

Home Lab: Simulated Corporate Network

*A Secure and Scalable Virtual Enterprise Environment for
Cybersecurity Training and Testing*

Writeup by Joseph Elbert

Email: Josephelb@comcast.net

LinkedIn: [LinkedIn Profile](#)

Table of Contents

Overview.....	
Executive Summary.....	3
Project Objectives	3
Network Architecture Overview	4
Operating Systems	5
Network Map	6
Enterprise Tools & Defense.....	9
Offense	9
Workstations	
Directory Service Server.....	10
Windows Server 2025	13
Linux Client.....	27
Email Security Server	33
Security Onion.....	35
Configuring SIEM	
Wazuh	37
Conclusion	
Closing Remarks	45
How I will use this lab.....	46

Executive Summary

This project involved the design and deployment of a simulated enterprise network using VMware, consisting of seven interconnected virtual machines that replicate a small-to-medium business environment. The lab includes essential enterprise services such as centralized authentication (Active Directory), internal email communication, endpoint clients, a security monitoring stack, and an attacker machine for red team exercises.

The goal of this home lab was to deepen practical knowledge in system administration, cybersecurity defense, offensive testing, and threat detection in a safe, isolated environment. It serves as both a training ground and a showcase of my hands-on cybersecurity skills.

Project Objectives

- Simulate a realistic enterprise IT infrastructure using virtual machines.
- Build a multi-platform environment with Windows and Linux systems.
- Implement core enterprise services: AD, DNS, DHCP, email server, and security monitoring.
- Practice both offensive (penetration testing) and defensive (network monitoring, incident detection) cybersecurity techniques.
- Develop a practical understanding of enterprise operations from both a blue and red team perspective.
- Implement redundancy by making snapshots of each machine after each main setup step in the project.

Network Architecture Overview

Network Setup:

- **NAT Network Name:** joe-corp
- **IP Range:** 10.0.0.0/24
- **DHCP Scope:** 10.0.0.100 – 10.0.0.200

Hosts:

Hostname	IP Address	Function
corp.joe-corp-dc.com	10.0.0.5	Domain Controller (DNS, DHCP, SSO)
email-svr	10.0.0.8	SMTP Relay Server
sec-box	10.0.0.10	Dedicated Security Server
sec-work	10.0.0.103	Security Playground
win-client	10.0.0.100	Windows Workstation
linux-client	10.0.0.101	Linux Desktop Workstation
attacker	dynamic	Attacker Environment

Operating Systems

Windows Server 2025: Designed to support enterprise-level applications, network management, and identity management. This will be used as the directory services server, acting as the central hub for network connections.

Windows 11 Enterprise: Desktop operating system optimized for everyday productivity. Most common operating system used in business environments for employees. This will be used to simulate a business user.

Ubuntu Desktop 22.04: General-purpose desktop. Commonly used for software development. This will be used to simulate an enterprise software development environment.

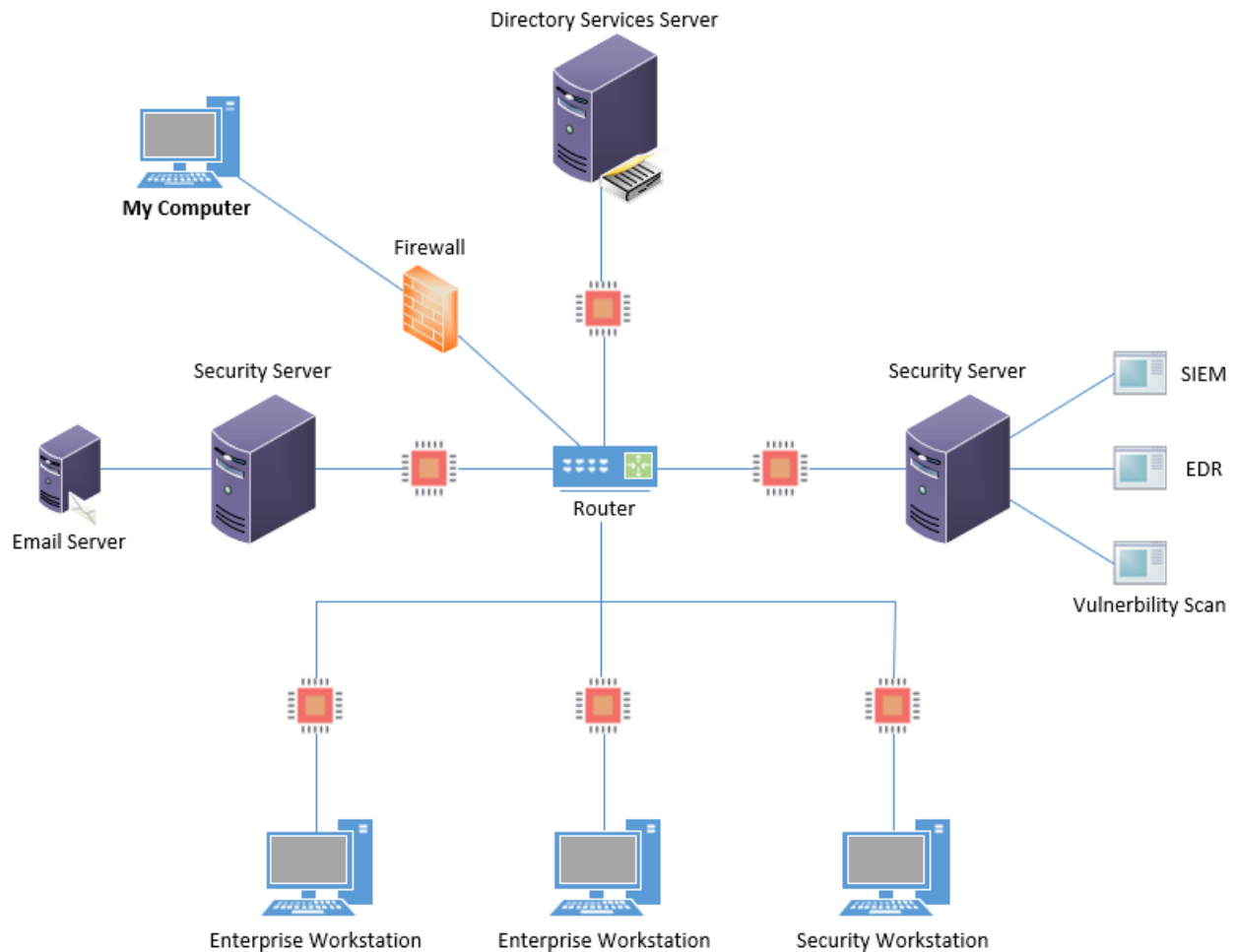
Security Onion: An open-source platform for security monitoring, log analysis, and intrusion detection, used by cybersecurity professionals to detect, investigate, and respond to network threats and incidents.

Ubuntu Server 2022: A Linux server operating system widely used for hosting applications, databases, and web services. This will be used as our email server.

Kali Linux: A Debian-based Linux distribution tailored for penetration testing and ethical hacking. It comes pre-installed with a wide range of tools for vulnerability assessment, exploitation, wireless testing, and digital forensics.

Network Map:

Here is my network map of the enterprise project that I simulated. The following diagram illustrates the overall design of the **Joe-Corp Enterprise Network**, representing the flow of data and segmentation of services within the home lab environment. This topology mirrors a real-world small-to-medium-sized business (SMB) setup and includes both production and security monitoring components.



Key Components:

- **Directory Services Server:**
Acts as the Domain Controller, providing centralized authentication via Active Directory. It manages user accounts, permissions, and Group Policy Objects (GPOs) for all Windows-based endpoints.
- **Firewall:**
Positioned between the simulated internal network and the administrative system ("My Computer"). This adds a basic segmentation layer, mimicking enterprise security perimeters.
- **Router/Switch:**
Central point of connectivity for all internal systems. While represented as a router, it functions as a logical switch in this lab to allow isolated traffic within the NAT network.

Endpoints:

- **Enterprise Workstations (Windows/Linux):**
Simulate standard user machines found in corporate environments. These were used to test authentication, email access, and vulnerability to attacks (e.g., RDP brute force).
- **Security Workstation:**
A machine running tools like Security Onion or Wazuh, used for manual analysis, log review, triage tasks, and a learning playground.

Email Server:

- Hosts Postfix to simulate internal business email flow. It supports phishing awareness exercises and protocol security configurations.

Security Infrastructure:

- **Security Servers (x2):**
 - One functions as a general-purpose server for installing defensive tools and collecting logs.
 - The second is dedicated to advanced monitoring services including:
 - **SIEM (Security Information and Event Management)**
 - **EDR (Endpoint Detection and Response)**
 - **Vulnerability Scanning** (e.g., Nessus, OpenVAS)

- These components support blue team operations, real-time threat detection, and incident response.

Administrative Host ("My Computer"):

- The host machine (my physical device) runs VMware and manages all of the lab VMs. It's segmented behind the firewall to mimic administrative access with restricted inbound connections.

Enterprise Tools & Defense

Microsoft Active Directory: A directory service used for managing and organizing network resources, users, and permissions in a Windows environment.

Wazuh: An open-source security monitoring platform that provides intrusion detection, log analysis, vulnerability detection, and compliance reporting.

Postfix: A popular open-source mail transfer agent (MTA) used for sending and receiving email on Unix-like operating systems.

Offense

Evil-WinRM: A powerful Ruby-based Windows Remote Management (WinRM) client used by penetration testers to connect to and interact with Windows systems, often for post-exploitation tasks such as command execution and data extraction.

Hydra: A fast and flexible password-cracking tool designed to perform brute-force and dictionary-based attacks on various network protocols, including SSH, HTTP, FTP, and more.

SecLists: A comprehensive collection of penetration testing resources, including wordlists for usernames, passwords, web directories, and other payloads used in reconnaissance and exploitation phases.

NetExec: A network exploitation tool that enables remote command execution on target machines through various protocols, assisting in lateral movement and privilege escalation scenarios.

XFreeRDP: An open-source implementation of the Remote Desktop Protocol (RDP), enabling penetration testers to connect to and control Windows systems remotely for reconnaissance and post-exploitation purposes.

Directory Service Server

Active Directory (AD) is a directory service developed by Microsoft that manages and organizes resources in a network. It acts as a centralized database to authenticate and authorize users and devices, making it the backbone of most Windows-based enterprise environments.

