

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 магістра

на тему: «Методи та технології тестування на проникнення мережної  
інфраструктури на базі Microsoft Active Directory»

Виконав студент 2-го курсу, групи КБм-22-1  
спеціальності 125 «Кібербезпека»

 М.В. Куліш

Керівник доцент кафедри комп'ютерної інженерії та  
кібербезпеки, кандидат педагогічних наук, доцент

 О.С. Головня

Рецензент професор кафедри комп'ютерної інжене-  
рії та кібербезпеки, доктор технічних наук, доцент

 В.В. Воротніков

Житомир – 2024

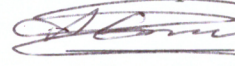
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 125 «Кібербезпека»  
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

## ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Куліш Михайло Валентинович

Тема роботи: **«Методи та технології тестування на проникнення мережної інфраструктури на базі Microsoft Active Directory»**

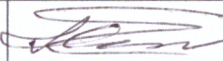
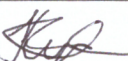
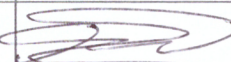
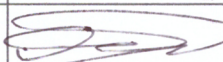
затверджена Наказом університету від 5 березня 2024 р. № 96/с

Термін здачі студентом закінченої роботи 29 квітня 2024 р.

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

1. Розроблено технічні вимоги до проекту
2. Розроблено топологію мережі та структуру домену Active Directory
3. Розгортання Active Directory на Windows Server 2019 Enterprise
4. План тестування на проникнення

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

| Розділ | Консультант   | Підпис, дата                                                                              |                                                                                             |
|--------|---------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
|        |               | Завдання видав                                                                            | Завдання прийняв                                                                            |
| 1      | А.А. Єфіменко |  5.03.24 |  5.03.24 |
| 2      | А.А. Єфіменко |  5.03.24 |  5.03.24 |
| 3      | А.А. Єфіменко |  5.03.24 |  5.03.24 |

Керівник



### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи               | Термін виконання етапів роботи | Примітка |
|-------|-------------------------------------------------------------|--------------------------------|----------|
| 1     | Аналіз отриманого завдання та уточнення поставлених завдань |                                | Виконано |
| 2     | Аналіз літературних джерел                                  |                                | Виконано |
| 3     | Аналіз об'єкта дослідження                                  |                                | Виконано |
| 4     | Вибір технології для реалізації                             |                                | Виконано |
| 5     | Налаштування мережі                                         |                                | Виконано |
| 6     | Адміністрування мережі                                      |                                | Виконано |
| 7     | Проведення сканування та проведення атаки                   |                                | Виконано |
| 8     | Оформлення пояснювальної записки                            |                                | Виконано |
|       | Захист                                                      |                                | Виконано |

Студент  М.В. Куліш

Керівник  О.С. Головня

## АНОТАЦІЯ

Кваліфікаційна робота складається з проекту в якому розглянуто методи та технології тестування на проникнення мережевої інфраструктури на базі Microsoft Active Directory. Пояснювальна записка містить 93 сторінок, 85 рисунка та 1 таблиця.

**Метою кваліфікаційної роботи є** вивчення сучасних методів та технологій тестування на проникнення на проникнення мережної інфраструктури на базі Active Directory задля розробки ефективного та високопродуктивного підходу до забезпечення безпеки корпоративної мережі.

Проаналізувавши основні вимоги технічного завдання та особливості побудови мережі вибрали мережеві пристрої для організації роботи мережі. Було наведено технічні характеристики вибраного обладнання та вдало розгорнуто AD на DC98. Було побудовано та налагоджено надійну мережу.

Проаналізовано функції мережевого екрану pfSense та Windows Server. Це дало розуміння поставленої задачі та визначило подальші дії для проектування мережі організації. Розробили проект корпоративної мережі організації. Розроблено структуру ядра глобальної мережі, наведено обґрунтування вибору міжмережного екрану, маршрутизатора, віртуального комутатора Hyper-V. Для побудованої мережі налагоджено DHCP-сервер, також можливість керувати pfSense за допомогою Веб-інтерфейсу тільки адміністратуру з робочої станції WS-ADMIN. Створено структуру домену cultoffillusion.local. Проведено сканування та атаку.

**Ключові слова:** ACTIVE DIRECTORY МЕРЕЖНИЙ ЕКРАН, ВІРТУАЛЬНИЙ КОМУТАТОР, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ.

## ANNOTATION

The qualification work consists of a project that considers methods and technologies for penetration testing of network infrastructure based on Microsoft Active Directory. The explanatory note contains 93 pages, 85 figures and 1 table.

The purpose of the qualification work is to study modern methods and technologies for penetration testing of network infrastructure based on Active Directory in order to develop an effective and high-performance approach to ensuring the security of a corporate network.

After analyzing the main requirements of the technical task and the features of network construction, we selected network devices for organizing the network. The technical characteristics of the selected equipment were provided and AD was successfully deployed on DC98. A reliable network was built and configured.

The functions of the pfSense firewall and Windows Server were analyzed. This gave an understanding of the task and determined further actions for designing the organization's network. Developed a project of the organization's corporate network. The structure of the core of the global network was developed, the choice of a firewall, router, and Hyper-V virtual switch was justified. For the built network, a DHCP server was configured, as well as the ability to manage pfSense using the Web interface only by the administration from the WS-ADMIN workstation. The structure of the cultoffillusion.local domain was created. The scanning and attack are carried out.

**Keywords:** ACTIVE DIRECTORY FIREWALL, VIRTUAL SWITCH, PENETRATION TESTING.



## ЗМІСТ

|                                                                                                                               |    |
|-------------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП .....                                                                                                                   | 9  |
| РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА<br>ПРОНИКНЕННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ACTIVE<br>DIRECTORY ..... | 11 |
| 1.1 Загальна концепція тестування на проникнення .....                                                                        | 11 |
| 1.2 Архітектура та принципи роботи AD .....                                                                                   | 12 |
| 1.3. Автентифікація в Active Directory .....                                                                                  | 15 |
| 1.3.1. Протокол автентифікації NTLM .....                                                                                     | 18 |
| 1.3.2 Протокол автентифікації Kerberos .....                                                                                  | 20 |
| 1.4. Огляд атак на Active Directory .....                                                                                     | 25 |
| 1.4.1 Kerberoasting .....                                                                                                     | 25 |
| 1.4.2 Атака password spraying .....                                                                                           | 28 |
| 1.4.3 Атака Golden Ticket .....                                                                                               | 29 |
| 1.4.4 Pass-the-hash .....                                                                                                     | 30 |
| 1.4.5 Атака LLMNR/NBT-NS отруєння та ретрансляція SMB (SMB relay) .....                                                       | 31 |
| 1.5. Аналіз методів та технологій для пентесту AD .....                                                                       | 32 |
| РОЗДІЛ 2. ПОБУДОВА ТА НАЛАГОДЖЕННЯ МЕРЕЖЕВОГО СЕРЕДОВИЩА<br>НА БАЗІ VMWARE, PFSENSE ТА РОЗГОРТАННЯ ACTIVE DIRECTORY .....     | 35 |
| 2.1 Створення віртуального мережевого середовища. ....                                                                        | 35 |
| 2.2 Створення віртуальних комутаторів Nupur-V та налагодження мережевих<br>адаптерів на хостах. ....                          | 38 |
| 2.3 Налagodження мережевого екрану pfSense. ....                                                                              | 47 |
| 3. Базове налаштування та розгортання Active Directory на ОС Windows Server<br>2019 .....                                     | 54 |

|                                                        |    |
|--------------------------------------------------------|----|
| РОЗДІЛ 3. РЕАЛІЗАЦІЯ СКАНУВАННЯ ACTIVE DIRECTORY ..... | 64 |
| ВИСНОВКИ.....                                          | 67 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                   | 68 |
| ДОДАТКИ.....                                           | 70 |

## ВСТУП

У сучасному світі, де інформаційні системи є об'єктом постійної уваги кіберзлочинців, забезпечення високого рівня безпеки стає надзвичайно актуальним завданням для будь-якої організації. Active Directory (AD) є популярним рішенням для організації центральної інфраструктури, забезпечуючи управління обліковими записами користувачів, групами, комп'ютерами та іншими ресурсами в мережі. Розповсюдженість AD призводить до підвищеного інтересу до нього зловмисників. AD є критичною частиною корпоративної інфраструктури, тому її захист пріоритетно важливим завданням для будь-якої організації.

Тестування на проникнення є одним із найефективніших способів виявлення та усунення вразливостей у системах та мережах. Пентест Active Directory може допомогти організації виявити та виправити вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережі та її ресурсів. Зловмисник буде робити все можливе для використання вразливості, щоб отримати доступ до облікових записів користувачів або для встановлення шкідливого програмного забезпечення, що надалі призведе до отримання контролю над комп'ютерами в мережі.

Методи та технології тестування на проникнення в Active Directory є важливим елементом програми безпеки корпоративної мережі, що зумовлює високу актуальність даної теми. Пентест Active Directory дозволяє організації підвищити рівень безпеки своєї мережі та захистити свої активи від кібератак.

**Метою кваліфікаційної роботи є** вивчення сучасних методів та технологій тестування на проникнення на проникнення мережної інфраструктури на базі Active Directory задля розробки ефективного та високопродуктивного підходу до забезпечення безпеки корпоративної мережі.

Для досягнення цієї мети необхідно вирішити такі завдання:

- Проаналізувати наявні методи та технології тестування на проникнення мережної інфраструктури на базі Active Directory.
- Визначити основні атаки на Active Directory, які можуть бути виявлені за допомогою пентесту.
- Розробити ефективний та високопродуктивний підхід до забезпечення безпеки корпоративної мережі..

Об'єктом дослідження є процес підвищення безпеки мережної інфраструктури на базі Active Directory.

Предметом дослідження є методи та технології тестування на проникнення мережної інфраструктури на базі Active Directory.

# РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ACTIVE DIRECTORY.

## 1.1 Загальна концепція тестування на проникнення

Тестування на проникнення (penetration testing, pentesting) - це метод оцінки безпеки комп'ютерних систем, мереж та програмного забезпечення, який полягає в імітації атаки зловмисника з метою виявлення вразливостей та недоліків, які можуть бути використані для отримання несанкціонованого доступу до інформації або систем.

Мета тестування на проникнення:

- виявити вразливості в системах, які можуть бути використані зловмисниками для проникнення.
- оцінити ризики, пов'язані з виявленими вразливостями.
- розробити рекомендації щодо усунення виявлених вразливостей.

Типи тестування на проникнення:

Чорна скринька (Black Box). Пентестер не має жодної інформації про систему, окрім її IP-адреси або доменного імені. Припустимо, що зловмисник без облікового запису (в домені) або внутрішнього тесту на проникнення до чорного ящика. У данному випадку передбачається, що зловмисник присутній в мережі, але не має попереднього доступу до обладнання. Це сценарій, який найкраще розглядає зловмисника, якому вдалося фізично підключитися до мережі або скомпрометувати обладнання, не пов'язане з доменом організації. Крім того, в контексті Active Directory це означає, що пентестер не має облікового запису користувача, що належить до домену. Фактично, метою пентестера буде отримати дійсний доступ до обладнання серверу, робочої станції користувача та облікового запису домену.

Сіра скринька (Gray Box). Тестувальник має обмежену інформацію про систему, наприклад, знання про її операційну систему та програмне забезпечення. Наприклад, уявимо ситуацію, коли зловмисник з обліковим записом в домені, а також має дійсний доступ до внутрішньої служби або частини обладнання. Цей сценарій розглядає зловмисника, якому вдалося скомпрометувати обліковий запис працівника, наприклад, за допомогою фішингу, робочу станцію або обладнання підключене до домену, або досягти мети попереднього сценарію. Крім того, в контексті Active Directory пентестер матиме дійсний обліковий запис у домені без спеціальних привілеїв. Використовуючи цей обліковий запис, пентестер отримає доступ до конфіденційних корпоративних активів, як правило, шляхом підвищення своїх привілеїв.

Біла скринька (white Box): тестувальник має повний доступ до вихідного коду системи та її документації. Тим самим передбачає надання тестувальнику повної інформації про мережу та систему, включаючи топологію мережі та облікові дані. Це допомагає заощадити час і знизити загальну вартість тесту[1]. Тому мета полягає у виявленні вразливостей, які не обов'язково були б очевидними без глибокого знання системи, а також у наданні рекомендацій щодо посилення безпеки.

## 1.2 Архітектура та принципи роботи AD

Active Directory(активний каталог) — служби, що використовуються для управління ресурсами мережі, такими як користувачі, комп'ютери, принтери та інші пристрої. AD використовує ієрархічну структуру для організації ресурсів, що робить її легкою та зручною для управління. Active Directory надається у вигляді набору служб, що входять до складу операційної системи Microsoft Windows Server. Служби AD можуть бути встановлені у вигляді декількох серверних ролей, при цьому найважливішими ролями є

Active Directory Domain Services (AD DS): надає методи зберігання даних каталогів і надання доступу до цих даних користувачам і адміністраторам мережі.

Наприклад, AD DS зберігає інформацію про облікові записи користувачів, таку як імена, паролі, номери телефонів тощо, і дозволяє іншим авторизованим користувачам у тій самій мережі отримати доступ до цієї інформації. Active Directory зберігає інформацію про об'єкти в мережі і полегшує пошук і використання цієї інформації для адміністраторів і користувачів. Active Directory використовує структуроване сховище даних як основу для логічної, ієрархічної організації інформації каталогу.[2]

Контролер домену - це сервер, який відповідає на запити автентифікації та перевіряє користувачів у комп'ютерних мережах. Домени - це ієрархічний спосіб організації користувачів і комп'ютерів, які працюють разом в одній мережі. Контролер домену зберігає всі ці дані впорядкованими та захищеними. Контролери домену керують і захищають доменні мережі, дозволяючи доступ до служб каталогів лише авторизованим користувачам і забороняючи несанкціонований доступ.[3]

Lightweight Directory Services (AD LDS) надає спеціальні служби каталогів для додатків. Він надає сховище даних і сервіси для доступу до сховища даних. Для доступу до даних програми використовуються стандартні інтерфейси прикладного програмування (API). До таких інтерфейсів належать інтерфейси Active Directory, Active Directory Service Interfaces, Lightweight Data Access Protocol та System.DirectoryServices. AD LDS працює незалежно від Active Directory і незалежно від доменів або лісів Active Directory. Вона працює або як автономне сховище даних, або з реплікацією. Її незалежність забезпечує локальний контроль і автономність служб каталогів для конкретних додатків. Це також сприяє створенню незалежних, гнучких схем і контекстів іменування.[4]

Federation Services (AD FS) забезпечує управління об'єднаною ідентичністю та доступом, безпечно обмінюючись цифровою ідентичністю та правами через кордони системи безпеки та корпоративні кордони. AD FS розширює можливості використання функції єдиного входу, доступної в межах однієї системи безпеки

або корпоративної межі, на інтернет-додатки, щоб забезпечити клієнтам, партнерам і постачальникам спрощений користувацький доступ до веб-додатків організації.[5]

Rights Management Services (AD RMS): це технологія Microsoft, призначена для обмеження доступу до інформації в корпоративному середовищі. RMS допомагає корпоративним клієнтам контролювати та захищати критично важливу цифрову інформацію, пропонуючи гнучкі та постійні політики для застосування.[6]

Certificate Services (AD CS) це сервер Windows, призначений для випуску цифрових сертифікатів. AD CS пропонує цифрові сертифікати, які мають широкий спектр застосування, включаючи шифрування та цифровий підпис документів і повідомлень, а також автентифікацію облікових записів комп'ютерів, користувачів або пристроїв у мережі. Сертифікати, видані AD\ CS, дійсні протягом певного періоду і можуть бути поновлені або відкликані за необхідності, забезпечуючи детальний контроль над терміном дії сертифікатів.[7]

Як було зазначено, сервер Windows, на якому запущено роль AD DS, називається контролером домену (DC). Контролери домену формують фізичну структуру AD. На них розміщується вся функціональність AD і підтримується багатоманітність база даних AD, яка реплікується між декількома контролерами домену в середовищі. Логічна структура AD побудована навколо концепції доменів, які зазвичай називають як домени Windows або домени AD. Домен являє собою адміністративну єдність та кордон безпеки для об'єктів, що містяться всередині нього. Домени можуть бути організовані у дерева доменів, а ті у свою чергу, у ліси, створюючи ієрархічну структуру. У меншому масштабі об'єкти всередині доменів можуть бути організовані у контейнери. Найпоширенішим типом контейнера є організаційна одиниця (OU). Членами OU можуть бути такі об'єкти, як користувачі, групи, комп'ютери або інші OU. Логічна структура AD зображена на рис. 1.1.

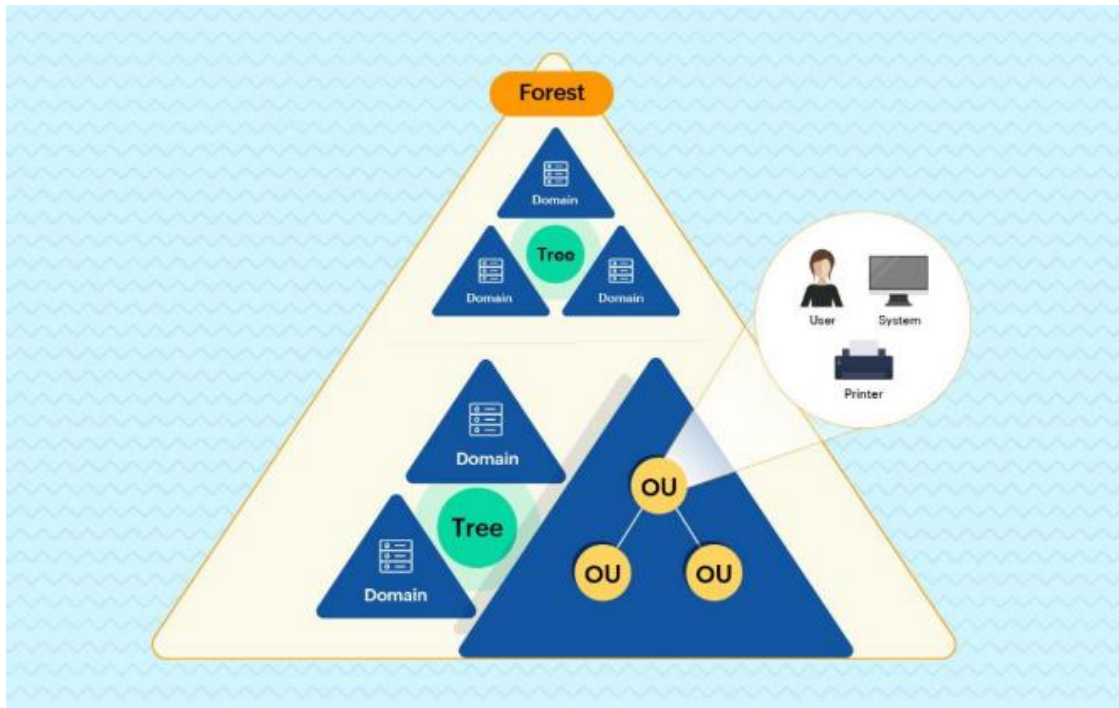


Рисунок 1.1 — Логічна структура Active Directory.

Адміністратори можуть керувати поведінкою об'єктів AD за допомогою групової політики. Групова політика дозволяє керувати різними конфігураціями об'єктів, включаючи їх налаштування безпеки. Логічна структура AD полегшує адміністрування домену, оскільки групові політики можна застосовувати до контейнерів, таких як OU або домени, а не до окремих об'єктів.

### 1.3. Автентифікація в Active Directory

Окрім зберігання інформації, пов'язаної з ідентифікацією, Active Directory слугує основою для служб автентифікації в доменному середовищі. Автентифікація - це процес перевірки ідентичності об'єкта або особи. Його мета - підтвердити, що сторона є справжньою і дійсно є тією, за кого себе видає. Її не слід плутати з авторизацією, яка є актом визначення правильних дозволів і надання доступу до запитуваних ресурсів.[8]

В ОС Windows будь-який користувач, служба або комп'ютер, який може ініціювати дію, є принципом безпеки. Принципи безпеки унікально ідентифікуються за допомогою ідентифікаторів безпеки (SID) і мають облікові записи, які можуть бути локальними для комп'ютера або доменними, що

зберігаються в AD. Перш ніж довірена особа зможе брати участь у мережевому домені, її обліковий запис має бути автентифіковано в AD. Для автентифікації довірена особа повинна надати певну форму секретних автентифікаційних даних, таких як сертифікат або пароль. [9]

Нижче наведено пояснення процесу автентифікації в AD. Для спрощення припускається, що користувач має ідентифікатор. Для автентифікації користувачів Windows реалізує інтерактивний процес входу в систему. Для того, щоб увійти в систему, користувач вводить облікові дані, як правило, ім'я користувача та пароль, у діалоговому вікні "Вхід до Windows". Це здійснюється за допомогою компонента графічної ідентифікації та автентифікації (GINA), який завантажується процесом Winlogon. Winlogon передає облікові дані, отримані з діалогового вікна, до служби Local Security Authority (LSA), як показано у лівій частині рис. 1.2. Крім використання пароля, користувачі можуть також представити свої облікові дані, вставивши смарт-карту або взаємодіючи з біометричним пристроєм.

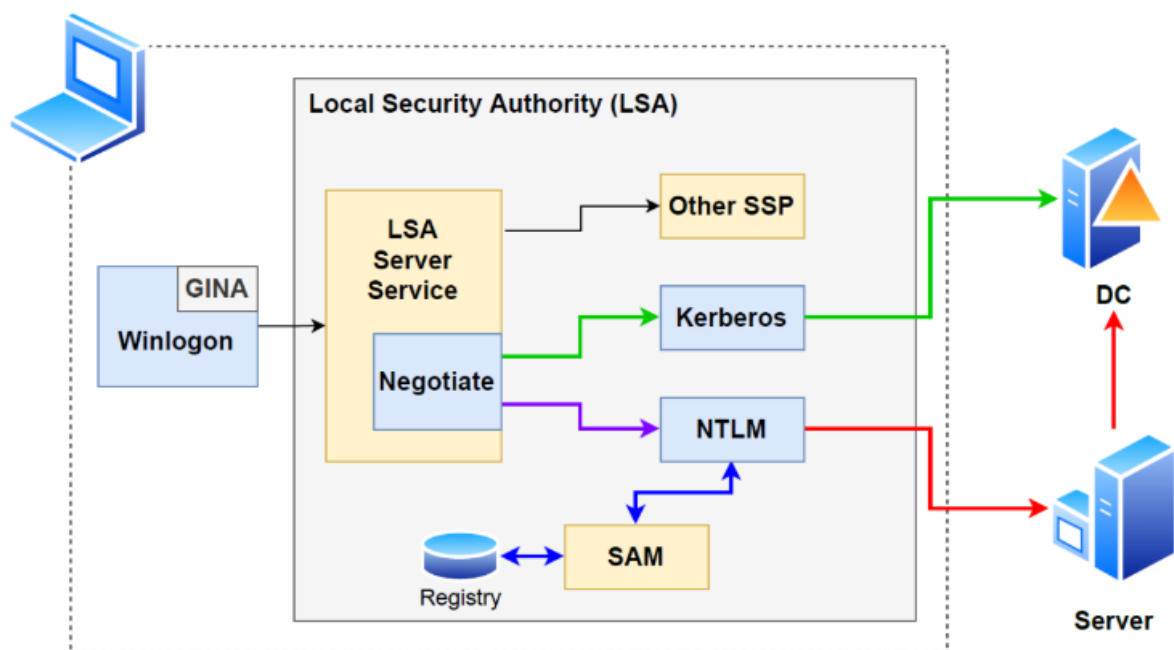


Рисунок 1.2 — Огляд автентифікації в Active Directory.

