VIRTUAL LAB

Vulnerability Assessment

Jeffrey Obi
October 2025

Contents

Introduction

This report documents the initial security assessment performed on the virtual network components after the setup of a virtualized lab environment. The primary objective was to simulate a small enterprise network with a Domain Controller and client machines, and then use a penetration testing Linux distribution (Parrot Security) to conduct reconnaissance and enumeration.

Goals of the Assessment

The main goals of this virtual machine vulnerability assessment were:

1. **Domain Configuration:** Configure the Windows Server 2022 machine as a Domain Controller (Active Directory + DNS) and successfully join the Windows 11 client to the domain (`mssp.local`).
2. **Network Connectivity:** Verify inter-machine communication within the isolated Host-Only virtual network.
3. **Security Testing Demonstration:** Demonstrate the use of common security tools available on Parrot Security to test the security posture of the newly configured domain, specifically focusing on information gathering (enumeration) and initial brute-force attempts.
4. **Vulnerability Identification:** Identify and document any initial vulnerabilities or insecure configurations (e.g., anonymous access, open ports) found during the reconnaissance phase.

Tools Used

The following key tools were utilized during the security testing phase performed from the Parrot Security machine:

Tool	Purpose
Nmap	Network scanner used for host discovery and port scanning to identify open services on the Domain Controller and client machines.
ldapsearch	Command-line utility for querying the Lightweight Directory Access Protocol (LDAP) service to discover domain metadata.

Tool	Purpose
Enum4linux	Tool for enumerating information from Windows and Samba systems via SMB/Samba, including user lists, group lists, and share information.
Hydra	A fast and flexible parallelized login cracker used for attempting a dictionary-based password attack against the Domain Controller's SMB service.
VMware Workstation Pro	Virtualizer software used to host and manage all virtual machines (Parrot Security, Windows Server 2022, Windows 11).

Procedure

Step 1: Configure the Windows Server as a Domain Controller (Active Directory + DNS)

a. Begin **Server Manager** Configuration.
   i. On the **WindowsServer2022** Virtual Machine tab, select **Power on this virtual machine.**
   ii. Log in to the machine and complete the booting process.
   iii. Open **Server Manager**.
   iv. On the **Dashboard,** select **Add roles and features.**

b. Configure Roles.
   i. On the **Before You Begin** tab: read through installation requirements.
   ii. On the **Installation Type** tab: choose **Role-based or feature-based installation.**
   iii. On the **Server Selection** tab: select Windows Server 2022 virtual machine.
   iv. On the **Server Roles** tab: select/check **Active Directory Domain Services** and confirm in the pop-up window**.**
   v. On the **Features** tab: leave default selections and proceed.
   vi. On the **AD DS** tab: read through final information regarding **Active Directory Domain Services** before installation.
   vii. On the **Confirmation** tab: read through installation details then click **Install**.

viii. On the **Results** tab: installation finishes. Click **Promote this server to a domain controller** from inside the window. This opens another window called **Active Directory Domain Services Configuration Wizard** for further configuration**.**

c. Configure **Active Directory Domain Services.**

i. Apply required configurations on the **Active Directory Domain Services Configuration Wizard**

ii. On the **Deployment Configuration** tab: select **Add new forest** and specify root domain name **(mssp.local).**

iii. On the **Domain Controller Options** tab: check **Domain Name System (DNS) Server** and create password in the provided entry boxes.

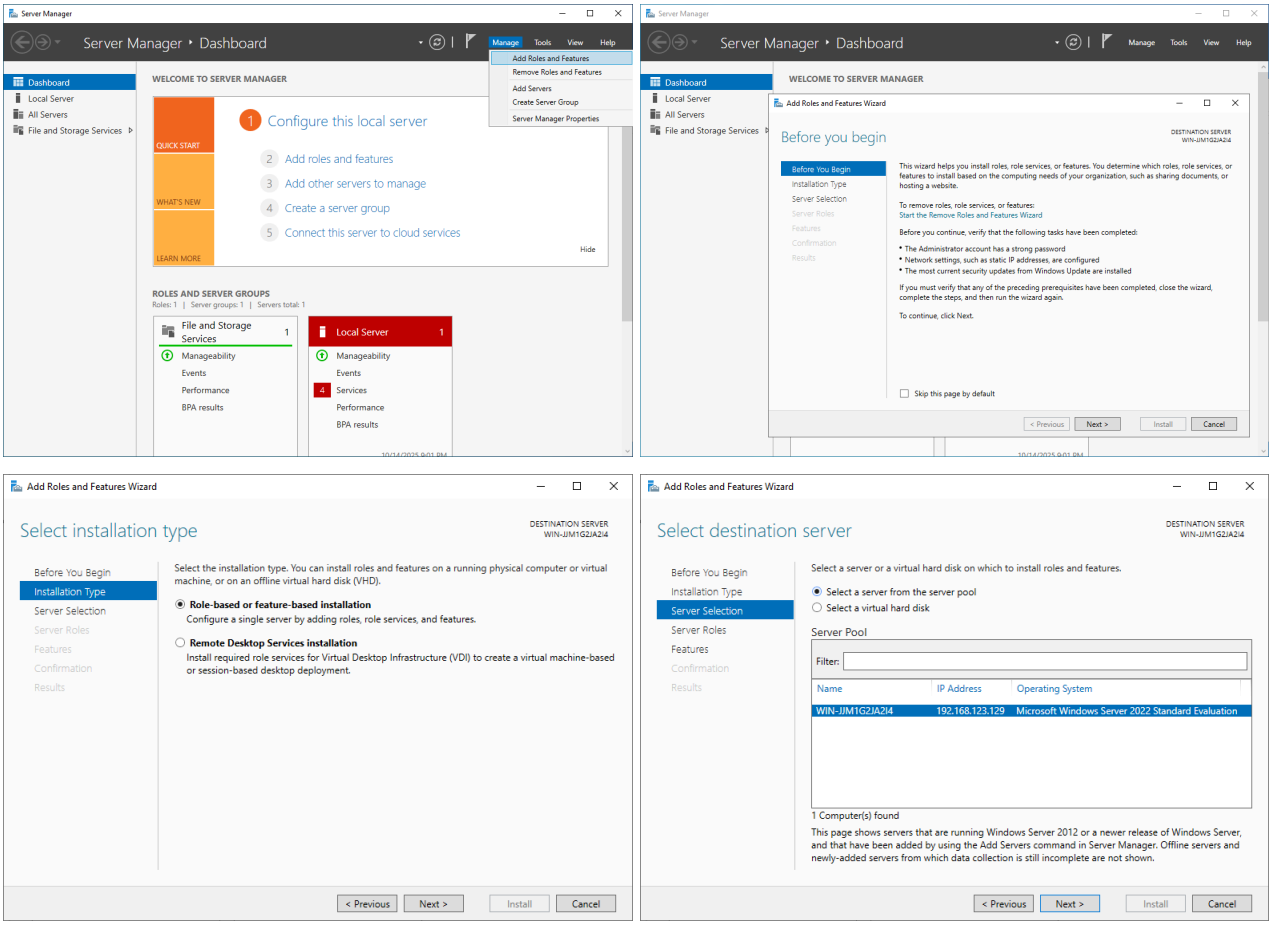
iv. On the **Additional Options** tab: **The NetBIOS domain name** is set to **MSSP.**

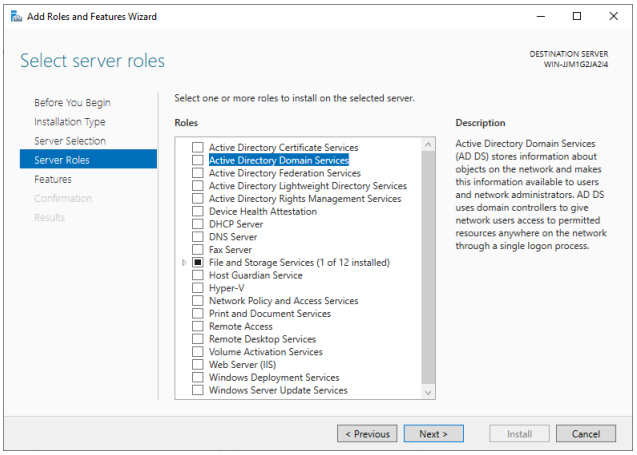
v. On the **Paths** tab: default set paths for Database, Log files and SYSVOL are accepted.

