

Lab 2: Perform SNMP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner

Overview of SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Task 1: Perform SNMP Enumeration using snmp-check

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is "public." As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

Here, we will use the snmp-check tool to perform SNMP enumeration on the target IP address

We will use a **Parrot Security** (10.10.10.13) machine to target a **Windows Server 2016** (10.10.10.16) machine.

1. ☐ Click [Parrot Security](#) to switch to the **Parrot Security** machine.

parrot

🌐 us 00:33 🔌

attacker



Password



2. ☐ In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.


If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

parrot

us 00:34

attacker



3.  Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Before starting SNMP enumeration, we must first discover whether the SNMP port is open. SNMP uses port 161 by default; to check whether this port is opened, we will first run Nmap port scan.



Parrot



CEHv11 Module 16
Hacking Wireless
Networks



attacker's Home



Security_Script.-
html



README.license



Trash



CEHv11 Module 13
Hacking Web
Servers



CEHv11 Module 14
Hacking Web
Applications



4. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

6. ☐ Now, type **cd** and press **Enter** to jump to the root directory.

File Edit View Search Terminal Help

```
[attacker@parrot]-[~] Module 16  
$sudo su  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#cd  
[root@parrot]-[~]  
#
```

READMElicense

Trash

CEHv11 Module 13
Hacking Web
Servers

CEHv11 Module 14
Hacking Web
Applications

Security_Script-
html

7. ☐ In the **Parrot Terminal** window, type **nmap -sU -p 161 [Target IP address]** (in this example, the target IP address is **10.10.10.16**) and press **Enter**.

-sU performs a UDP scan and **-p** specifies the port to be scanned.

8. ☐ The results appear, displaying that port 161 is **open/filtered** and being used by SNMP, as shown in the screenshot.

File Edit View Search Terminal Help

`[attacker@parrot]-[~] Module 16``$sudo su``[sudo] password for attacker:``[root@parrot]-[/home/attacker]``#cd``[root@parrot]-[~]``#nmap -sU -p 161 10.10.10.16``Starting Nmap 7.80 (https://nmap.org) at 2020-08-21 00:39 EDT``Nmap scan report for 10.10.10.16``Host is up (0.00029s latency).``README license`

PORT	STATE	SERVICE
------	-------	---------

161/udp	open filtered	snmp
---------	---------------	------

`MAC Address: 02:15:5D:08:11:75 (Unknown)``Trash``Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds``[root@parrot]-[~]``#``CEHv11 Module 13``Hacking Web
Servers``CEHv11 Module 14``Hacking Web
Applications`

9. ☐ We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. ☐ In the **Parrot Terminal** window, type **snmp-check [Target IP Address]** (in this example, the target IP address is **10.10.10.16**) and press **Enter**.
11. ☐ The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default "public" community string.

If the target machine does not have a valid account, no output will be displayed.

12. ☐ The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.

```
[root@parrot]-[~] #snmp-check 10.10.10.16
```

snmp-check v1.9 - SNMP enumerator

Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.16:161 using SNMPv1 and community 'public'

[*] System information:

```
Host IP address      : 10.10.10.16
Hostname             : Server2016.CEH.com
Description          : Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - S
oftware: Windows Version 6.3 (Build 14393 Multiprocessor Free)
Contact              : -
Location             : -
Uptime snmp          : 00:16:26.03
Uptime system        : 00:15:59.99
System date          : 2020-8-20 21:40:24.1
Domain               : CEH
```

[*] User accounts:

```
Guest
jason
krbtgt
martin
shiela
Administrator
DefaultAccount
```

13. ☐ Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections** and **listening ports**.