Підсистема LSA може взаємодіяти з віддаленим джерелом автентифікації (наприклад, DC). Це відбувається через протокольний рівень, на якому доступ до

різних протоколів автентифікації надається через інтерфейс постачальника підтримки безпеки (Security Support Provider, SSP). В ОС Windows реалізовано стандартний набір SSP автентифікації, зокрема Negotiate, Kerberos, NTLM, Secure channel і Digest.

Протокол автентифікації NT LAN Manager (NTLM) - це сімейство протоколів, розроблених компанією Microsoft для використання у середовищі Windows. Ці протоколи призначені для забезпечення автентифікації між клієнтами та серверами на основі механізму запиту/відповіді. NTLM розвивався протягом всієї історії ОС Windows, а його поточна версія, NTLMv2 використовується з Windows 2000. [11, 12]

Інтерактивний вхід може бути ініційований за допомогою локального або доменного облікового запису користувача. Локальними обліковими записами керує диспетчер облікових записів безпеки (Security Accounts Manager, SAM), і вони зберігаються в базі даних реєстру на локальному комп'ютері. Локальні облікові записи - це тип облікових записів за замовчуванням на комп'ютері Windows, який не приєднано до домену AD. Ці облікові записи дозволяють користувачам отримувати доступ до локальних ресурсів, але не є достатніми для доступу і використання ресурсів домену.

Облікові записи користувачів домену зберігаються в базі даних AD на контролері домену. Вхід до домену надає користувачеві доступ до локальних і доменних ресурсів. Для успішного входу в домен потрібно, щоб і користувач, і комп'ютер мали обліковий запис в AD, а комп'ютер був фізично підключений до мережі. Для автентифікації доменних облікових записів використовується протокол Kerberos або NTLM.

Протокол Kerberos забезпечує більшу безпеку, ніж NTLM, і тому він є кращим протоколом для використання в домені AD. Тим не менш, NTLM все ще підтримується. Kerberos і NTLM SSP не повинні використовуватися безпосередньо, а через пакет безпеки Negotiate, який автоматично вибирає між

ними. За замовчуванням вибирається Kerberos, якщо тільки він не може бути використаний однією з систем, що беруть участь у процесі автентифікації. [10]

Після інтерактивного входу в систему відбувається мережевий вхід, який використовується для підтвердження ідентифікації користувача для мережевої служби, до якої він намагається отримати доступ. Зазвичай це відбувається непомітно для користувача, оскільки повторно використовуються раніше встановлені облікові дані. Таким чином, інтегрована функціональність SSO забезпечується за допомогою підтримуваних програм. На рис. 1.2 показано спрощений огляд описаних концепцій автентифікації. Проілюстровано різні сценарії входу: а) локальний обліковий запис (синій шлях); б) доменний обліковий запис з протоколами NTLM (червоний шлях) і Kerberos (зелений шлях).

#### 1.3.1. Протокол автентифікації NTLM

Хоча автентифікація NTLM замінена на Kerberos як кращий протокол автентифікації, він все ще підтримується і повинен використовуватися для автентифікації в автономних системах або системах, налаштованих як члени робочої групи [11]. Крім того, автентифікація NTLM може також використовуватися в ситуаціях, коли автентифікація Kerberos неможлива, наприклад, якщо:

- одна зі сторін автентифікації не підтримує Kerberos
- сервер не приєднано до домену AD
- автентифікація Kerberos налаштована неправильно
- реалізація безпосередньо вибирає використання NTLM

При NTLM-автентифікації сервер ресурсів, до якого здійснюється доступ, повинен виконати одну з наступних дій для перевірки ідентичності комп'ютера або користувача, що звертається до нього, в залежності від сценарію автентифікації:

1. Звернутися до служби автентифікації домену на сервері ресурсів, якщо обліковий запис, що автентифікується, є обліковим записом домену.
- 2.

Знайти обліковий запис у локальній базі даних облікових записів, якщо це локальний обліковий запис.

2. Знайти обліковий запис у локальній базі даних облікових записів, якщо це локальний обліковий запис.

Оскільки інформація про облікові записи доменів зберігається в центрі керування, лише центр керування може перевірити облікові дані користувача та завершити послідовність автентифікації. Для цього сервер ресурсів використовує віддалений протокол Netlogon для зв'язку з центром керування, який також називається наскрізною автентифікацією NTLM. [13] Автентифікація NTLM може використовуватися як під час інтерактивного, так і під час мережевого входу в систему. Нижче наведено опис типової послідовності автентифікації на основі документації Microsoft [13, 14]. Передбачається, що користувач домену отримує доступ до служби на сервері ресурсів. Пояснення підтверджується схемою на рис. 1.3.



Рисунок 1.3 — Автентифікація на основі протоколу NTLM.

- 1) Користувач входить на клієнтську робочу станцію, вводячи ім'я користувача та пароль. Клієнт обчислює NTLM-хеш пароля і відкидає справжній пароль. Щоб ініціювати автентифікацію, клієнт надсилає серверу повідомлення **NEGOTIATE MESSAGE**. Окрім параметрів NTLM, це повідомлення містить

ім'я робочої станції клієнта та ім'я домену. На основі наданого доменного імені сервер визначає, чи має клієнт право на локальну або доменну автентифікацію.

- 2) Сервер генерує випадкове число (nonce) і надсилає його клієнту в **CHALLENGE MESSAGE**.
- 3) Клієнт шифрує виклик за допомогою хешу пароля NTLM і надсилає його в **AUTHENTICATE MESSAGE** на сервер. Це повідомлення також містить ім'я користувача облікового запису для автентифікації та ім'я робочої станції клієнта.
- 4) Сервер пересилає отриману відповідь на DC, включаючи виклик, раніше надісланий клієнту, у вигляді повідомлення **NETLOGON NETWORK INFO**.
- 5) Контролер домену використовує ім'я користувача для отримання хешу пароля користувача з бази даних AD. Він використовує цей хеш для шифрування запиту і порівнює його з відповіддю клієнта. Результат повертається в повідомленні **NETLOGON VALIDATION SAM INFO4** на сервер. Якщо перевірка пройшла успішно, повідомлення містить сертифікат привілейованого облікового запису користувача (PAC) з даними для авторизації. Після цього сервер може прийняти рішення про авторизацію.

### 1.3.2 Протокол автентифікації Kerberos

Kerberos — це протокол, який забезпечує безпечну взаємну автентифікацію довірених осіб, що спілкуються через ненадійну мережу. Протокол Kerberos був розроблений в Массачусетському технологічному інституті для проекту Athena і спочатку базувався на протоколі автентифікації Нідхема-Шредера з модифікаціями, запропонованими Деннінгом і Сакко. Однією з головних переваг протоколу Kerberos є те, що він забезпечує функціональність SSO. Сучасна версія Kerberos v5 описана в RFC 4120, який замінив колишній RFC 1510. [15, 16]

Microsoft включила Kerberos v5 в Windows 2000 (на основі RFC 1510) з метою заміни автентифікації NTLM в доменах AD. У 2006 році протокол було оновлено відповідно до RFC 4120. Реалізація Kerberos від Microsoft вносить деякі відмінності та додаткову функціональність за межами специфікації RFC, включаючи авторизацію, іншу реалізацію інтерфейсу SSP або необов'язкову перевірку PAC. [15, 17]

Протокол Kerberos складається з трьох підпротоколів або обмінів:

- Обмін службою автентифікації (Authentication Service, AS).
- Обмін службою видачі квитків (TGS).
- Обмін між клієнтом і сервером.

У реалізації Microsoft Центр розподілу ключів (KDC) реалізований як доменна служба, встановлена на контролері домену, яка використовує AD як базу даних облікових записів і виконує дві сервісні функції: Служба автентифікації та Служба видачі квитків. Таким чином, обмін AS і TGS відбувається між клієнтом і центром розподілу ключів, як показано на рис. 1.4. Обмін AS зазвичай відбувається на початку сеансу входу в систему, наприклад, коли служба LSA перевіряє доменні облікові дані користувача під час інтерактивного входу в систему. Окрім автентифікації самого себе, клієнту потрібно отримати облікові дані для TGS, які згодом будуть використовуватимуться для входу в мережу, коли клієнт запитуватиме доступ до інших серверів.

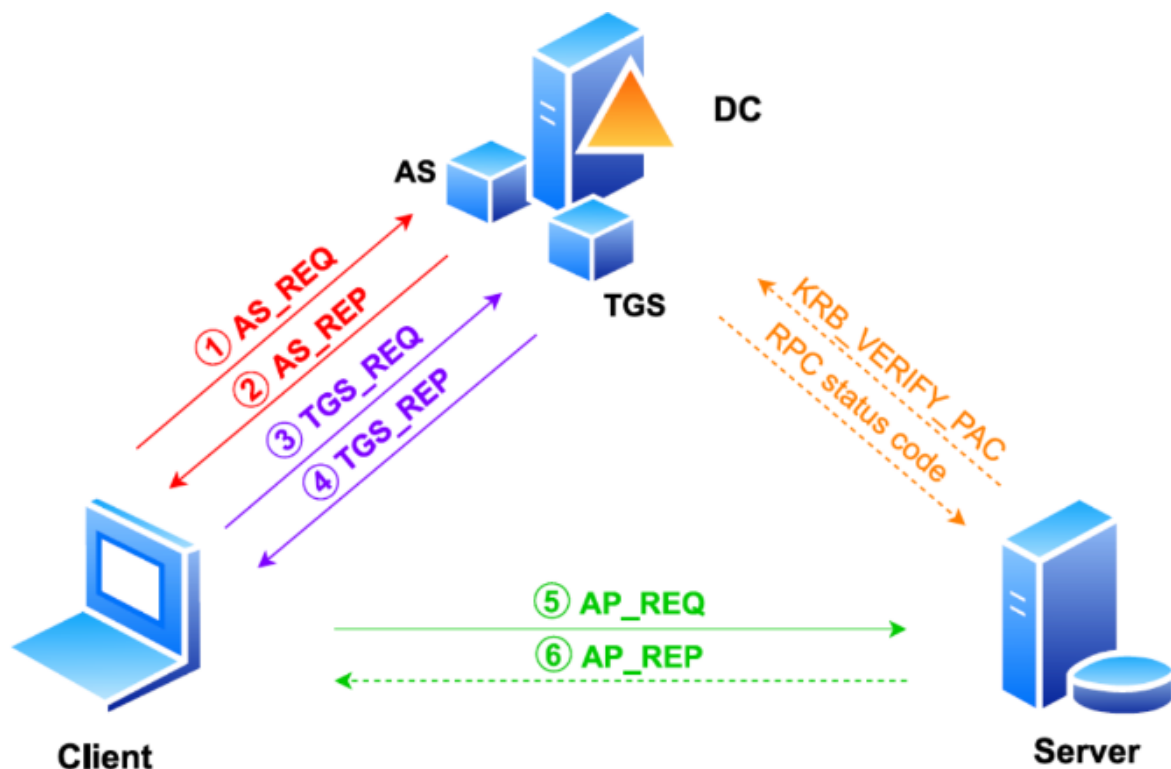


Рисунок 1.4 — Автентифікація на основі протоколу Kerberos.

Етапи автентифікації за протоколом Kerberos:

- 1) Клієнт надсилає AS REQ повідомлення до AS на KDC. Це повідомлення містить ідентифікатор клієнта, TGS і дані попередньої автентифікації, які є міткою часу, зашифрованою за допомогою головного ключа, отриманого з пароля входу користувача.
- 2) Клієнт надсилає AS REQ повідомлення до AS на KDC. Це повідомлення містить ідентифікатор клієнта, TGS і дані попередньої автентифікації, які є міткою часу, зашифрованою за допомогою головного ключа, отриманого з пароля входу користувача. сеансу входу в систему у двох копіях, одна з яких зашифрована головним ключем користувача, а інша вбудована в Ticket-Granting Ticket (TGT) разом з даними авторизації. Сам TGT зашифрований власним головним ключем KDC, отриманим від його принципу безпеки - облікового запису KRBTGT. Створені облікові дані надсилаються клієнту в

повідомленні AS REP. Клієнт витягує TGT і сеансовий ключ і зберігає їх у своєму кеші.

Після обміну AS клієнт отримує TGT, який він може використовувати для того, щоб запросити авіаквиток в KDC для доступу до певної послуги. Це відбувається при обміні TGS. TGT є багаторазовим і за замовчуванням втрачає чинність через 10 годин, після чого його можна поновити. TGT містить PAC, який містить інформацію про всі групи безпеки, в яких користувач є членом. TGT зашифрований і підписаний обліковим записом KRBGTGT, тому тільки KDC може розшифрувати його і прочитати дані. [18]

- 3) Клієнт надсилає повідомлення TGS REQ до KDC. Це повідомлення містить ідентифікатор запитуваного сервісу, повідомлення автентифікатора, зашифроване за допомогою ключа сеансу входу користувача, і TGT.
- 4) KDC розшифровує TGT за допомогою свого секретного ключа і витягує ключ сеансу входу користувача. Витягнутий сеансовий ключ використовується для розшифрування повідомлення автентифікатора. Якщо повідомлення проходить перевірку, KDC вигадує сеансовий ключ для користувача, яким він може поділитися з цільовою службою. KDC шифрує одну копію ключа сеансу служби за допомогою ключа сеансу входу користувача. Інша копія вбудовується в квиток надання послуг (SGT) разом з даними авторизації користувача і шифрується головним ключем сервісу. KDC відповідає клієнту повідомленням TGS REP. Клієнт витягує SGT з цього повідомлення, розшифровує ключ сеансу служби за допомогою свого ключа сеансу входу і зберігає ці облікові дані у своєму кеші.

Якщо обмін TGS пройшов успішно, клієнт отримує SGT, який він пред'являє для допуску до сервісу в клієнт-серверному обміні.

- 5) Клієнт надсилає повідомлення AP REQ на сервер, на якому розміщено цільовий сервіс. Повідомлення містить автентифікатор, зашифрований за допомогою ключа сеансу служби, отриманого від KDC, SGT для

використання зі службою, і прапорець, який вказує, чи запитує клієнт взаємну автентифікацію (необов'язково).

- 6) Сервер розшифровує квиток, витягує інформацію про членство користувача в групі, ключ сеансу і використовує його для оцінки автентифікатора. На цьому етапі сервер має достатньо інформації, щоб прийняти рішення про авторизацію. Якщо була запитана взаємна автентифікація, сервер використовує ключ сеансу для шифрування часу з повідомлення автентифікатора користувача і повертає результат у повідомленні AP REP.

Під час обміну між клієнтом і сервером сервер може опціонально переслати PAC, розібраний SGT, до DC у повідомленні KERB VERIFY PAC, щоб перевірити правильність представленої групової приналежності користувача. DC перевіряє підпис і повертає результат на сервер у вигляді коду статусу віддаленого виклику процедури (RPC). Після цього клієнту надсилається повідомлення AP REP.

У повідомленні TGS REQ (крок 3 вище) клієнт запитує доступ до певного екземпляра служби. В Active Directory екземпляри служб унікально ідентифікуються за допомогою основних імен служб (Service Principal Names, SPN). Перш ніж екземпляр служби можна використовувати з автентифікацією Kerberos, його SPN має бути зареєстровано в об'єкті облікового запису, який екземпляр служби використовує для входу в систему. Дане SPN може бути зареєстроване лише з одним обліковим записом. [19]

SPN має наступний формат: <svc\_клас>/<хост>[:<порт>[/<svc\_ім'я>]]. Перші два компоненти є обов'язковими. <svc\_class> - це рядок, який ідентифікує загальний клас служби. Існують загальновідомі назви класів сервісів [20], але ім'я також може бути довільним рядком, унікальним для типу сервісу. <host> - це ім'я комп'ютера, на якому запущено службу, зазвичай ідентифікується за допомогою повного доменного імені (FQDN). Номер порту може використовуватися для розрізнення декількох екземплярів одного класу служби на одному комп'ютері. Нарешті, <svc\_name> використовується для

реплікованих служб. Прикладами SPN для спільних служб можуть бути MSSQLSvc\dbmain[.]testx[.]local[:]1433 або SERV4X\server1[.]testx[.]local[.] [19]

## 1.4. Огляд атак на Active Directory

### 1.4.1 Kerberoasting

Kerberoasting - це техніка атаки після експлуатації, яка намагається отримати хеш пароля облікового запису Active Directory, що має Service Principal Name. У такій атаці автентифікований користувач домену запитує квиток Kerberos для SPN. Отриманий Kerberos-квиток шифрується хешем пароля облікового запису служби, пов'язаного з SPN. Потім зловмисник працює в автономному режимі, щоб зламати хеш пароля, часто використовуючи методи грубої сили. Отримавши відкриті текстові облікові дані службового облікового запису, зловмисник може видати себе за власника облікового запису та успадкувати доступ до будь-яких систем, активів або мереж, наданих скомпрометованому обліковому запису. В певних моментах атаку Kerberoasting складно виявити, тому що деякі із традиційних інструментів і рішень для кібербезпеки не призначені для моніторингу або аналізу поведінки та активності авторизованих користувачів.

Зловмисники докладають чимало зусиль, щоб отримати доступ до облікових даних користувача за допомогою таких методів, як Kerberoasting, оскільки можливість видавати себе за легітимного користувача допомагає зловмиснику уникнути виявлення та просуватись все далі. Після викрадення облікових даних зловмисник отримує доступ до будь-якої системи, служби або мережі, на яку має право цей обліковий запис. Досвідчені зловмисники також можуть спробувати підвищити привілеї свого облікового запису і просуватися по мережі, збираючи облікові дані інших облікових записів, встановлюючи бекдори для подальшого тривалого доступу і викрадаючи дані на цьому шляху.

Атаки kerberoasting використовують комбінацію слабких методів шифрування та простих або низько складних паролів. Ці атаки зазвичай відбуваються за наступною схемою:

1. Суб'єкт загрози компрометує обліковий запис користувача домену.
2. Зловмисник використовує контекст користувача домену для запиту квитка служби Kerberos у службі видачі квитків (TGS) за допомогою таких інструментів, як Rubeus від GhostPack або GetUserSPNs.py від SecureAuth Corporation.
3. Зловмисник отримує квиток від центру розподілу ключів Kerberos (KDC). Квиток зашифрований хешованою версією пароля облікового запису.
4. Зловмисник захоплює квиток на TGS і виводить його в офлайн. 5. Зловмисник намагається зламати хеш облікових даних SPN, щоб отримати відкритий пароль облікового запису служби, використовуючи методи грубої сили або такі інструменти, як Hashcat або JohnTheRipper.
5. Маючи на руках пароль службового облікового запису, зловмисник намагається авторизуватися під цим обліковим записом і отримує доступ до будь-якої служби, мережі або системи, пов'язаної зі скомпрометованим обліковим записом.
6. Після цього зловмисник може викрасти дані, підвищити привілеї або встановити бекдори в мережі, щоб забезпечити собі доступ у майбутньому.

Варто розуміти, що для проведення атаки Kerberoasting не потрібен обліковий запис адміністратора домену або обліковий запис з підвищеними привілеями. Насправді, будь-який обліковий запис користувача домену може бути використаний в цьому типі атаки, оскільки будь-який обліковий запис може запитувати квитки на обслуговування від TGS. Kerberoasting вимагає, щоб зловмисник мав доступ до облікового запису користувача для запиту квитків з KDC. Цей доступ може бути отриманий

різними методами, такими як соціальна інженерія, шкідливе програмне забезпечення або навіть купівля облікових даних користувача в темному інтернеті.

Варто розуміти що для проведення атаки Kerberoasting не потрібен обліковий запис адміністратора домену або обліковий запис з підвищеними привілеями. Насправді, будь-який обліковий запис користувача домену може бути використаний в цьому типі атаки, оскільки будь-який обліковий запис може запитувати квитки на обслуговування від TGS.Kerberoasting вимагає, щоб зловмисник мав доступ до облікового запису користувача для запиту квитків з KDC. Цей доступ може бути отриманий різними методами, такими як соціальна інженерія, шкідливе програмне забезпечення або навіть купівля облікових даних користувача в темному інтернеті. зазвичай не перевіряє, чи має користувач дозвіл на доступ до цієї служби. Служба сама перевіряє права доступу, що створює лазівку, за допомогою якої можна здійснити офлайн-атаку.

Найкращі практики, щоб запобігти загрозі для всього домену в якості стратегії пом'якшення наслідків:

- переконатися, що всі службові облікові записи мають довгі, складні паролі (більше 25).
- регулярно змінювати паролі службових облікових записів (щонайменше раз на рік).
- використовувати службові облікові записи з груповим керуванням (gMSA), які забезпечують керування паролями та усувають необхідність для адміністратора вручну керувати обліковими даними кожного службового облікового запису.
- MITRE ATT&CK також рекомендує використовувати шифрування AES Kerberos (або інший надійний алгоритм шифрування) замість RC4, що ускладнює зловмисникам злом хешів в автономному режимі. Увімкнути тип шифрування AES 128/256-біт за допомогою прапорців на вкладці "Обліковий запис".

#### 1.4.2 Атака password spraying

В основі атаки password spraying ("розпилення паролів") лежить використання зловмисником одного загального пароля для кількох облікових записів в одному додатку. Це дозволяє уникнути блокування облікового запису, яке зазвичай відбувається, коли зловмисник використовує атаку грубої сили на один обліковий запис, перебираючи багато паролів. Розпорошення паролів особливо ефективно проти компаній, які беруть участь у спільному використанні паролів. Атака відбувається у два етапи: зловмисник отримує список імен користувачів, а потім намагається увійти під цими іменами, використовуючи один і той самий пароль. Зловмисник повторює процес з новими паролями, доки не зламає систему автентифікації і не отримає доступ до облікових записів і систем.

Password spraying - це атака грубої сили, яка відрізняється від традиційних атак грубої сили, які намагаються вгадати пароль для одного облікового запису. Однак вона все ще використовує метод масових спроб і помилок, який визначає атаку грубої сили. Атака методом розпилення паролів вважається грубою силою, оскільки вона підбирає паролі до численних облікових записів, поки не знайде збіг.

Ознаки атаки розпилення паролів включають в себе наступні:

- високий обсяг активності входу в систему за короткий період.
- сплеск невдалих спроб входу від активних користувачів.
- входи з неіснуючих або неактивних акаунтів.

