

### Scenario:

- You are an ethical hacker with a large organization (EC-Council).
- You must demonstrate knowledge of enumeration, as gaining competitive advantage over your target significantly enhances your ability to perceive and bypass security measures.

### Objectives:

- Extraction various pieces of information about the target
  - e.g.: machine names/ports/OS/services, network resources and shares, usernames/user groups, policies and passwords, routing tables, audit and service settings, etc.

### TASKS (XX items total):

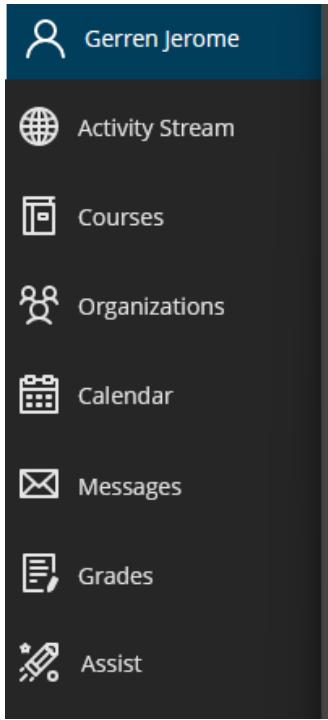
Ethical hackers and pentesters use various tools and techniques to enumerate a target network.

The following tasks will assist you in learning various enumeration techniques:

#### 1) Perform enumeration (NetBIOS) (7 tasks)

##### a) NetBIOS enumeration via Windows command line (3 tasks)

###### i) **Screengrab: Step 5** – nbtstat result



```
'nbtstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>nbtstat -a 10.10.1.19

Ethernet 2:
NodeIpAddress: [10.10.1.19] Scope Id: []

Host not found.

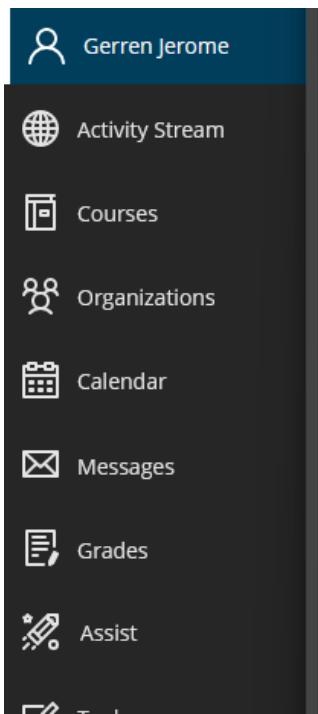
C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
NodeIpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Machine Name Table

      Name          Type        Status
-----+-----+-----+-----+
      WINDOWS11    <00>    UNIQUE    Registered
      WORKGROUP    <00>    GROUP     Registered
      WINDOWS11    <20>    UNIQUE    Registered
      WORKGROUP    <1E>    GROUP     Registered
      WORKGROUP    <1D>    UNIQUE    Registered
      @0_MS BROWSE_@<01> GROUP     Registered

MAC Address = 00-15-5D-01-80-00
```

ii) **Screengrab: Step 7** – nbtstat result


```

Administrator: Command Prompt
C:\Users\Administrator>nbtstat -c

Ethernet 2:
NodeIpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Machine Name Table
Name          Type        Status
-----        -----
WINDOWS11     <00>      UNIQUE    Registered
WORKGROUP     <00>      GROUP     Registered
WINDOWS11     <20>      UNIQUE    Registered
WORKGROUP     <1E>      GROUP     Registered
WORKGROUP     <1D>      UNIQUE    Registered
@0_MSBROWSE_0<01> GROUP     Registered

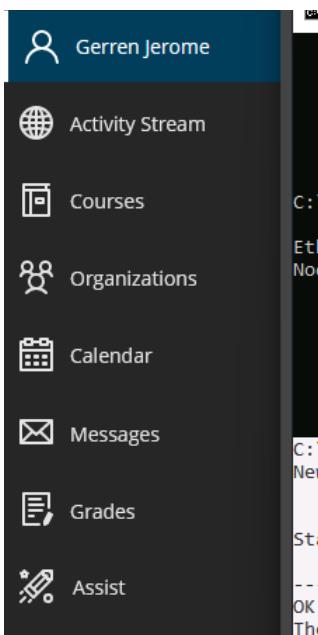
MAC Address = 00-15-5D-01-80-00

C:\Users\Administrator>nbtstat -c

Ethernet 2:
NodeIpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Cache Name Table
Name          Type        Host Address  Life [sec]
-----        -----
WINDOWS11     <20>      UNIQUE      10.10.1.11   85

```

iii) **Screengrab: Step 9** – net use result


```

Administrator: Command Prompt
C:\Users\Administrator>nbtstat -c

Ethernet 2:
NodeIpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Cache Name Table
Name          Type        Host Address  Life [sec]
-----        -----
WINDOWS11     <20>      UNIQUE      10.10.1.11   85

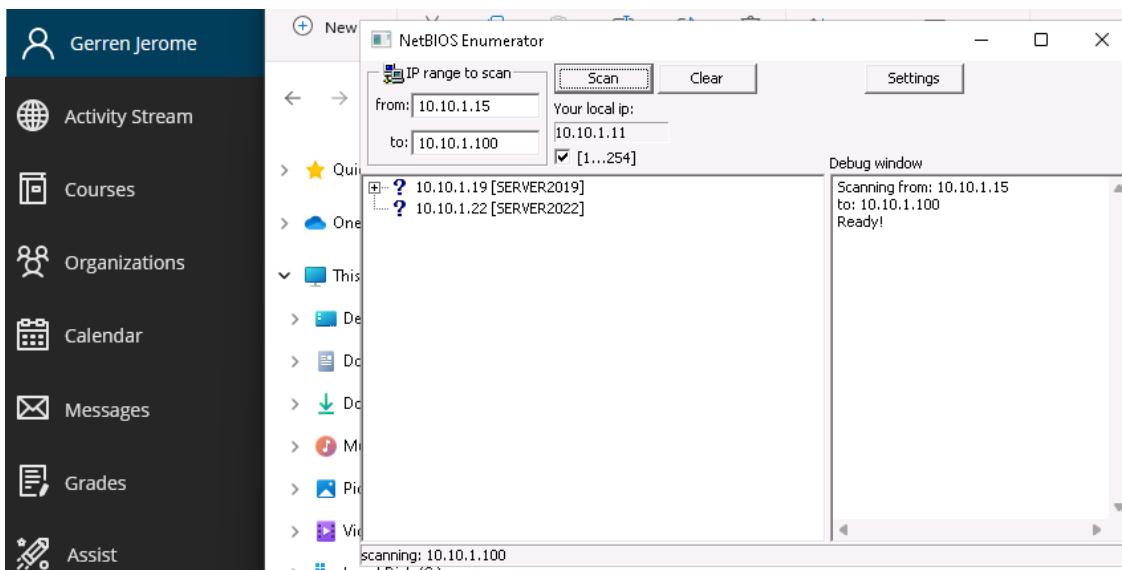
C:\Users\Administrator>net use
New connections will be remembered.

Status       Local      Remote                  Network
-----       Z:          \\WINDOWS11\CEH-Tools  Microsoft Windows Network
OK          The command completed successfully.

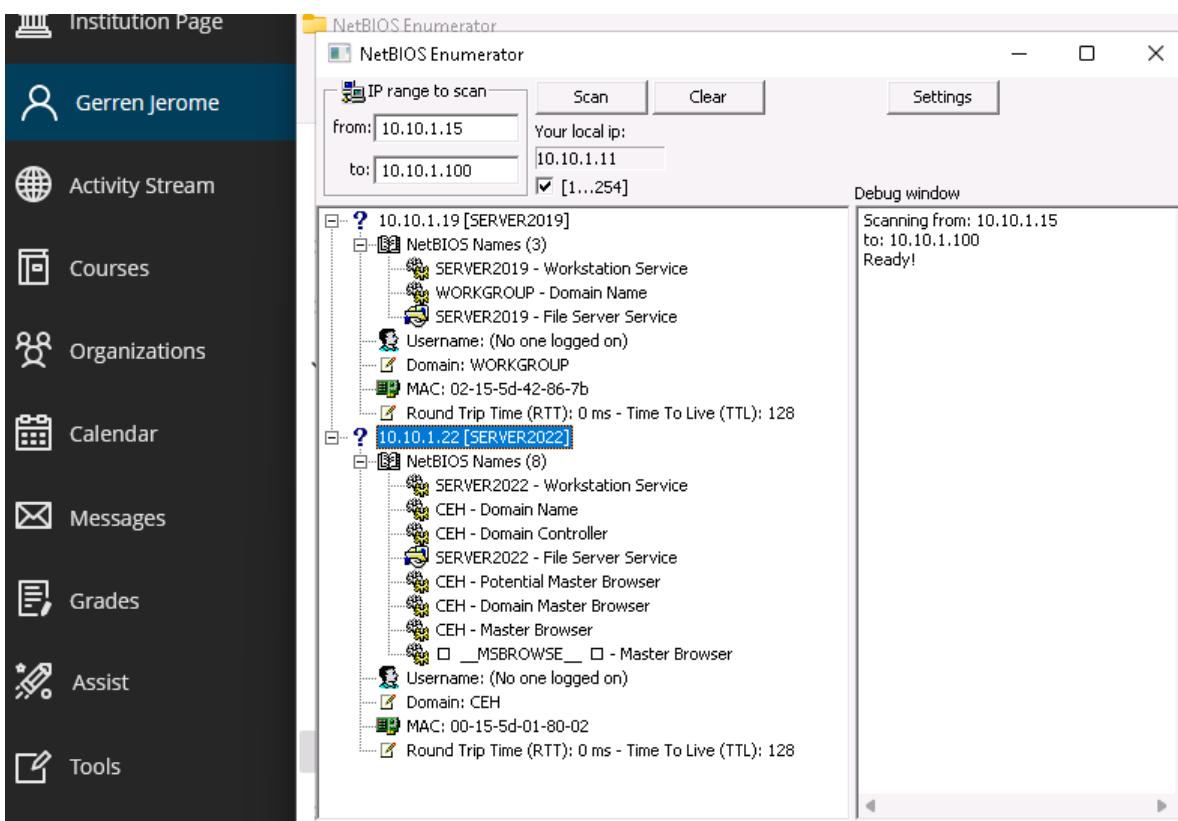
```

b) NetBIOS enumeration via NetBIOS enumerator (2 tasks)

i) **Screengrab: Step 7** – NBE result (Debug)



ii) **Screengrab: Step 8** – Expanded result



## c) NetBIOS enumeration via NSE Script (2 tasks)

i) **Screengrab: Step 7** – Nmap scan (-sV)

```

Parrot Terminal
File Edit View Search Terminal Help
Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>,
| NetBIOS MAC: 00:15:5d:01:80:02 (Microsoft)
| Names:
| SERVER2022<00> Flags: <unique><active>
| CEH<00> Flags: <group><active>
| CEH<1c> Flags: <group><active>
| SERVER2022<20> Flags: <unique><active>
| CEH<1e> Flags: <group><active>
| CEH<1b> Flags: <unique><active>
| CEH<1d> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
Statistics:
 00 15 5d 01 80 02 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
NSE: Script Post-scanning.
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18