File Edit View Search Terminal Help

DefaultAccount

CEHv11 Module 16

Parrot

Hacking Wireless

works

[*] Network information:

```
IP forwarding enabled      : no
Default TTL                : 128
TCP segments received      : 56540
TCP segments sent          : 13061
TCP segments retrans       : 6
Input datagrams            : 51948
Delivered datagrams        : 52014
Output datagrams           : 8286
```

[*] Network interfaces:

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

```
Interface                  : [ down ] WAN Miniport (L2TP)
Id                          : 2
Mac Address                 : :::::
Type                       : unknown
Speed                      : 0 Mbps
MTU                         : 0
```

File Edit View Search Terminal Help

[*] Network IP:

Id	IP Address	Netmask	Broadcast
3	10.10.10.16	255.255.255.0	1
1	127.0.0.1	255.0.0.0	1

[*] Routing information:

Destination	Next hop	Mask	Metric
0.0.0.0	10.10.10.1	0.0.0.0	271
10.10.10.0	10.10.10.16	255.255.255.0	271
10.10.10.16	10.10.10.16	255.255.255.255	271
10.10.10.255	10.10.10.16	255.255.255.255	271
127.0.0.0	127.0.0.1	255.0.0.0	331
127.0.0.1	127.0.0.1	255.255.255.255	331
127.255.255.255	127.0.0.1	255.255.255.255	331
224.0.0.0	127.0.0.1	240.0.0.0	331
255.255.255.255	127.0.0.1	255.255.255.255	331

[*] TCP connections and listening ports:

Local address	Local port	Remote address	Remote port	State
0.0.0.0	80	0.0.0.0	0	listen
0.0.0.0	88	0.0.0.0	0	listen
0.0.0.0	135	0.0.0.0	0	listen
0.0.0.0	389	0.0.0.0	0	listen

14. ☐ Similarly, scrolling down reveals further sensitive information on **Processes**, **Storage information**, **File system information**, **Device information**, **Share**, etc.

File Edit View Search Terminal Help

[*] Processes:

Id	Status	Name	Path	Parameters
1	running	System Idle Process		
4	running	System		
252	running	svchost.exe	C:\Windows\system32\	-k LocalSer
264	running	smss.exe		
356	running	csrss.exe		
380	running	svchost.exe	C:\Windows\system32\	-k NetworkS
436	running	csrss.exe		
452	running	wininit.exe		
488	running	winlogon.exe		
552	running	services.exe		
560	running	lsass.exe	C:\Windows\system32\	
688	running	svchost.exe	C:\Windows\system32\	-k ICService
716	running	svchost.exe	C:\Windows\system32\	-k DcomLaun

[*] Storage information:

```
Description : ["A:\\"]
Device id : [#<SNMP::Integer:0x00005600254ef798 @value=1>]
Filesystem type : ["unknown"]
Device unit : [#<SNMP::Integer:0x00005600254e7458 @value=0>]
Memory size : 0 bytes
Memory used : 0 bytes

Description : ["C:\\ Label: Serial Number fe46261c"]
Device id : [#<SNMP::Integer:0x000056002552a708 @value=2>]
Filesystem type : ["unknown"]
Device unit : [#<SNMP::Integer:0x0000560025525f78 @value=4096>]
Memory size : 79.51 GB
Memory used : 22.80 GB

Description : ["D:\\"]
Device id : [#<SNMP::Integer:0x0000560025393b38 @value=3>]
Filesystem type : ["unknown"]
Device unit : [#<SNMP::Integer:0x0000560025363050 @value=0>]
Memory size : 0 bytes
Memory used : 0 bytes

Description : ["Virtual Memory"]
Device id : [#<SNMP::Integer:0x00005600252af550 @value=4>]
Filesystem type : ["unknown"]
Device unit : [#<SNMP::Integer:0x00005600252502f8 @value=65536>]
Memory size : 4.69 GB
```


File Edit View Search Terminal Help

[*] File system information:

Index : 1
Mount point :
Remote mount point : -
Access : 1
Bootable : 0

[*] Device information:

Id	Type	Status	Descr
1	unknown	running	Microsoft XPS Document Writer v4
2	unknown	running	Microsoft Print To PDF
3	unknown	running	Unknown Processor Type
4	unknown	unknown	Software Loopback Interface 1
5	unknown	unknown	WAN Miniport (L2TP)
6	unknown	unknown	Microsoft Hyper-V Network Adapter
#2			
7	unknown	unknown	Microsoft ISATAP Adapter #2
8	unknown	unknown	Microsoft ISATAP Adapter
9	unknown	unknown	WAN Miniport (GRE)
10	unknown	unknown	WAN Miniport (IKEv2)
11	unknown	unknown	WAN Miniport (IP)
12	unknown	unknown	WAN Miniport (Network Monitor)
13	unknown	unknown	WAN Miniport (PPPOE)
14	unknown	unknown	WAN Miniport (IPv6)
15	unknown	unknown	Microsoft Hyper-V Network Adapter
16	unknown	unknown	Microsoft Kernel Debug Network Ad

