

Lab #3: Enumeration

Course Name: Ethical Hacking and Offensive Security(HOD401)

Student Name: Nguyễn Trần Vinh – SE160258

Instructor Name: Mai Hoàng Đình

Lab Due Date: 20/09/2023

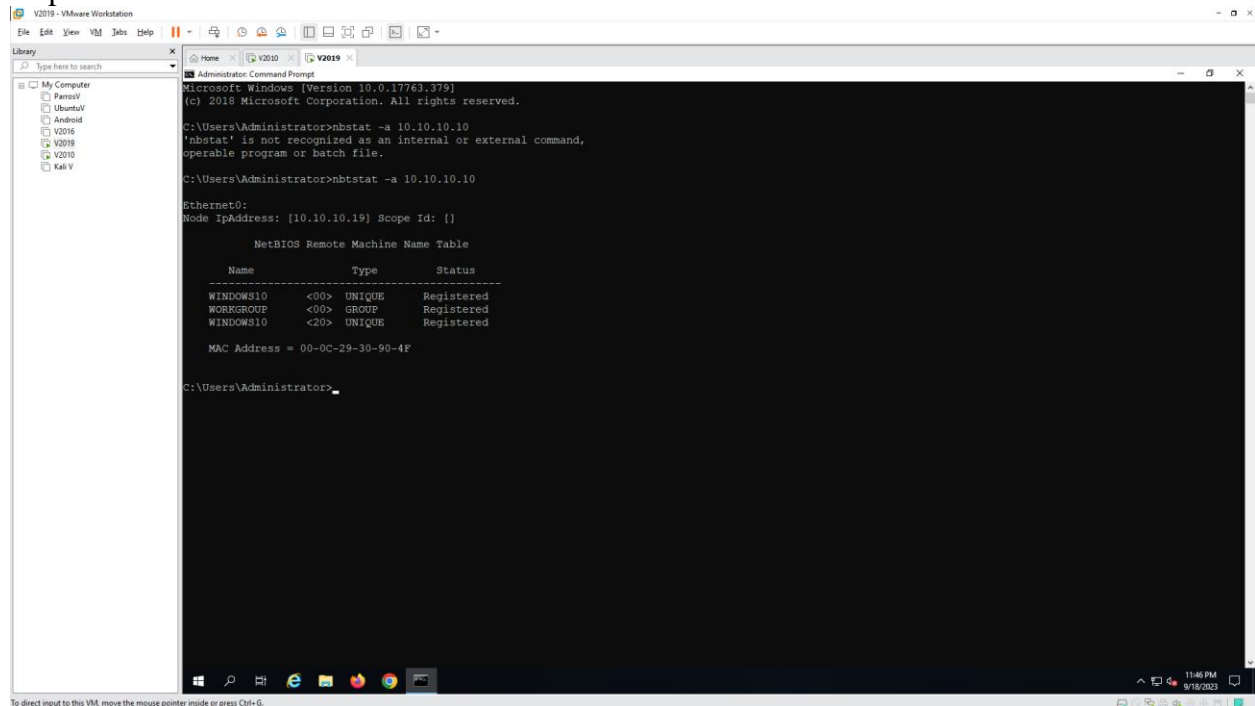
Lab Tasks

1. Perform NetBIOS Enumeration

1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities

- Open Windows 2010 and Windows Server 2019

- Open cmd



```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.10.10
'nbtstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>nbtstat -a 10.10.10.10

Ethernet0:
Node IpAddress: [10.10.10.19] Scope Id: {}

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    WINDOWS10            <00>             UNIQUE         Registered
    WORKGROUP             <00>             GROUP          Registered
    WINDOWS10            <20>             UNIQUE         Registered

    MAC Address = 00-0C-29-30-90-4F

C:\Users\Administrator>
```

Administrator Command Prompt

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbstat -a 10.10.10.10
'nbstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>nbstat -a 10.10.10.10

Ethernet0:
Node IpAddress: [10.10.10.19] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
WINDOWS10           <00> UNIQUE         Registered
WORKGROUP            <00> GROUP          Registered
WINDOWS10           <20> UNIQUE         Registered

MAC Address = 00-0C-29-30-90-4F

C:\Users\Administrator>nbstat -c

Ethernet0:
Node IpAddress: [10.10.10.19] Scope Id: []

NetBIOS Remote Cache Name Table

Name                Type                Host Address    Life [sec]
-----
WINDOWS10           <20> UNIQUE         10.10.10.10     507

C:\Users\Administrator>
```

Administrator Command Prompt

```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbstat -a 10.10.10.10
'nbstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>nbstat -a 10.10.10.10

Ethernet0:
Node IpAddress: [10.10.10.19] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
WINDOWS10           <00> UNIQUE         Registered
WORKGROUP            <00> GROUP          Registered
WINDOWS10           <20> UNIQUE         Registered

MAC Address = 00-0C-29-30-90-4F

C:\Users\Administrator>nbstat -c

Ethernet0:
Node IpAddress: [10.10.10.19] Scope Id: []

NetBIOS Remote Cache Name Table

Name                Type                Host Address    Life [sec]
-----
WINDOWS10           <20> UNIQUE         10.10.10.10     507

