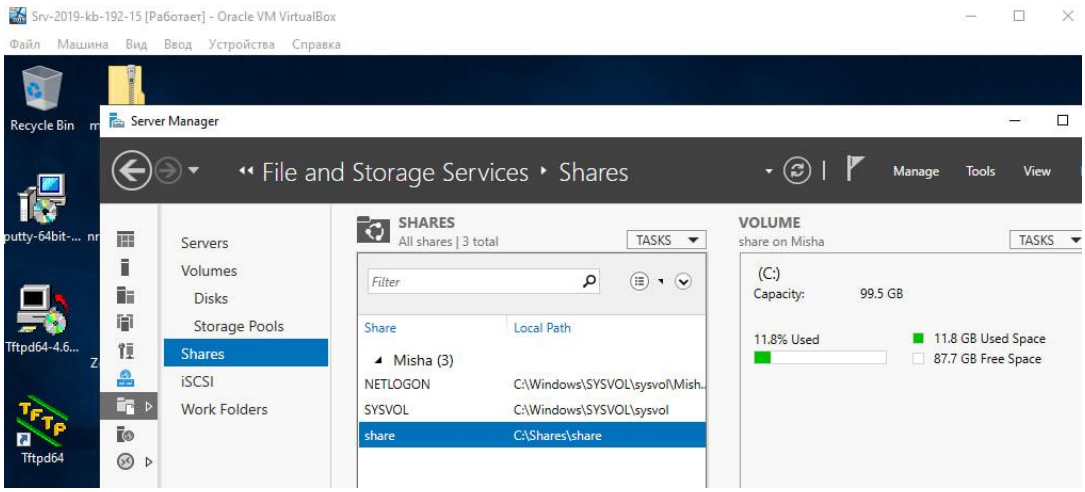


Рисунок 3.45 – Файловий сервер створений

3.3 Реалізація атаки AS – REP Roasting на Active Directory та захист від неї.

Зараз ми реалізуємо атаку на AD AS – REP Roasting, спочатку ми створимо нового користувача, задамо йому пароль та заберемо всі галочки, щоб був вільний доступ.

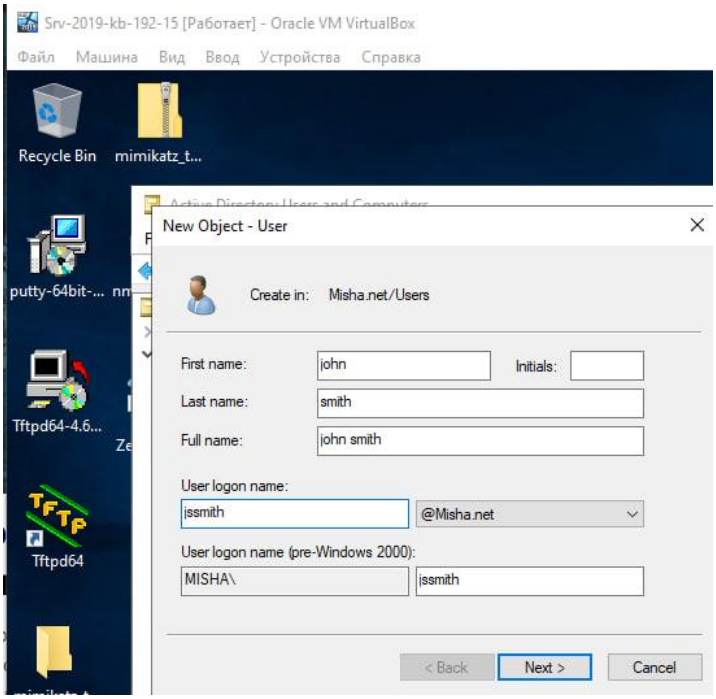


Рисунок 3.46 – Створений користувач

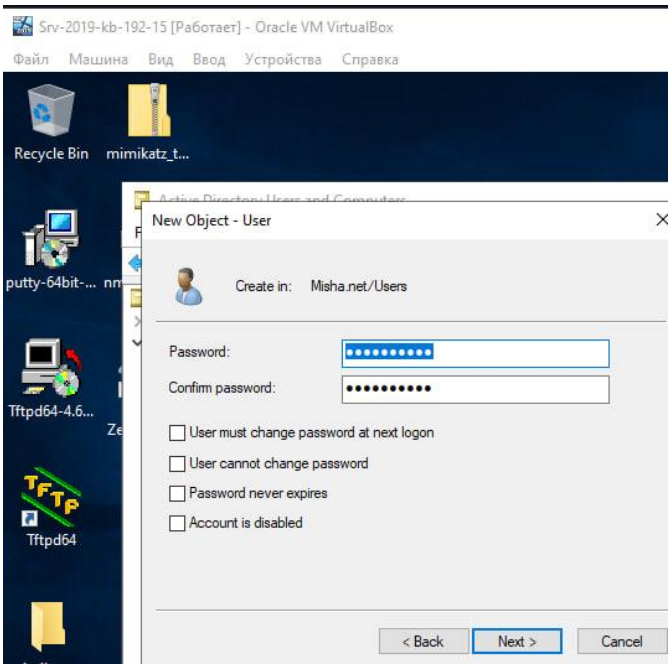


Рисунок 3.47 – Поставили пароль

Далі зайдемо в профіль користувача натиснемо прапорець не вимагати попередню аутентифікацію kerberos, щоб не бути вразливими до azrap roasting. Встановимо скрипт на kali GETNPUsers.py, знайдемо зашифрований tgt та створимо файл з паролями, щоб атака змогла підібрати пароль.

