Lab 6: Perform RPC, SMB, and FTP Enumeration

Lab Scenario

As an ethical hacker or penetration tester, you should use different enumeration techniques to obtain as much information as possible about the systems in the target network. This lab will demonstrate various techniques for extracting detailed information that can be used to exploit underlying vulnerabilities in target systems, and to launch further attacks.

Lab Objectives

- Perform SMB enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Overview of Other Enumeration Techniques

Besides the methods of enumeration covered so far (NetBIOS, SNMP, LDAP, NFS, and DNS), various other techniques such as RPC, SMB, and FTP enumeration can be used to extract detailed network information about the target.

- **RPC Enumeration**: Enumerating RPC endpoints enables vulnerable services on these service ports to be identified
- **SMB Enumeration**: Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running
- **FTP Enumeration**: Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Task 1: Perform SMB Enumeration using NetScanTools Pro

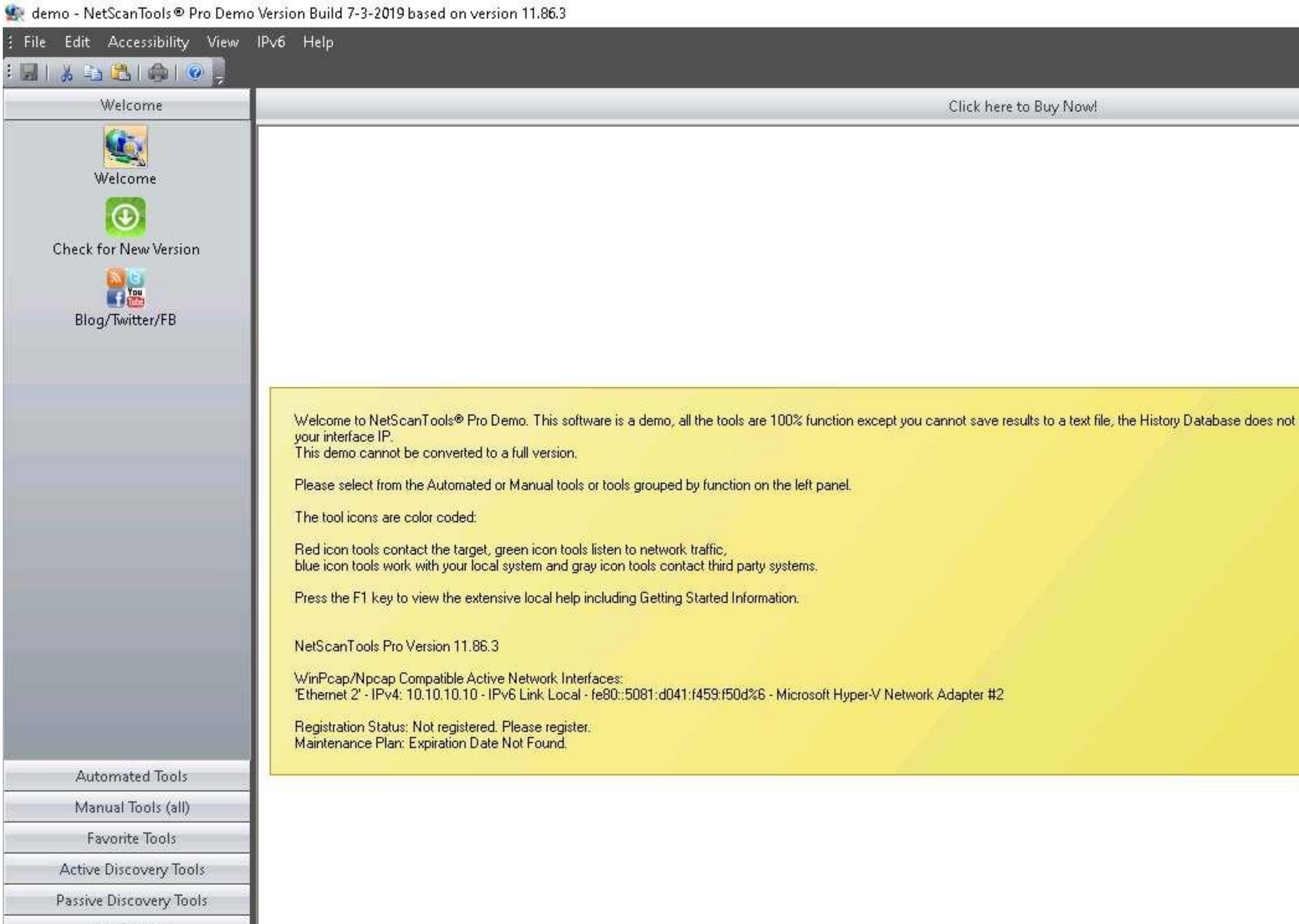
NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

Here, we will use the NetScanTools Pro tool to perform SMB enumeration.

1. □ Click Windows 10 to switch to the **Windows 10** machine.
2. □ Double-click the **NetScanTools Pro Demo** icon from **Desktop** to launch the tool.

If the **Reminder** window opens, click **Start the DEMO**, and in the **DEMO Version** window, click **Start NetScanTools Pro Demo…**.

3. □ The **NetScanTools Pro** main window appears, as shown in the screenshot.



Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not
your interface IP.
This demo cannot be converted to a full version.

Please select from the Automated or Manual tools or tools grouped by function on the left panel.

The tool icons are color coded:

Red icon tools contact the target, green icon tools listen to network traffic,
blue icon tools work with your local system and gray icon tools contact third party systems.

Press the F1 key to view the extensive local help including Getting Started Information.

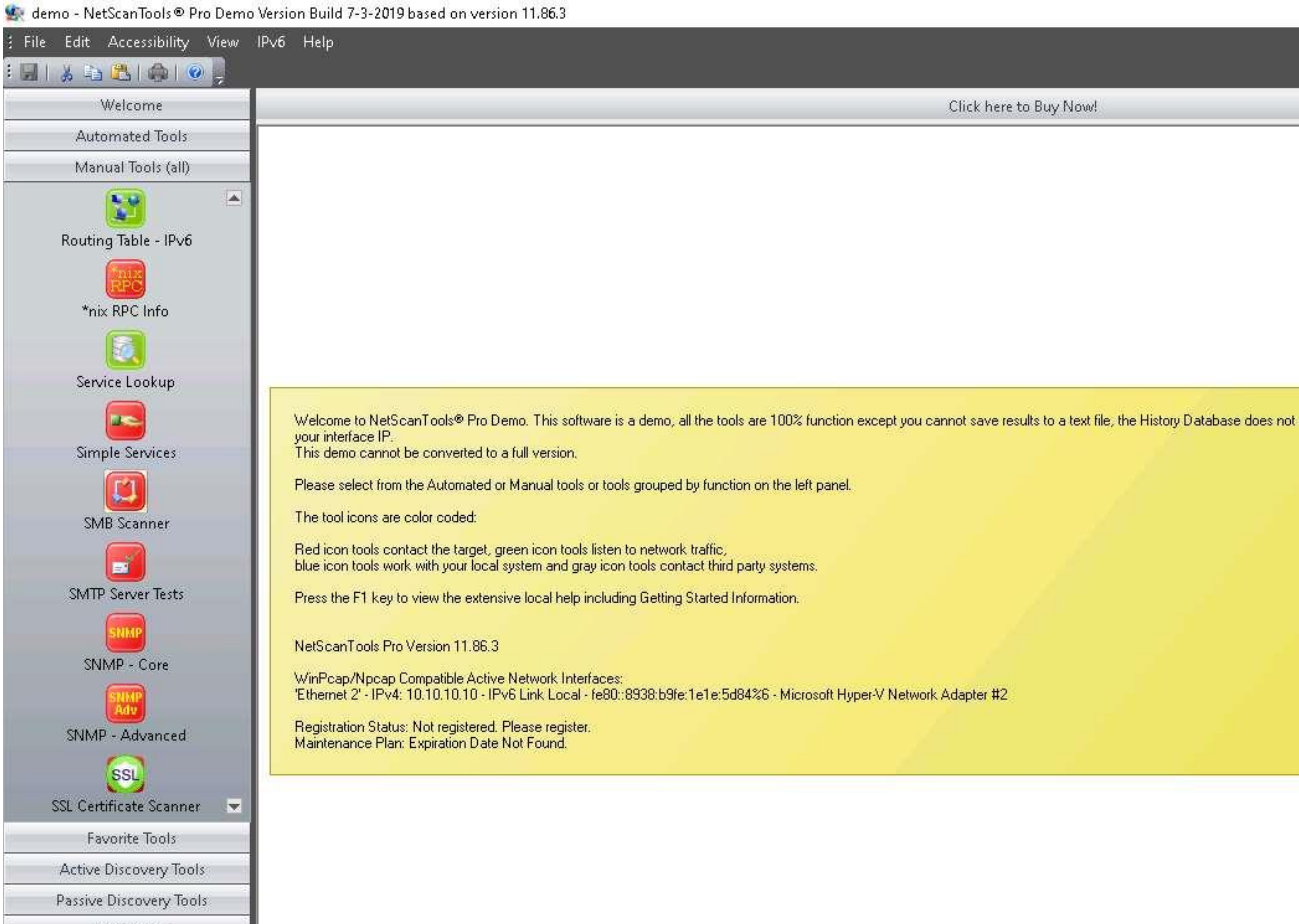
NetScanTools Pro Version 11.86.3

WinPcap/Npcap Compatible Active Network Interfaces:
'Ethernet 2' - IPv4: 10.10.10.10 - IPv6 Link Local - fe80::5081:d041:f459:f50d%6 - Microsoft Hyper-V Network Adapter #2

Registration Status: Not registered. Please register.
Maintenance Plan: Expiration Date Not Found.

4. □ In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

If a dialog box appears explaining the tool, click **OK**.



Welcome to NetScanTools® Pro Demo. This software is a demo, all the tools are 100% function except you cannot save results to a text file, the History Database does not
your interface IP.
This demo cannot be converted to a full version.

Please select from the Automated or Manual tools or tools grouped by function on the left panel.

The tool icons are color coded:

Red icon tools contact the target, green icon tools listen to network traffic,
blue icon tools work with your local system and gray icon tools contact third party systems.

Press the F1 key to view the extensive local help including Getting Started Information.

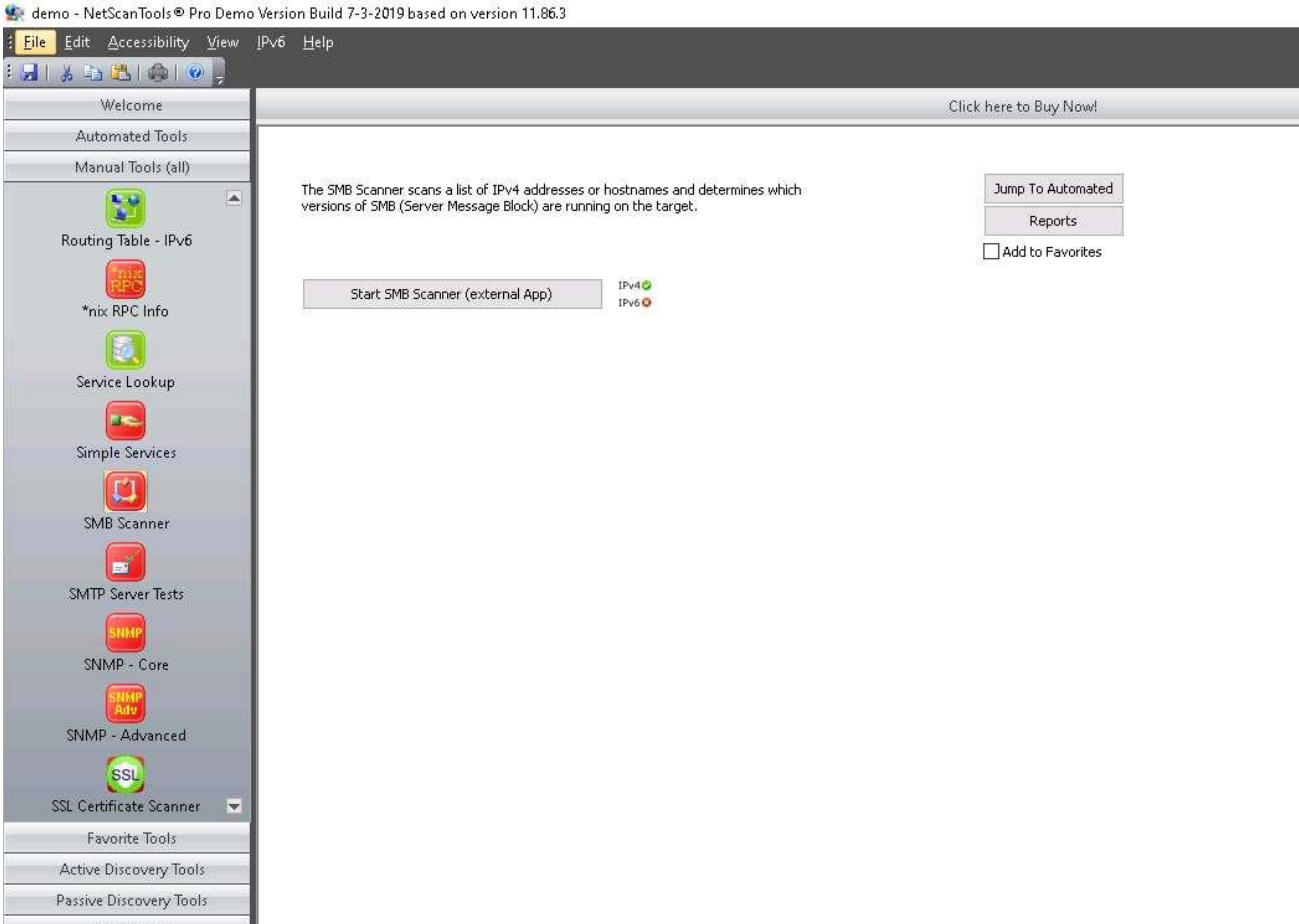
NetScanTools Pro Version 11.86.3

WinPcap/Npcap Compatible Active Network Interfaces:
'Ethernet 2' - IPv4: 10.10.10.10 - IPv6 Link Local - fe80::8938:b9fe:1e1e:5d84%6 - Microsoft Hyper-V Network Adapter #2

Registration Status: Not registered. Please register.
Maintenance Plan: Expiration Date Not Found.