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

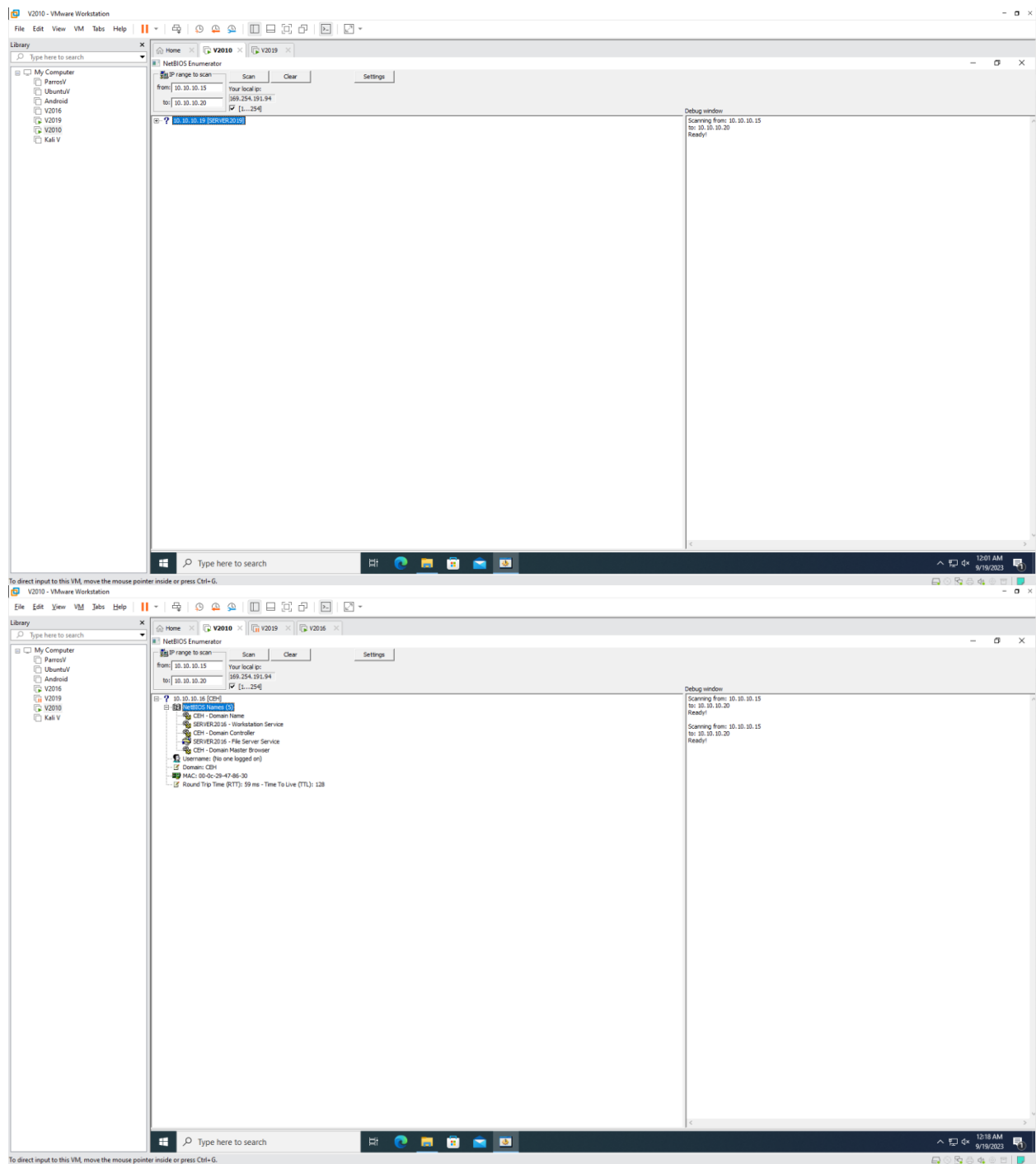
Status      Local      Remote              Network
-----
OK          2:         \\WINDOWS10\CEH-Tools  Microsoft Windows Network

The command completed successfully.

