

# Enumeration Methods: Comprehensive Network Analysis

## Introduction

In my role as an ethical hacker with the EC-Council, I embarked on a detailed enumeration project to demonstrate my ability to extract vital information from a target network. Enumeration is a critical phase in penetration testing, providing insights that significantly enhance the ability to perceive and bypass security measures. This project showcases my proficiency in using various enumeration techniques and tools to gather comprehensive information about a target network.

## Objectives

The primary objectives of this project included the extraction of various pieces of information about the target, such as:

- Machine names, ports, operating systems, and services.
- Network resources and shares.
- Usernames, user groups, policies, and passwords.
- Routing tables, audit settings, and service configurations.

## Tasks and Techniques

This project involved performing a series of tasks using a variety of tools and techniques to achieve thorough enumeration. The tasks included:

### 1. NetBIOS Enumeration:

- Using Windows command line and tools like nbtstat to gather NetBIOS information.
- Employing NetBIOS Enumerator for detailed results.
- Conducting NetBIOS scans with Nmap's NSE scripts.

### 2. SNMP Enumeration:

- Using tools like snmp-check, SoftPerfect Network Scanner, and snmpwalk to extract SNMP information.
- Performing SNMP scans with Nmap for additional insights.

### 3. **LDAP Enumeration:**

- Utilizing Active Directory Explorer (AD Explorer) and Python with ldap3 to explore LDAP directories.
- Performing LDAP brute force and directory object retrieval with Nmap.

### 4. **NFS Enumeration:**

- Conducting NFS scans using RPCScan and SuperEnum tools.

### 5. **DNS Enumeration:**

- Performing DNS zone transfers, DNSSEC zone walking, and service discovery with tools like dig, dnsrecon, and Nmap.

### 6. **SMTP Enumeration:**

- Listing mail users and open SMTP relays with Nmap.

### 7. **RPC, SMB, and FTP Enumeration:**

- Using tools like NetScanTools Pro and Nmap to enumerate RPC, SMB, and FTP services.

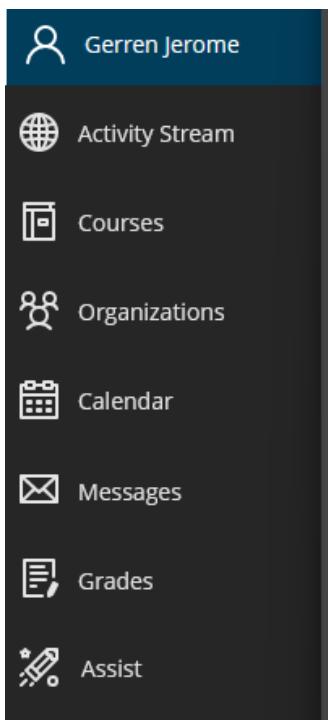
## **General Enumeration Tools:**

- Employing tools like Global Network Inventory, Advanced IP Scanner, and Enum4linux to gather information from network resources, Windows, and Samba hosts.

## **Tools Utilized**

Throughout this project, I utilized several key tools to perform enumeration tasks, including:

- **Nmap:** For scanning and service discovery.
- **NetBIOS Enumerator:** For detailed NetBIOS information.
- **snmp-check and snmpwalk:** For SNMP enumeration.
- **Active Directory Explorer and Python (ldap3):** For LDAP exploration.
- **RPCScan and SuperEnum:** For NFS enumeration.
- **dig, dnsrecon:** For DNS enumeration.
- **Global Network Inventory and Advanced IP Scanner:** For comprehensive network resource enumeration.
- **Enum4linux:** For extracting information from Windows and Samba hosts.

**Perform enumeration (NetBIOS)****NetBIOS enumeration via Windows command line****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.

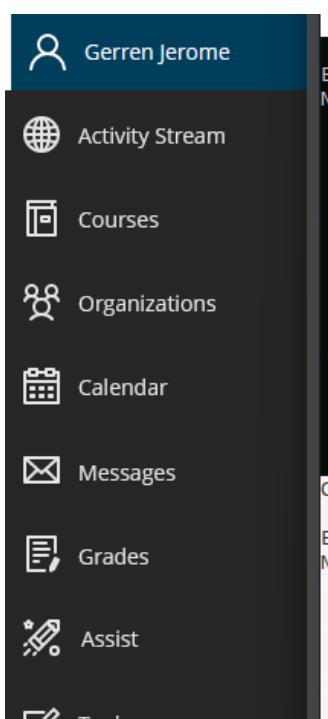
C:\Users\Administrator>nbtstat -a 10.10.1.11

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_MSBROWSE_@<01> GROUP     Registered

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

**nbtstat result**


```
Windows PowerShell - Select Administrator: Command Prompt
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_@<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
```

## Gerren Jerome - Enumeration

net use result

The screenshot shows the Windows Start Menu interface. On the left, there is a sidebar with various icons for 'Activity Stream', 'Courses', 'Organizations', 'Calendar', 'Messages', 'Grades', and 'Assist'. The main area displays the output of several commands:

```
WORKGROUP      <1E>  GROUP      Registered
WORKGROUP      <1D>  UNIQUE     Registered
00_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

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

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

## NetBIOS enumeration via NetBIOS enumerator

NBE result (Debug)

The screenshot shows the NetBIOS Enumerator tool window. On the left, there is a sidebar with icons for 'Activity Stream', 'Courses', 'Organizations', 'Calendar', 'Messages', 'Grades', and 'Assist'. The main window has a 'Scan' tab selected. It shows the configuration for a scan:

IP range to scan  
from: 10.10.1.15  
to: 10.10.1.100  
Your local ip:  
10.10.1.11  
 [1...254]

The results pane shows two entries:

- [+] ? 10.10.1.19 [SERVER2019]
- [+] ? 10.10.1.22 [SERVER2022]

The debug window on the right shows the following log:

```
Scanning From: 10.10.1.15
to: 10.10.1.100
Ready!
```

At the bottom, it says "scanning: 10.10.1.100".

**Expanded result**

The screenshot shows the NetBIOS Enumerator interface. On the left is a sidebar with links: Institution Page, Gerren Jerome (selected), Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, and Tools. The main window has tabs for 'NetBIOS Enumerator' and 'NetBIOS Names'. The 'NetBIOS Enumerator' tab is active, showing a configuration panel with 'IP range to scan' fields set to 'from: 10.10.1.15' and 'to: 10.10.1.100', a checkbox for 'Scan' (unchecked), 'Your local ip:' set to '10.10.1.11', and a checked checkbox for '[1...254]'. Below this is a tree view of scanned hosts:

- 10.10.1.19 [SERVER2019]
  - NetBIOS Names (3)
    - SERVER2019 - Workstation Service
    - WORKGROUP - Domain Name
    - SERVER2019 - File Server Service
  - Username: (No one logged on)
  - Domain: WORKGROUP
  - MAC: 02-15-5d-42-86-7b
  - Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
- 10.10.1.22 [SERVER2022]
  - NetBIOS Names (8)
    - SERVER2022 - Workstation Service
    - CEH - Domain Name
    - CEH - Domain Controller
    - SERVER2022 - File Server Service
    - CEH - Potential Master Browser
    - CEH - Domain Master Browser
    - CEH - Master Browser
    - MSBROWSE - Master Browser
  - Username: (No one logged on)
  - Domain: CEH
  - MAC: 00-15-5d-01-80-02
  - Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128

A 'Debug window' on the right shows the command: 'Scanning from: 10.10.1.15 to: 10.10.1.100 Ready!'

**NetBIOS enumeration via NSE Script****Nmap scan (-sV)**

The screenshot shows a terminal window titled 'Parrot Terminal' with the title bar 'File Edit View Search Terminal Help'. The main area displays the output of an Nmap scan using the '-sV' option. The output is as follows:

```

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

```

### 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>
```

### Perform enumeration (SNMP)

SNMP enumeration via snmp-check

### Nmap scan (-sU)

```
nmap -sU -p161 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
\x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
Hacking_Wireless
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
[root@parrot]~/.home/attacker]
#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
```

## snmp-check results (1 of 3)

```

● ● ●
File Edit View Search Terminal Help
snmp-check 10.10.1.22 - Parrot Terminal
[*] Try to connect to 10.10.1.22:161 using SNMPv1 and community 'public'
[*] System information:
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 :