Також password spraying може зачепити кілька рівнів бізнесу. Атака може бути спрямована на облікові записи клієнтів, щоб використовувати їхню інформацію для заповнення облікових даних на інших сайтах. Атака може бути використано для проникнення в обліковий запис нового працівника. Зловмисники можуть спробувати підвищити привілеї, використовуючи викрадені облікові дані, щоб отримати більший доступ до конфіденційних даних. Успішна атака розпилення паролів робить жертву більш вразливою до різноманітних майбутніх атак.

Для мінімізації ризиків атаки password spraying потрібно:

- впровадження надійних паролів
- відслідковувати вхід у систему
- контролювати політики блокування

#### 1.4.3 Атака Golden Ticket

Golden Ticket ("золотий квиток") – це атака, під час якої зловмисник намагається отримати майже необмежений доступ до домену організації (пристроїв, файлів, контролерів домену тощо) шляхом доступу до даних користувачів, що зберігаються в Microsoft Active Directory (AD). Вона використовує слабкі місця в протоколі автентифікації особистості Kerberos,

який використовується для доступу до AD, що дозволяє зловмиснику обійти звичайну автентифікацію. Оскільки все більше компаній переходять на хмарні технології та віддалений режим роботи, поверхня атаки вийшла за межі традиційного периметру, оскільки співробітники входять в системи компанії, використовуючи власні пристрої та мережі. Це, в свою чергу, збільшило ризик того, що зловмисники зможуть проникнути в мережу і використати атаку золотого квитка для отримання доступу.

Атаки Golden Ticket переплітаються з інструментом з відкритим вихідним кодом Mimikatz, який був створений у 2011 році для демонстрації недоліків Microsoft Windows. Він витягує облікові дані, такі як імена користувачів, паролі, хеші та квитки Kerberos. Атака Golden Ticket отримала таку назву тому, що вона використовує вразливість в протоколі автентифікації Kerberos. Як і в книзі та фільмі "Чарлі і шоколадна фабрика", звідки і походить назва, атака являє собою "золотий квиток", який дозволяє необмежений доступ, але замість цукерні, що добре охороняється, вона дозволяє обійти кібербезпеку компанії та отримати доступ до її ресурсів, файлів, комп'ютерів та контролерів доменів. Як правило, автентифікація Kerberos використовує центр розподілу ключів для захисту та перевірки особи користувача. Мета цієї системи полягає в тому, щоб усунути необхідність

багаторазових запитів облікових даних у користувача, а замість цього перевірити особу користувача і призначити йому квиток для доступу. У розподільчому центрі є сервер видачі квитків (TGS), який з'єднує користувача з сервером обслуговування. База даних Kerberos містить паролі всіх перевірених користувачів. Сервер автентифікації, або AS, виконує первинну автентифікацію користувача. Якщо AS пройшов перевірку, користувач отримує Kerberos Ticket Grant Ticket, або TGT, який є доказом автентифікації.

#### 1.4.4 Pass-the-hash

Pass the hash (PtH) - це тип атаки, при якому зловмисник викрадає хешовані облікові дані користувача і використовує їх для створення нового сеансу користувача в тій же мережі. На відміну від інших атак на крадіжку облікових даних, атака pass the hash не вимагає від зловмисника знання або злому пароля для отримання доступу до системи. Замість цього він використовує збережену версію пароля для ініціювання нового сеансу.

Хеш-пароль - це одностороння математична функція, яка перетворює пароль користувача на рядок тексту, який неможливо змінити або розшифрувати, щоб розкрити справжній пароль. Простіше кажучи, паролі зберігаються не у вигляді тексту або символів, а у вигляді невиразних хеш символів.

Оскільки все більше організацій використовують технологію єдиного входу (SSO), щоб забезпечити віддалену роботу співробітників і зменшити тертя у взаємодії з користувачами, зловмисники усвідомили вразливість збережених паролів і облікових даних користувачів. Атаки на основі ідентифікаційних даних, такі як атаки PtH, коли зловмисники видають себе за легітимних користувачів, особливо важко виявити, оскільки більшість традиційних рішень з кібербезпеки не можуть відрізнити справжнього користувача від зловмисника, що маскується під нього.

Захист від атак на передачу хешу є критично важливим, оскільки цей метод часто слугує воротами до інших, більш серйозних проблем безпеки, таких як витік

даних, крадіжка особистих даних, атаки зловмисних програм або програм-вимагачів. Для зменшення ризиків виникнення атаки потрібно зробити:

- контролювати доступ до мережі та привілеїв облікового запису
- впровадити рішення для виявлення загроз та реагування на них
- проводити регулярне тестування на проникнення
- використовувати проактивне полювання на загрози

#### 1.4.5 Атака LLMNR/NBT-NS отруєння та ретрансляція SMB (SMB relay)

Відповідаючи на мережевий трафік LLMNR/NBT-NS, зловмисники можуть підмінити авторитетне джерело дозволу імен, щоб примусити до зв'язку з системою, контрольованою зловмисником. Ці дії можуть бути використані для збору або передачі матеріалів для автентифікації. Link-Local Multicast Name Resolution (LLMNR) і NetBIOS Name Service (NBT-NS) - це компоненти Microsoft Windows, які слугують альтернативними методами ідентифікації хостів. LLMNR базується на форматі системи доменних імен (DNS) і дозволяє хостам на одному локальному підключенні здійснювати

розпізнавання імен для інших хостів. NBT-NS ідентифікує системи в локальній мережі за їхніми NetBIOS-іменами.

Зловмисники можуть підмінити авторитетне джерело дозволу імен у мережі жертви, відповідаючи на трафік LLMNR (UDP 5355)/NBT-NS (UDP 137) так, ніби їм відома ідентичність запитуваного хоста, фактично отруюючи службу, щоб жертви спілкувалися з системою, контрольованою зловмисником. Якщо запитуваний хост належить до ресурсу, який вимагає ідентифікації/автентифікації, ім'я користувача та хеш NTLMv2 будуть надіслані до системи, контрольованої зловмисником. Зловмисник може зібрати хеш-інформацію, надіслану по дроту, за допо-

могою інструментів, які відстежують трафік на портах, або за допомогою мережевого сніфінгу, і зламати хеші в автономному режимі за допомогою перебору, щоб отримати відкритий текст паролів.

У деяких випадках, коли зломисник має доступ до системи, яка знаходиться на шляху автентифікації між системами, або коли автоматизоване сканування, яке використовує облікові дані, намагається автентифікуватися в системі, контрольованій зломисником, хеші NTLMv1/v2 можуть бути перехоплені та передані для доступу та виконання коду проти цільової системи. Етап ретрансляції може відбуватися разом з отруєнням, але може і незалежно від нього. Крім того, зломисники можуть інкапсулювати хеші NTLMv1/v2 в різні протоколи, такі як LDAP, SMB, MSSQL і HTTP, щоб розширити і використовувати різні сервіси з дійсною відповіддю NTLM.

Для того щоб зменшити ризик атаки потрібно:

- вимкнути LLMNR та NetBIOS у локальних налаштуваннях безпеки комп'ютера або у груповій політиці, якщо вони не потрібні у середовищі.
- використовувати програмне забезпечення безпеки на основі хоста для блокування трафіку LLMNR/NetBIOS. Увімкнення SMB підпису може зупинити атаки ретрансляції NTLMv2.
- системи виявлення та запобігання вторгненням у мережу, які можуть виявляти шаблони трафіку, що вказують на активність трафіку, можуть бути використані для зменшення активності на мережевому рівні.
- сегментація мережі може бути використана для ізоляції компонентів інфраструктури, які не потребують широкого доступу до мережі.

## 1.5. Аналіз методів та технологій для пентесту AD

Аналіз методів і технологій для пентестування Active Directory передбачає розуміння структури і вразливостей середовища AD організації. Оскільки кіберзагрози продовжують ускладнюватися і поширюватися, організації повинні вживати

проактивних заходів для оцінювання та зміцнення безпеки своєї інфраструктури Active Directory. Тестування на проникнення в Active Directory стає життєво важливою практикою. Пентестування передбачає імітацію кібератак на середовище AD організації з метою виявлення вразливостей, оцінки засобів контролю безпеки та перевірки ефективності механізмів захисту.

Важло зазначити розподіл етапів процесу пентеста:

- 1) Перерахування це початковий етап, на якому збирається інформація про інфраструктуру AD. Для цього зазвичай використовуються такі інструменти, як BloodHound, Nmap і ldapsearch. Перерахування передбачає виявлення контролерів доменів, облікових записів користувачів, членства в групах, довірчих відносин та іншої відповідної інформації.
- 2) Атаки на паролі. Слабкі або повторно використовувані паролі є поширеними вразливостями в середовищах AD. Атаки на паролі включають такі методи, як розпилення паролів, атаки грубої сили та підбір паролів для отримання доступу до облікових записів користувачів. Для атак на паролі зазвичай використовуються такі інструменти, як CrackMapExec, Hydra і Mimikatz.
- 3) Експлуатація вразливостей. Після виявлення вразливостей їх можна використати для отримання несанкціонованого доступу. До найпоширеніших вразливостей відносяться неправильні конфігурації, не виправлені системи та слабкі засоби контролю доступу. Для використання вразливостей в середовищах AD можна використовувати такі інструменти, як Metasploit, PowerSploit та Empire.
- 4) Ескалація привілеїв. Як отримали початковий доступ зломисники часто намагаються підвищити свої привілеї, щоб отримати подальший доступ до середовища AD. Для підвищення привілеїв можуть використовуватися такі методи, як передача хешу, передача квитка і Kerberoasting. Такі інструменти, як Mimikatz і PowerUp, зазвичай використовуються для підвищення привілеїв в середовищах AD.

- 5) Латеральне переміщення. Після встановлення доступу зловмисники можуть переміщатися в середовищі AD, щоб отримати доступ до конфіденційних ресурсів. Для бічного переміщення можуть використовуватися такі методи, як SMB Relay, DCOM Relay і протокол віддаленого робочого столу (RDP). Такі інструменти, як BloodHound і CrackMapExec, зазвичай використовуються для латерального переміщення в середовищах AD.
- 6) Викрадення даних: Зловмисники можуть викрадати конфіденційні дані з середовища AD у зловмисних цілях. Для витоку даних можуть використовуватися такі методи, як використання скомпрометованих облікових даних для доступу до конфіденційних файлів і баз даних. Такі інструменти, як PowerSploit і Metasploit, можуть використовуватися для витоку даних в середовищах AD.
- 7) Видалення слідів. Щоб уникнути виявлення, зловмисники можуть намагатися видалити сліди або приховати наприклад видаляючи журнали, змінюючи мітки часу та видаляючи докази своєї діяльності. Для замітання слідів в середовищах AD можна використовувати такі інструменти, як Windows Event Viewer і сценарії PowerShell.

Отже як зазначено, аналіз методів і технологій для тестування на проникнення Active Directory передбачає розуміння різних етапів тестування, включаючи перебір, атаку паролів, експлуатацію вразливостей, підвищення привілеїв, стійкість в скомпрометованій мережі, латеральне переміщення, витік даних і замітання слідів. Використовуючи комбінацію інструментів і методів, пентестери можуть виявляти і зменшувати вразливості в середовищах AD, для покращення загального стану безпеки.

## РОЗДІЛ 2. ПОБУДОВА ТА НАЛАГОДЖЕННЯ МЕРЕЖЕВОГО СЕРЕДОВИЩА НА БАЗІ VMWARE, PFSENSE ТА РОЗГОРТАННЯ ACTIVE DIRECTORY

### 2.1 Створення віртуального мережевого середовища.

Віртуальне середовище, у якому здійснюватиметься тестування на проникнення, буде ізольованим середовищем. Важливість ізольованості такого середовища обґрунтовано у табл. 2.1

Таблиця 2.1 – Основні причини ізоляції тестового середовища

| Причина                        | Пояснення                                                                                                                                                                         |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Безпека                        | Ізольований запуск пентестів запобігає непередбачуваним наслідкам, таким як порушення безпеки виробничих систем або витік конфіденційних даних.                                   |
| Пом'якшення ризиків            | Ізольоване тестування знижує ризик пошкодження або порушення роботи критично важливих систем або сервісів.                                                                        |
| Дотримання правових норм       | Ізольовані тести гарантують, що діяльність залишається в межах закону, уникаючи потенційних порушень законів або правил, пов'язаних з несанкціонованим доступом.                  |
| Доступність ресурсів           | Ізоляція тестувань від інших процесів забезпечує стабільність і швидкість реагування, запобігаючи боротьбі за ресурси.                                                            |
| Повторюваність і послідовність | Ізоляція середовища дозволяє проводити послідовні та повторювані випробування без втручання зовнішніх факторів.                                                                   |
| Тренінги та навчання           | Ізольоване мережеве середовище полегшує безпечні експерименти з методами та інструментами тестування на проникнення, підтримуючи навчання без ризику пошкодження реальних систем. |

|                          |                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Конфіденційність клієнта | Захищають конфіденційні дані клієнта від несанкціонованого доступу, забезпечуючи конфіденційність під час тестування на проникнення. |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|

Отже, для створення віртуального мережного середовища потрібно гіпервізор vmware workstation 16.5 також віртуальні комутатори L2 Hyper-V та мережний екран pfSense. Таким чином, це буде представлено як невелика корпоративна мережа, об'єднана своїми розподіленими підмережами в яких наявні робочі станції та контролер домену, а також наявна робоча станція пентестера для проведення подальшого тестування на проникнення. Розроблену топологію мережі представлено на рис. 2.1.

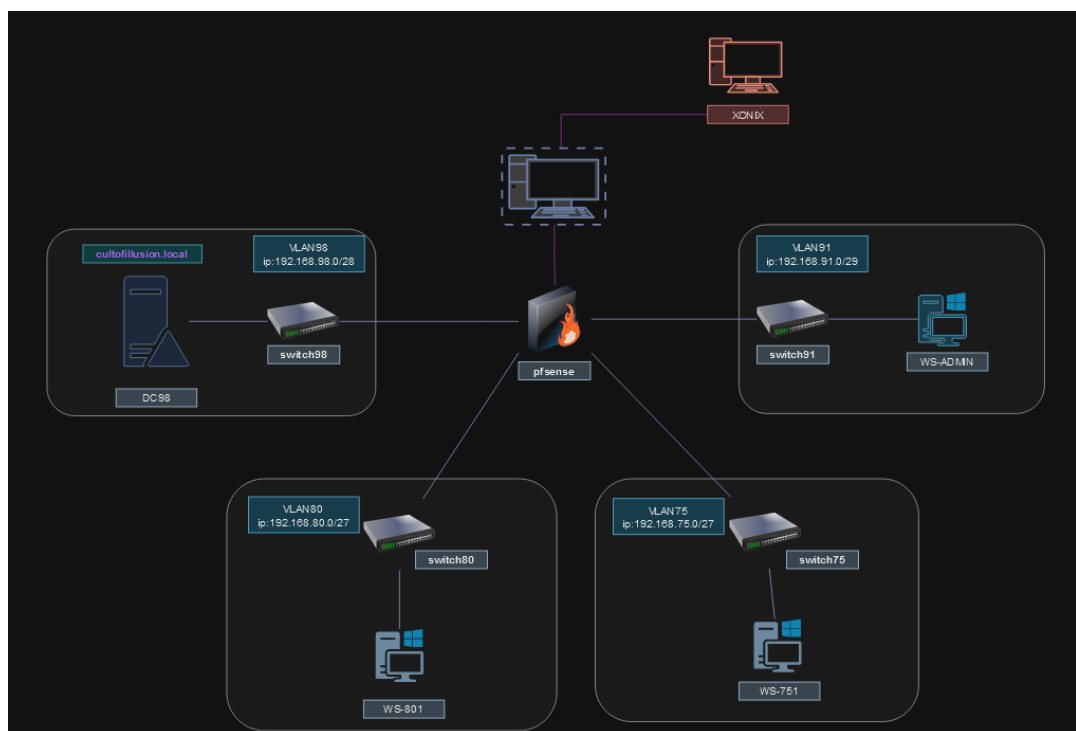


Рисунок 2.1 — Топологія мережі.

В підмережі VLAN75 наявна робоча станція WS-751 із операційною системою Windows 10 Enterprise (рис. 2.2).

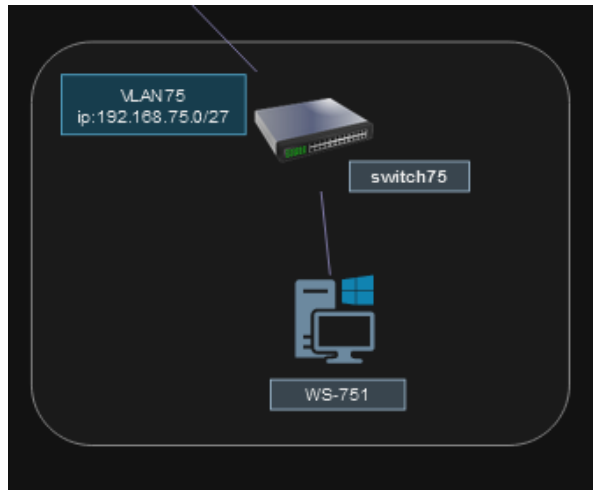


Рисунок 2.2 — Загальний вигляд підмережі VLAN75.

В підмережі VLAN80 наявна робоча станція WS-801 із операційною системою Windows 10 Enterprise, що продемонстровано рис. 2.3.

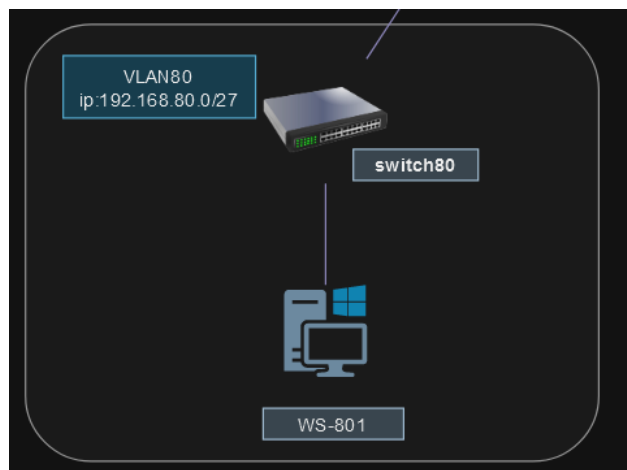


Рисунок 2.3 — Загальний вигляд підмережі VLAN80.

В підмережі VLAN91 наявна робоча станція адміністратора WS-ADMIN із операційною системою Windows 10 Enterprise, звідки в подальшому буде здійснюватися налаштування мережевого екрану pfSense (продемонстровано на рис. 2.4).

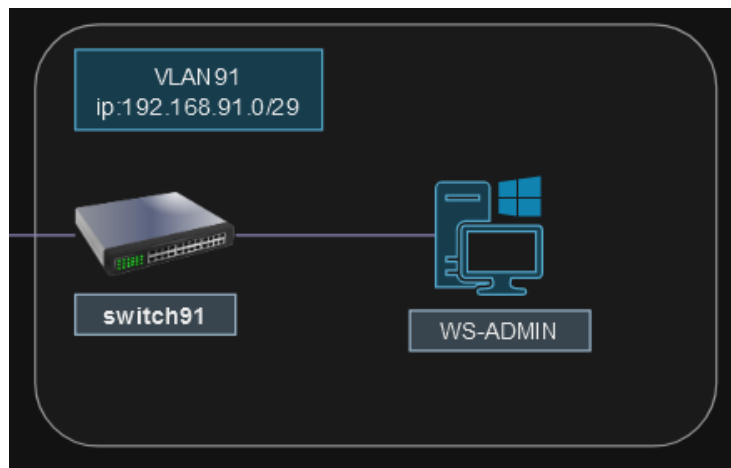


Рисунок 2.4 — Загальний вигляд підмережі VLAN91.

В підмережі VLAN98 наявний Windows Server 2019 Enterprise DC98, на якому планується розгортання AD та подальше тестування це представлено на рис. 2.5.

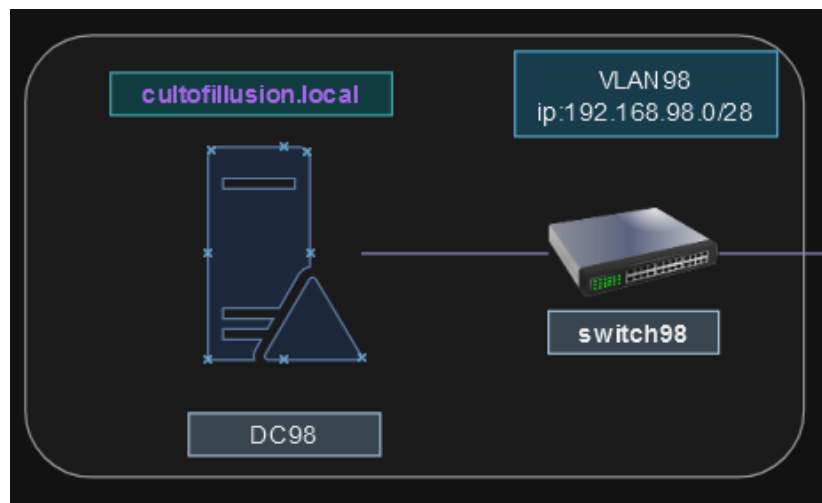


Рисунок 2.5 — Загальний вигляд підмережі VLAN98.

## 2.2 Створення віртуальних комутаторів Hyper-V та налагодження мережевих адаптерів на хостах.

Віртуальний мережевий адаптер можна розглядати як віртуалізовану версію фізичного мережевого адаптера. Він використовується в середовищах Hyper-V для з'єднання фізичного сервера з іншими серверами, віртуальними машинами або будь-якими іншими мережевими пристроями через локальне з'єднання. vNIC дозволяє і керує всіма мережевими зв'язками. Кожна віртуальна машина має один або

кілька vNIC, які забезпечують підключення до однієї підмережі. Однак можна призначити додаткові IP-адреси цьому NIC, щоб отримати доступ до кількох підмереж.

Є три віртуальні комутатори, які забезпечують різні рівні підключення до мережі:

- 1) Зовнішній віртуальний комутатор може підключатися до фізичного мережевого адаптера, що дозволяє віртуальним машинам отримати доступ до фізичної мережі.
- 2) Внутрішній віртуальний комутатор забезпечує зв'язок між віртуальними машинами, що працюють на одному сервері Hyper-V.
- 3) Приватний віртуальний комутатор забезпечує підключення лише між віртуальними машинами, які працюють на одному хості Hyper-V.