C:\Users\Administrator>
```

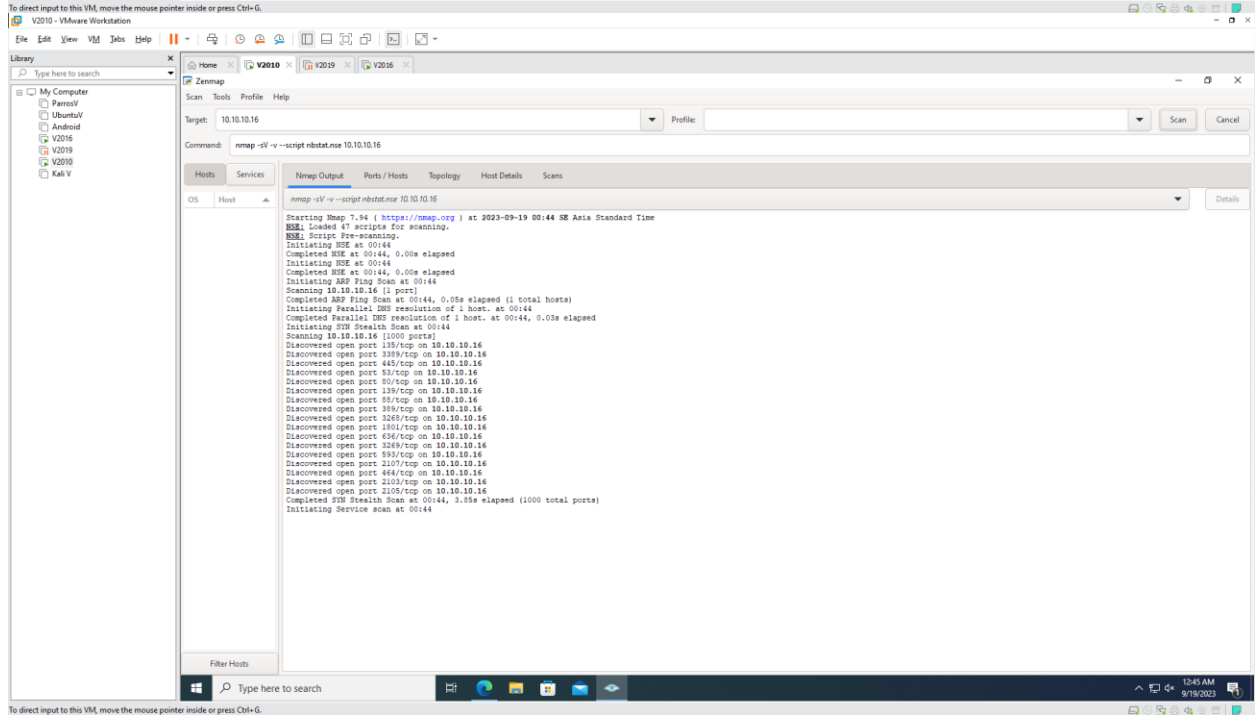
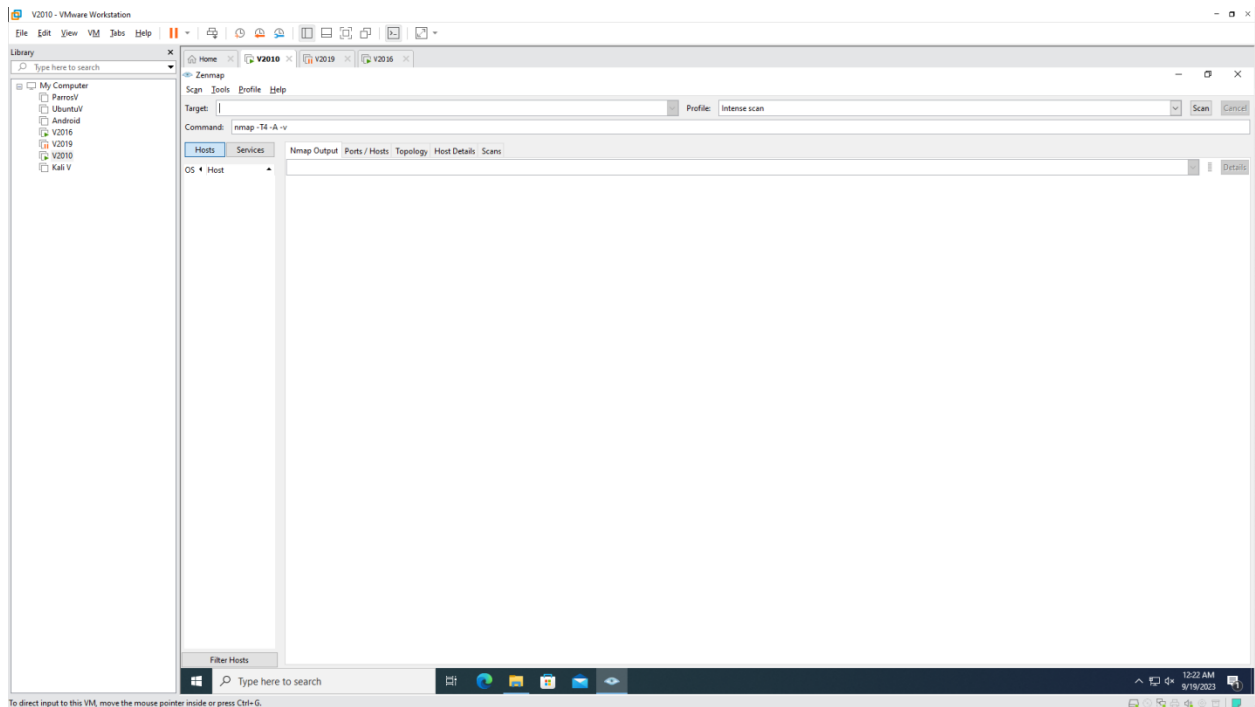
1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator

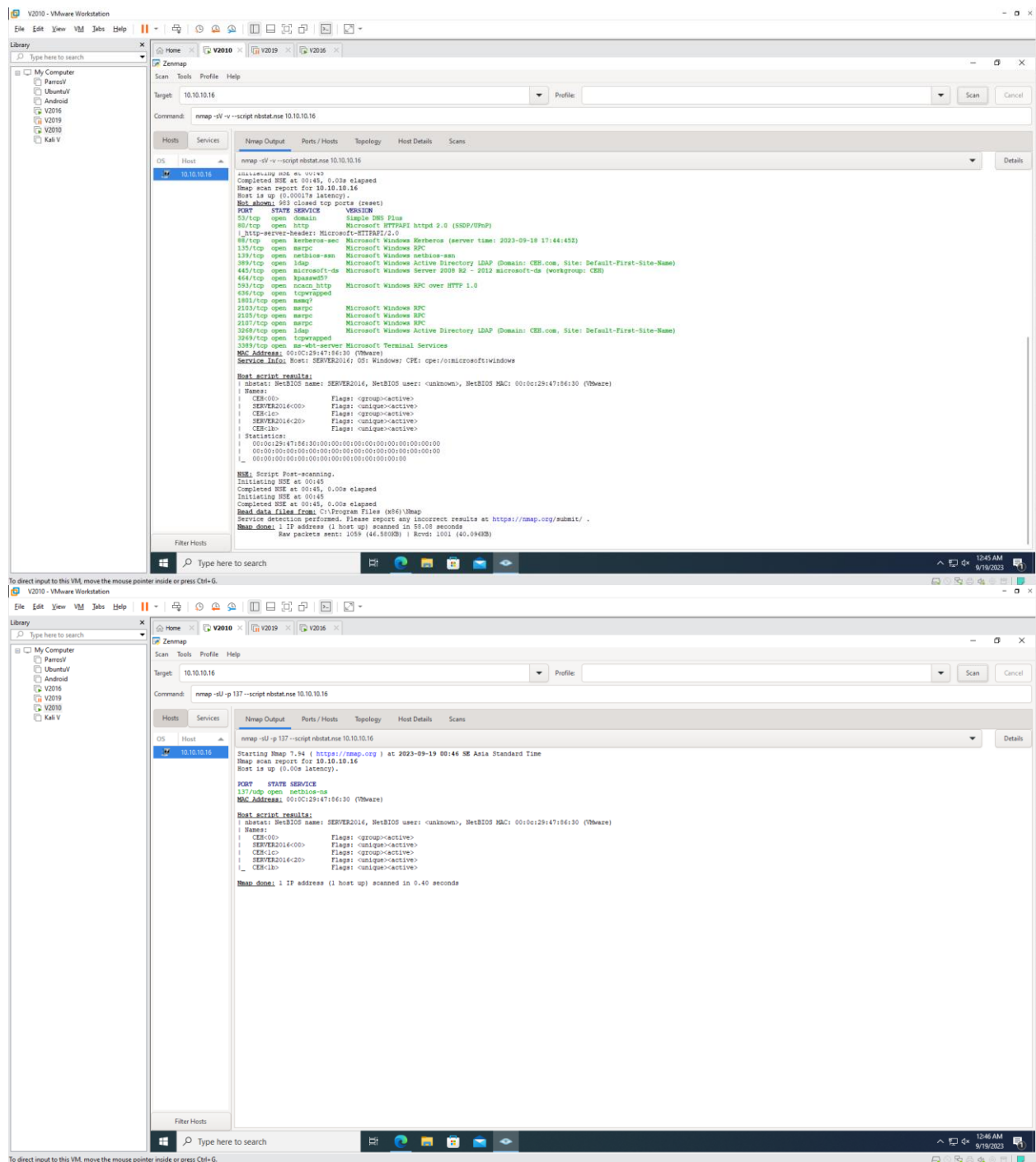