File Edit View Search Terminal Help

```
MaxNonAnonymousUsers : 0
CurrentConnections : 0
MaxConnections : 0
ConnectionAttempts : 0
LogonAttempts : 0
Gets : 0
Posts : 0
Heads : 0
Others : 0
CGIRequests : 0
BGIRRequests : 0
NotFoundErrors : 0
```

[*] Share:

```
Name : Users
Path : C:\Users
Comment :
```

```
Name : SYSVOL
Path : C:\Windows\SYSVOL\sysvol
Comment : Logon server share
```

```
Name : NETLOGON
Path : C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS
Comment : Logon server share
```

```
[root@parrot]-[~]
#
```

15. ☐ This concludes the demonstration of performing SNMP enumeration using the snmp-check.
 16. ☐ Close all open windows and document all the acquired information.
-

Task 2: Perform SNMP Enumeration using SoftPerfect Network Scanner

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell.

The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and display options, and can export the NetScan results to a variety of formats, from XML to JSON. In addition, it supports remote shutdown and Wake-On-LAN.

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

1. ☐ Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.
2. ☐ Navigate to **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

If a **User Account Control** pop-up appears, click **Yes**.

3. ☐ When the **Setup - SoftPerfect Network Scanner** window appears, click **Next** and follow the installation steps to install SoftPerfect Network Scanner, using all default settings.
4. ☐ On completion of the installation, click **Finish**.

Ensure that the **Launch SoftPerfect Network Scanner option** is selected.

← → ↕ ↑ This PC > CEH-Tools (\\WINDOWS10) (Z:) > CEHv11 Module 04 Enumeration > SNMP Enumeration Tools > SoftPerfect Network Scanner

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND
- Network

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB



5.  When the **Welcome to the Network Scanner** wizard appears, click **Continue**.

← → ↕ ↑ > This PC > CEH-Tools (\\WINDOWS10) (Z:) > CEHv11 Module 04 Enumeration > SNMP Enumeration Tools > SoftPerfect Network Scanner

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND
- Network

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

SoftPerfect Network Scanner

File View Actions Options Bookmarks Help

IPv4 From

0 . 0 . 0 . 0

To

0 . 0 . 0 . 0

+

×

↶


↷

☑

Start Scanning

IP Address

MA



Welcome to the Network Scanner!
SoftPerfect Network Scanner is a versatile administration tool.
It is now available as a free trial.

The trial version displays a maximum of 10 devices. To
remove this limitation, you need to purchase a licence, which
will also give you 1 year of free updates.