```

## snmp-check results (2 of 3)

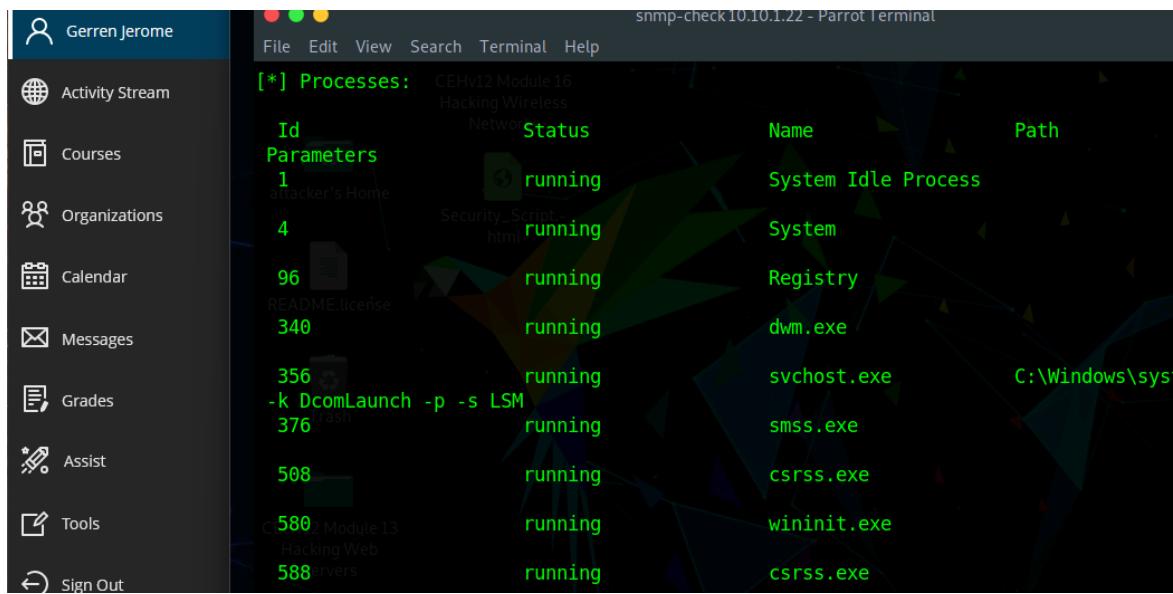
```

● ● ●
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 :
  Id : 1
  Mac Address :
  Type : softwareLoopback
  Speed : 1073 Mbps
  MTU : 1500
  In octets :
  Out octets :

```

## Gerren Jerome - Enumeration

### snmp-check results (3 of 3)

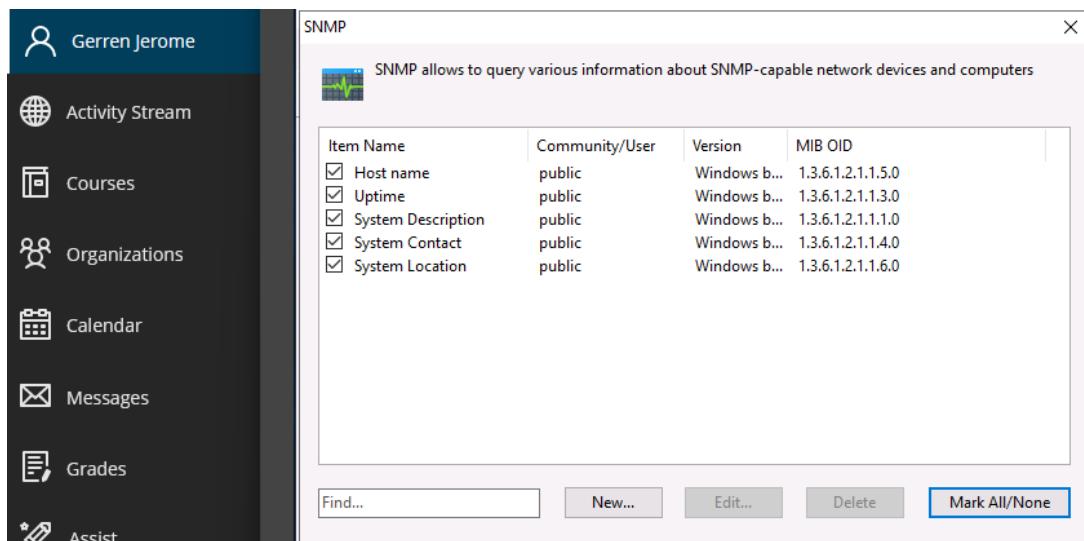


The screenshot shows a terminal window titled "snmp-check 10.10.1.22 - Parrot Terminal". The title bar also includes "CEHv12 Module 16 Hacking Wireless Networks". The terminal displays a table of running processes:

Id	Parameters	Status	Name	Path
1	stacker's Home	running	System Idle Process	
4	Security_Script.html	running	System	
96	README.license	running	Registry	
340		running	dwm.exe	C:\Windows\system32\
356	-k DcomLaunch -p -s LSM	running	svchost.exe	C:\Windows\system32\
376	flash	running	smss.exe	C:\Windows\system32\
508		running	csrss.exe	C:\Windows\system32\
580	C:\Windows\system32\Hacking\CEHv12 Module 13 Hacking Web Servers	running	wininit.exe	C:\Windows\system32\
588		running	csrss.exe	C:\Windows\system32\

### SNMP enumeration via SoftPerfect Network Scanner

### prescan config



The screenshot shows a "SNMP" configuration dialog from the SoftPerfect Network Scanner. The title bar says "SNMP". The main area contains a table of items to be queried:

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 dialog are buttons for "Find...", "New...", "Edit...", "Delete", and "Mark All/None".

## Gerren Jerome - Enumeration

### SPNS scan results

The screenshot shows the SoftPerfect Network Scanner interface. On the left is a sidebar with user information and navigation links. The main window displays a table of scanned hosts. The columns include IP Address, MAC Address, Response Time, Host Name, Uptime, System Description, and System Contact. The table lists several hosts, including 'ubuntu-Virtual...', 'WINDOWS11', 'Android.local', 'www.goodsho...', 'Server2019', 'Server2022', and 'Server2022.CEH.com'.

IP Address	MAC Address	Response Time	Host Name	Uptime	System Descr...	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: Inte...
10.10.1.22	00-15-5D-01-8...	1 ms	Server2022	Server2022.CE...	473180 (0d 1h ...)	Hardware: Inte...

### properties of target machine (10.10.1.22)

The screenshot shows the SoftPerfect Network Scanner interface with the 'Properties' tab selected. It displays various system information for the host at 10.10.1.22. The properties listed include Shared Resources (NETLOGON, SYSVOL, Users), IP Address (10.10.1.22), MAC Address (00-15-5D-01-80-02), Response Time (1 ms), Host Name (Server2022), Host name (Server2022.CEH.com), Uptime (473180 (0d 1h 18m 51s)), System Description (Hardware: Intel64 Family 6 Model...), System Contact, and System Location.

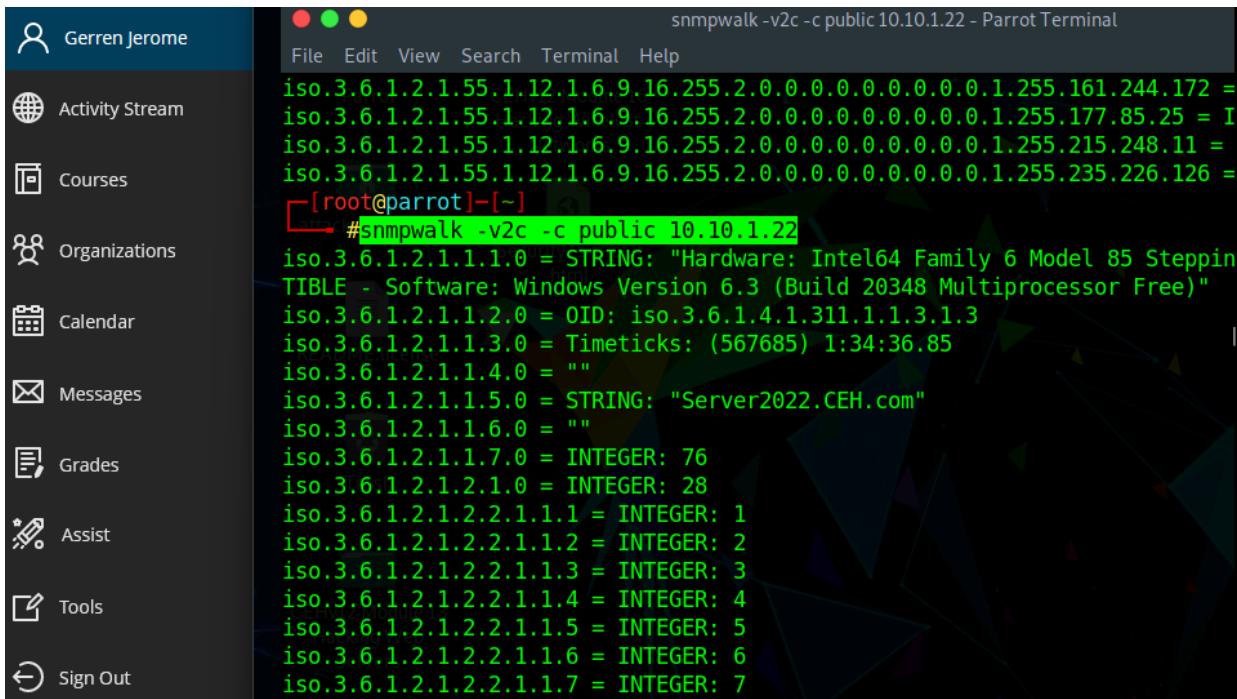
### SNMP enumeration via SnmpWalk

#### scan result (snmpwalk -v1)

The screenshot shows a terminal window titled 'snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal'. The command entered was '#snmpwalk -v1 -c public 10.10.1.22'. The output displays various SNMP variables and their values for the target host.

```
[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 TABLE - 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.3.6.1.2.1.2.1.1 = 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
```