- Open Windows 2010, Windows Server 2016, 2019
- Install Enumerator.exe



1.3 Perform NetBIOS Enumeration using NSE Script

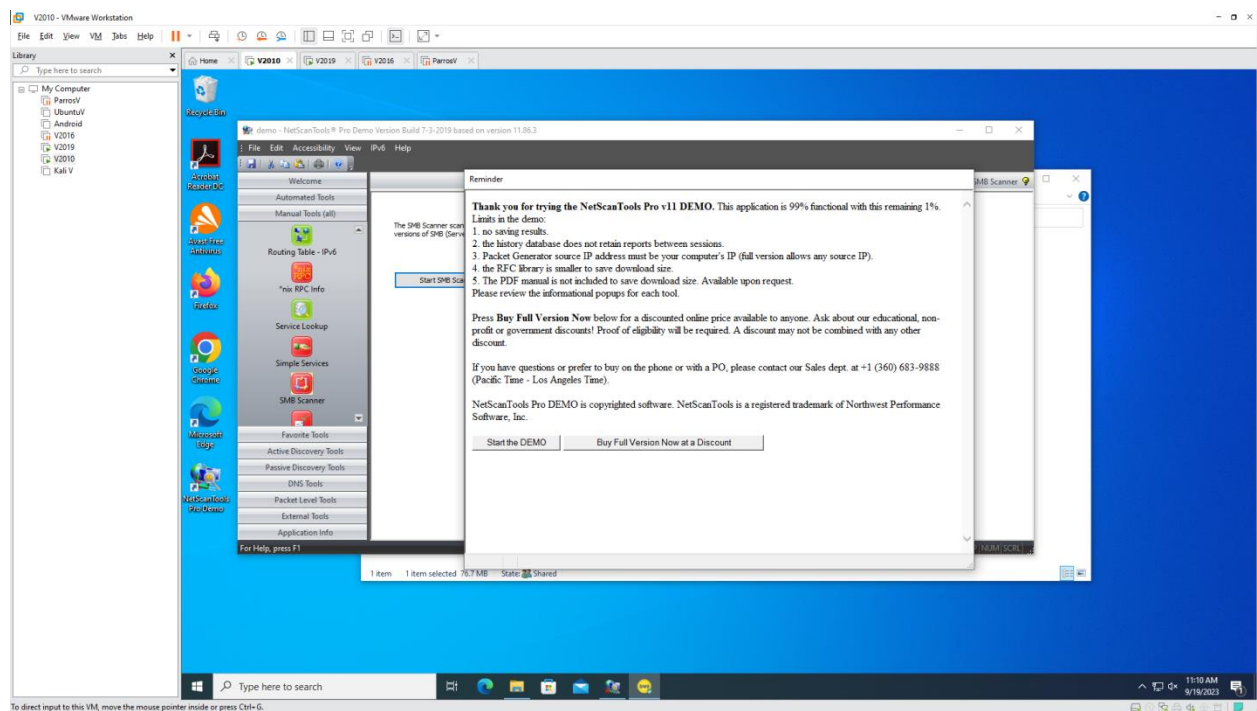
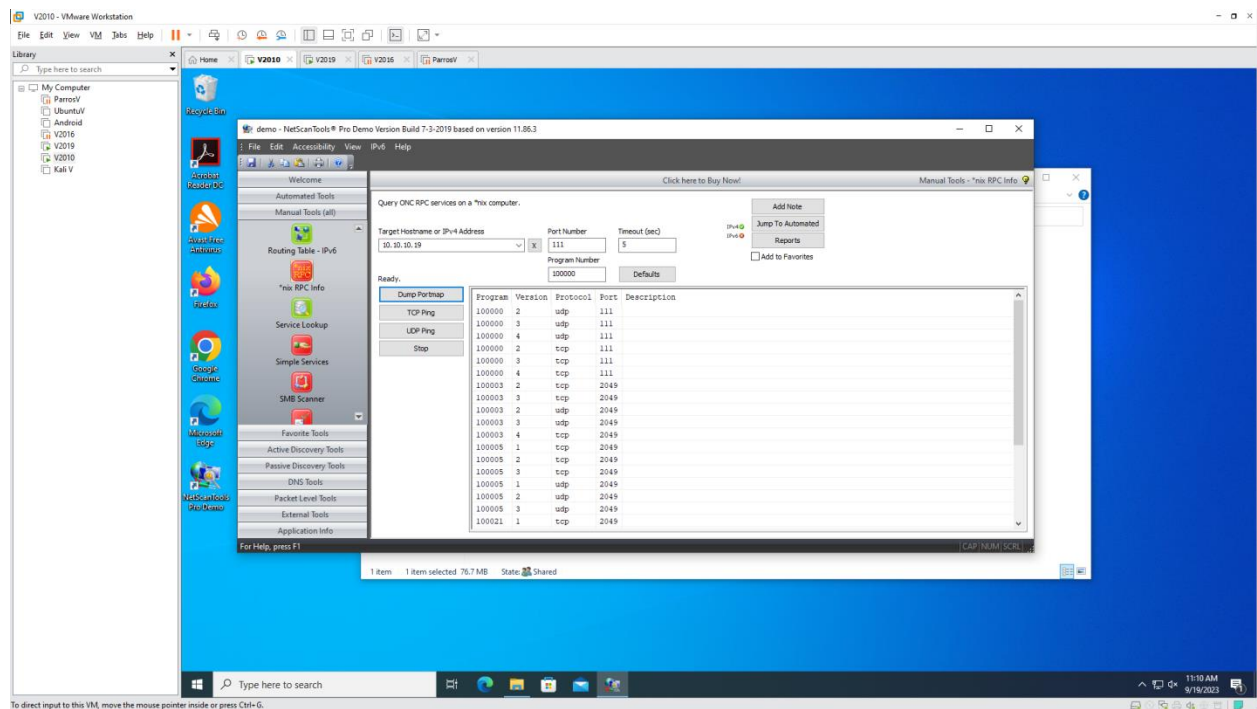