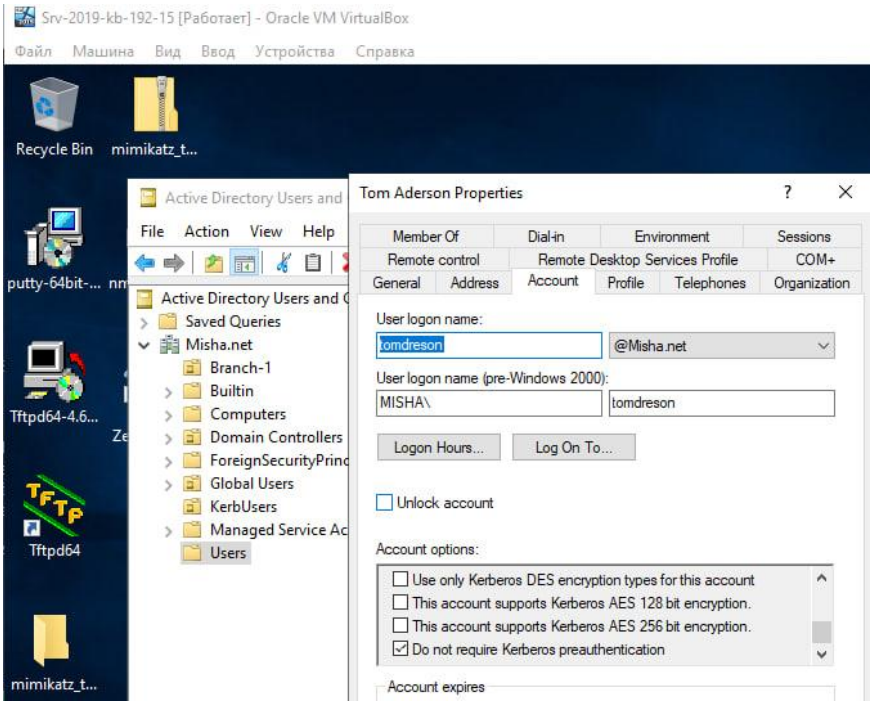


Рисунок 3.48 – Натиснули прапорець

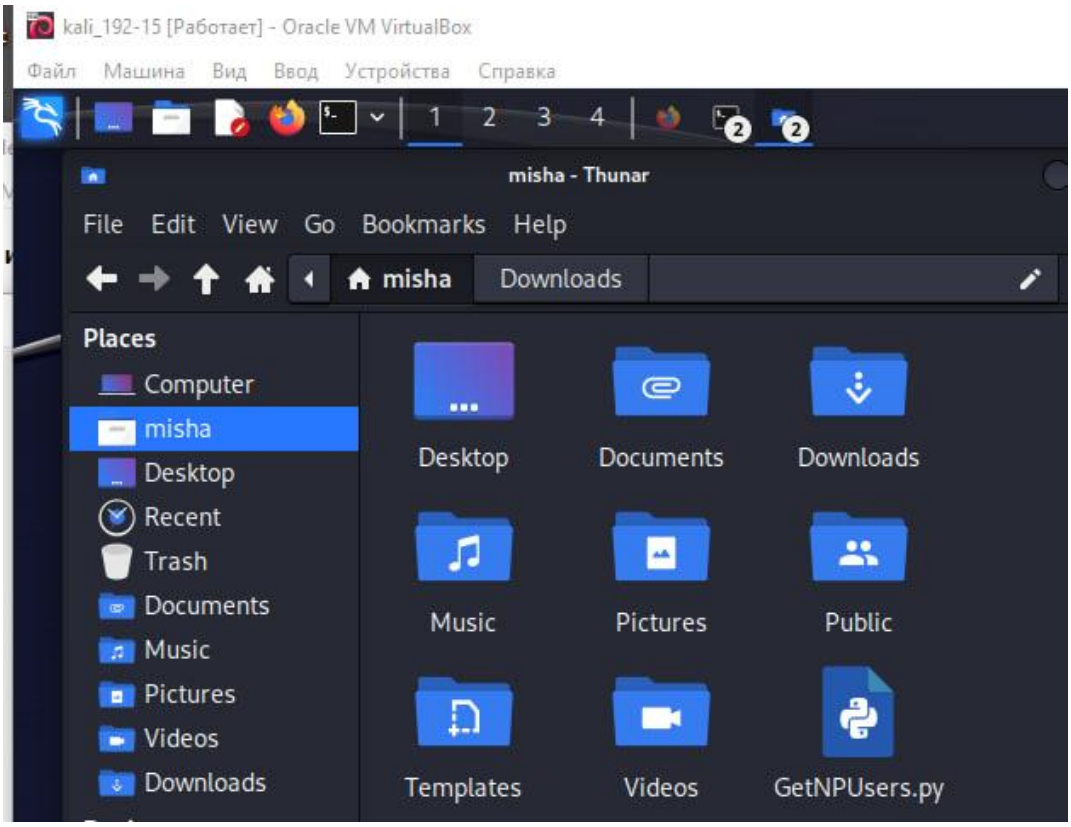


Рисунок 3.49 – Встановили скрипт

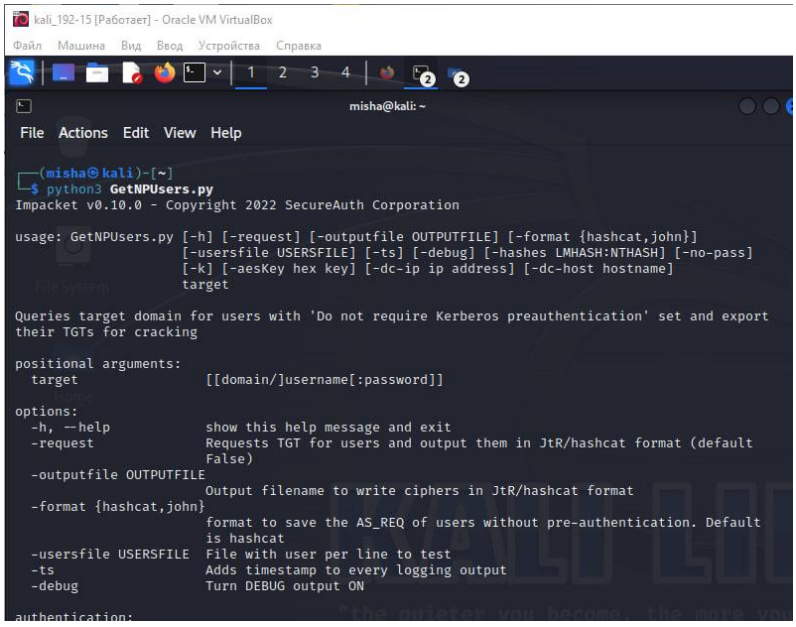


Рисунок 3.50 – Скрипт працює



Рисунок 3.51 – Знайшли зашифрований tgt

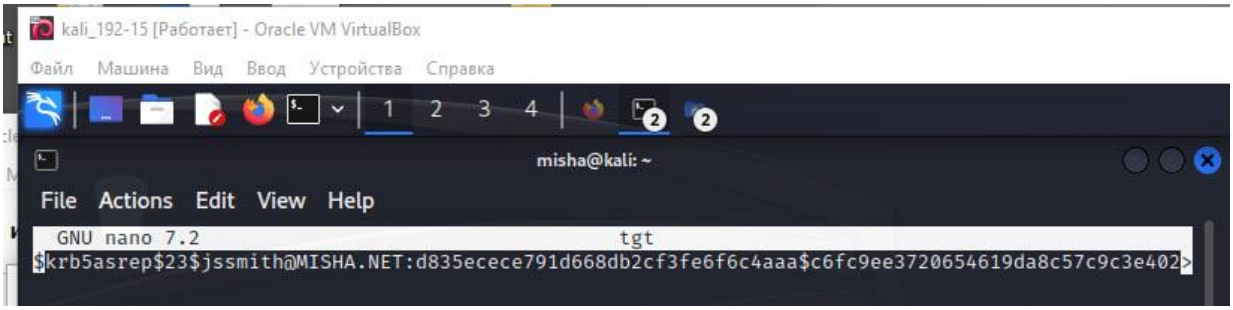


Рисунок 3.52 – Створили файл щоб добавити зашифрований tgt в nano tgt

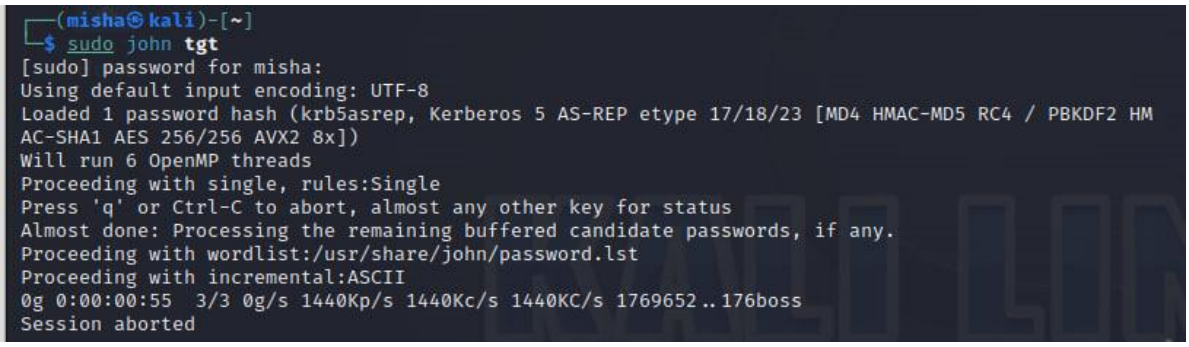


Рисунок 3.53 – Ввели команду john tgt і воно автоматично підібрало для нього формат шифрування