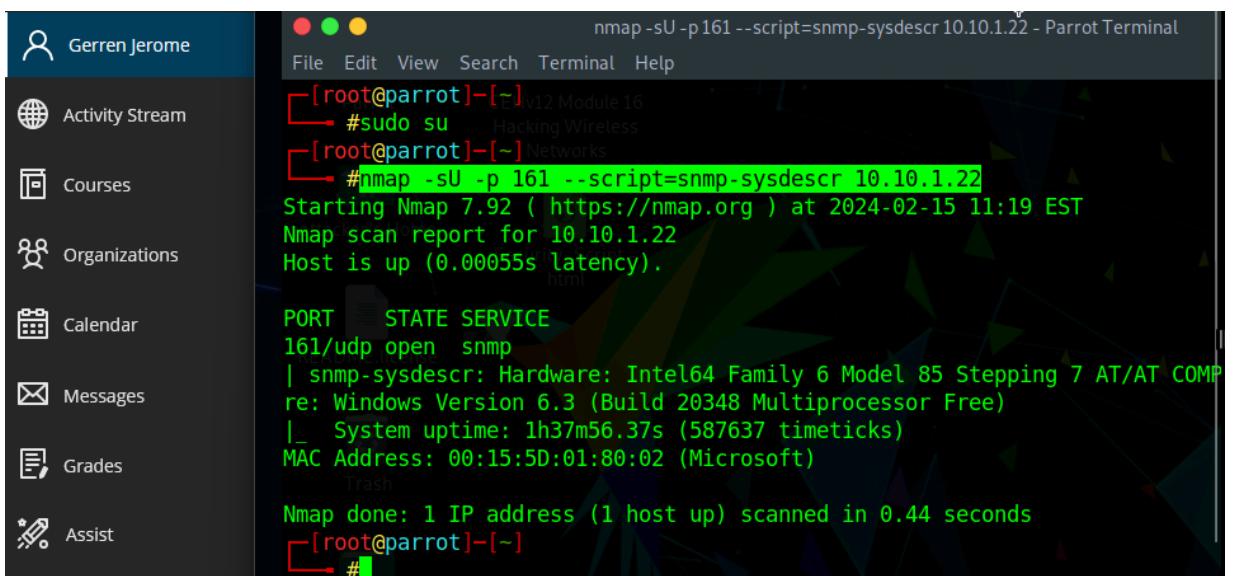
scan result (snmpwalk -v2c)



```
snmpwalk -v2c -c public 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.1.255.161.244.172 =
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.1.255.177.85.25 = I
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.1.255.215.248.11 =
iso.3.6.1.2.1.55.1.12.1.6.9.16.255.2.0.0.0.0.0.0.0.1.255.235.226.126 =
[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 Steppin
TIBLE - 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
```

SNMP enumeration via Nmap (4 tasks)

scan result (type and description)



```
nmap -sU -p161 --script=snmp-sysdescr 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#sudo su
[root@parrot]~[~]
#nmap -sU -p 161 --script=snmp-sysdescr 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:19 EST
Nmap scan report for 10.10.1.22
Host is up (0.00055s latency).

PORT      STATE SERVICE
161/udp    open  snmp
|_snmp-sysdescr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMP
re: Windows Version 6.3 (Build 20348 Multiprocessor Free)
|_ 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
[root@parrot]~[~]
#
```

## scan result (ports and processes)

```
nmap -sU -p 161 --script=snmp-processes 10.10.1.22 - Parr
#nmap -sU -p 161 --script=snmp-processes 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-15 11:21 EST
Nmap scan report for 10.10.1.22
Host is up (0.00067s latency).

PORT      STATE SERVICE
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
```

## scan result (applications)

```
nmap -sU -p 161 --script=snmp-win32-software 10.10.1.22 - Parrot
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
```

### scan result (interfaces)

```
nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22 -Pn
[+] 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 6to4 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 (DDI)\x00
|   Type: tunnel Speed: 0 Kbps
|   Status: down
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
```

### Perform enumeration (LDAP)

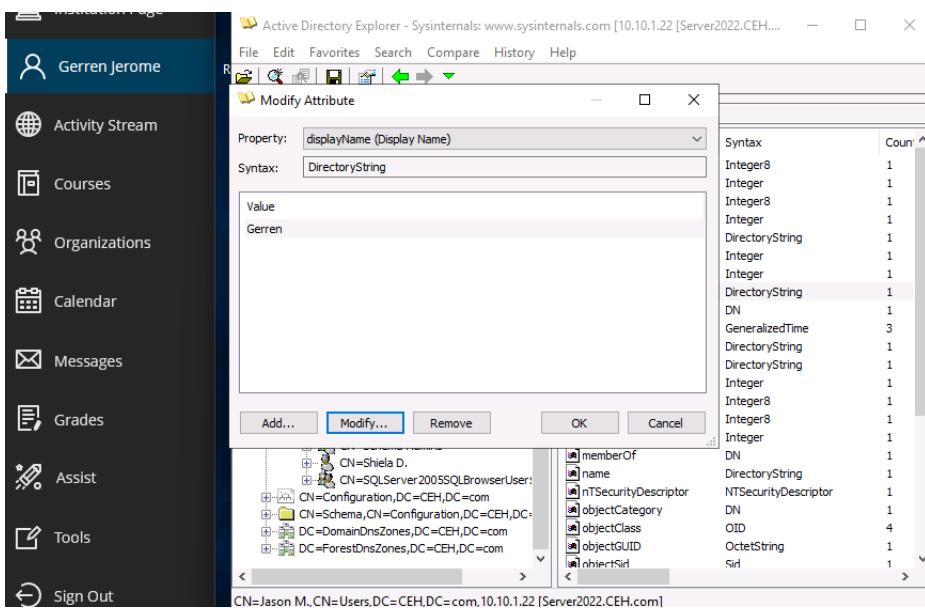
Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

### Navigating ADExplorer

The screenshot shows the Active Directory Explorer interface. The left sidebar contains a navigation menu with options like Institution Page, Gerren Jerome, Activity Stream, Courses, Organizations, Calendar, Messages, Grades, Assist, Tools, and Sign Out. The main pane displays the LDAP tree structure under the path "10.10.1.22 [Server2022.CEH.com]". The tree includes nodes for DC, CN=BuiltIn, CN=Computers, CN=Deleted Objects, OU=Domain Controllers, CN=ForeignSecurityPrincipals, CN=Infrastructure, CN=Keys, CN=LostAndFound, CN=Managed Service Accounts, CN=NTDS Quotas, CN=Program Data, CN=System, CN=TPM Devices, and CN=Users. Under CN=Users, there are numerous user objects with names such as Administrator, Allowed RODC Password Replicat, Cert Publishers, Cloneable Domain Controllers, Denied RODC Password Replicati, DnsAdmins, DnsUpdateProxy, Domain Admins, and Domain Computers.