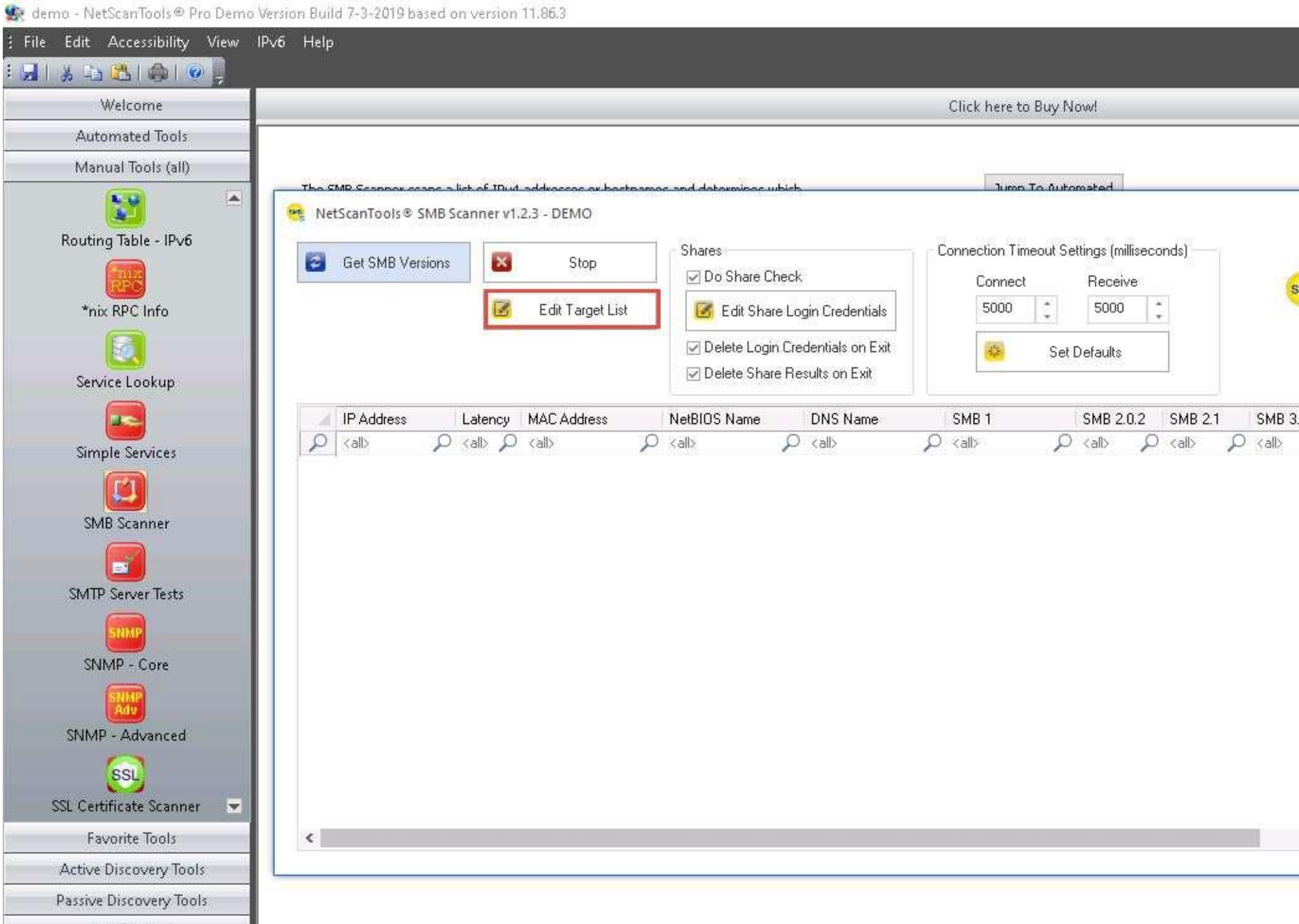
5. □ In the right pane, click the **Start SMB Scanner (external App)** button.

If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.



The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which versions of SMB (Server Message Block) are running on the target.

6. The **SMB Scanner** window appears; click the **Edit Target List** button.



The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which

☑ Do Share Check

☑ Delete Login Credentials on Exit

☑ Delete Share Results on Exit

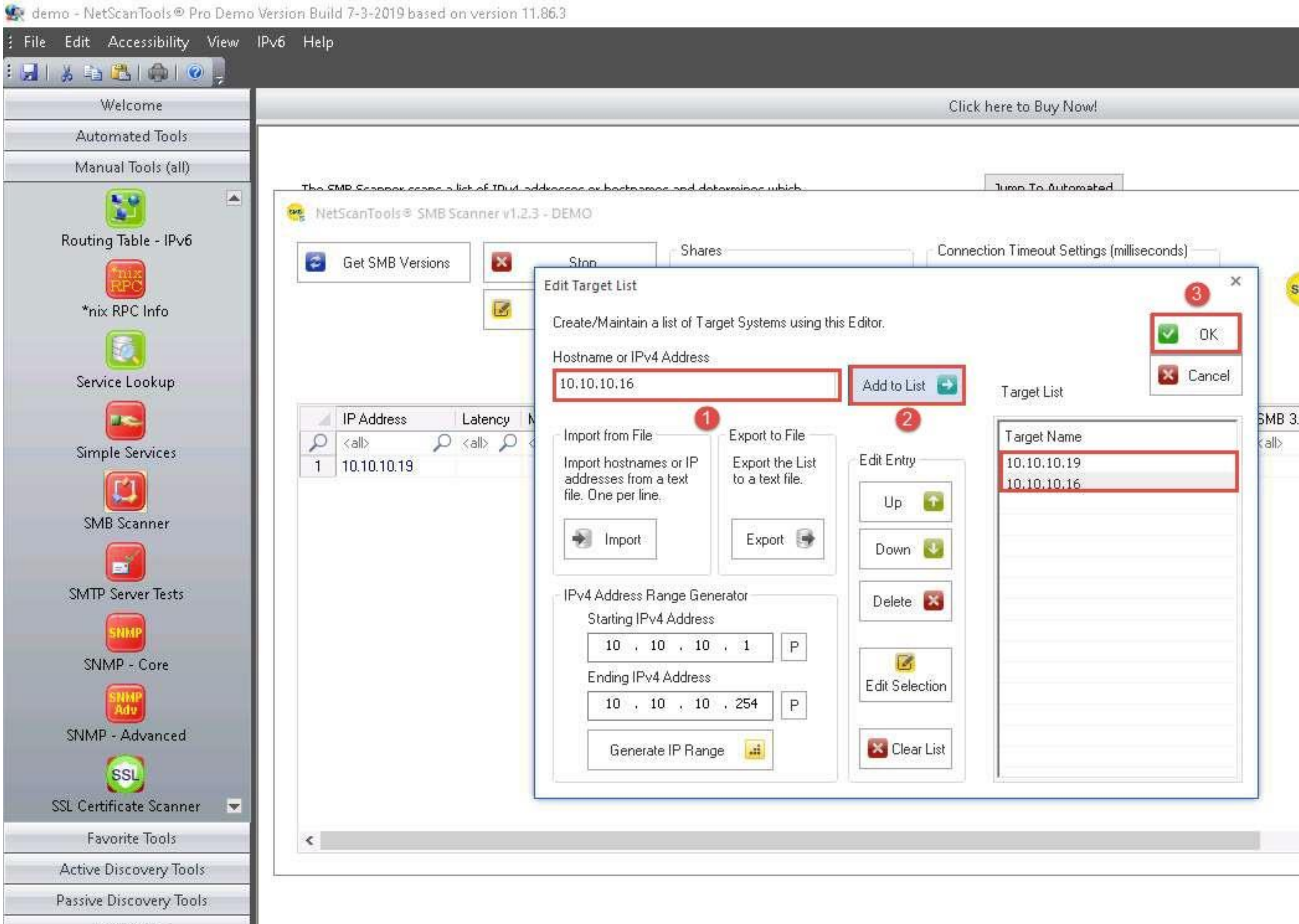
Connect: 5000

Receive: 5000

IP Address	Latency	MAC Address	NetBIOS Name	DNS Name	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.
<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>

7. □ The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.10.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List**.
8. □ Similarly, add another target IP address (**10.10.10.16**, in this example) to **Target List** and click **OK**.

In this task, we are targeting the **Windows Server 2019** (10.10.10.19) and **Windows Server 2016** (10.10.10.16) machines.



The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which

	IP Address	Latency
	<all>	<all>
1	10.10.10.19	

Create/Maintain a list of Target Systems using this Editor.

Hostname or IPv4 Address: 10.10.10.16

Import hostnames or IP addresses from a text file. One per line.

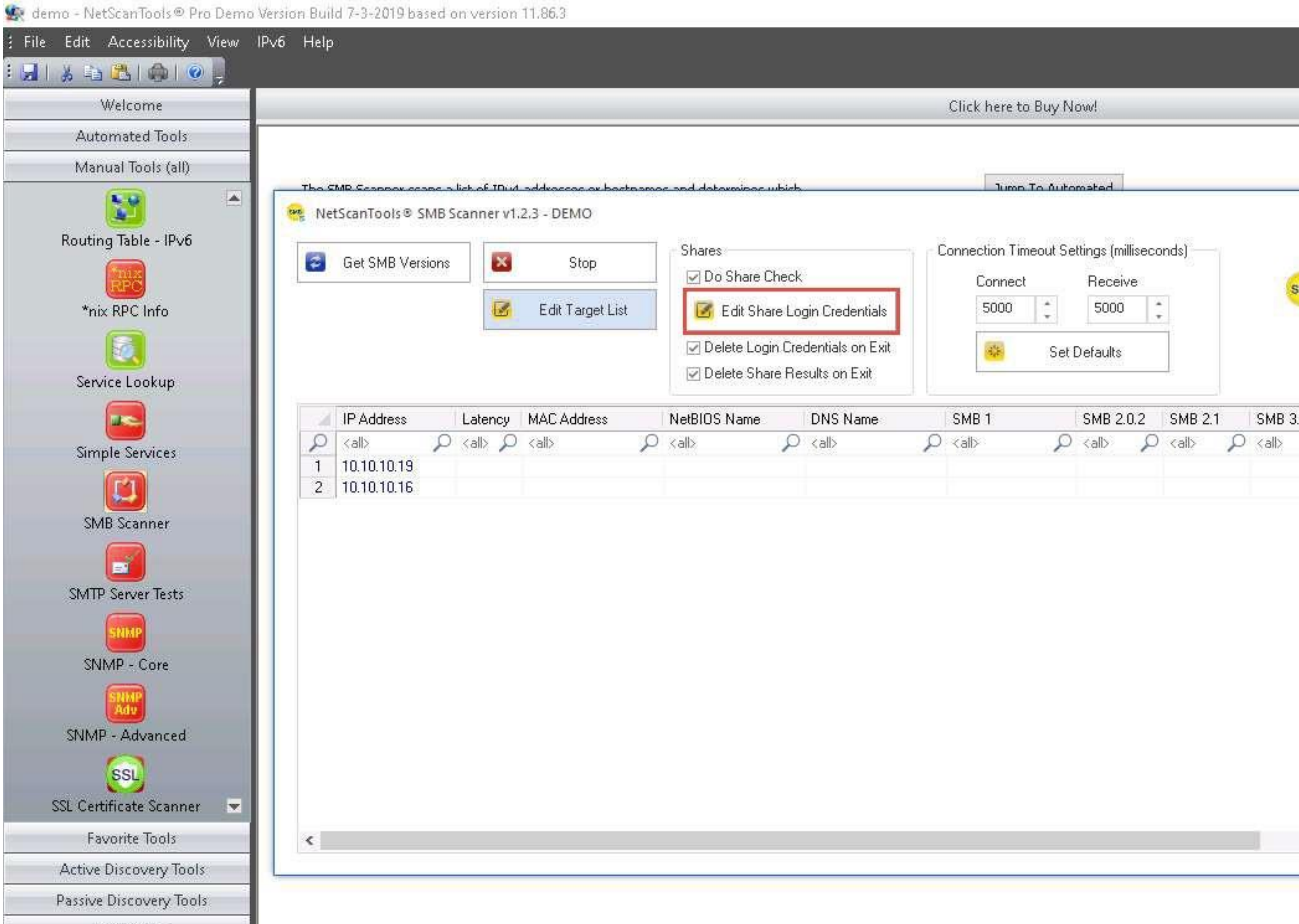
Export the List to a text file.

Starting IPv4 Address: 10 . 10 . 10 . 1

Ending IPv4 Address: 10 . 10 . 10 . 254

Target Name
10.10.10.19
10.10.10.16

9. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.



Shares

☑ Do Share Check

☑ Delete Login Credentials on Exit

☑ Delete Share Results on Exit

Connection Timeout Settings (milliseconds)

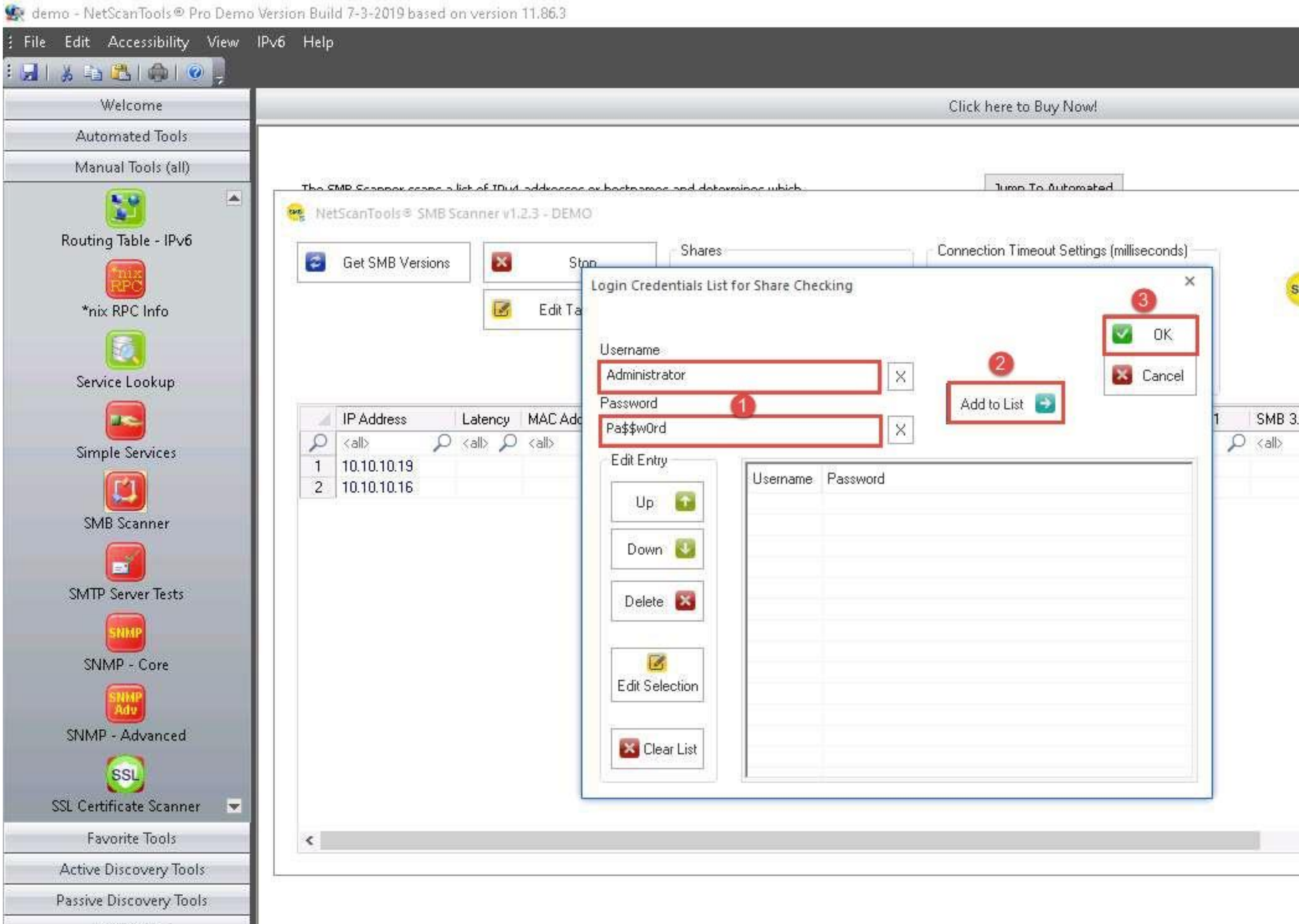
Connect: 5000

Receive: 5000

	IP Address	Latency	MAC Address	NetBIOS Name	DNS Name	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.
	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
1	10.10.10.19								
2	10.10.10.16								

10. □ The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

    In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2016** machines to understand the tool. In reality, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.