- Open Windows 2010
- Open Zenmap

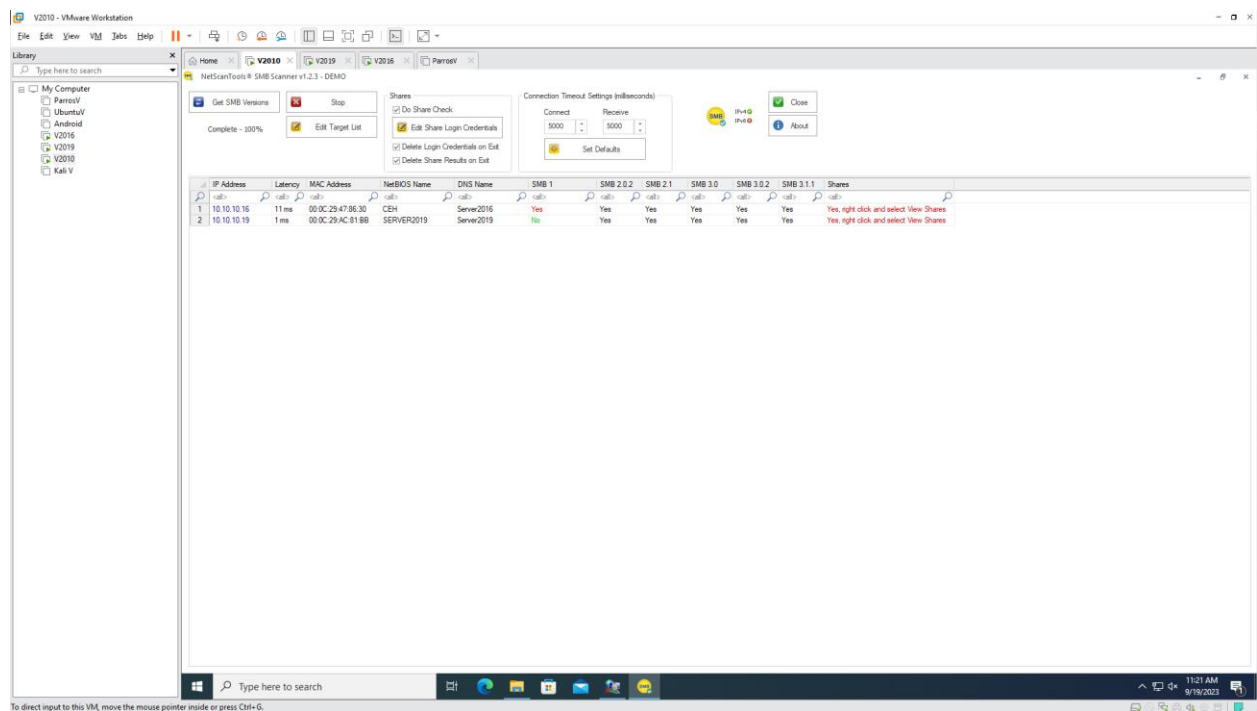
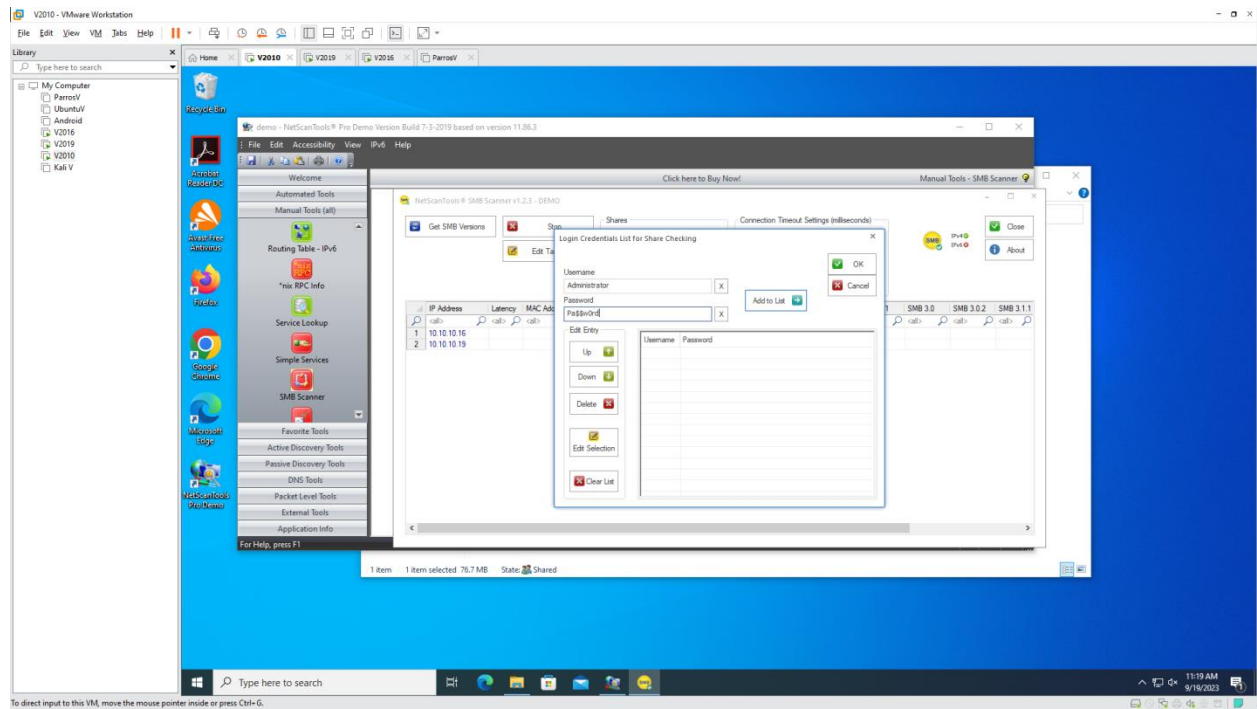


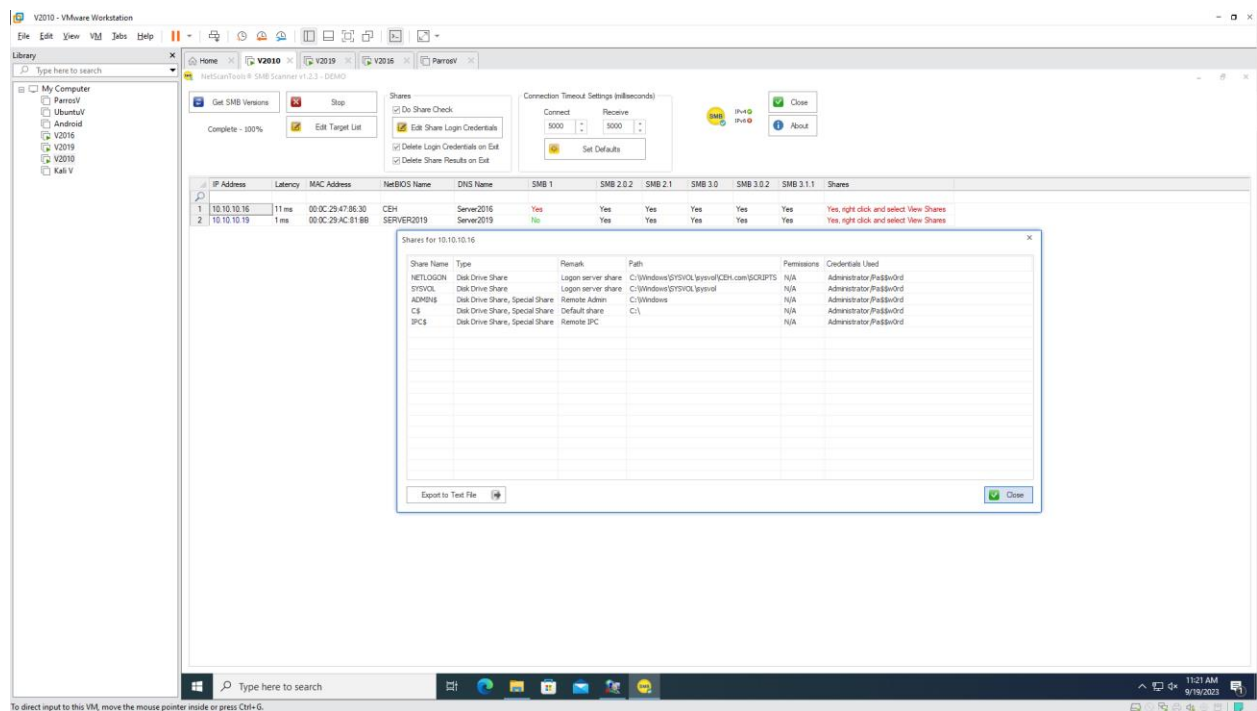
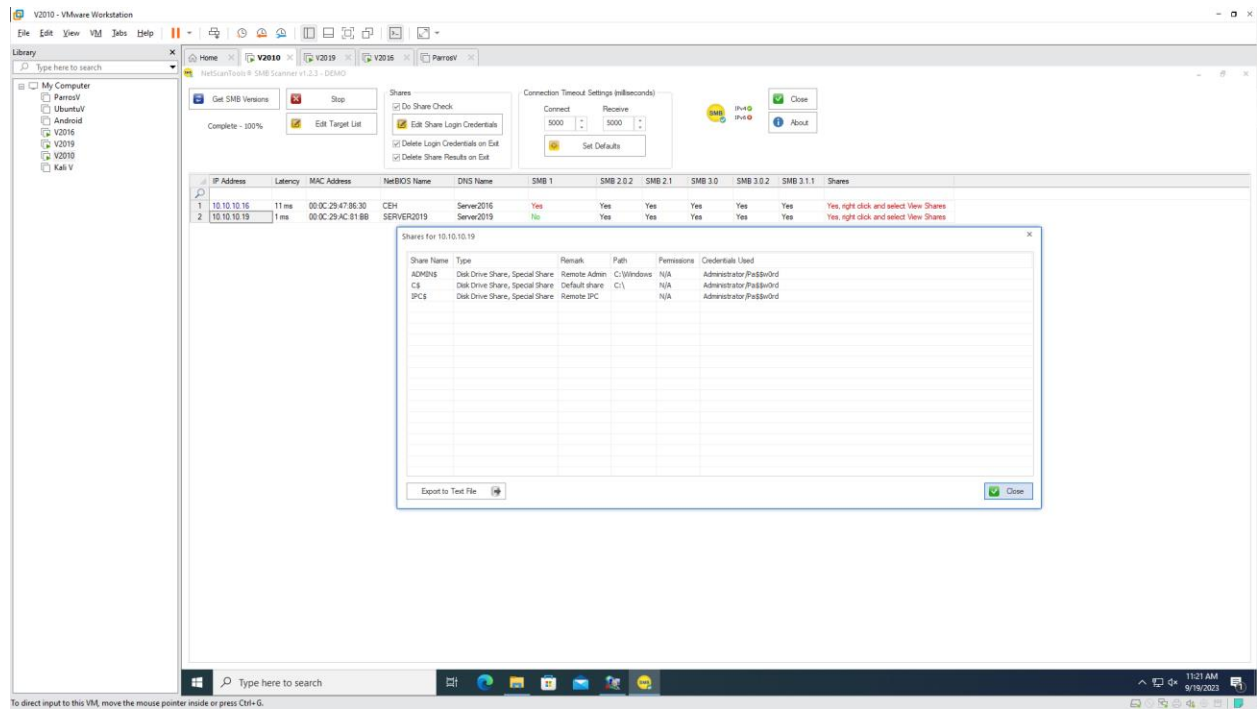