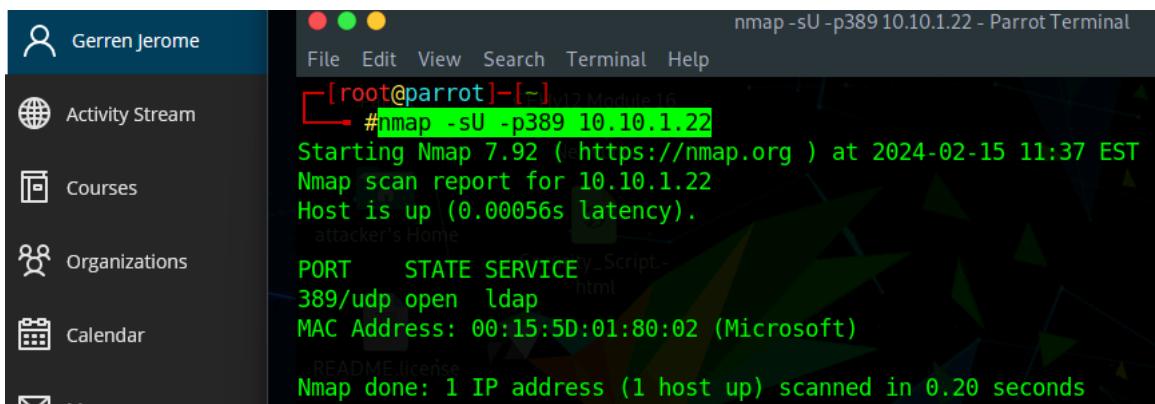
## Gerren Jerome - Enumeration

### user attribute modification



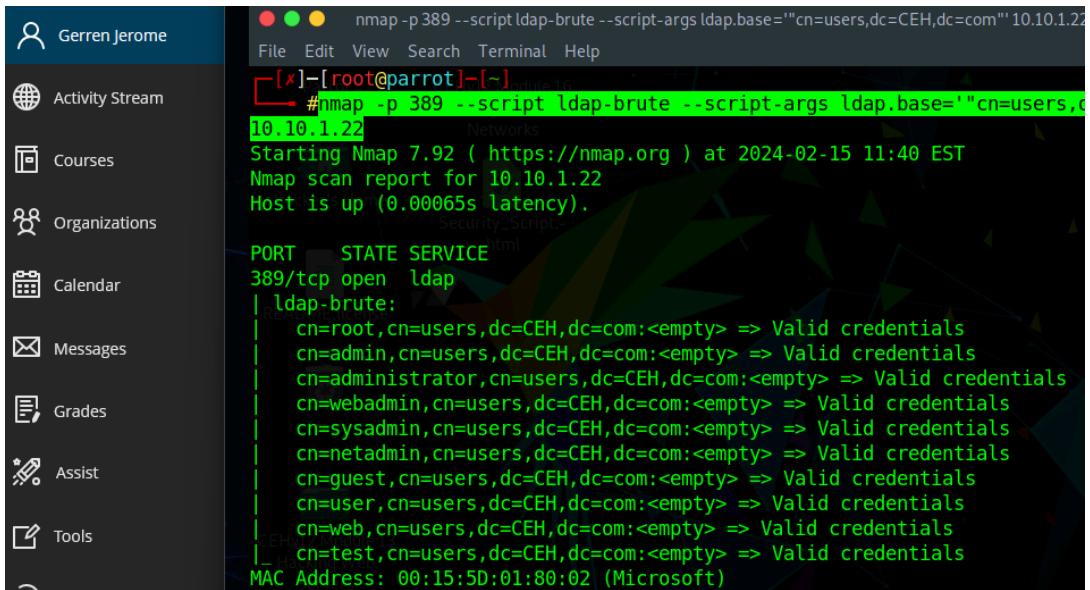
### Perform LDAP enumeration using Python and Nmap

#### scan result (Nmap -sU)



## Gerren Jerome - Enumeration

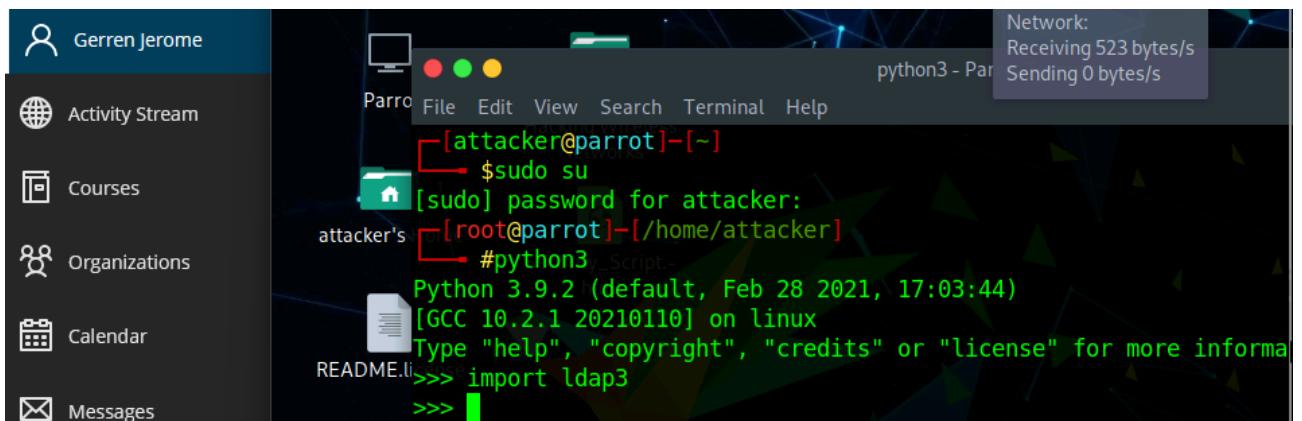
### result (Nmap LDAP bruteforce)



```
nmap -p 389 --script ldap-brute --script-args ldap.base="cn=users,dc=CEH,dc=com" 10.10.1.22
[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).

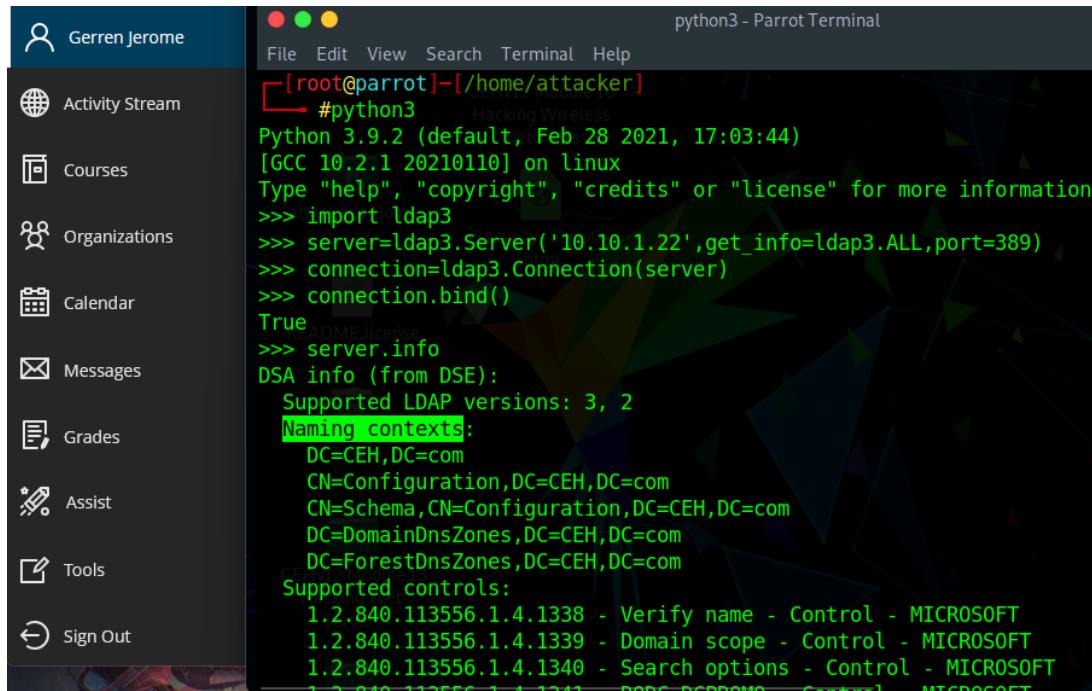
PORT      STATE SERVICE
389/tcp    open  ldap
| ldap-brute:
|   cn=root,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=admin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=administrator,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=webadmin,cn=users,dc=CEH,dc=com:<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)
```