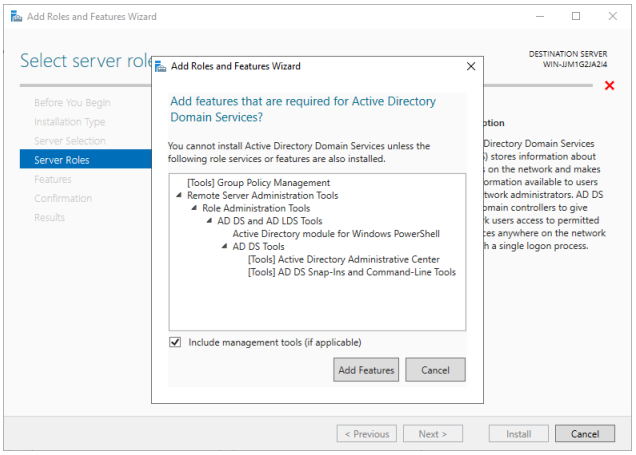
vi. On the **Review Options** tab: read through applied configurations.

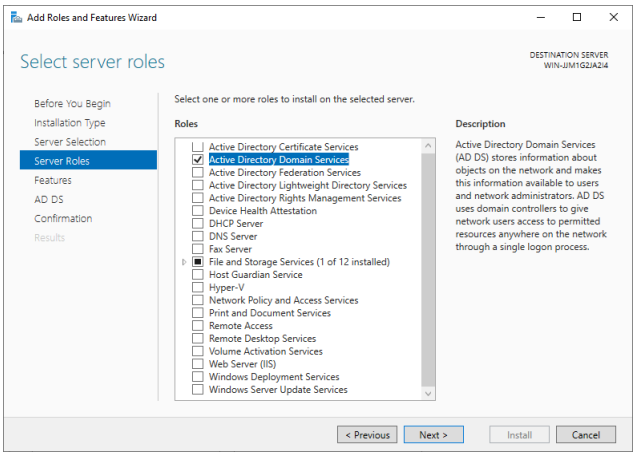
vii. On the **Prerequisites Check** tab: select **Run prerequisites check.** All prerequisite checks passed successfully. Click **Install.**

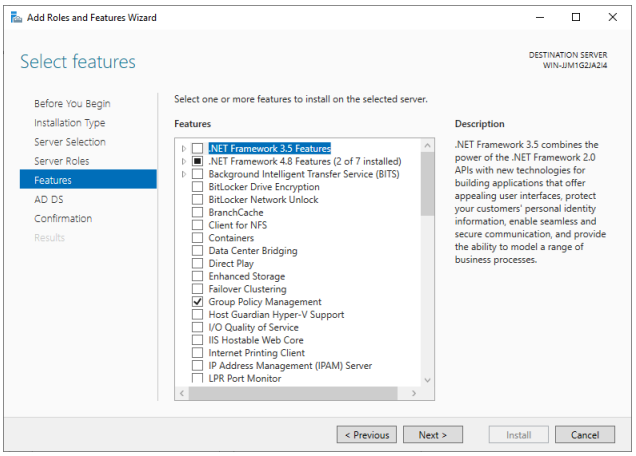
viii. After installation, the system restarts.

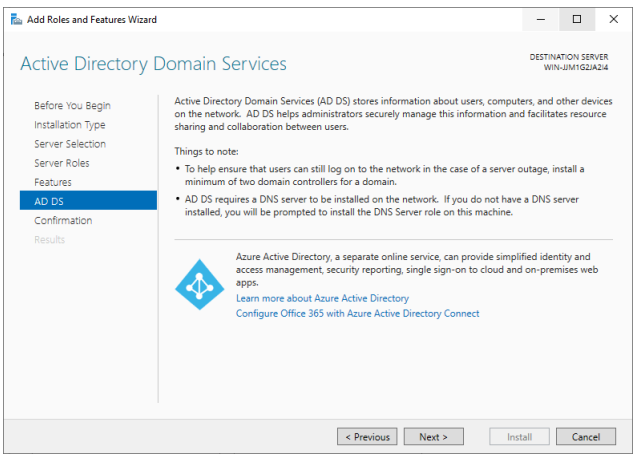


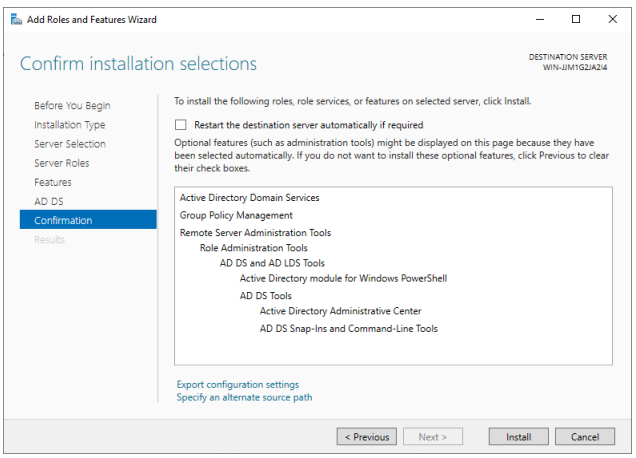

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

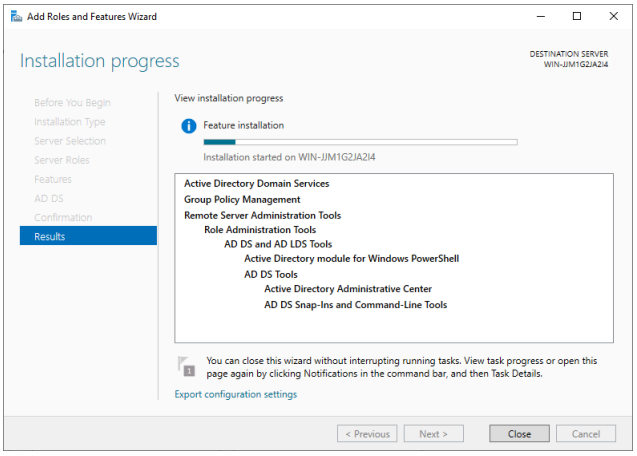

Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel

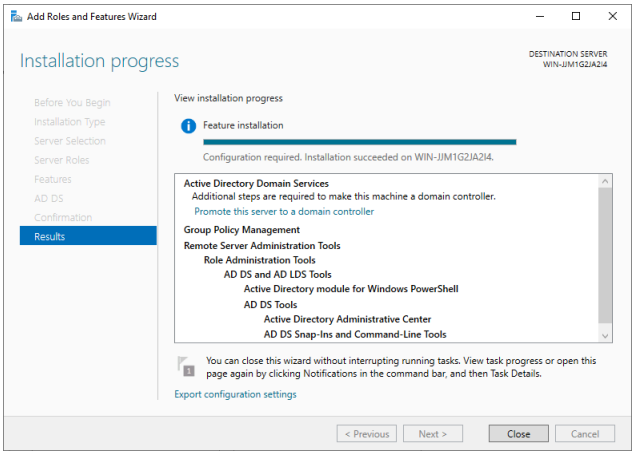

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

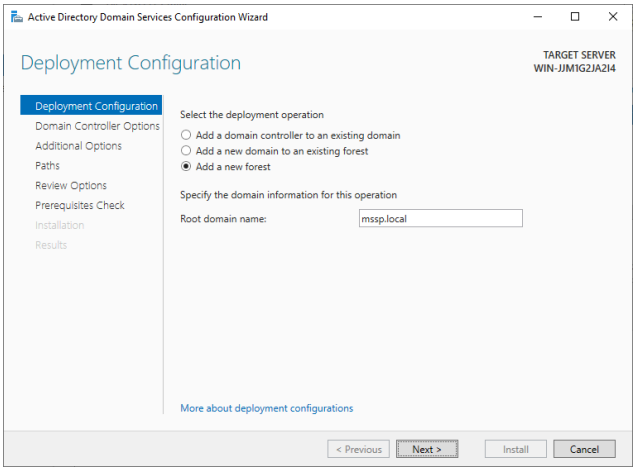

Add Roles and Features Wizard
Select features
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.8 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
LPR Port Monitor
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