6. Perform RPC, SMB and FTP Enumeration

6.1 Perform RPC, SMB Enumeration using NetScanTools Pro - Open Windows 2010, Windows Server 2016, 2019

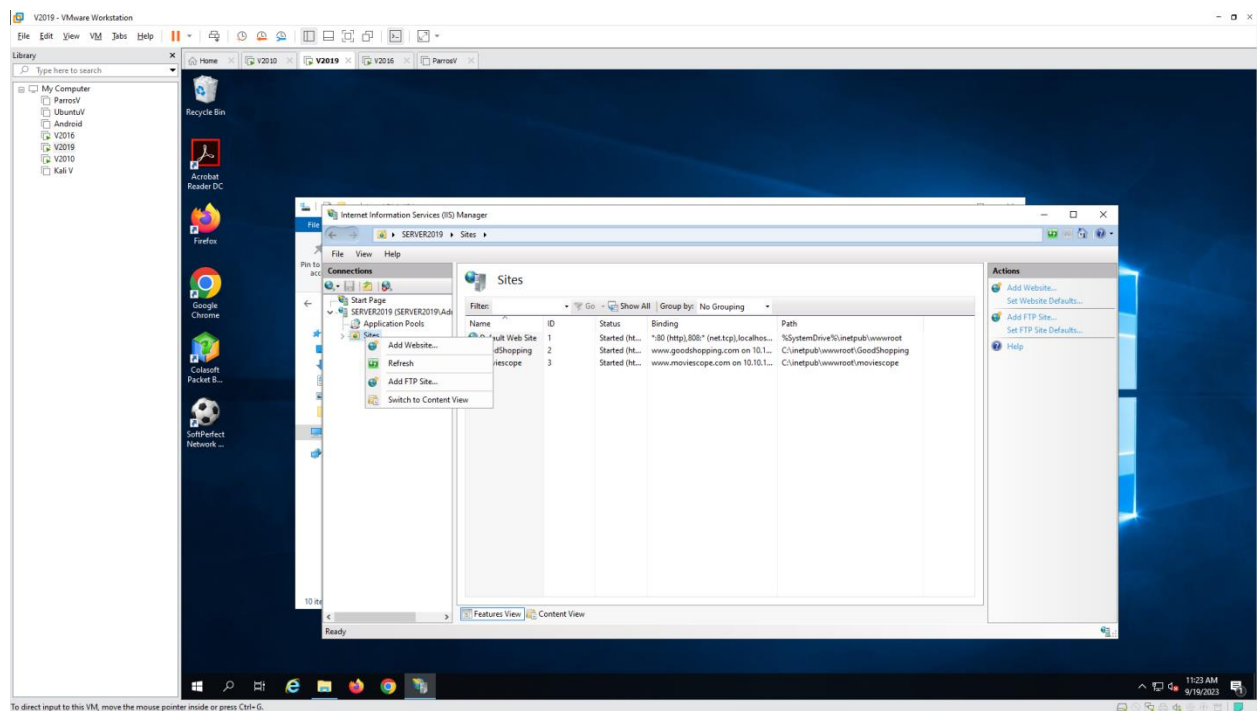
