Lab 6 Part 1: Port Scanning

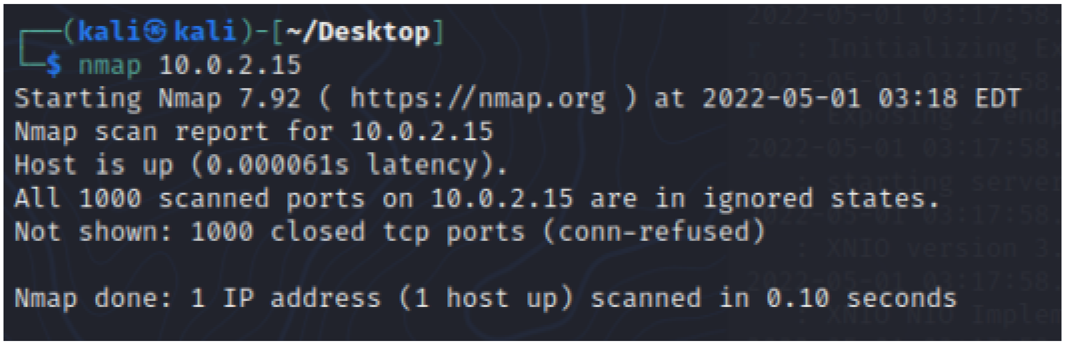
Introduction:

Port scanning is yet another technique that hackers and penetration testers can use to identify vulnerabilities in an organization and exploit them. Port scanning is often very resource intensive and is usually done after having conducted reconnaissance on a target organization. The focus of this lab will be on the use of various different port scanning utilities. Namely, the command line based nmap, and the GUI based Zenmap. We will then see how port scanning can be used in conjunction with packet sniffers and crafters to identify active hosts on a network that may exist behind a firewall.

Part 1: Using nmap

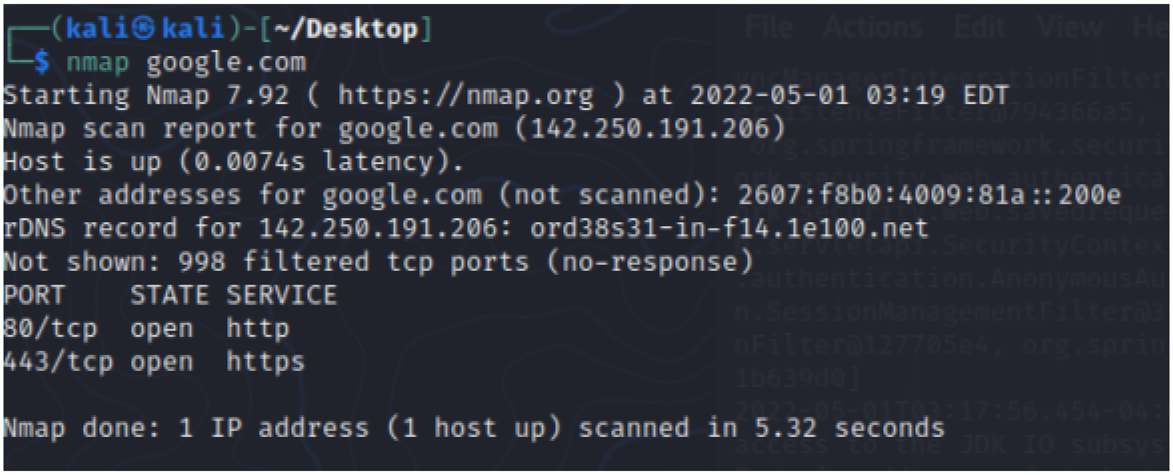
Nmap is a widely used command line port scanner that can be customized to suit a wide variety of port scanning and footprinting needs. The utility comes preinstalled on our kali VM, and its functionality can be viewed using the man command. The following figures demonstrate the basic use of nmap.

Figure 1: nmap of Kali VM Attached to NAT:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:18 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000061s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

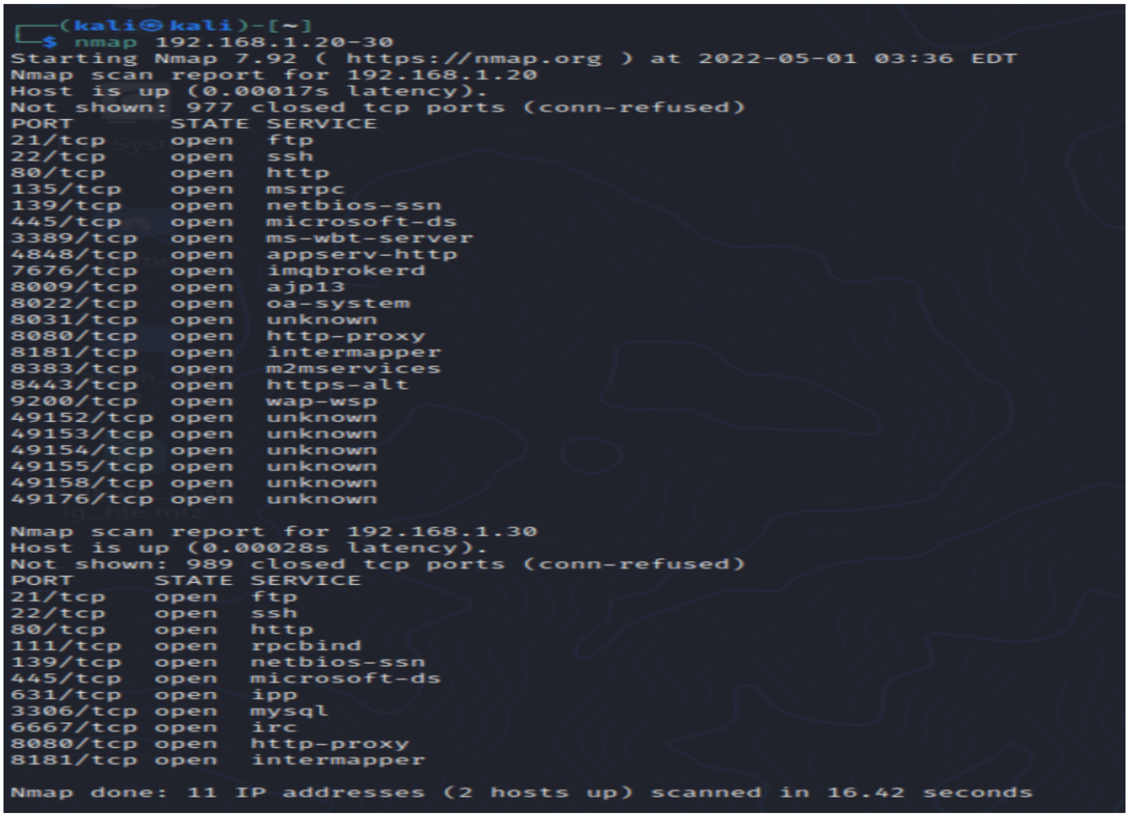
Figure 2: nmap of Google



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:19 EDT
Nmap scan report for google.com (142.250.191.206)
Host is up (0.0074s latency).
Other addresses for google.com (not scanned): 2607:f8b0:4009:81a::200e
rDNS record for 142.250.191.206: ord38s31-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
```

We can see in the output the various different ports and services open and running on the domain/ip that we search.

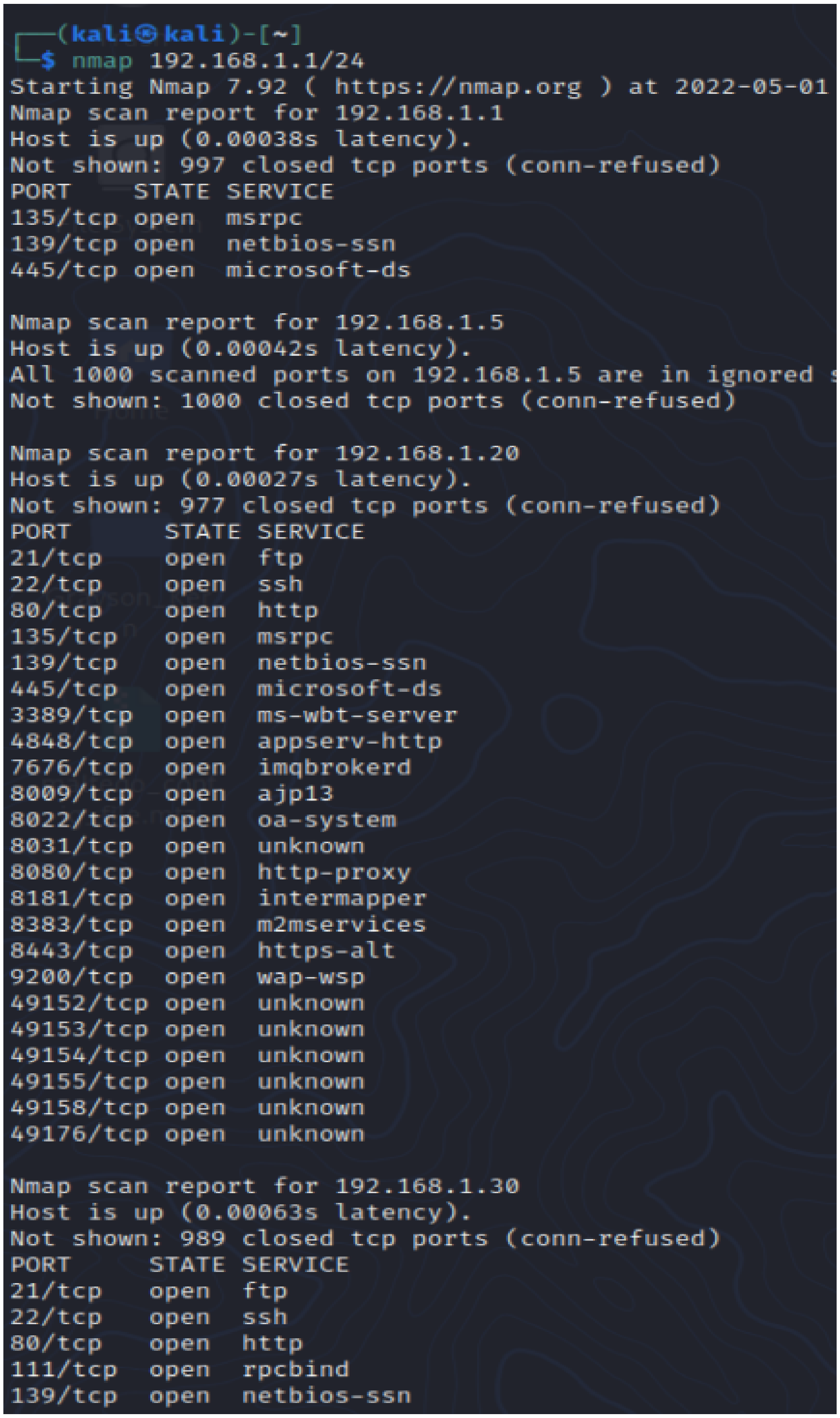
Figure 3: nmap on Range of IP addresses



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20-30
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:36 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49176/tcp open  unknown

Nmap scan report for 192.168.1.30
Host is up (0.00028s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql
6667/tcp open  irc
8080/tcp open  http-proxy
8181/tcp open  intermapper

Nmap done: 11 IP addresses (2 hosts up) scanned in 16.42 seconds
```

Here we demonstrate the ability of nmap to scan a range of IP addresses by switching our Kali VM back to host only networking, and running our windows 2k8 and Ubuntu VMs in the background.