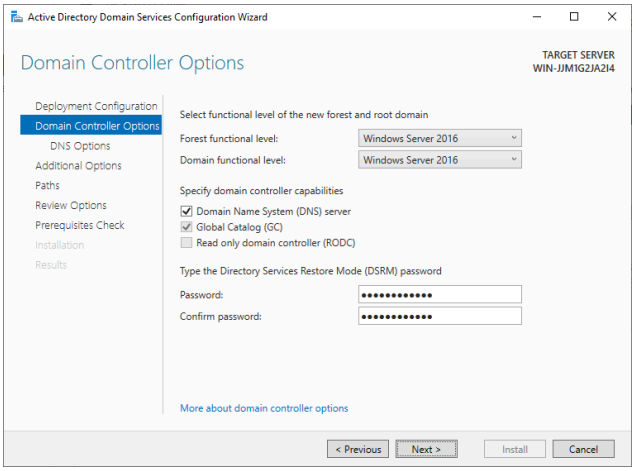

Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel

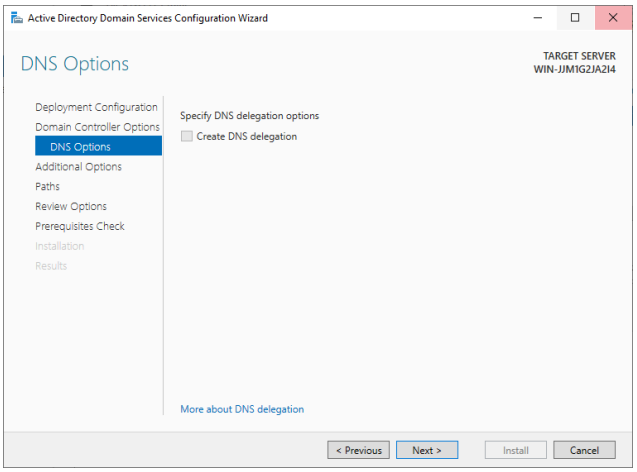

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

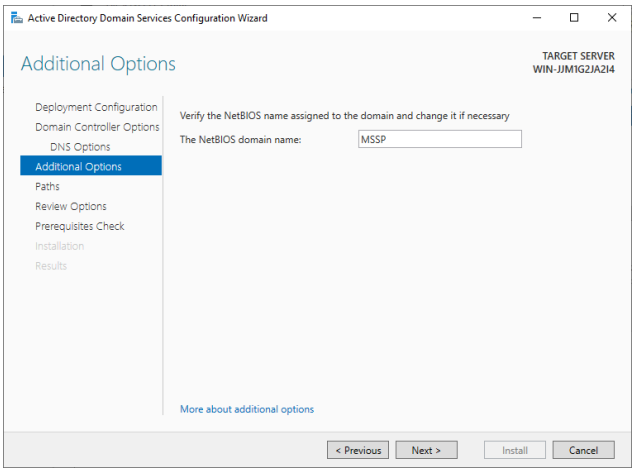

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Installation started on WIN-JJM1G2JA2I4
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

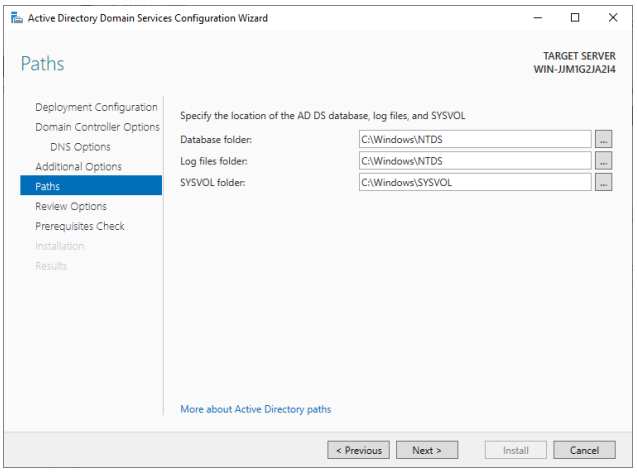

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-JJM1G2JA2I4
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN-JJM1G2JA2I4.
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

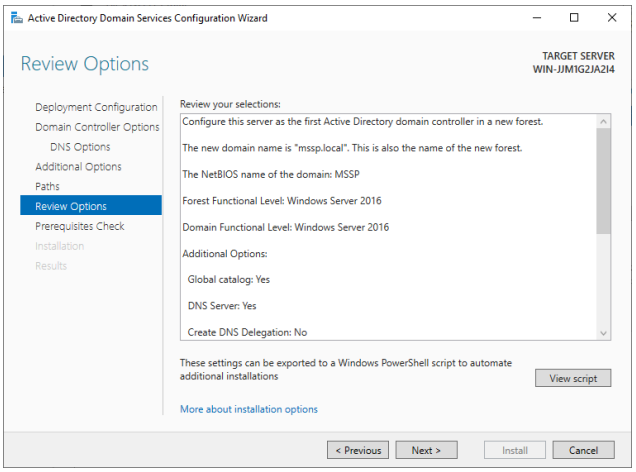

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
mssp.local
More about deployment configurations
< Previous
Next >
Install
Cancel

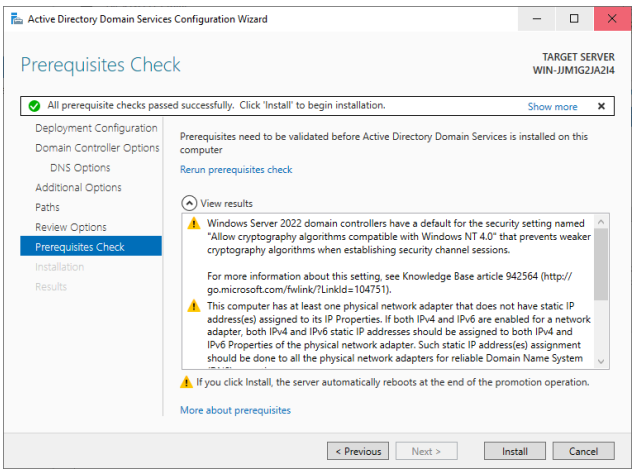

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
MSSP
More about additional options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
WIN-JJM1G2JA2I4
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "mssp.local". This is also the name of the new forest.
The NetBIOS name of the domain: MSSP
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel



Step 2: Configure Virtual Network Topology

a. Configure Domain Controller Machine Network Adapters
   i. Open the **WindowsServer2022** Virtual Machine tab
   ii. Click **Edit Virtual Machine Settings** and access the **Virtual Machine Settings** window.
   iii. Under the **Hardware** tab, select **Add** and in the **Add Hardware Wizard** window which pops up, select **Network Adapter** and click **Finish.** This adds a second network adapter called **Network Adapter 2,** as displayed under the **Hardware** tab.
   iv. For **Network Adapter,** select **Custom: Specific virtual network** and in the drop-down menu, select **Vmnet11 (Host-Only).**
   v. For **Network Adapter 2,** select **Custom: Specific virtual network** and in the drop-down menu, select **Vmnet8 (NAT)**
   vi. Select **OK** and exit the **Virtual Machine Settings** window, returning to the **WindowsServer2022** Virtual Machine tab.

b. Configure Domain Controller Machine IP Addresses
   i. On the **WindowsServer2022** Virtual Machine tab, select **Power on this virtual machine.**
   ii. Log in to the machine and complete the booting process.
   iii. Open the **Control Panel** and enter **Network and Sharing Center,** then open **Change Adapter Settings.**
   iv. It contains 2 Ethernet adapters. (**Ethernet0** and **Ethernet1**). Right-click each one and select **Status.** In the Status window, you will see which adapter is active (the **NAT** adapter connected to the internet) and which adapter is inactive with no active connection (the **Host-only** adapter).