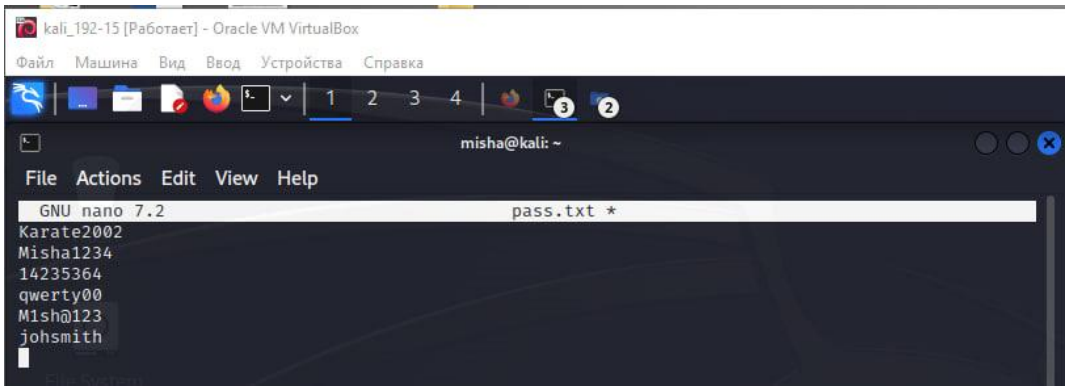


Рисунок 3.54 – Створили файл паролів

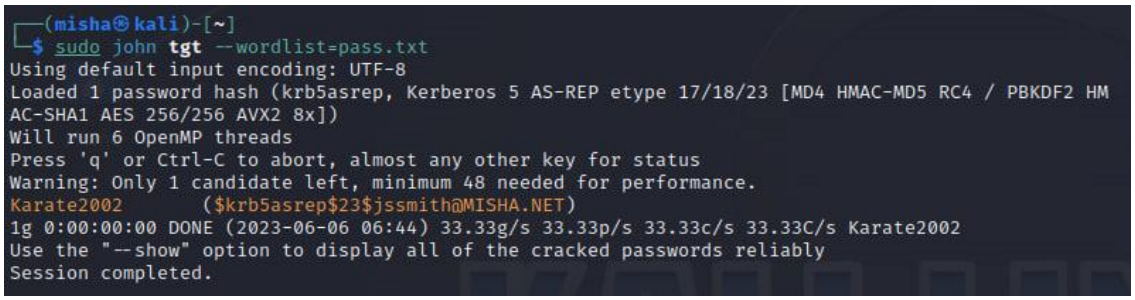


Рисунок 3.55 – Ввели команду john tgt – worldlist=pass.txt та воно зломало пароль користувача

Таким чином, атака виконана успішно, після команди john tgt – worldlist=pass.txt підібрало автоматично пароль, та зламало користувача jssmith, та показало інші функції, тепер для цієї атаки проведемо захист від злому. Для захисту ми поставимо надто складні паролі та налаштуємо групові політики паролів.

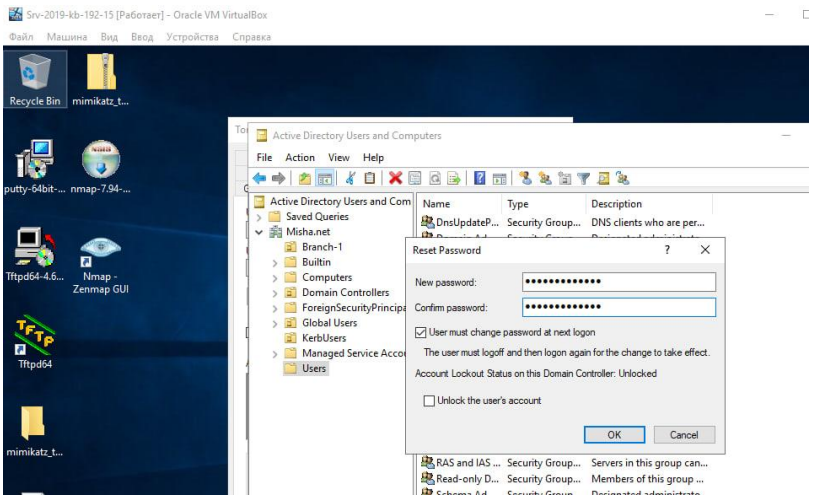


Рисунок 3.56 – Змінили пароль на складний K@@r@te2oo211

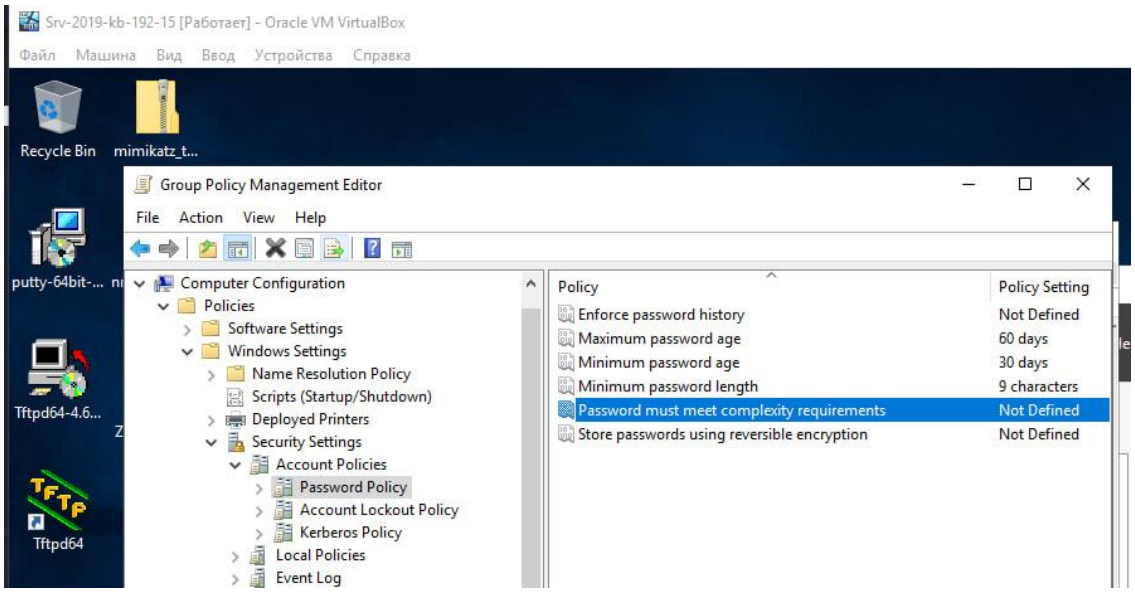


Рисунок 3.57 – Налаштували політику паролів

Спробуємо ще раз ввести команду john tgt – worldlist=pass.txt, та атака не буде спарцьована, пароль не підібрано, та поставимо галочку користувач має змінити пароль при наступному вході.

```
┌──(misha㉿kali)-[~]
└─$ sudo john tgt --wordlist=pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HM
AC-SHA1 AES 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)
```