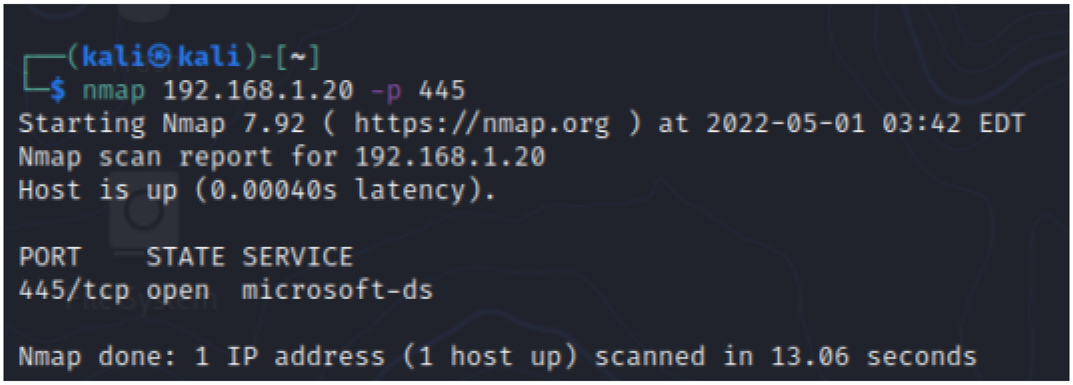
Figure 4: nmap on a Subnet of IP Addresses



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01
Nmap scan report for 192.168.1.1
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.1.5
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.1.20
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49176/tcp open  unknown

Nmap scan report for 192.168.1.30
Host is up (0.00063s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
```

Nmap can also be used to scan a range of ip addresses in a particular subnet using the above notation.

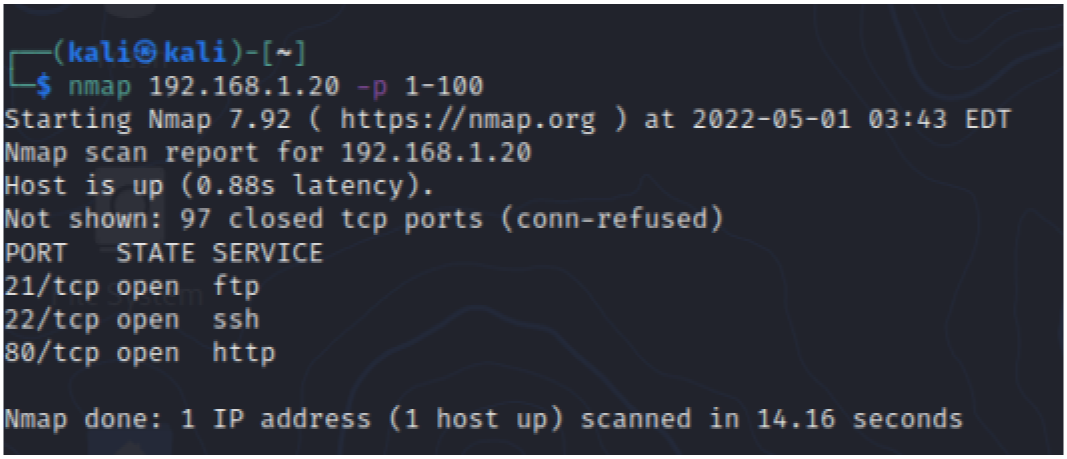
Figure 5: Using nmap to scan a particular port



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20 -p 445
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:42 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00040s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```

Many applications with vulnerabilities often run on a certain port. We can refine the output of nmap to a particular port.

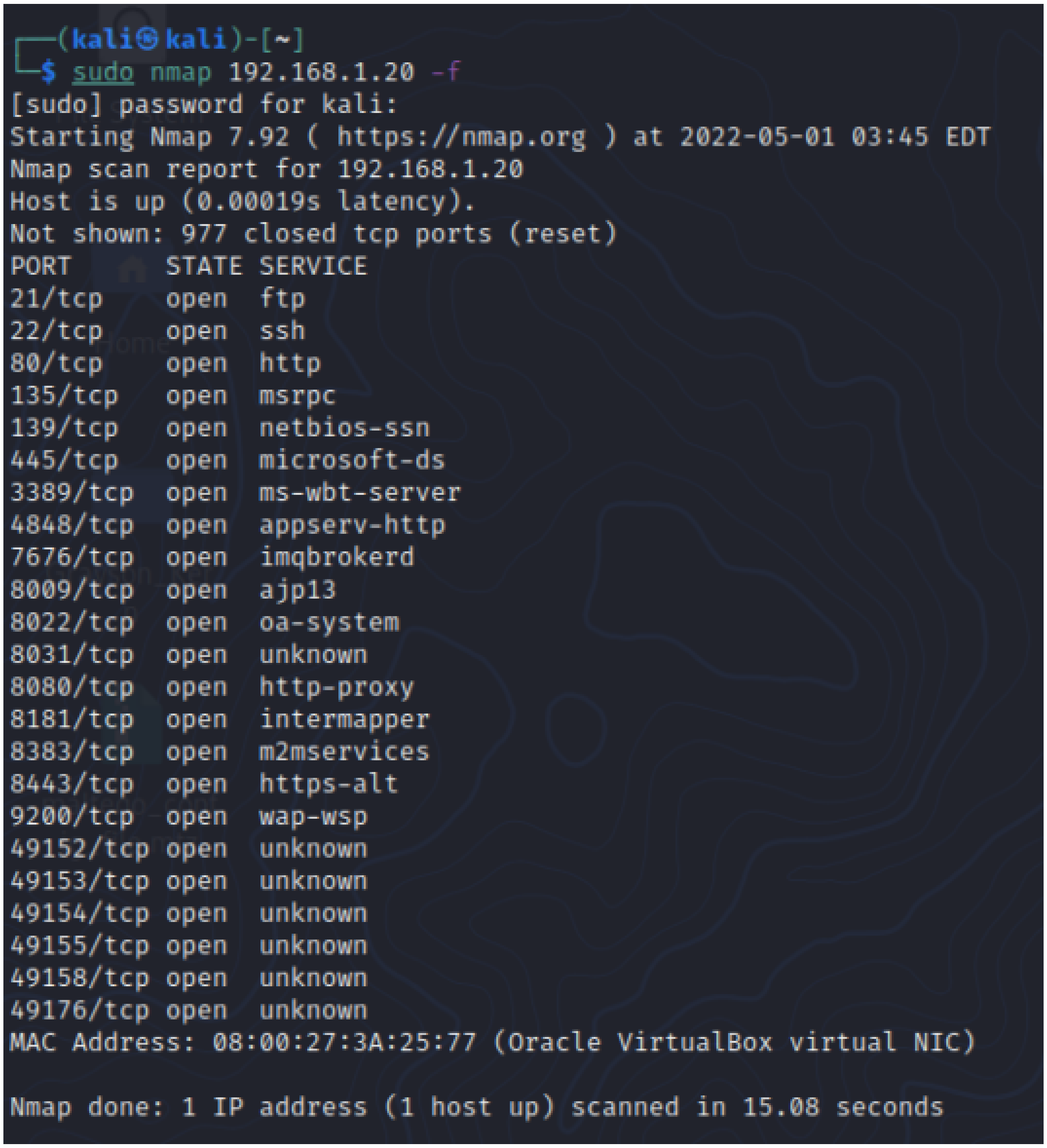
Figure 6: Using nmap to scan a range of ports



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20 -p 1-100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:43 EDT
Nmap scan report for 192.168.1.20
Host is up (0.88s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds
```

Nmap can also be used to scan a range of ports with the above notation.