### import ldap3 into Python

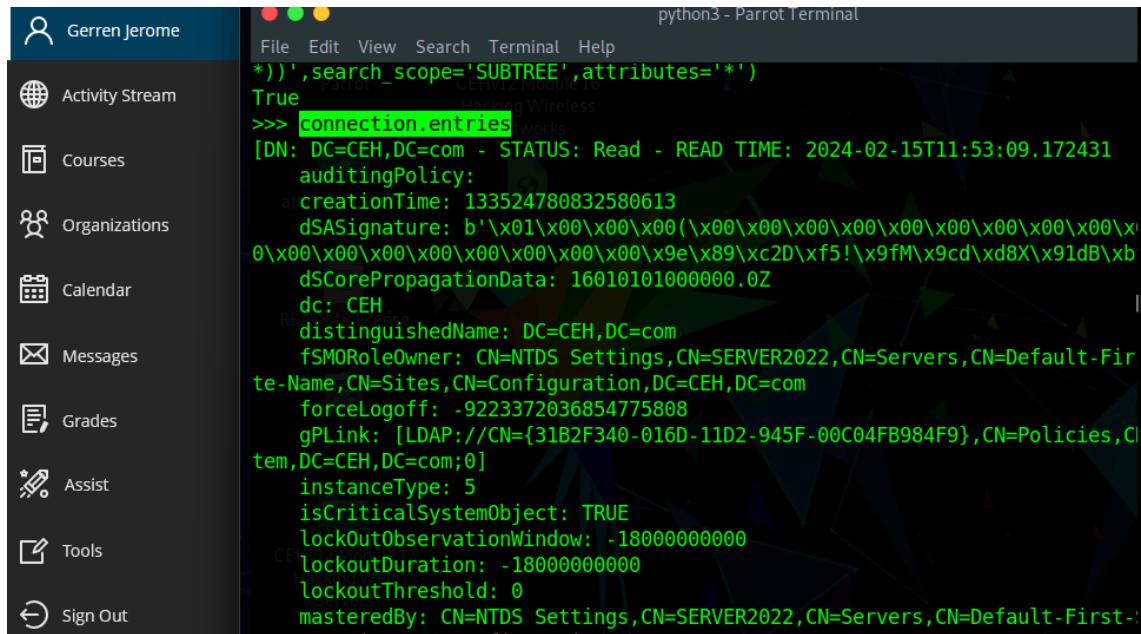


```
File Edit View Search Terminal Help
[attacker@parrot]-[~]
[sudo] password for attacker:
[attacker@parrot]-[~/home/attacker]
#python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information
>>> import ldap3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

gain naming context



retrieve directory objects



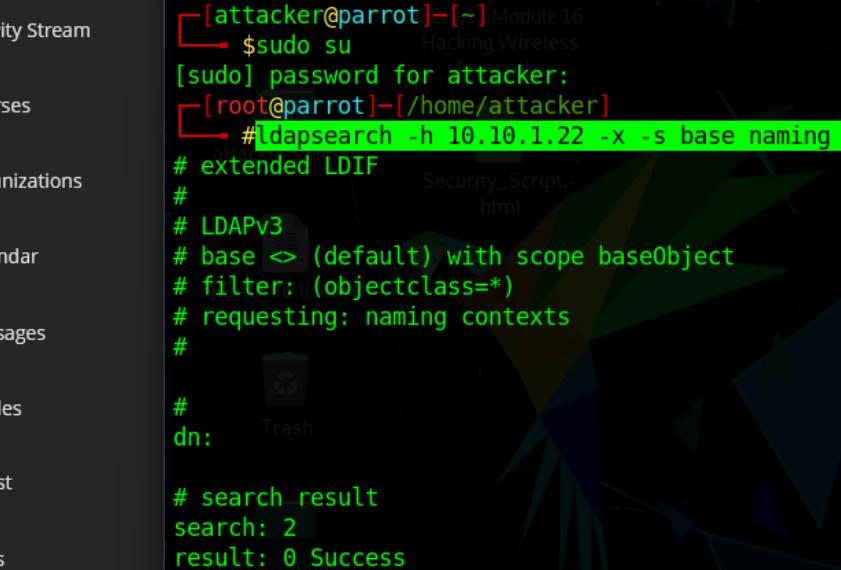
## result (LDAP dump)

```
python3 - Parrot Terminal
File Edit View Search Terminal Help

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
\x87\x a0\x9\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
]
```

Perform LDAP enumeration using ldapsearch

gain naming context via ldapsearch



```
ldapsearch -h 10.10.1.22 -x -s base naming contexts -P
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# 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
```

## more information about primary domain

The screenshot shows a terminal window running on a Linux desktop. The terminal is titled 'ldapsearch-h 10.10.1.22 -x -b "DC=CEH,DC=com"'. The command executed is '# ldapsearch -h 10.10.1.22 -x -b "DC=CEH,DC=com"'. The output shows details of the 'CEH.com' domain entry, including its distinguished name (dn: DC=CEH,DC=com), object classes (top, domain, domainDNS), and various attributes like instanceType, whenCreated, whenChanged, and subRefs.

```

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

```

## retrieve info about objects in directory tree

The screenshot shows a terminal window running on a Linux desktop. The terminal is titled 'ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectclass=\*" - Parrot Terminal'. The command executed is '# ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectclass=\*"'. The output is identical to the previous screenshot, displaying the same domain entry details.