Рисунок 3.58 – Не може підібрати пароль

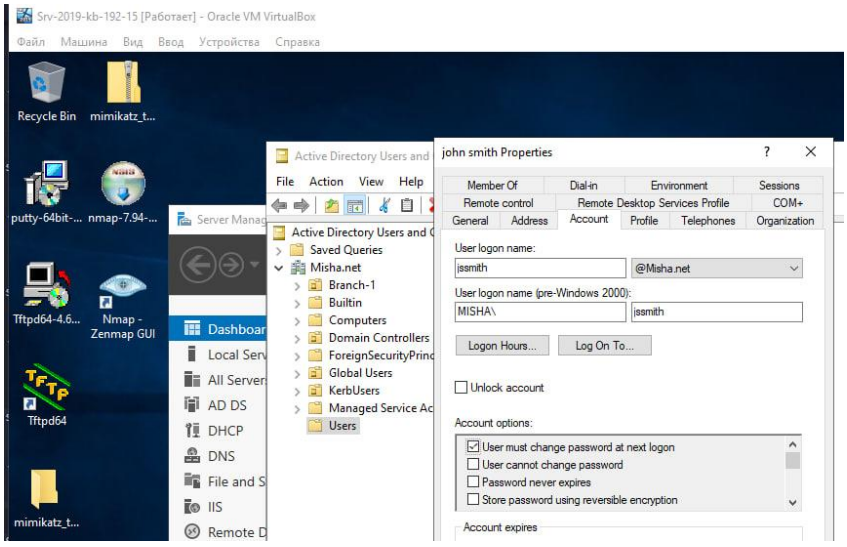


Рисунок 3.59 – Поставили галочку

```
┌──(misha㉿kali)-[~]
└─$ python3 GetNPUsers.py Misha.net/jssmith -dc-ip=192.192.15.251
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Cannot authenticate jssmith, getting its TGT
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
```

Рисунок 3.60 – не виконується команда

Отже, після того, як ми поставили галочку, що користувач має змінити пароль при наступному вході, атака не може бути спрацьована.

3.4 Реалізація атаки DHCP starvation attack, та DHCP Spoofing на Active Directory та захист від них.

Для атаки DHCP starvation спочатку потрібно встановити застосунок Yersinia на kali linuks, далі потрібно провести атаку типу DHCP Starvation/DHCP Exhaustion.