English

▼

Continue

Purchase a licence

Ready

Threads

Devices 0 / 0

Scan

6.  The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

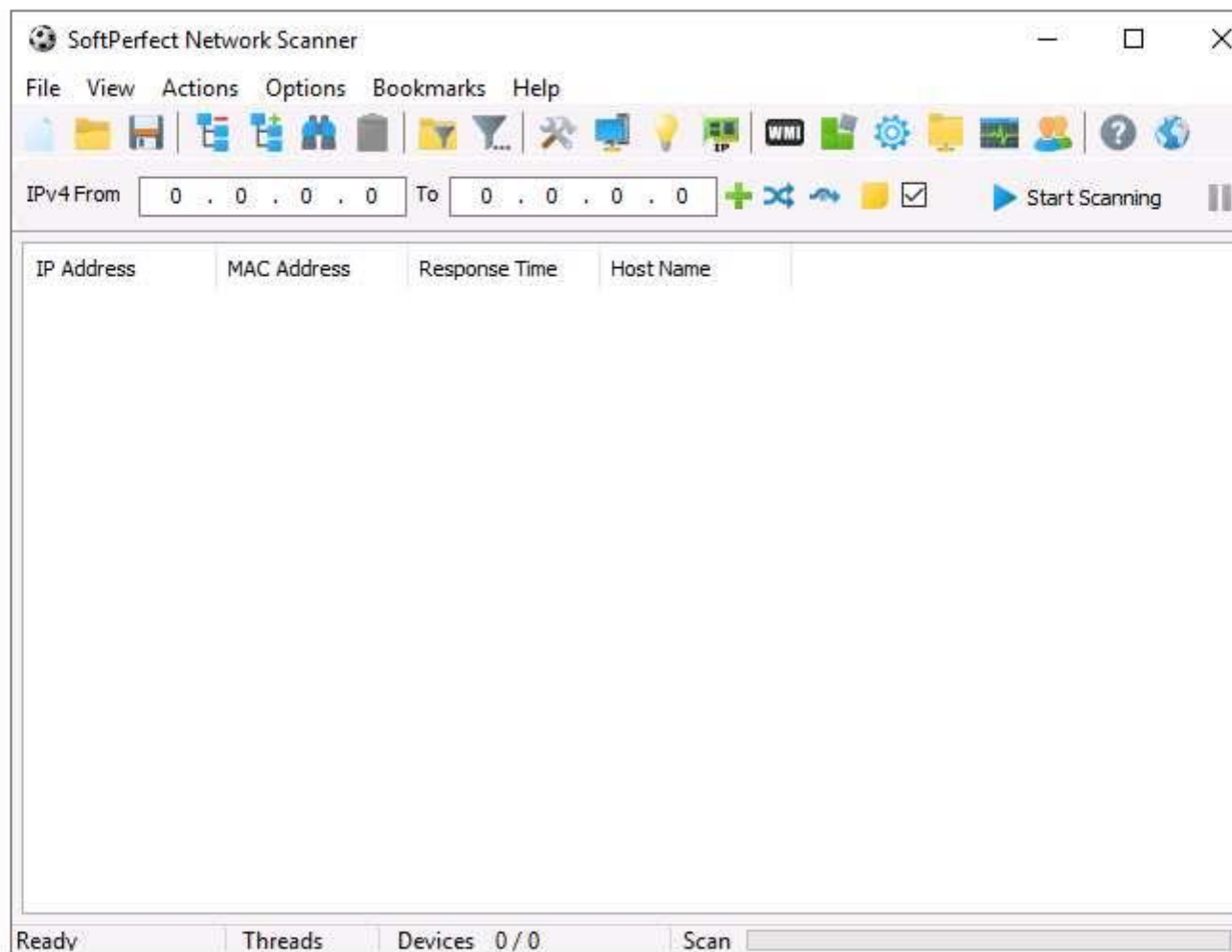
Name	Date modified	Type	Size
15 nmap_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS
- System32

 This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND
- Network



7. ☐ In the **Options** menu, click **Remote SNMP....** The **SNMP** pop-up window will appear.
8. ☐ Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

9. ☐ To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.10.5-10.10.10.20**), and click the **Start Scanning** button.