```

ii) **Screengrab: Step 9** – Nmap scan (-sU)

```

nmap -sU -p137 --script nbstat.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
#nmap -sU -p137 --script nbstat.nse 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 10:22
EST
Nmap scan report for 10.10.1.22
Host is up (0.00047s latency).
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>,
| NetBIOS MAC: 00:15:5d:01:80:02 (Microsoft)
| Names:
| SERVER2022<00> Flags: <unique><active>
| CEH<00> Flags: <group><active>
| CEH<1c> Flags: <group><active>
| SERVER2022<20> Flags: <unique><active>
| CEH<1e> Flags: <group><active>
| CEH<1b> Flags: <unique><active>
| CEH<1d> Flags: <unique><active>
```

## 2) Perform enumeration (SNMP) (13 tasks)

## a) SNMP enumeration via snmp-check (4 tasks)

i) **Screengrab: Step 8** – Nmap scan (-sU)

```
nmap -sU -p 161 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
|_ \x01\x02__MSBROWSE_N\x02<01> Flags: <group><active>
Hacking Wireless
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
[root@parrot]~
#cd
[root@parrot]~
#sudo su
[root@parrot]~
#nmap -sU -p 161 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 10:24
EST
Nmap scan report for 10.10.1.22
Host is up (0.00055s latency).

PORT      STATE SERVICE
161/udp  open  snmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

ii) **Screengrab: Step 12** – snmp-check results (1 of 3)

```
snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot]~
#snmp-check 10.10.1.22
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)
[+] Try to connect to 10.10.1.22:161 using SNMPv1 and community 'public'

[*] System information:
[REDACTED]
Host IP address : 10.10.1.22
Hostname : Server2022.CEH.com
Description : Hardware: Intel64 Family 6
Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)
Contact : -
Location : -
Uptime snmp : 00:50:13.43
Uptime system : 00:49:52.60
System date : 2024-2-15 07:31:27.2
Domain : CEU
```

iii) **Screengrab: Step 13** – snmp-check results (2 of 3)

```

snmp-check10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

[*] Network information:
IP forwarding enabled : no
Default TTL : 128
TCP segments received : 214650
TCP segments sent : 56381
TCP segments retrans : 0
Input datagrams : 205004
Delivered datagrams : 205013
Output datagrams : 52604

[*] Network interfaces:
Interface 1 : [ up ] Software Loopback Interface 1
  Id : 1
  Mac Address : ::::
  Type : softwareLoopback
  Speed : 1073 Mbps
  MTU : 1500
  In octets : 0
  Out octets : 0

```

iv) **Screengrab: Step 14** – snmp-check results (3 of 3)

Id	Parameters	Status	Name	Path
1	attacker's Home	running	System Idle Process	
4		running	System	
96	README.license	running	Registry	
340		running	dwm.exe	
356	-k DcomLaunch -p -s LSM	running	svchost.exe	C:\Windows\system32\svchost.exe
376	[task]	running	smss.exe	
508		running	csrss.exe	
580		running	wininit.exe	
588		running	csrss.exe	

b) **SNMP enumeration via SoftPerfect Network Scanner (3 tasks)**i) **Screengrab: Step 6 – prescan config**

The screenshot shows the 'SNMP' configuration window within the SoftPerfect Network Scanner. The window title is 'SNMP' and it contains the following text: 'SNMP allows to query various information about SNMP-capable network devices and computers'. Below this is a table with the following data:

Item Name	Community/User	Version	MIB OID
<input checked="" type="checkbox"/> Host name	public	Windows b...	1.3.6.1.2.1.1.5.0
<input checked="" type="checkbox"/> Uptime	public	Windows b...	1.3.6.1.2.1.1.3.0
<input checked="" type="checkbox"/> System Description	public	Windows b...	1.3.6.1.2.1.1.1.0
<input checked="" type="checkbox"/> System Contact	public	Windows b...	1.3.6.1.2.1.1.4.0
<input checked="" type="checkbox"/> System Location	public	Windows b...	1.3.6.1.2.1.1.6.0

At the bottom of the window are buttons for 'Find...', 'New...', 'Edit...', 'Delete', and 'Mark All/None'.

ii) **Screengrab: Step 9 – SPNS scan results**

The screenshot shows the main interface of the SoftPerfect Network Scanner. The title bar says 'SoftPerfect Network Scanner'. The left sidebar shows the user profile 'Gerren Jerome' and navigation links for 'Institution Page', 'Activity Stream', 'Courses', and 'Organizations'. The main pane displays a table of scan results for IPv4 range 10.10.1.5 to 10.10.1.23. The table columns are: IP Address, MAC Address, Response Time, Host Name, Host name, Uptime, System Descri..., and System Contac... . The data in the table is as follows:

IP Address	MAC Address	Response Time	Host Name	Host name	Uptime	System Descri...	System Contac...
10.10.1.9	02-15-5D-42-8...	1 ms	ubuntu-Virtual...				
10.10.1.11	00-15-5D-01-8...	0 ms	WINDOWS11				
10.10.1.13	02-15-5D-42-8...	0 ms					
10.10.1.14	02-15-5D-42-8...	2 ms	Android.local				
10.10.1.19	02-15-5D-42-8...	0 ms	www.goodsho...	Server2019	474162 (0d 1h ...	Hardware: Intel...	
10.10.1.22	00-15-5D-01-8...	1 ms		Server2022	473180 (0d 1h ...	Hardware: Intel...	

iii) **Screengrab: Step 11 – properties of target machine (10.10.1.22)**

The screenshot shows the 'Properties' window within the SoftPerfect Network Scanner. The title bar says 'Properties'. The left sidebar shows the user profile 'Gerren Jerome' and navigation links for 'Institution Page', 'Activity Stream', 'Courses', and 'Organizations'. The main pane displays a table of properties for the target machine. The table columns are: Shared Resources, IP Address, MAC Address, Response Time, Host Name, Host name, Uptime, System Description, System Contact, and System Location. The data in the table is as follows:

Shared Resources	IP Address	MAC Address	Response Time	Host Name	Host name	Uptime	System Description	System Contact	System Location
NETLOGON, SYSVOL, Users	10.10.1.22	00-15-5D-01-80-02	1 ms	Server2022	Server2022.CEH.com	473180 (0d 1h 18m 51s)	Hardware: Intel64 Family 6 Model...		

c) **SNMP enumeration via SnmpWalk (2 tasks)**i) **Screengrab: Step 6** – scan result (snmpwalk -v1)

```

Gerren Jerome
Activity Stream
Courses
Organizations
Calendar
Messages
Grades
Assist
Tools
Sign Out

File Edit View Search Terminal Help
[root@parrot] ~]# snmpwalk -v1 -c public 10.10.1.22
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping T
BIE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (519813) 1:26:38.13
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11

```

ii) **Screengrab: Step 8** – scan result (snmpwalk -v2c)

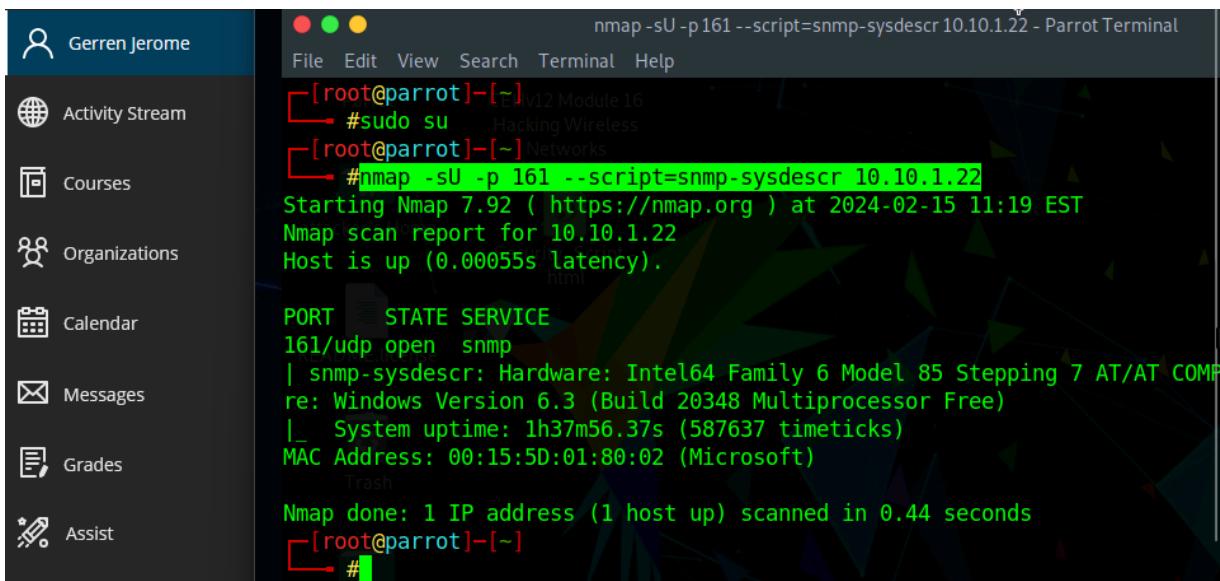
```

Gerren Jerome
Activity Stream
Courses
Organizations
Calendar
Messages
Grades
Assist
Tools
Sign Out