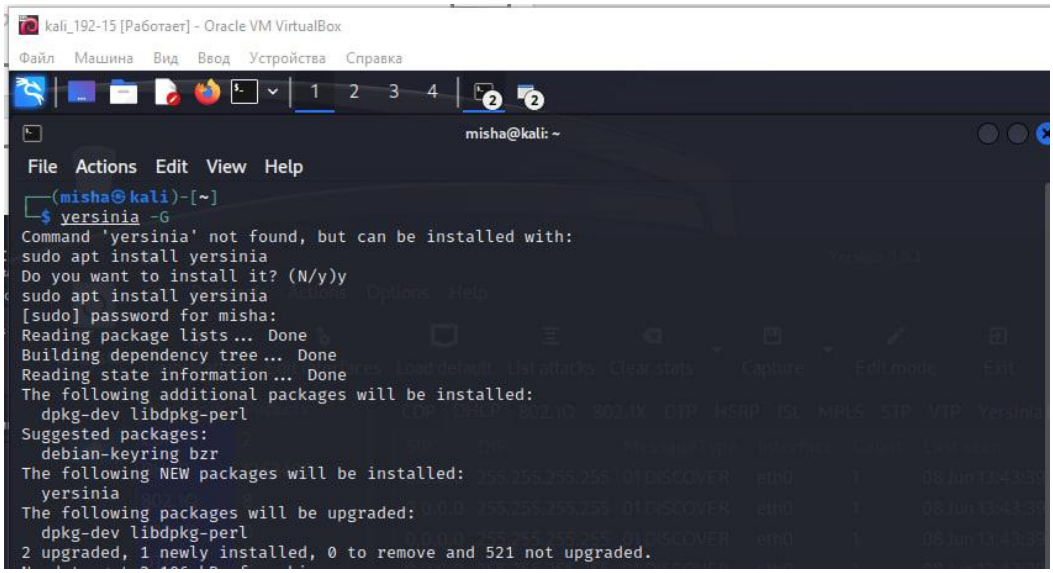


Рисунок 3.61 – встановлений застосуно

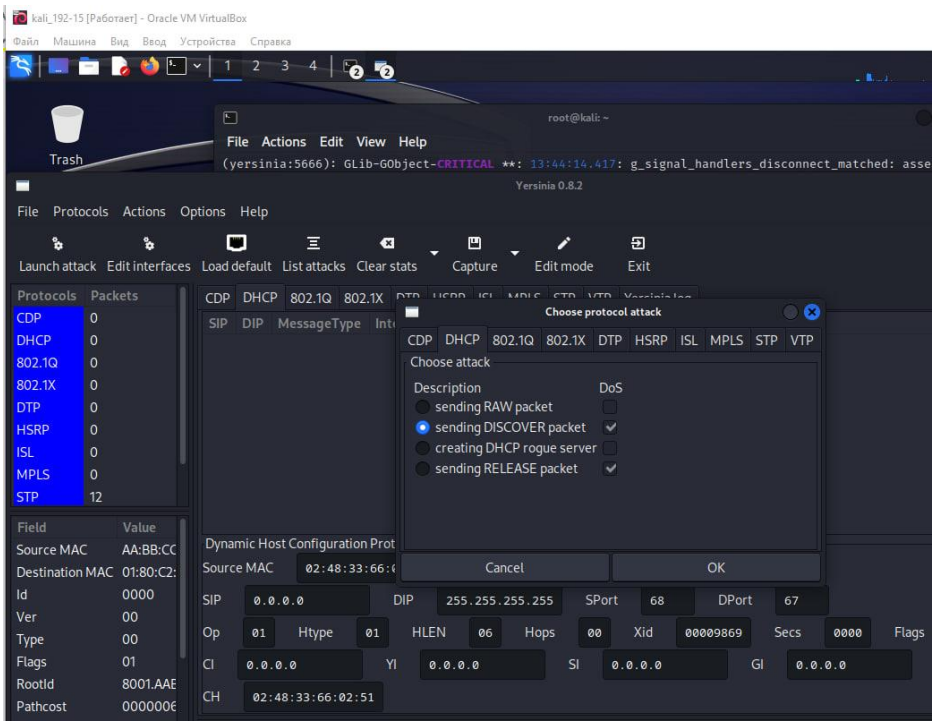


Рисунок 3.62 – нажали sending discover packet

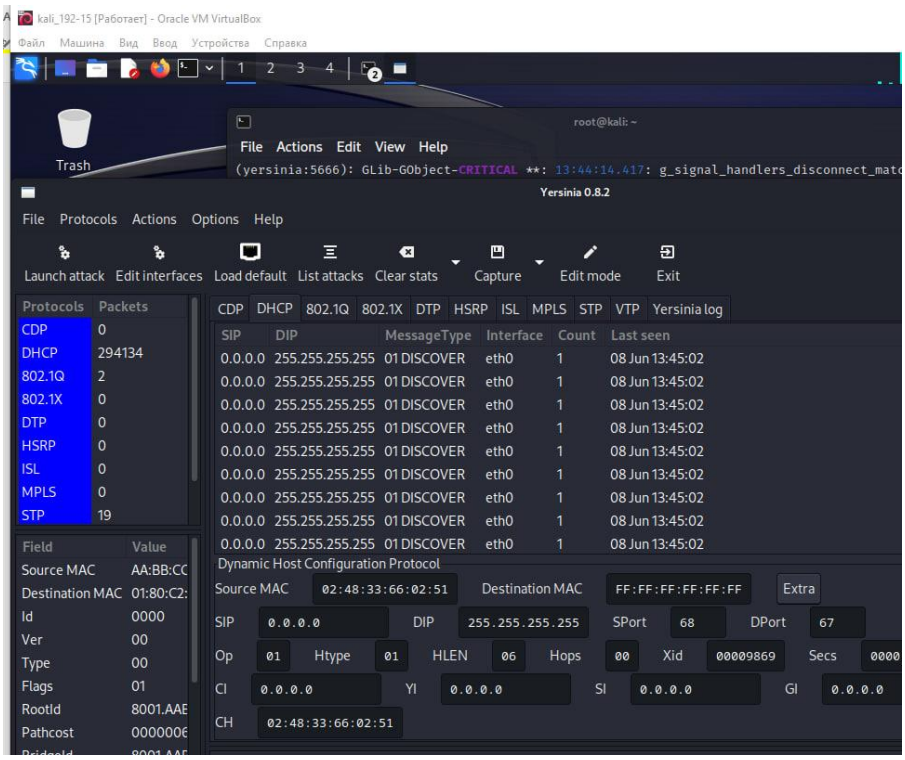


Рисунок 3.63 – DHCP

Як бачимо, весь доступний діапазон IP – адрес був призначений «неіснуючим» MAC – адресам. І тепер легальні робочі станції не зможуть отримати MAC – адресу.

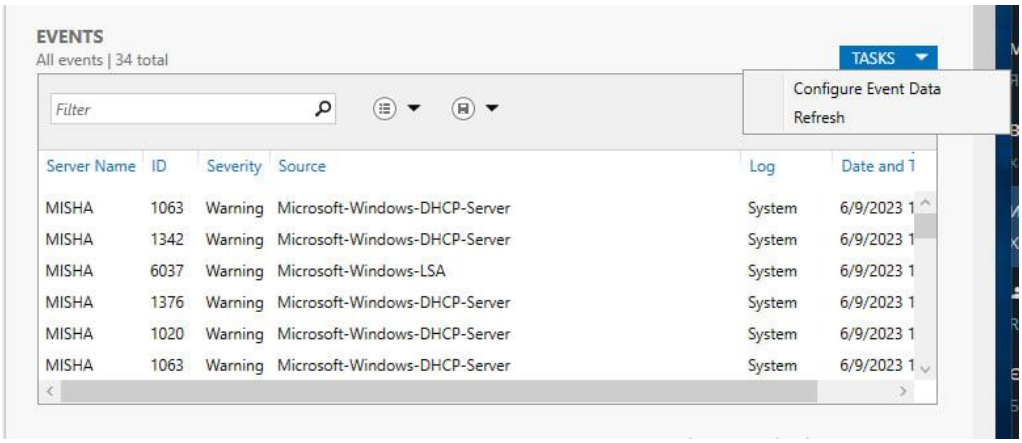


Рисунок 3.64 – Нажали refresh

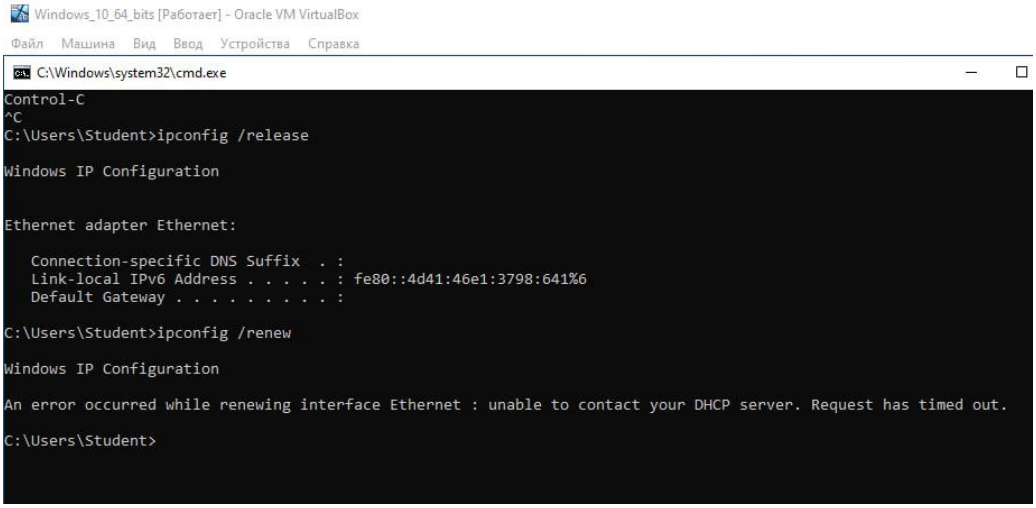


Рисунок 3.65 – атака спрацьована

Ми бачимо що DHCP не надсилається, отже атака спрацьована успішно, далі ми зупинимо роботу Yersinia та спробуємо знову прописати ipconfig /renew, побачимо що пакети DHCP будуть надходить. Тому після відключення Yersinia атака не спрацює.

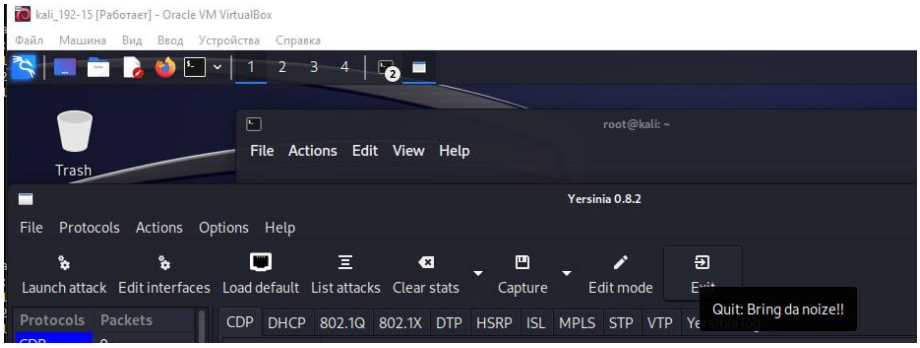


Рисунок 3.66 – Відключили Yersinia

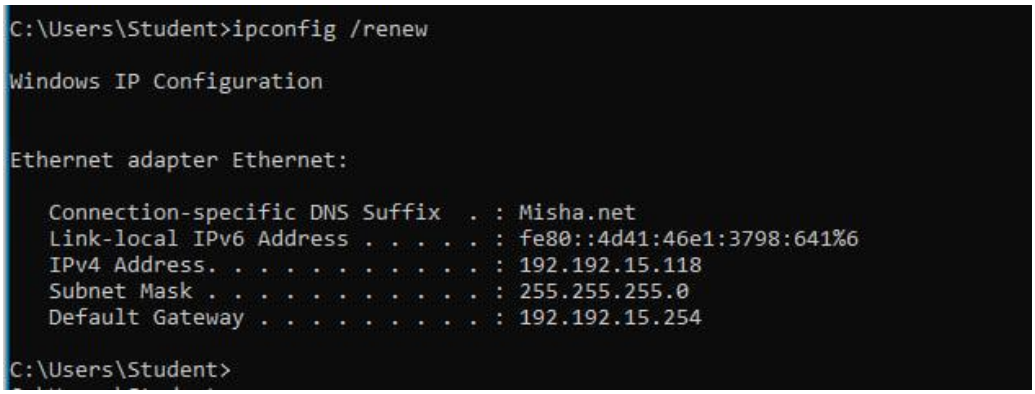


Рисунок 3.67 – DHCP знову працює

Для наступної атаки нам спочатку потрібно встановити застосунок Ettercap, далі створимо фальшивий DHCP сервер та покажемо що атака буде спрацьована.