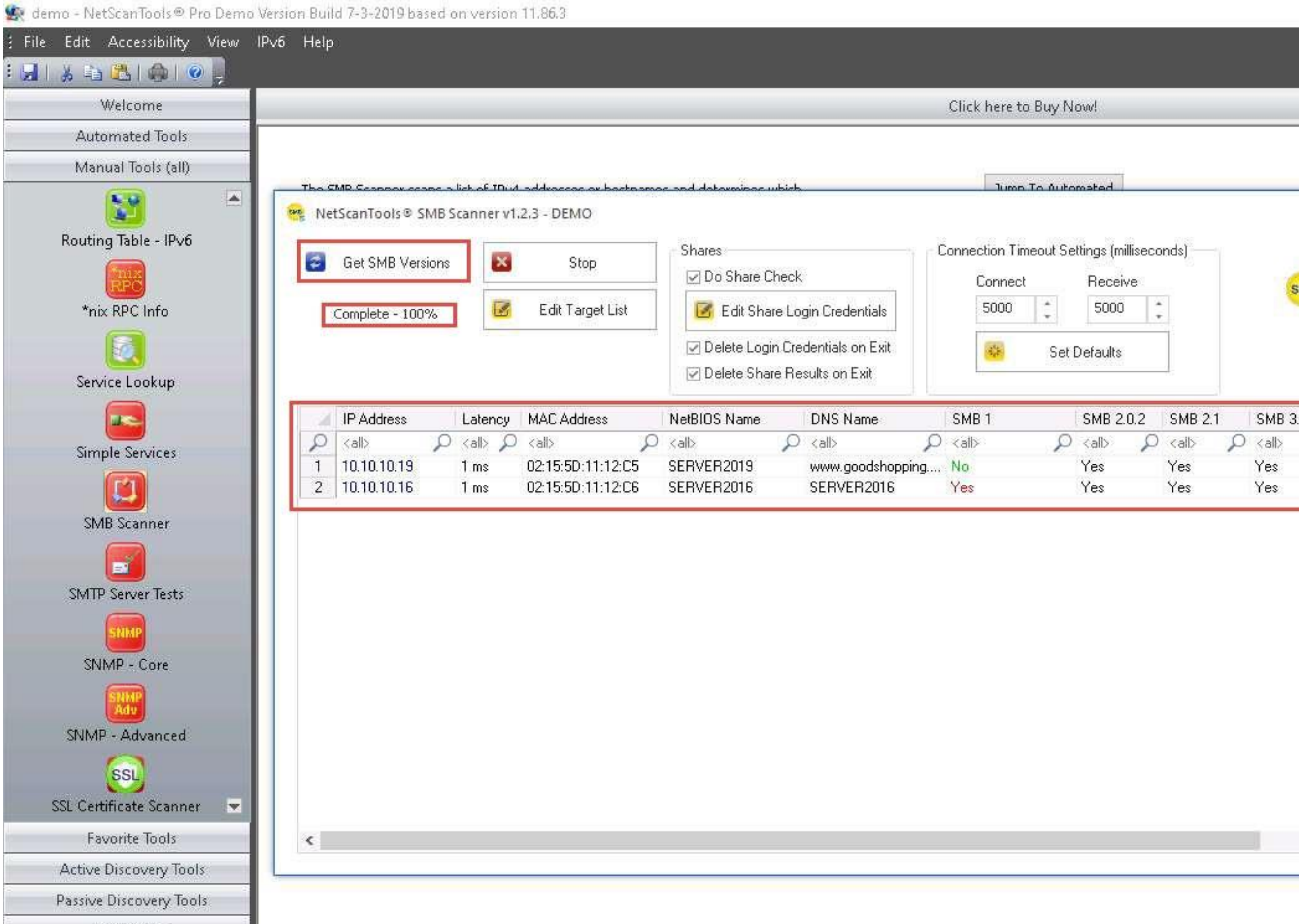
	IP Address
1	10.10.10.19
2	10.10.10.16

Username: Administrator

Password: Pa$$w0rd

Username	Password

11. □ In the **SMB Scanner** window, click the **Get SMB Versions** button.
12. □ Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.



Complete - 100%

Shares

☑ Do Share Check

☑ Delete Login Credentials on Exit

☑ Delete Share Results on Exit

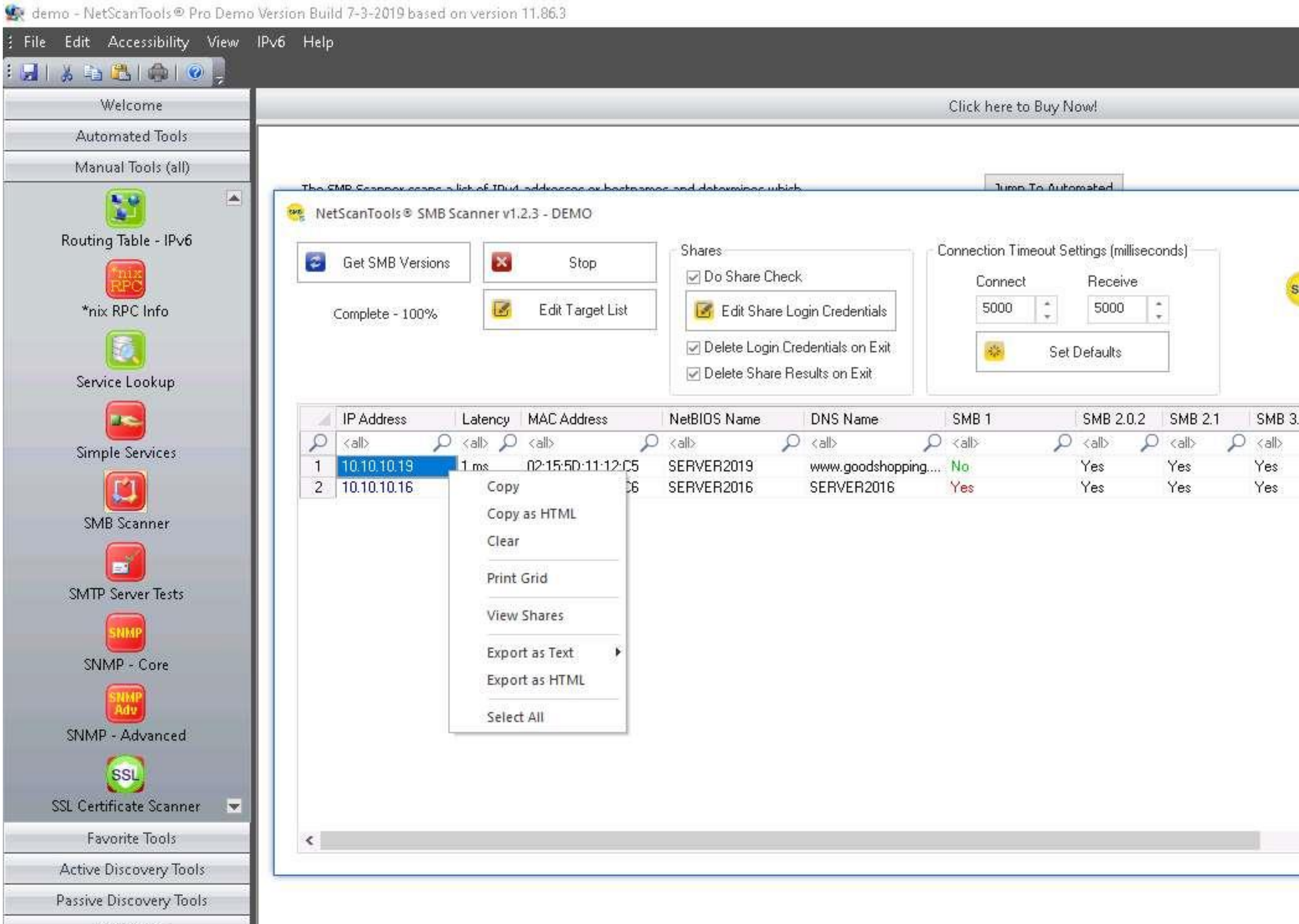
Connection Timeout Settings (milliseconds)

Connect: 5000

Receive: 5000

	IP Address	Latency	MAC Address	NetBIOS Name	DNS Name	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.
	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
1	10.10.10.19	1 ms	02:15:5D:11:12:C5	SERVER2019	www.goodshopping....	No	Yes	Yes	Yes
2	10.10.10.16	1 ms	02:15:5D:11:12:C6	SERVER2016	SERVER2016	Yes	Yes	Yes	Yes

13. □ Right-click on any of the machines (in this example, we will use **10.10.10.19**) and click **View Shares** from the available options.



The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which

Complete - 100%

Shares

☑ Do Share Check

☑ Delete Login Credentials on Exit

☑ Delete Share Results on Exit

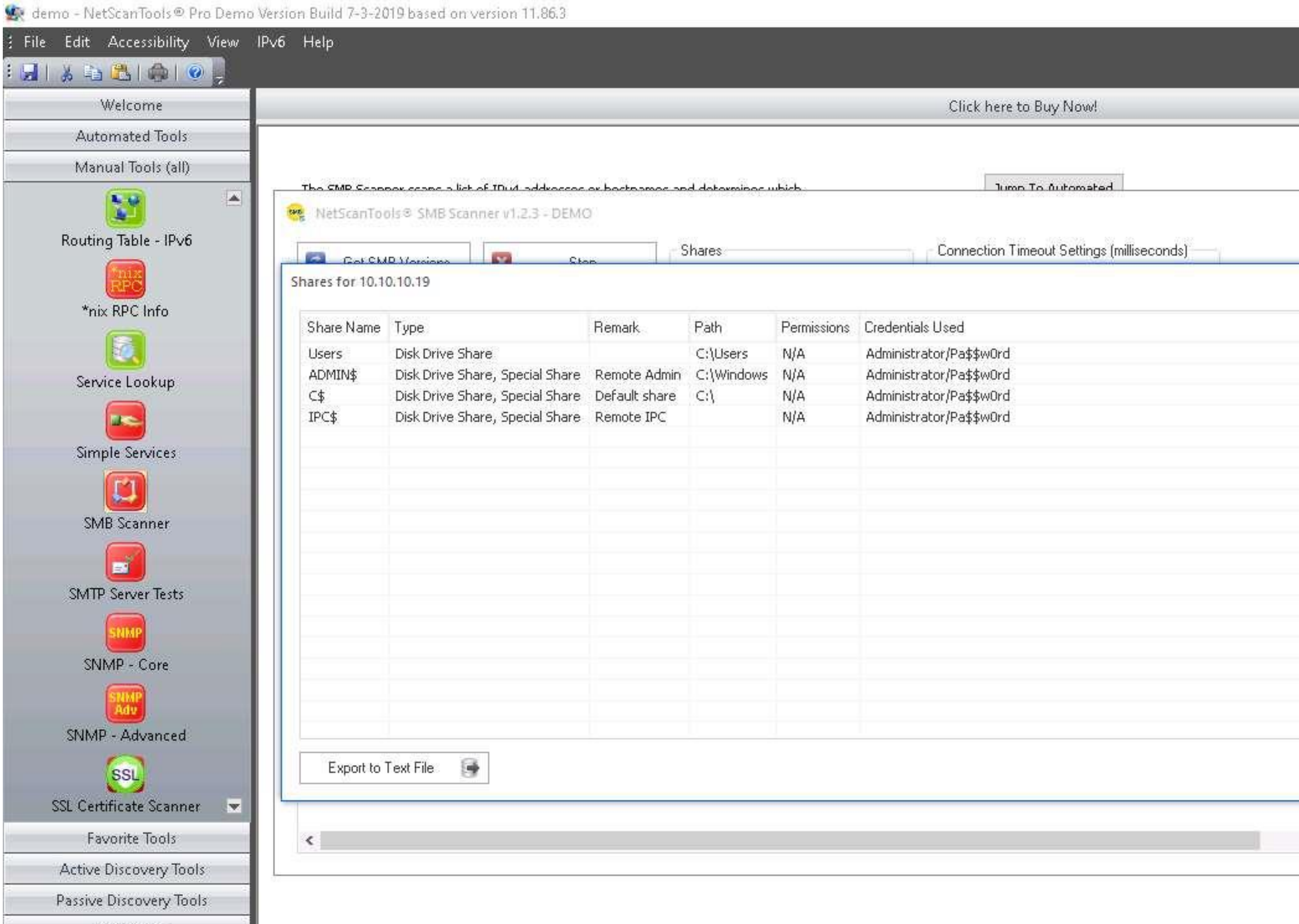
Connection Timeout Settings (milliseconds)

Connect: 5000

Receive: 5000

	IP Address	Latency	MAC Address	NetBIOS Name	DNS Name	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.
	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
1	10.10.10.19	1 ms	02:15:5D:11:12:C5	SERVER2019	www.goodshopping....	No	Yes	Yes	Yes
2	10.10.10.16		C6	SERVER2016	SERVER2016	Yes	Yes	Yes	Yes

14. The **Shares for 10.10.10.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used.



The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which

Shares for 10.10.10.19

Share Name	Type	Remark	Path	Permissions	Credentials Used
Users	Disk Drive Share		C:\Users	N/A	Administrator/Pa$$w0rd
ADMIN$	Disk Drive Share, Special Share	Remote Admin	C:\Windows	N/A	Administrator/Pa$$w0rd
C$	Disk Drive Share, Special Share	Default share	C:\	N/A	Administrator/Pa$$w0rd
IPC$	Disk Drive Share, Special Share	Remote IPC		N/A	Administrator/Pa$$w0rd

15. □ You can view the details of the shared files for the target IP address **10.10.10.16** in the same way.
16. □ This concludes the demonstration of performing SMB enumeration on the target systems using NetScanTools Pro.
17. □ Close all open windows and document all the acquired information.