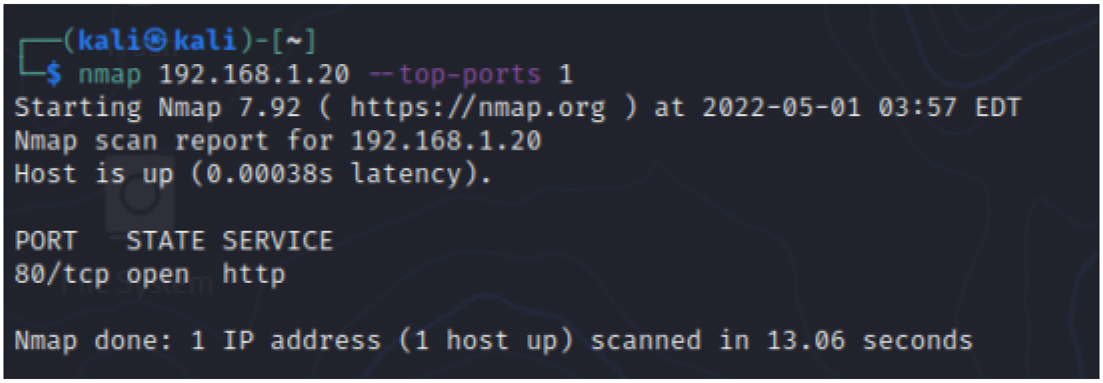
Figure 7: Using nmap to scan the most common ports



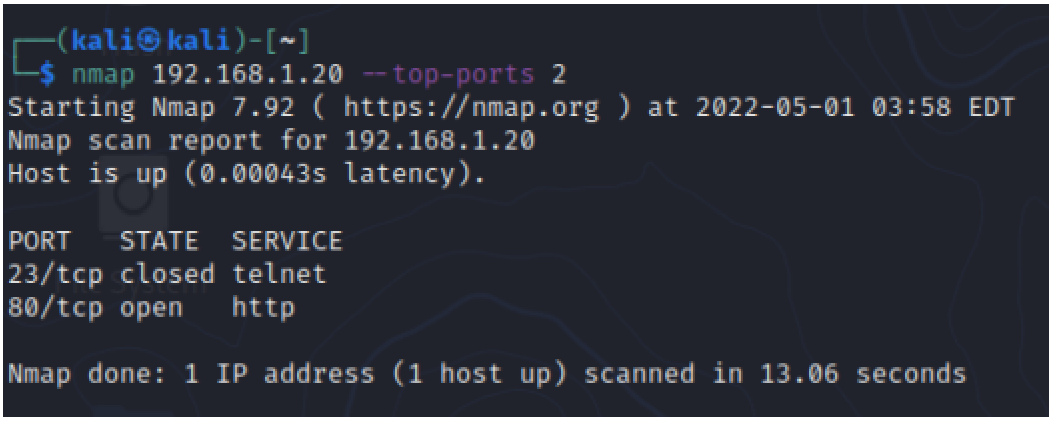
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.1.20 -f
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:45 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49176/tcp open  unknown
MAC Address: 08:00:27:3A:25:77 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds
```

Nmap supports a fast scan of some of the most common ports. The output above shows what they are.

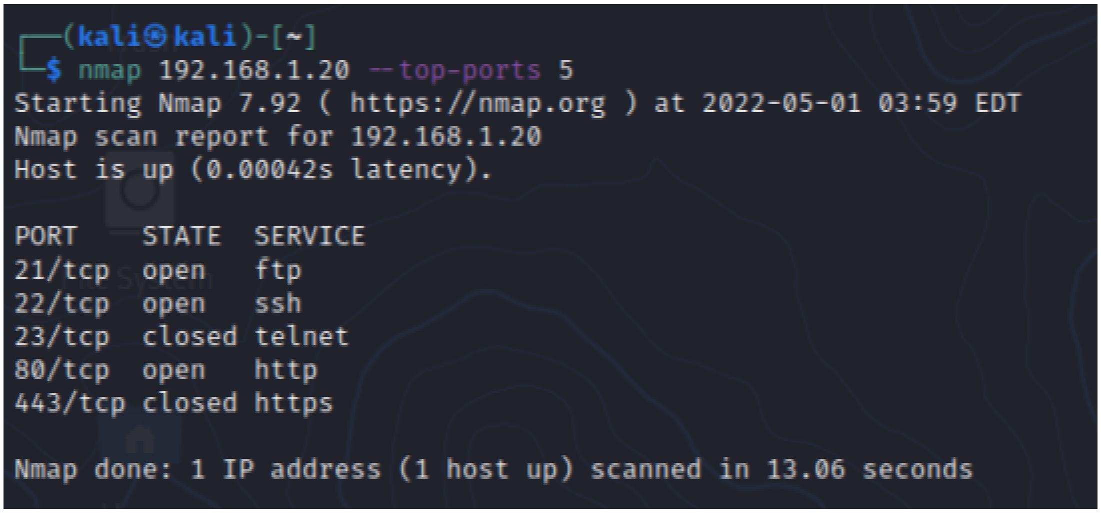
Figure 8: Using nmap to scan the top n ports



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20 --top-ports 1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:57 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00038s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```



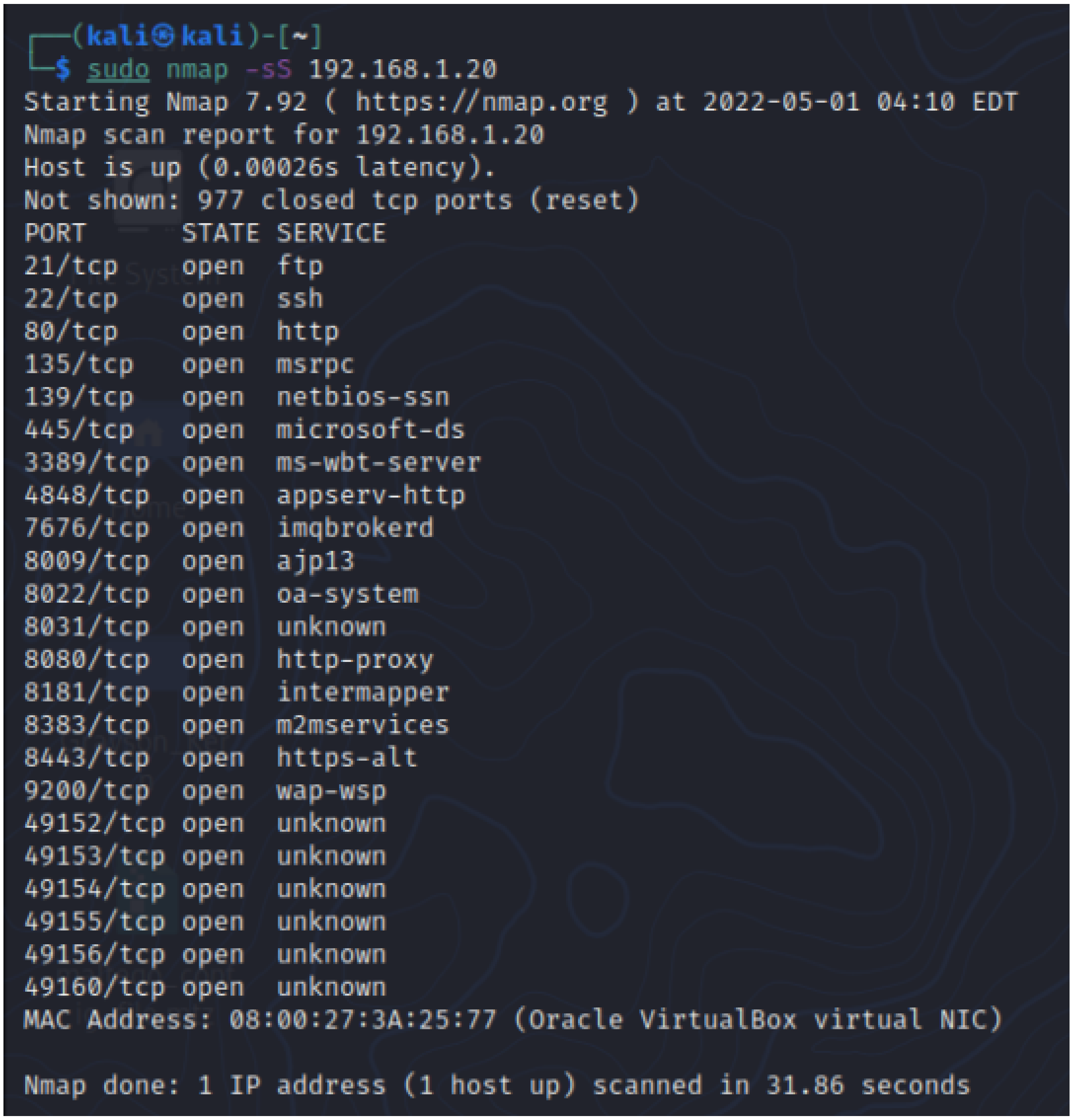
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20 --top-ports 2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:58 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00043s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```



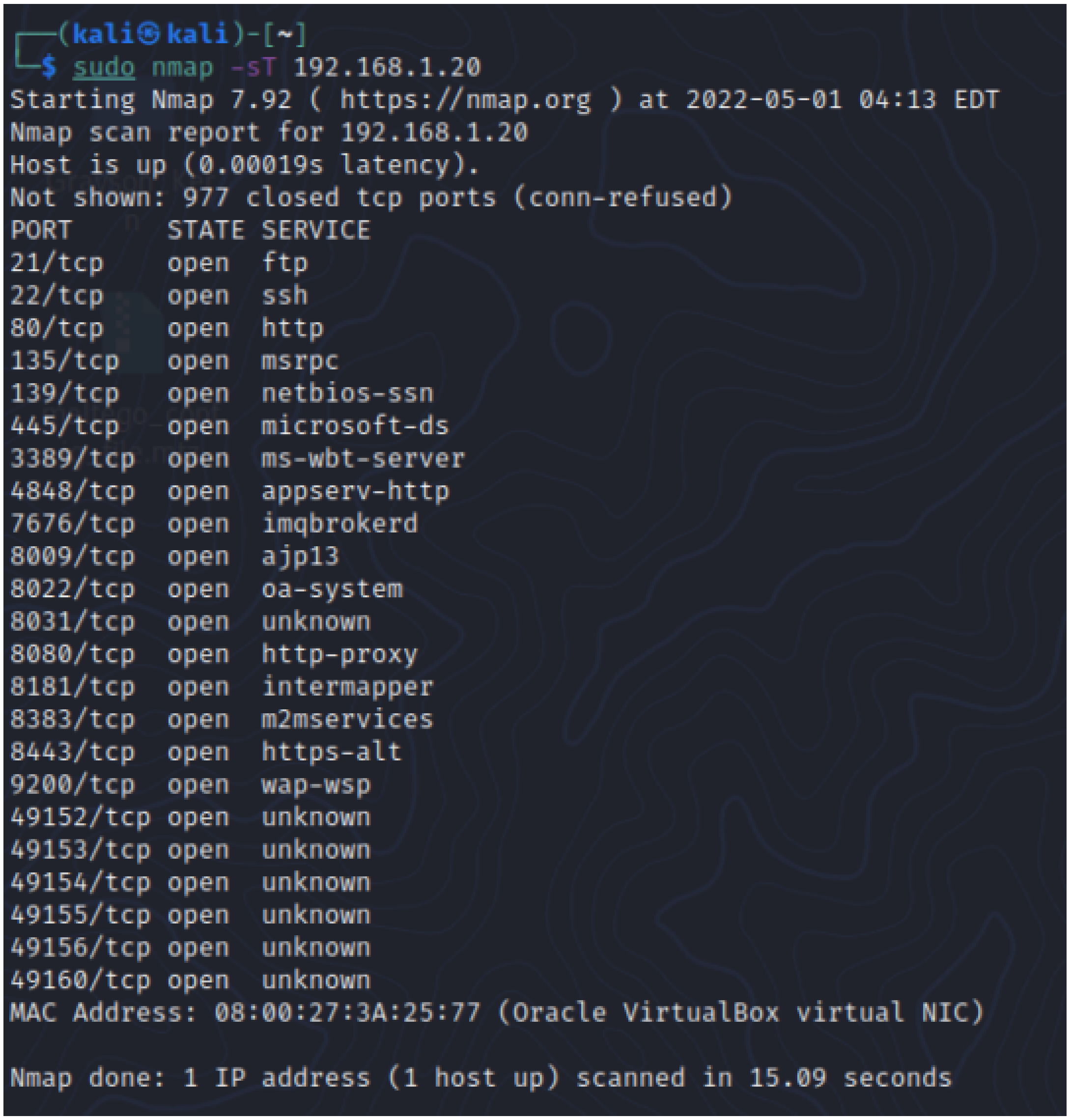
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.20 --top-ports 5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 03:59 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00042s latency).

PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  closed telnet
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
```