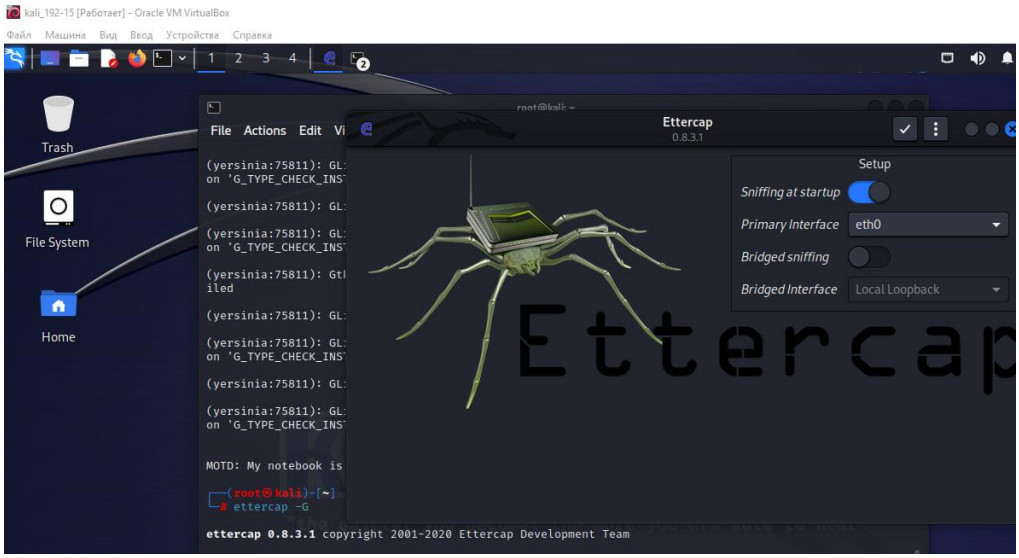


Рисунок 3.68 – Запустили застосунок

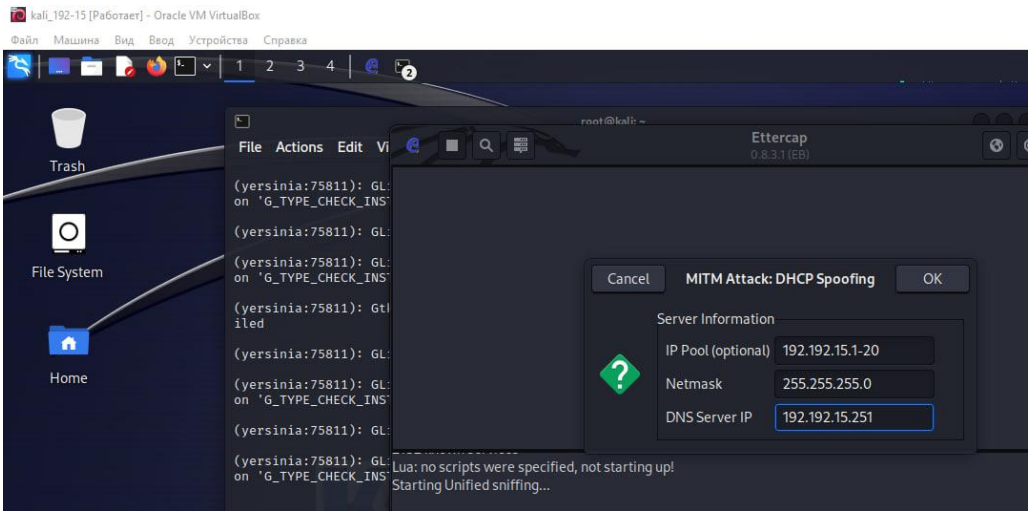


Рисунок 3.69 – Створили фальшивий DHCP сервер

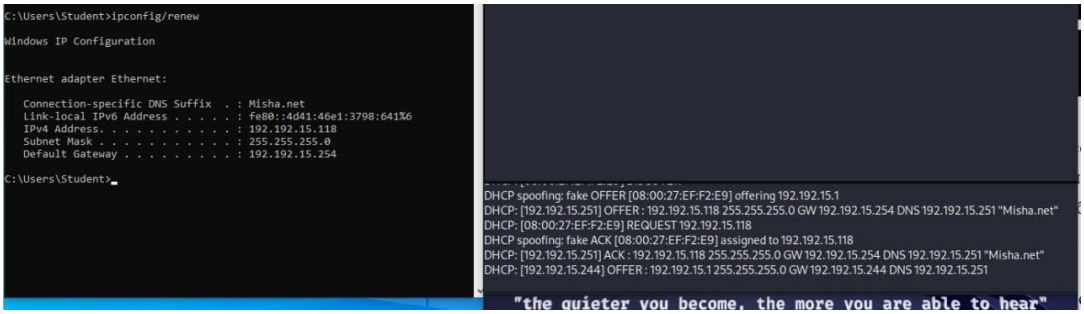


Рисунок 3.70 – Атака спрацьована успішно

Далі ми налаштуємо захист від атаки DHCP starvation attack та DHCP Spoofing, для захисту ми налаштуємо port– security SW – 192 – 15 – 1 та SW – 192 – 15– 2 та налаштуємо DHCP – Snooping.

```
SW-192-15-1(config)#int range eth0/2, eth0/3, eth1/0
SW-192-15-1(config-if-range)#switchport mode access
SW-192-15-1(config-if-range)#switchport port-security
SW-192-15-1(config-if-range)#switchport port-security mac-address sticky
SW-192-15-1(config-if-range)#
```

```
SW-192-15-2(config)#int range eth0/1, eth0/2, eth1/0
SW-192-15-2(config-if-range)#switchport mode access
SW-192-15-2(config-if-range)#switchport port-security
SW-192-15-2(config-if-range)#switchport port-security mac-address sticky
SW-192-15-2(config-if-range)#
```

Рисунок 3.71 – Налагодженний port– security на інтерфейсах SW– 1 та SW– 2

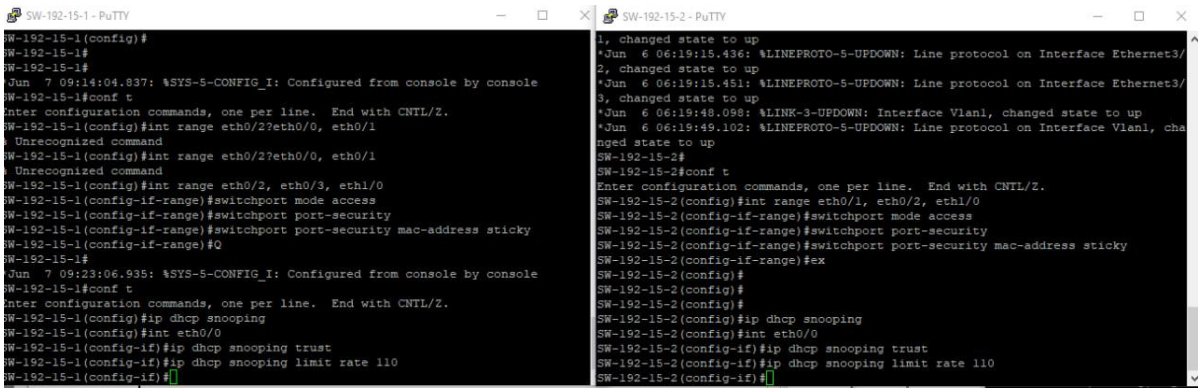


Рисунок 3.72 – Налагодження DHCP– Snoopin

Ми покажемо що після налаштування захисту, захист від 2 атак був спрацьований успішно рис. 3.73– 3.74.