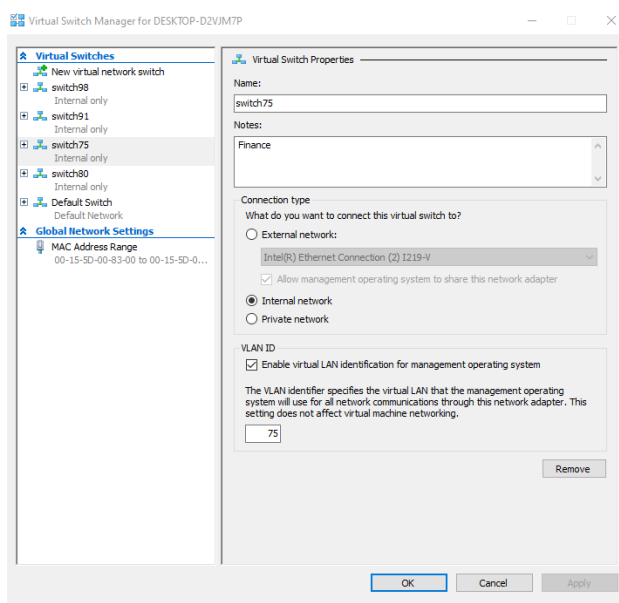


Рисунок 2.6 — Створення внутрішнього віртуального комутатора switch75 для підмережі VLAN75.

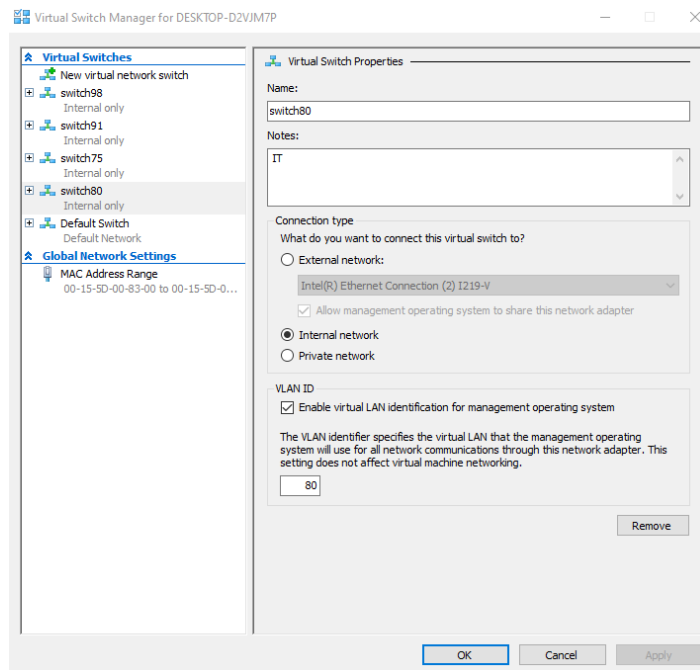


Рисунок 2.7 — Створення внутрішнього віртуального комутатора switch80 для підмережі VLAN80.

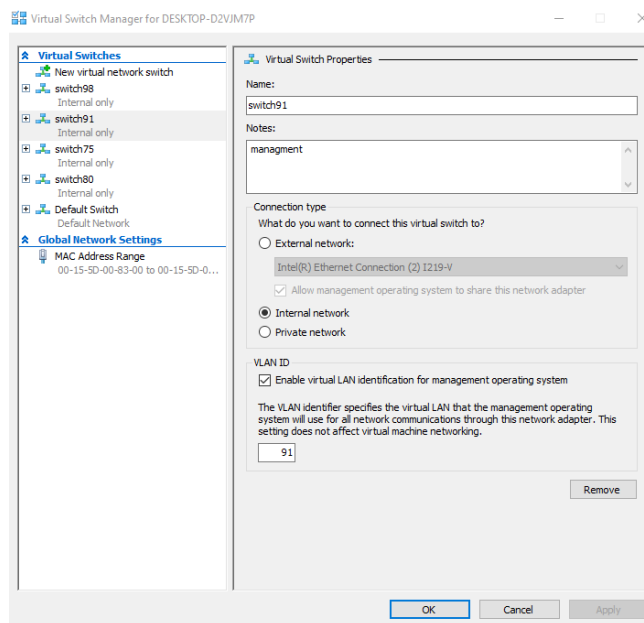


Рисунок 2.8 — Створення внутрішнього віртуального комутатора switch91 для підмережі VLAN91.

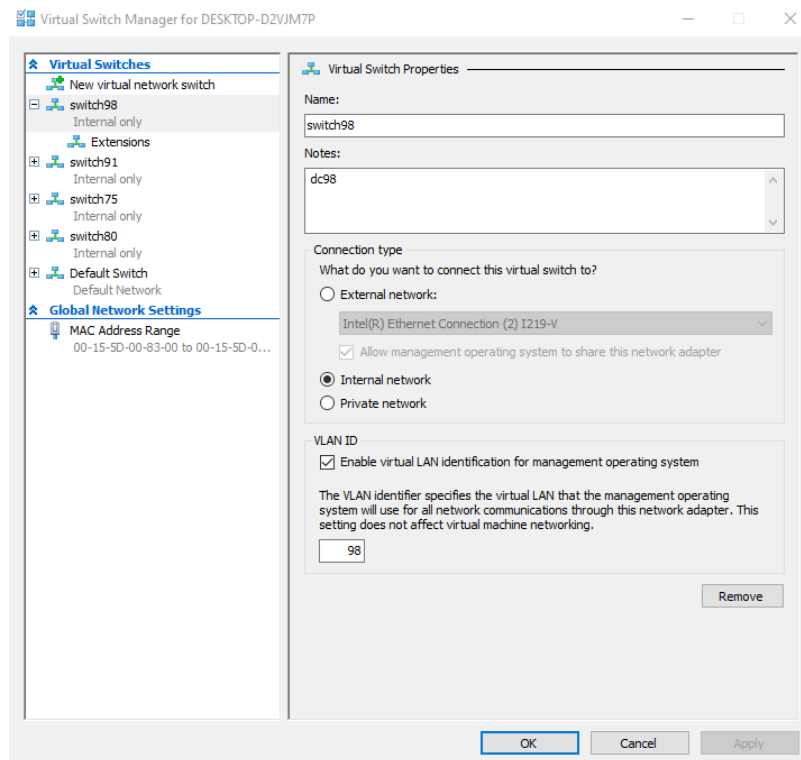


Рисунок 2.9 — Створення внутрішнього віртуального комутатора switch98 для підмережі VLAN98.

За допомогою створених віртуальних комутаторів потрібно додати NIC до ВМ та мережевого екрану pfSense в гіпервізорі VMware Workstation 16 Pro. В редакторі віртуальної мережі(рис. 2.10) можливість використовувати для перегляду та зміни налаштувань мереж ключів, додавання та видалення віртуальних мереж та створення спеціальних конфігурацій віртуальної мережі. Зміни, які вносяться у редакторі віртуальної мережі, впливають на всі віртуальні машини, що працюють на хости. Дуже важливо зробити відкати на віртуальних машинах поточного стану.

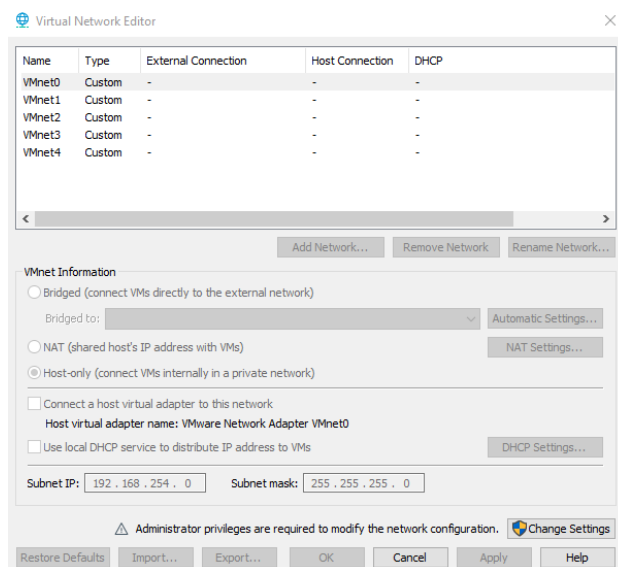


Рисунок 2.10 — Доданий до віртуальної мережі мережеві адаптери комутаторів в Virtual Network Editor.

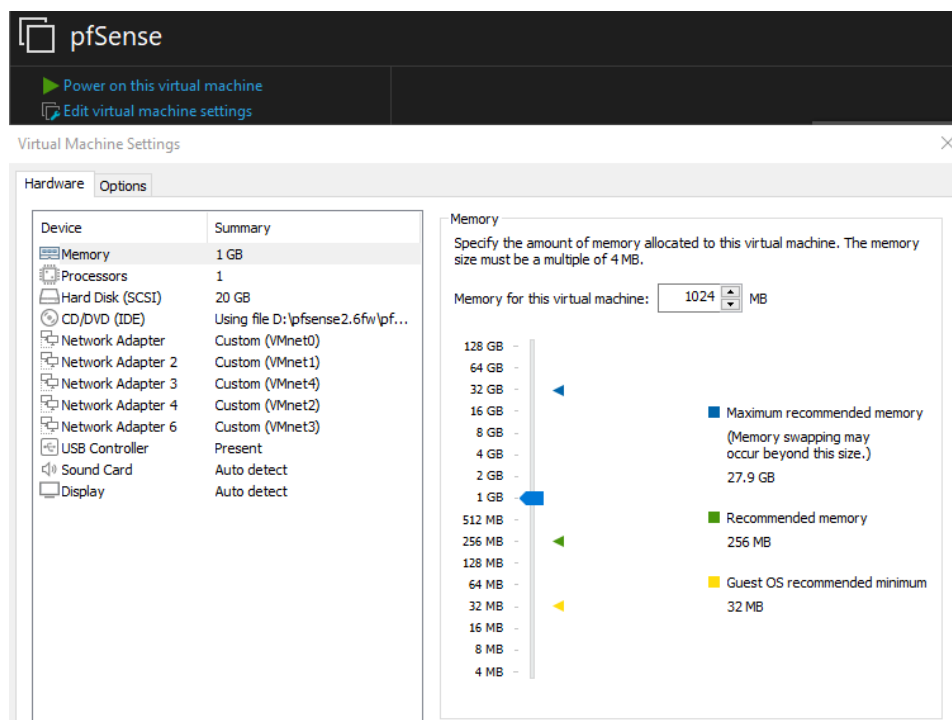


Рисунок 2.11 — Додавання мережевих адаптерів віртуальних мереж на брандмауєрі pfSense.

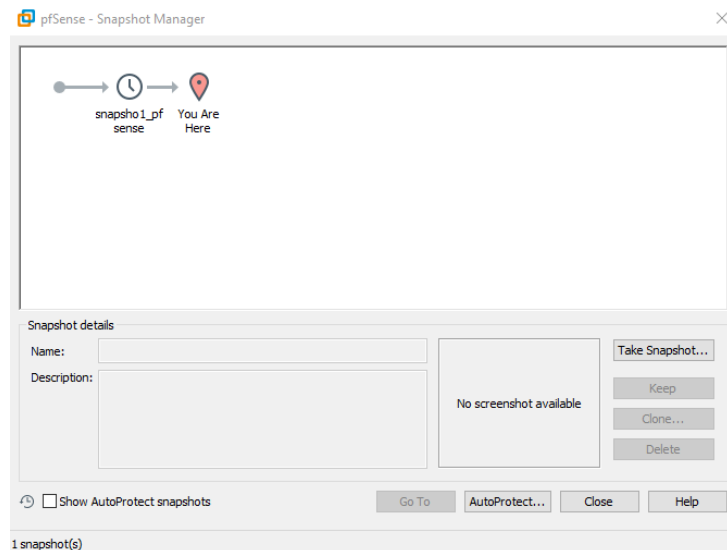


Рисунок 2.12 — Створений знімок для ВМ мережевого екрану pfSense.

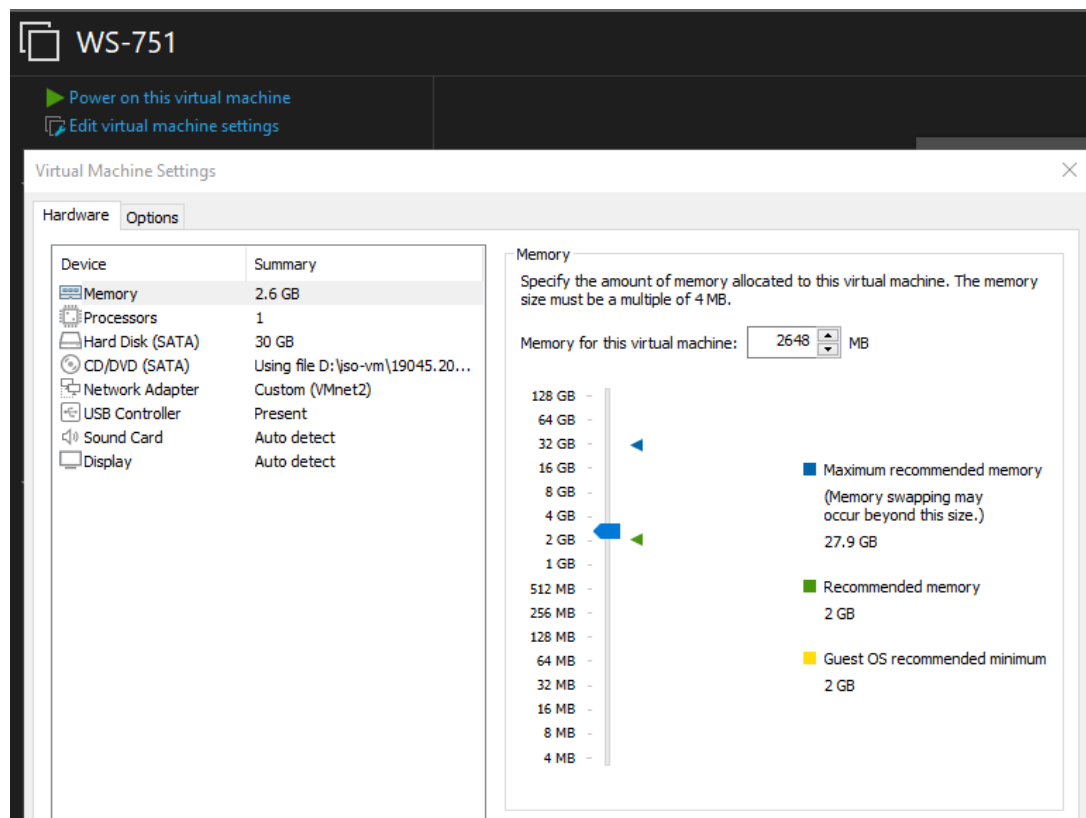


Рисунок 2.13 — Доданий мережевий адаптер віртуальної мережі на WS-751.

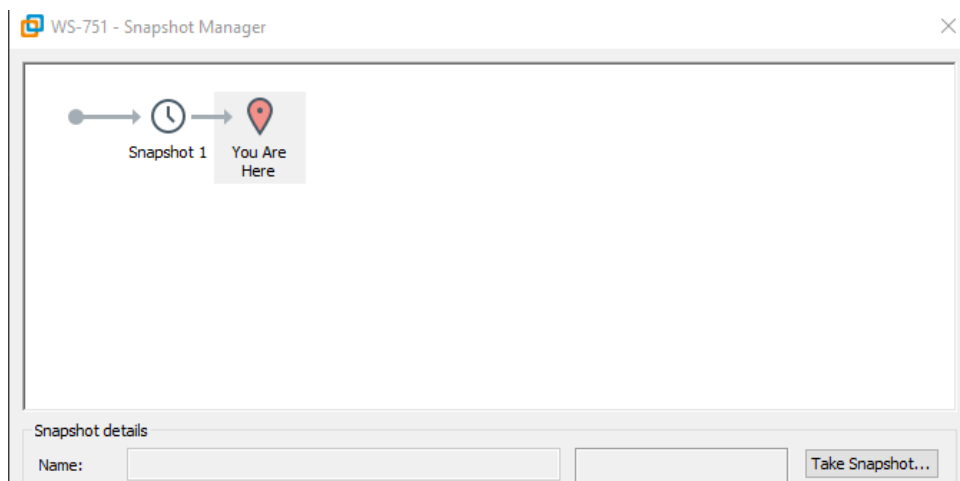


Рисунок 2.14 — Створений знімок для ВМ WS-751.

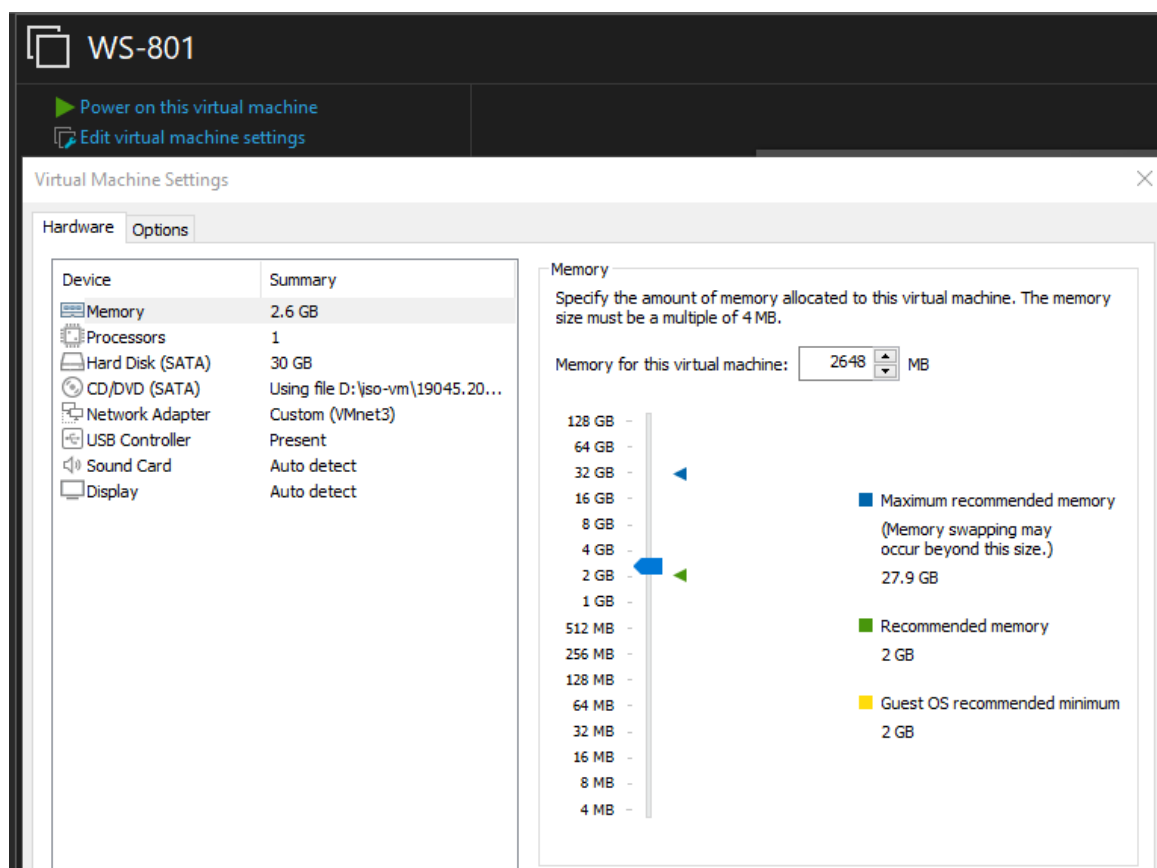


Рисунок 2.15 — Доданий мережевий адаптер віртуальної мережі на WS-801.

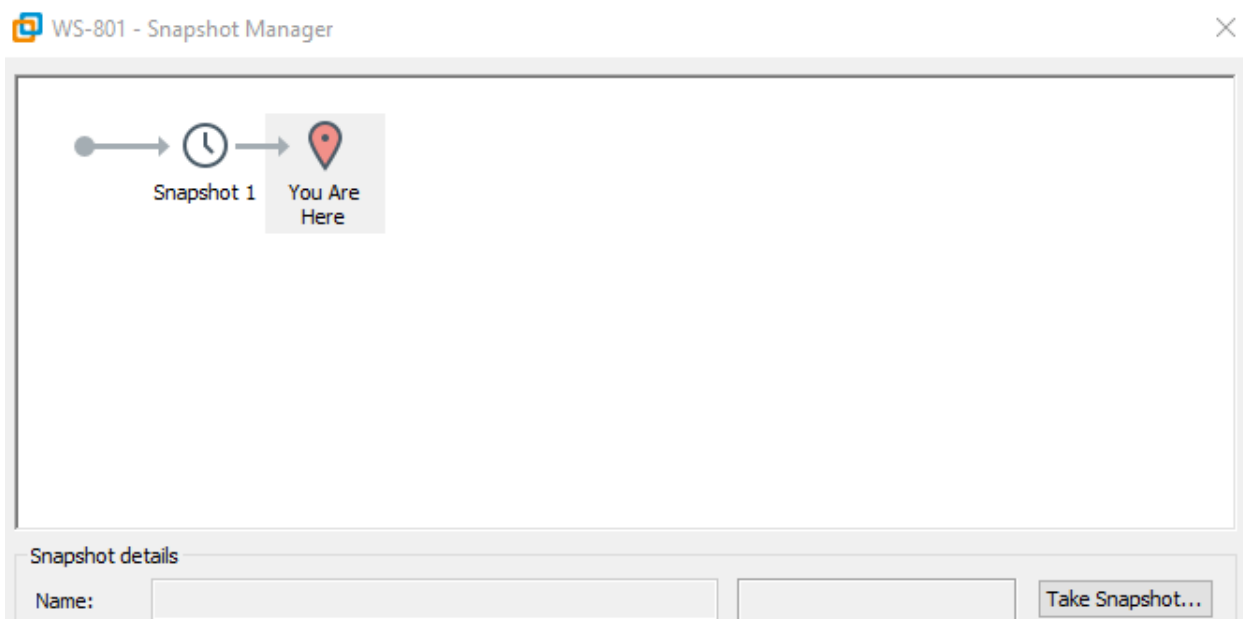


Рисунок 2.16 — Створений знімок для ВМ WS-801.