Key components:

- Authentication: Verifies user identity using credentials like username and password.
- Authorization: Grants or denies access to network resources based on permissions.
- Management: Centralizes control over users, computers, and other resources.

Why it's important:

Active Directory is widely used in enterprise environments to streamline and secure network management. It serves multiple purposes:

1. Centralized Resource Management AD enables administrators to manage users, devices, and permissions from a single location, reducing complexity.
2. Scalability It can handle environments ranging from small businesses to multinational corporations with millions of objects.
3. Authentication and Authorization AD provides a robust framework for verifying users and granting access to resources using security protocols like Kerberos and LDAP.
4. Group Policy Management Administrators can enforce security settings, deploy software, and manage updates across the network using Group Policy Objects (GPOs).
5. Integration with Other Services Active Directory integrates seamlessly with services like Microsoft Exchange, Azure AD, and other enterprise applications.

Active Directory Core Concepts:

1. Domains

- A domain is a logical grouping of objects (users, devices, etc.) that share the same database and security policies.
- Example: corp.local could be a domain for an organization. corp.joe-corp.com will be the domain used in this project.

2. Domain Controllers (DCs)

- Servers that host the Active Directory database and perform authentication, authorization, and replication.

3. Organizational Units (OUs)

- Containers within a domain used to organize objects logically.
- Example: Separate OUs for HR, IT, and Finance.

4. Objects

- Every entity in AD, such as users, computers, printers, and groups, is an object.

5. Groups

- Security Groups: Used for managing permissions to resources.
- Distribution Groups: Used for email distribution.

6. Forest and Trees

- A forest is the highest-level container, encompassing multiple domains that share a common schema.
- A tree is a hierarchy of domains within a forest.

7. Global Catalog (GC)

- A distributed data repository that provides information about all objects in the forest for faster lookups.

8. Trust Relationships

- Trusts enable users in one domain to access resources in another domain.

Security Implications:

Active Directory is often a prime target for attackers due to its central role in managing network resources. Misconfigurations or vulnerabilities can lead to significant security risks.

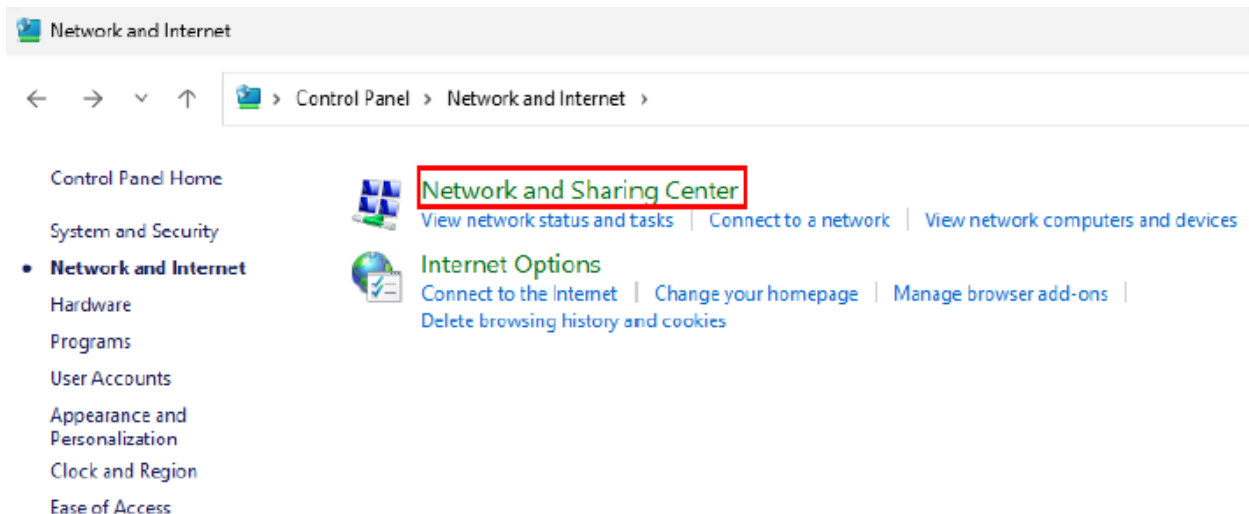
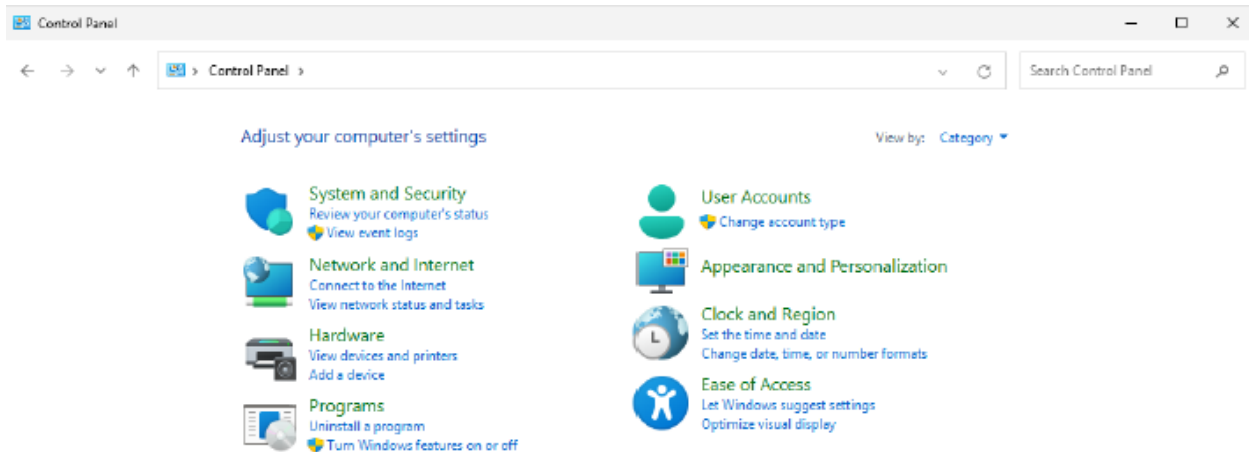
1. Common Security Threats

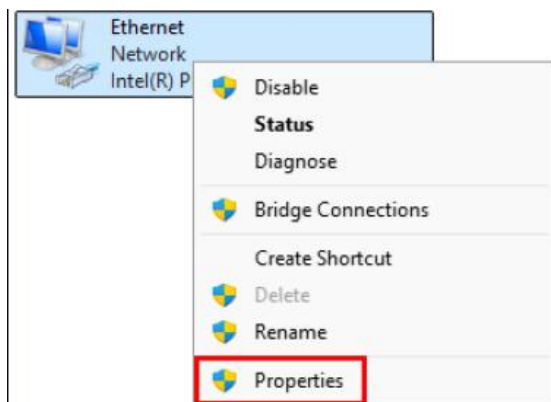
- **Credential Theft:** Techniques like Pass-the-Hash or Kerberoasting can allow attackers to escalate privileges.
- **Privilege Escalation:** Exploiting misconfigured permissions to gain higher access levels.
- **Lateral Movement:** Once inside, attackers can move through the network using AD to identify valuable targets.

Many organizations are transitioning to hybrid environments using Microsoft Entra ID (formerly Azure Active Directory), which combines on-premises and cloud-based identity management. I will be using on-premises infrastructure so I can fully control the setup, configuration, and isolation of the lab.

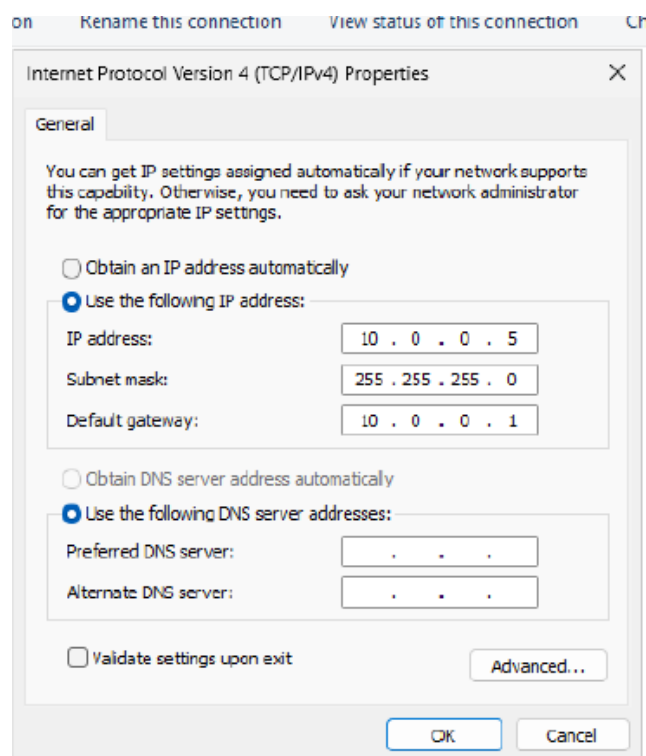
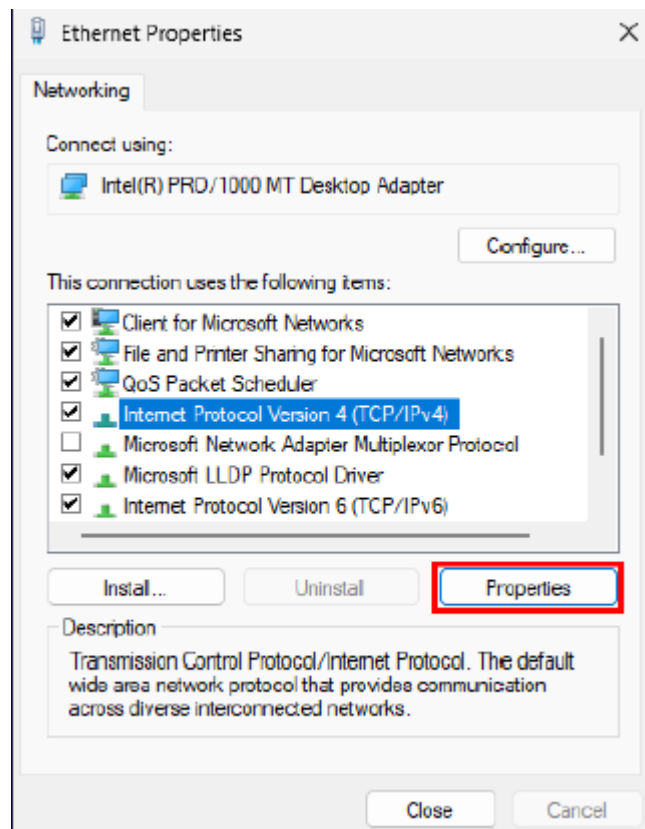
Windows Server 2025

First, I setup the VM on my VMware workstation and configured it to connect to the NAT network I setup for this project. Once the VM was setup, it was now time to assign a static IP address. Inside control panel I went to Network and Internet. Then Network and Sharing Center and change adapter settings.