v. Rename the adapters from **Ethernet1** (which is the active **NAT** adapter) to **Internet NIC** and from **Ethernet0** (which is the inactive **Host-only** adapter) to **Internal NIC.**
vi. Right-click the **Internal NIC** adapter and select **Properties.** In the Wi-Fi Properties window, select **Internet Protocol Version 4 (TCP/IPv4)** and select the **Properties** button underneath.
vii. Under the **General** tab, select **Use the following IP address:** and **Use the following DNS Server addresses** to input static IP addresses and a DNS server address, respectively, for the network adapter.
viii. Input the following addresses:
- IP address: 192.168.1.10
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1
- Preferred DNS server: 192.168.1.10
- Alternative DNS server: (left blank)

ix. Select **OK** and validate all changes as you close the settings windows.

c. Configure Windows Client **(Windows 11)** Network Adapter.
i. Open the **Windows11** Virtual Machine Tab
ii. Click **Edit Virtual Machine Settings** and access the **Virtual Machine Settings** window.
iii. Under the **Hardware** tab, select **Network Adapter.**
iv. On the right, select **Host-only.**
v. Select **OK** and exit the **Virtual Machine Settings** window, returning to the **Windows11** Virtual Machine tab.

d. Configure Windows Client **(Windows 11)** IP Address.
i. On the **Windows11** Virtual Machine tab, select **Power on this virtual machine.**
ii. Log in to the machine and complete the booting process.
iii. Open the **Control Panel** and enter **Network and Sharing Center,** then open **Change Adapter Settings.**
iv. Right-click the **Ethernet** adapter and select **Properties.** In the Wi-Fi Properties window, select **Internet Protocol Version 4 (TCP/IPv4)** and select the **Properties** button underneath.
v. Under the **General** tab, select **Use the following IP address:** and **Use the following DNS Server addresses** to input static IP addresses and a DNS server address, respectively, for the network adapter.
vi. Input the following addresses:
- IP address: 192.168.1.20
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1

- Preferred DNS server: 192.168.1.10
- Alternative DNS server: (left blank)
- **Note:** The main IP address for this machine is different from the previous Windows Server 2022 virtual machine.

vii. Select **OK** and validate all changes as you close the settings windows.

e. Configure Linux Client **(Parrot Security)** Network Adapter.
   i. Open the **Parrot_Security** Virtual Machine Tab
   ii. Click **Edit Virtual Machine Settings** and access the **Virtual Machine Settings** window.
   iii. Under the **Hardware** tab, select **Network Adapter.**
   iv. On the right, select **Host-only.**
   v. Select **OK** and exit the **Virtual Machine Settings** window, returning to the **Parrot_Security** Virtual Machine tab.

f. Configure Linux Client **(Parrot Security)** IP Address.
   i. On the **Parrot_Security** Virtual Machine tab, select **Power on this virtual machine.**
   ii. Log in to the machine and complete the booting process.
   iii. Open the **Terminal.**
   iv. Use the `sudo su` command and input password.
   v. Apply the following commands:

```
nmcli con modify "Wired connection 1" ipv4.addresses 192.168.1.30/24
nmcli con modify "Wired connection 1" ipv4.gateway 192.168.1.1
nmcli con modify "Wired connection 1" ipv4.method manual
nmcli con up "Wired connection 1"
```

   vi. CLI return message (Configuration Successful):

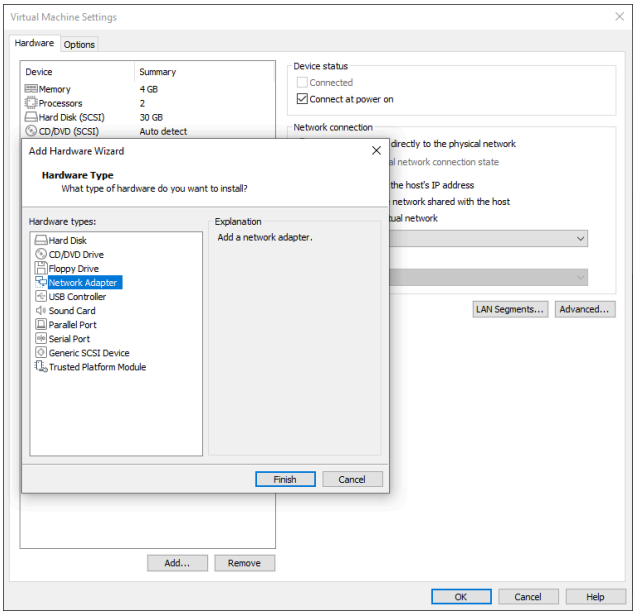
```
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/3)
```

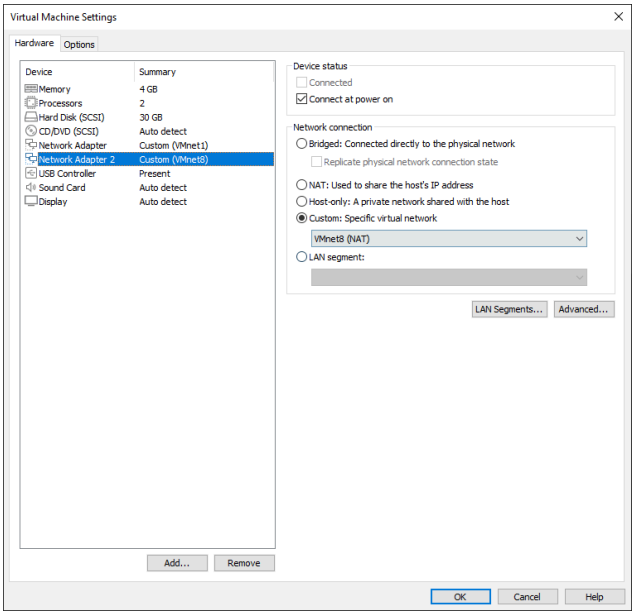
   vii. Close the **Terminal.**

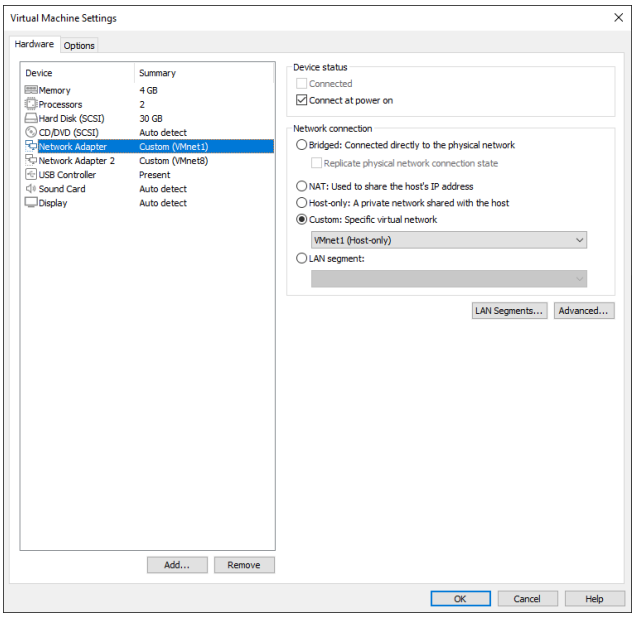
g. Test Connection Between Clients and Domain Controller
   i. Ping Test from Windows Client:
      - Boot into **Windows11** virtual machine
      - Launch **Command Prompt.**
      - Initiate ping test using the following command to send ICMP echo request packets to the Domain system **(Windows Server 22):** `ping 192.168.1.10`
      - Result: All 4 packets returned with 0% packet loss **(Success).**
   ii. Ping Test from Linux Client:
      - Boot into **Windows11** virtual machine
      - Launch the **Terminal,**
      - Initiate ping test using the following command to send ICMP echo request packets to the Domain system **(Windows Server 22):**