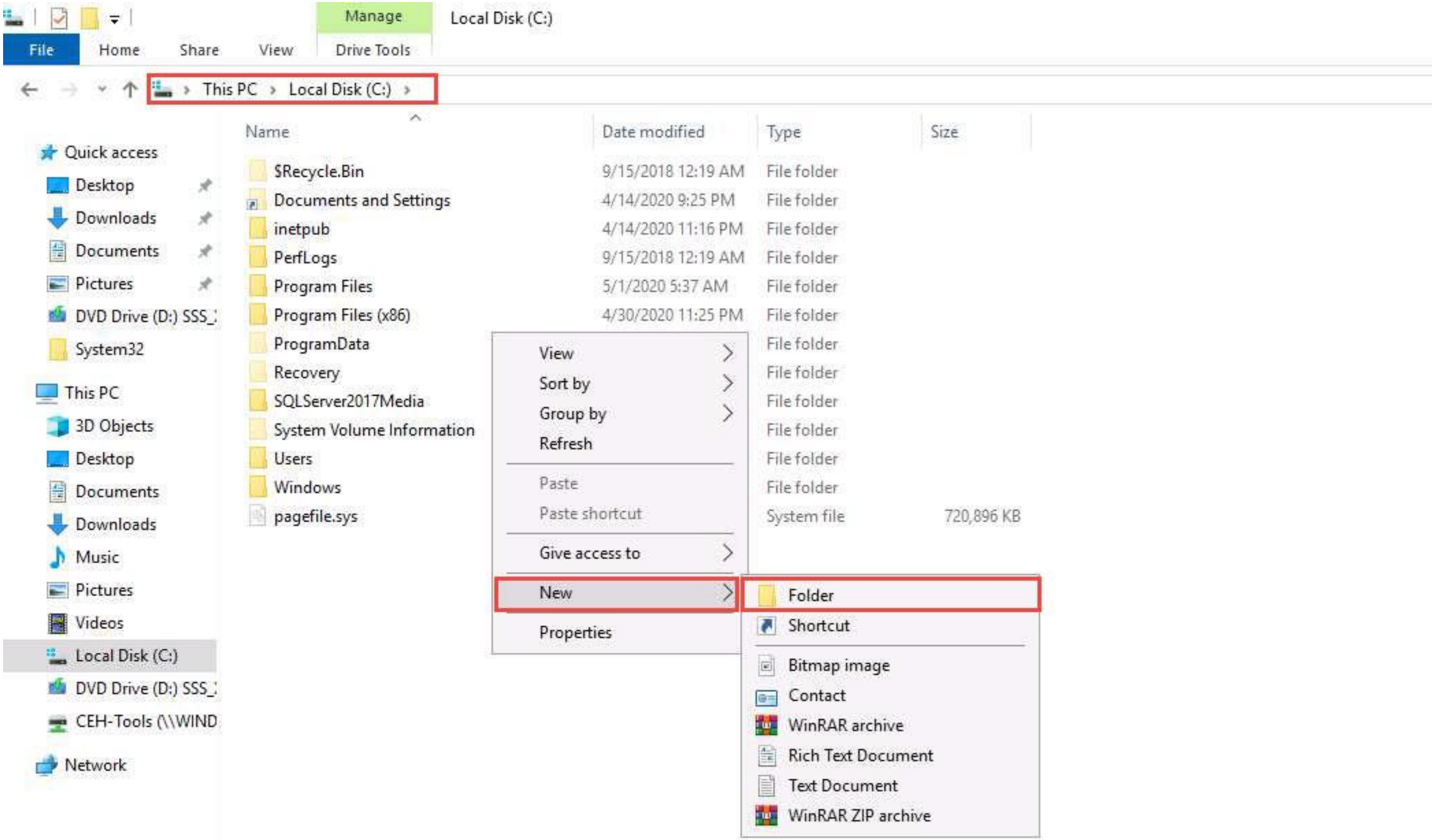
Task 2: Perform RPC, SMB, and FTP Enumeration using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

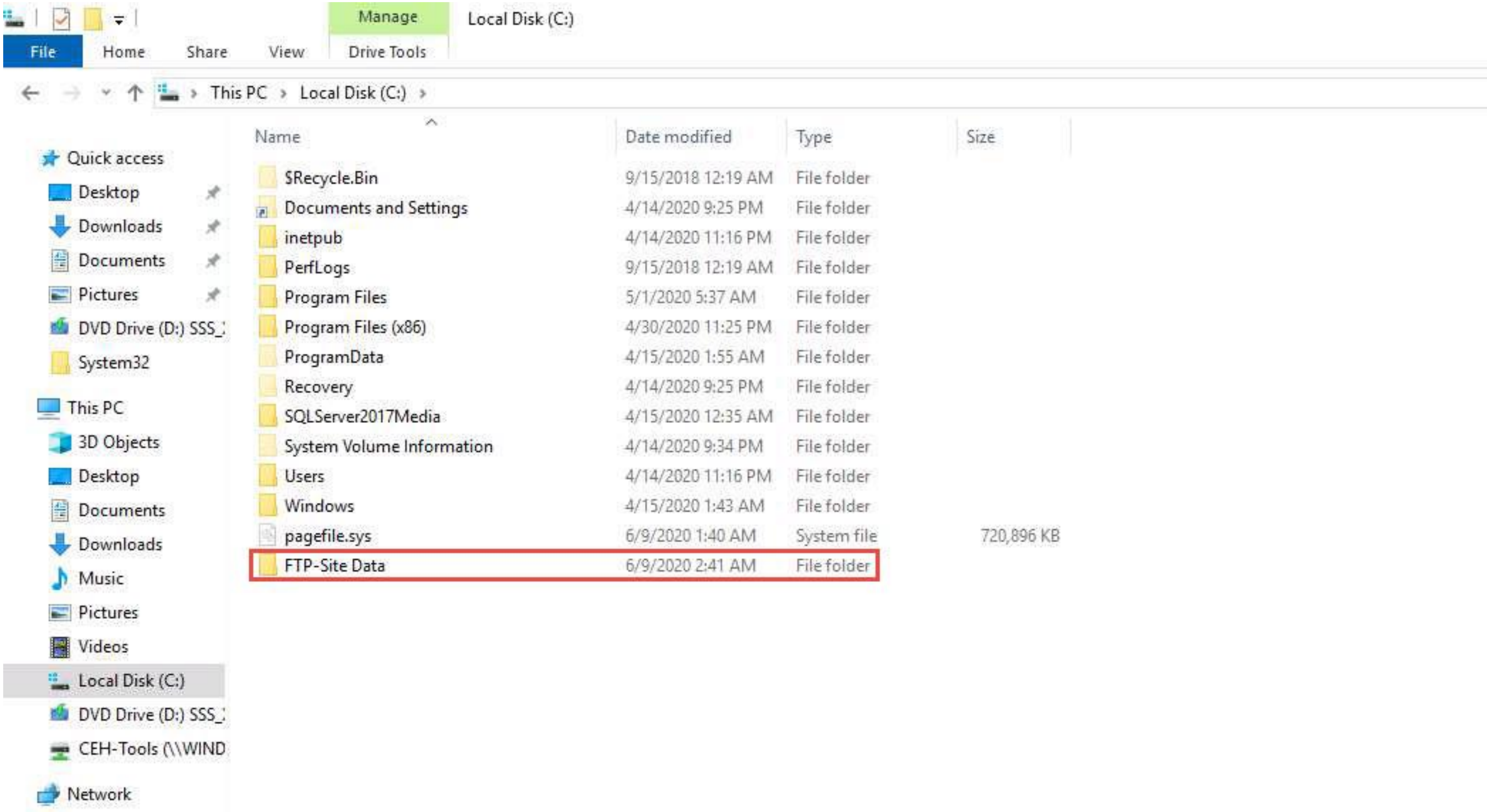
Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 1-10**.

1. □ Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. □ Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New** --> **Folder**.



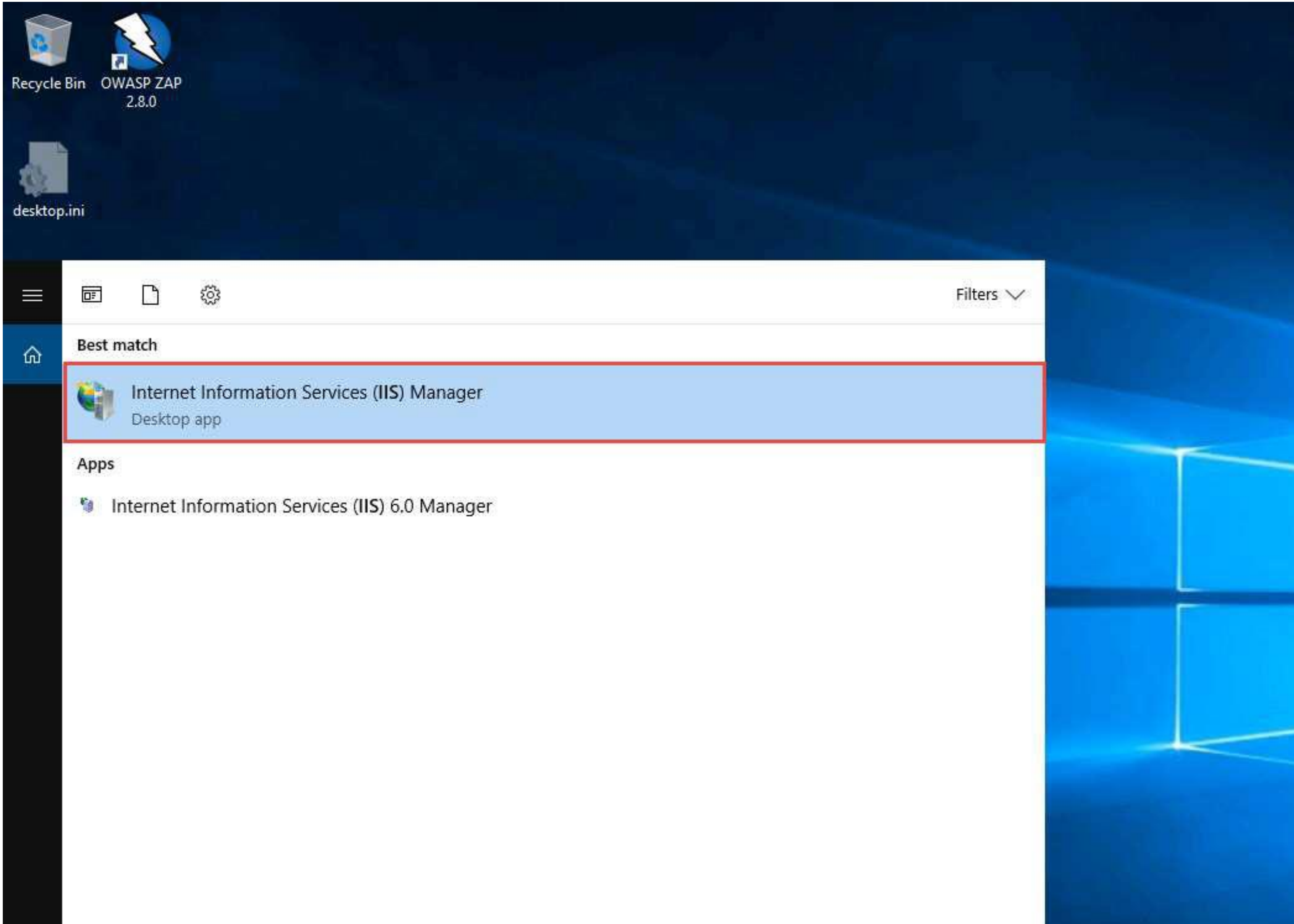
Name	Date modified	Type	Size
$Recycle.Bin	9/15/2018 12:19 AM	File folder	
Documents and Settings	4/14/2020 9:25 PM	File folder	
inetpub	4/14/2020 11:16 PM	File folder	
PerfLogs	9/15/2018 12:19 AM	File folder	
Program Files	5/1/2020 5:37 AM	File folder	
Program Files (x86)	4/30/2020 11:25 PM	File folder	
ProgramData		File folder	
Recovery		File folder	
SQLServer2017Media		File folder	
System Volume Information		File folder	
Users		File folder	
Windows		File folder	
pagefile.sys		System file	720,896 KB

3. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

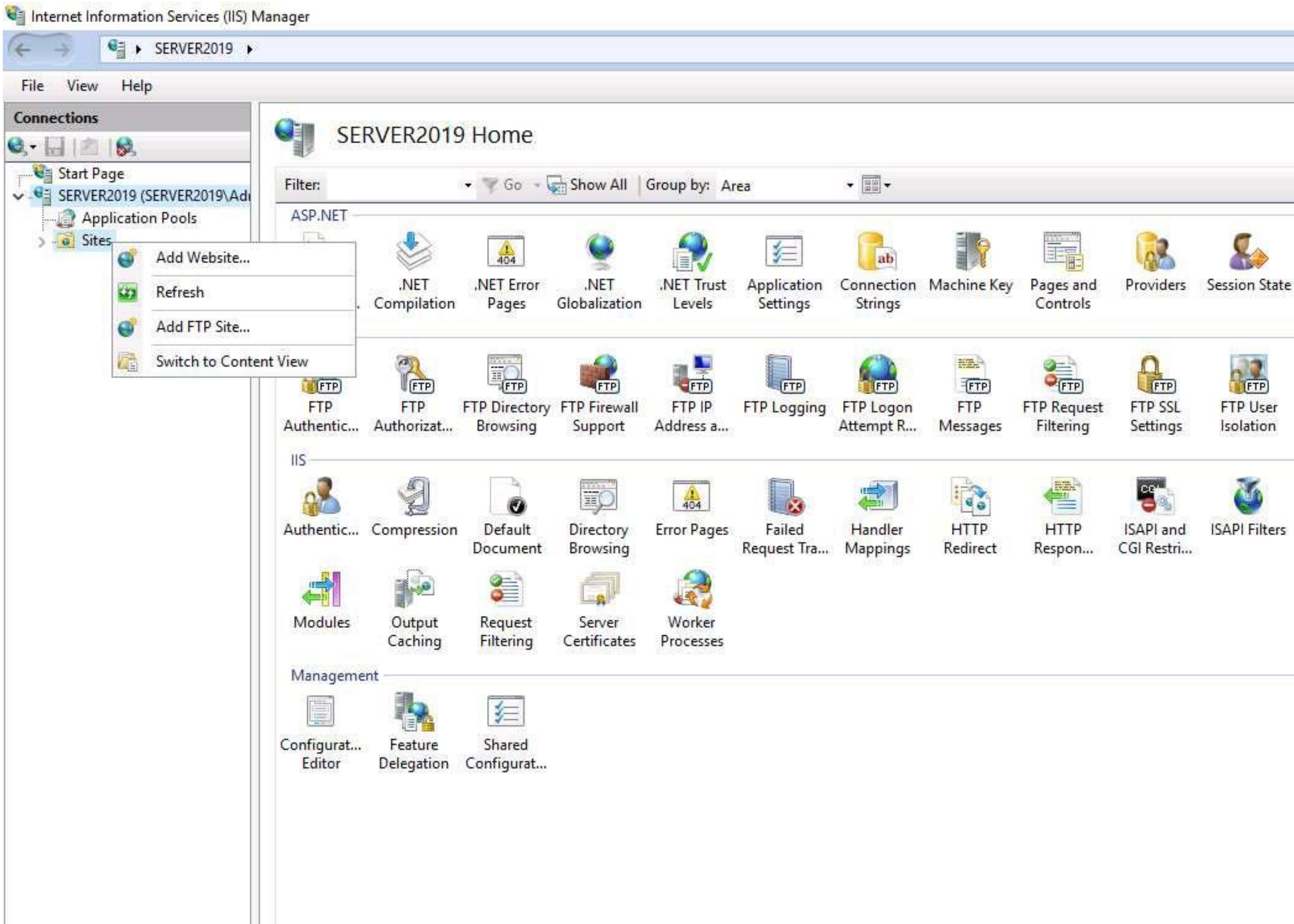


Name	Date modified	Type	Size
$Recycle.Bin	9/15/2018 12:19 AM	File folder	
Documents and Settings	4/14/2020 9:25 PM	File folder	
inetpub	4/14/2020 11:16 PM	File folder	
PerfLogs	9/15/2018 12:19 AM	File folder	
Program Files	5/1/2020 5:37 AM	File folder	
Program Files (x86)	4/30/2020 11:25 PM	File folder	
ProgramData	4/15/2020 1:55 AM	File folder	
Recovery	4/14/2020 9:25 PM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
System Volume Information	4/14/2020 9:34 PM	File folder	
Users	4/14/2020 11:16 PM	File folder	
Windows	4/15/2020 1:43 AM	File folder	
pagefile.sys	6/9/2020 1:40 AM	System file	720,896 KB
FTP-Site Data	6/9/2020 2:41 AM	File folder	