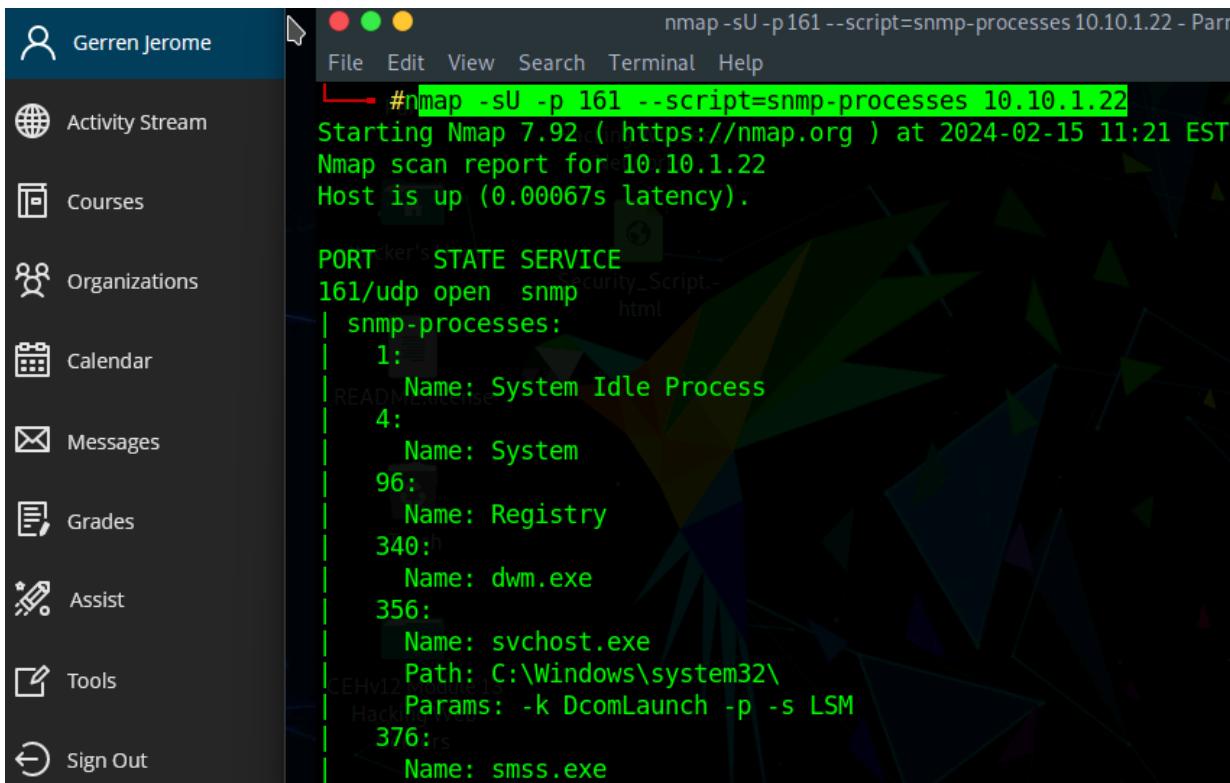
File Edit View Search Terminal Help
[root@parrot] ~]# snmpwalk -v2c -c public 10.10.1.22
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.0.1.255.161.244.172 =
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.0.1.255.177.85.25 =
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.0.1.255.215.248.11 =
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.0.1.255.235.226.126 =
[root@parrot] ~]# snmpwalk -v2c -c public 10.10.1.22
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping T
BIE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (567685) 1:34:36.85
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7

```

## d) SNMP enumeration via Nmap (4 tasks)

i) **Screengrab: Step 5** – scan result (type and description)


```
nmap -sU -p 161 --script=snmp-sysdescr 10.10.1.22 - Parrot Terminal
[+] Port 161/udp open|snmp
|_ snmp-sysdescr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMP
|_ System uptime: 1h37m56.37s (587637 timeticks)
|_ MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
[~] #
```

ii) **Screengrab: Step 7** – scan result (ports and processes)


```
nmap -sU -p 161 --script=snmp-processes 10.10.1.22 - Parrot Terminal
[+] Port 161/udp open|snmp
|_ snmp-processes:
|   1:
|     Name: System Idle Process
|   4:
|     Name: System
|   96:
|     Name: Registry
|   340:
|     Name: dwm.exe
|   356:
|     Name: svchost.exe
|     Path: C:\Windows\system32\
|     Params: -k DcomLaunch -p -s LSM
|   376:
|     Name: smss.exe
[~] #
```

iii) **Screengrab: Step 9** – scan result (applications)

The terminal window shows the command: `nmap -sU -p 161 --script=snmp-win32-software 10.10.1.22 - Parrot`. The output indicates 1 IP address scanned in 1.13 seconds. The host is up. The service at port 161 is snmp, running snmp-win32-software. The output lists various software versions installed on the host:

```
Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
[+] root@parrot:[~]
└─# nmap -sU -p 161 --script=snmp-win32-software 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:26 EST
Nmap scan report for 10.10.1.22
Host is up (0.0011s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-win32-software:
|_ Adobe Acrobat DC (64-bit); 2022-02-01T04:01:22
|_ Adobe Refresh Manager; 2022-11-01T03:59:58
|_ Browser for SQL Server 2017; 2022-05-03T21:26:42
|_ Google Chrome; 2022-05-08T23:01:56
|_ Java 8 Update 321 (64-bit); 2022-02-03T04:36:12
|_ Java Auto Updater; 2022-02-03T04:36:36
|_ Microsoft Edge; 2022-11-01T03:59:36
|_ Microsoft Edge Update; 2022-11-01T03:53:58
|_ Microsoft ODBC Driver 13 for SQL Server; 2022-05-03T21:26:36
|_ Microsoft SQL Server 2012 Native Client ; 2022-05-03T21:26:20
|_ Microsoft SQL Server 2017 (64-bit); 2022-05-03T21:26:14
|_ Microsoft SQL Server 2017 (64-bit); 2022-05-03T21:26:14
```

iv) **Screengrab: Step 11** – scan result (interfaces)

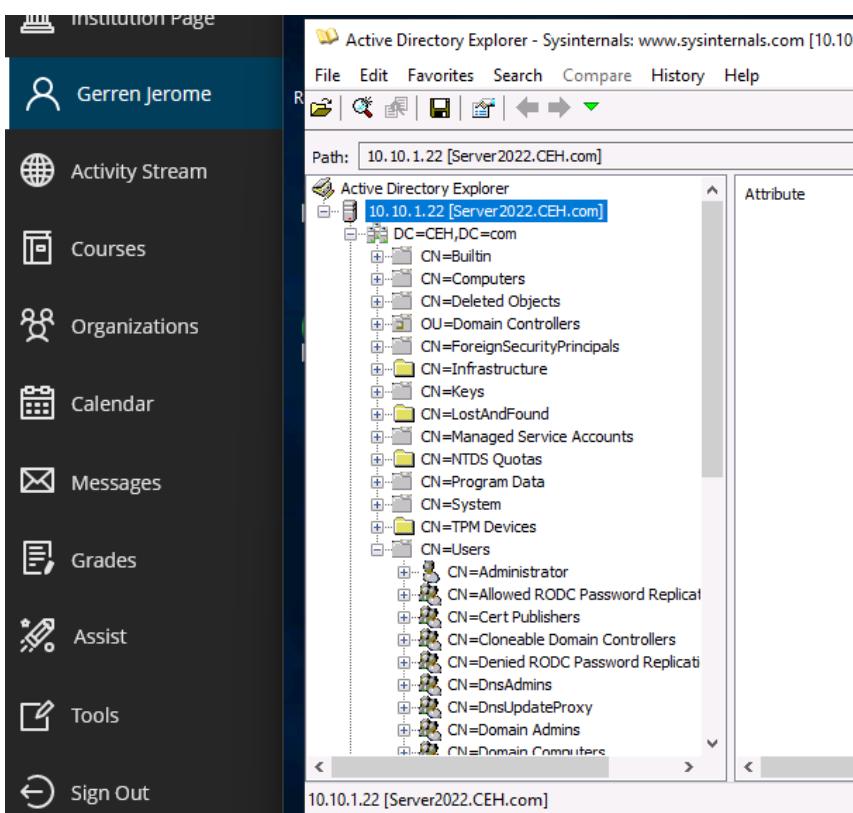
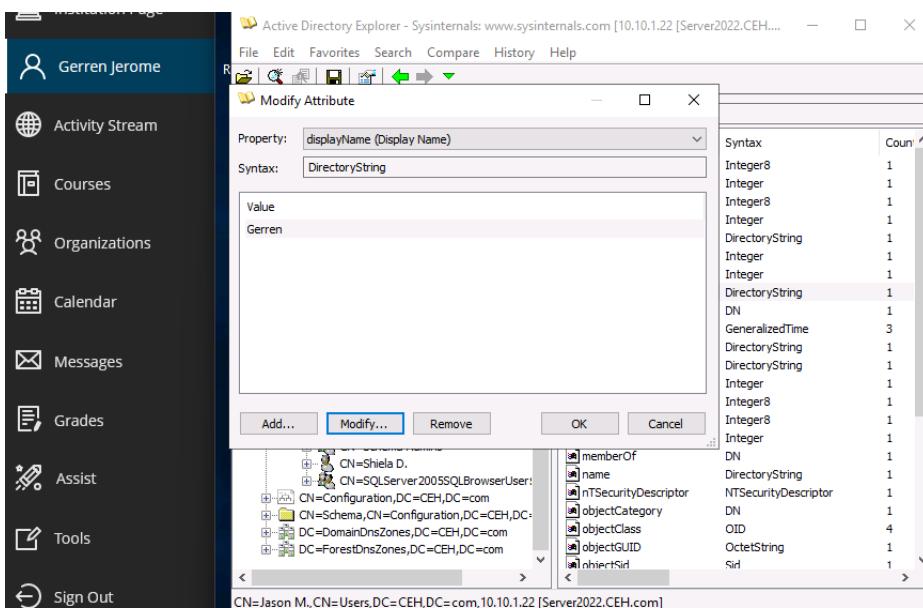
The terminal window shows the command: `nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22 - Parrot`. The output indicates 1 IP address scanned in 0.71 seconds. The host is up. The service at port 161 is snmp, running snmp-interfaces. The output lists the network interfaces and their details:

```
nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22 - Parrot
File Edit View Search Terminal Help
nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
[+] root@parrot:[~]
└─# nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:28 EST
Nmap scan report for 10.10.1.22
Host is up (0.00060s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-interfaces:
|_ Software Loopback Interface 1\x00
|   IP address: 127.0.0.1 Netmask: 255.0.0.0
|   Type: softwareLoopback Speed: 1 Gbps
|   Status: up
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|_ Microsoft Gto4 Adapter\x00
|   Type: tunnel Speed: 0 Kbps
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|_ WAN Miniport (IKEv2)\x00
|   Type: tunnel Speed: 0 Kbps
|   Status: down
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|_ WAN Miniport (BPTP)\x00
```

## 3) Perform enumeration (LDAP) (11 tasks)

## a) Perform LDAP enumeration using Active Directory Explorer (AD Explorer) (2 tasks)

i) **Screengrab: Step 7** – Navigating ADExplorerii) **Screengrab: Step 10** – user attribute modification

## b) Perform LDAP enumeration using Python and Nmap (6 tasks)

i) **Screengrab: Step 6** – scan result (Nmap -sU)

```
nmap -sU -p389 10.10.1.22 - Parrot Terminal
[root@parrot] ~
# nmap -sU -p389 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:37 EST
Nmap scan report for 10.10.1.22
Host is up (0.00056s latency).
          attacker's Home
PORT      STATE SERVICE
389/udp  open   ldap
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

ii) **Screengrab: Step 9** – result (Nmap LDAP bruteforce)

```
nmap -p 389 --script ldap-brute --script-args ldap.base="cn=users,dc=CEH,dc=com" 10.10.1.22 - Parrot Terminal
[x]-[root@parrot] ~
# nmap -p 389 --script ldap-brute --script-args ldap.base='cn=users,dc=CEH,dc=com' 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:40 EST
Nmap scan report for 10.10.1.22
Host is up (0.00065s latency).

PORT      STATE SERVICE
389/tcp  open   ldap
| ldap-brute:
|   ch=root,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=admin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=administrator,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=webadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=sysadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=netadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=guest,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=user,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=web,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=test,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
MAC Address: 00:15:5D:01:80:02 (Microsoft)
```

iii) **Screengrab: Step 15** – import ldap3 into Python

```
Parrot File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[attacker@parrot] ~
#python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information
>>> import ldap3
```

iv) **Screengrab: Step 21** – gain naming context

The screenshot shows a terminal window titled "python3 - Parrot Terminal". The user is running a Python script to exploit an LDAP server. The terminal output is as follows:

```
[root@parrot]~[/home/attacker]
└─#python3
      Hacking Wireless
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>> connection=ldap3.Connection(server)
>>> connection.bind()
True
>>> server.info
DSA info (from DSE):
Supported LDAP versions: 3, 2
Naming contexts:
DC=CEH,DC=com
CN=Configuration,DC=CEH,DC=com
CN=Schema,CN=Configuration,DC=CEH,DC=com
DC=DomainDnsZones,DC=CEH,DC=com
DC=ForestDnsZones,DC=CEH,DC=com
Supported controls:
1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
1.2.840.113556.1.4.1341 - PAGED - Control - MICROSOFT
```

v) **Screengrab: Step 23** – retrieve directory objects

vi) **Screengrab: Step 25** – result (LDAP dump)

```
python3 - Parrot Terminal
objectGUID: b'\x14\x91\x11)\x1f\xd5\x84E\x87\x a9\xd6Y\x e5\x a1\x01\x86'
objectSid: b'\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00\x00\xb8_.|\x e
\x87\x a0z9\xb0W)\n\x00\x00'
sAMAccountName: SQLServer2005SQLBrowserUser$SERVER2022
sAMAccountType: 536870912
uSNChanged: 41181
uSNCreated: 41178
whenChanged: 20220504042648.0Z
whenCreated: 20220504042648.0Z
]
>>> connection.entries
[DN: CN=Guest,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2024-02-15
7:00.441661
, DN: CN=SERVER2022,OU=Domain Controllers,DC=CEH,DC=com - STATUS: Read - RE
ME: 2024-02-15T11:57:00.441722
, DN: CN=Martin J.,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2024-
T11:57:00.441765
, DN: CN=Shiela D.,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2024-
T11:57:00.441805
]
```

c) Perform LDAP enumeration using ldapsearch (3 tasks)

- i) **Screengrab: Step 4** – gain naming context via ldapsearch

The terminal window displays the output of an LDAP search command:

```
ldapsearch -h 10.10.1.22 -x -s base naming contexts - Par  
File Edit View Search Terminal Help  
[attacker@parrot]~ [Module 16]  
$ sudo su  
[sudo] password for attacker:  
[root@parrot]~ [/home/attacker]  
# ldapsearch -h 10.10.1.22 -x -s base naming contexts  
# extended LDIF  
#  
# LDAPv3  
# base <> (default) with scope baseObject  
# filter: (objectclass=*)  
# requesting: naming contexts  
#  
# dn: Trash  
#  
# search result  
search: 2  
result: 0 Success  
# numResponses: 2  
# numEntries: 1
```

ii) **Screengrab: Step 5** – more information about primary domain

```

Gerren Jerome                               ldapsearch-h 10.10.1.22 -x -b "DC=CEH,DC=com"
File Edit View Search Terminal Help
# numEntries: 1  CEHv12 Module 16
[root@parrot]~[/home/attacker]
└─ #ldapsearch -h 10.10.1.22 -x -b "DC=CEH,DC=com"
# extended LDIF
#
# LDAPv3
# base <DC=CEH,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
# README.license

# CEH.com
dn: DC=CEH,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=CEH,DC=com
instanceType: 5
whenCreated: 20220201120107.0Z
whenChanged: 20240215134123.0Z
subRefs: DC=ForestDnsZones,DC=CEH,DC=com
subRefs: DC=DomainDnsZones,DC=CEH,DC=com
subRefs: CN=Configuration,DC=CEH,DC=com

```

iii) **Screengrab: Step 6** – retrieve info about objects in directory tree

```

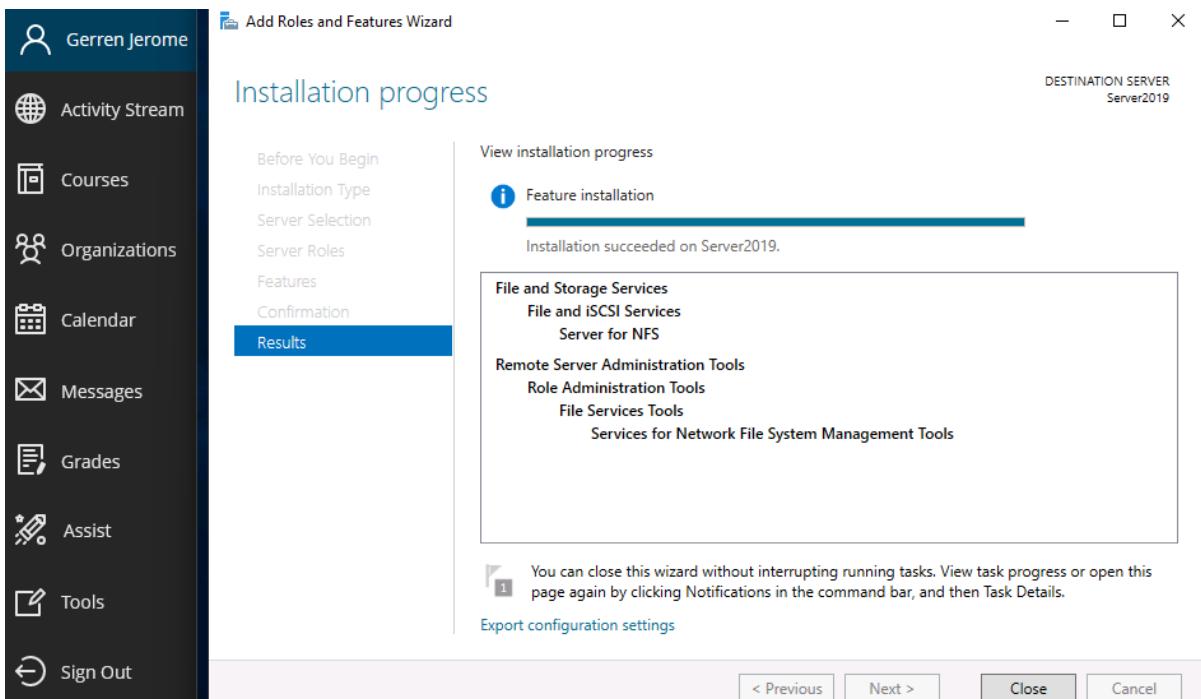
Gerren Jerome                               ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectclass=*" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─ #ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectclass=*" - Parrot Terminal
# extended LDIF
#
# LDAPv3
# base <DC=CEH,DC=com> with scope subtree
# filter: objectclass=*
# requesting: ALL
#
# README.license
# CEH.com
dn: DC=CEH,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=CEH,DC=com
instanceType: 5
whenCreated: 20220201120107.0Z
whenChanged: 20240215134123.0Z
subRefs: DC=ForestDnsZones,DC=CEH,DC=com
subRefs: DC=DomainDnsZones,DC=CEH,DC=com
subRefs: CN=Configuration,DC=CEH,DC=com