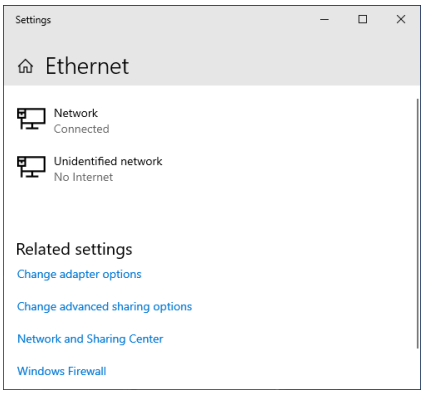
```
ping 192.168.1.10
```

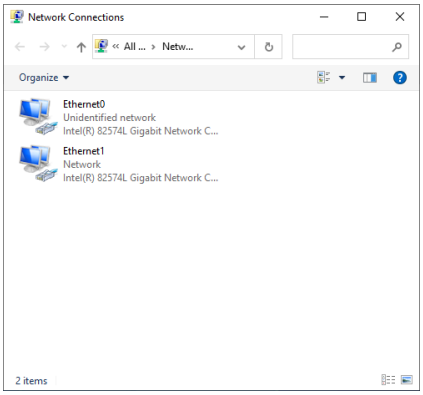
- Result: All 9 packets returned with 0% packet loss **(Success).**

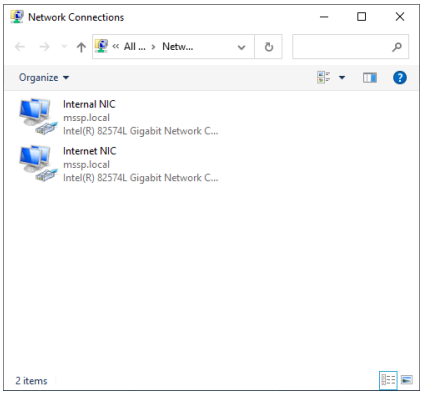


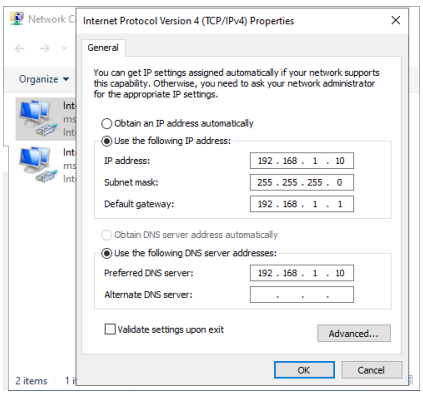


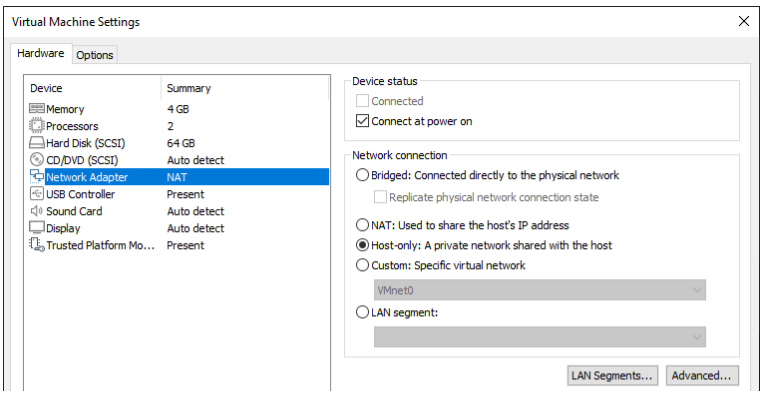


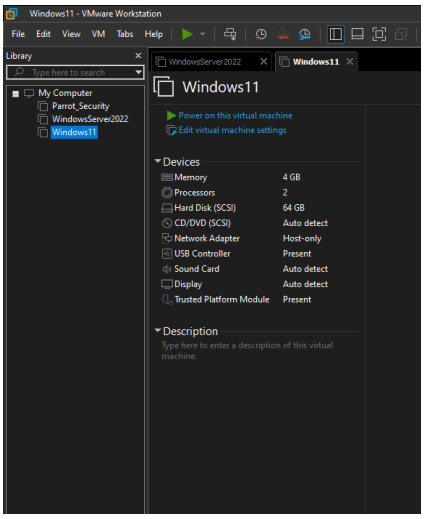


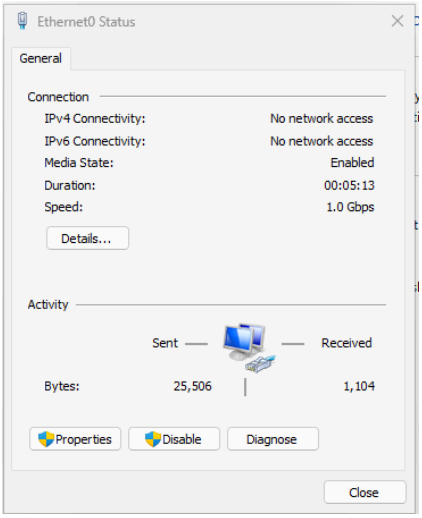


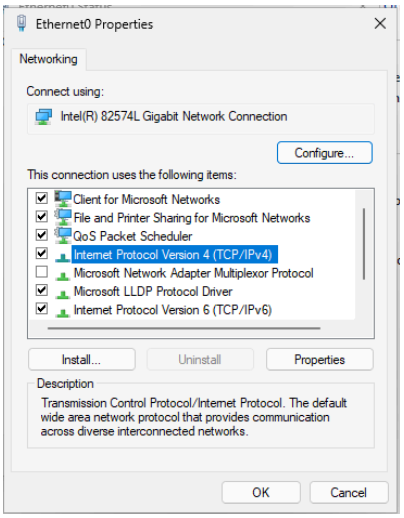


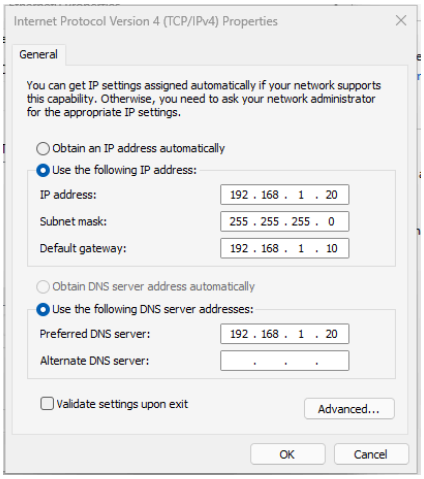

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 10
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

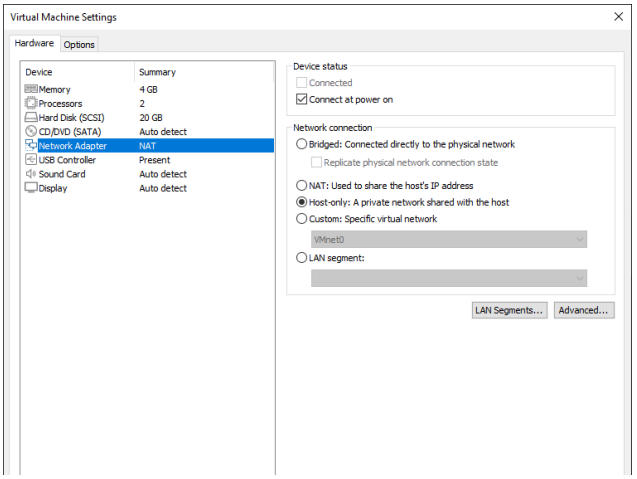

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 4 GB
Processors 2
Hard Disk (SCSI) 64 GB
CD/DVD (SCSI) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Trusted Platform Mo... Present
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...