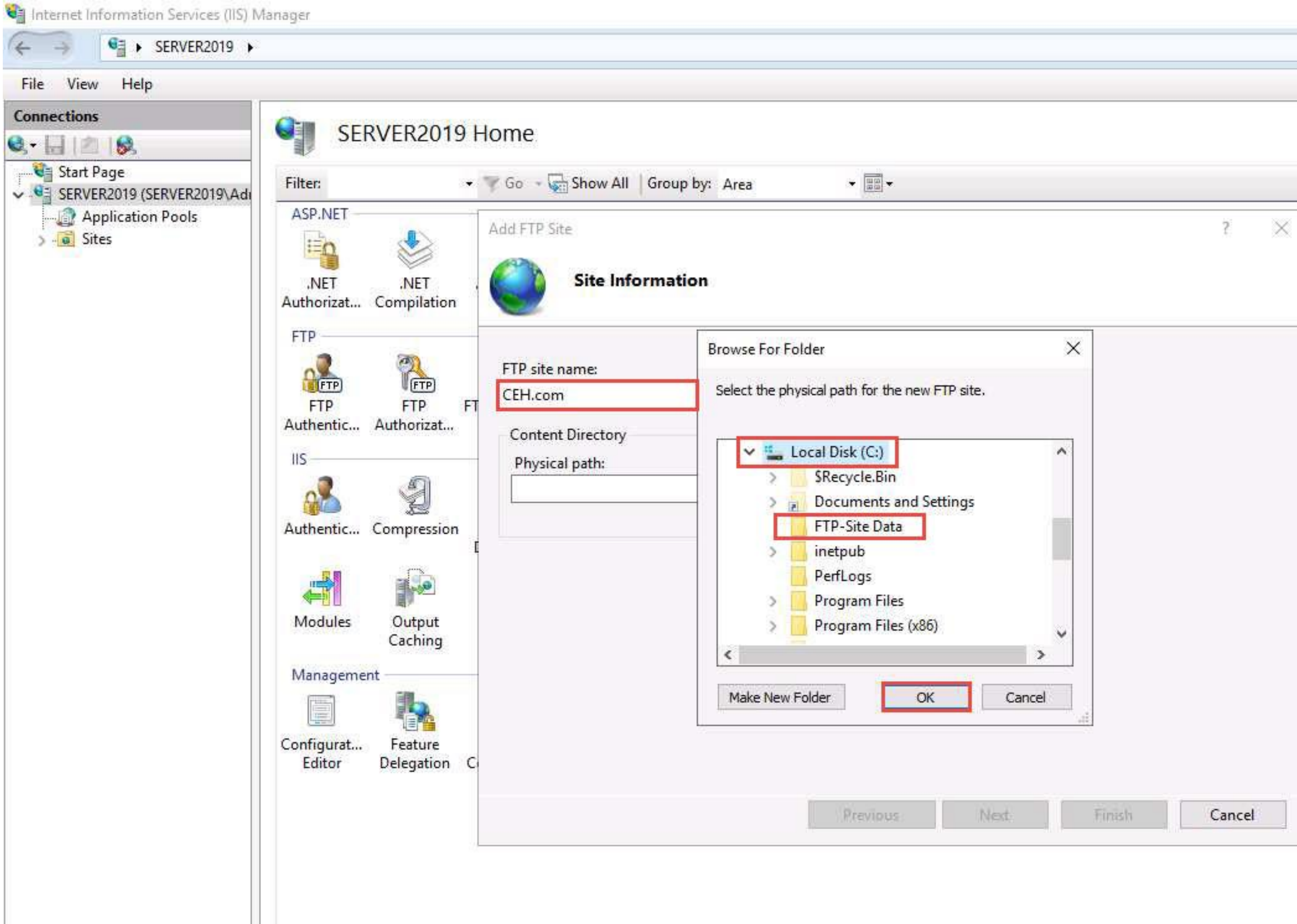
4. □ Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Filters
Best match
Internet Information Services (IIS) Manager
Desktop app
Apps
Internet Information Services (IIS) 6.0 Manager

5. □ In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site...**.


Internet Information Services (IIS) Manager
SERVER2019
File
View
Help
Connections
Start Page
SERVER2019 (SERVER2019\Ad
Application Pools
Sites
Add Website...
Refresh
Add FTP Site...
Switch to Content View
SERVER2019 Home
Filter:
Go
Show All
Group by:
Area
ASP.NET
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
FTP Authentic...
FTP Authorizat...
FTP Directory Browsing
FTP Firewall Support
FTP IP Address a...
FTP Logging
FTP Logon Attempt R...
FTP Messages
FTP Request Filtering
FTP SSL Settings
FTP User Isolation
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI and CGI Restri...
ISAPI Filters
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Configurat... Editor
Feature Delegation
Shared Configurat...

6. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.



Add FTP Site

Site Information

FTP site name: CEH.com

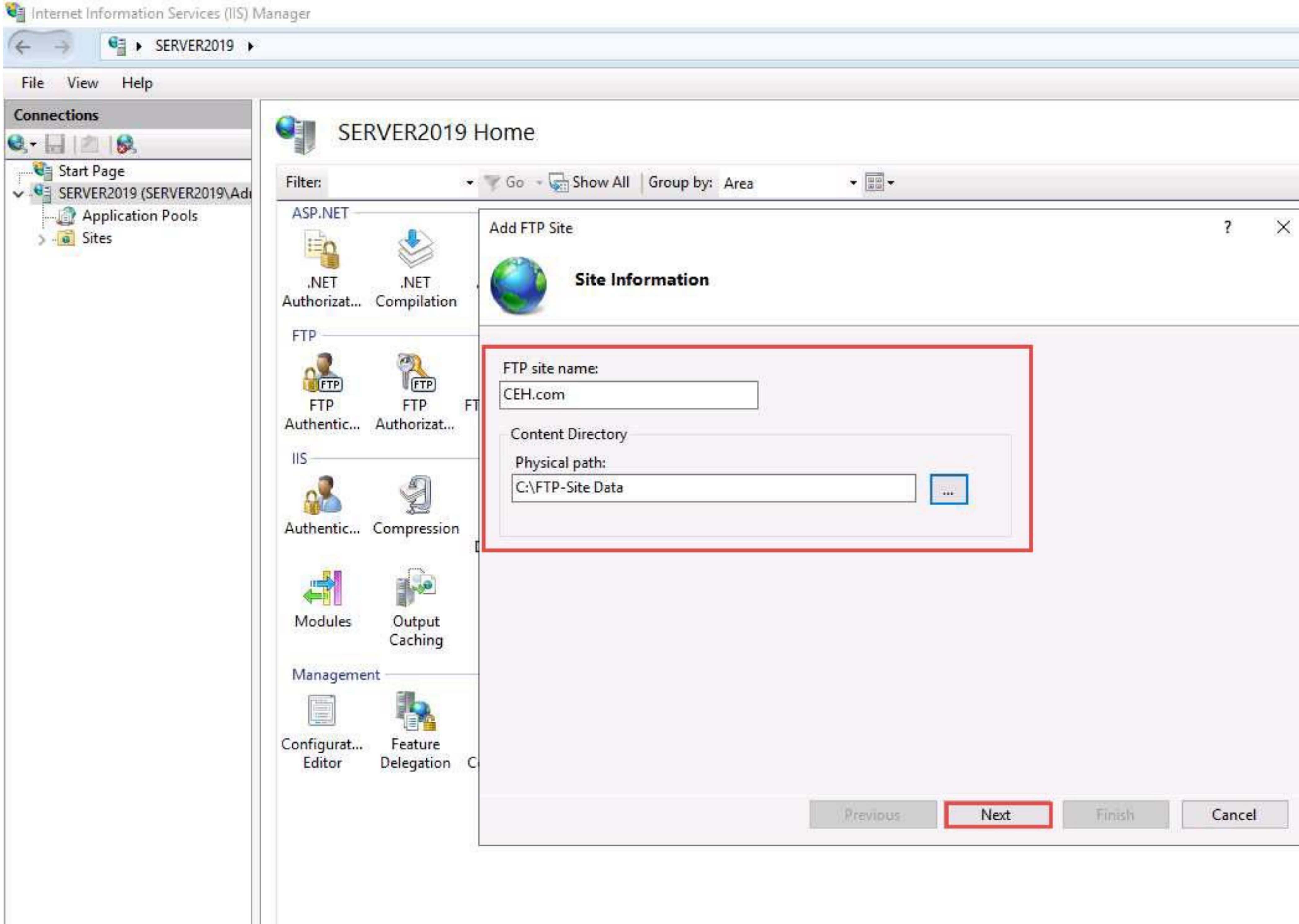
Content Directory

Physical path:

Browse For Folder

Select the physical path for the new FTP site.

7. In the **Add FTP Site** window, check the entered details and click **Next**.

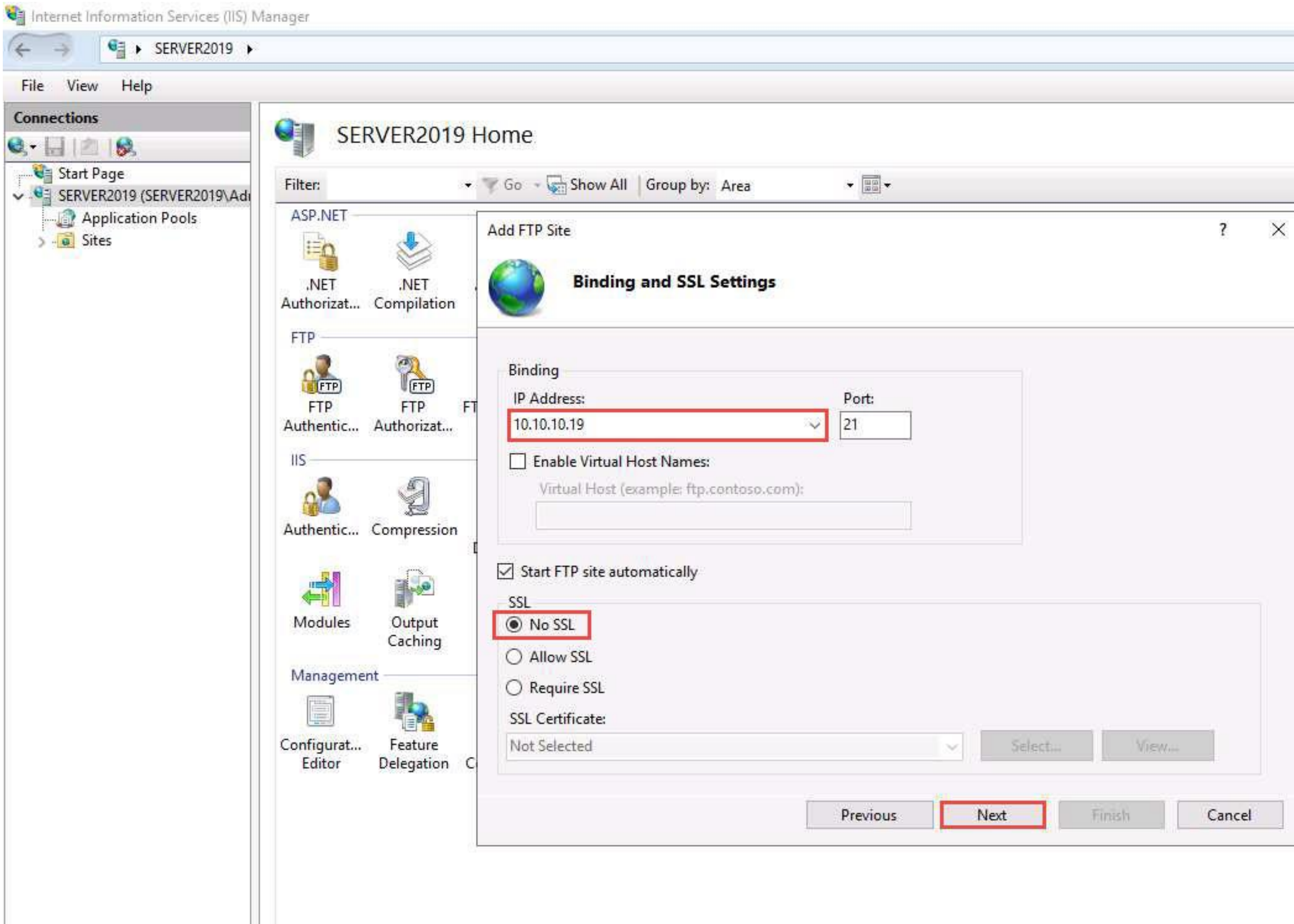


FTP site name: CEH.com

Content Directory

Physical path: C:\FTP-Site Data

8. □ The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.10.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.