```

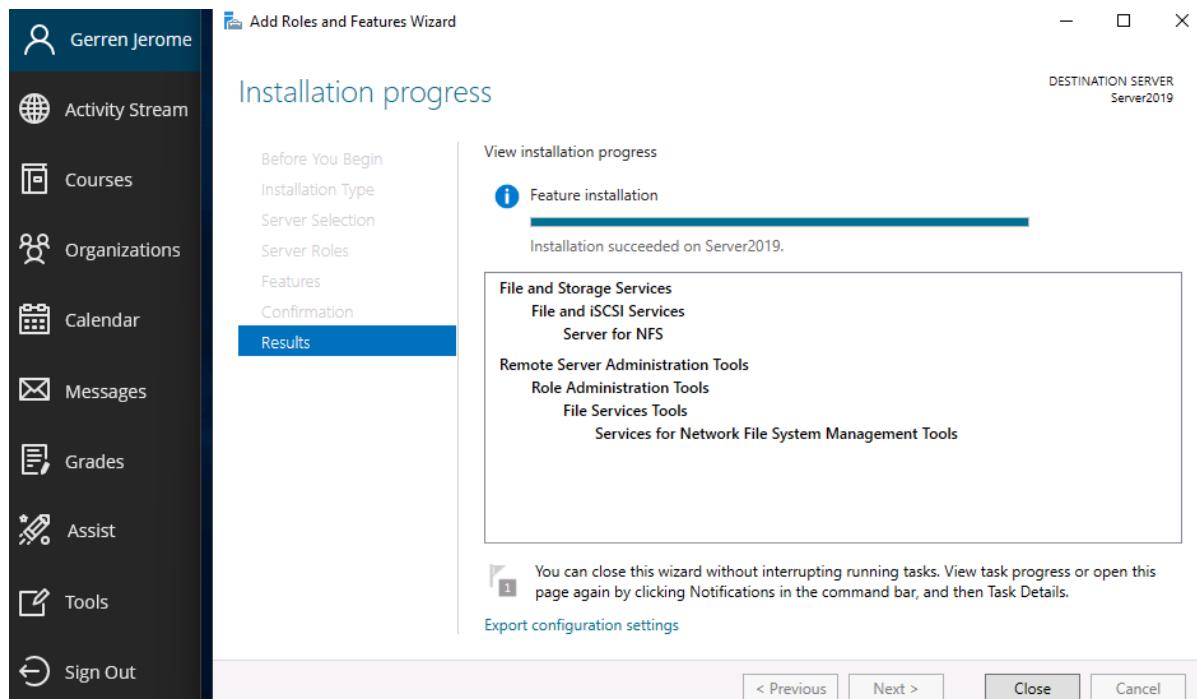
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectclass=*" - Parrot Terminal
# extended LDIF
#
# LDAPv3
# base <DC=CEH,DC=com> with scope subtree
# filter: objectclass=*
# requesting: ALL
#
# README.license
# CEH.com
dn: DC=CEH,DC=com
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

```

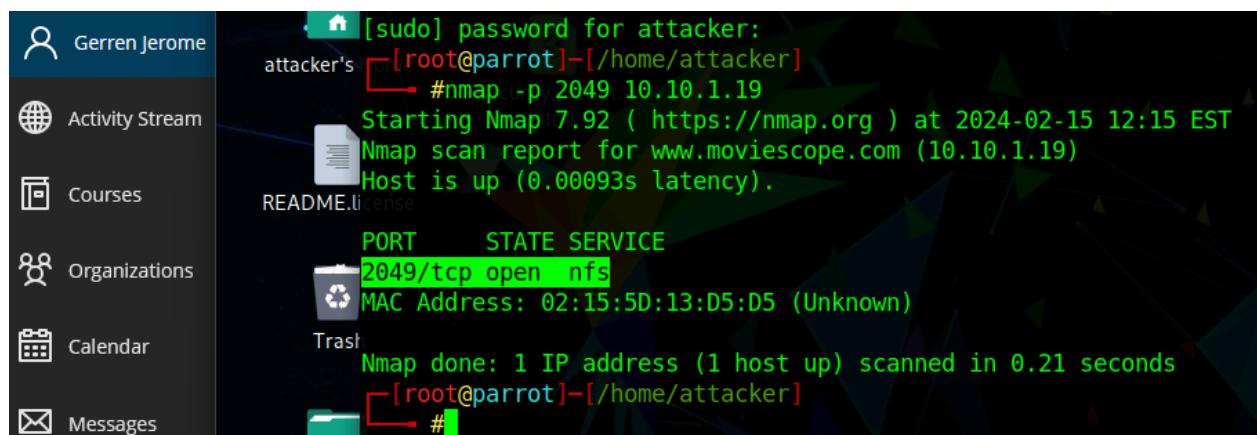
Perform enumeration (NFS)

Perform NFS enumeration using RPCScan and SuperEnum

confirm install/enable of NFS service in Windows



scan result (NFS running?)



**scan result (SuperEnum)**

 Gerren Jerome	Testing for 10.10.1.19: 1801 15-02-2024/10.10.1.19/open_ports/1801/telnet: line 3: expect: command not found
 Activity Stream	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
 Courses	Testing for 10.10.1.19: 2103 15-02-2024/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found
 Organizations	Testing for 10.10.1.19: 2105 15-02-2024/10.10.1.19/open_ports/2105/telnet: line 3: expect: command not found
 Calendar	Testing for 10.10.1.19: 2107 15-02-2024/10.10.1.19/open_ports/2107/telnet: line 3: expect: command not found
 Messages	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
 Grades	
 Assist	
 Tools	
 Sign Out	

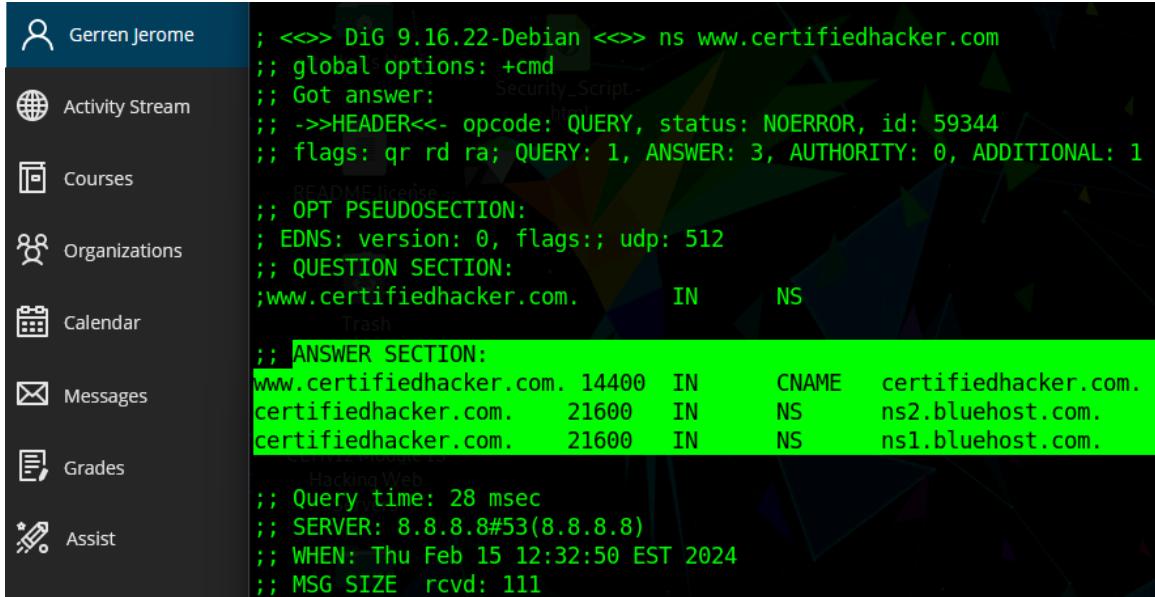
**scan result (RPCScan)**

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

Perform enumeration (DNS)

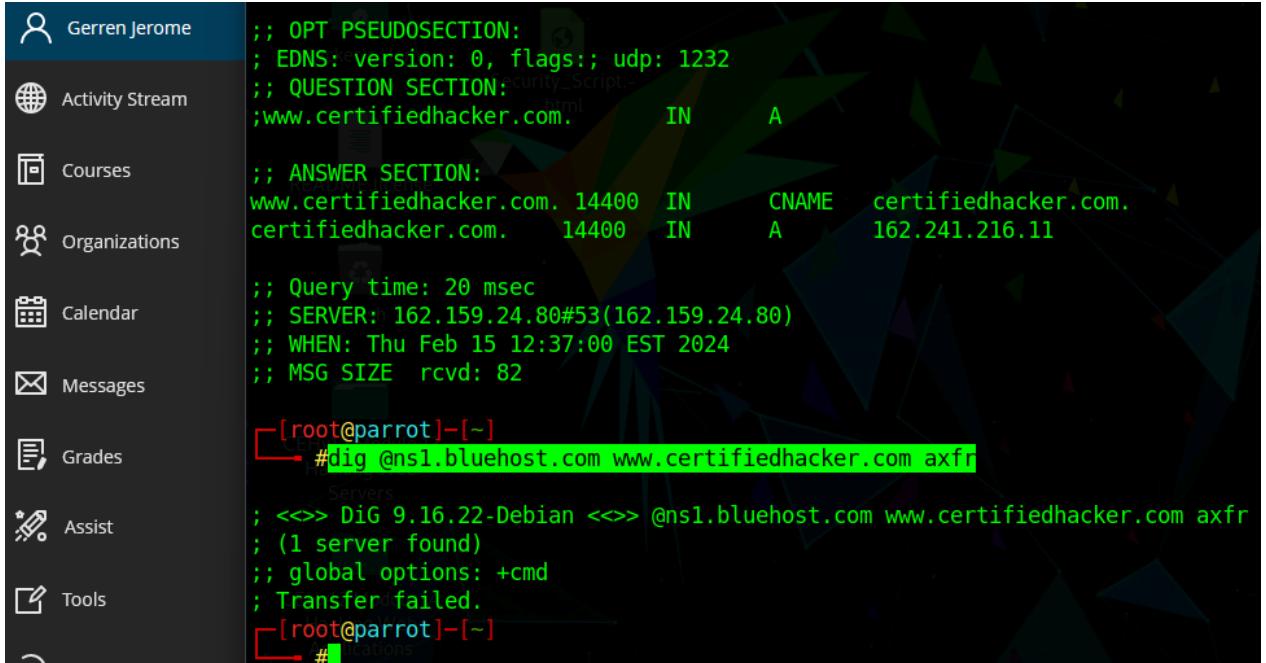
Perform DNS enumeration using zone transfer.

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. IN NS ns2.bluehost.com.
certifiedhacker.com. IN NS ns1.bluehost.com.
;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 21600 IN NS ns2.bluehost.com.
certifiedhacker.com. 21600 IN NS ns1.bluehost.com.
;; 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
```

scan result (dig transfer failed?)



```
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.certifiedhacker.com. IN A
;ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com. 14400 IN A 162.241.216.11
;; Query time: 20 msec
;; SERVER: 162.159.24.80#53(162.159.24.80)
;; WHEN: Thu Feb 15 12:37:00 EST 2024
;; MSG SIZE rcvd: 82
[root@parrot]~#
#dig @ns1.bluehost.com www.certifiedhacker.com axfr
; <>> DiG 9.16.22-Debian <>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
[root@parrot]~#
#
```

## Gerren Jerome - [Enumeration](#)

### scan result (nslookup (interactive mode) – certifiedhacker)

```
C:\ Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>set querytype=soa

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)
```

### scan result (nslookup (interactive mode) – bluehost)

```
C:\Users\Admin>set querytype=soa

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.
```

## Perform DNS enumeration using DNSSEC zone walking

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

```

## Perform DNS enumeration using Nmap

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:3b1e
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

```

## scan result (associated subdomains)

```
[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
[root@parrot]~[/home/attacker]
└─#
```

## scan result (SRV records)

```
● ● ○ 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]
└─#
```

Perform enumeration (SMTP)

Perform SMTP enumeration using Nmap

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
|   vers
|   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]
└─#
```

list open SMTP relays

```
[x]-[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)