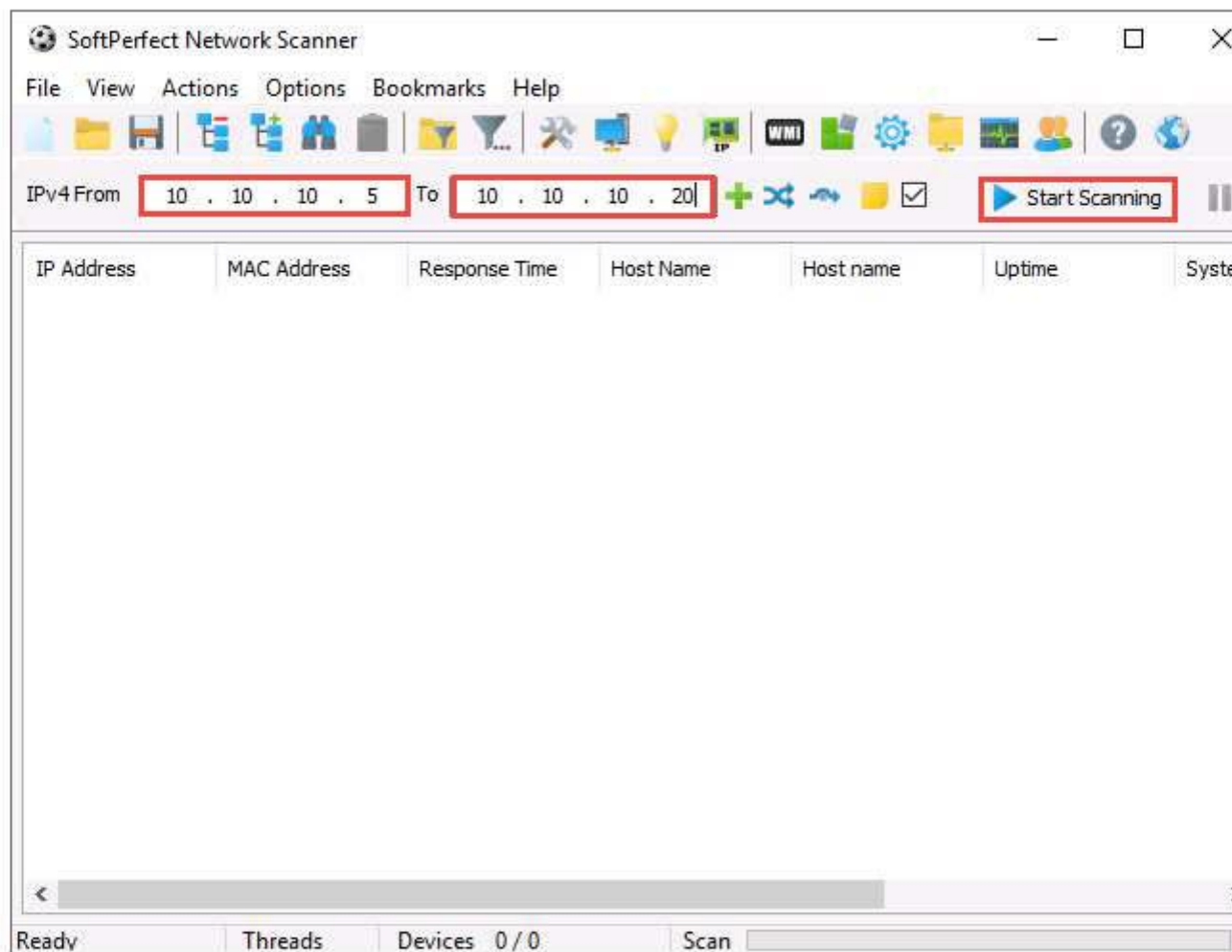
Name	Date modified	Type	Size
15 nescan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS...
- System32

 This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\WIND
- Network



10. ☐ The **status bar** at the lower-right corner of the GUI displays the status of the scan.
11. ☐ The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.



File Home Share View **Manage** Application Tools

SoftPerfect Network Scanner

← → ↕ ↑ > This PC > CEH-Tools (\\WINDOWS10 (Z:)) > CEHv11 Module 04 Enumeration > SNMP Enumeration Tools > SoftPerfect Network Scanner

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND**
- Network

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

SoftPerfect Network Scanner


File View Actions Options Bookmarks Help















IPv4 From 10 . 10 . 10 . 5 To 10 . 10 . 10 . 20 + - Start Scanning

IP Address	MAC Address	Response Time	Host Name	Host name	Uptime
10.10.10.9	02-...	0 ms	ubuntu-Virtual-...		
10.10.10.10	02-...	0 ms	WINDOWS10		
10.10.10.13	02-...	0 ms			
10.10.10.14	02-...	0 ms	Android.local		
10.10.10.16	02-...	1 ms	SERVER2016	Server2016.CE...	510598 (0d 1h ...)
10.10.10.19	02-...	0 ms	www.goodshop...	Server2019	511519 (0d 1h ...)