```

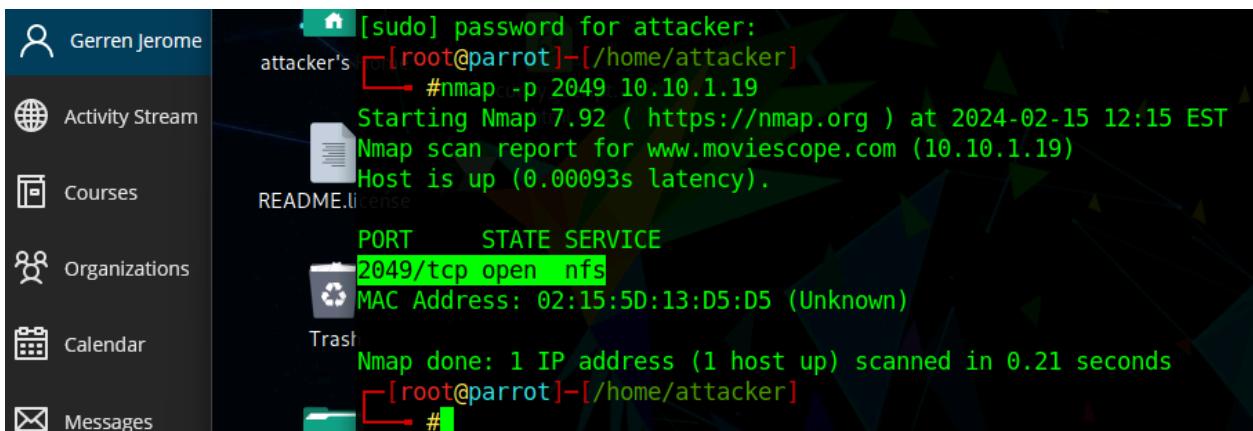
4) Perform enumeration (NFS) (4 tasks)

a) Perform NFS enumeration using RPCScan and SuperEnum (4 tasks)

i) **Screengrab: Step 6** – confirm install/enable of NFS service in Windows



ii) **Screengrab: Step 13** – scan result (NFS running?)



iii) **Screengrab: Step 18** – scan result (SuperEnum)

```

Testing for 10.10.1.19: 1801
15-02-2024/10.10.1.19/open_ports/1801/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.1.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found
15-02-2024/10.10.1.19/open_ports/2049/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2103
15-02-2024/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2105
15-02-2024/10.10.1.19/open_ports/2105/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2107
15-02-2024/10.10.1.19/open_ports/2107/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 25
Testing for 10.10.1.19: 25, Tool: nmap_smtp-commands
Testing for 10.10.1.19: 25, Tool: nmap_smtp-enum-users
Testing for 10.10.1.19: 25, Tool: nmap_smtp-open-relay

```

iv) **Screengrab: Step 23** – scan result (RPCScan)

Gerren Jerome	portmapper (100000)	4	udp	111
Gerren Jerome	portmapper (100000)	2	tcp	111
Gerren Jerome	portmapper (100000)	3	tcp	111
Gerren Jerome	portmapper (100000)	4	tcp	111
Activity Stream	nfs (100003)	2	tcp	2049
Activity Stream	nfs (100003)	3	tcp	2049
Activity Stream	nfs (100003)	2	udp	2049
Activity Stream	nfs (100003)	3	udp	2049
Activity Stream	nfs (100003)	4	tcp	2049
Courses	mount demon (100005)	1	tcp	2049
Courses	mount demon (100005)	2	tcp	2049
Courses	mount demon (100005)	3	tcp	2049
Courses	mount demon (100005)	1	udp	2049
Courses	mount demon (100005)	2	udp	2049
Courses	mount demon (100005)	3	udp	2049
Organizations	network lock manager (100021)	1	tcp	2049
Organizations	network lock manager (100021)	2	tcp	2049
Organizations	network lock manager (100021)	3	tcp	2049
Organizations	network lock manager (100021)	4	tcp	2049
Organizations	network lock manager (100021)	1	udp	2049
Organizations	network lock manager (100021)	2	udp	2049
Organizations	network lock manager (100021)	3	udp	2049
Organizations	network lock manager (100021)	4	udp	2049
Organizations	status monitor 2 (100024)	1	tcp	2049

## 5) Perform enumeration (DNS) (8 tasks)

## a) Perform DNS enumeration using zone transfer (4 tasks)

i) **Screengrab: Step 7** – scan result (dig ns [www.certifiedhacker.com](http://www.certifiedhacker.com))

```

; <>> DiG 9.16.22-Debian <>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 59344
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com. IN NS
;www.certifiedhacker.com. IN CNAME certifiedhacker.com.
certifiedhacker.com. 21600 IN NS ns2.bluehost.com.
certifiedhacker.com. 21600 IN NS ns1.bluehost.com.
;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 21600 IN A 162.241.216.11
;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Feb 15 12:32:50 EST 2024
;; MSG SIZE rcvd: 111

```

ii) **Screengrab: Step 9** – scan result (dig transfer failed?)

```

; <>> DiG 9.16.22-Debian <>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.

```

iii) **Screengrab: Step 17** – scan result (nslookup (interactive mode) – certifiedhacker)

The screenshot shows a Windows Command Prompt window titled "Command Prompt - nslookup". The title bar also displays "Microsoft Windows [Version 10.0.22000.469]" and "(c) Microsoft Corporation. All rights reserved." The command entered was "C:\Users\Admin>nslookup". The output shows the following details:

```
C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024021500
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
```

iv) **Screengrab: Step 19** – scan result (nslookup (interactive mode) – bluehost)

The screenshot shows a Windows Command Prompt window titled "Command Prompt - nslookup". The title bar also displays "Microsoft Windows [Version 10.0.22000.469]" and "(c) Microsoft Corporation. All rights reserved." The command entered was "C:\Users\Admin>nslookup". The output shows the following details:

```
C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024021500
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)

> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
```

## b) Perform DNS enumeration using DNSSEC zone walking (1 task)

i) **Screengrab: Step 8** – result (dnsrecon – certifiedhacker)

```

Institution Page
Gerren Jerome
Activity Stream
Courses
Organizations
Calendar
Messages
Grades
Assist
Tools
Sign Out

[+] Against all TLDs registered in IANA.
[+] Networks zonewalk: Perform a DNSSEC zone walk using NSEC records.
[+] [root@parrot]~/home/attacker/dnsrecon]
[+] ./dnsrecon.py -d www.certifiedhacker.com -z
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*] SOA ns1.bluehost.com 162.159.24.80
[*] NS ns2.bluehost.com 162.159.25.175
[*] NS ns1.bluehost.com 162.159.24.80
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[+] 2 records found
[+] [root@parrot]~/home/attacker/dnsrecon]
[+] # Module14

```

## c) Perform DNS enumeration using Nmap (3 tasks)

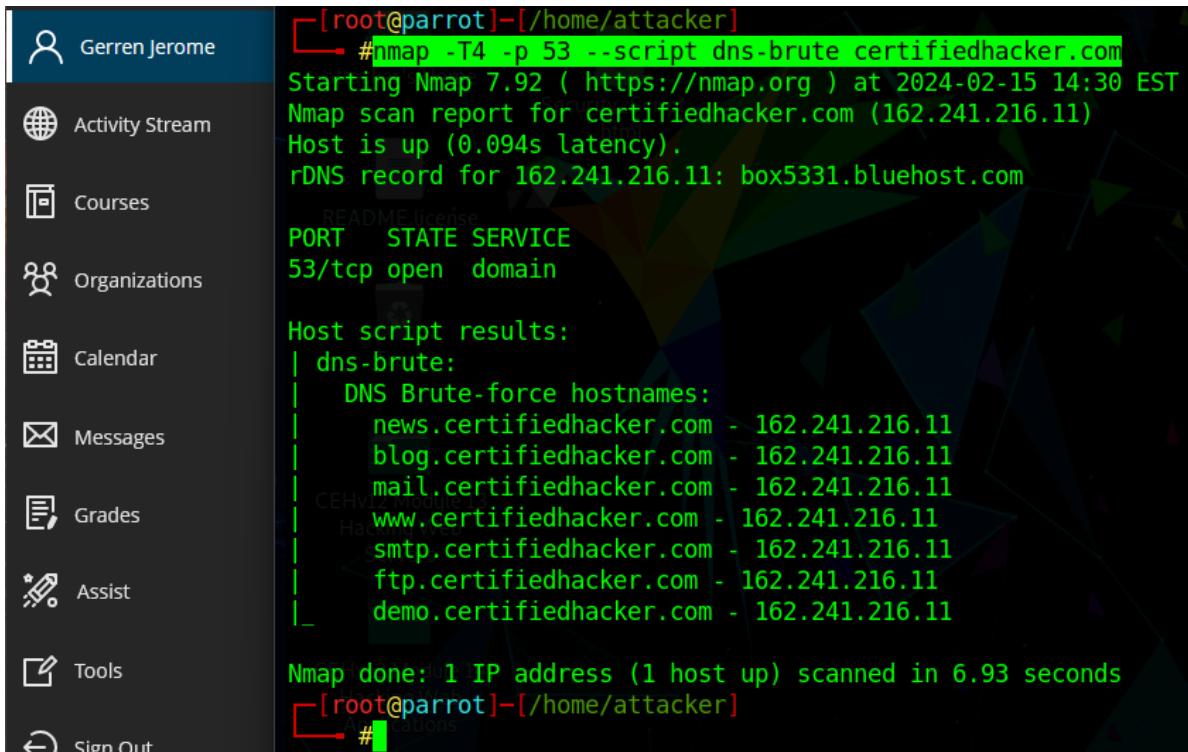
i) **Screengrab: Step 5** – scan result (nmap service discovery)

```

Institution Page
Gerren Jerome
Activity Stream
Courses
Organizations
Calendar
Messages
Grades
Assist
Tools
Sign Out

● ● ● nmap --script=broadcast-dns-service-discovery certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[+] [root@parrot]~/home/attacker]
[+] #nmap --script=broadcast-dns-service-discovery certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 14:27 EST
Pre-scan script results:
| broadcast-dns-service-discovery:
|_ 224.0.0.251
|_ 5555/tcp adb
|   Address=10.10.1.14 fe80::7e2a:9357:a80e:3ble
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.099s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    filtered  smtp
26/tcp    open      rsftp
53/tcp    open      domain
80/tcp    open      http
110/tcp   open      pop3
143/tcp   open      imap
443/tcp   open      https
465/tcp   filtered  smtps
587/tcp   open      submission

```

ii) **Screengrab: Step 7** – scan result (associated subdomains)


The screenshot shows a terminal window titled '[root@parrot] - [/home/attacker]' displaying the output of an Nmap scan. The command used was '#nmap -T4 -p 53 --script dns-brute certifiedhacker.com'. The output shows the host is up with 0.094s latency, and a rDNS record for 162.241.216.11 is found to be box5331.bluehost.com. The scan results for port 53/tcp show it is open and the service is domain. Host script results for the dns-brute script are shown, listing various subdomains of certifiedhacker.com that resolve to 162.241.216.11. The final message indicates the scan took 6.93 seconds.