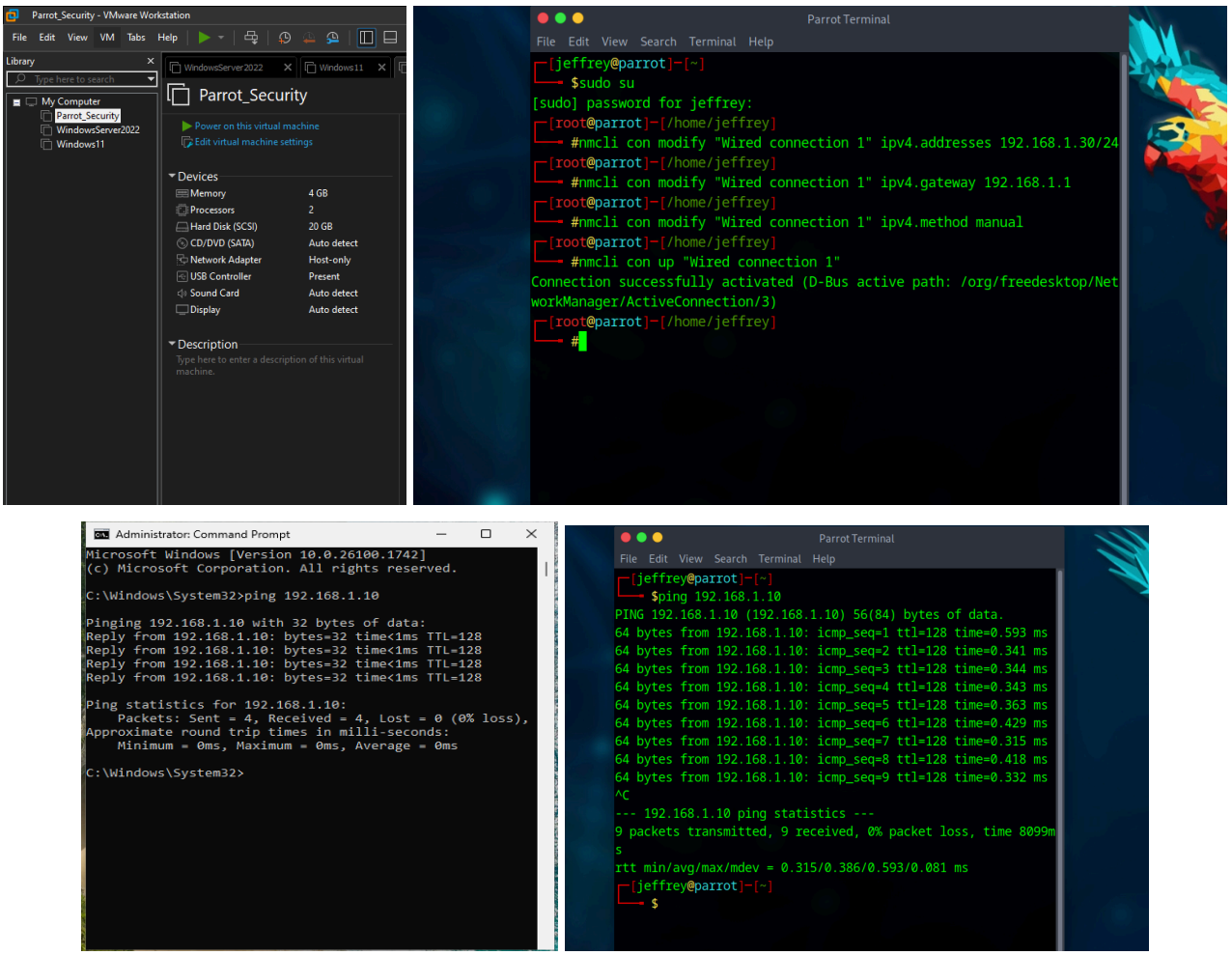

Windows11 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Parrot_Security
WindowsServer2022
Windows11
Windows11
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 4 GB
Processors 2
Hard Disk (SCSI) 64 GB
CD/DVD (SCSI) Auto detect
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect
Trusted Platform Module Present
Description


Ethernet0 Status
General
Connection
IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:05:13
Speed: 1.0 Gbps
Details...
Activity
Sent
Received
Bytes: 25,506 1,104
Properties
Disable
Diagnose
Close


Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

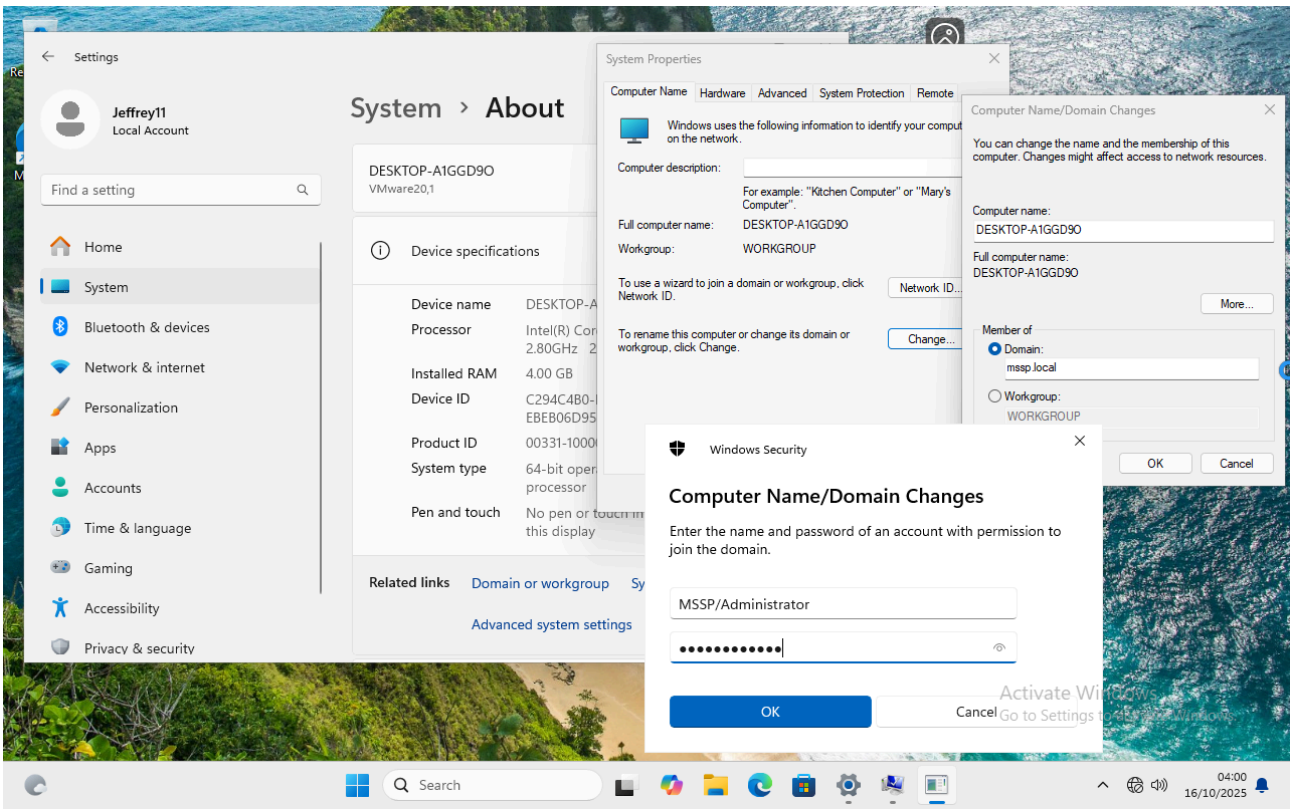

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 20
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 10
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 20
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

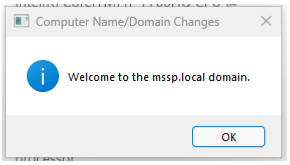

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 4 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...