Add FTP Site

Binding and SSL Settings

Binding

IP Address: 10.10.10.19

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

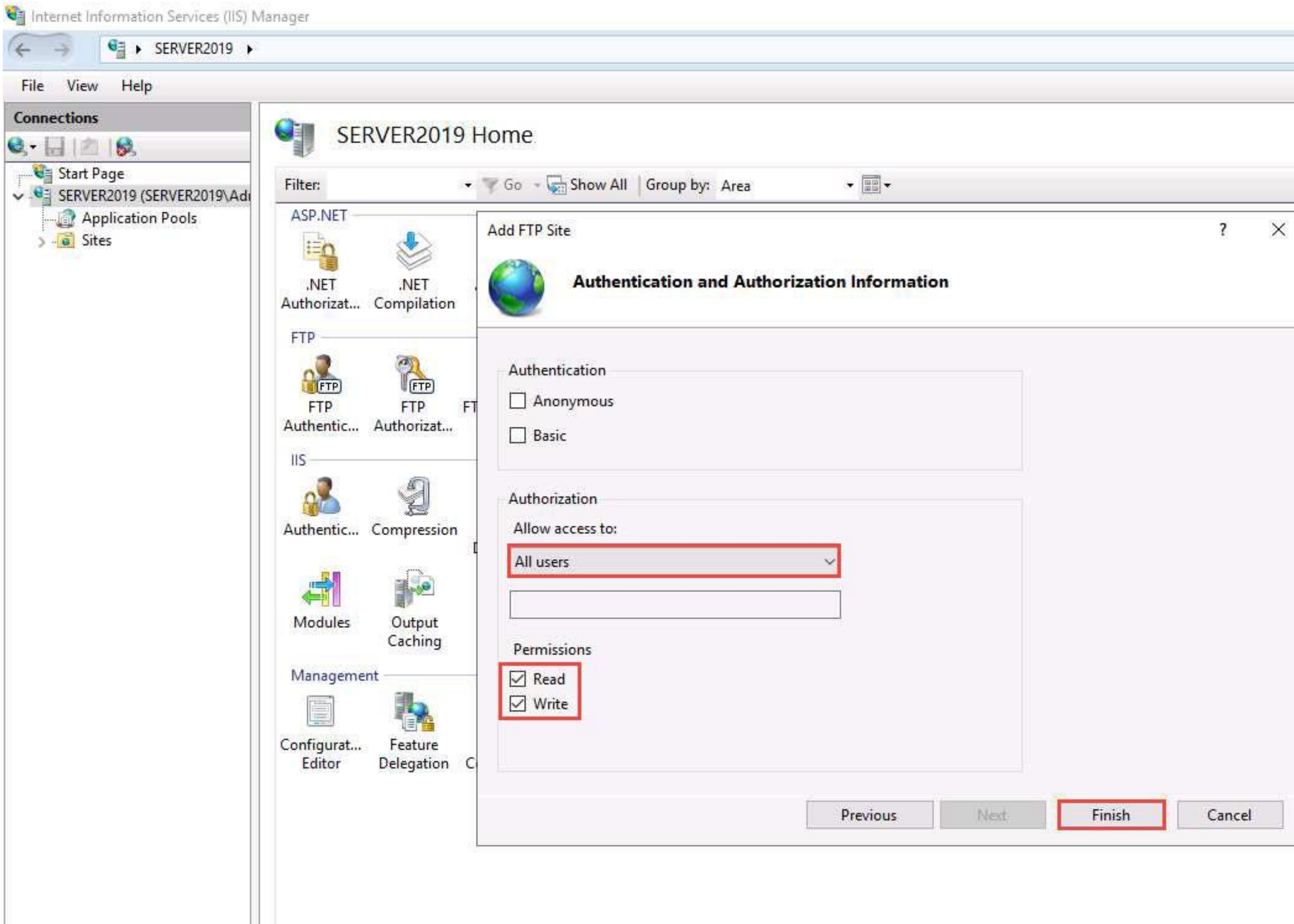
● No SSL

○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

9. The **Authentication and Authorization Information** wizard appears. In the **Allow access to** section, select **All users** from the drop-down list. In the **Permissions** section, select both the **Read** and **Write** options and click **Finish**.



Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

□ Basic

Authorization

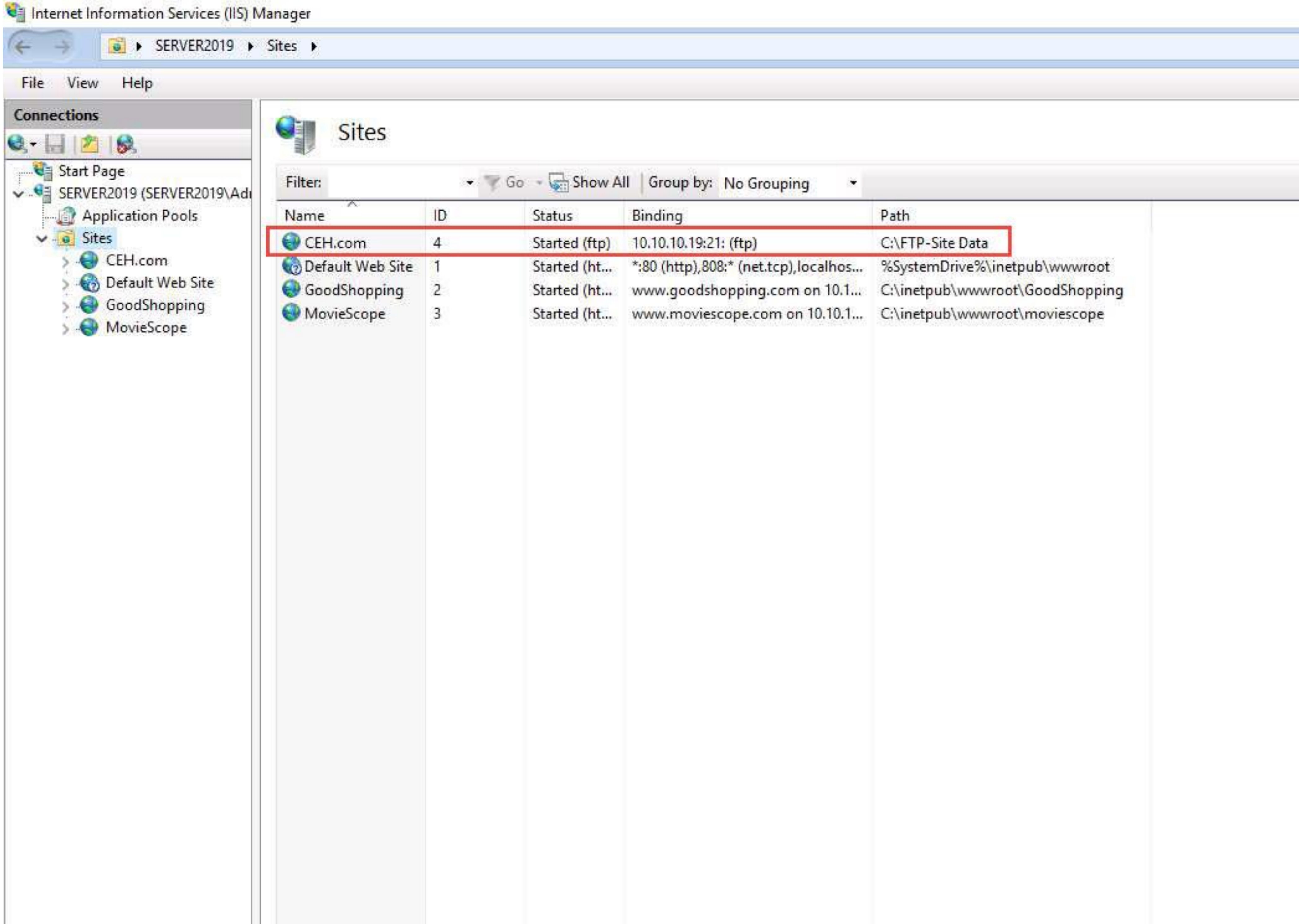
Allow access to: All users

Permissions

☑ Read

☑ Write

10. □ The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started** (**ftp**), as shown in the screenshot.



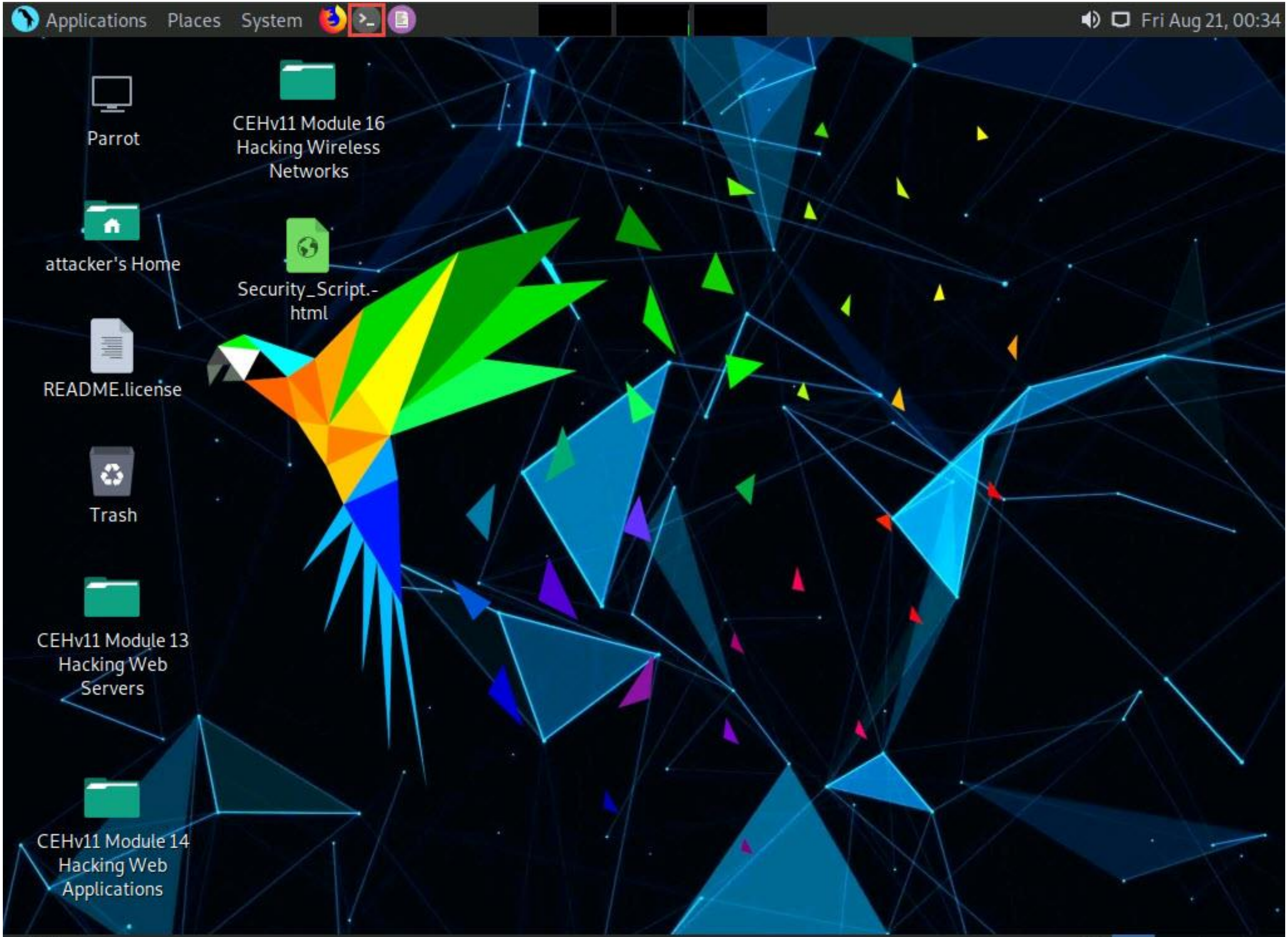
Sites

Name	ID	Status	Binding	Path
CEH.com	4	Started (ftp)	10.10.10.19:21: (ftp)	C:\FTP-Site Data
Default Web Site	1	Started (ht...	*:80 (http),808:* (net.tcp),localhos...	%SystemDrive%\inetpub\wwwroot
GoodShopping	2	Started (ht...	www.goodshopping.com on 10.1...	C:\inetpub\wwwroot\GoodShopping
MovieScope	3	Started (ht...	www.moviescope.com on 10.10.1...	C:\inetpub\wwwroot\moviescope

11. □ Close all windows.

12. □ Click Parrot Security to switch to the **Parrot Security** machine.

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

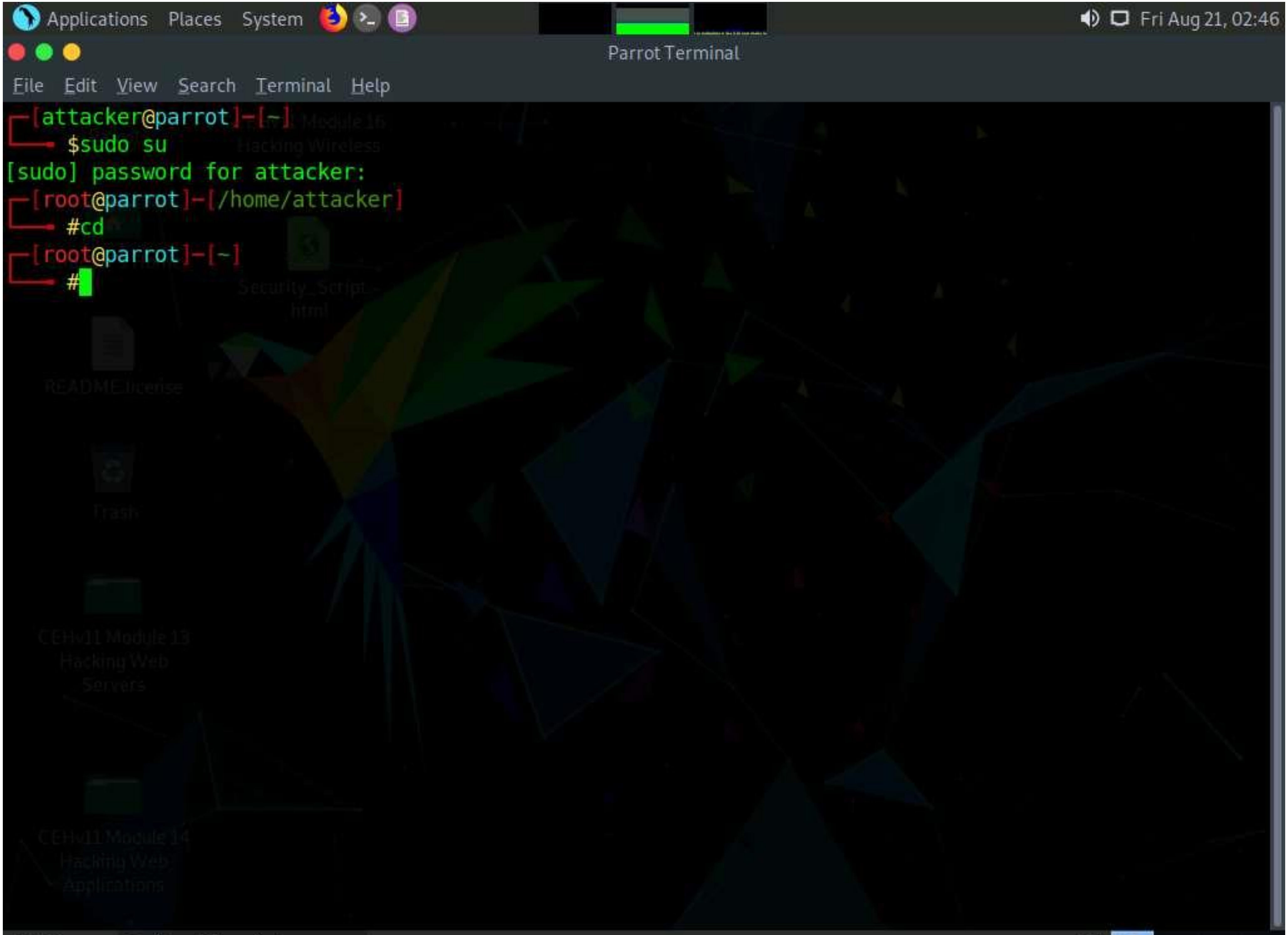

Applications
Places
System
Fri Aug 21, 00:34
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

