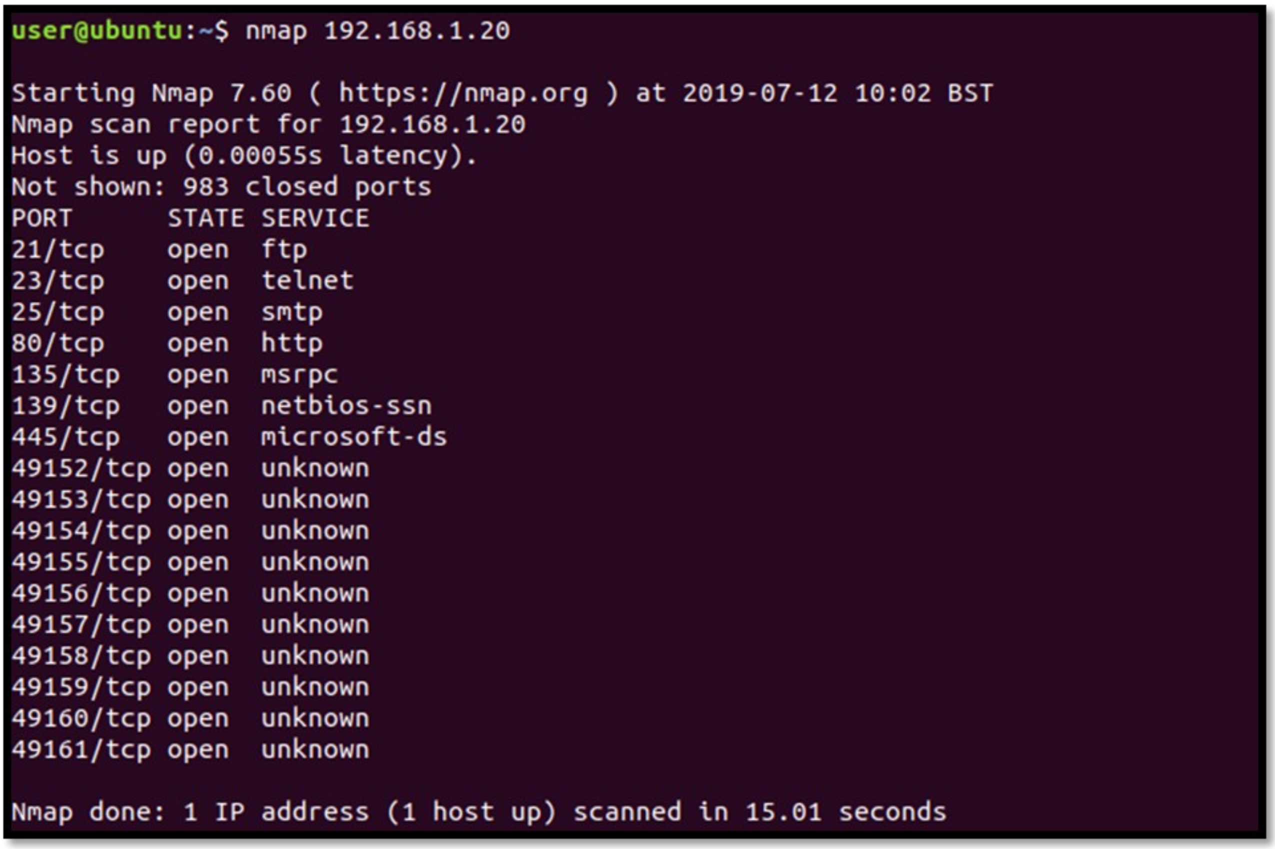
10.4 Guided Exercise: Probing the Network

Resources	
Files	None
Machines	Ubuntu Server, Windows Server, Windows 10

In this exercise you will use a tool called Nmap to scan and identify open ports on the Windows Server and Windows 10.

Login to Ubuntu Server. Once logged in run the command nmap 192.168.1.20 to find which ports are open on Windows Server.