The output of the fast scan can further be refined using the –top-ports flag. Here we can see what the software considers to be the most common ports.

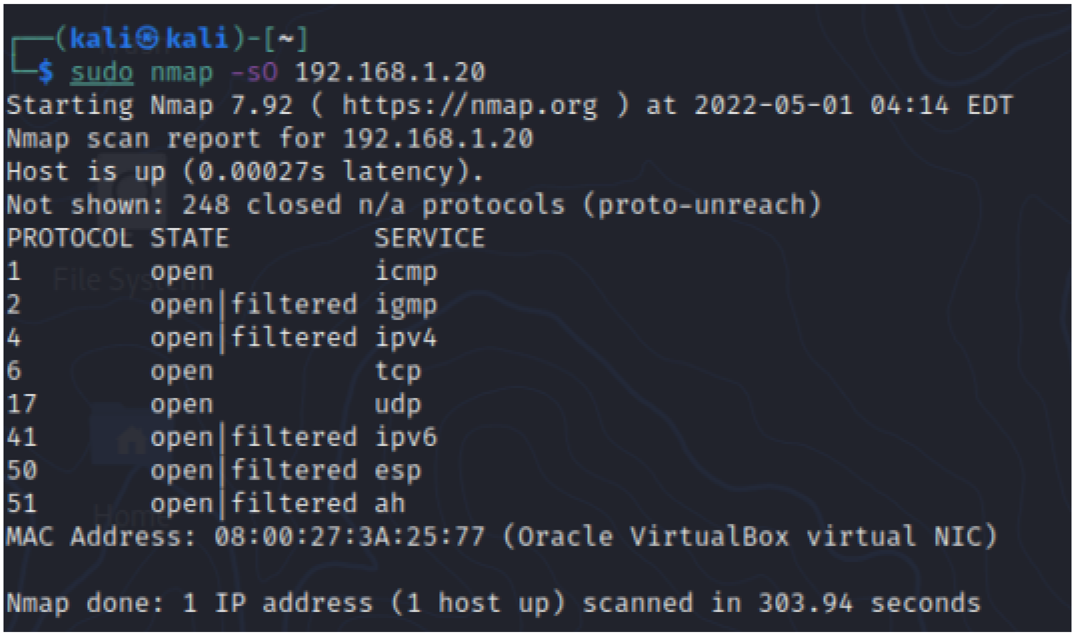
Figure 9: nmap scan types



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:10 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:3A:25:77 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.86 seconds
```



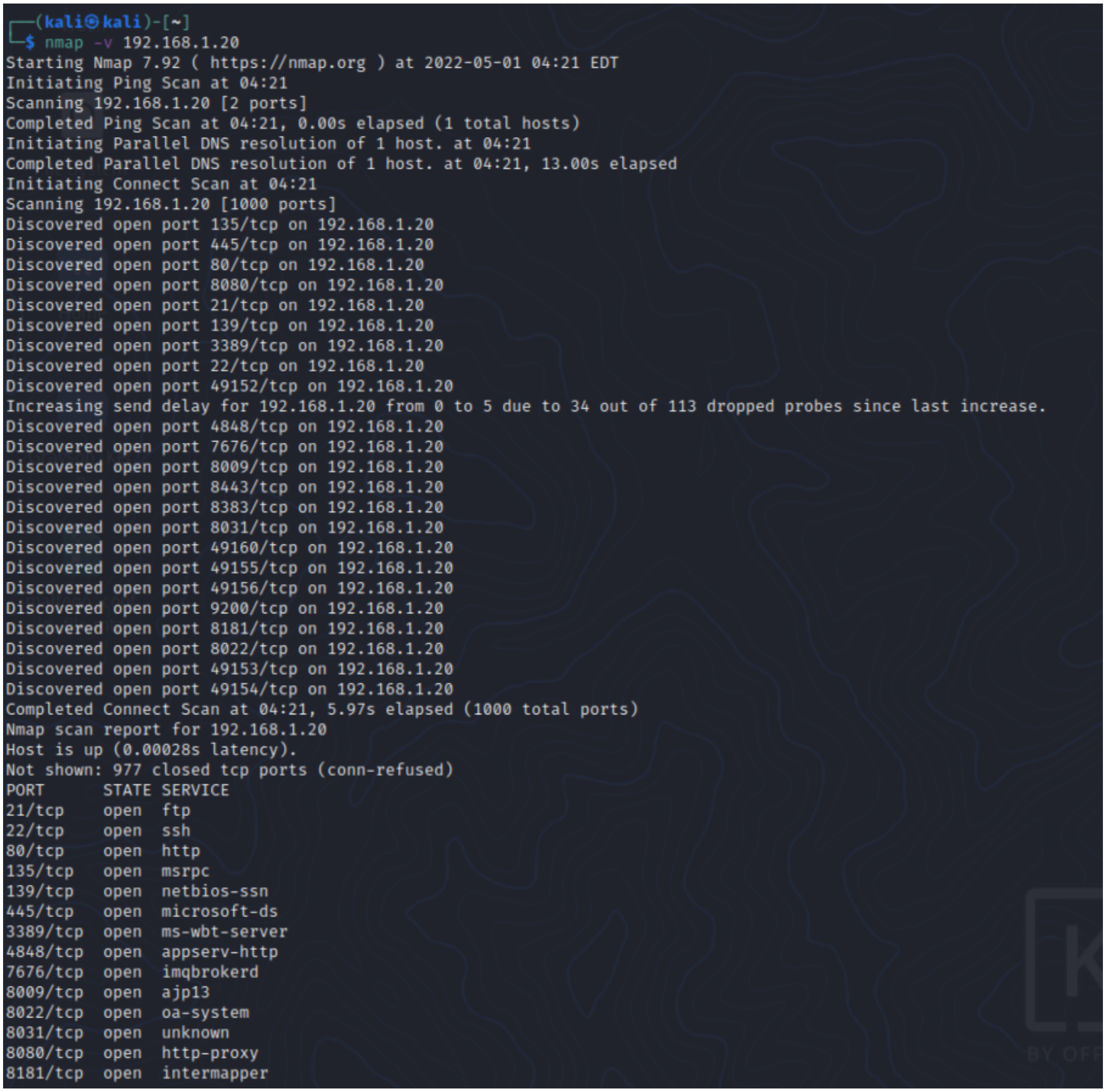
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:13 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:3A:25:77 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sO 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:14 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00027s latency).
Not shown: 248 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
4        open|filtered ipv4
6        open          tcp
17       open          udp
41       open|filtered ipv6
50       open|filtered esp
51       open|filtered ah
MAC Address: 08:00:27:3A:25:77 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 303.94 seconds
```

Hackers and testers can use different nmap scan types based on the information they know about a target organization. I.e its footprint in terms of domains, subdomains, DNS servers etc. Certain scans are more resource intensive than others, as the above outputs show.