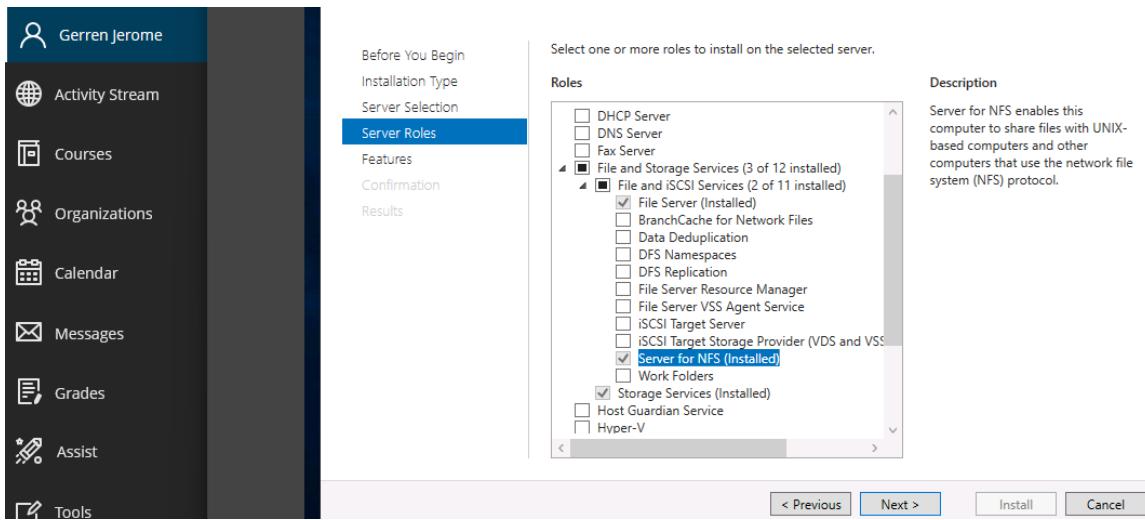
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
[root@parrot]-[/home/attacker]
└─#
```

Gerren Jerome - Enumeration

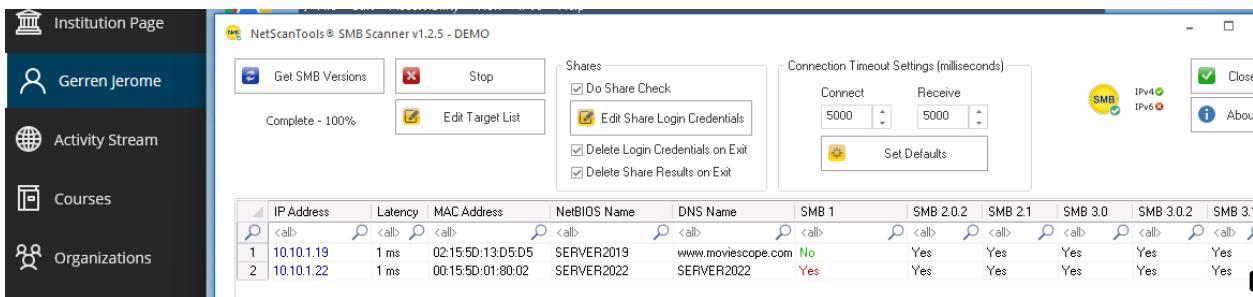
Perform enumeration (RPC, SMB, and FTP)

## Perform SMB and RPC enumeration using NetScanTools Pro

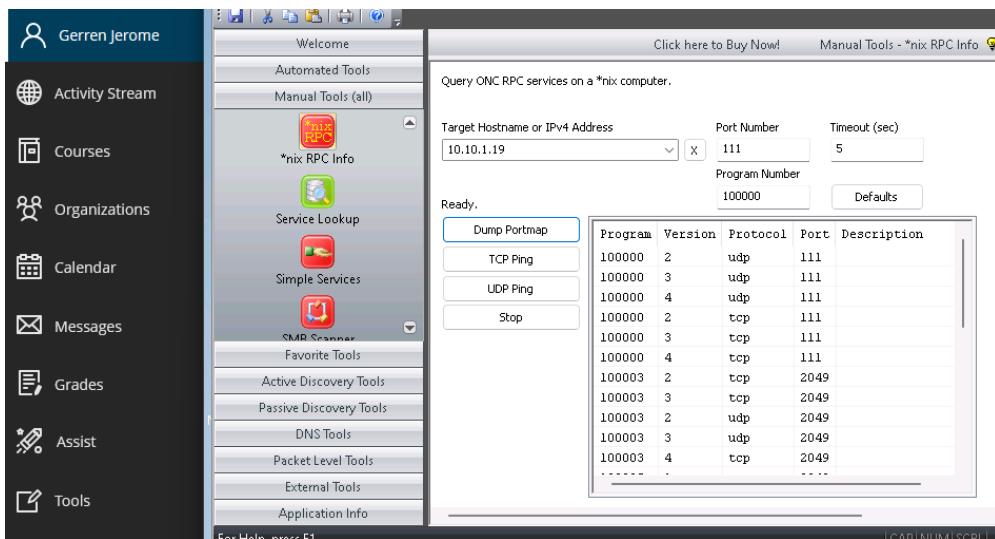
confirm install/enable NFS services.



## SMB scanner results



## portmap dump (WIN\_SVR\_19)



Perform RPC, SMB, and FTP enumeration using Nmap.

confirm addition of CEH.com FTP site to IIS

nmap scan (Port 21 - FTP)

```

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
[root@parrot]~/.nmap/modules/16
└─#cd
[root@parrot]~/.nmap
└─#sudo su
[root@parrot]~/.nmap
└─#cd
[root@parrot]~/.nmap
└─#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 (Unknown)

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

```

nmap scan (other services and ports)

```

[root@parrot]~/.nmap/modules/16
└─#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 RSE
T 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

```

**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/tcp  mountd
|_ 100005 1,2,3,4 2049/udp  mountd
|_ 100005 1,2,3,4 2049/udp6 mountd
|_ 100005 1,2,3,4 2049/tcp6 nlockmgr
|_ 100005 1,2,3,4 2049/udp6 nlockmgr
|_ start date: N/A
|_ 100021 1,2,3,4 2049/udp  nlockmgr
```