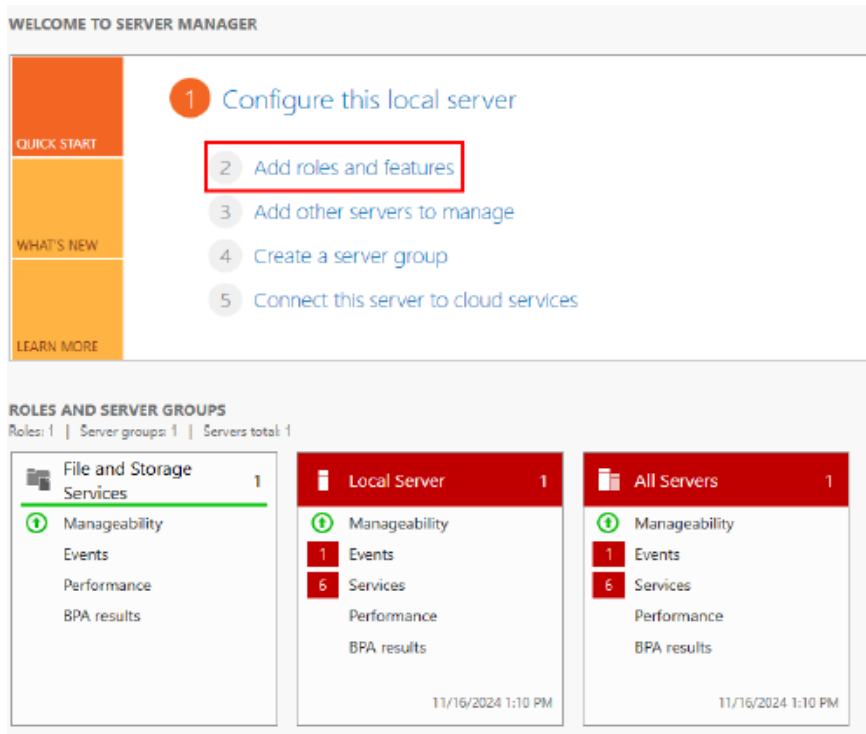


I went into adapter properties, then into the IPv4 properties. There, I could set a static IP address, subnet mask, and gateway for the user to stay connected to the network.

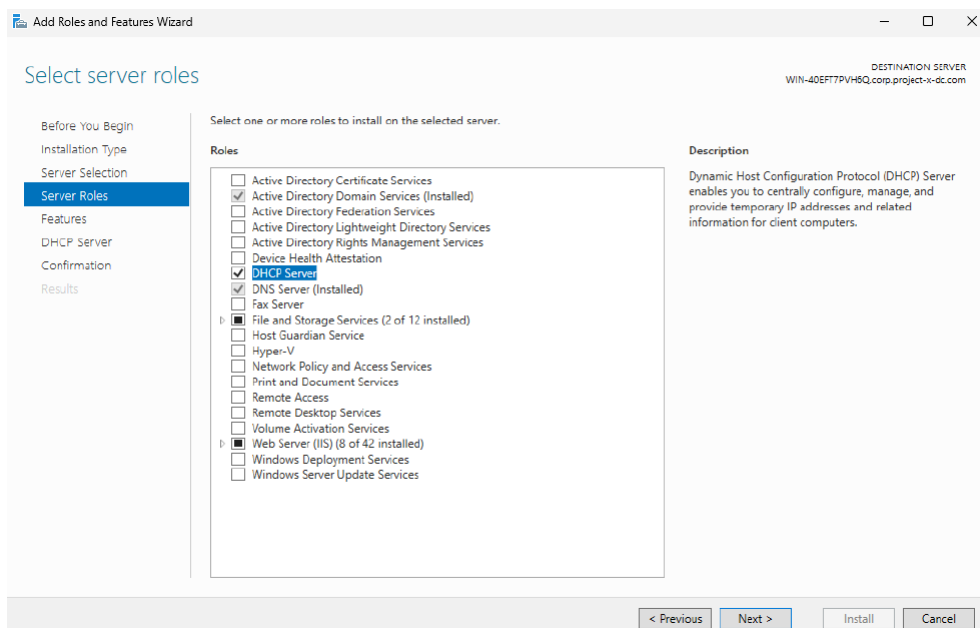


Promote Active Directory to Domain Controller:

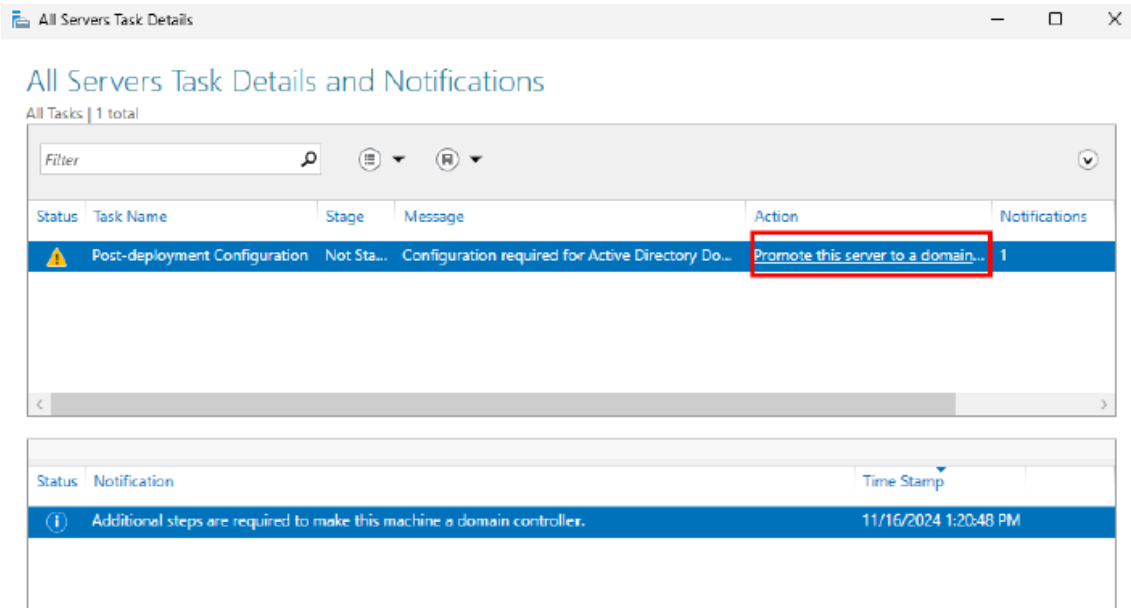
Once I opened the server manager, I was able to begin to assign the Windows Server 2025 VM to the Domain Controller of the network. First thing to do was to go to the Add roles and features tab.



I added server roles like DHCP server, DNS server, and left the others default for now.



Once that was complete, I went to the side menu AD DS in order to promote the server to a domain controller.



I made sure to add a new forest and I made the root domain name “corp.joe-corp.com”. The next thing to do was setup a secure password for Directory Services Restore Mode (DSRM). The NetBIOS domain needed a name so I called it “CORP”. Once these settings were configured, I had to run some prerequisite checks in order to make sure the DHCP and DNS servers were setup correctly.

Next, I rebooted the system and signed into the CORP\Administrator account. In PowerShell, I had to verify that the server was now apart of the domain I just created.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

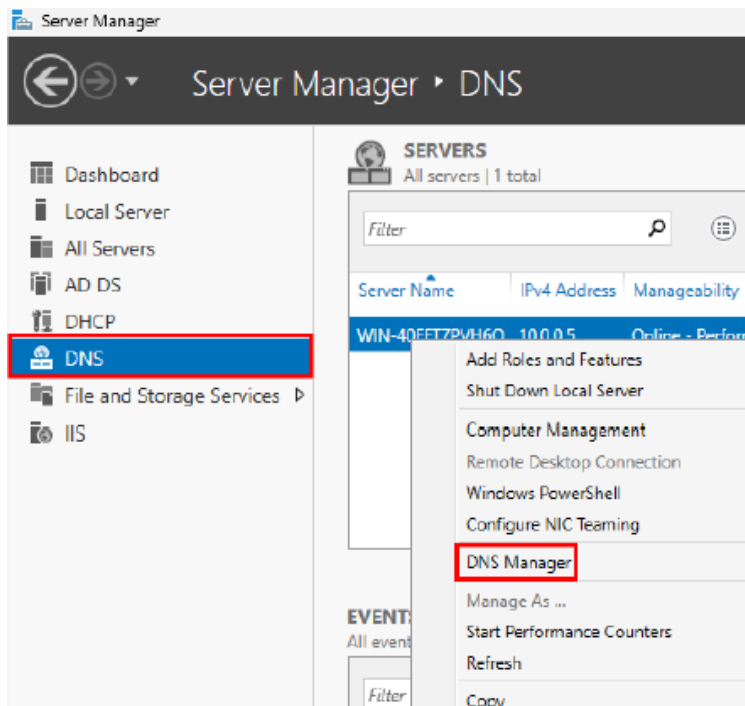
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-ADDomainController