Step 3: Join Windows Client to the Domain

a. On the **Windows11** Virtual Machine tab, select **Power on this virtual machine.**
b. Log in to the machine and complete the booting process.
c. Open the **Settings.** Select the **System** tab on the left.
d. Select **About** and then select **Domain or workgroup.** This opens a **System Properties** window.
e. Under the **Computer Name** tab, select the **Change** button. This opens another window called **Computer Name/Domain Changes.**
f. In the **Computer Name/Domain Changes** window, input the name **(MSSP\Administrator)** and password of the Domain Controller **(Windows Server 2022).**
g. Select **OK.**
h. A confirmation dialog saying "**Welcome to the mssp.local domain"** appears.
i. Select **OK** to close the dialog.
j. A request to restart the machine to apply changes appears.
k. Select **OK.**





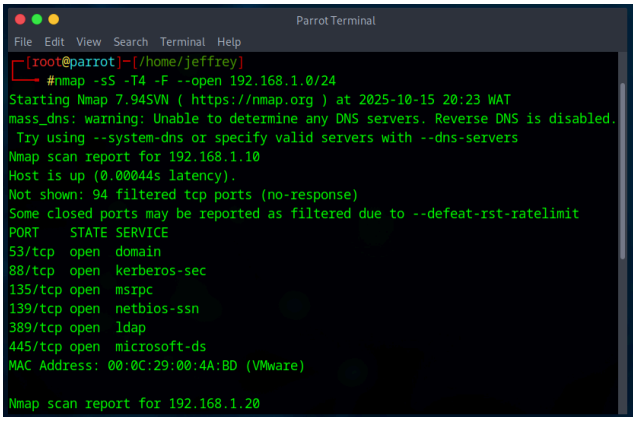
Step 4: Linux Client Security Testing

a. Boot Virtual Machine
   i. On the **Parrot_Security** Virtual Machine tab, select **Power on this virtual machine.**
   ii. Log in to the machine and complete the booting process.
   iii. Open the **Terminal.**

b. Reconnaissance
   i. Nmap Scan
      - Conduct a port scan on the domain's subnet to determine which ports are open and vulnerable.
      - Command:
        `nmap -sS -T4 -F -open 192.168.1.0/24`
      - The Nmap tool returned the open ports within the subnet on the CLI.
      - Observations
        a. There are three devices on the subnet with the IP Addresses **192.168.1.10** (which is actually the **Windows**

Server 2022 machine), **192.168.1.20** (which is actually the **Windows 11** machine) and **192.168.1.30** (which is actually the **Parrot Security** machine).

b. The **Windows Server 2022** machine (192.168.1.10) has the following open ports: 53, 83, 135,139, 389, & 445.
c. The **Windows 11** machine (192.168.1.20) has the following open port: 135.
d. The **Parrot Security** machine (192.168.1.30) has the following open port: 53.



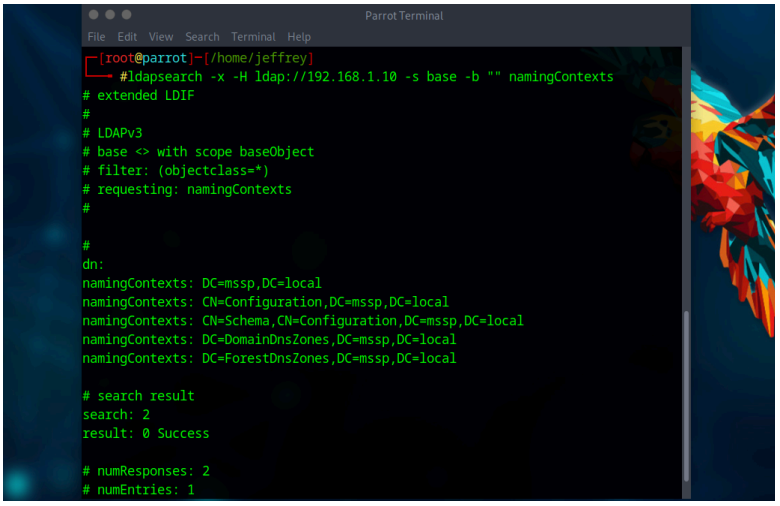
c. Conduct LDAP Search
    i. From the **Nmap** scan, **Port 389** (Directory Server port) is open on the Domain machine **(Windows Server 2022)**.
    ii. This means a Lightweight Directory Access Protocol (LDAP) search can be used to find its domain name.
    iii. Command:
    `ldapsearch -x -H ldap://192.168.1.10 -s base -b "" namingContexts`
    iv. Command Breakdown:

Option	Command Component	Function
ldapsearch	`ldapsearch`	The command-line utility used for searching entries in an LDAP directory.
Simple Auth	`-x`	Uses simple authentication. Since no username/password is specified, it attempts an anonymous bind.
Host	`-H ldap://192.168.1.10`	Specifies the LDAP server to connect to via its IP address (`192.168.1.10`).
Scope	`-s base`	Limits the search to the "base" Distinguished Name (DN) only.
Base DN	`-b ""`	Sets the base DN to an empty string (""), targeting the server's special "root DSE" entry for metadata.

Attribute	`namingContexts`	The specific attribute to request, which contains the directory's base DNs or partitions.
Purpose		Discovering the root of the LDAP directory to inform more specific searches.

v. Results:

- Domain name (second-level domain): **mssp**
- Domain name extension (top-level domain): **local**



d. Enumeration Security Testing

i. From the **Nmap** scan, **Port 445** (SMB port) is open on the Domain machine **(Windows Server 2022)**.

ii. This means Enum4linux can be used to enumerate information from SMB services on the 3 machines on the subnet.

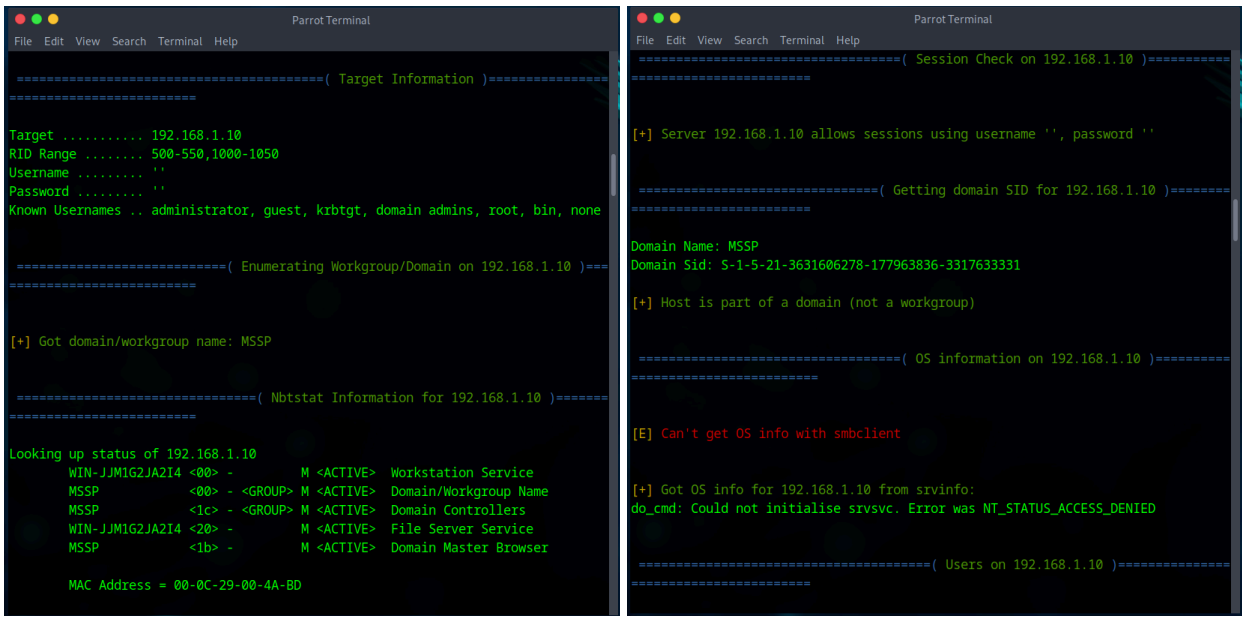
iii. Commands:

```
enum4linux -a 192.168.1.10
enum4linux -a 192.168.1.20
enum4linux -a 192.168.1.30
```