Figure 10: nmap Verbose output



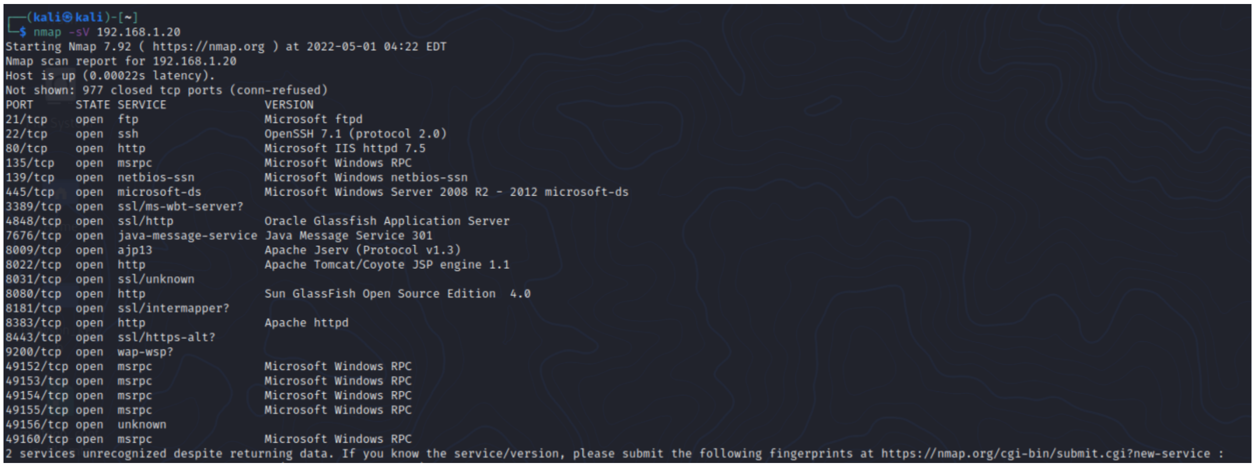
```
┌──(kali㉿kali)-[~]
└─$ nmap -v 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:21 EDT
Initiating Ping Scan at 04:21
Scanning 192.168.1.20 [2 ports]
Completed Ping Scan at 04:21, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:21
Completed Parallel DNS resolution of 1 host. at 04:21, 13.00s elapsed
Initiating Connect Scan at 04:21
Scanning 192.168.1.20 [1000 ports]
Discovered open port 135/tcp on 192.168.1.20
Discovered open port 445/tcp on 192.168.1.20
Discovered open port 80/tcp on 192.168.1.20
Discovered open port 8080/tcp on 192.168.1.20
Discovered open port 21/tcp on 192.168.1.20
Discovered open port 139/tcp on 192.168.1.20
Discovered open port 3389/tcp on 192.168.1.20
Discovered open port 22/tcp on 192.168.1.20
Discovered open port 49152/tcp on 192.168.1.20
Increasing send delay for 192.168.1.20 from 0 to 5 due to 34 out of 113 dropped probes since last increase.
Discovered open port 4848/tcp on 192.168.1.20
Discovered open port 7676/tcp on 192.168.1.20
Discovered open port 8009/tcp on 192.168.1.20
Discovered open port 8443/tcp on 192.168.1.20
Discovered open port 8383/tcp on 192.168.1.20
Discovered open port 8031/tcp on 192.168.1.20
Discovered open port 49160/tcp on 192.168.1.20
Discovered open port 49155/tcp on 192.168.1.20
Discovered open port 49156/tcp on 192.168.1.20
Discovered open port 9200/tcp on 192.168.1.20
Discovered open port 8181/tcp on 192.168.1.20
Discovered open port 8022/tcp on 192.168.1.20
Discovered open port 49153/tcp on 192.168.1.20
Discovered open port 49154/tcp on 192.168.1.20
Completed Connect Scan at 04:21, 5.97s elapsed (1000 total ports)
Nmap scan report for 192.168.1.20
Host is up (0.00028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
```

In the event that none of the nmap scan types provide the hacker the information of interest, one can always use nmap's verbose flag to get more output.

Part 2: Service and OS Detection

As mentioned above, nmap is widely used for port scanning to detect vulnerabilities in a network. These vulnerabilities are first identified by knowing what softwares and services an organization is using. I.e server software and operating systems. The figures below show how nmap can be configured to show these details about an organization.

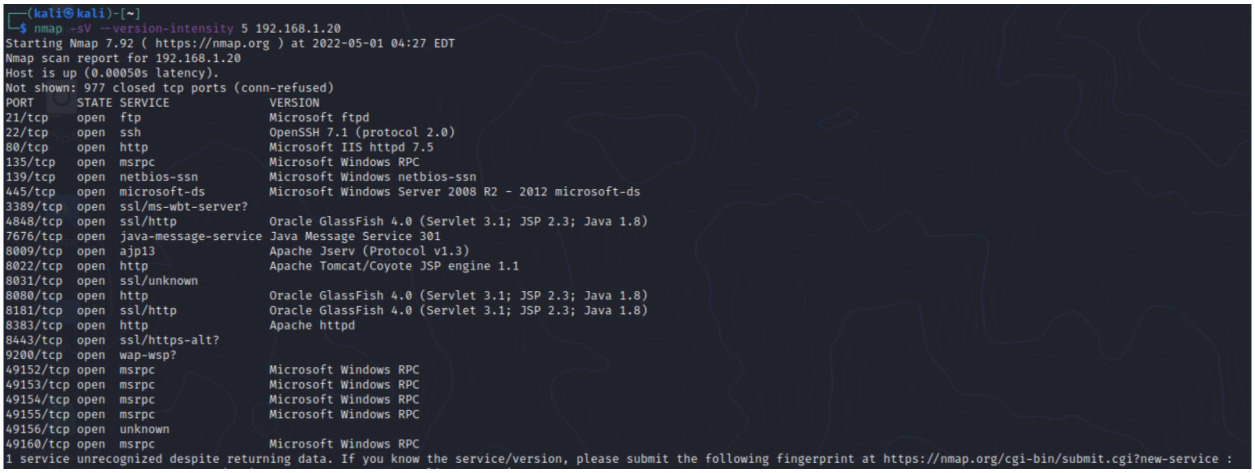
Figure 11: nmap service scan on windows 2k8 VM



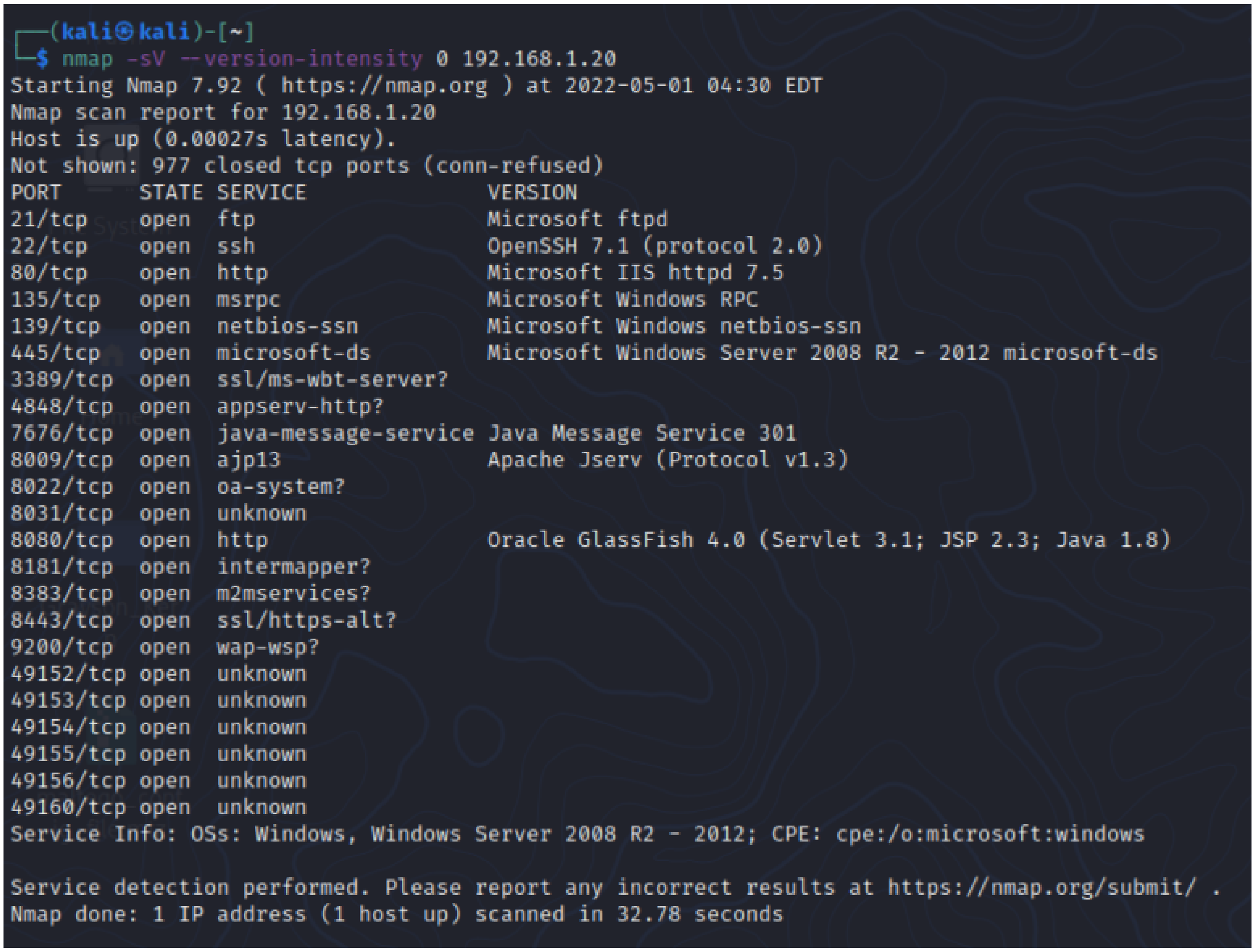
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:22 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                 Microsoft IIS httpd 7.5
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-ds
3389/tcp  open  ssl/ms-wbt-server?
4848/tcp  open  ssl/http             Oracle Glassfish Application Server
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http                 Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
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  unknown
49160/tcp open  msrpc                Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Here we can see a list of services running on the machine, as well as their associated ports.

Figure 12: nmap service scans with varying intensity levels



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-intensity 5 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:27 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                 Microsoft IIS httpd 7.5
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-ds
3389/tcp  open  ssl/ms-wbt-server?
4848/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http                 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  http                 Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
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  unknown
49160/tcp open  msrpc                Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```