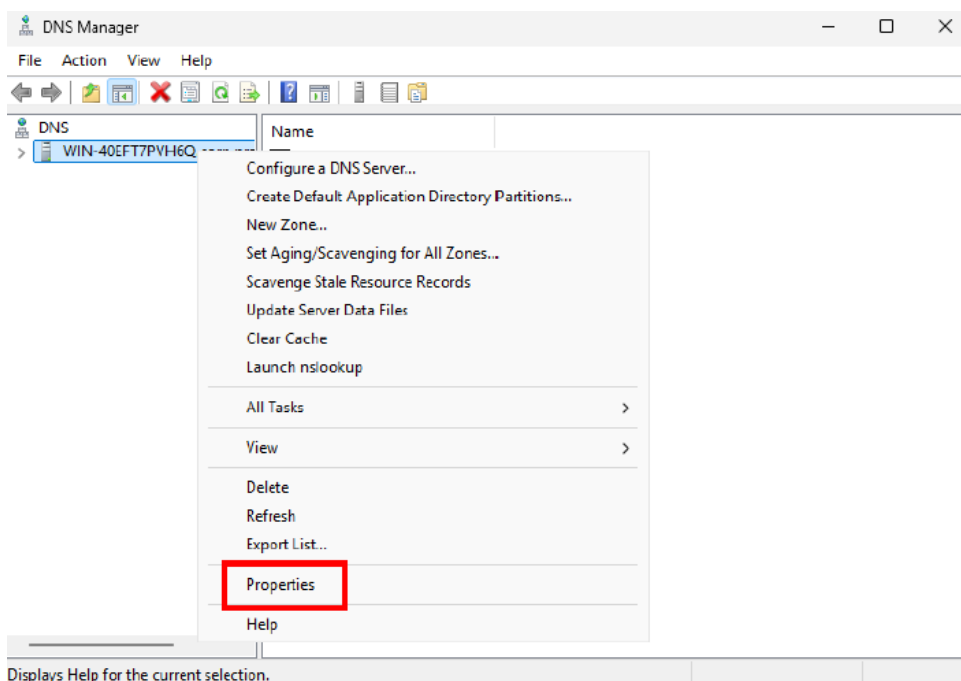
ComputerObjectDN      : CN=WIN-R60M18HH0GL,OU=Domain Controllers,DC=corp,DC=joe-inc,DC=com
DefaultPartition      : DC=corp,DC=joe-inc,DC=com
Domain                : corp.joe-inc.com
Enabled               : True
Forest                : corp.joe-inc.com
HostName              : WIN-R60M18HH0GL.corp.joe-inc.com
InvocationId          : a3d39816-8a76-404a-851e-633f5d072215
IPv4Address           : 10.0.0.5
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : WIN-R60M18HH0GL
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=WIN-R60M18HH0GL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=joe-inc,DC=com
OperatingSystem        : Windows Server 2025 Datacenter Evaluation
OperatingSystemHotfix :
OperatingSystemServicePack :
OperatingSystemVersion : 10.0 (26100)
OperationMasterRoles   : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions             : {DC=DomainDnsZones,DC=corp,DC=joe-inc,DC=com, DC=ForestDnsZones,DC=corp,DC=joe-inc,DC=com, CN=Schema,CN=Configuration,DC=corp,DC=joe-inc,DC=com, CN=Configuration,DC=corp,DC=joe-inc,DC=com...}
ServerObjectDN        : CN=WIN-R60M18HH0GL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=joe-inc,DC=com
ServerObjectGuid       : 41e594b5-afb8-4668-b86b-3a223ce8a128
Site                  : Default-First-Site-Name
SslPort               : 636
```

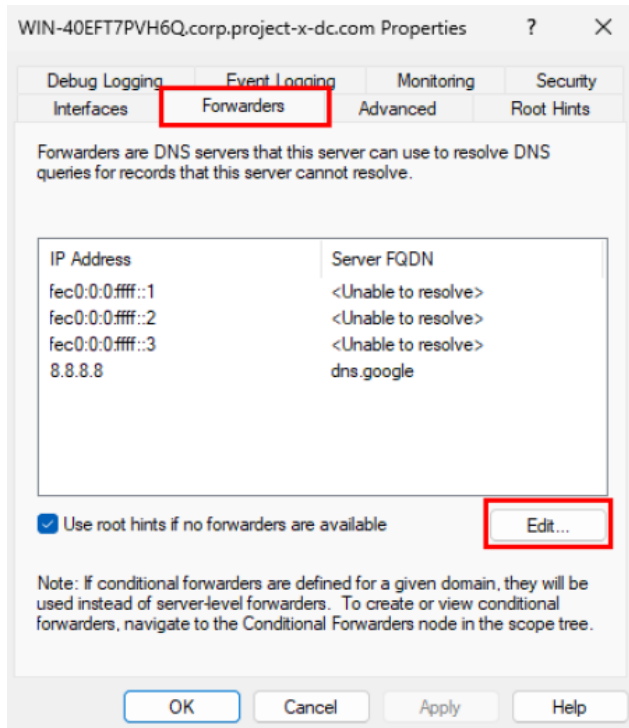

DNS for Internet Access:

Next, it is time to assign a DNS so the server can connect to the internet. I had to go back into server manager and go to the side menu called “DNS”. Then I went into the DNS Manager to start this process.

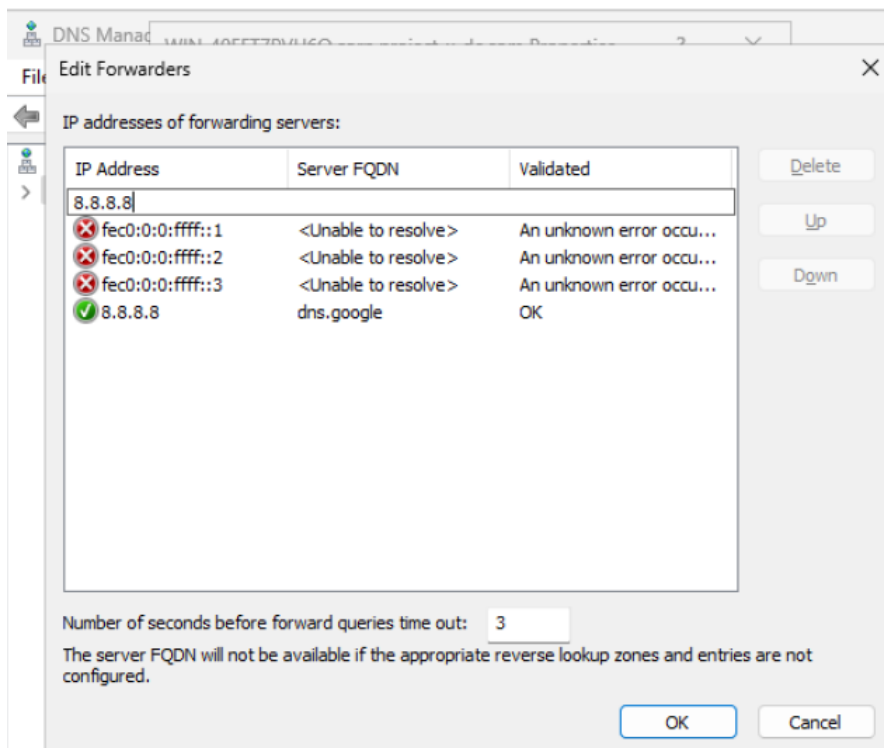


Once in the DNS manager, I chose the properties tab in order to choose the forwarding address that the workstation will connect to in order to get forwarded to the real internet.





I tested google.com's DNS server first in order to test the connection to the internet. I ran a ping after to test if ICMP packets could reach Google's DNS server. I also performed an nslookup to find the network's domain.



```
Administrator: Windows Powe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ping google.com

Pinging google.com [74.125.136.100] with 32 bytes of data:
Reply from 74.125.136.100: bytes=32 time=20ms TTL=128
Reply from 74.125.136.100: bytes=32 time=21ms TTL=128
Reply from 74.125.136.100: bytes=32 time=18ms TTL=128
Reply from 74.125.136.100: bytes=32 time=22ms TTL=128

Ping statistics for 74.125.136.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 22ms, Average = 20ms
PS C:\Users\Administrator>
```

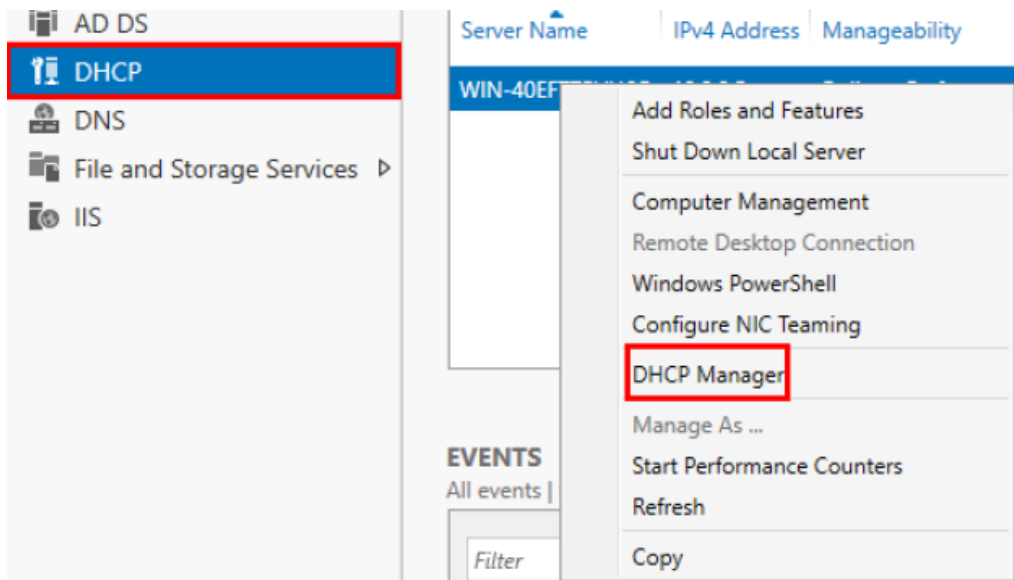
```
Administrator: Windows Powe
PS C:\Users\Administrator> nslookup corp.joe-corp.com
Server:      UnKnown
Address:     ::1

Non-authoritative answer:
Name:   77980.bodis.com
Address: 199.59.243.228
Aliases: corp.joe-corp.com