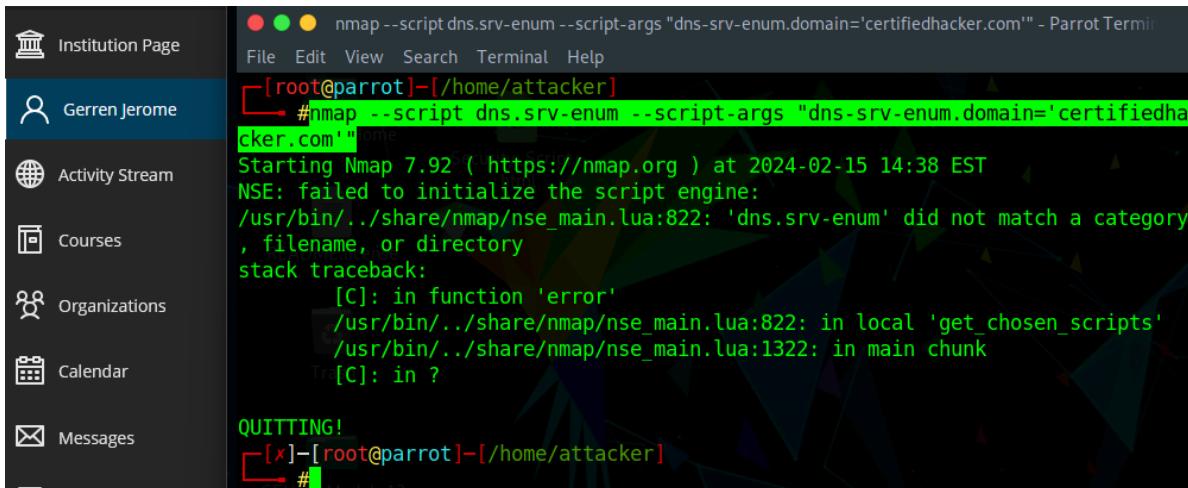
```
[root@parrot] - [/home/attacker]
#nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 14:30 EST
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.094s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
53/tcp    open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     demo.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds

```

iii) **Screengrab: Step 9** – scan result (SRV records)


The screenshot shows a terminal window titled '[root@parrot] - [/home/attacker]' displaying the output of an Nmap scan for SRV records. The command used was '#nmap --script dns.srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"'. The output shows that the script failed to initialize due to a mismatch between the script name and the category, filename, or directory. It then provides a stack traceback and a quit message. The terminal prompt is '[x]-[root@parrot] - [/home/attacker]'.

```
● ● ● nmap --script dns.srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] - [/home/attacker]
#nmap --script dns.srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 14:38 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:822: 'dns.srv-enum' did not match a category
, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/bin/../share/nmap/nse_main.lua:822: in local 'get_chosen_scripts'
/usr/bin/../share/nmap/nse_main.lua:1322: in main chunk
[C]: in ?

QUITTING!
[x]-[root@parrot] - [/home/attacker]
```

6) Perform enumeration (SMTP) (2 tasks)

a) Perform SMTP enumeration using Nmap (2 tasks)

i) **Screengrab: Step 5** – list all mail users

```
nmap -p 25 --script=smtp-enum-users 10.10.1.19 - Parrot Terminal
[x]-[root@parrot]-[/home/attacker]
└─# nmap -p 25 --script=smtp-enum-users 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 14:40 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00078s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_ smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|   test
MAC Address: 02:15:5D:13:D5:D5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
[root@parrot]-[/home/attacker]
└─#
```

ii) **Screengrab: Step 7** – list open SMTP relays

```
guest
user
web
test
MAC Address: 02:15:5D:13:D5:D5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
[root@parrot]-[/home/attacker]
└─# nmap -p 25 --script=smtp-open-relay 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 14:41 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00085s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_ smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:13:D5:D5 (Unknown)

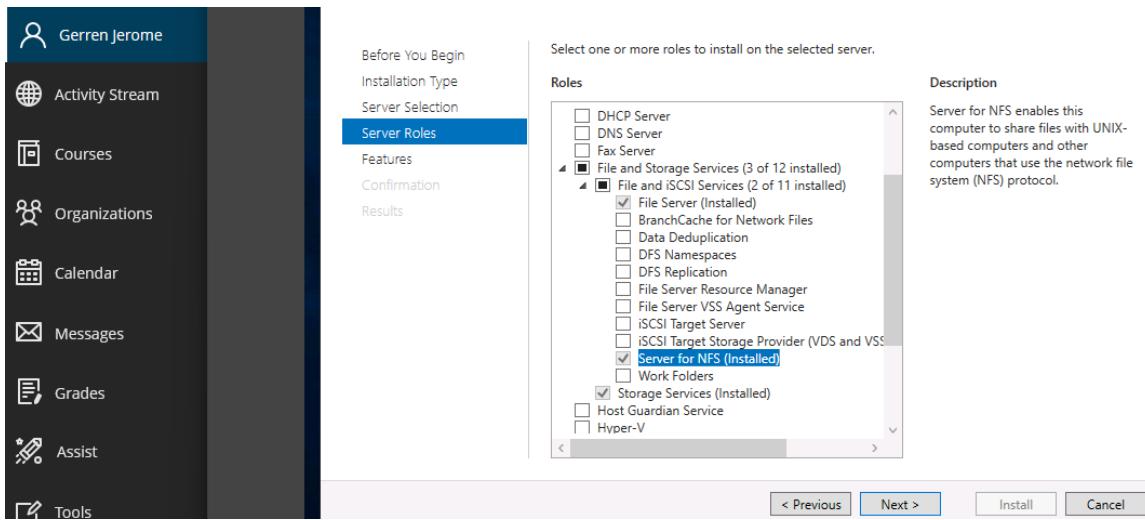
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
[root@parrot]-[/home/attacker]
└─#
```

## Gerren Jerome - Enumeration

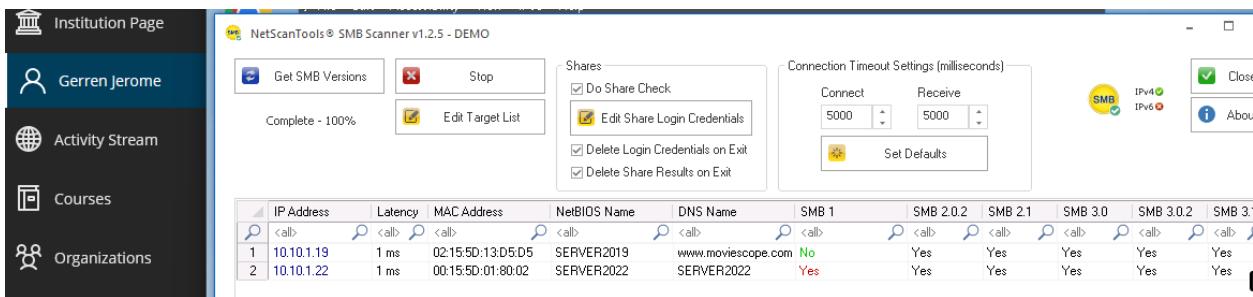
### 7) Perform enumeration (RPC, SMB, and FTP) (8 tasks)

#### a) Perform SMB and RPC enumeration using NetScanTools Pro (3 tasks)

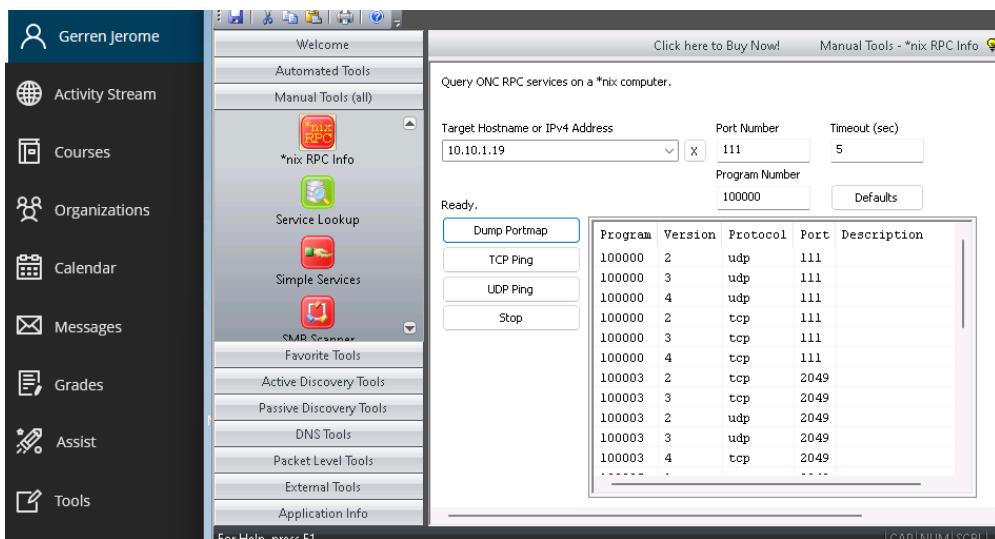
##### i) **Screengrab: Step 6** – confirm install/enable NFS services



##### ii) **Screengrab: Step 22** – SMB scanner results



##### iii) **Screengrab: Step 28** – portmap dump (WIN\_SVR\_19)



## b) Perform RPC, SMB, and FTP enumeration using Nmap (5 tasks)

i) **Screengrab: Step 10** – confirm addition of CEH.com FTP site to IIS

The screenshot shows the Windows Server 2019 IIS Manager interface. On the left, there's a navigation bar with options like 'Activity Stream', 'Courses', and 'Organizations'. The main area is titled 'Connections' and shows the 'Start Page' and 'SERVER2019 (SERVER2019\Administrator)' node expanded. Under 'Application Pools', the 'Default Web Site' pool is selected, and its 'Sites' section contains four entries: 'CEH.com', 'Default Web Site', 'GoodShopping', and 'MovieScope'. To the right, there's a separate window titled 'Sites' with a table listing the same four sites along with their IDs, statuses, and binding details.