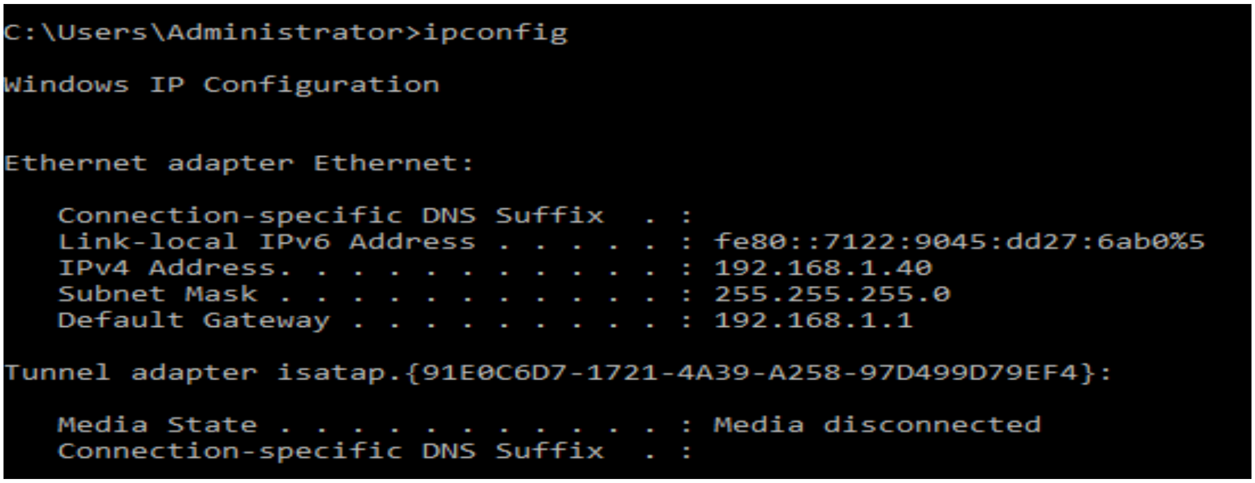
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-intensity 0 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 04:30 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                 Microsoft IIS httpd 7.5
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-ds
3389/tcp  open  ssl/ms-wbt-server?
4848/tcp  open  appserv-http?
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8022/tcp  open  oa-system?
8031/tcp  open  unknown
8080/tcp  open  http                 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  intermapper?
8383/tcp  open  m2mservices?
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; 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 32.78 seconds
```

The intensity level of nmap’s service scan can be further refined with the above flags.

Part 3: Using Zenmap to Scan a Target Network

Zenmap is a GUI alternative to nmap that often simplifies the processing of port scanning, and makes the output of nmap much more readable and useful. Both tools have their use cases depending on the organization one wishes to scan. The figures below demonstrate the use of Zenmap, and how it compares to nmap.

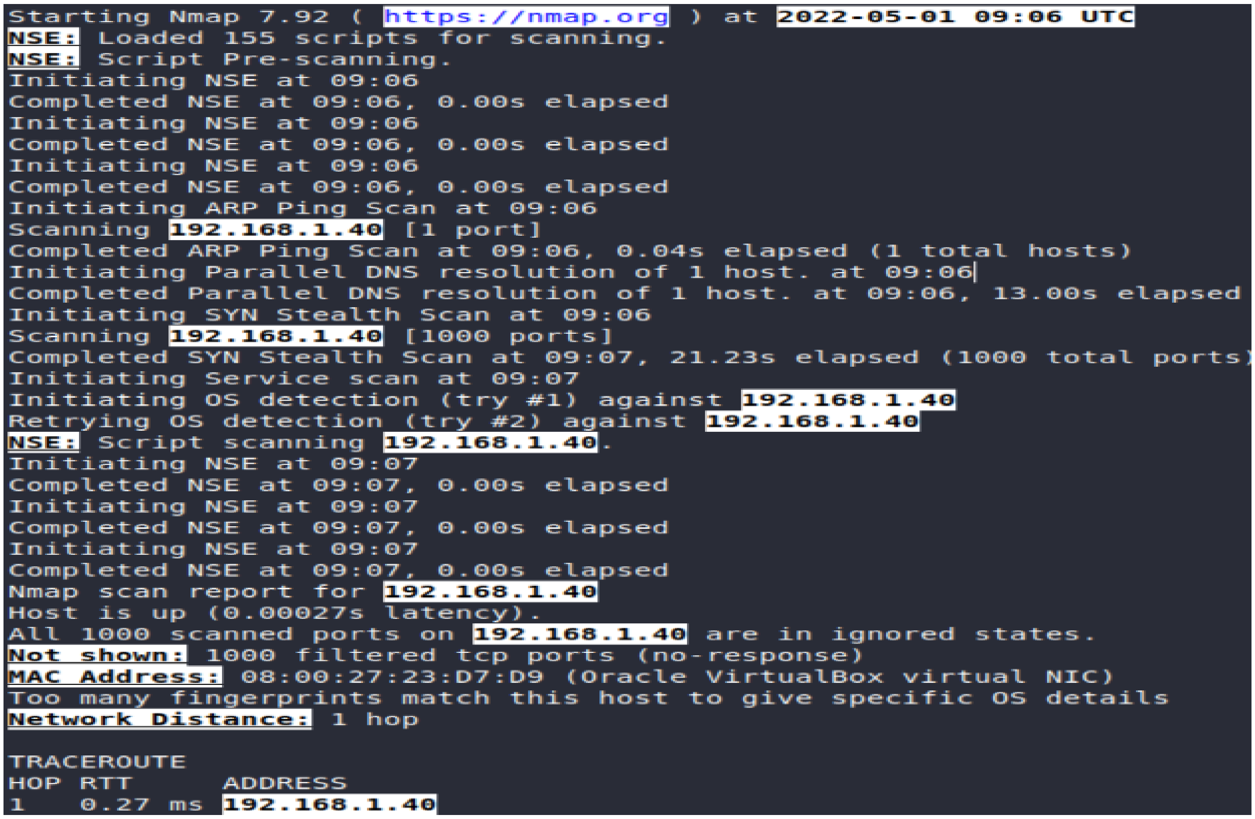
Figure 13: IP address of Windows 2k16 VM



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7122:9045:dd27:6ab0%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.40
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{91E0C6D7-1721-4A39-A258-97D499D79EF4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

We open up our Windows Server 2k16 VM along with the other VMS that are already open. The IP address of the Windows Server 2k16 VM is shown above.

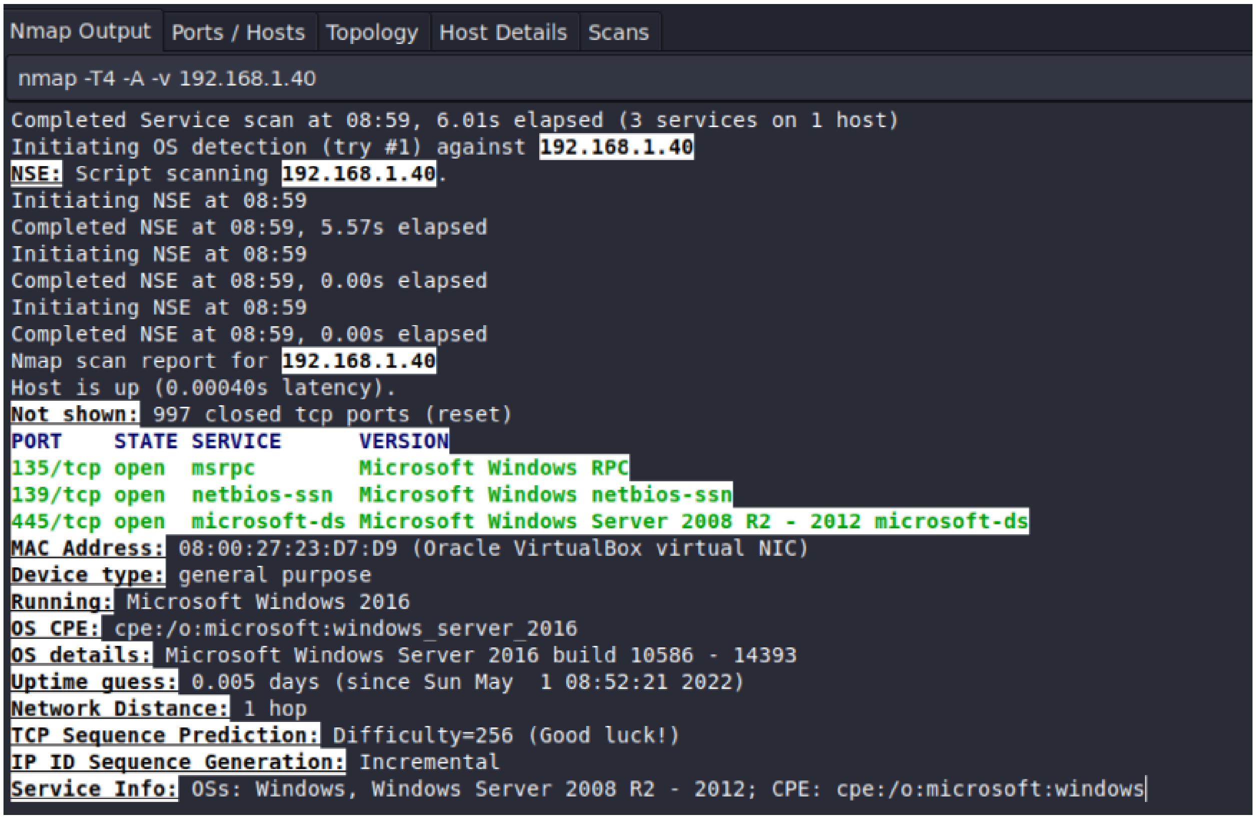
Figure 14: Zenmap with Windows Firewall



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 09:06 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:06
Completed NSE at 09:06, 0.00s elapsed
Initiating NSE at 09:06
Completed NSE at 09:06, 0.00s elapsed
Initiating NSE at 09:06
Completed NSE at 09:06, 0.00s elapsed
Initiating ARP Ping Scan at 09:06
Scanning 192.168.1.40 [1 port]
Completed ARP Ping Scan at 09:06, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:06
Completed Parallel DNS resolution of 1 host. at 09:06, 13.00s elapsed
Initiating SYN Stealth Scan at 09:06
Scanning 192.168.1.40 [1000 ports]
Completed SYN Stealth Scan at 09:07, 21.23s elapsed (1000 total ports)
Initiating Service scan at 09:07
Initiating OS detection (try #1) against 192.168.1.40
Retrying OS detection (try #2) against 192.168.1.40
NSE: Script scanning 192.168.1.40.
Initiating NSE at 09:07
Completed NSE at 09:07, 0.00s elapsed
Initiating NSE at 09:07
Completed NSE at 09:07, 0.00s elapsed
Initiating NSE at 09:07
Completed NSE at 09:07, 0.00s elapsed
Nmap scan report for 192.168.1.40
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.1.40 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:23:D7:D9 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms 192.168.1.40
```

For this test, we turned on the windows firewall and disable all incoming connections from foreigfn networks. We can see here that Windows Firewall, when enabled and running properly, prevents the port scan from running successfully.