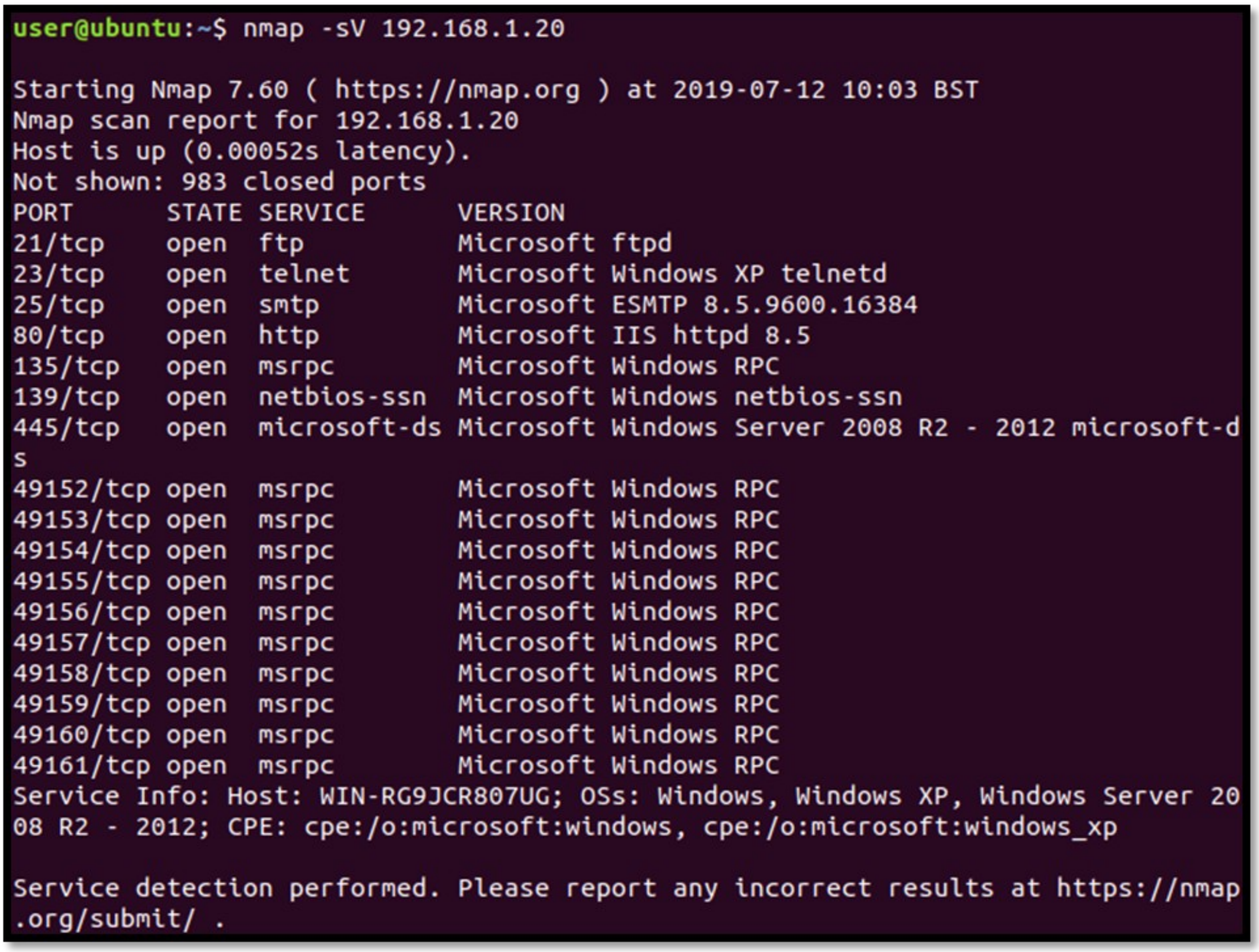


```
user@ubuntu:~$ nmap 192.168.1.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:02 BST
Nmap scan report for 192.168.1.20
Host is up (0.00055s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

Determine the actual service running on each port by running the command “nmap –sV 192.168.1.20”

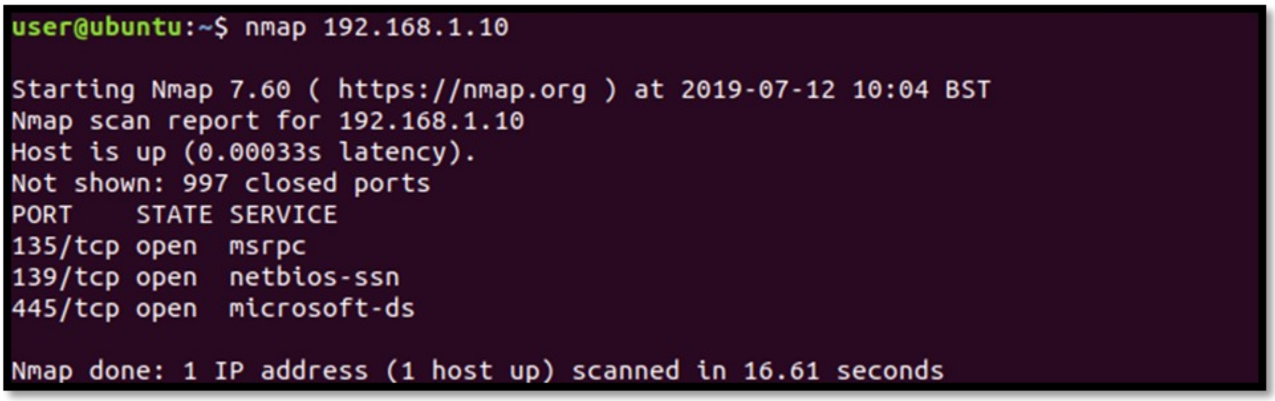