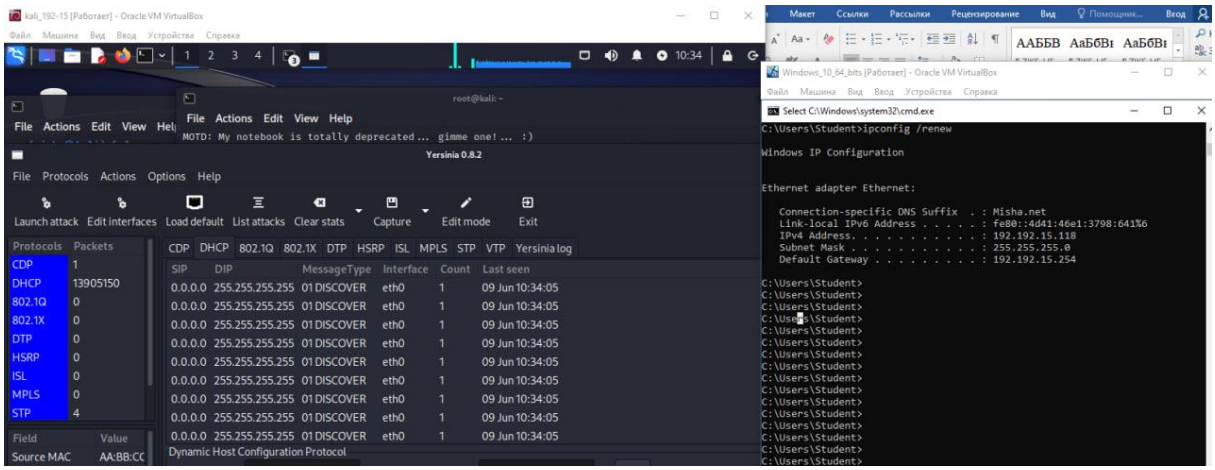


Рисунок 3.73 – Захист спрацьований

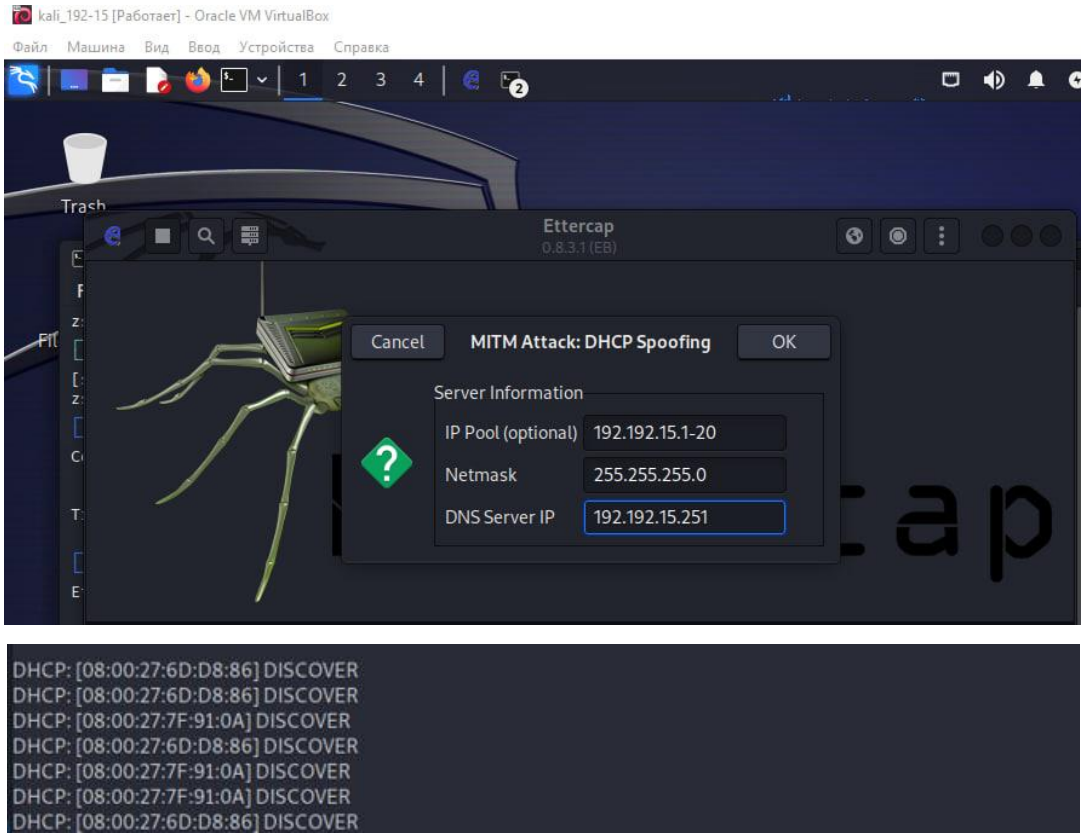


Рисунок 3.74 – Захист спрацьований

Висновки до третього розділу:

У цьому розділі ми показали налаштування різних параметрів, таких як ip адреси, ssh, ntp, syslog, динамічна аутентифікація, реплікацію, в розділі виконано 3 атаки, показали як працюють атаки, та які потрібні утиліти для них, та як правильно захищатись від атак.

ВИСНОВКИ

В даній кваліфікаційній роботі була спроєктована модель клієнт – серверної мережі. Для побудови мережі ми використали технології від компанії CISCO, також ми обрали графічний емулятор GNS3,Windows server 2019, Kali Linuks.

В першому розділі було досліджено принципи роботи клієнт – серверної мережі, та її ролі, ми вивчили як працює Active Directory, розглянули які є види атак на AD, ознайомилися з цими атаками та розглянули які є захисти від них.

В другому розділі було описано клієнт – серверну мержу. Складено таблицю параметрів підключень мережевих пристроїв, описані пристрої комп'ютерної мережі, її характеристика та параметри, розділили мережу на рівень ядра, рівень доступу, та рівень розподілу. Розглянули які є моделі загроз, та використали модель загроз, побудували модель загроз, визначили конкретні загрози клієнт – серверної мережі, критичні елементи підсистеми, визначили різні потоки даних в системі, побудували діаграму загроз для системи. Для побудови діаграми загроз, ми використали модель Stride, вона складається з таких елементів як Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

В третьому розділі виконали налаштування пристроїв мережі, виконали налаштування в мережі, та Active Directroty, налаштували основні функції, всі комп'ютери отримали динамічну адресу від сервера DHCP. Показали налаштування 3 атак, та показали що всі атаки були проведені та виконані успішно, налаштували захист від цих атак та показали що цей захист працює.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Клієнт– серверна архітектура та ролі серверів [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@IvanZmerzlyi/клієнт– серверна– архітектура– та– ролі– серверів– 9893d8048229

2. What is Active Directory and how does it work [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchwindowsserver/definition/Active– Directory

3.What is Kerberos [Електронний ресурс] – Режим доступу до ресурсу: https://web.mit.edu/kerberos/

4. Top 10 Active Directory Attack Methods [Електронний ресурс] – Режим доступу до ресурсу: https://www.lepide.com/blog/top– 10– active– directory– attack– methods/