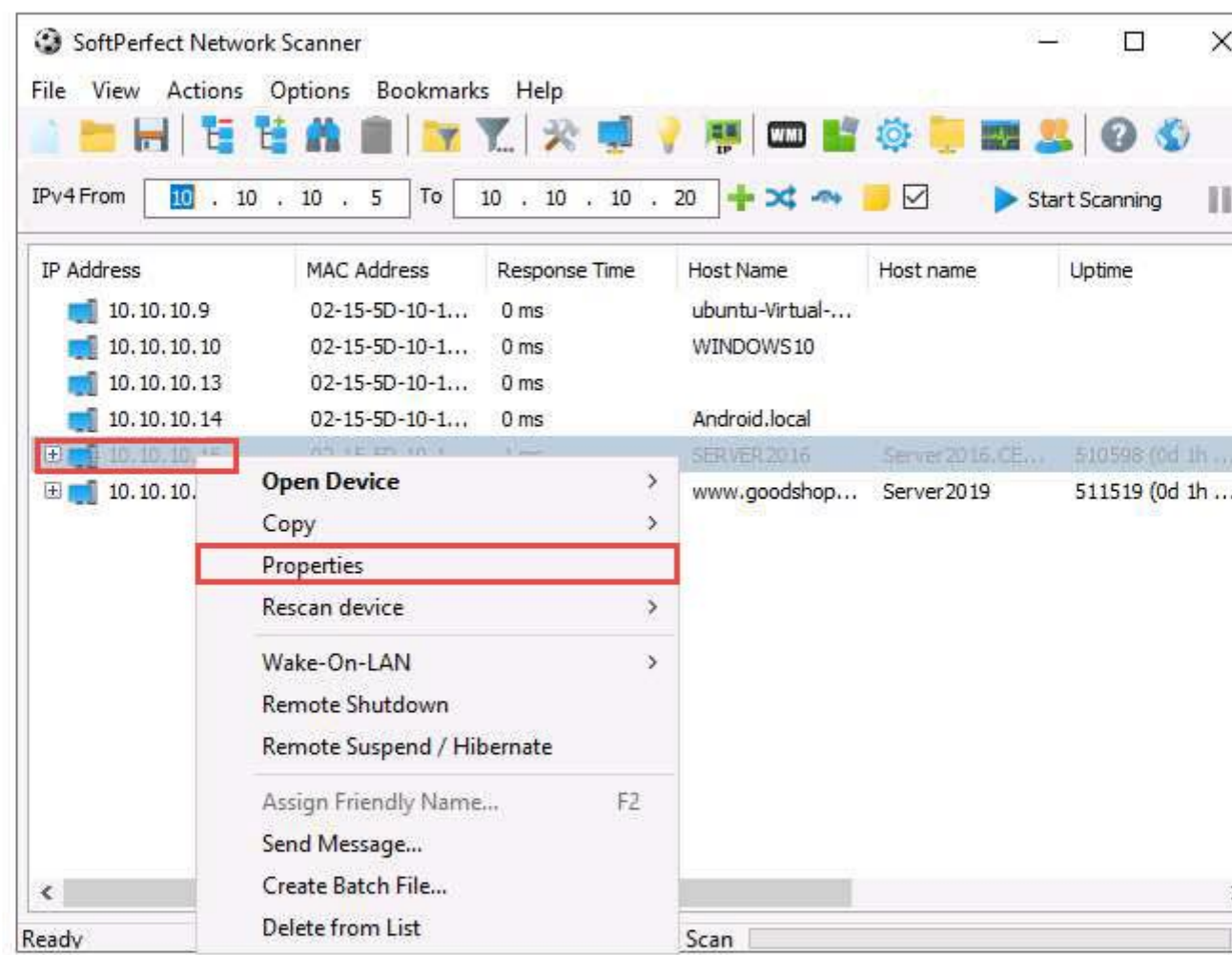
Ready Threads 0 Devices 6 / 6 Scan

12.  To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.10.16**) and select **Properties**, as shown in the screenshot.



-  This PC
-  3D Objects
-  Desktop
-  Documents
-  Downloads
-  Music
-  Pictures
-  Videos
-  Local Disk (C:)
-  DVD Drive (D:)
-  CEH-Tools (\\WIND
-  Network

Name	Date modified	Type	Size
15 netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB



13.  The **Properties** window appears, displaying the **Shared Resources** and **Basic Info** of the machine corresponding to the selected IP address.