```
user@ubuntu:~$ nmap -sV 192.168.1.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:03 BST
Nmap scan report for 192.168.1.20
Host is up (0.00052s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         Microsoft ESMTP 8.5.9600.16384
80/tcp    open  http         Microsoft IIS httpd 8.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-d
s
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-RG9JCR807UG; OSs: Windows, Windows XP, Windows Server 20
08 R2 - 2012; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

Run the command nmap 192.168.1.10 to identify the open ports on the Windows 10 machine.

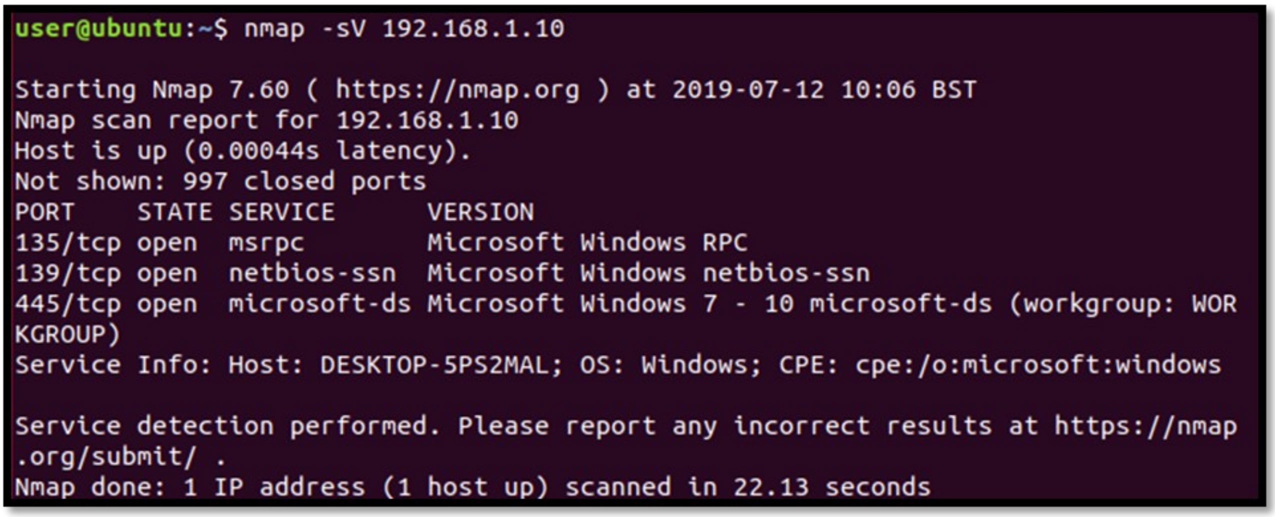


```
user@ubuntu:~$ nmap 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:04 BST
Nmap scan report for 192.168.1.10
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
```

Run the command nmap –sV 192.168.1.10 to identify theactual service running on the open ports.



```
user@ubuntu:~$ nmap -sV 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:06 BST
Nmap scan report for 192.168.1.10
Host is up (0.00044s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WOR
KGROUP)
Service Info: Host: DESKTOP-5PS2MAL; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.13 seconds
```