ii) **Screengrab: Step 18** – nmap scan (Port 21 - FTP)

```

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
[root@parrot]~ 
└─# cd /home/attacker
[root@parrot]~ 
└─# sudo su
[root@parrot]~ 
└─# cd
[root@parrot]~ 
└─# nmap -p 21 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 15:06 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00089s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 02:15:5D:13:D5:D5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
[root@parrot]~ 
└─#

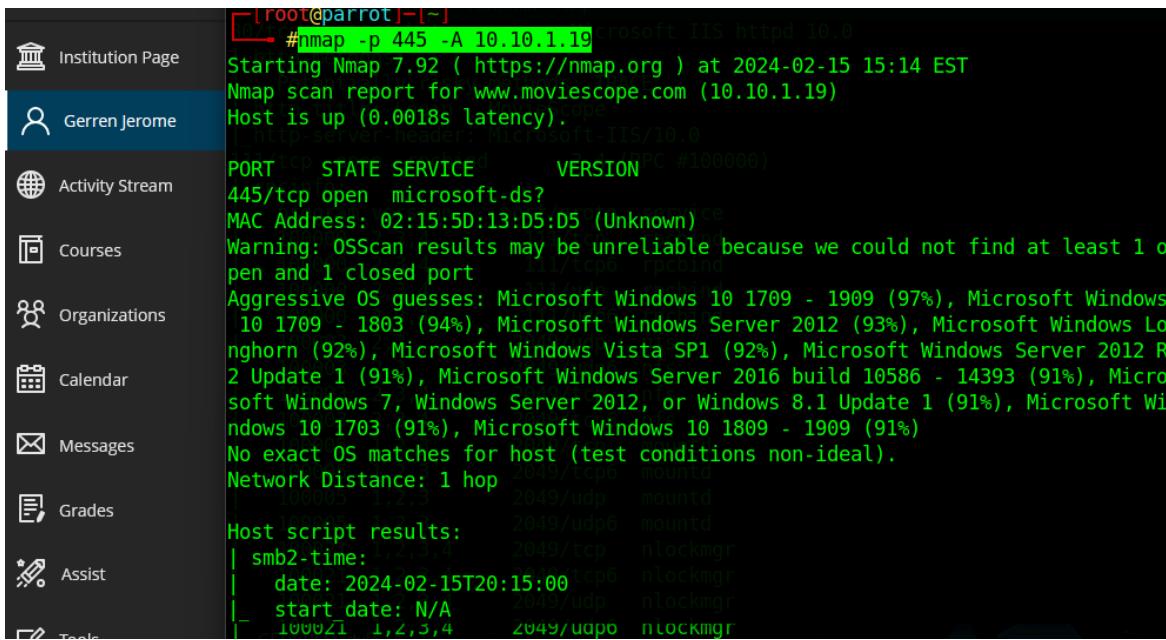
```

iii) **Screengrab: Step 20** – nmap scan (other services and ports)

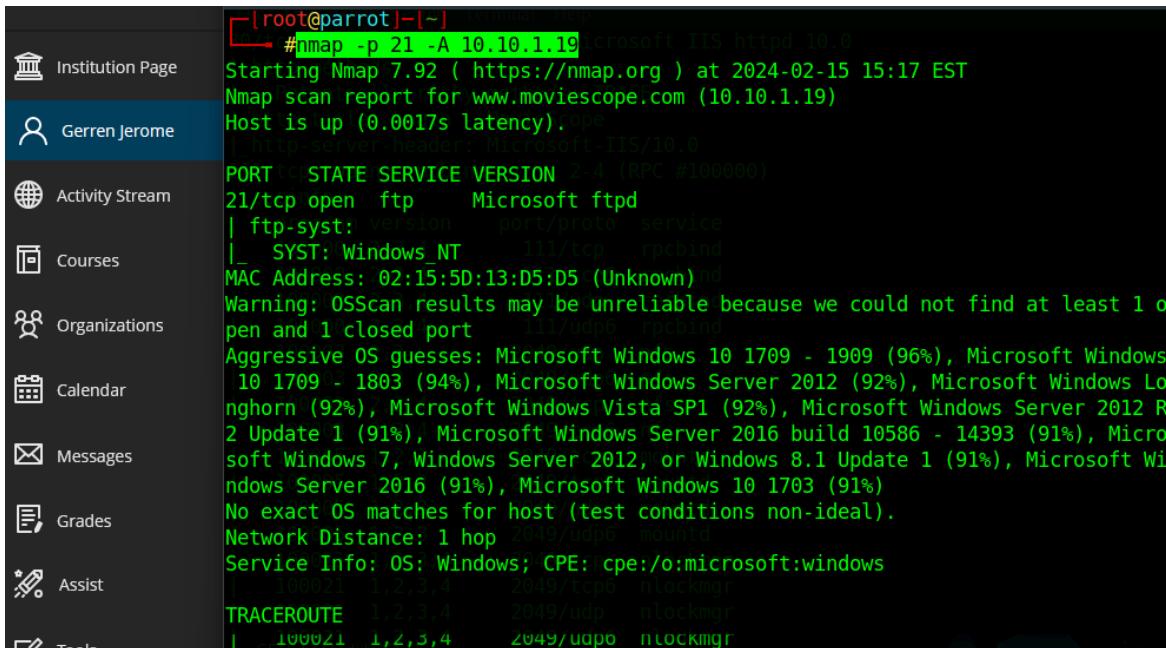
```

[root@parrot]~ 
└─# nmap -T4 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 15:08 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0021s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
|_ftp-syst:
|_SYST: Windows NT
25/tcp    open  smtp             Microsoft ESMTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
80/tcp    open  http             Microsoft IIS httpd 10.0
| http-methods:
|_Potentially risky methods: TRACE
| http-title: Login - MovieScope
| http-server-header: Microsoft-IIS/10.0
111/tcp   open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|_program version  port/proto  service
| 100000  2,3,4        111/tcp  rpcbind

```

iv) **Screengrab: Step 25** – nmap scan (Port 445 – SMB)


```
[root@parrot] ~
└─# nmap -p 445 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 15:14 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0018s latency).
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
MAC Address: 02:15:5D:13:D5:D5 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
|_ 100005 1,2,3,4 2049/udp  mountd
|_ 100005 1,2,3,4 2049/udp  mountd
Host script results:
| smb2-time:
|   | date: 2024-02-15T20:15:00
|   | start date: N/A
|_ 100001 1,2,3,4 2049/udp  nlockmgr
|_ 100001 1,2,3,4 2049/udp  nlockmgr
```

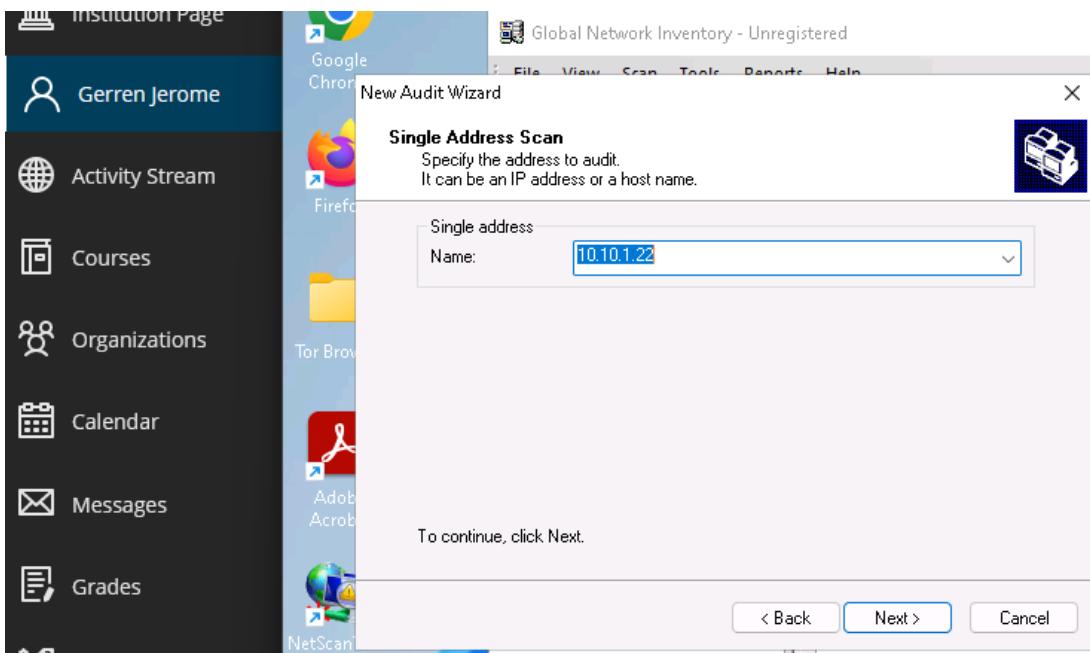
v) **Screengrab: Step 28** – nmap scan (Port 21 + traceroute)


```
[root@parrot] ~
└─# nmap -p 21 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 15:17 EST
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0017s latency).
|_ http-server-header: Microsoft-IIS/10.0
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
|_ ftp-syst: version  port/proto service
|_ SYST: Windows NT 113/tcp  rpcbind
MAC Address: 02:15:5D:13:D5:D5 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 2016 (91%), Microsoft Windows 10 1703 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
|_ 2049/udp  mountd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
|_ 100021 1,2,3,4 2049/tcp  nlockmgr
TRACEROUTE
|_ 100021 1,2,3,4 2049/udp  nlockmgr
|_ 100021 1,2,3,4 2049/udp  nlockmgr
```