14. □ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

15. □ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

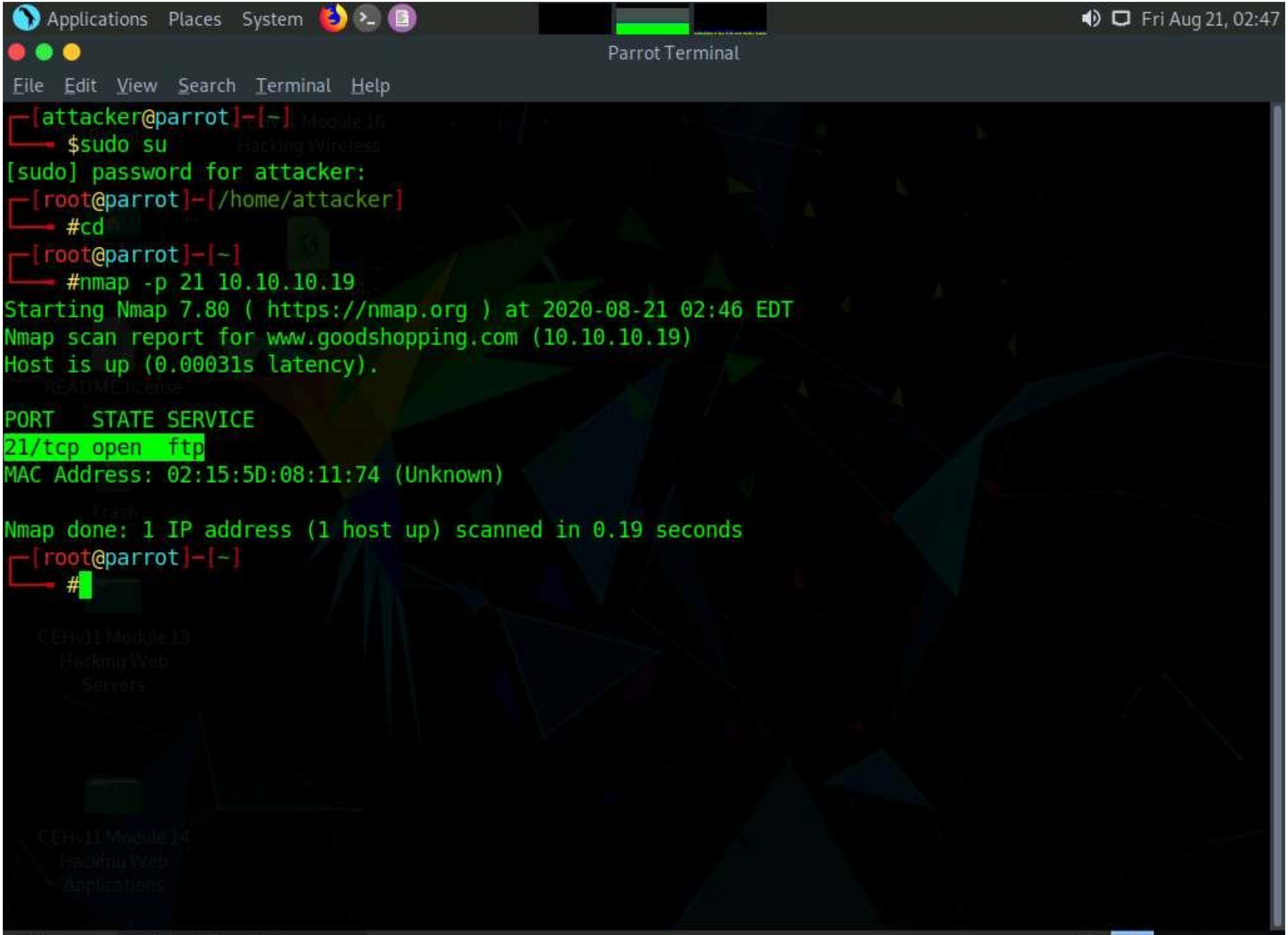
The password that you type will not be visible.

16. □ Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

17. □ In the **Parrot Terminal** window, type **nmap -p 21 [Target IP Address]** (in this case, **10.10.10.19**) and press **Enter**.
18. □ The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

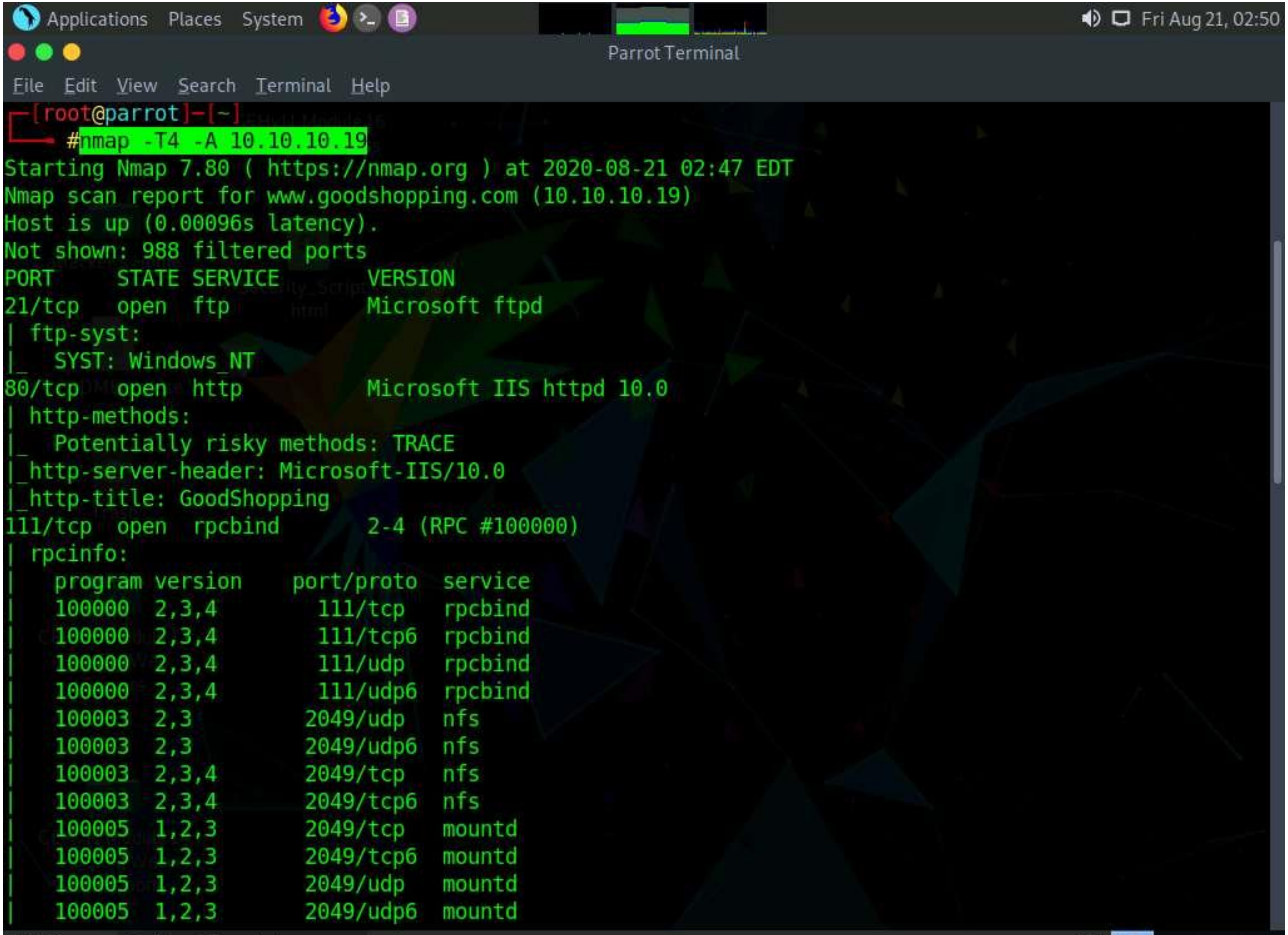


Applications Places System
Fri Aug 21, 02:47
Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap -p 21 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 02:46 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00031s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 02:15:5D:08:11:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
┌─[root@parrot]─[~]
└──╼ #
```

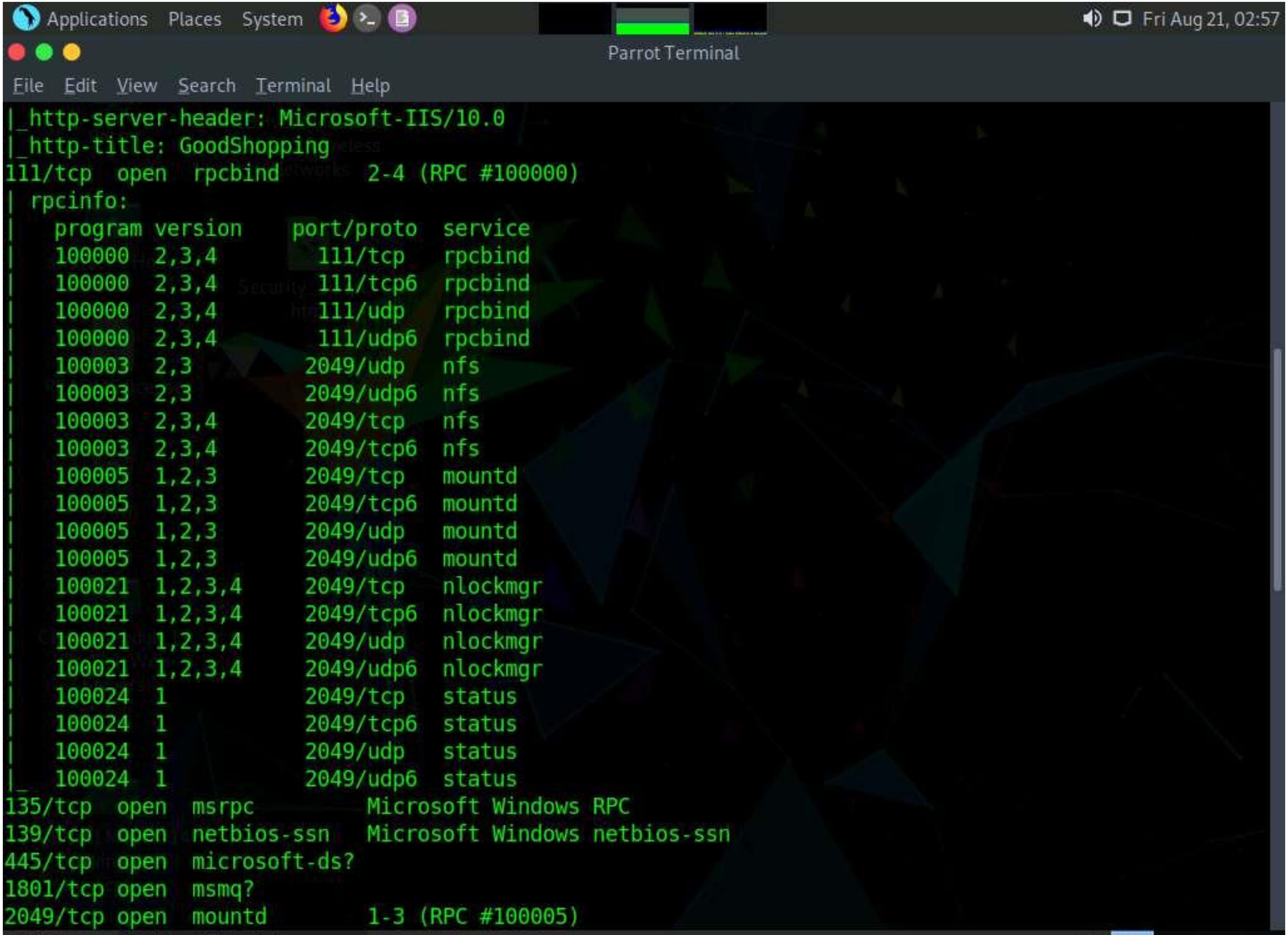
19. □ In the terminal window, type **nmap -T4 -A [Target IP Address]** (in this example, the target IP address is **10.10.10.19**) and press **Enter**.

In this command, **-T4** specifies the timing template (the number can be 0-5) and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

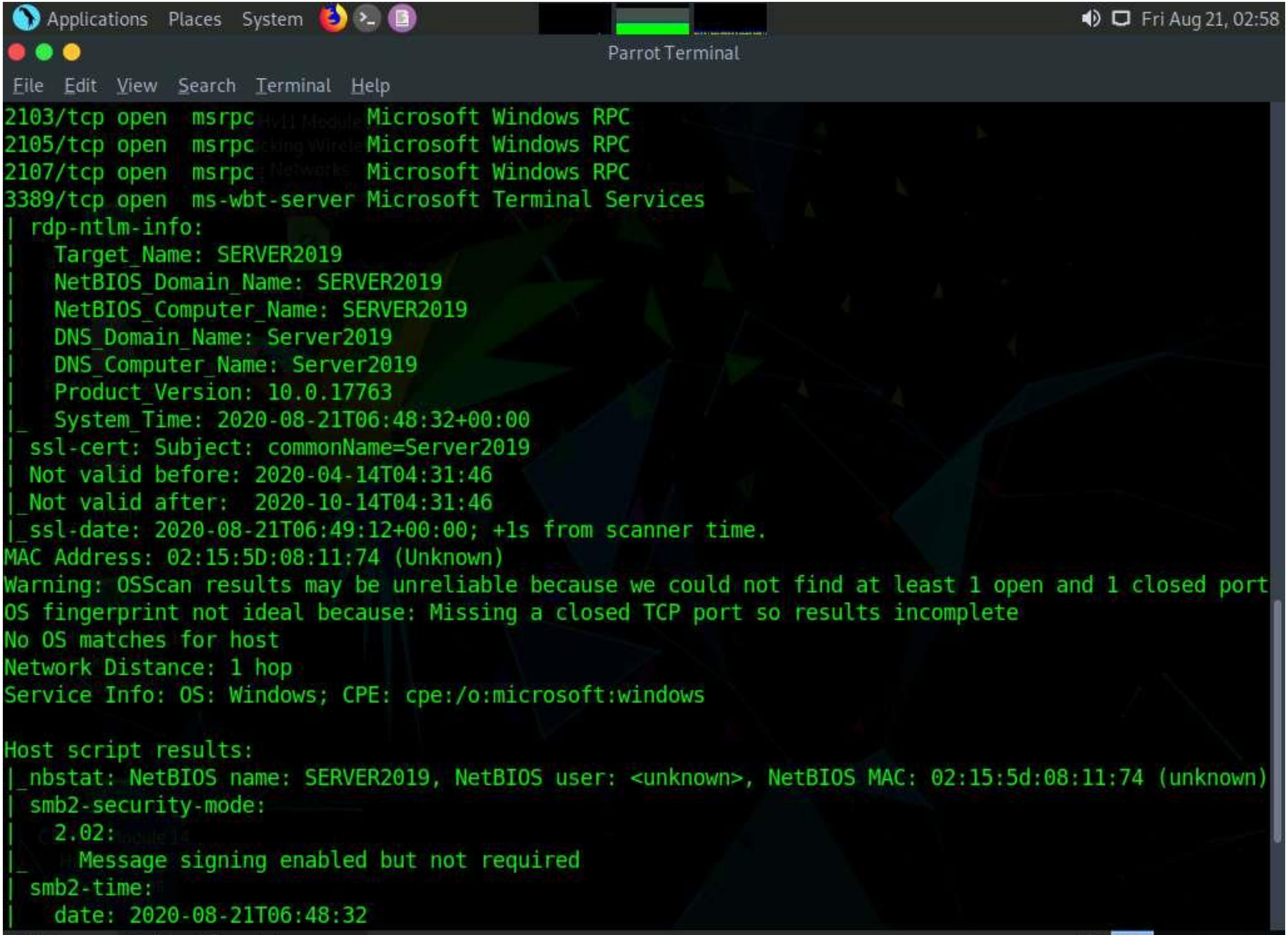


```
┌─[root@parrot]─[~]
└──╼ #nmap -T4 -A 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 02:47 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00096s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: GoodShopping
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
```

20. □ The scan result appears, displaying that port 80 is open, and giving detailed information about the services running on it, along with their versions.