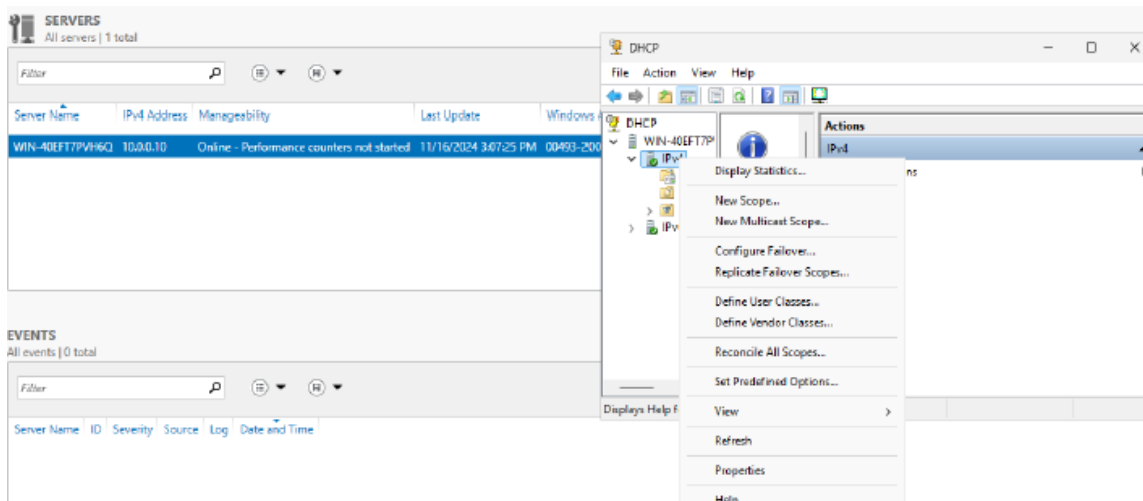
PS C:\Users\Administrator>
```

Setup DHCP:

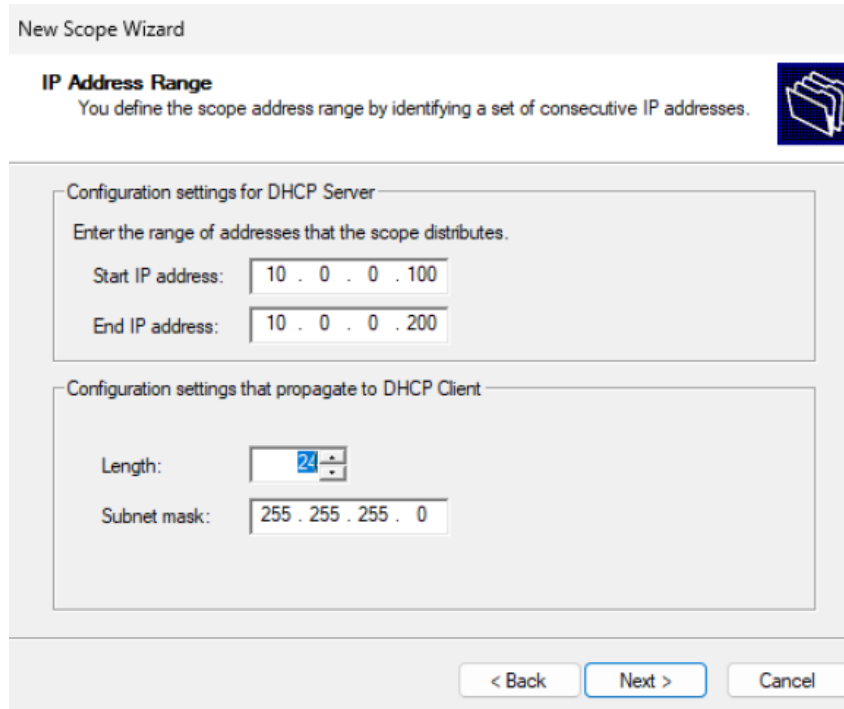
Now it's time to setup the DHCP settings. I began this process by going to the DHCP tab in the server manager. Then, I went to the DHCP manager setting.



The first thing that I entered was the CORP\Administrator username to set the server's administrator username. Once I was in the DHCP manager, it was time to add a new IPv4 scope.



The new DHCP scope include the address range of **10.0.0.100** to **10.0.0.200**. The subnet mask for this network is **255.255.255.0** because the CIDR notation of /24 on the IP address range for this network. The default gateway for this project is **10.0.0.2**. All of the workstations will go through this address before they hit the actual internet (my personal device).

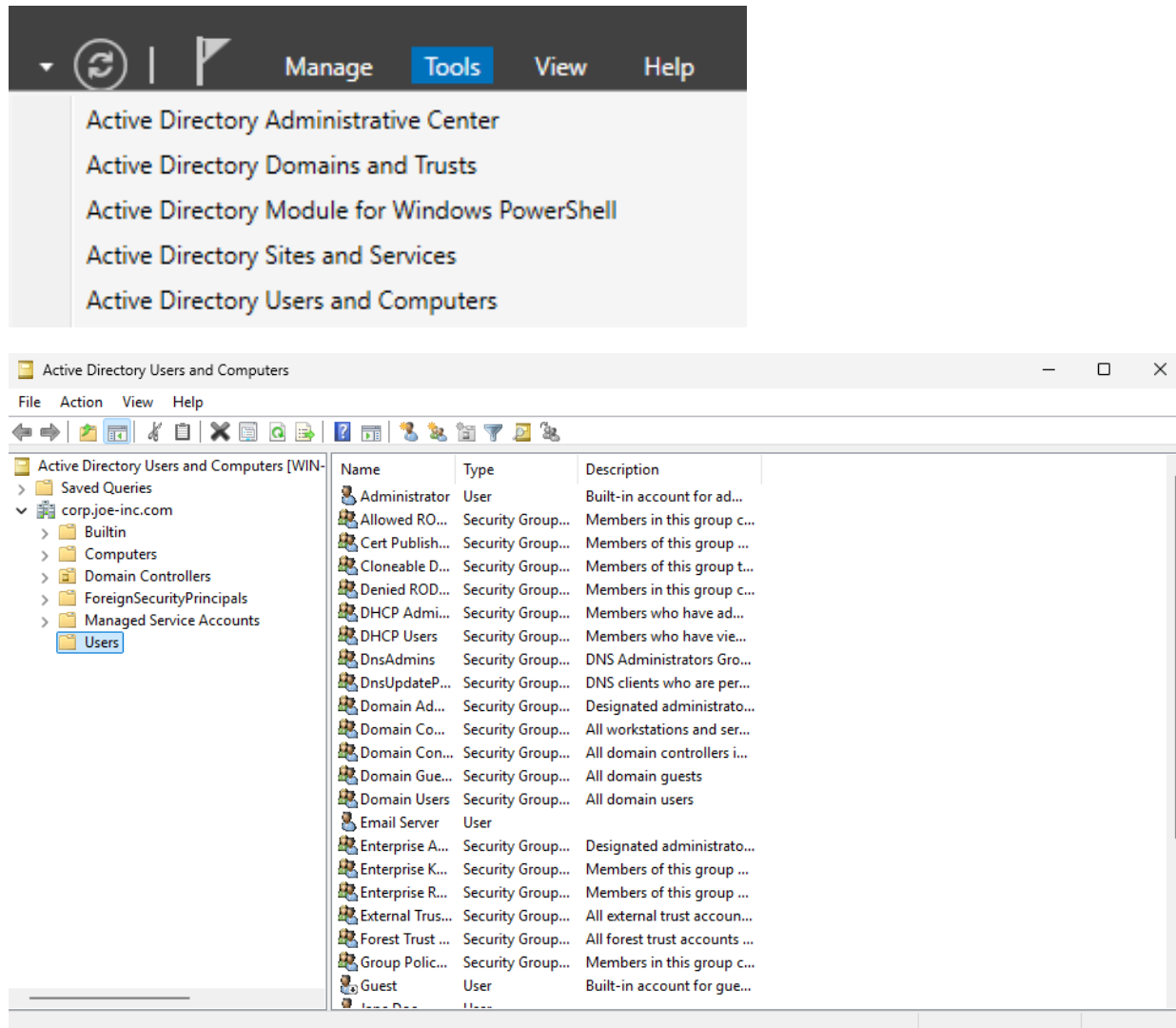


The screenshot shows the 'New Scope Wizard' window. The title bar says 'New Scope Wizard'. Below the title bar, the section is 'IP Address Range' with a sub-instruction: 'You define the scope address range by identifying a set of consecutive IP addresses.' To the right of this text is a blue icon of a folder with a document. The main area is divided into two sections. The first section is 'Configuration settings for DHCP Server' with the instruction 'Enter the range of addresses that the scope distributes.' It contains two input fields: 'Start IP address:' with the value '10 . 0 . 0 . 100' and 'End IP address:' with the value '10 . 0 . 0 . 200'. The second section is 'Configuration settings that propagate to DHCP Client' and contains two input fields: 'Length:' with a dropdown menu showing '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

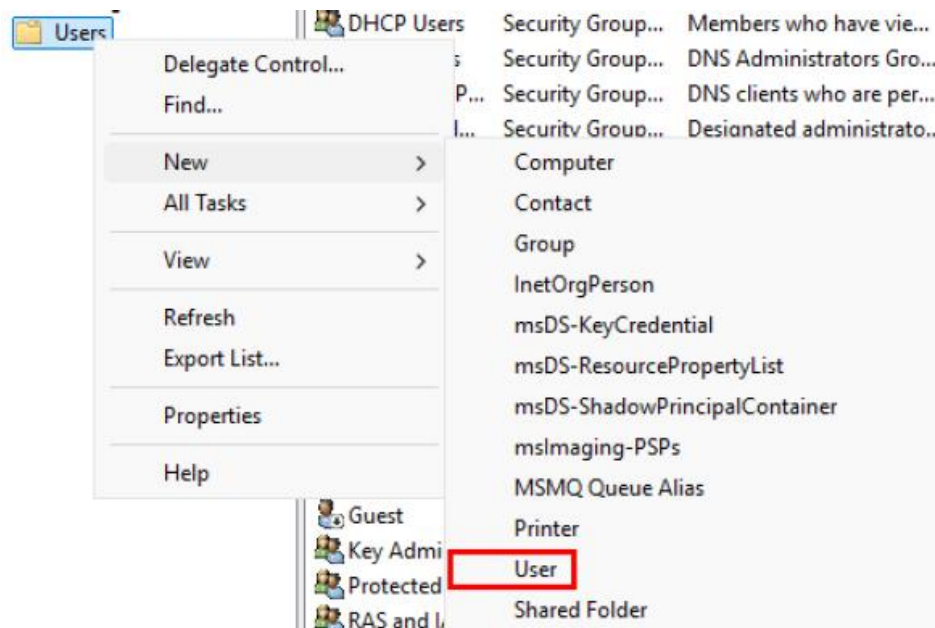
The parent domain for this network is set to corp.joe-corp.com. All of the workstations on this network will be apart of this domain.

Adding User Accounts in Active Directory:

First, I went into server manager and went to the “Tools” tab at the top. Once the drop down appears I clicked on the Active Directory Users and Computers. Here, I was able to manage all of the user’s that are apart of this domain.



I then had to right-click on the “Users” folder in order to add a new user. Later on I will be using this to add a new Group to the domain as well. The first user I will be adding is a workstation user named John Doe.



 A screenshot of the 'New Object - User' dialog box. The 'Create in' field is set to 'corp.joe-inc.com/Users'. The 'First name' field is 'John', 'Last name' is 'Doe', and 'Full name' is 'John Doe'. The 'User logon name' field is 'johnd@corp.joe-inc.com'. The 'User logon name (pre-Windows 2000)' field is 'CORP\johnd'. The 'Next >' button is highlighted.

In the real world, I would not set it where the user cannot change the password. This is a security issue because once the user's password is compromised by an outside entity, they will not be able to change their password. An attacker could continuously access the account because they have the permanent password set by this rule in Active Directory. In the real world, I would just leave it where the user must change the password at next logon.

New Object - User

Create in: corp.joe-inc.com/Users

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

I repeated this step for a second user named Jane Doe as well.

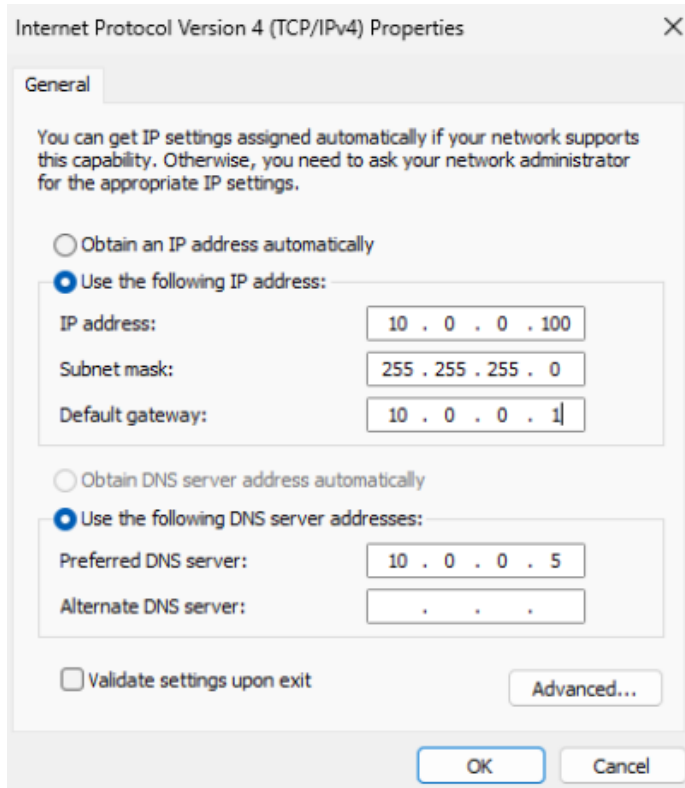
Name	Type	Description
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
External Trus...	Security Group...	All external trust accoun...
Forest Trust ...	Security Group...	All forest trust accounts ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for que...
Jane Doe	User	
John Doe	User	
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

Now, both of our users are setup in Active Directory on the Domain Controller. A system snapshot was then taken after this step was completed.

Windows 11 Enterprise

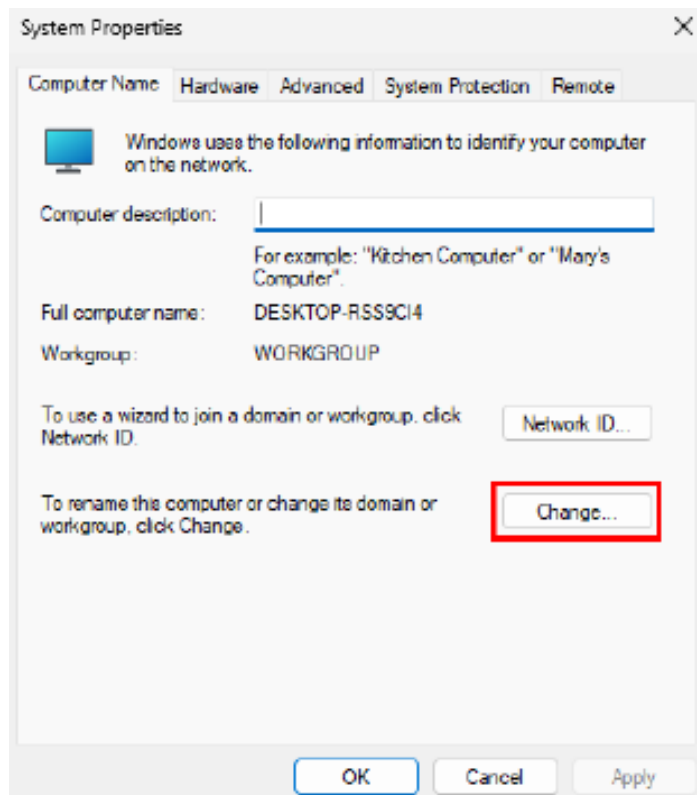
I began by setting up both of the machines in VMware. I configured the network to be on the NAT network so they could be on the same local network as the Domain Controller.

For the windows 11 workstation, I configured the static IPv4 address the same way I did for the Domain Controller. The IP address instead is now 10.0.0.100 which is the first address in the scope of the DHCP server I set up earlier.



Next, it was time to go to “Change workgroup name” in control panel in order to add the Windows 11 Enterprise workstation to the “corp.joe-corp.com” domain.

At the “Change” menu, I made sure Domain was selected and I typed in the domain name on this network.



After this, I was then prompted to enter a username and password for this new user to be added to this domain.

Username entered was "johnd@corp.joe-corp.com".