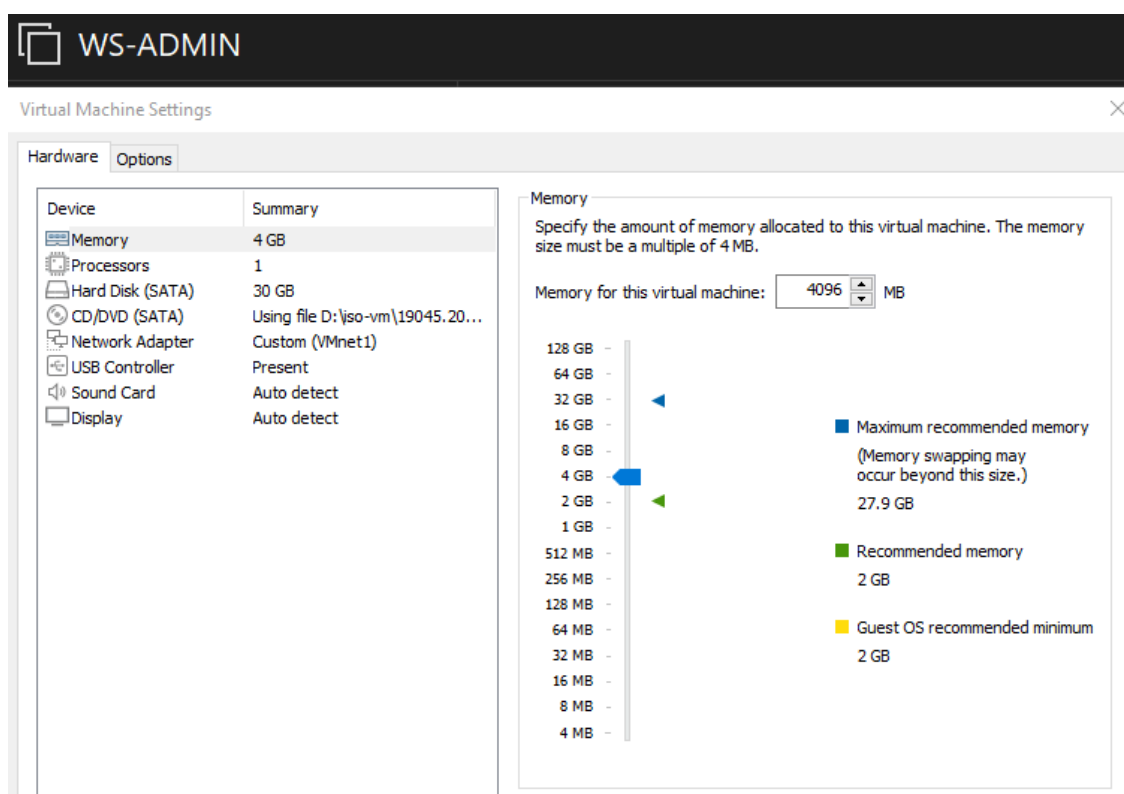


Рисунок 2.17 — Доданий мережевий адаптер віртуальної мережі на WS-ADMIN.

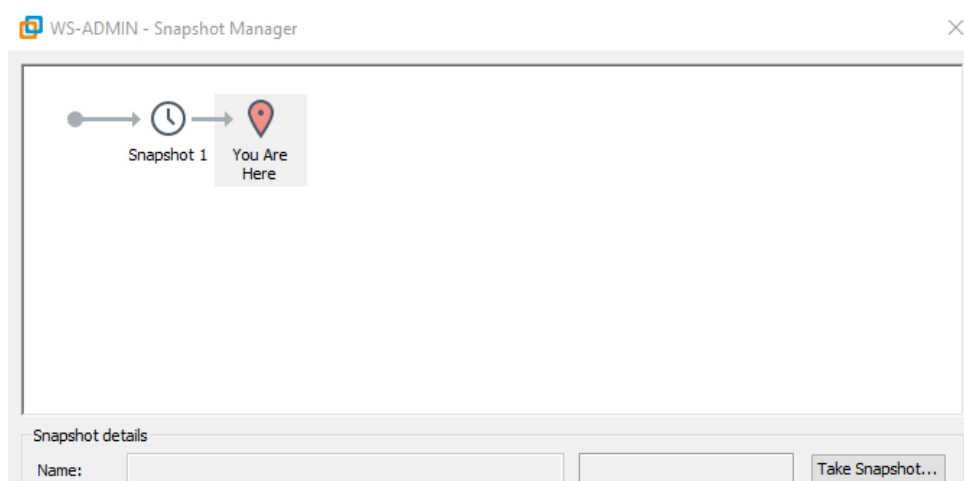


Рисунок 2.18 — Створений знімок для VM WS- ADMIN.

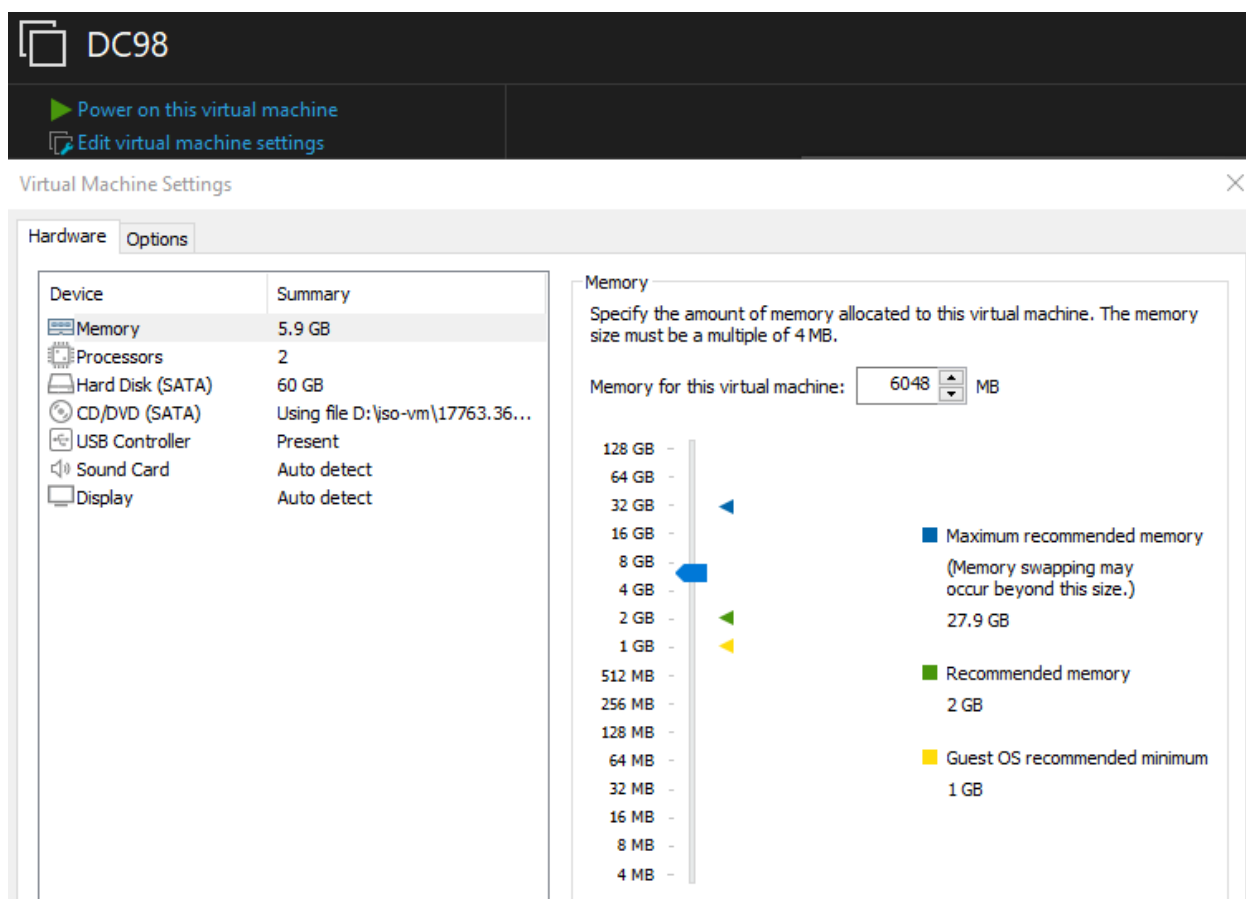


Рисунок 2.19 — Доданий мережевий адаптер віртуальної мережі на DC98.

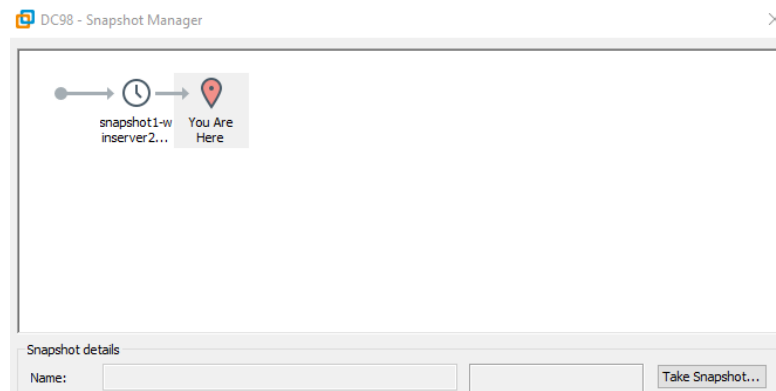


Рисунок 2.20 — Створений знімок для VM WS- ADMIN.

### 2.3 Налаштування мережевого екрану pfSense.

Після процесу встановлення із зовнішнього носія на жорсткий диск брандмауера pfSense було успішно встановлено та перезавантажено. Одразу запускається початкове меню налаштування мережевого екрану. В данній конфігурації піднялося два мережеві інтерфейси WAN та LAN. Інтерфейс WAN отримав IP-адресу. На інтерфейсі LAN також призначено IP-адреса, але її потрібно змінити та призначити іншу. Саме цей інтерфейс буде здійснювати керування мережевим екраном, тому потрібно на ньому виконати веб-конфігурацію всього брандмауера.

```
The interfaces will be assigned as follows:
WAN  -> em0
LAN  -> em1

Do you want to proceed [y/n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

Рисунок 2.21 — Доступні інтерфейси для налаштування на pfsense.

```

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.91.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 29

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

```

Рисунок 2.22 — Налаштування ір-адреси для інтерфейсу LAN.

```

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.108/24
LAN (lan)      -> em1      -> v4: 192.168.91.1/29

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 

```

Рисунок 2.23 — Основне консольне меню мережевого екрану pfSense для налаштування.

```

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.91.1/29
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://192.168.91.1/