← → ↕ ↑ > This PC > CEH-Tools (\\WINDOWS10) (Z:) > CEHv11 Module 04 Enumeration > SNMP Enumeration Tools > SoftPerfect Network Scanner

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND
- Network

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

Properties

Shared Resources

FoldersSYSVOL, NETLOGON, Users

Basic Info

IP address10.10.10.16

MAC address02- - - - -

Response Time1 ms

Host nameSERVER2016

Remote SNMP

Host nameServer2016.CEH.com

Uptime510598 (0d 1h 25m 5s)

System DescriptionHardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE...

System Contact

System Location

14. ☐ Close the **Properties** window.
15. ☐ To view the shared folders, note the scanned hosts that have a + node before them. Expand the node to view all the shared folders.

In this example, we are targeting the Windows Server 2016 machine (10.10.10.16).



File Home Share View **Manage** Application Tools

SoftPerfect Network Scanner

← → ↕ ↑ > This PC > CEH-Tools (\\WINDOWS10) (Z:) > CEHv11 Module 04 Enumeration > SNMP Enumeration Tools > SoftPerfect Network Scanner

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND
- Network

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

SoftPerfect Network Scanner


File View Actions Options Bookmarks Help



IPv4 From 10 . 10 . 10 . 5 To 10 . 10 . 10 . 20 + Start Scanning

IP Address	MAC Address	Response Time	Host Name	Host name	Upt
10.10.10.9	02-...	0 ms	ubuntu-Virtual-...		
10.10.10.10	02-...	1 ms	WINDOWS10		
10.10.10.13	02-...	1 ms			
10.10.10.14	02-...	1 ms	Android.local		
10.10.10.16	02-...	0 ms	SERVER.2016	Server2016.CE...	540
SYSVOL					
NETLOGON					
Users					
10.10.10.19	02-15-5D-10-1A-AC	0 ms	www.goodshop...	Server2019	541

Ready Threads 0 Devices 6 / 6 Scan

16.  Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine over HTTP, HTTPS, FTP, and Telnet.

Name	Date modified	Type	Size
netscan_setup.exe	10/13/2019 9:57 PM	Application	6,310 KB

★ Quick access

- Desktop
- Downloads
- Documents
- Pictures
- DVD Drive (D:) SSS_
- System32

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- DVD Drive (D:) SSS_
- CEH-Tools (\\WIND

Network

SoftPerfect Network Scanner

File View Actions Options Bookmarks Help

IPv4 From 10 . 10 . 10 . 5 To 10 . 10 . 10 . 20 + - Start Scanning

IP Address	MAC Address	Response Time	Host Name	Host name	Up
10.10.10.9	02-...	0 ms	ubuntu-Virtual-...		
10.10.10.10	02-...	1 ms	WINDOWS10		
10.10.10.13	02-...	1 ms			
10.10.10.14	02-...	1 ms	Android.local		
10.10.10.16					
SYSVOL					
NETLOGON					
Users					
10.10.10.19					

Open Device >

- Copy >
- Properties
- Rescan device >
- Wake-On-LAN >
- Remote Shutdown
- Remote Suspend / Hibernate
- Assign Friendly Name... F2
- Send Message...
- Create Batch File...
- Delete from List

As Web (HTTP)

As Secure Web (HTTPS)

As File Server (FTP)

As Telnet

As Telnet to...

Computer Management Ctrl+M

Remote Desktop Ctrl+R

Ready Th

If the selected host is not secure enough, you may use these options to connect to the remote machines. You may also be able to perform activities such as sending a message and shutting down a computer remotely. These features are applicable only if the selected machine has a poor security configuration.

17. ☐ This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
18. ☐ You can also use other SNMP enumeration tools such as **Network Performance Monitor** (<https://www.solarwinds.com>), **OpUtils** (<https://www.manageengine.com>), **PRTG Network Monitor** (<https://www.paessler.com>), **Engineer's Toolset** (<https://www.solarwinds.com>), and **WhatsUp® Gold** (<https://www.ipswitch.com>) to perform SNMP enumeration on the target network.
19. ☐ Close all open windows and document all the acquired information.