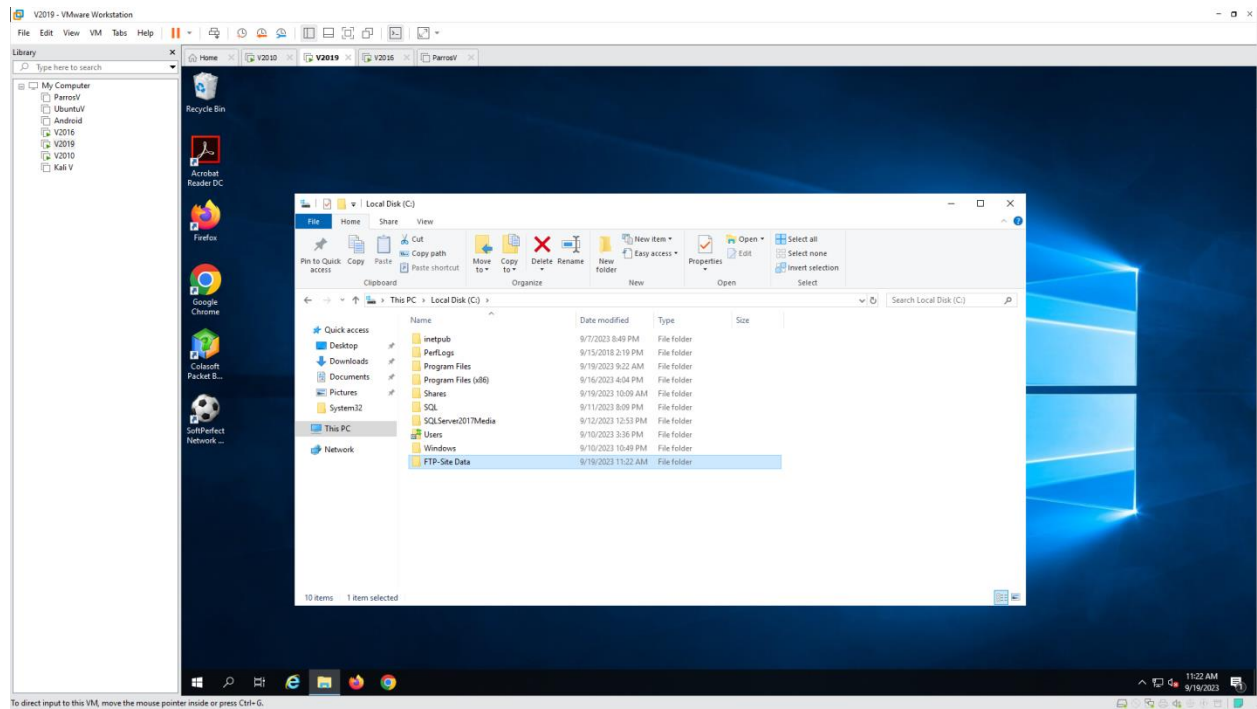


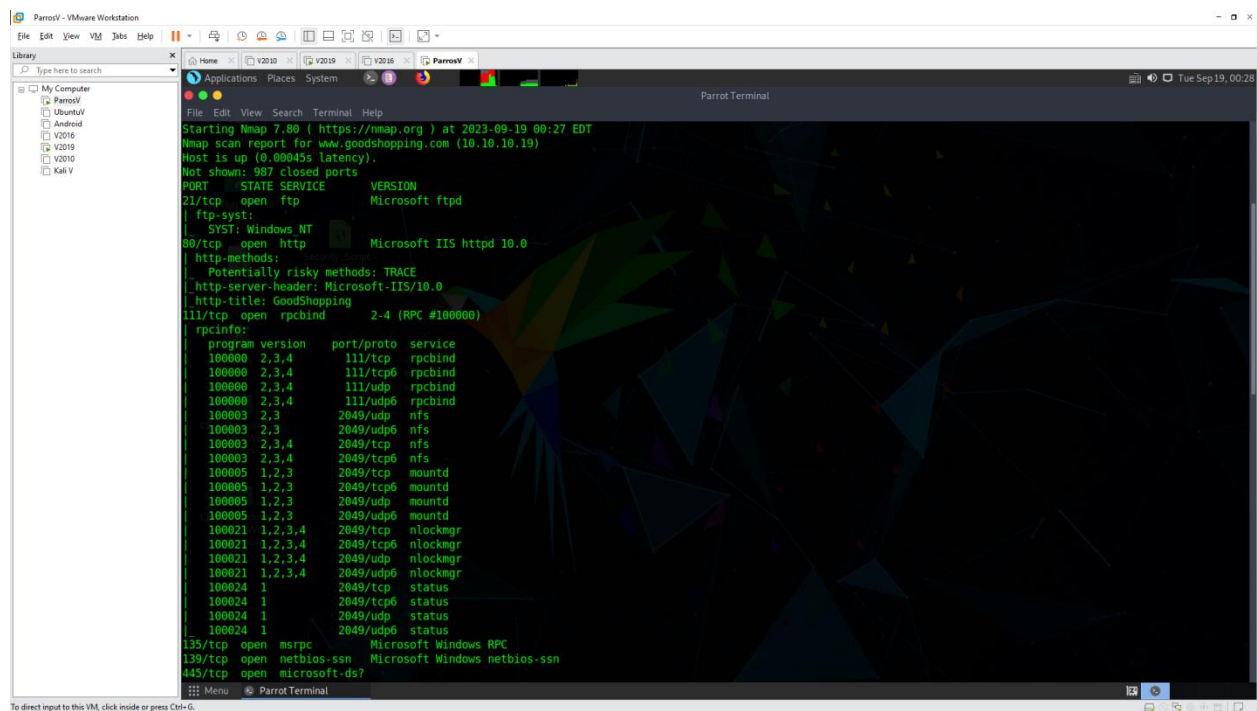
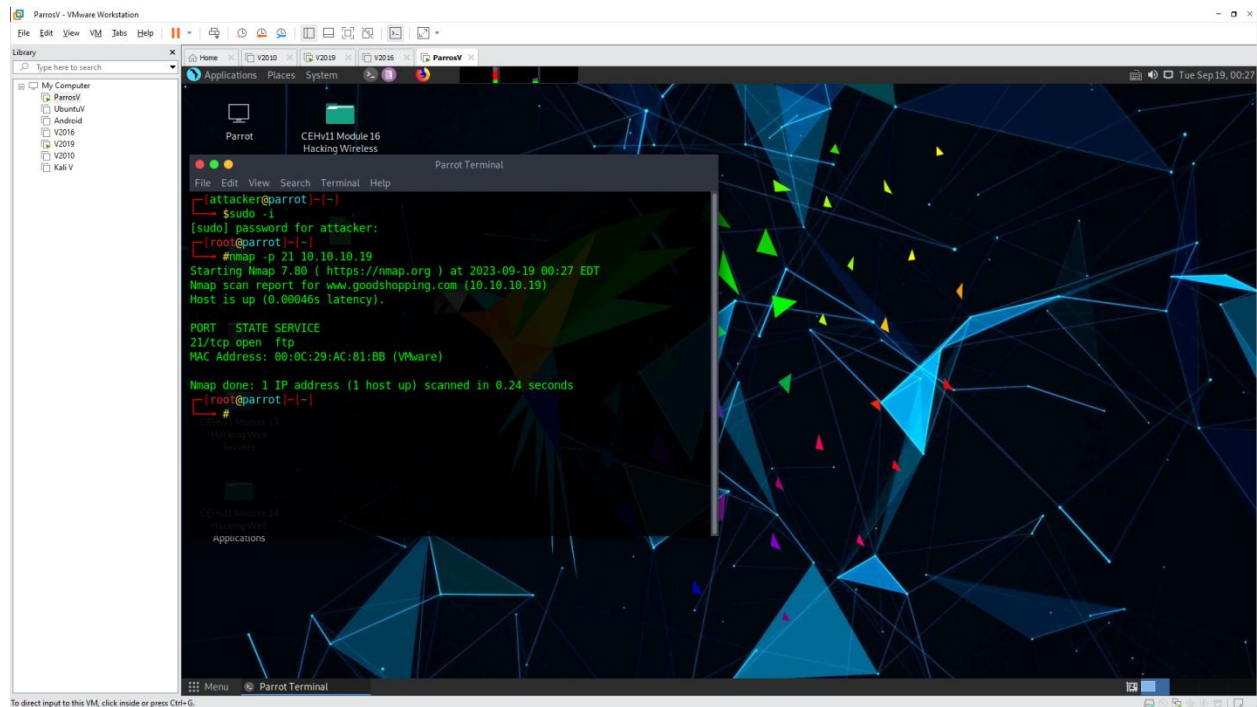




6.2 Perform RPC, SMB, and FTP Enumeration using Nmap

- Open Windows Server 2019