Press <ENTER> to continue.

```

Рисунок 2.24 — Налаштування webConfigurator protocol для налагодження через веб-сайт pfsense.

Далі заходимо в WS-ADMIN та подальші налаштування мережевого екрану pfSense будуть здійснюватися за допомогою веб-браузера за URL-адресою **http[:]//192[.]168[.]91[.]1/**.

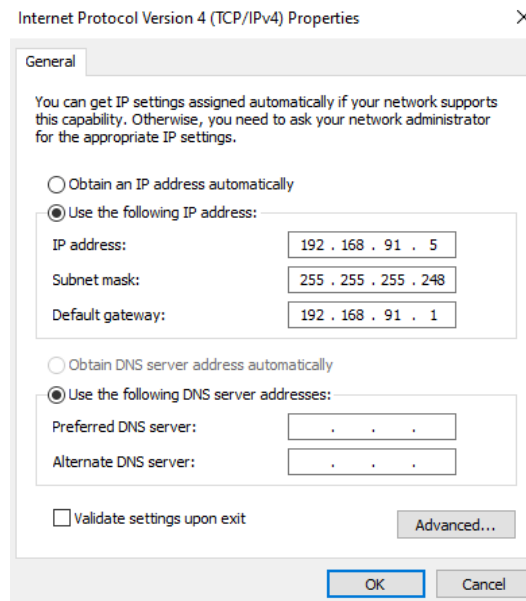


Рисунок 2.25 — Налаштування статичної Ірv4 адреси на робочій станції WS-ADMIN в підмережі VLAN91.

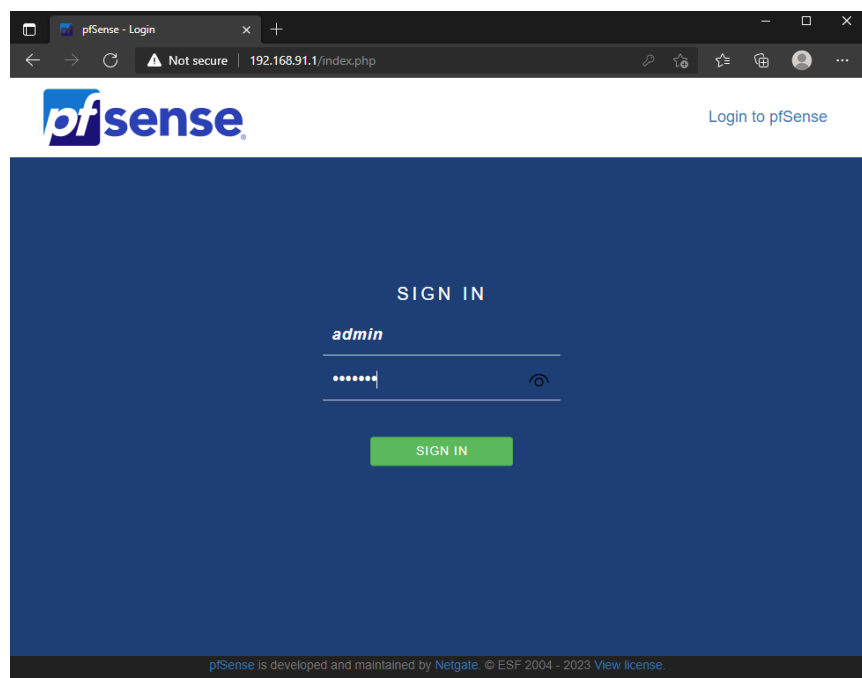


Рисунок 2.25 — Введення облікових даних для керування мережевим екраном pfSense за допомогою веб-інтерфейсу.

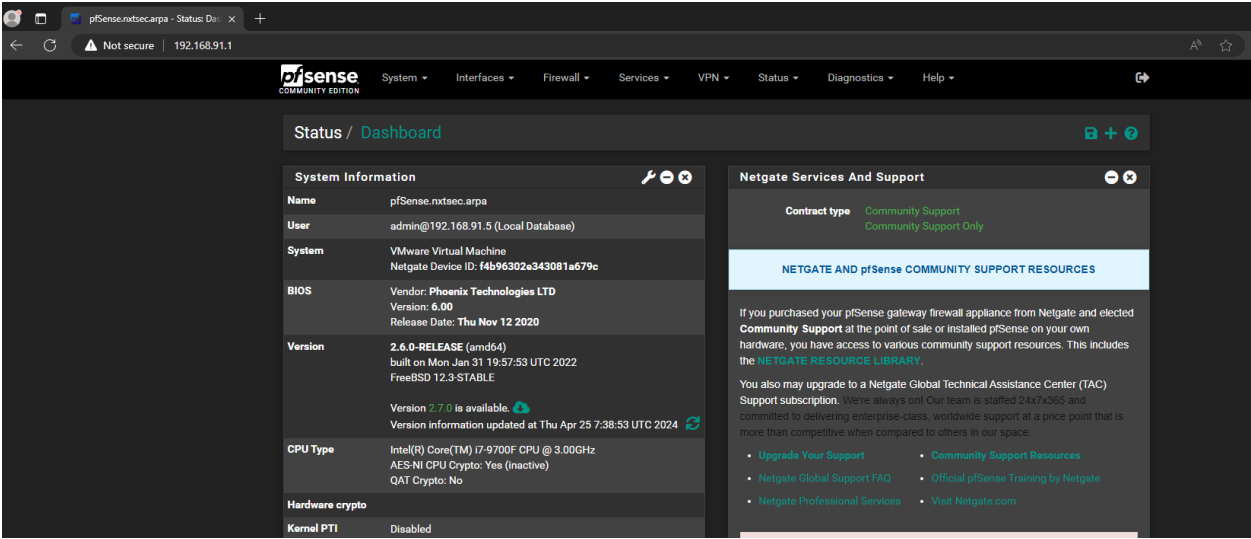


Рисунок 2.26 — Інформаційна панель мережевого екрану pfSense.

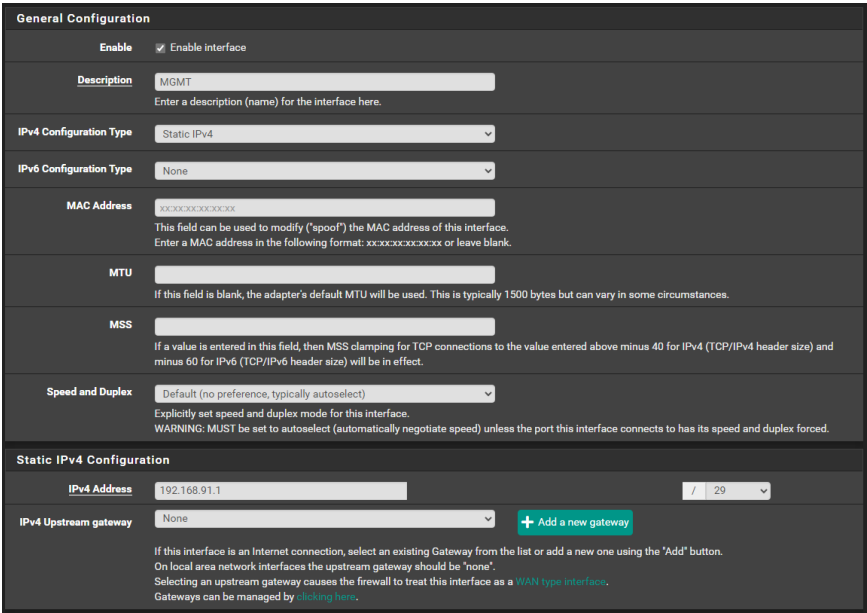


Рисунок 2.27 — Налаштована ір-адреса для підмережі VLAN91 та активований інтерфейс на мережевому екрані pfSense.

Interfaces / VLAN98 (em2)

General Configuration

Enable

☒ Enable interface

Description

VLAN98

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.98.1

/ 28

IPv4 Upstream gateway

None

+ Add a new gateway

Рисунок 2.28 — Налаштована ір-адреса для підмережі VLAN98 та активований інтерфейс на мережевому екрані pfSense .

Interfaces / VLAN75 (em3)

General Configuration

Enable

☒ Enable interface

Description

VLAN75

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.75.1

/ 27

IPv4 Upstream gateway

None

+ Add a new gateway

Рисунок 2.29 — Налаштована ір-адреса для підмережі VLAN75 та активований інтерфейс на мережевому екрані pfSense .

Interfaces / **VLAN80 (em4)**

**General Configuration**

**Enable** ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxx:xxxxxx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address**  /

**IPv4 Upstream gateway**  [+ Add a new gateway](#)

Рисунок 2.30 — Налаштована ір-адреса для підмережі VLAN80 та активований інтерфейс на мережевому екрані pfSense.

Правила брандмауера pfSense дають змогу контролювати вхідний та вихідний трафік підмереж таких як VLAN91, VLAN98, VLAN80, VLAN75. За допомогою правил pfSense приймає рішення відхиляти, приймати або блокувати трафік, який проходить так і виходить із мережі. Для налаштування правила потрібно перейти до підрозділу Rules в розділі Firewall . Поведінка брандмауера pfSense за замовчуванням полягає в тому, щоб блокувати весь трафік, якщо правило брандмауера не дозволяє цей трафік явно.

Firewall / **Rules** / **WAN**

Floating **WAN** MGMT VLAN98 VLAN75 VLAN80

Rules (Drag to Change Order)

|                          | States     | Protocol      | Source | Port | Destination  | Port     | Gateway | Queue | Schedule | Description       | Actions                                                                                    |
|--------------------------|------------|---------------|--------|------|--------------|----------|---------|-------|----------|-------------------|--------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | ✓ 0/0 B    | IPv4 ICMP any | *      | *    | *            | *        | *       | none  |          | Allow ping on WAN | <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Save</a> <a href="#">Separator</a> |
| <input type="checkbox"/> | ✓ 0/75 KiB | IPv4 TCP      | *      | *    | 192.168.91.5 | 22 (SSH) | *       | none  |          | NAT               | <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Save</a> <a href="#">Separator</a> |

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Рисунок 2.31 — Приклад дозволених правила мережевого екрану для інтерфейсу WAN.

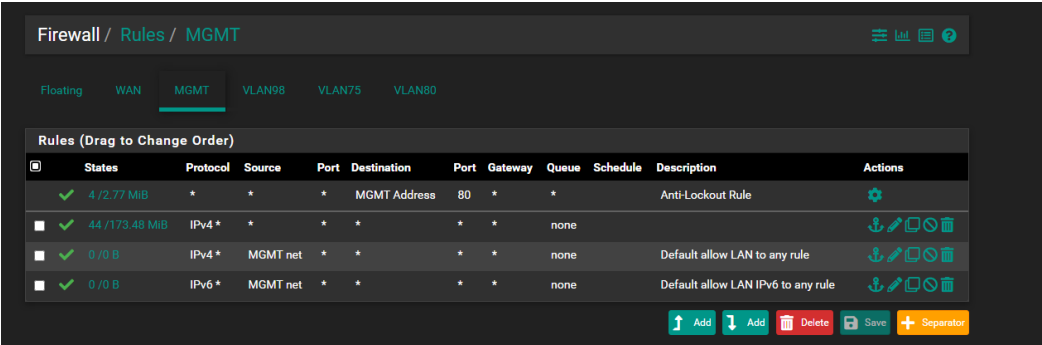


Рисунок 2.32 — Приклад дозвільного правила для вхідного та вихідного трафіку мережевого екрану для інтерфейсу MGMT.

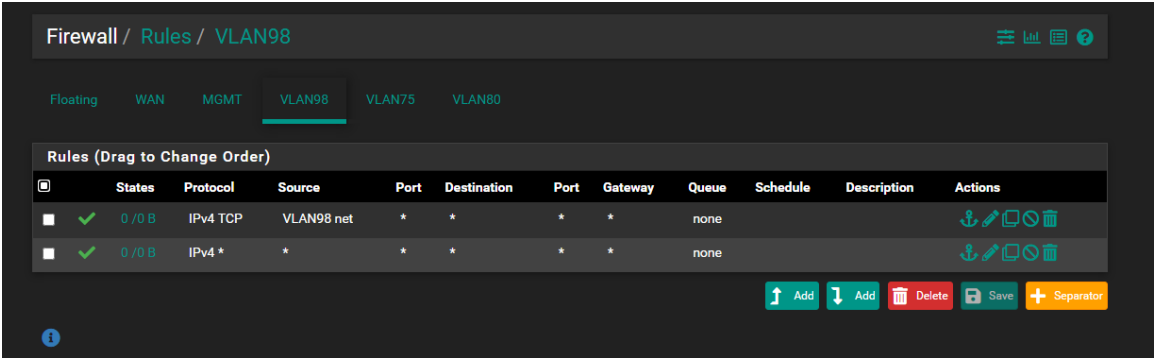


Рисунок 2.33 — Приклад дозвільного правила для вхідного та вихідного трафіку мережевого екрану для інтерфейсу VLAN98.

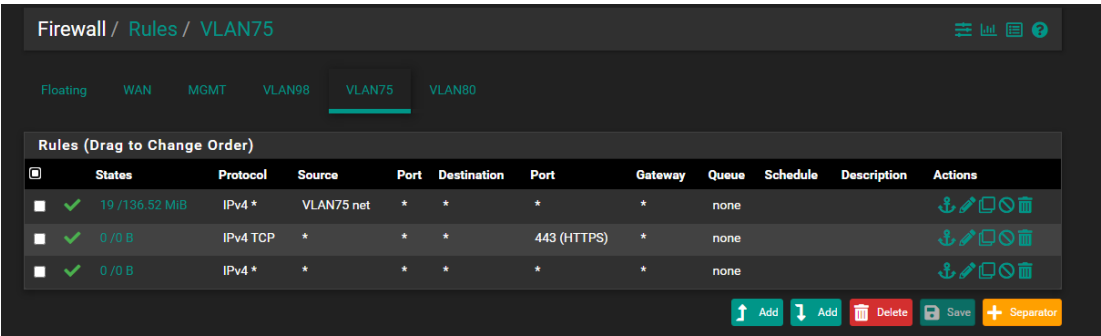


Рисунок 2.34 — Приклад дозвільного правила для вхідного та вихідного трафіку мережевого екрану для інтерфейсу VLAN75.

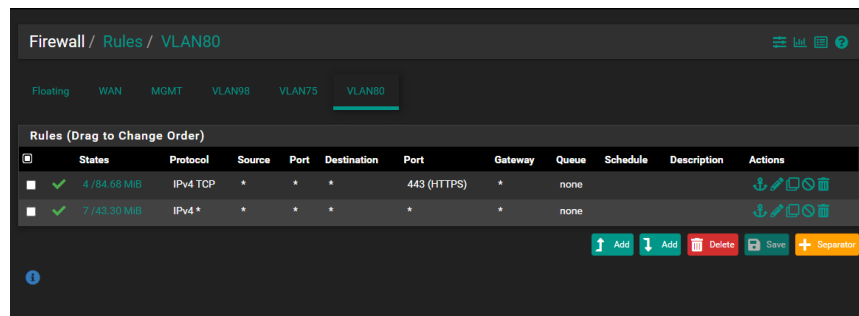


Рисунок 2.35 — Приклад дозвільного правила для вхідного та вихідного трафіку мережевого екрану для інтерфейсу VLAN80.

### 3. Базове налаштування та розгортання Active Directory на ОС Windows Server 2019.

Як вже згадувалося вище, Active Directory є базовою технологією, що дозволяє мережевим адміністраторам ефективно створювати та керувати доменами, користувачами та об'єктами в мережі. Її розроблено з можливістю масштабування, що полегшує об'єднання великої кількості користувачів у керовані групи та підгрупи, одночасно контролюючи права доступу на різних рівнях.

Структура Active Directory складається з трьох основних рівнів: доменів, дерев і лісів. Домен охоплює набір об'єктів, таких як користувачі або пристрої, що мають спільну базу даних. Древа - це групи цих доменів, пов'язані спільною структурою, а ліс - це сукупність декількох дерев, пов'язаних між собою довірчими відносинами, що утворюють верхній рівень організаційної структури. На кожному з цих рівнів можуть бути визначені конкретні права доступу та комунікації.

Ключові поняття в Active Directory включають в себе наступні:

- Каталог - містить усю інформацію про об'єкти Active Directory.
- Об'єкт - позначає об'єкти у каталозі, зокрема користувачів, групи або спільні теки.
- Домен - слугує контейнером для об'єктів каталогу, з можливістю співіснування кількох доменів у лісі, кожен з яких підтримує власну колекцію об'єктів.
- Дерево - група доменів, які мають спільний кореневий домен.

- Ліс - вершина організаційної структури в Active Directory, що складається з декількох дерев з довірчими відносинами між ними.

При першому вході на Windows Server 2019 завантажується програма Server Manager(рис. 2.38), що має вигляд графічної консолі який дає змогу керувати локальними та віддаленими серверами на базі Windows, при цьому не вимагаючи фізичного доступу до серверів або необхідності вмикати підключення до кожного сервера за протоколом RDP. Також наявна можливість керувати компонентами і сервісами на сервері [20].

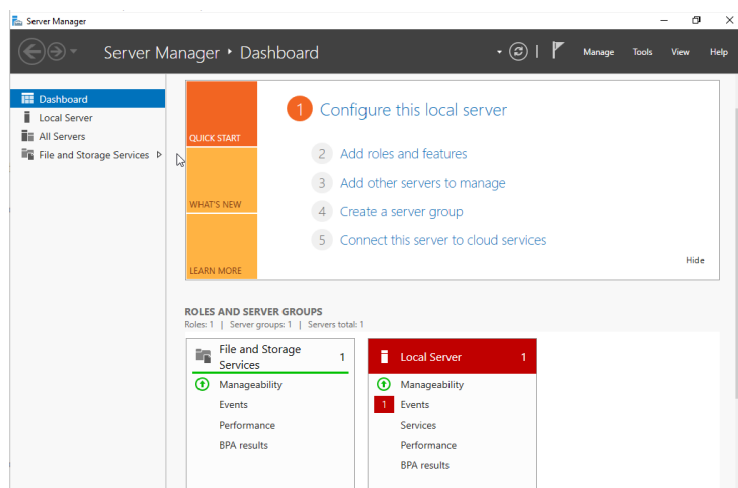


Рисунок 2.38 — Панель управління диспетчера серверів.

Перед тим, як розгортати Active Directory потрібно налаштувати статичну IPv4 адресу та змінити ім'я серверу (рис.2.39-40).

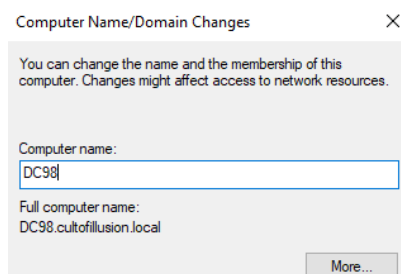


Рисунок 2.39 — Панель управління диспетчера серверів.

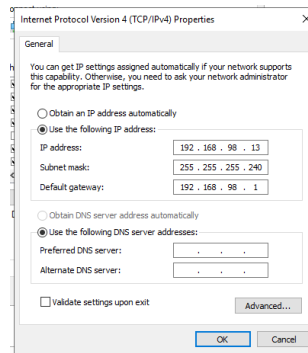


Рисунок 2.40 — Призначення статичну IPv4 адресу для мережевого адаптера на DC98.

На даному етапі (рис. 2.40) важливо вибрати встановлення на основі ролей або функцій, адже це дає можливість адміністратору тонкого контролю над тим, які компоненти сервера будуть встановлені, а отже налаштувати Windows Server до відповідно до потреб.

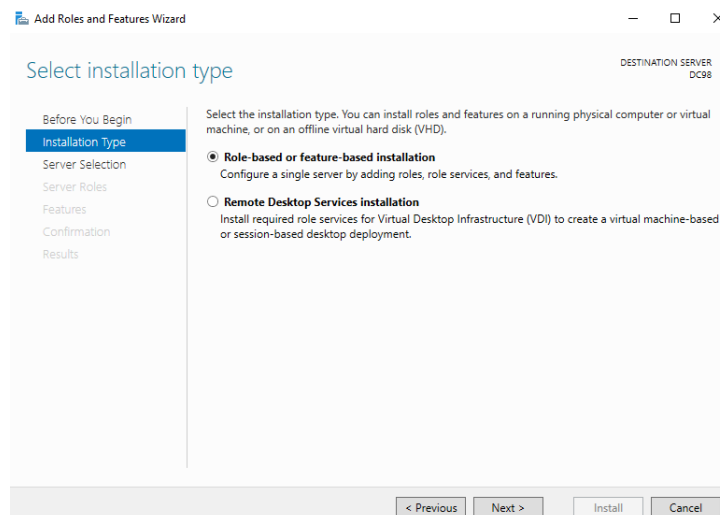


Рисунок 2.41 — Вибір встановлення на основі ролей або функцій .

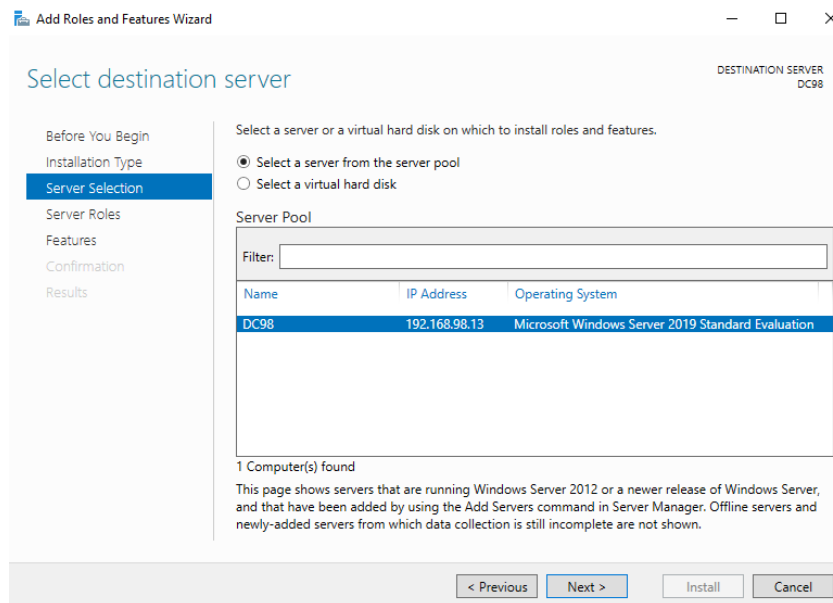


Рисунок 2.42 — Вибір сервера DC98 із пулу серверів.

Доступно багато ролей для серверу DC98 (рис. 2.43), але спочатку обираємо Active Directory Domain Services, інші можна, додати, коли буде нагода.

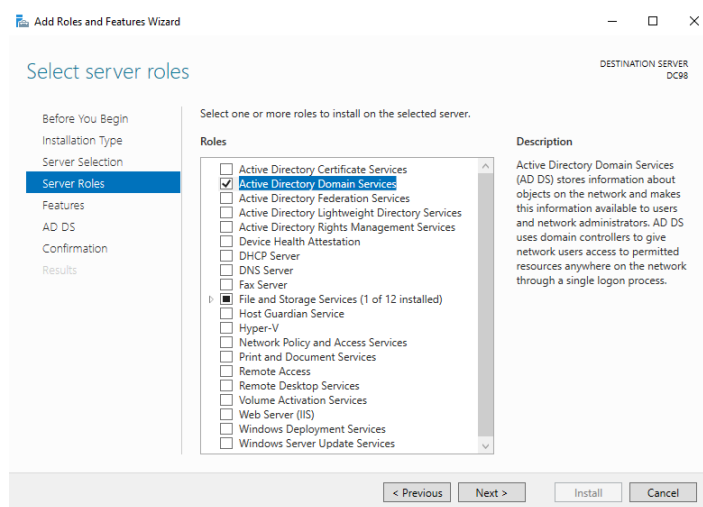


Рисунок 2.43 — Встановлення ролі AD DS сервера DC98.

Далі важливо встановити функцію керування груповою політикою(рис. 2.44), яка дає змогу керувати кількома користувачами та конфігураціями хостів, присутніх у середовищі Active Directory.

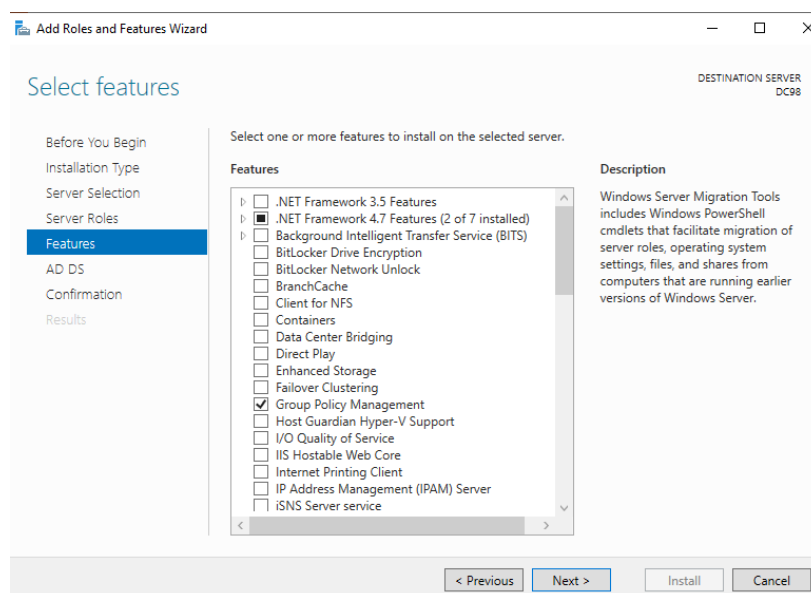


Рисунок 2.44 — Встановлення функції Group Policy Management.

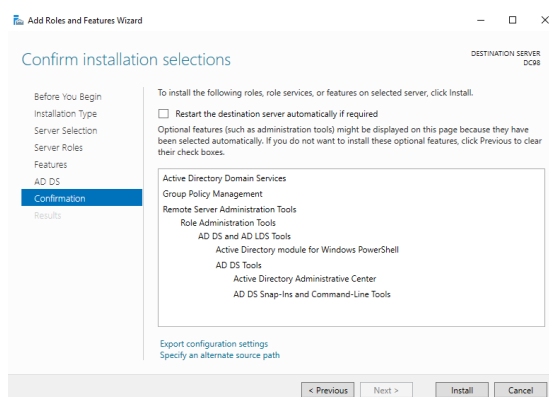


Рисунок 2.45 — Підтвердження попередніх встановлених ролей та функцій на сервер DC98.

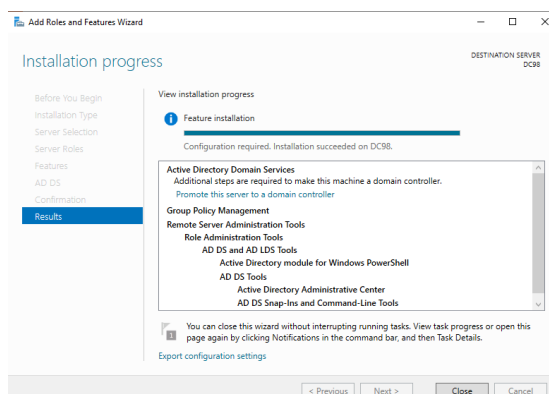


Рисунок 2.46 — Процес встановлення функцій AD DS.

Після завершення встановлення функції AD DS з'явилося сповіщення з прапорцем (рис. 2.47), тому варто перейти до конфігурацій, необхідних на етапі після розгортання.

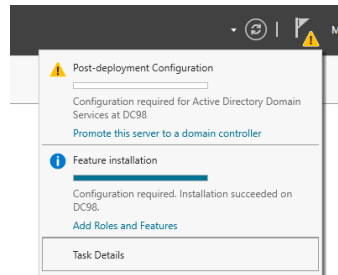


Рисунок 2.47 — Вікно із сповіщенням.

Отже, у конфігурації розгортання одразу потрібно створити новий ліс з кореневим ім'ям домену cultofillusion.local (2.47). Ліс в Active Directory є найвищим організаційним рівнем. Кожен ліс може мати спільну базу даних, глобальний список адрес і межі безпеки. Тому за замовчуванням адміністратор, що належить до одного лісу, не може зробити його представником іншого лісу.

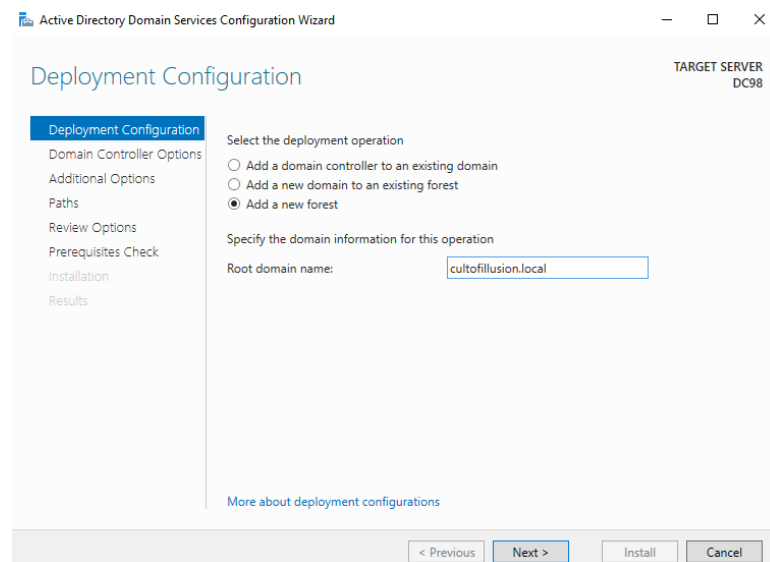


Рисунок 2.48 — Розгортання контролера домена.

Далі налаштовується можливість контролера домену(рис. 2.49)., позначивши перші два пункти, які дозволяють доступ до DNS-сервера і глобального каталогу. Також потрібно ввести пароль режиму відновлення служб каталогів (Directory Services Restore Mode), який є методом завантаження у безпечному режимі для контролерів доменів серверів Windows. Функціональний рівень домену залежатиме від функціонального рівня лісу.

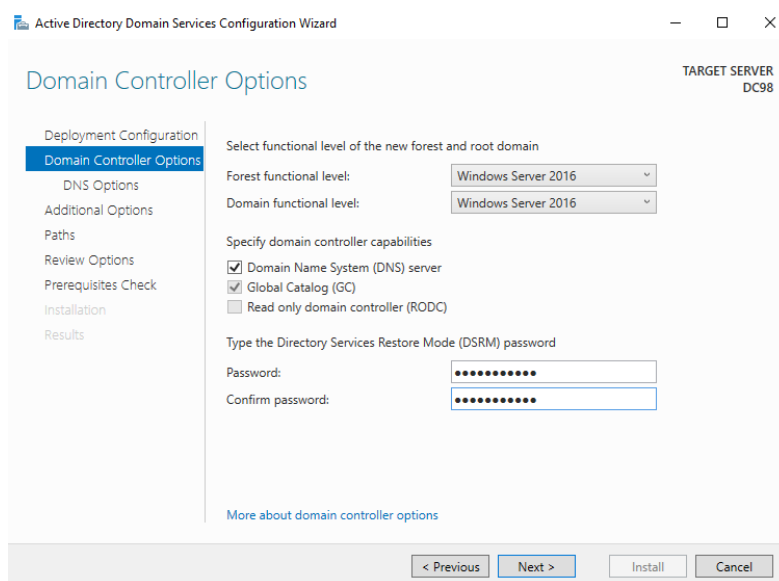


Рисунок 2.49 — Процес налаштування контролера домена.

Зазвичай доменне ім'я NetBIOS є субдоменом доменного імені DNS. Якщо доменне ім'я DNS – cultofillusion.local, то доменне ім'я NetBIOS – cultofillusion, тому підтвердження (рис. 2.50).

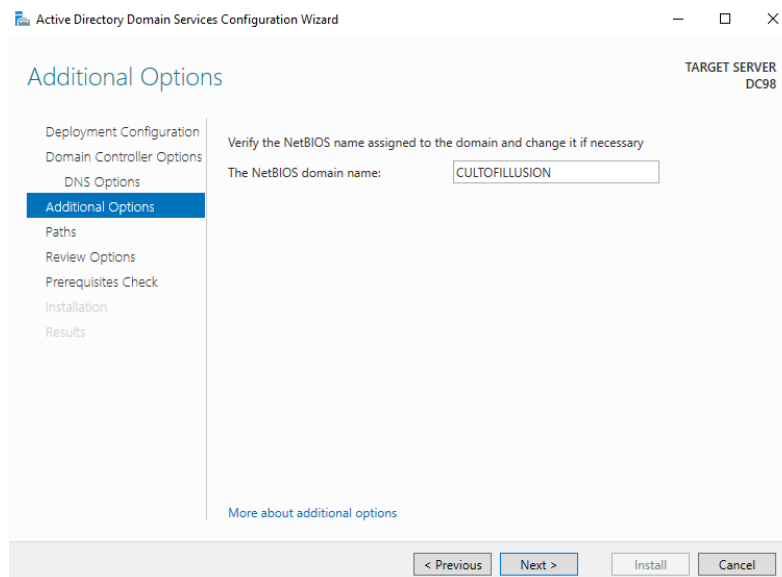


Рисунок 2.50 — Автоматично призначене доменне ім'я NetBIOS.

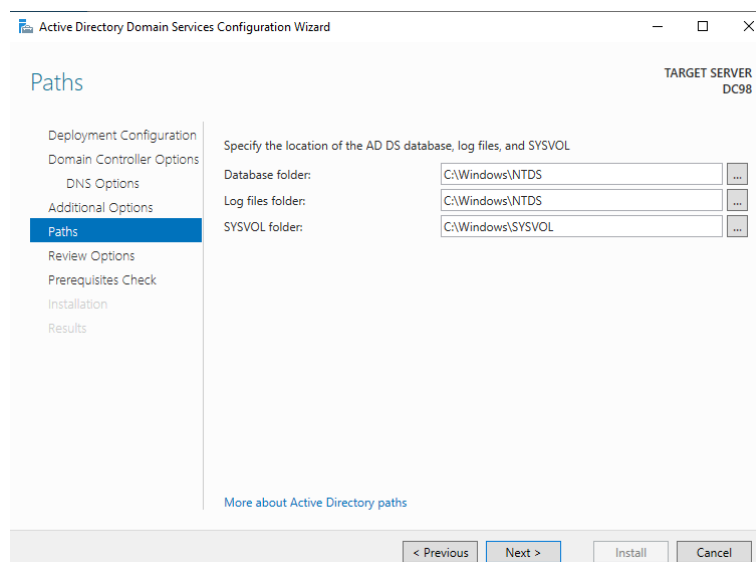


Рисунок 2.51 — Вказання шляхів до бази даних AD DS, файлів журналів та сховища SYSVOL.

Після проходження перевірки встановлених специфікацій відбувається подальше вдале встановлення. Сервер DC98 перезавантажиться, а потім потрібно увійти обліковим записом (наприклад, administrator) у домен cultofillusion (рис. 2.52).

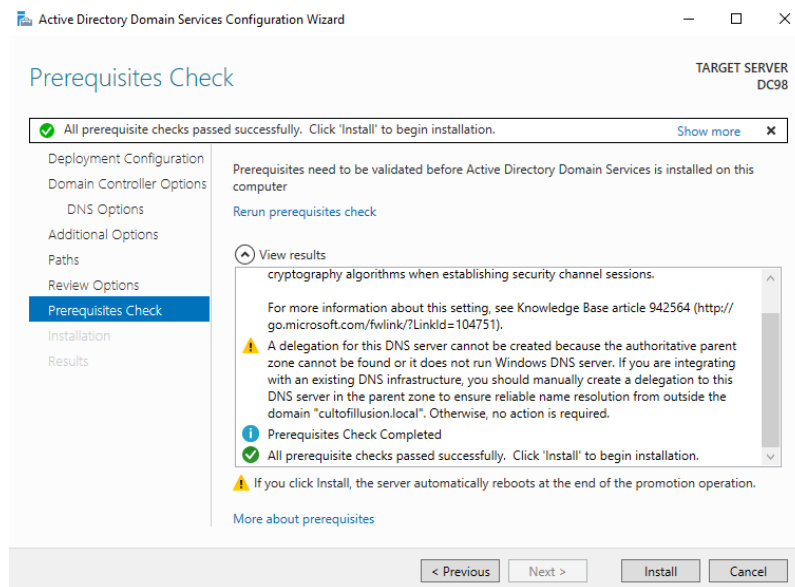


Рисунок 2.52 — Успішна пройдена перевірка специфікацій.



Рисунок 2.52 — Вхід обліковим записом Administrator у домен cultofillusion.local.

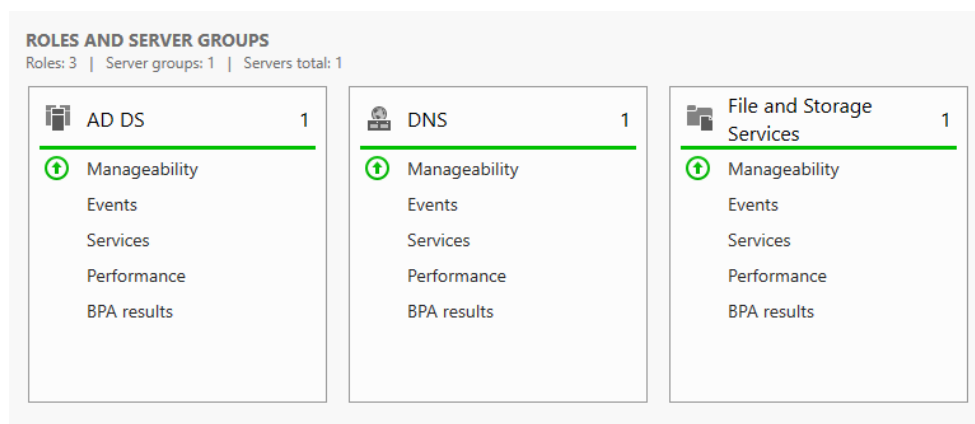


Рисунок 2.53 — Результат на панелі менеджера після налаштувань AD.

Наступний етап створення організаційних одиниць та користувачів які представлені на структурній діаграмі домену рис. 2.54 за допомогою

Active Directory Users and Computers а також налаштування dhcp-серверу і підключення до домену робочих станцій представлено в Додатку Б.

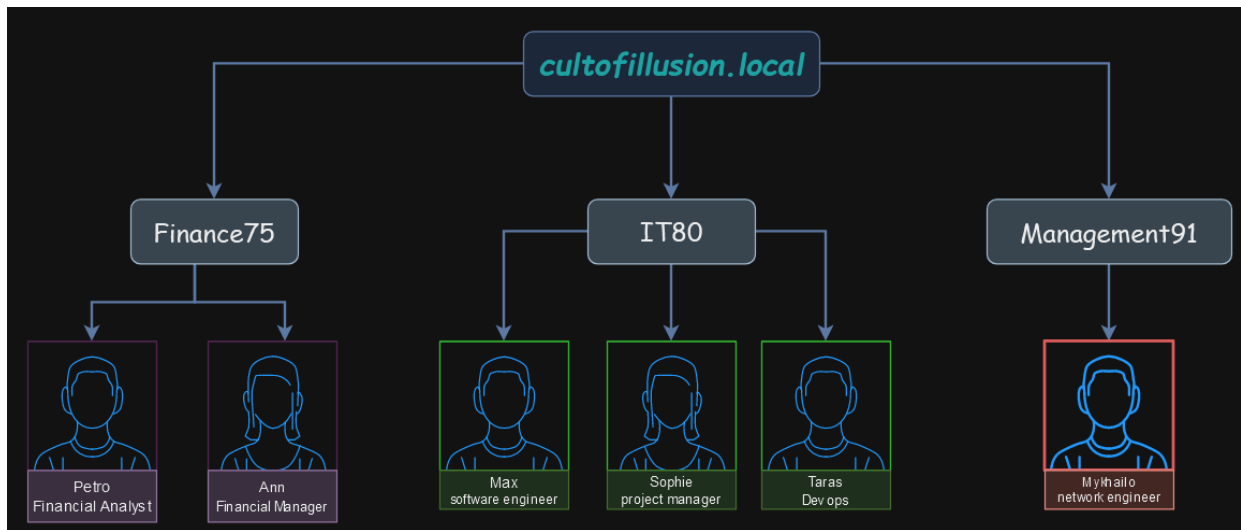


Рисунок 2.54 — Структурна діаграма домену cultofillusion.local.

## РОЗДІЛ 3. РЕАЛІЗАЦІЯ СКАНУВАННЯ ACTIVE DIRECTORY

Сканування системи є важливим етапом для подальшого знаходження вразливості та розуміння системи.