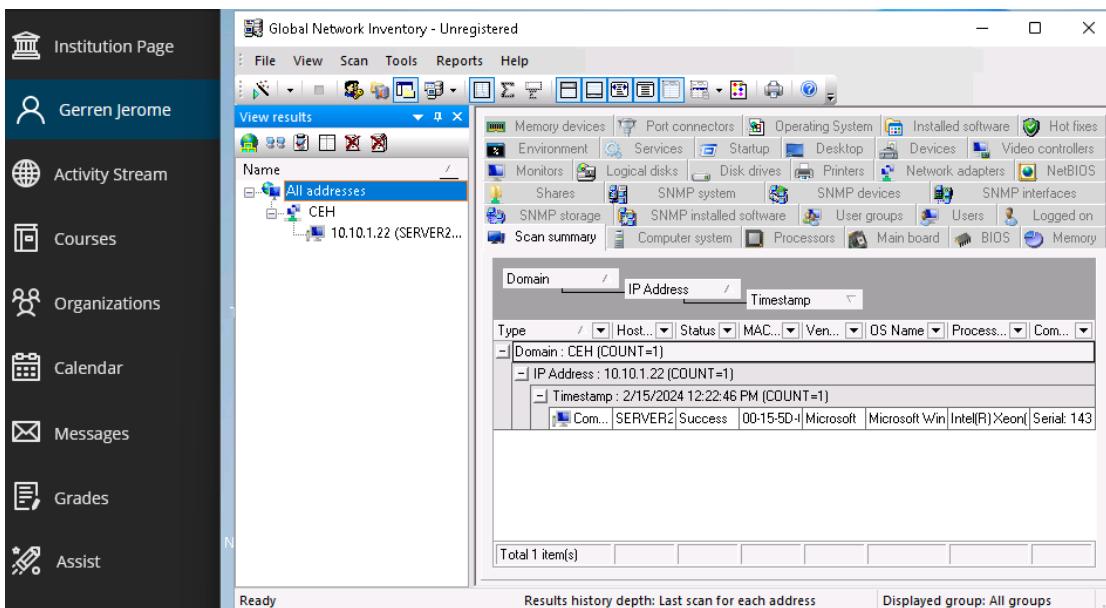
8) Perform enumeration using various enumeration tools (XX tasks)

a) Enumerate information using Global Network Inventory (6 tasks)

i) **Screengrab: Step 6** – confirm settings (GNI single address scan)



ii) **Screengrab: Step 10** – Scan summary (GNI)



iii) **Screengrab: Step 12 – GNI Scan Result (Operating System)**

The screenshot shows the GNI interface with the operating system results for the host 10.10.1.22 (SERVER2...). The results table displays the following information:

Type	Host	Name	Serial No.	Cd Key
Domain	CEH	10.10.1.22 (COUNT=1)		
IP Address	10.10.1.22 (COUNT=1)			
Timestamp	2/15/2024 12:22:46 PM (COUNT=1)			
WINNT	SERVER Microsoft Windows	20348	00454-20441-6	Windows

Total 1 item(s)

iv) **Screengrab: Step 15 – GNI Scan Result (User Groups)**

The screenshot shows the GNI interface with user group results for the host 10.10.1.22 (SERVER2...). The results table displays the following information:

Name	Type
Host Name : SERVER2022 (COUNT=12)	
Timestamp : 2/15/2024 12:22:46 PM (COUNT=12)	
Group : Administrators (COUNT=4)	
CEH\Administrator	User account
CEH\Domain Admins	Global group account
CEH\Enterprise Admins	Global group account
CEH\jason	User account
Group : Guests (COUNT=2)	
CEH\Domain Guests	Global group account
CEH\Guest	User account
Group : IIS_IUSRS (COUNT=1)	

Total 12 item(s)

v) **Screengrab: Step 17 – GNI Scan Result (Services)**

The screenshot shows the GNI interface with service results for the host 10.10.1.22 (SERVER2...). The results table displays the following information:

Name	Start T...	State	File
Domain : CEH (COUNT=234)			
Host Name : SERVER2022 (COUNT=234)			
Timestamp : 2/15/2024 12:22:46 PM (COUNT=234)			
Active Directory Domain Services	Automatic	Running	C:\Windows\System32\lsass.exe
Active Directory Web Services	Automatic	Running	C:\Windows\ADWS\Microsoft\ActiveDirectory
ActiveX Installer (AxinstSV)	Disabled	Stopped	C:\Windows\system32\svchost.exe + Axinst
Adobe Acrobat Update Service	Automatic	Running	"C:\Program Files (x86)\Common Files\Adobe
AllJoyn Router Service	Manual	Stopped	C:\Windows\system32\svchost.exe + Local
App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe + AppR
Application Host Helper Service	Automatic	Running	C:\Windows\system32\svchost.exe + appho
Application Identity	Manual	Stopped	C:\Windows\system32\svchost.exe + Local
Application Information	Manual	Stopped	C:\Windows\system32\svchost.exe + netsvc
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe

Total 234 item(s)

vi) **Screengrab: Step 19** – GNI Scan Result (Shares)

The screenshot shows the GNI Scan interface with the following details:

- Scan summary:** All addresses, CEH, 10.10.1.22 (SERVER2022).
- Shares:**

Type	Name	Path	File System	Size, GB	Free Space, GB
Special share	C\$	C:\	NTFS	99.39	78.63
Special share	ADMIN\$		NTFS	78.63	0.00
Special share	IPC\$		NTFS	0.00	0.00
Disk drive	NETLOGON		NTFS	0.00	0.00
Disk drive	SYSVOL		NTFS	0.00	0.00
Disk drive	Users		NTFS	99.39	78.63

## b) Enumerate network resources using Advanced IP Scanner (1 task)

i) **Screengrab: Step 6** – Advanced IP Scanner results

The screenshot shows the Advanced IP Scanner interface with the following details:

- Scan:** 10.10.1.5-10.10.1.23.
- Results:**

Status	Name	IP	Manufacturer	MAC address
Up	10.10.1.9	10.10.1.9	Microsoft Corporation	02:15:5D:13:D5:D6
Up	Windows11	10.10.1.11	Microsoft Corporation	00:15:5D:01:80:00
Up	10.10.1.13	10.10.1.13		02:15:5D:13:D5:D7
Up	10.10.1.14	10.10.1.14		02:15:5D:13:D5:D8
Up	www.goodshopping.com	10.10.1.19		02:15:5D:13:D5:D5
Up	Server2022	10.10.1.22	Microsoft Corporation	00:15:5D:01:80:02

## c) Enumerate information from Windows and Samba hosts using Enum4linux (X tasks)

i) **Screengrab: Step 9** – NetBIOS scan (10.10.1.22)

The screenshot shows the output of the NetBIOS scan for host 10.10.1.22:

```

=====
[+] Got domain/workgroup name: CEH
=====
| Nbtstat Information for 10.10.1.22 |
=====
Looking up status of 10.10.1.22
| 100 SERVER2022 <00> - <nfs> B <ACTIVE> Workstation Service
| 100 CEH <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
| 100 CEH <2,3,4> <1c> - <GROUP> B <ACTIVE> Domain Controllers
| 100 SERVER2022 <20> - <nfs> B <ACTIVE> File Server Service
| 100 CEH <1,2,3> <le> - <GROUP> B <ACTIVE> Browser Service Elections
| 100 CEH <1,2,3> <1b> - <nfs> B <ACTIVE> Domain Master Browser
| 100 CEH <1,2,3> <ld> - <nfs> B <ACTIVE> Master Browser
| 100005 MSBROWSE <01> - <GROUP> B <ACTIVE> Master Browser
| 100021 <1,2,3,4> 2049/tcp nlockmgr
| 100021 <1,2,3,4> 2049/udp nlockmgr
| 100021 <1,2,3,4> 2049/udpo nlockmgr
=====
MAC Address = 00-15-5D-01-80-02

```

Gerren Jerome - Enumeration

ii) **Screengrab: Step 11** – SID/RID info (10.10.1.22)

```
| Target Information |
=====
| Target ..... 10.10.1.22 | Methods: TRACE
| RID Range ..... 500-550,1000-1050 | Scope: /tts/10.0
| Username ..... 'martin' |
| Password ..... 'apple' |
| Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none |
| 100000 2,3,4 111/tcp6 rpcbind |
| 100000 2,3,4 111/udp rpcbind |
=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
| 100003 2,3,4 2049/tcp6 nmb |
| 100003 2,3,4 2049/udp nmb |
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'
| 100021 1,2,3,4 2049/tcp nmb |
| 100021 1,2,3,4 2049/udp nmb |
| Getting domain SID for 10.10.1.22 |
=====
| 100021 1,2,3,4 2049/udp nmb |
| 100021 1,2,3,4 2049/udp nmb |
```

iii) **Screengrab: Step 13** – OS Details (10.10.1.22)

Gerren.Jerome

Domain Name: CEH  
Domain Sid: S-1-5-21-2083413944-2693254119-1471166842  
[+] Host is part of a domain (not a workgroup)

OS information on 10.10.1.22

Use of uninitialized value \$os in concatenation (.) or string at ./enum4linux.pl line 464.

[+] Got OS info for 10.10.1.22 from smbclient:  
[+] Got OS info for 10.10.1.22 from srvinfo:  
10.10.1.22 Wk Sv Sql PDC Tim NT LMB  
platform\_id : 049/tcp 500  
os\_version : 049/tcp 10.0  
server\_type : 049/udp 0x84102f

enum4linux complete on Thu Feb 15 15:46:43 2024

[root@parrot]~[-]

iv) **Screengrab: Step 15** – Password policy (10.10.1.22)

Password Policy Information for 10.10.1.22	
[+] Potentially risky methods: TRACE	
[+] http-title: Login - MovieScore	
[+] Attaching to 10.10.1.22 using martin:apple	
[+] rpcbind: 10.10.1.22:139 (RPC #100000)	
[+] Trying protocol 139/SMB...	
[+] Program version: 2.2.1/prot0 service	
[+] 100000 [!] Protocol failed: Cannot request session (Called Name:10.10.1.22	
[+] 100000 2.2.1 111/tcp6 rpcbind	
[+] 100000 2.2.1 111/udp6 rpcbind	
[+] Trying protocol 445/SMB...[+] rpcbind	
[+] Found domain(s): 2049/udp nts	
[+] 100003 2.2.1 2049/udp nts	
[+] 100004 [+] CEH 2049/tcp nts	
[+] Builtin 2049/tcp6 nts	
[+] 100005 1.2.3 2049/tcp mounted	
[+] Password Info for Domain: CEH mounted	
[+] 100005 1.2.3 2049/udp mounted	
[+] Minimum password length: None	
[+] Password history length: None	
[+] Maximum password age: Not Set	
[+] Password Complexity Flags: 000000	

v) **Screengrab: Step 17** – Group Policy (10.10.1.22)

vi) **Screengrab: Step 19** – Shares (10.10.1.22)