The computer gave me a prompt saying it was added to the corp.joe-corp.com domain. Then, I rebooted the computer for the changes to save. I then took a snapshot of the system.

Linux Client

What is Linux & Ubuntu?

Linux: Linux is an open-source operating system kernel that serves as the foundation for various distributions (distros) like Ubuntu, Debian, Fedora, and CentOS. It is known for its flexibility, stability, and security, making it a popular choice for servers, desktops, and embedded systems.

Ubuntu: Ubuntu is a Linux distribution based on Debian, developed and maintained by Canonical. It is designed to be user-friendly, making it a go-to choice for beginners while remaining robust enough for advanced users and enterprise environments. Ubuntu is available in various editions: Desktop, Server, and Core (for IoT).

Key Features:

- **Open-Source:** Free to use, modify, and distribute.
- **Wide Compatibility:** Supports a variety of hardware and software.
- **Active Community:** Backed by a vast community and regular updates.

How is Linux used?

Linux, and specifically Ubuntu, is utilized across various fields for diverse purposes:

1. Servers and Hosting

- **Web Servers:** Ubuntu is a leading choice for hosting websites, applications, and databases using services like Apache, Nginx, and MySQL.
- **Cloud Computing:** Powers major cloud platforms like AWS, Google Cloud, and Azure.

2. Development and Testing

- Popular among developers for its built-in tools, package management (APT), and scripting capabilities.
- Ideal for DevOps workflows with support for Docker, Kubernetes, and CI/CD pipelines.

Security Implications:

While Linux and Ubuntu are inherently more secure than many other operating systems, they are not immune to threats. Understanding their security implications is crucial for safe and effective usage.

Common Threats:

1. **Privilege Escalation**
 - Misconfigured sudo or excessive permissions can allow attackers to gain root access.
2. **Unpatched Vulnerabilities**
 - Delays in applying updates can leave systems exposed to exploits like kernel vulnerabilities.
3. **Weak SSH Configurations**
 - Using default settings or weak passwords can lead to brute-force attacks.
4. **Malware and Rootkits**
 - Though less common, Linux-specific malware and rootkits exist and can compromise systems.
5. **Supply Chain Attacks**
 - Threats can arise from malicious packages or software downloaded from untrusted sources.

Connect Ubuntu Desktop to Active Directory

Since Ubuntu (and Linux-native operating systems) are not native to the Microsoft ecosystem. Connecting Ubuntu (and Debian-based systems) to Active Directory can be accomplished in a couple ways. The easiest way is to connect Ubuntu to Active Directory with realmd and SSSD (System Security Services Daemon). Samba Winbind can also be used to join Linux systems if realmd / SSSD is not working.

!!! Currently realmd and SSSD integration do not work for Windows Server 2025 and Debian/Ubuntu-based systems.

About SSSD / Realmd

- **System Security Services Daemon (SSSD):** A service on Linux systems that provides a central access point for identity management and authentication. When connecting a Linux system to Active Directory (AD), SSSD allows for the integration by acting as an intermediary between the Linux system and AD needing to know what files should be edited.
- **realmd:** A tool that simplifies the process of joining Linux machines to AD domains. It automates the discovery, configuration, and enrollment of Linux systems in Active Directory, making it easier to integrate Linux systems into existing AD environments.

Realmd is especially useful for administrators because it manages the complexities of setting up Kerberos, configuring LDAP settings, and ensuring proper authentication protocols.

- realmd is a tool that automates domain joining and manages configurations for sssd, which provides caching, more flexible configuration options, and better performance.

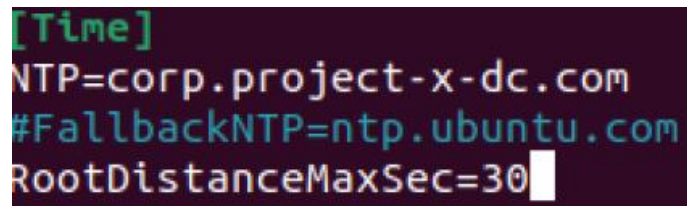
About Samba Winbind

- Samba Winbind: A component of the Samba suite that allows Linux systems to authenticate users against Windows Active Directory (AD) and integrate with Windows network environments. Is a more direct integration, especially useful for legacy systems and environments where tight compatibility with Windows protocols is necessary. It's often preferred when working in older Windows Server environments or where native Samba compatibility is crucial.

Realmd + SSSD:

I will be using Winbind to connect the Linux client to the Windows Active Directory. I had to edit the timesyncd.conf file by adding Network Time Protocol and RootDistance to make sure the time was synced with the Domain Controller. I installed the necessary packages for Realmd and SSSD.

sudo nano /etc/systemd/timesyncd.conf