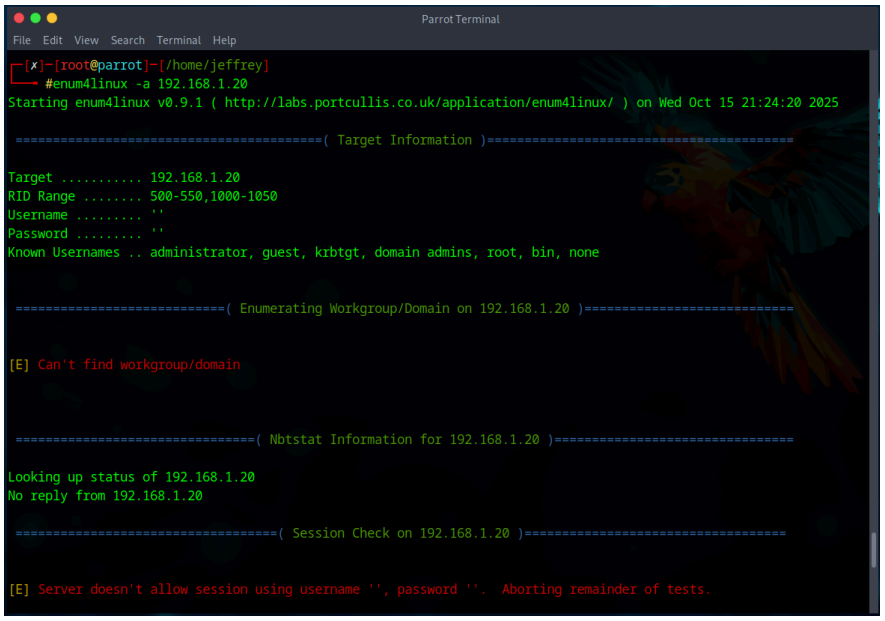
iv. Results &Findings:

- The **Windows Server 2022** machine (192.168.1.10)
  a. RID Range (for users): 500-550, 1000-1050
  b. Known usernames: administrator, guest, krbtgt, domain admins, root, bin, none
  c. Domain/workgroup name: MSSP
  d. Workstation name: WIN-JJM1G2JA2I4
  e. Domain controller: MSSP
  f. Domain Master Browser: MSSP
  g. File Server Service: WIN-JJM1G2JA2I4
  h. Mac Address: 00-0C-29-00-4A-BD
  i. Session Check: "server allows sessions using username '', password ''"

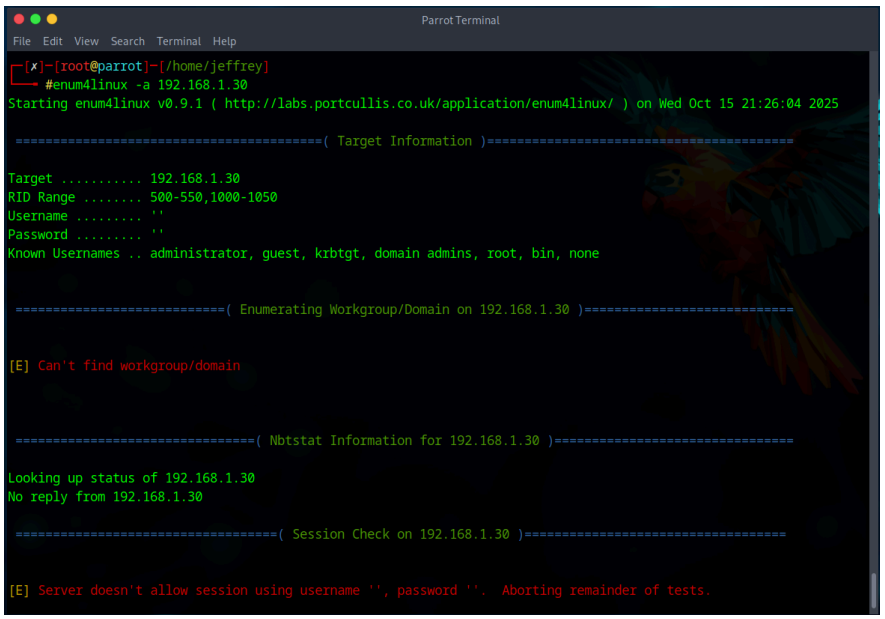
This indicates that the targeted server accepts anonymous access via the SMB (Server Message Block) protocol.



- The **Windows 11** machine (192.168.1.20)
    a. RID Range (for users): 500-550, 1000-1050
    b. Known usernames: administrator, guest, krbtgt, domain admins, root, bin, none
    c. Not much was found.



- The **Parrot Security** machine (192.168.1.30) (Self)
    a. RID Range (for users): 500-550, 1000-1050
    b. Known usernames: administrator, guest, krbtgt, domain admins, root, bin, none
    c. Not much was found.



v. Conclusion

- The Windows 11 client and the Parrot Security client proved resilient against the Enum4linux information enumeration tool.
- The Domain Controller Machine (Windows Server 2022) wasn't as resilient, as the Enum4linux tool was able to get some useful information about the domain, indicating a potential vulnerability in its security.

e. Attempt Password attack using Hydra.

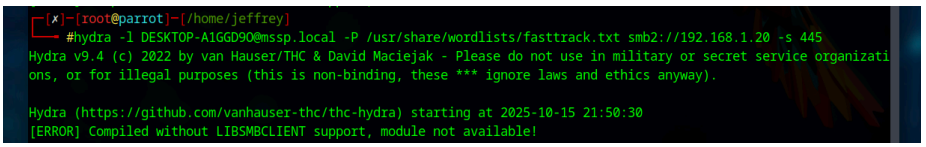
i. Attempt password attack on Domain machine **(Windows Server 2022).**

ii. Linux Terminal Command:

```
hydra -l DESKTOP-A1GGD90@mssp.local -P
/usr/share/wordlists/fasttrack.txt
smb2://192.168.1.20 -s 445
```

iii. Results:

- Return message: [Error] Compiled without LIBSMBCLIENT support, module not available!
- The Hydra compilation is defective.



Conclusion

The successful deployment of the virtualized environment, including the configuration of the Windows Server 2022 as a Domain Controller for the `mssp.local` domain, and the establishment of an isolated Host-Only network with verified connectivity, met the initial setup

goals. The security assessment using the Parrot Security machine successfully demonstrated reconnaissance and enumeration capabilities. The key finding was the Domain Controller's vulnerability to anonymous access via the SMB protocol (Port 445), which allowed the `enum4linux` tool to gather significant domain metadata, user information, and the NetBIOS name. In contrast, the Windows 11 client machine proved more resilient to the tested enumeration techniques. The password brute-force attempt using Hydra was inconclusive due to a tool compilation error, indicating a need for future environment refinement. Overall, the assessment confirmed the network's basic functionality while immediately identifying a critical misconfiguration (anonymous SMB access) on the Domain Controller that requires immediate remediation.

Lessons Learned

- **Initial Configuration Security Review is Essential:** The Domain Controller was immediately found to be susceptible to anonymous SMB enumeration (`enum4linux`), highlighting that even after a standard setup, critical security configurations (like restricting anonymous access to SMB) must be manually reviewed and hardened.
- **Host-Only Network Isolation:** The successful configuration of the Host-Only network (Vmnet11) provided a secure, isolated environment for testing, preventing unintended interaction with the live corporate or home network. This is crucial for safe security testing.
- **Tool Dependency Management:** The failure of the Hydra brute-force attempt due to a missing library dependency (LIBSMBCLIENT) illustrates the importance of verifying that all penetration testing tools are correctly installed, configured, and have the necessary dependencies compiled before beginning an assessment.
- **Enumeration vs. Exploit:** Simple reconnaissance tools like `ldapsearch` and `enum4linux` were highly effective in gathering sensitive domain structure and user information *without* exploiting a known vulnerability, reinforcing the principle that attackers often succeed through robust information gathering rather than zero-day exploits.