```
(xonix@kali) ~/pwnd
$ nmap -sC -sV -A -T4 -Pn 192.168.98.13 -oN scan-dc98.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-29 03:22 EEST
Nmap scan report for 192.168.98.13
Host is up (0.00086s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-04-29 10:22:32Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: cultofillusion.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: cultofillusion.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ ssl-date: 2024-04-29T10:23:18+00:00; +9h59m59s from scanner time.
|_ ssl-cert: Subject: commonName=DC98.cultofillusion.local
|_ Not valid before: 2024-04-24T23:17:59
|_ Not valid after: 2024-10-24T23:17:59
|_ rdp-ntlm-info:
|   Target Name: CULTOFILLUSION
|   NetBIOS Domain Name: CULTOFILLUSION
|   NetBIOS Computer Name: DC98
|   DNS Domain Name: cultofillusion.local
|   DNS Computer Name: DC98.cultofillusion.local
|   DNS Tree Name: cultofillusion.local
|   Product Version: 10.0.17763
|   System Time: 2024-04-29T10:22:37+00:00
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Service Unavailable
|_ http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC98; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Рисунок 3.1 – Сканування за допомогою nmap контролера домену DC98.

```
(xonix@kali) ~/pwnd
$ nmap -sC -sV -A -Pn -T4 192.168.80.9
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-29 22:13 EEST
Nmap scan report for 192.168.80.9
Host is up (0.00082s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ ssl-date: 2024-04-30T05:08:06+00:00; +9h53m58s from scanner time.
|_ ssl-cert: Subject: commonName=WS-801.cultofillusion.local
|_ Not valid before: 2024-04-27T22:04:43
|_ Not valid after: 2024-10-27T22:04:43
|_ rdp-ntlm-info:
|   Target Name: CULTOFILLUSION
|   NetBIOS Domain Name: CULTOFILLUSION
|   NetBIOS Computer Name: WS-801
|   DNS Domain Name: cultofillusion.local
|   DNS Computer Name: WS-801.cultofillusion.local
|   DNS Tree Name: cultofillusion.local
|   Product Version: 10.0.19041
|   System Time: 2024-04-30T05:07:57+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   311:
|     Message signing enabled but not required
|_ clock-skew: mean: 9h53m57s, deviation: 0s, median: 9h53m57s
|_ smb2-time:
|   date: 2024-04-30T05:07:59
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 23.00 seconds

(xonix@kali) ~/pwnd
$
```

Рисунок 3.2 – Сканування робочої станції WS-801.

```

(xonix@kali) [~/pwnd]
$ nmap -sC -sV -A -Pn -T4 192.168.75.6
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-29 22:16 EEST
Nmap scan report for 192.168.75.6
Host is up (0.00072s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   3072 465586a0dfe0d951af51201836cc3e71 (RSA)
|   256 93c4ebcca79a273728fbc2cafb2ebd70 (ECDSA)
|   256 ffb6c69f992055b6904fcc34b0a5bdf (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Windows 10 Enterprise Evaluation 19045 microsoft-ds (workgroup: CULTOFILLUSION)
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
| rdp-ntlm-info:
|   Target Name: CULTOFILLUSION
|   NetBIOS Domain Name: CULTOFILLUSION
|   NetBIOS Computer Name: WS-751
|   DNS Domain Name: cultofillusion.local
|   DNS Computer Name: WS-751.cultofillusion.local
|   DNS Tree Name: cultofillusion.local
|   Product Version: 10.0.19041
|   System Time: 2024-04-30T05:16:56+00:00
|   ssl-date: 2024-04-30T05:17:06+00:00; +10h00m01s from scanner time.
|   ssl-cert: Subject: commonName=WS-751.cultofillusion.local
|   Not valid before: 2024-04-27T19:38:08
|   Not valid after: 2024-10-27T19:38:08
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-title: Service Unavailable
| http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: WS-751; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 10 Enterprise Evaluation 19045 (Windows 10 Enterprise Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10:-
|   Computer name: WS-751
|   NetBIOS computer name: WS-751\*00
|   Domain name: cultofillusion.local
|   Forest name: cultofillusion.local
|   FQDN: WS-751.cultofillusion.local
|   System time: 2024-04-29T22:17:00-07:00
|_

```

Рисунок 3.3 – Сканування робочої станції WS-751.

```

(xonix@kali) [~/pwnd]
$ nmap -sC -sV -A -Pn -T4 192.168.91.5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-29 22:27 EEST
Nmap scan report for 192.168.91.5
Host is up (0.00019s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh           OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   2048 bdf072ca6d23d978dd81fa065fef2c5 (RSA)
|   256 0ad24e2201ef570e8943b76c1469795e (ECDSA)
|   256 df48fdd5fb8b46364a95e3d6ef922cba (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
| ssl-date: 2024-04-30T05:28:01+00:00; +10h00m05s from scanner time.
| ssl-cert: Subject: commonName=WS-ADMIN.cultofillusion.local
|   Not valid before: 2024-04-27T19:27:51
|   Not valid after: 2024-10-27T19:27:51
| rdp-ntlm-info:
|   Target Name: CULTOFILLUSION
|   NetBIOS Domain Name: CULTOFILLUSION
|   NetBIOS Computer Name: WS-ADMIN
|   DNS Domain Name: cultofillusion.local
|   DNS Computer Name: WS-ADMIN.cultofillusion.local
|   Product Version: 10.0.19041
|   System Time: 2024-04-30T05:27:55+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| clock-skew: mean: 10h00m04s, deviation: 0s, median: 10h00m04s
| nbstat: NetBIOS name: WS-ADMIN, NetBIOS user: <unknown>, NetBIOS MAC: 000c29319bf6 (VMware)
| smb2-time:
|   date: 2024-04-30T05:27:55
|   start date: N/A
| smb2-security-mode:
|   311:
|     Message signing enabled but not required
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.58 seconds

```

Рисунок 3.4 – Сканування робочої станції WS-ADMIN.

```
(xoniX@kali) ~/pwnd
$ sudo responder -i eth0

[+] You don't have an IPv6 address assigned.

[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]

[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
```

Рисунок 3.5 – Запуск responder на інтерфесі хоста kali.

```
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]

[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.91.3]
Responder IPv6 [::1]
Challenge set [random]
Don't Respond To Names ['ISATAP']

[+] Current Session Variables:
Responder Machine Name [WIN-9QII8D18YCK]
Responder Domain Name [529P.LOCAL]
Responder DCE-RPC Port [47397]

[+] Listening for events...

[!] Error starting TCP server on port 389, check permissions or other servers running.
[!] Error starting TCP server on port 53, check permissions or other servers running.
```

Рисунок 3.6 – конфігурація responder.

Проведена невдала атака smb relay за допомогою responder.

## ВИСНОВКИ

У даній кваліфікаційній роботі розглянуто методи та технології тестування на проникнення мережевої інфраструктури на базі Microsoft Active Directory.

У першому розділі проаналізовано які наявні методи та технології тестування на проникнення в мережній інфраструктурі на базі Active Director.

У другому розділі розроблено та налагоджено в віртуальному мережевому середовищі організації на базі Vmware, мережного екрану Pfsense та розгорнутого на DC98 Active Directory.

У третьому розділі проведений невдала атака SMB relay але вдало проскановані кінцеві точки.

В результаті було отримано досвід аналізу методів та технологій тестування на проникнення та розгортання Active Directory в мережі.

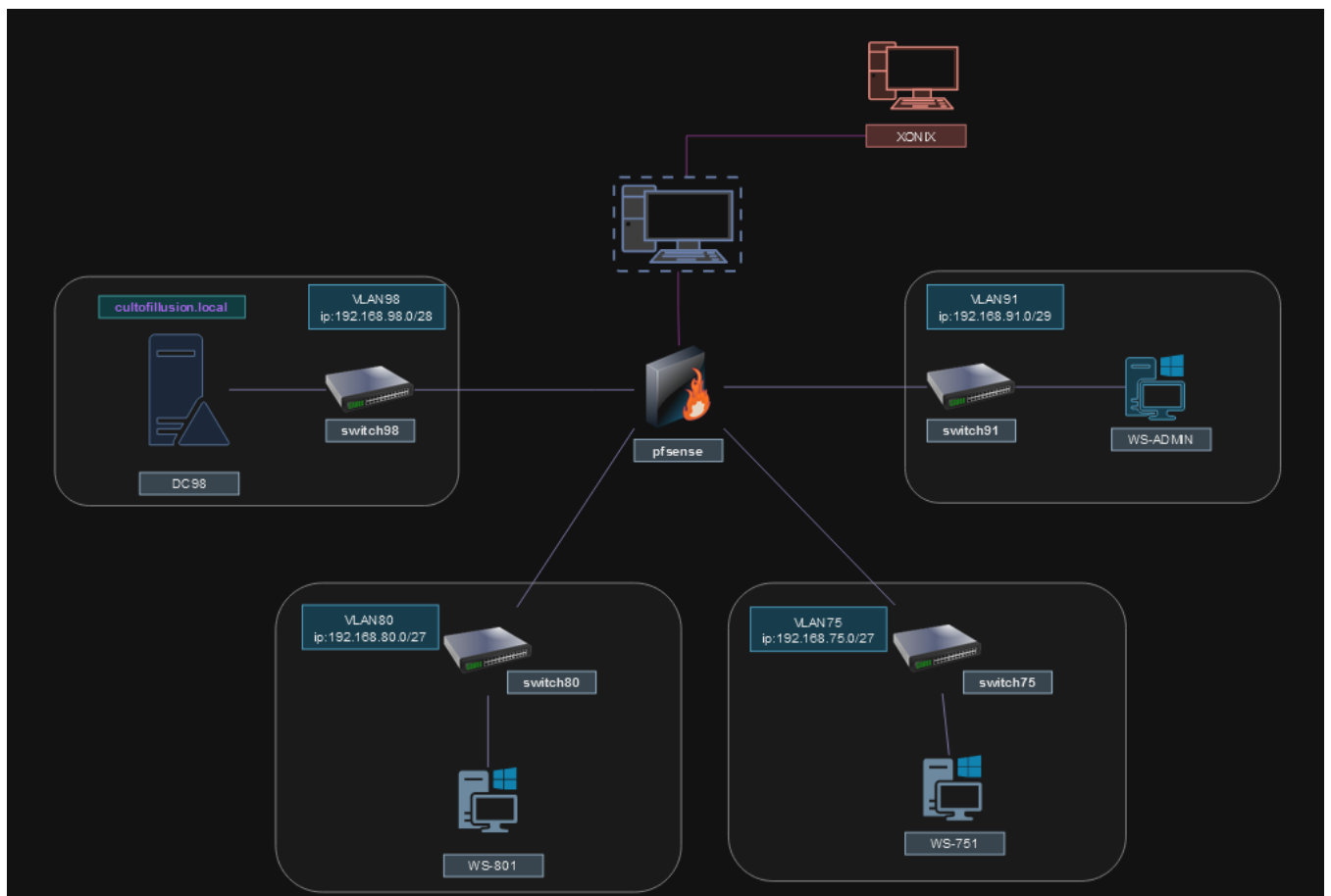
## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. <https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/#:~:text=White%20box%20penetration%20testing%2C%20sometimes,overall%20cost%20of%20an%20engagement.>
2. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
3. <https://www.varonis.com/blog/domain-controller>
4. <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/adam/what-is-active-directory-lightweight-directory-services>
5. <https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview>
6. [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-wpo/1c11d4ee-98c7-46a9-99e0-d6899d4522b9](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-wpo/1c11d4ee-98c7-46a9-99e0-d6899d4522b9)
7. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11))
8. <https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization>
9. <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-technical-overview>
10. <https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-negotiate>
11. <https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-ntlm>
12. <https://learn.microsoft.com/en-us/troubleshoot/windows-client/windows-security/enable-ntlm-2-authentication>
13. [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-apds/dd444344-fd7e-430e-b313-7e95ab9c338e](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-apds/dd444344-fd7e-430e-b313-7e95ab9c338e)
14. [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-nlmp/b38c36ed-2804-4868-a9ff-8dd3182128e4](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/b38c36ed-2804-4868-a9ff-8dd3182128e4)
15. <https://medium.com/@robert.broeckelmann/kerberos-and-windows-security-history-252ccb510137>
16. <https://www.rfc-editor.org/rfc/rfc4120.txt>

17. <https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-kerberos>
18. <https://adsecurity.org/?p=227>
19. <https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names>
20. <https://learn.microsoft.com/en-us/windows-server/administration/server-manager/server-manager#start-server-manager>

ДОДАТКИ

## Додаток А – Детальна схема побудованої мережі (Логічна Топологія)



Додаток Б – Створення структури Active Directory та налагодження DHCP-серверу.

New Object - Organizational Unit ×

 Create in: cultofillusion.local/

---

Name:

☒ Protect container from accidental deletion

---

New Object - Organizational Unit

Create in: cultofillusion.local/CULTOFILLUSION

Name:  
Finance75

☒ Protect container from accidental deletion

OK Cancel Help

New Object - Organizational Unit

Create in: cultofillusion.local/CULTOFILLUSION

Name:  
IT80

☒ Protect container from accidental deletion

OK Cancel Help

New Object - Organizational Unit ✕

 Create in: cultofillusion.local/CULTOFILLUSION

---

Name:

☒ Protect container from accidental deletion

---

New Object - User ✕

 Create in: cultofillusion.local/CULTOFILLUSION/Finance75

---

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

---

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/Finance75

Password:

••••••••

Confirm password:

••••••••

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back

Next >

Cancel

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/Finance75

When you click Finish, the following object will be created:

Full name: Ann O. Rudenko

User logon name: ann7501@cultofillusion.local

The user must change the password at next logon.

< Back

Finish

Cancel

New Object - User ✕

 Create in: cultofillusion.local/CULTOFILLUSION/Finance75

---

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

New Object - User ✕

 Create in: cultofillusion.local/CULTOFILLUSION/Finance75

---

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/Finance75

When you click Finish, the following object will be created:

Full name: Petro L. Kramar  
User logon name: petro7501@cultofillusion.local  
The user must change the password at next logon.

&lt; Back

Finish

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

First name: Max Initials: M

Last name: Melnyk

Full name: Max M. Melnyk

User logon name:  
max801 @cultofillusion.localUser logon name (pre-Windows 2000):  
CULTOFILLUSION\ max801

&lt; Back

Next &gt;

Cancel

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

Password:

••••••••

Confirm password:

••••••••

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled

< Back

Next >

Cancel

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

When you click Finish, the following object will be created:

Full name: Max M. Melnyk

User logon name: max801@cultofillusion.local

The password never expires.

< Back

Finish

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

First name: Sophie Initials: M

Last name: Kovalenko

Full name: Sophie M. Kovalenko

User logon name: sophie802 @cultofillusion.local

User logon name (pre-Windows 2000): CULTOFILLUSION\ sophie802

&lt; Back

Next &gt;

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

Password: .....

Confirm password: .....

☒ User must change password at next logon☐ User cannot change password☐ Password never expires☐ Account is disabled

&lt; Back

Next &gt;

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

When you click Finish, the following object will be created:

Full name: Sophie M. Kovalenko

User logon name: sophie802@cultofillusion.local

The user must change the password at next logon.

< Back

Finish

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

First name:

Taras

Initials:

I

Last name:

Chumak

Full name:

Taras I. Chumak

User logon name:

taras803

@cultofillusion.local

User logon name (pre-Windows 2000):

CULTOFILLUSION\

taras803

< Back

Next >

Cancel

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

Password:

••••••••

Confirm password:

••••••••

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back

Next >

Cancel

New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/IT80

When you click Finish, the following object will be created:

Full name: Taras I. Chumak

User logon name: taras803@cultofillusion.local

The user must change the password at next logon.

< Back

Finish

Cancel

## New Object - User



Create in: ltofillusion.local/CULTOFILLUSION/Managment91

First name: Mykhailo Initials: O

Last name: Bondar

Full name: Mykhailo O. Bondar

User logon name: mykhailo91 @cultofillusion.local

User logon name (pre-Windows 2000): CULTOFILLUSION\ mykhailo91

&lt; Back

Next &gt;

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/Managment91

Password: .....

Confirm password: .....

☐ User must change password at next logon☐ User cannot change password☒ Password never expires☐ Account is disabled

&lt; Back

Next &gt;

Cancel

## New Object - User



Create in: cultofillusion.local/CULTOFILLUSION/Managment91

When you click Finish, the following object will be created:

Full name: Mykhailo O. Bondar  
User logon name: mykhailo91@cultofillusion.local  
The password never expires.