```
[Time]
NTP=corp.project-x-dc.com
#FallbackNTP=ntp.ubuntu.com
RootDistanceMaxSec=30
```

Next command downloads the packages and a screen that asks for Kerberos Authentication configurations where I entered the domain name in all caps "CORP.JOE-CORP.COM".

sudo apt install realmd sssd sssd-tools samba common krb5-user packagekit libnss-sss libpam-sss adcli samb-common-bin

Then, I searched for the domain with the realm command and joined the Administrator.

```
sudo realm join --verbose --user=Administrator corp.joe-corp.com
```

Samba Winbind:

It is now time to install the necessary packages for winbind. After, the configurations with Kerberos Authentications required me to enter the domain name again but in all caps "CORP.JOE-CORP.COM".

```
sudo apt -y install winbind libpam-winbind libnss-winbind krb5-config samba-dsdb-modules  
samba-vfs-modules
```

Next I moved the smb.conf file in order to make some edits.

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.org
```

Now, I am going to edit the Server Message Block (SMB) config file.

```
sudo nano /etc/samba/smb.conf
```

I added realm and workgroup to the file with these parameters:

```
[global]
```

```
kerberos method = secrets and keytab
```

```
realm = CORP.JOE-CORP.COM
```

```
workgroup = CORP
```

```
security = ads
```

```
template shell = /bin/bash
```

```
winbind enum groups = Yes
```

```
winbind enum users = Yes
```

```
winbind separator = +
```

```
idmap config * : rangesize = 1000000
```

```
idmap config * : range = 1000000-19999999
```

```
idmap config * : backend = autorid
```

I confirmed the passwd and group had winbind set on their values.

```
sudo nano /etc/nsswitch.conf
```

```
passwd:      files systemd sss winbind
group:       files systemd sss winbind
shadow:      files sss
gshadow:     files
```

On Ubuntu, every user that has an interactive logon to the system needs a home directory. For domain users, I need to set this up before a user is able to successfully logon and start working. This allowed me to “Create home directory on login”.

```
sudo pam-auth-update
```

I need to change the DNS settings in order for the Linux client to refer to the Domain Controller’s IP address.

```
sudo nano /etc/resolv.conf
```

```
nameserver 10.0.0.5
nameserver 127.0.0.53
options edns0 trust-ad
search .
```

I joined the domain with Administrator.

```
sudo net ads join -U Administrator
```

I had to restart winbind. It is always a good idea to restart services after you change their configuration files.

```
systemctl restart winbind
```

Next, I ran “**net ads info**” to get Active Directory services information listing, and “**wbinfo -u**” to list all of the available users.

```
jane@linux-client:~$ wbinfo -u
CORP+administrator
CORP+guest
CORP+krbtgt
CORP+johnd
```

If you are following along with this walkthrough, you might need to add Jane Doe as a user in Active Directory like I did earlier. After you add her, you must restart winbind with “**sudo systemctl restart winbind**”. Then search with “wbinfo -u” to list all of the available users again. I already have her added in there, so I just have to connect her now. Now I need to login as janed:

sudo login

```
jane@linux-client:~$ sudo login
linux-client login: CORP+janed
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)
```

id

```
CORP+janed@linux-client:~$ id
uid=2001117(CORP+janed) gid=2000513(CORP+domain users) groups=2000513(CORP+domain users),2001117(CORP+janed)
```

Back in the Server Manager in Active Directory. I need to navigate to “Active Directory Users and Computers”. Look under the corp.joe-corp.com > Computers folder, now I see LINUX-CLIENT as a computer connected to the domain now.

Email Security Server

An email server is a system designed to send, receive, store, and manage email communication for users. It uses protocols such as SMTP (Simple Mail Transfer Protocol) for sending emails, and IMAP (Internet Message Access Protocol) or POP3 (Post Office Protocol) for receiving and managing email messages.

Working Here:

I will be configuring Postfix as a Mail Transfer Agent (MTA), which is used for sending and routing emails on Linux servers.

Email servers are much less common today than they were 20+ years ago. Running an email server requires expertise with configuring DNS records, securing against spam, developing a good reputation via IP address for email delivery, and more. With the emergence of third-party application such as Gmail, Microsoft 365, and ProtonMail (for personal use), these managed services provide scalable, secure email without having to manage the infrastructure of an email server.

The project provides good insight into how email works and why it's important to secure your email gateways. I will set up the underlying Operating System, Ubuntu 22.04 Server LTS, and connection through Active Directory. Additional guides will be provided for configuring Postfix.

Security Implications:

While running an email server like Postfix on Ubuntu Server 22.04 gives you control, it also introduces several security considerations:

1. **Open Relay Exploitation:** If improperly configured, your server can be used by spammers to send large volumes of email, damaging your IP reputation.
2. **Brute Force Attacks:** Attackers often attempt to compromise accounts via brute force or credential stuffing.
3. **Spam and Phishing:** Attackers may spoof your domain or use your server for phishing campaigns.
4. **Data Breaches:** Poorly secured servers can expose sensitive emails and user credentials.
5. **Malware Delivery:** Your server could inadvertently become a vehicle for spreading malware if attachments are not scanned.

First, I installed the Ubuntu Server VM with default items to begin. Once I got to the profile configuration part, I entered the following:

Your name: email-svr

Your servers name: email-svr

Choose a password: *****

Next option that came up I decided to install OpenSSH Server because this will be an attack vector that I will utilize in the attack section.

Connect Ubuntu Server to Active Directory:

I had to switch the NAT Network to a Bridged connection in order to have a internet connection before I could connect the accounts. I switched it back after it connected. Refer back to the tutorial just before this to connect the server the same way you connect the Linux Client to Active Directory.

To confirm everything worked, go into “Active Directory Users and Computers” again and check the corp.joe-corp.com > Computers folder and you should see EMAIL-SVR.

Security Onion

Here is the first Defensive tool utilized in this network setup. Let me provide some background that I learned while doing this project.

What is Security Onion?

Security Onion is a free, open-source platform for network security monitoring (NSM), log management, and intrusion detection. It provides a comprehensive suite of tools designed to help analysts detect, investigate, and respond to cyber threats in real time. Think of Security Onion as the operating system equivalent of Kali Linux. Security Onion comes set with a suite of preconfigured tools, including Zeek (formerly Bro), Suricata, and Elastic Stack (Elasticsearch, Logstash, and Kibana).

How is Security Onion Used?

Security Onion is used for a wide range of security monitoring and incident response tasks:

1. Network Security Monitoring (NSM)
 - Packet Capture and Analysis: Tools like Zeek analyze network traffic for anomalies or suspicious activity.
 - Intrusion Detection Systems (IDS): Suricata performs real-time deep packet inspection to identify malicious activity.
2. Log Management and Analysis
 - Collects and aggregates logs from endpoints, firewalls, servers, and other devices to provide visibility into network activity.
 - Elastic Stack enables querying, visualizing, and analyzing logs in an intuitive dashboard.
3. Incident Response
 - Alerts and Correlation: Generates alerts for suspicious activities, helping analysts prioritize threats.
 - Threat Hunting: Analysts can proactively search for signs of compromise using enriched datasets.

Security Implications:

Security Onion plays a critical role in enhancing an organization's security posture by providing advanced detection and monitoring capabilities.

- **Proactive Threat Detection:** Identifies threats before they escalate, reducing the impact of cyberattacks.
- **Comprehensive Visibility:** Aggregates network and endpoint data for a holistic view of the environment.
- **Incident Response Readiness:** Equips analysts with tools to quickly investigate and respond to alerts.

Best Practice - Separate Monitoring Infrastructure: Keep Security Onion servers isolated to minimize the risk of compromise.

Security Onion Setup:

First, use VMware to setup a new VM with a security onion image or known as a .iso file. First settings is Security Onion Desktop. Next few settings are default. There will be a setting that comes up that asks for a hostname and not a Fully Qualified Domain Name (FQDN).

- hostname: **joe-corp-sec-work**
- Assign the IPv4 Address with CIDR notation: **10.0.0.103/24**
- Gateway's IPv4 address: **10.0.0.2**
- DNS servers: **8.8.8.8** (Google)
- DNS search domain: **corp.joe-corp.com**

It's easy, feel free to login and search around for the various defensive security tools that it provides!

Wazuh SIEM

Wazuh is an open-source platform that provides extended detection response (XDR) and Security Information and Event Management (SIEM) to protect cloud, container, and server workloads. Wazuh comes with an array of capabilities including log data analytics, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and support for regulatory compliance.

- **Extended Detection Response (XDR):** XDR is a defensive approach that integrates data and insights from multiple security layers. Data is collected and aggregated into a unified platform from data sources such as workstations, servers, cloud environments, and network traffic. XDR provides improved detection, investigation, and response to threats by centralizing all data to identify patterns, trends, and analyze malicious activity. In the context of Wazuh, there are many capabilities and features which enable XDR including multi-source data collection, threat detection, intrusion detection, incident investigation, and file integrity monitoring (FIM).
- **Security Information and Event Management (SIEM):** Refers to a system that combines log management, threat detection, and incident response to help organizations monitor and secure their IT environments. Wazuh acts as a SIEM solution by collecting and analyzing security data from multiple sources, detecting threats in real time, and facilitating efficient incident response.

Wazuh relies on an agent-based ecosystem. Software agents are deployed to workstations, servers, containers, and virtual machines which send data to Wazuh's server for processing, aggregation, and visualization of security-relevant information.

3 Main Components:

- **Wazuh Indexer:** A highly scalable, full-text search and analytics engine. This central component indexes and stores alerts generated by the Wazuh server.
- **Wazuh Server:** Analyzes data received from the agents. It processes it through decoders and rules, using threat intelligence to look for well-known indicators of compromise (IOCs). A single server can analyze data from hundreds or thousands of agents, and scale horizontally when set up as a cluster. This central component is also used to manage the agents, configuring and upgrading them remotely when necessary.