```
ParrotV - VMware Workstation
File Edit View VM Help
Library
Type here to search
My Computer
ParrotV
UbuntuV
Android
V2016
V2019
V2010
Kali V
Parrot Terminal
File Edit View Search Terminal Help
HOP RTT ADDRESS
1 0.45 ms www.goodshopping.com (10.10.10.19)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.88 seconds
[root@parrot:~]# nmap -p 445 -A 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-19 00:29 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00045s latency).

PORT      STATE SERVICE VERSION
445/tcp   open  microsoft-ds?
MAC Address: 00:0C:29:AC:81:BB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 (92%), 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 Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows 10 1511 (90%), Microsoft Windows Server 2008 SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_ clock-skew: 1s
|_ nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 00:0C:29:AC:81:BB (VMware)
|_ smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2023-09-19T04:29:17
|   start date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 0.46 ms www.goodshopping.com (10.10.10.19)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
[root@parrot:~]#
```

To direct input to this VM, click inside or press Ctrl-G.

```
ParrotV - VMware Workstation
File Edit View VM Help
Library
Type here to search
My Computer
ParrotV
UbuntuV
Android
V2016
V2019
V2010
Kali V
Parrot Terminal
File Edit View Search Terminal Help
2.02:
|_ Message signing enabled but not required
|_ smb2-time:
|   date: 2023-09-19T04:29:17
|   start date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 0.46 ms www.goodshopping.com (10.10.10.19)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
[root@parrot:~]# nmap -p 21 -A 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-19 00:29 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
|_ ftp-syst:
|   SYST: Windows NT
MAC Address: 00:0C:29:AC:81:BB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 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 Server 2012 R2 (91%), Microsoft Windows 10 1511 (90%), Microsoft Windows Server 2008 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT ADDRESS
1 0.49 ms www.goodshopping.com (10.10.10.19)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds
[root@parrot:~]#
```

To direct input to this VM, click inside or press Ctrl-G.