Figure 15: Zenmap with Windows Firewall Off



```
nmap -T4 -A -v 192.168.1.40
```

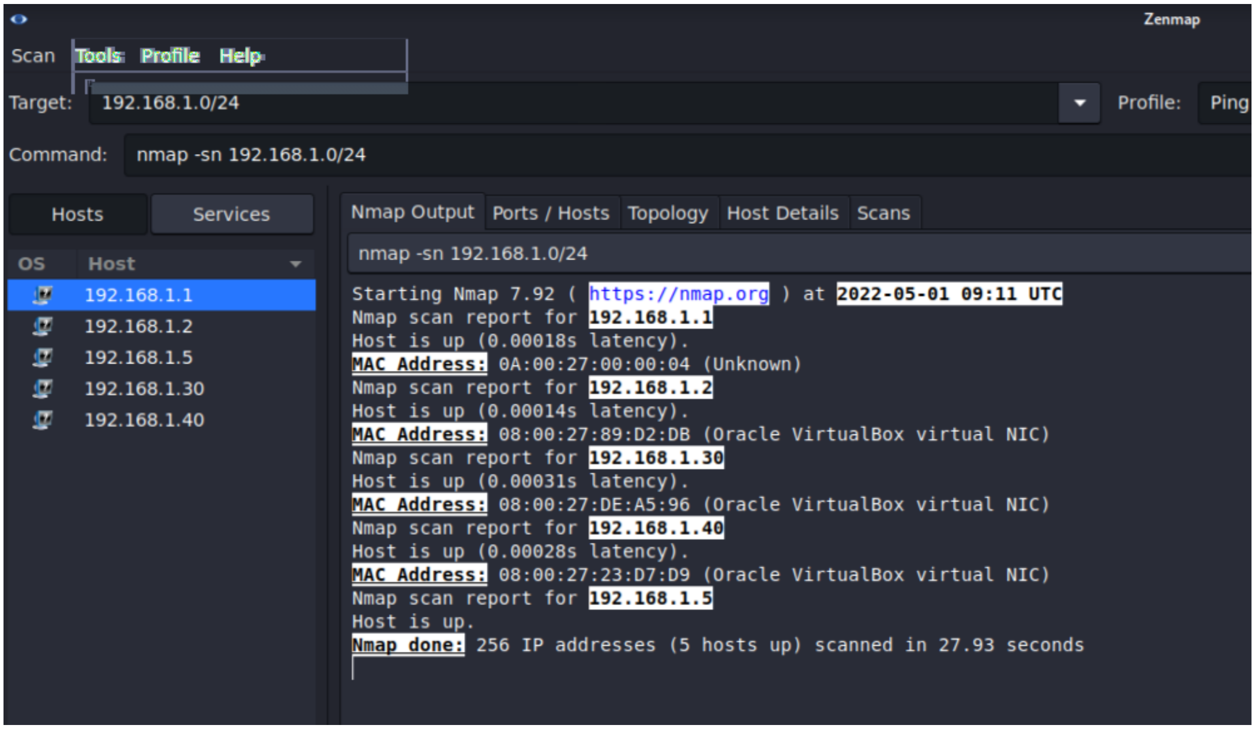
```
Completed Service scan at 08:59, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.40
NSE: Script scanning 192.168.1.40.
Initiating NSE at 08:59
Completed NSE at 08:59, 5.57s elapsed
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Nmap scan report for 192.168.1.40
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (reset)
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 Server 2008 R2 - 2012 microsoft-ds
MAC Address: 08:00:27:23:D7:D9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Uptime guess: 0.005 days (since Sun May  1 08:52:21 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Running the port scan with Windows firewall up shows us the ports that are being used by the machine, as well as by what service and their state. Very valuable for information would be attackers or security professionals. The output here is obviously a great deal more comprehensible than what nmap would provide. Which is why the Zenmap utility is prefered a lot of the time.

Part 3: Analyzing Port Scans

For large organizations, the output of nmap or zenmap can often be difficult or impossible to analyze. Which is where packet sniffers like Wireshark come in. The screenshots below show how Wireshark can be used for this purpose.

Figure 16: Using Zenmap to Ping VM LAN



Target: 192.168.1.0/24

Profile: Ping

Command: nmap -sn 192.168.1.0/24

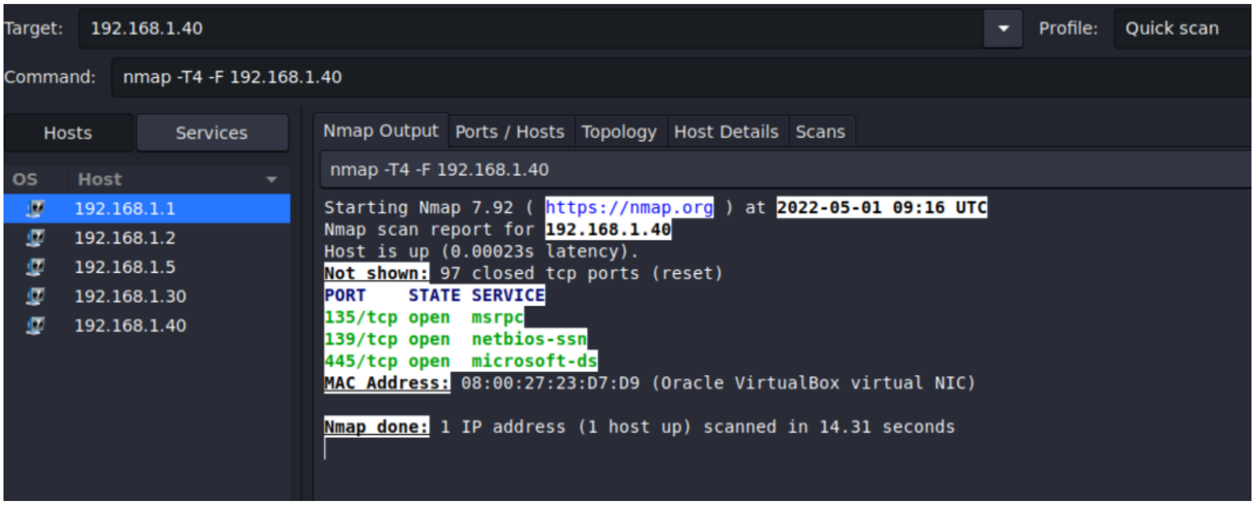
```
192.168.1.1
192.168.1.2
192.168.1.5
192.168.1.30
192.168.1.40
```

```
nmap -sn 192.168.1.0/24
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 09:11 UTC
Nmap scan report for 192.168.1.1
Host is up (0.00018s latency).
MAC Address: 0A:00:27:00:00:04 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.00014s latency).
MAC Address: 08:00:27:89:D2:DB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.30
Host is up (0.00031s latency).
MAC Address: 08:00:27:DE:A5:96 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.40
Host is up (0.00028s latency).
MAC Address: 08:00:27:23:D7:D9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.93 seconds
```

Here we can see a list of host machines that returned packets following our ping of the provided subnet. We see all the VMS currently running, including the Windows Server 2k16 one. Whose IP we have discovered again.

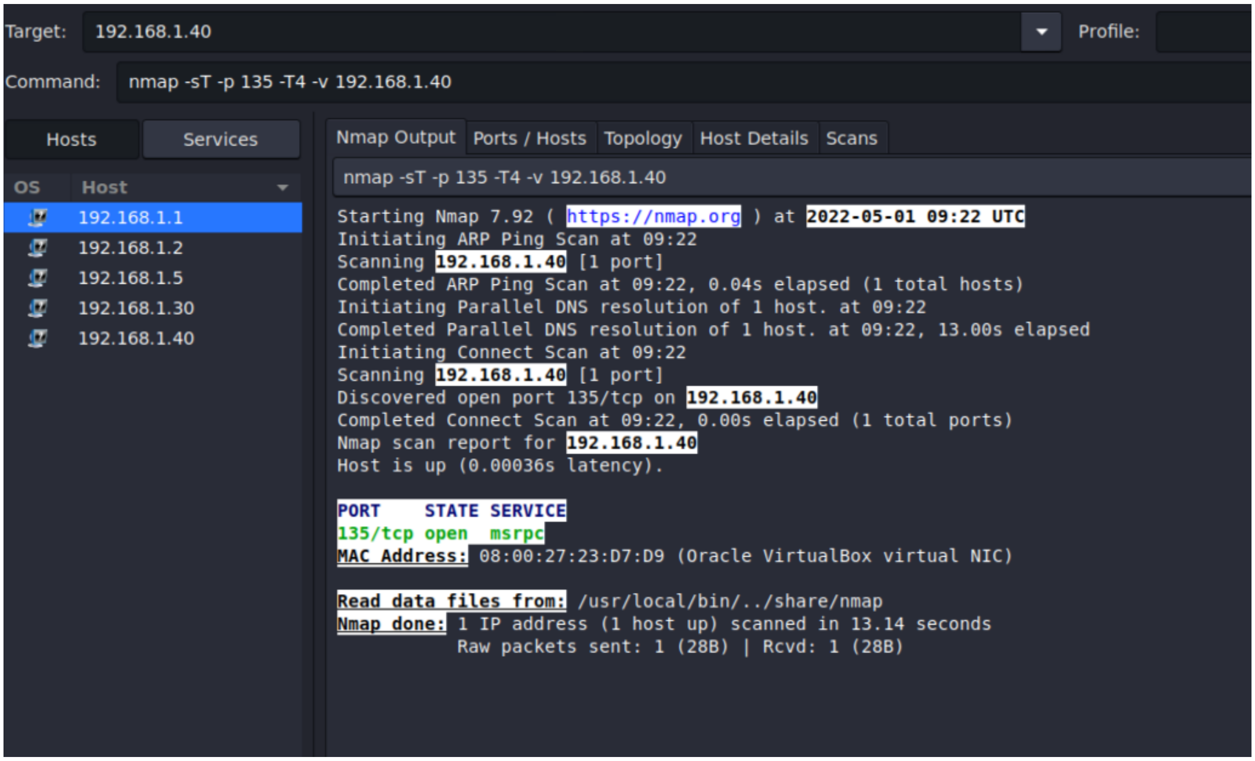
Figure 17: Running Fast Scan on Windows 2k16



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 09:16 UTC
Nmap scan report for 192.168.1.40
Host is up (0.00023s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:23:D7:D9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
```