&lt; Back

Finish

Cancel

```
PS C:\Users\Administrator> get-aduser -filter * -SearchBase "OU=Finance75,OU=CULTOFILLUSION,DC=cultofillusion,DC=local"

DistinguishedName : CN=Ann O. Rudenko,OU=Finance75,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Ann
Name             : Ann O. Rudenko
ObjectClass      : user
ObjectGUID       : fc3d8ec0-cdc3-4193-8be1-53e2346f8a1b
SamAccountName   : ann7501
SID              : S-1-5-21-2438270518-4041768161-1684763614-1106
Surname          : Rudenko
UserPrincipalName : ann7501@cultofillusion.local

DistinguishedName : CN=Petro L. Kramar,OU=Finance75,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Petro
Name             : Petro L. Kramar
ObjectClass      : user
ObjectGUID       : b2073339-0289-4378-8b0d-b4e0ebb29955
SamAccountName   : petro7501
SID              : S-1-5-21-2438270518-4041768161-1684763614-1107
Surname          : Kramar
UserPrincipalName : petro7501@cultofillusion.local

PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> get-aduser -filter * -SearchBase "OU=IT80,OU=CULTOFILLUSION,DC=cultofillusion,DC=local"

DistinguishedName : CN=Max M. Melnyk,OU=IT80,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Max
Name             : Max M. Melnyk
ObjectClass      : user
ObjectGUID       : 24472b4a-2545-4a5e-b7e5-2e880103e7b7
SamAccountName   : max801
SID              : S-1-5-21-2438270518-4041768161-1684763614-1108
Surname          : Melnyk
UserPrincipalName : max801@cultofillusion.local

DistinguishedName : CN=Sophie M. Kovalenko,OU=IT80,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Sophie
Name             : Sophie M. Kovalenko
ObjectClass      : user
ObjectGUID       : 0d22eb1a-5874-497c-b144-c2c53f96f4e4
SamAccountName   : sophie802
SID              : S-1-5-21-2438270518-4041768161-1684763614-1109
Surname          : Kovalenko
UserPrincipalName : sophie802@cultofillusion.local

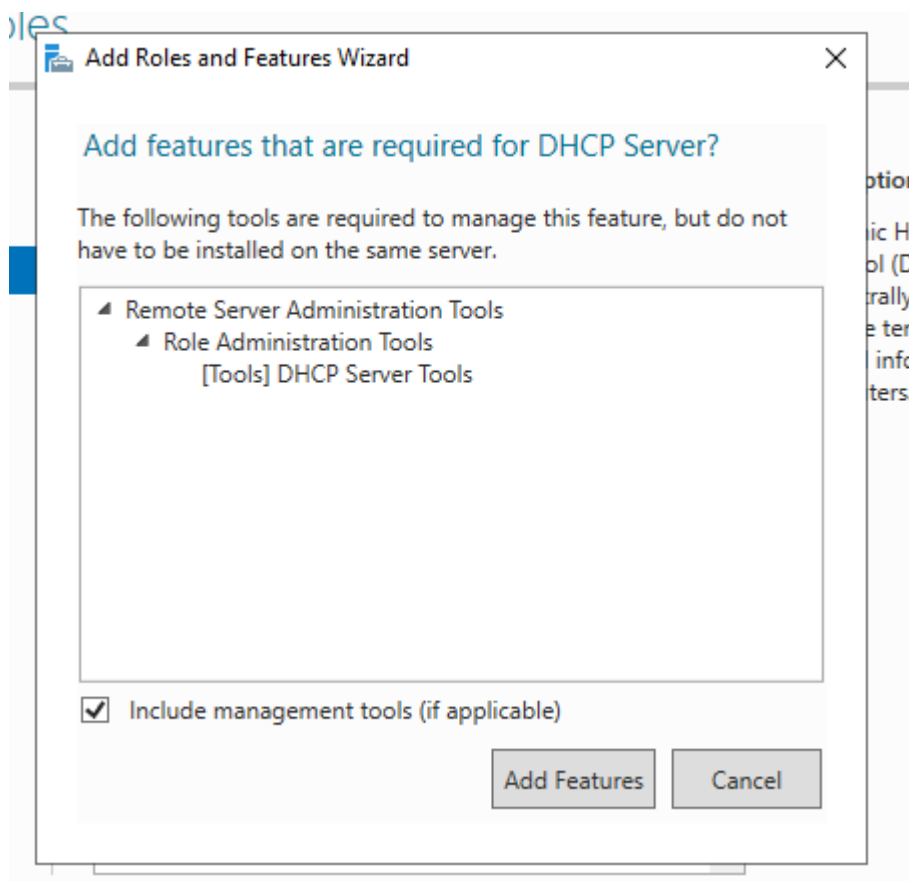
DistinguishedName : CN=Taras I. Chumak,OU=IT80,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Taras
Name             : Taras I. Chumak
ObjectClass      : user
ObjectGUID       : 2903326c-d1a7-4449-90a8-9b1a29bebcf3
SamAccountName   : taras803
SID              : S-1-5-21-2438270518-4041768161-1684763614-1110
Surname          : Chumak
UserPrincipalName : taras803@cultofillusion.local

PS C:\Users\Administrator> _
```

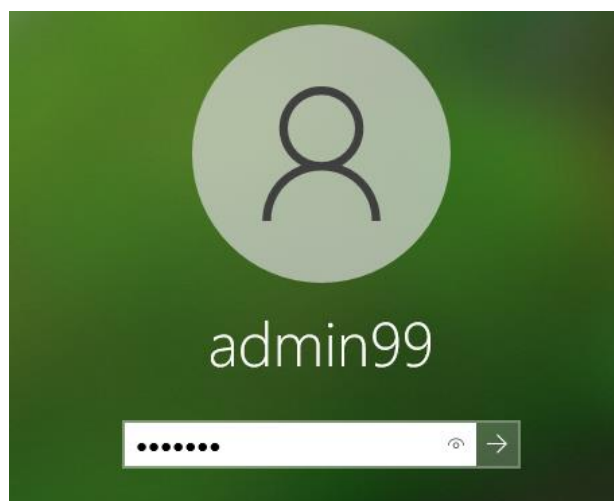
```
PS C:\Users\Administrator> get-aduser -filter * -SearchBase "OU=Managment91,OU=CULTOFILLUSION,DC=cultofillusion,DC=local"

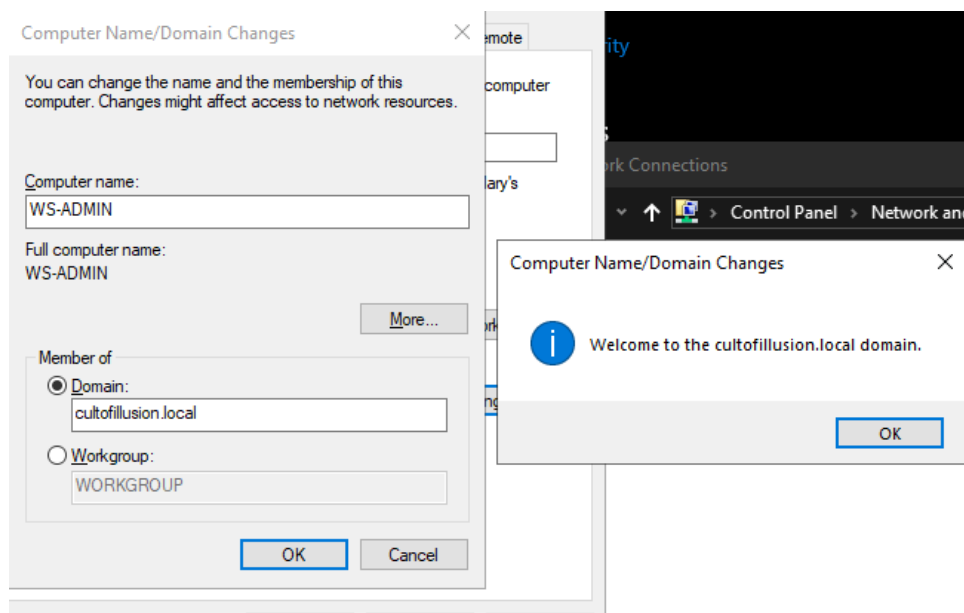
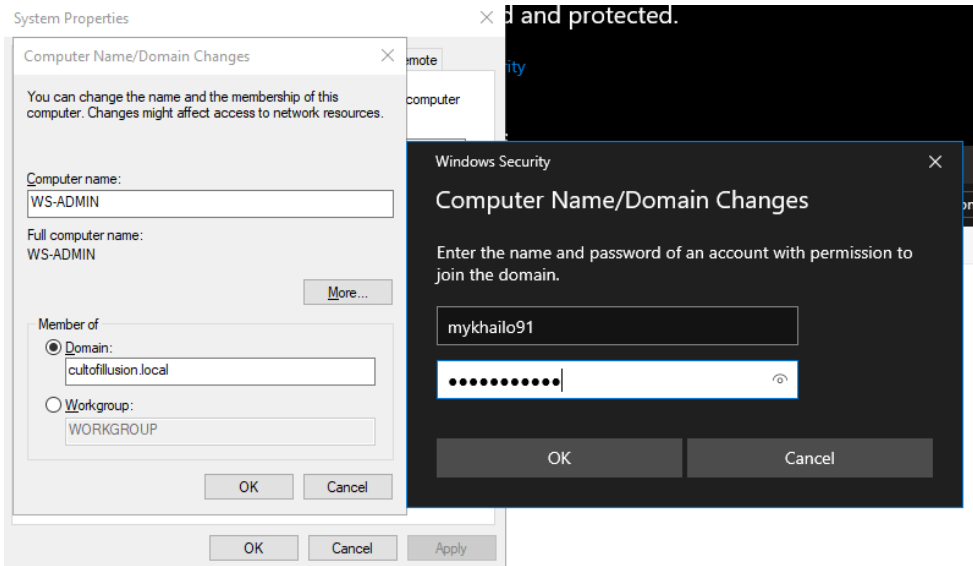
DistinguishedName : CN=Mykhailo O. Bondar,OU=Managment91,OU=CULTOFILLUSION,DC=cultofillusion,DC=local
Enabled           : True
GivenName        : Mykhailo
Name             : Mykhailo O. Bondar
ObjectClass      : user
ObjectGUID       : c7cd1f9c-9278-4ed0-a1f9-8505812bb9b9
SamAccountName   : mykhailo91
SID              : S-1-5-21-2438270518-4041768161-1684763614-1112
Surname          : Bondar
UserPrincipalName : mykhailo91@cultofillusion.local

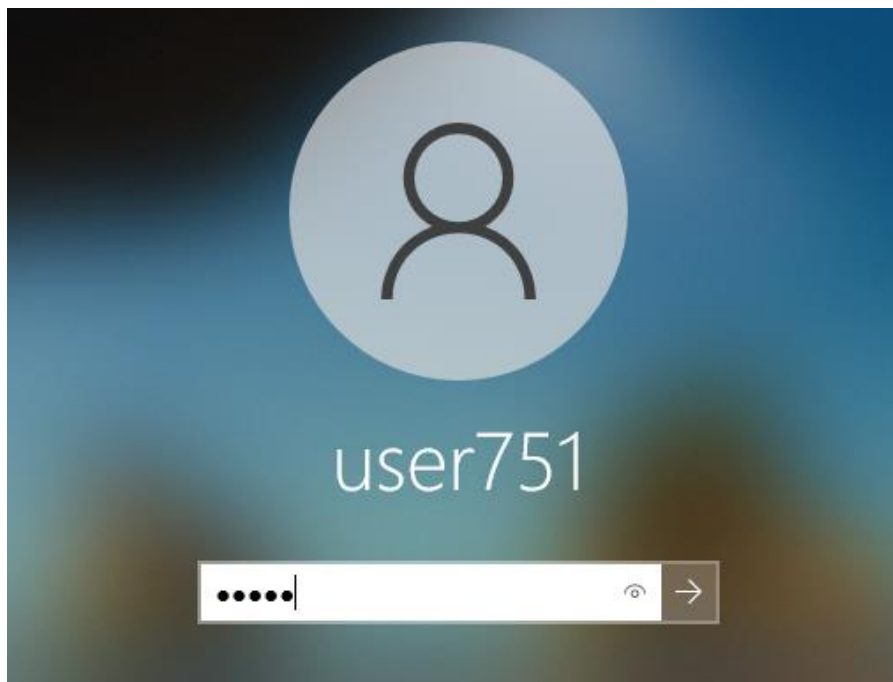
PS C:\Users\Administrator> _
```



```
PS C:\Users\Administrator> Import-Module -Name 'DHCPServer'
PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name 'Finance75' -StartRange '192.168.75.5' -EndRange '192.168.75.15' -SubnetMask '255.255.255.224' -Description 'vlan75'
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeId '192.168.75.0' -DnsServer '192.168.98.13' -DnsDomain 'cultofillusion.local' -Router '192.168.75.1'
PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name 'IT80' -StartRange '192.168.80.8' -EndRange '192.168.80.20' -SubnetMask '255.255.255.224' -Description 'vlan80'
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeId '192.168.80.0' -DnsServer '192.168.98.13' -DnsDomain 'cultofillusion.local' -Router '192.168.80.1'
PS C:\Users\Administrator>
```







Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 75 . 3

Subnet mask: 255 . 255 . 255 . 224

Default gateway: 192 . 168 . 75 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

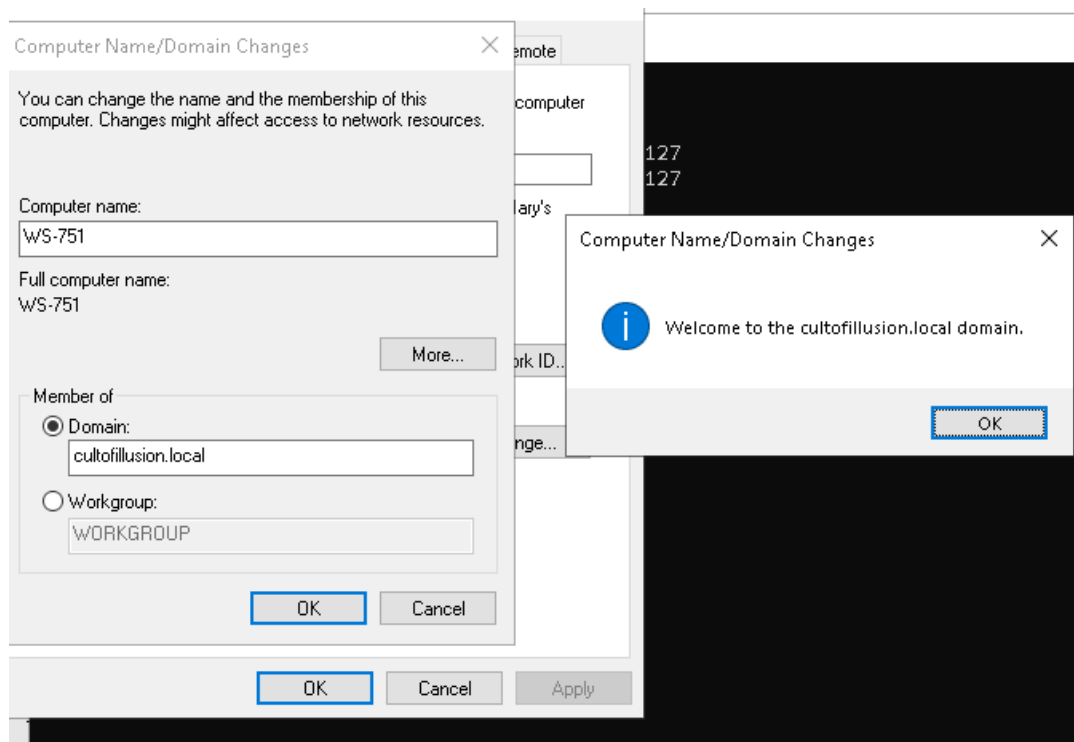
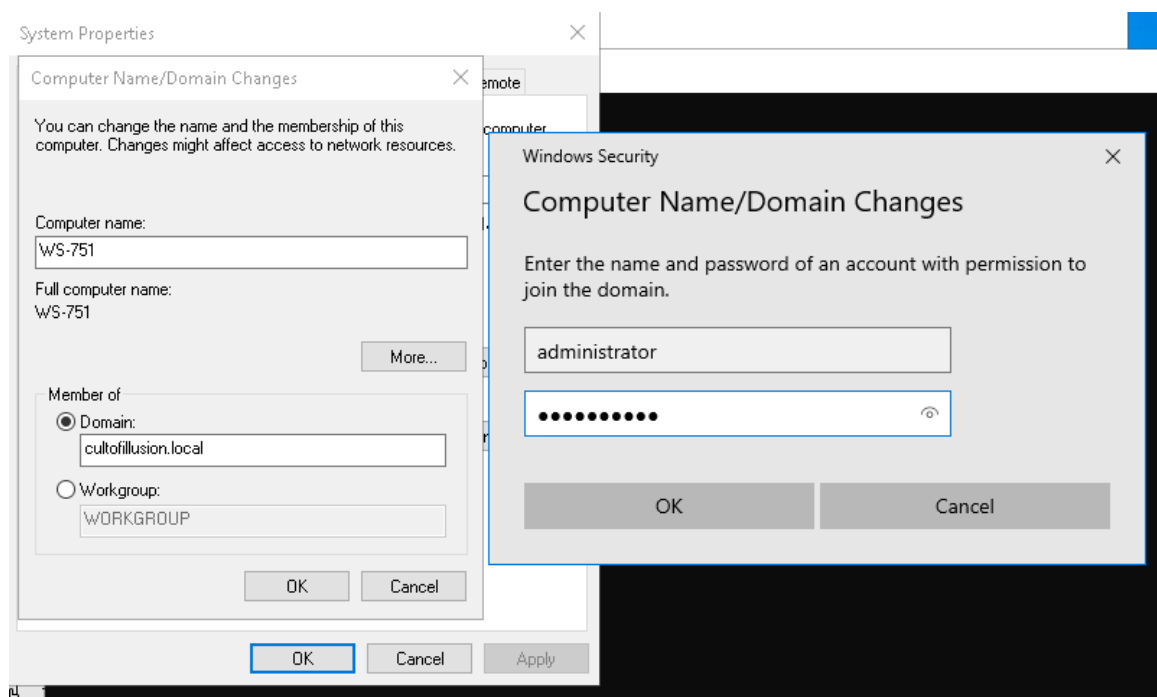
Preferred DNS server: 192 . 168 . 98 . 13

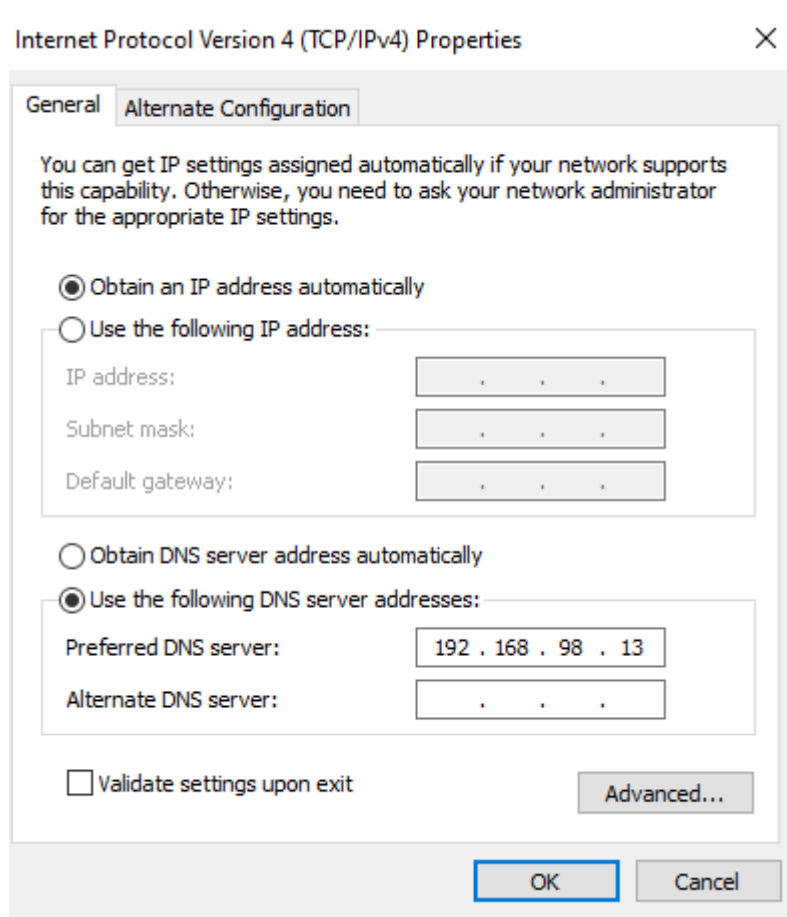
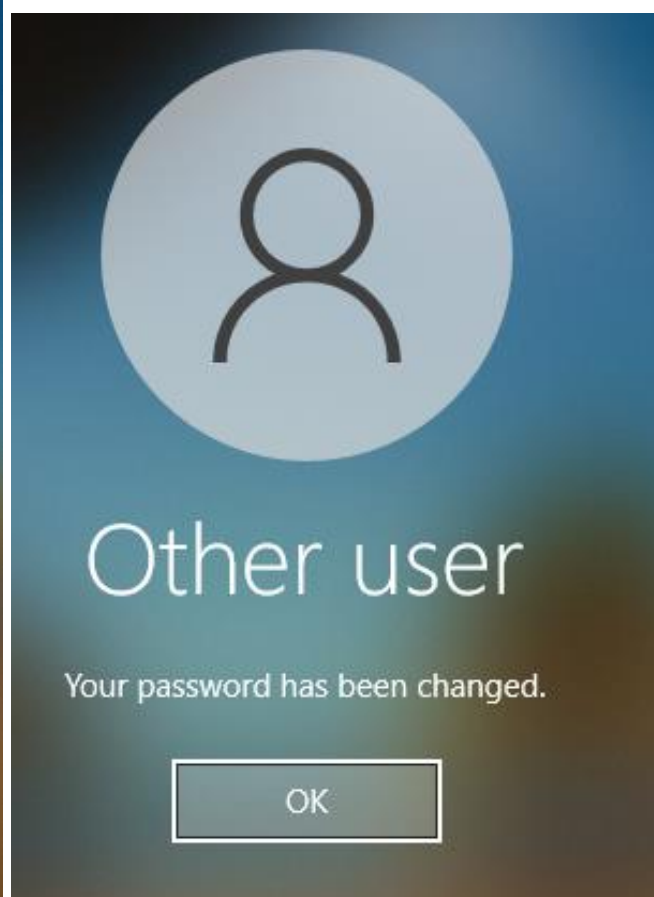
Alternate DNS server: . . .

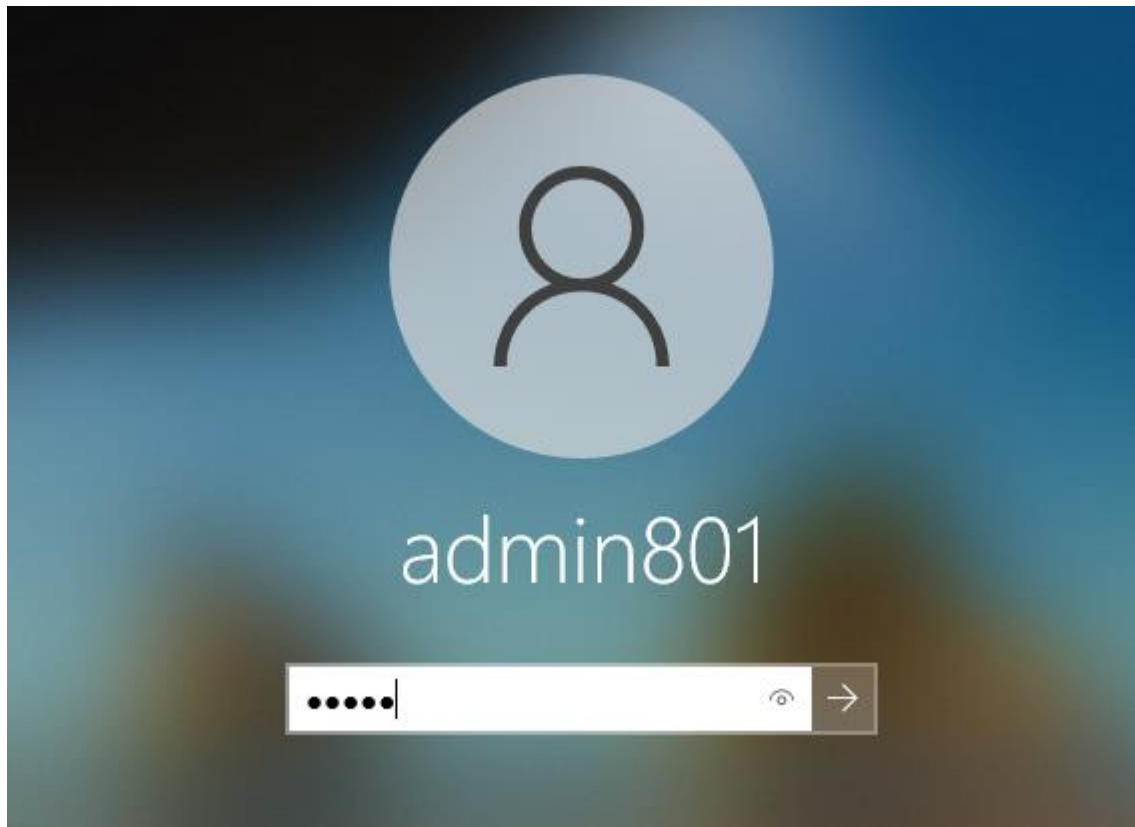
☐ Validate settings upon exit

Advanced...

OK Cancel







Internet Protocol Version 4 (TCP/IPv4) Properties ✕

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit Advanced...

OK Cancel