```
|_http-server-header: Microsoft-IIS/10.0
|_http-title: GoodShopping
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2049/tcp open  mountd        1-3 (RPC #100005)
```



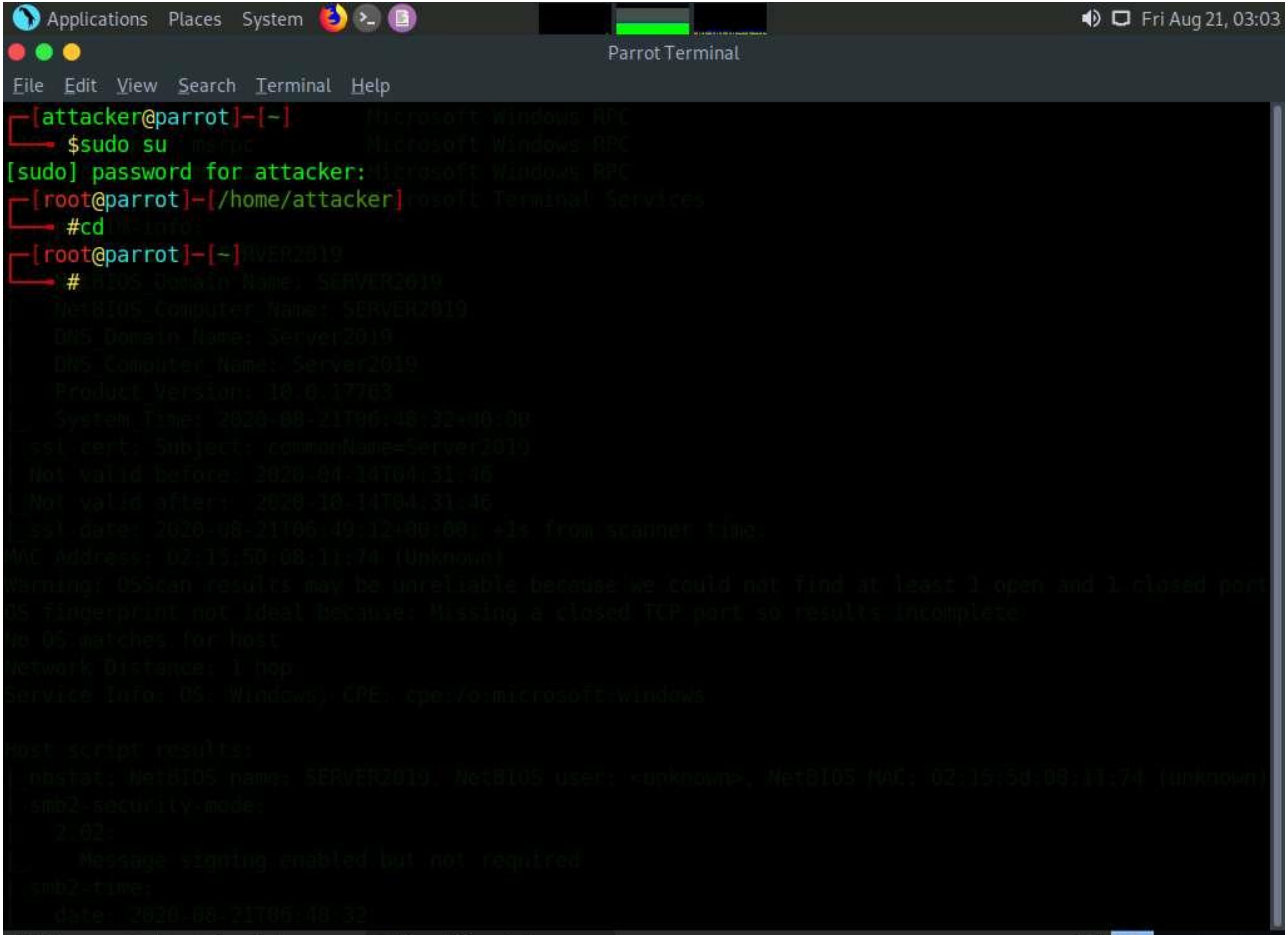
Applications Places System
Fri Aug 21, 02:58
Parrot Terminal
File Edit View Search Terminal Help

```
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_  System_Time: 2020-08-21T06:48:32+00:00
| ssl-cert: Subject: commonName=Server2019
| Not valid before: 2020-04-14T04:31:46
|_Not valid after:  2020-10-14T04:31:46
|_ssl-date: 2020-08-21T06:49:12+00:00; +1s from scanner time.
MAC Address: 02:15:5D:08:11:74 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:08:11:74 (unknown)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-21T06:48:32
```

21. □ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
22. □ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
23. □ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

24. □ Now, type **cd** and press **Enter** to jump to the root directory.

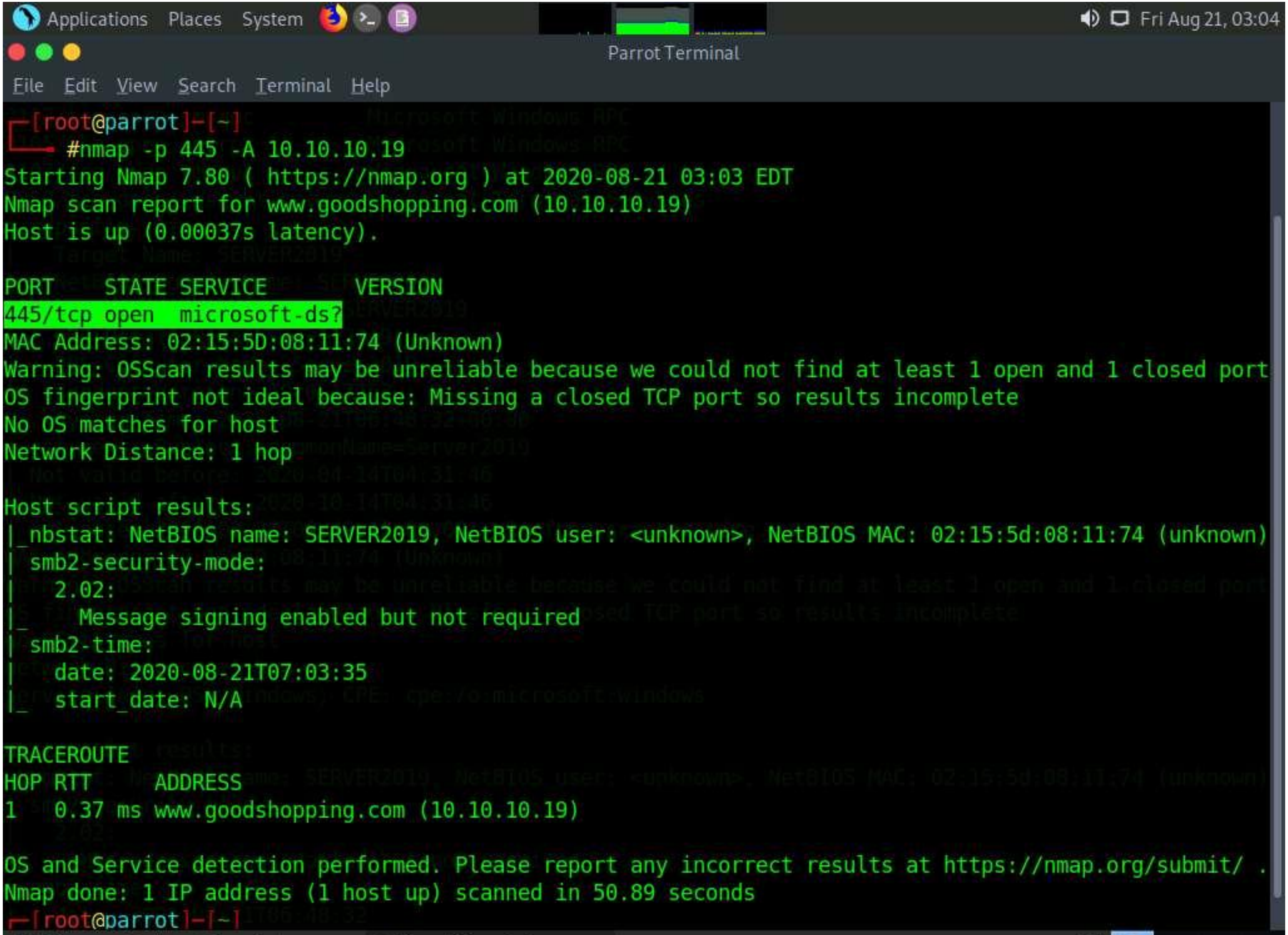


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

25. □ In the terminal window, type **nmap -p [Target Port] -A [Target IP Address]** (in this example, the target port is **445** and the target IP address is **10.10.10.19**) and press **Enter**.

In this command, **-p** specifies the port to be scanned, and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

26. □ The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.

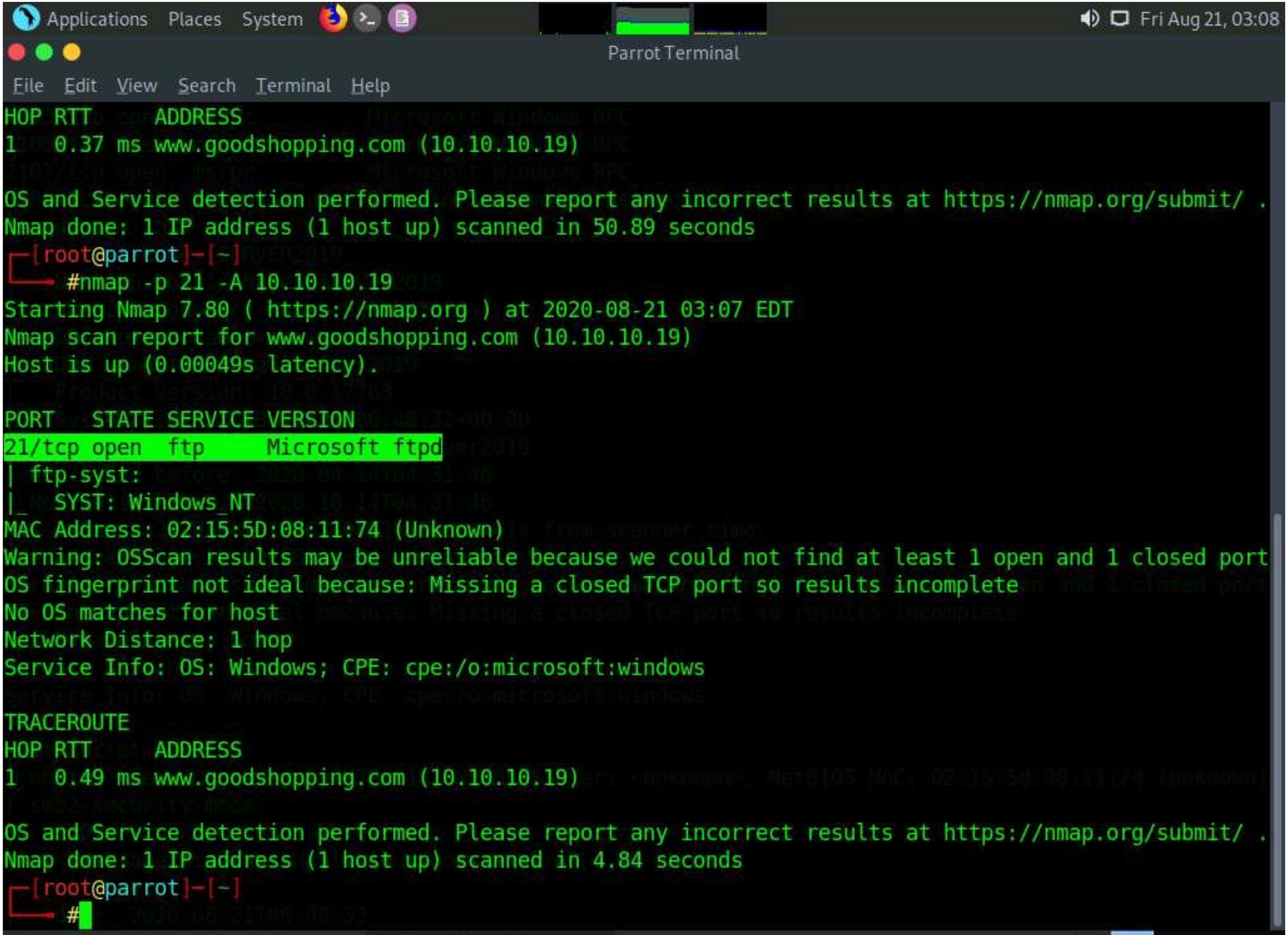


```
┌─[root@parrot]─[~]
└──╼ #nmap -p 445 -A 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 03:03 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00037s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 02:15:5D:08:11:74 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:08:11:74 (unknown)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-21T07:03:35
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 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 50.89 seconds
┌─[root@parrot]─[~]
```

27. □ In the terminal window, type **nmap -p [Target Port] -A [Target IP Address]** (in this example, the target port is **21** and target IP address is **10.10.10.19**) and press **Enter**.

    In this command, **-p** specifies the port to be scanned and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

28. □ The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.



```
HOP RTT     ADDRESS
1   0.37 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 50.89 seconds
┌─[root@parrot]─[~]
└──╼ #nmap -p 21 -A 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 03:07 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: 02:15:5D:08:11:74 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
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 4.84 seconds
┌─[root@parrot]─[~]
└──╼ #
```

29. □ This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.

30. □ Close all open windows and document all the acquired information.