5.Опис Маршрутизатора Cisco 7201 [Електронний ресурс] – Режим доступу до ресурсу: https://stack– systems.com.ua/marshrutizator– cisco– 7201

6. Cyber Kill Chain Model in Cyber Threat Intelligence [Електронний ресурс] – Режим доступу до ресурсу: https://socradar.io/cyber– kill– chain– model– in– cyber– threat– intelligence/

7. What Is DHCP Snooping and How It Works? [Електронний ресурс] – Режим доступу до ресурсу: https://community.fs.com/blog/what– is– dhcp– snooping– and– how– it– works.html

8. Threat Modeling Process | OWASP Foundation [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www– community/Threat_Modeling_Process

9. F. Swiderski and W. Snyder, Threat modeling. Redmond, Wash.: Microsoft Press, 2004, ст. 67– 73.

10. Microsoft Windows Server 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://itpro.ua/product/Microsoft-windows-server-2019-standard/?tab=description

11.Захист від атак [Електронний ресурс] – Режим доступу до ресурсу: https://www.taxtalks.com.au/asset-protection/

12. Світч IBM 2498-B40 [Електронний ресурс] – Режим доступу до ресурсу: https://servak.com.ua/ua/kommutator/svitch-ibm-2498-b40-40-port.html

13. Attack Defense & Detection [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?page_id=4031

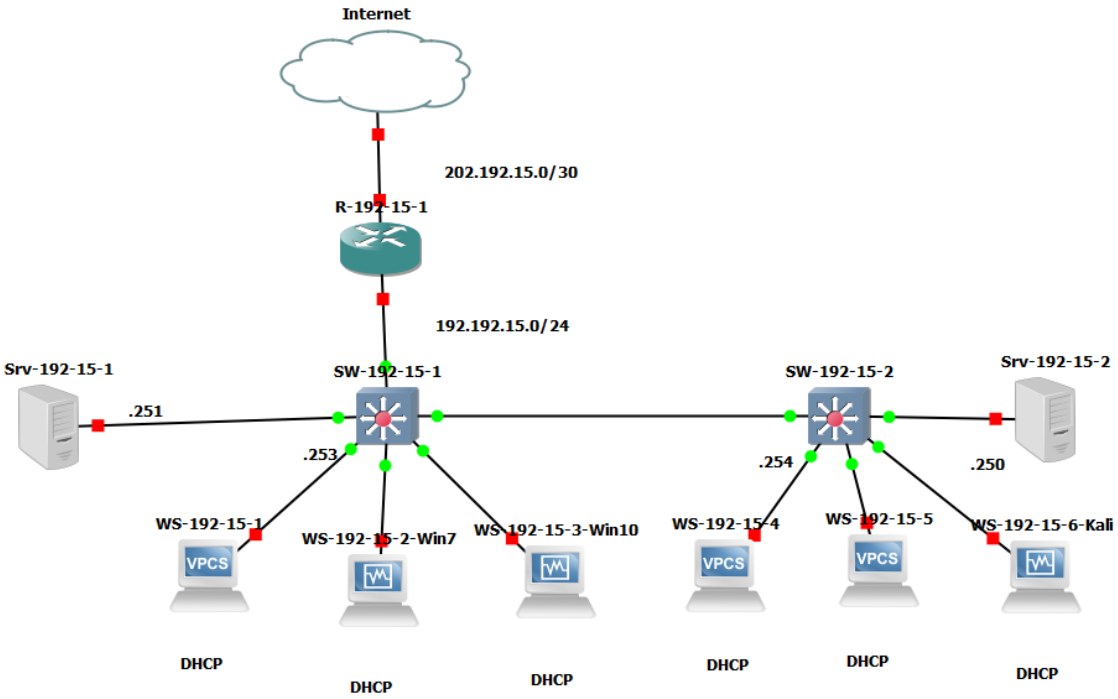
14. Why BloodHound? [Електронний ресурс] – Режим доступу до ресурсу: https://www.crowdstrike.com/blog/how-to-block-bloodhound-attacks/

15. Password Spraying [Електронний ресурс] – Режим доступу до ресурсу: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

16. What is in the MITRE ATT&CK Matrix? [Електронний ресурс] – Режим доступу до ресурсу: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

ДОДАТКИ

Додаток А – Детальна схема побудованої мережі



Додаток Б. Конфігураційні файли окремих пристроїв

```
Internet#show run
Building configuration...

Current configuration : 2220 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 202.192.15.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 qwerty123
 duplex half
!
interface Ethernet1/1
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/4
 no ip address
 shutdown
 duplex half
!
```

```
interface Ethernet1/5
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/6
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/7
 no ip address
 shutdown
 duplex half
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 19215
 log-adjacency-changes
 passive-interface Ethernet1/1
 network 192.192.15.0 0.0.0.255 area 0
 network 202.192.15.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
End

R-192-15-1#show run
Building configuration...
```

```
Current configuration : 2539 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-192-15-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$R6d8$wIFUeVTm5Zl5wxmnQs71D1
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name Misha.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 password 0
passAdmin
archive
 log config
  hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 202.192.15.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 qwerty123
 duplex half
!
interface Ethernet1/1
 ip address 192.192.15.254 255.255.255.0
 duplex half
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/4
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/5
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/6
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/7
 no ip address
```

```
 shutdown
 duplex half
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 19215
 log-adjacency-changes
 passive-interface Ethernet1/1
 network 192.192.15.0 0.0.0.255 area 0
 network 202.192.15.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
logging trap notifications
logging 192.192.15.251
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
ntp update-calendar
ntp server 192.192.15.251
end

SW-192-15-1#show run
Building configuration...

Current configuration : 2384 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
service compress-config
!
hostname SW-192-15-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
0lHJ.OKIF0c/lcKJEPmnu/NB41omYri341J2
9qbJmIs
!
username admin privilege 15 password 0
passAdmin
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name Misha.net
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 duplex auto
 ip dhcp snooping limit rate 110
 ip dhcp snooping trust
!
interface Ethernet0/1
 duplex auto
 ip dhcp snooping limit rate 110
 ip dhcp snooping trust
!
interface Ethernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 duplex auto
!
interface Ethernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.279e.2740
 duplex auto
!
interface Ethernet1/0
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.27ef.f2e9
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
```

```
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 ip address 192.192.15.253 255.255.255.0
!
ip default-gateway 192.192.15.254
!
no ip http server
!
!
logging trap notifications
logging host 192.192.15.251
!
!
!
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
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
ntp update-calendar
ntp server 192.192.15.251
end

SW-192-15-2#show run
Building configuration...

Current configuration : 2267 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-192-15-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
0lHJ.OKIF0c/lcKJEPmnu/NB41omYri341J2
9qbJmIs
!
username admin privilege 15 password 0
passAdmin
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name Misha.net
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
```

```
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
!
!
!
interface Ethernet0/0
 duplex auto
 ip dhcp snooping limit rate 110
 ip dhcp snooping trust
!
interface Ethernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 duplex auto
!
interface Ethernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 duplex auto
!
interface Ethernet0/3
 duplex auto
!
interface Ethernet1/0
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.2728.3ba2
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 duplex auto
!
interface Ethernet3/1
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
interface Vlan1
 ip address 192.192.15.252 255.255.255.0
!
ip default-gateway 192.192.15.254
!
no ip http server
!
!
logging trap notifications
logging host 192.192.15.251
!
!
!
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
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
ntp update-calendar
ntp server 192.192.15.251
```

```
end
```