- **Wazuh Dashboard:** Is the web user interface for data visualization and analysis. It includes out-of-the-box dashboards for threat hunting, regulatory compliance (e.g., PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration assessment results, cloud infrastructure monitoring events, and others. It is also used to manage Wazuh configuration and to monitor its status.

I will be using Wazuh as our central hub for security logging, analysis, defense, and remediation while I conduct cyber-attack/defend exercises. Wazuh provides a solid foundation for gathering relevant data while applying remediations. I will be able to actively view and visualize what happens when attackers are able to achieve initial access, lateral movement, elevation of privileges, persistence, and exfiltration.

As part of this project, I will be configuring Wazuh's SIEM, XDR, and File Integrity Monitoring (FIM) modules. The Vulnerability Detection module has a default configuration applied.

Wazuh Agent Deployment:

In Wazuh, there are two primary ways to manage and configure agents: centralized configuration via `agent.conf` and local configuration on each agent via `ossec.conf`.

Centralized Configuration (agent.conf):

Configuration changes and centralized management are applied to all agents via the Wazuh manager. The `agent.conf` file is edited on the Wazuh manager to define settings such as log collection rules, configuration changes and active response policies. This is best used for environments with many agents where centralized management is preferred.

This is the configuration style used in this walkthrough guide.

Local Configuration (ossec.conf):

Allows individual agents to have unique configurations. This offers flexibility for agents with specific requirements and is useful when agents are deployed in standalone environments. The `ossec.conf` file is manually edited on each agent. Manually editing each agent can lead to configuration drift, where configurations are difficult to manage.

When both configurations are utilized, the local and shared configuration changes are merged. However, the last configuration of any setting is read in the `agent.conf` file. The `agent.conf` file will overwrite any conflicting changes between the two.

Security Implications:

Running an XDR and SIEM services provides significant advantages to monitor, detect, prevent, and respond to security-related activity. Most mainstream XDR and SIEMs work in a similar fashion, providing similar information. Wazuh is not the only tool or solution offered. Since it's free and provides a suite of capabilities, Wazuh was chosen as the security tool for this lab.

Some security implications or enhancements include:

1. Threat Detection

- **Event Correlation:** Wazuh analyzes and correlates log data from a wide range of sources (servers, endpoints, network devices) to detect malicious activities such as brute-force attacks, privilege escalation, and suspicious login attempts. This helps in identifying threats across multiple layers of the IT infrastructure.
- **Real-time Alerts:** Wazuh generates real-time alerts for malicious behavior, such as unauthorized access, potential malware infections, or network anomalies, enabling immediate response. I am going to configure a few alerts later on.

2. Proactive Defense

- **Intrusion Detection:** Wazuh acts as a host-based intrusion detection system (HIDS), monitoring file integrity, log integrity, and detecting unauthorized changes.
- **Endpoint Visibility:** As a part of its XDR functionality, Wazuh collects and analyzes endpoint data to detect advanced threats like fileless malware, lateral movement, and ransomware activities.

3. Incident Response and Investigation

- **Automated Responses:** Wazuh can be configured to automatically trigger responses (e.g., blocking an IP address or executing scripts to quarantine infected machines), significantly reducing the time between detection and mitigation.
- **Forensics and Data Collection:** By storing logs and system data, Wazuh provides critical information for incident investigation. This allows teams to retrace attack steps, identify attack vectors, and determine the scope of the breach.

4. Centralized Security Management

- **The UI:** Wazuh aggregates data from multiple sources (network, endpoint, and cloud), providing a centralized security management platform. This allows security teams to monitor the health of the entire infrastructure from a single pane of glass, reducing complexity and enhancing situational awareness.
- **Integration with Other Tools:** Wazuh integrates with other security technologies such as threat intelligence feeds, vulnerability scanners, and security orchestration tools, creating a cohesive security ecosystem that strengthens overall defense.

5. Threat Hunting

- **Behavioral Analysis:** With Wazuh's ability to monitor system behavior, security teams can hunt for signs of advanced persistent threats (APTs), exploits, and other sophisticated attack methods by analyzing anomalies in system and network behavior.
- **Custom Rules and Detection:** Wazuh allows the creation of custom detection rules based on unique organizational needs, enabling more targeted threat hunting and response strategies.

Setup Wazuh Indexer & Server:

Follow the link to the quick start guide on the Wazuh website:

<https://documentation.wazuh.com/current/quickstart.html>

After you install the indexer and server, make sure you add each endpoint that you will be using in your lab to the Wazuh server. I did this by adding agents. Here is how to add an agent. It is extremely simple:

<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>

Custom Logs:

Wazuh offers a variety of default logs that are automatically ingested into the Wazuh indexer. This is a great place to start.

Based on our upcoming Attack/Defend scenario, I will aim to expand the types of logs collected by both Linux and Windows agents to gather a more comprehensive dataset of log activity.

Let's edit the *agent.conf* file located in the Linux and Windows Wazuh groups. Configuration statements (XML declarations) will apply to all endpoints in the group.

Windows Group:

Go to "Server Management" > "Endpoint Groups" > Pencil Icon to edit the *agent.conf* file for the Windows group.

```
<agent_config>
  <!-- Shared agent configuration here -->
  <localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
  </localfile>
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>
</agent_config>
```

Here I am onboarding the Windows Security and Application Event Logs. These are default log sources used to collect host-base activity.

Linux Group:

Go to “Server Management” > “Endpoint Groups” > Pencil Icon to edit the agent.conf file for the Linux group.

```
<agent_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/auth.log</location>
  </localfile>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/secure</location>
  </localfile>
  <localfile>
    <log_format>audit</log_format>
    <location>/var/log/audit/audit.log</location>
  </localfile>
</agent_config>
```

Here I am onboarding “**/var/log/auth.log**”, “**/var/log/secure**”, and “**/var/log/audit.log**”. These are log sources that can be used to collect host-based activities.

Kali Linux

Kali Linux is a specialized Linux distribution tailored for cybersecurity professionals and ethical hackers. Developed by Offensive Security, it is a Debian-based operating system preloaded with tools designed for penetration testing, ethical hacking, and digital forensics. Kali Linux is widely used for assessing system vulnerabilities, testing network security, and investigating cyber incidents. Kali comes with a suite of security tools to assist in the operations.

How is Kali Linux Used?

Kali Linux serves multiple purposes in the cybersecurity field, including:

1. **Penetration Testing:** Professionals use Kali Linux to simulate real-world cyberattacks and identify vulnerabilities in systems, networks, and applications. Tools like Metasploit and Burp Suite are often employed in these scenarios.
2. **Vulnerability Assessment:** It provides tools to scan and identify weaknesses in infrastructure, ensuring they are addressed before exploitation.
3. **Cybersecurity Training:** Kali Linux is widely used in cybersecurity training programs, competitions, and certifications.

Security Implications:

Leveraging an operating system like Kali Linux carries certain benefits and risks.

Benefits:

- Can be used by trained professionals to help understand their organizational security controls and identify vulnerabilities before actors can exploit them.
- Offers a platform to safely practice offense security techniques in controlled environments.
- Tools are aggregated in one centralized ecosystem.

Risks:

- This tool can also be used maliciously by attackers if accessed by unauthorized individuals.

- Kali Linux is not meant to be a production environment without isolation. Be careful.

Configuring a Kali Linux virtual machine is very easy to setup. It has a ton of offensive security preinstalled on the system. Just download the iso file off of the Kali Linux website and set it up on VMware.

Conclusion

The **Simulated Enterprise Network project** has been a foundational hands-on experience in designing, configuring, and operating a realistic enterprise IT environment. Through the simulation of core business infrastructure—including Active Directory, DHCP, DNS, internal email services, client workstations, monitoring systems, and an attacker environment—I've gained critical skills that bridge theory and practice in cybersecurity.

This project has deepened my understanding of how enterprise networks are architected, how attackers exploit misconfigurations, and how defenders detect and respond to those threats. I worked with industry-standard tools like **Windows Server 2025**, **Security Onion**, **Wazuh**, and **Kali Linux**, and navigated the full workflow from system provisioning to red/blue team exercises.

Beyond technical skills, this project also reinforced the importance of:

- **Documentation** for repeatability and clarity
- **Segmentation** for defense-in-depth
- **Logging and visibility** for early detection
- **User management and access control** as critical security layers

With this lab complete, I now have a flexible platform to practice advanced skills like incident response, lateral movement detection, vulnerability assessments, and even policy implementation. It also serves as a strong demonstration of my initiative and readiness for entry-level roles such as **Cybersecurity Analyst**, **SOC Analyst**, or **Cybersecurity Consultant**.

This environment will continue to evolve as I expand it with more detection rules, automation tools, and cloud integrations to reflect modern hybrid networks. Check out my other projects to see how I am using this enterprise environment to learn.

Now that the core infrastructure for project is in place, I plan to use this lab environment as a foundation for expanding my cybersecurity knowledge and skillset, especially in **defensive operations**. The modular design and isolated NAT configuration make it ideal for layering new tools, testing attacks safely, and experimenting with enterprise-grade solutions.

Upcoming Learning Areas and Projects:

- **SIEM Tuning and Use Case Development**

I will expand Wazuh and Security Onion integrations by simulating real attack patterns (e.g., brute force, lateral movement, data exfiltration) to write custom detection rules and alerts.

- **Threat Hunting Practice**

Using Zeek and Suricata logs, I'll practice identifying anomalies through log analysis and develop hypotheses to search for indicators of compromise (IOCs).

- **Windows Event Log Analysis & Sysmon Integration**

I plan to deploy Sysmon on Windows clients to enrich endpoint visibility and learn how to detect behavior-based indicators like process injections and parent-child anomalies.

- **Incident Response Simulations**

I'll simulate and document complete incidents, including timeline reconstruction, containment steps, and eradication plans—building my ability to write professional IR reports.

- **Purple Teaming**

By executing known attack techniques from MITRE ATT&CK and observing their artifacts in the logs, I'll connect offensive actions to defensive controls, improving both detection and attacker mindset.

- **Policy and Compliance Simulation**

I also plan to build out Group Policy Objects (GPOs), password policies, and endpoint hardening baselines to mimic a compliant, secure enterprise environment.

This system is not just a static lab—it's a growing testbed that will evolve alongside my skills. It will help me stay sharp on emerging threats and defenses in the field.