**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).

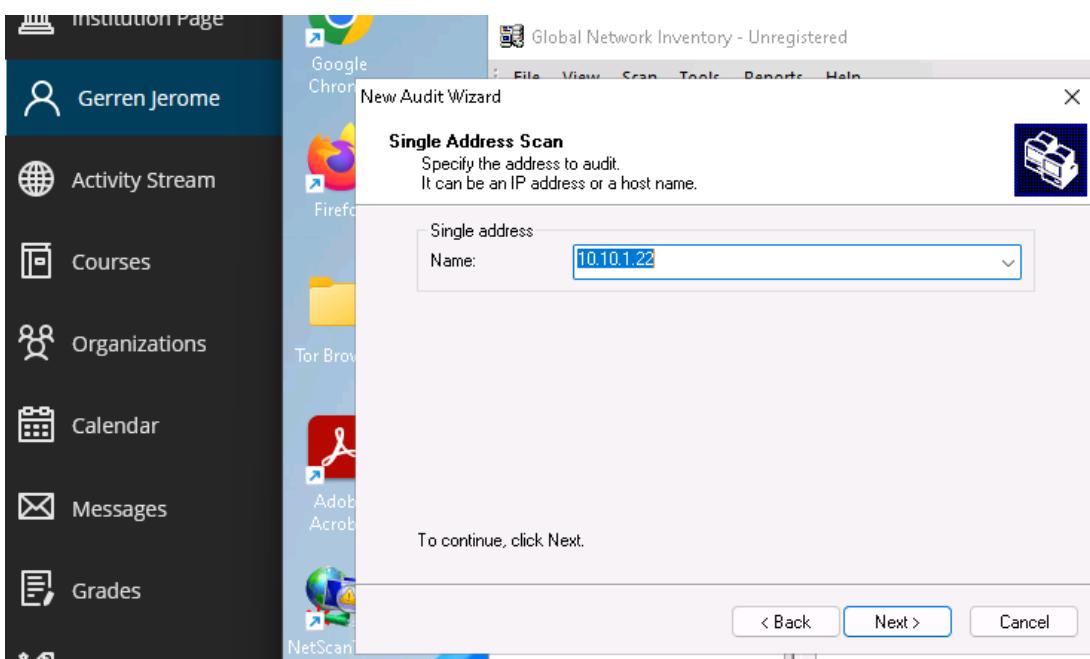
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        Microsoft ftptd
|_  ftp-syst: version  port/proto  service
|_  SYST: Windows NT   111/tcp   rpcbind
MAC Address: 02:15:5D:13:D5:D5 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed 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 Server 2016 (91%), Microsoft Windows 10 1703 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
|_  100021 1,2,3,4 2049/tcp6 nlockmgr
TRACEROUTE
|_ 100021 1,2,3,4 2049/udp6 nlockmgr
|_ 100021 1,2,3,4 2049/udp  nlockmgr
```

## Gerren Jerome - Enumeration

Perform enumeration using various enumeration tools.

Enumerate information using Global Network Inventory

confirm settings (GNI single address scan)



Scan summary (GNI)

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

Global Network Inventory - Unregistered

View results

Name

All addresses

CEH

10.10.1.22 (SERVER2...)

Memory devices Port connectors Operating System Installed software Hot fixes

Environment Services Startup Desktop Devices Video controllers

Monitors Logical disks Disk drives Printers Network adapters NetBIOS

Shares SNMP system SNMP devices SNMP interfaces

SNMP storage SNMP installed software User groups Users Logged on

Scan summary Computer system Processors Main board BIOS Memory

Domain IP Address Timestamp

Type / Host... / Status / MAC... / Ven... / OS Name / Process... / Com... /

-| Domain : CEH (COUNT=1)

-| IP Address : 10.10.1.22 (COUNT=1)

-| Timestamp : 2/15/2024 12:22:46 PM (COUNT=1)

-| Com... SERVER2 Success 00-15-5D-1 Microsoft Microsoft Win|Intel(R) Xeon| Serial: 143

Total 1 item(s)

Results history depth: Last scan for each address      Displayed group: All groups

## Gerren Jerome - Enumeration

### GNI Scan Result (Operating System)

The screenshot shows the GNI interface with the title "Global Network Inventory - Unregistered". The left sidebar shows user information and navigation links. The main window displays a tree view under "View results" with "All addresses" selected, which further branches into "CEH" and "10.10.1.22 (SERVER2...)".

The right pane shows a detailed list of operating system findings:

Type	Host	Name	Serial No.	Cd Key	Re...	Org...
Domain	CEH (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-B Windows				

Total 1 item(s)

Results history depth: Last scan for each address | Displayed group: All groups

### GNI Scan Result (User Groups)

The screenshot shows the GNI interface with the title "Global Network Inventory - Unregistered". The left sidebar shows user information and navigation links. The main window displays a tree view under "View results" with "All addresses" selected, which further branches into "CEH" and "10.10.1.22 (SERVER2...)".

The right pane shows a detailed list of user group findings:

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)

Results history depth: Last scan for each address | Displayed group: All groups

### GNI Scan Result (Services)

The screenshot shows the GNI interface with the title "Global Network Inventory - Unregistered". The left sidebar shows user information and navigation links. The main window displays a tree view under "View results" with "All addresses" selected, which further branches into "CEH" and "10.10.1.22 (SERVER2...)".

The right pane shows a detailed list of service findings:

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 -k AxInst
Adobe Acrobat Update Service	Automatic	Running	"C:\Program Files\b681\Adobe\Adobe
AllJoyn Router Service	Manual	Stopped	C:\Windows\system32\svchost.exe -k Local
App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe -k AppR
Application Host Helper Service	Automatic	Running	C:\Windows\System32\svchost.exe -k appho
Application Identity	Manual	Stopped	C:\Windows\System32\svchost.exe -k LocalF
Application Information	Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvc
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe

Total 234 item(s)

Results history depth: Last scan for each address | Displayed group: All groups

Gerren Jerome - Enumeration

## GNI Scan Result (Shares)

The screenshot shows the NetworkMiner interface with several panes. The left pane displays the 'Activity Stream' and 'Courses' sections. The main pane has tabs for 'Scan summary', 'Computer system', 'Processor', 'Main board', 'CPU', 'Memory', and 'Network devices'. The 'Processor' tab is active, showing details for a CPU on SERVER22. The 'Shares' section lists a 'Special share' at IP 10.10.1.22 with name '\$'. The 'Memory' section shows logical disks with 99.39 GB free space. The 'Network devices' section lists several interfaces, including 'Interprocess co.', 'NETLOGON', 'SYSVOL', and 'Users'.

Enumerate network resources using Advanced IP Scanner

## Advanced IP Scanner results

The screenshot shows the NetworkMiner interface. On the left is a dark sidebar with user info (Gerren Jerome) and links for Activity Stream, Courses, Organizations, Calendar, and Messages. The main window has a toolbar with Scan, Stop, IP, C, and Network icons. A search bar at the top contains the IP range "10.10.1.5-10.10.1.23". Below it is a table titled "Results" with columns: Status, Name, IP, Manufacturer, MAC address, and a timestamp column. The table lists several network devices and hosts:

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

Enumerate information from Windows and Samba hosts using Enum4linux.

## NetBIOS scan (10.10.1.22)

Gerren Jerome - Enumeration

SID/RID info (10.10.1.22)

```
Institution Page | Target Information | [+] enum4nmb -a -T: TRACE  
=====  
Usernames .. 10.10.1.22 -> [+] enum4nmb -a -T: TRACE  
RID Range ..... 500-550,1000-1050  
Username ..... 'martin'  
Password ..... 'apple'++/proto service  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
| 100000 2,3,4 111/tcp b rpcbind  
| 100000 2,3,4 111/udp b rpcbind  
=====  
| Enumerating Workgroup/Domain on 10.10.1.22 |  
=====  
[+] Got domain/workgroup name: CEH  
| 100003 2,3,4 2049/tcp b nfs  
| 100003 2,3,4 2049/udp b nfs  
=====  
| 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 b nlockmgr  
| 100021 1,2,3,4 2049/udp b nlockmgr  
=====  
| Getting domain SID for 10.10.1.22 |  
=====  
| 100021 1,2,3,4 2049/udp b nlockmgr
```

## OS Details (10.10.1.22)

Gerren Jerome	<pre>   [+] Getting domain SID for 10.10.1.22   ===== 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_info 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: 1000 10.10.1.22 Wk Sv Sql PDC Tim NT LMB 1000 platform_id : 2049/tcp 500 mounted 1000 os_version : 2049/tcp 10.0 mounted 1000 server_type : 2049/udp 0x84102f enum4linux complete on Thu Feb 15 15:46:43 2024 100021 1.1,3,4 2049/tcp nlockmgr 100021 1.1,3,4 2049/udp nlockmgr [+] [root@parrot]--[-] └── #</pre>
Activity Stream	
Courses	
Organizations	
Calendar	
Messages	
Grades	
Assist	

## Password policy (10.10.1.22)

```
| /etc/Password Policy Information for 10.10.1.22 | [+] [+] Reproducing [+] Potentially risky methods: TRACE [+] Error title: Local MailScope [+] Attaching to 10.10.1.22 using martin:apple [+] [+] Trying protocol 139/SMB... [+] [+] Protocol failed: Cannot request session (Called Name:10.10.1.22) [+] [+] Trying protocol 445/SMB... [+] [+] Found domain(s): CEH [+] [+] CEH [+] [+] Builtin [+] [+] Password Info for Domain: CEH [+] [+] Minimum password length: None [+] [+] Password history length: None [+] [+] Maximum password age: Not Set [+] [+] Password Complexity Flags: 000000
```

## Group Policy (10.10.1.22)

Institution Page	Groups on 10.10.1.22
Gerren Jerome	[+] Getting builtin groups: group:[Server Operators] rid:[0x225] group:[Account Operators] rid:[0x224] group:[Pre-Windows 2000 Compatible Access] rid:[0x22a] group:[Incoming Forest Trust Builders] rid:[0x22d] group:[Windows Authorization Access Group] rid:[0x230] group:[Terminal Server License Servers] rid:[0x231] group:[Administrators] rid:[0x220] group:[Users] rid:[0x221] group:[Guests] rid:[0x222] group:[Print Operators] rid:[0x226] group:[Backup Operators] rid:[0x227] group:[Replicator] rid:[0x228] group:[Remote Desktop Users] rid:[0x22b] group:[Network Configuration Operators] rid:[0x22c] group:[Performance Monitor Users] rid:[0x22e] group:[Performance Log Users] rid:[0x22f] group:[Distributed COM Users] rid:[0x232] group:[IIS_IUSRS] rid:[0x238] group:[Cryptographic Operators] rid:[0x239]

## Shares (10.10.1.22)

Share Enumeration on 10.10.1.22					
	Sharename	Type	Comment	Scope	Protocol
111/tcp	ADMIN\$	rpcbind	Disk	2-4	Remote Admin
	rpcsvc	C\$	Disk		Default share
	IPC\$	prog\$	IPC/proto		Remote IPC
	NETLOGON	version			
100003/tcp	1		Disk/tcp	Logon server	share
100003/tcp6	3,4		Disk/tcp6	Logon server	share
100003/udp	3,4	Users	Disk/udp		rpcbind
100003/udp	3,4				nfs
SMB1 disabled -- no workgroup available					
[+] Attempting to map shares on 10.10.1.22					
//10.10.1.22/ADMIN\$ Mapping: DENIED, Listing: N/A					
//10.10.1.22/C\$ Mapping: DENIED, Listing: N/A					
//10.10.1.22/IPC\$ [E] Can't understand response:					
NT_STATUS_INVALID_INFO_CLASS listing \*					
//10.10.1.22/NETLOGON Mapping: OK, Listing: OK					
//10.10.1.22/SYSVOL Mapping: OK, Listing: OK					
//10.10.1.22/Users Mapping: OK, Listing: OK					
enum4linux complete on Thu Feb 15 15:52:17 2024					
	100021	1,2,3,4	2049/udp		nlockmgr
	100021	1,2,3,4	2049/udp		uapo nlockmqr

### Reflection

This project provided valuable hands-on experience with various enumeration techniques essential for ethical hacking and penetration testing. I developed a deeper understanding of how to effectively gather and analyze information from a target network, which is crucial for identifying potential security weaknesses.