We see again a list of open ports

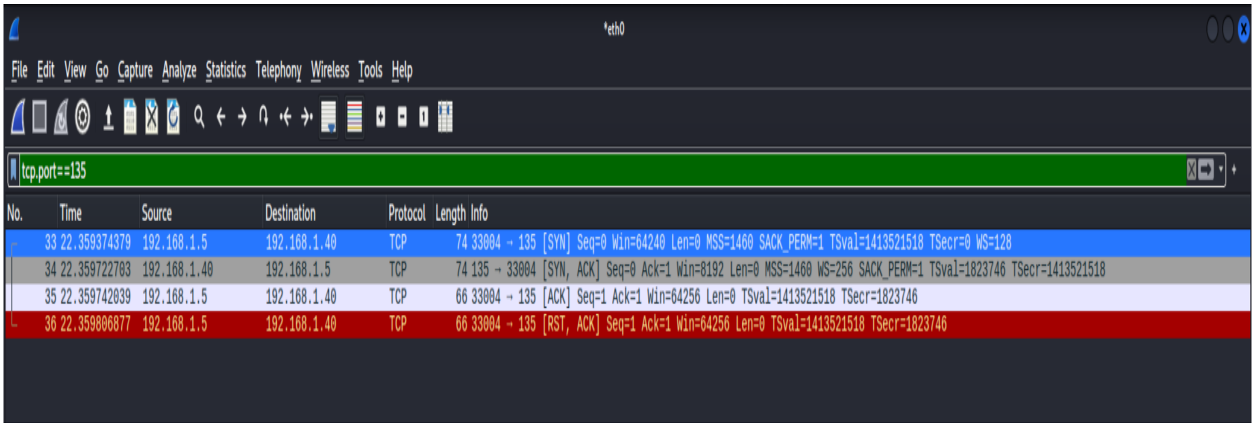
Figure 18: Scanning port 135 on Windows 2k16 VM



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 09:22 UTC
Initiating ARP Ping Scan at 09:22
Scanning 192.168.1.40 [1 port]
Completed ARP Ping Scan at 09:22, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:22
Completed Parallel DNS resolution of 1 host. at 09:22, 13.00s elapsed
Initiating Connect Scan at 09:22
Scanning 192.168.1.40 [1 port]
Discovered open port 135/tcp on 192.168.1.40
Completed Connect Scan at 09:22, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.1.40
Host is up (0.00036s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 08:00:27:23:D7:D9 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Here we see the specific service and state of our particular port of interest. In this case port 135.

Figure 19: Using Wireshark to Intercept Port Scan


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==135
```

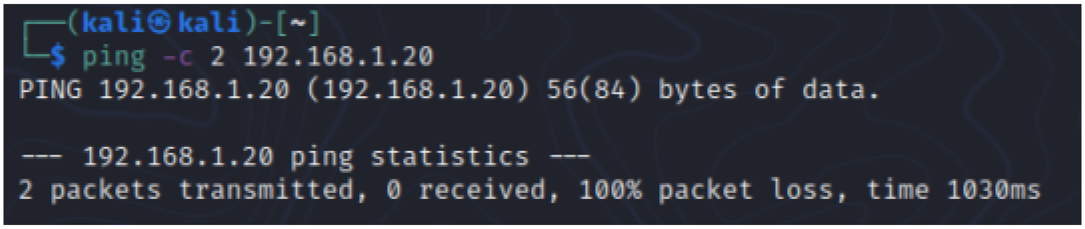
```
No.  Time          Source        Destination   Protocol Length Info
  33 22.359374379  192.168.1.5   192.168.1.40  TCP      74 33004 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1413521518 TSecr=0 WS=128
  34 22.359722703  192.168.1.40  192.168.1.5   TCP      74 135 → 33004 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1823746 TSecr=1413521518
  35 22.359742039  192.168.1.5   192.168.1.40  TCP      66 33004 → 135 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1413521518 TSecr=1823746
  36 22.359806877  192.168.1.5   192.168.1.40  TCP      66 33004 → 135 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1413521518 TSecr=1823746
```

By configuring Wireshark to listen to eth0, and filtering the output to tcp.port 135, we can see the exact packets that are exchanged between the two machines when the port scan is run. From this we can gather even more information about the target system, and infer what types of packets would cause the system to behave abnormally if sent.

Part 4: Crafting IP Packets With HPing

If a hackers or tester is aware of the ports that are open and the services that are running on a system, then specially crafted IP packets can be employed for host discovery. For example, if a hacker is aware that a server is running HTTP, then he or she can send specially formatted HTTP packets to that server to discover to get a response from behind a firewall. The figures below illustrate this concept.

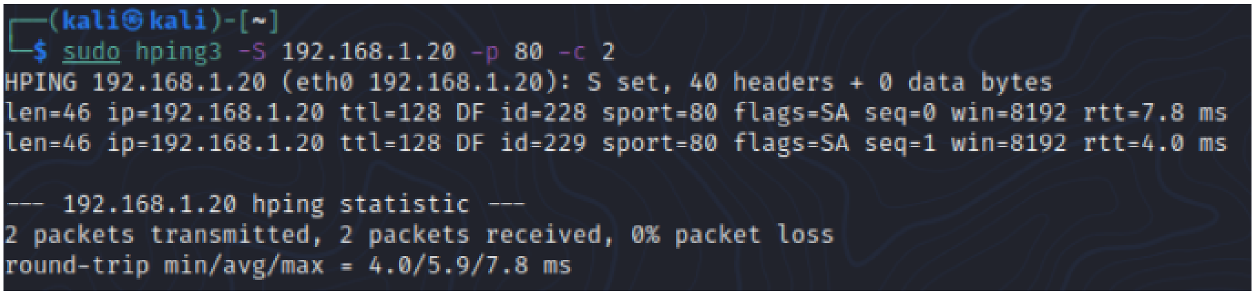
Figure 20: Pinging Windows 2k8 VM with Firewall On



```
┌──(kali㉿kali)-[~]
└─$ ping -c 2 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.

--- 192.168.1.20 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1030ms
```

Based on this response, a hacker might be under the impression that this host is inactive within the organization.

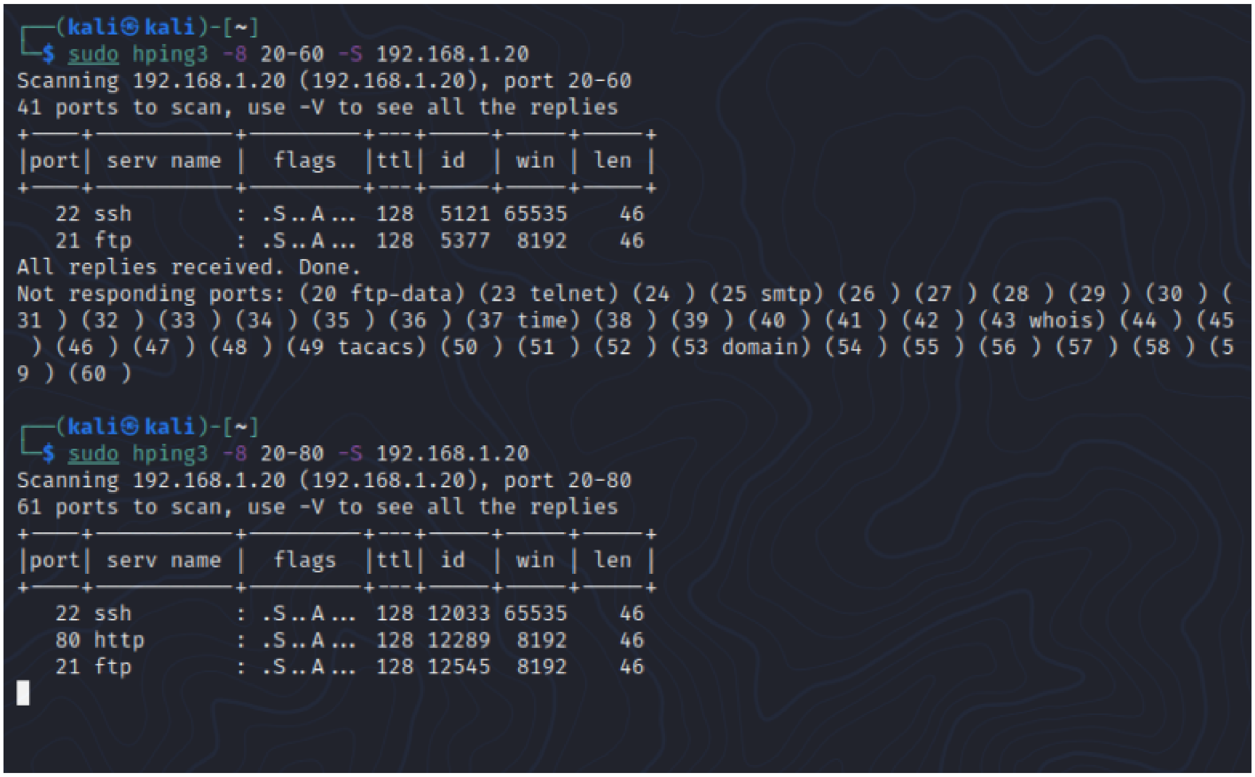
Figure 21: Using hping3 For Host Discovery



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.1.20 -p 80 -c 2
HPING 192.168.1.20 (eth0 192.168.1.20): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.20 ttl=128 DF id=228 sport=80 flags=SA seq=0 win=8192 rtt=7.8 ms
len=46 ip=192.168.1.20 ttl=128 DF id=229 sport=80 flags=SA seq=1 win=8192 rtt=4.0 ms

--- 192.168.1.20 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 4.0/5.9/7.8 ms
```

Using the knowledge that port 80 (HTTP) is open and is being used by the system, we can send a specially crafted HTTP packet using hping3 to get a response back.

Figure 22: Using hping3 to send packets to a range of ports



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -8 20-60 -S 192.168.1.20
Scanning 192.168.1.20 (192.168.1.20), port 20-60
41 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh        : .S..A... 128  5121 65535    46
   21 ftp        : .S..A... 128  5377  8192    46
All replies received. Done.
Not responding ports: (20 ftp-data) (23 telnet) (24 ) (25 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (
31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 time) (38 ) (39 ) (40 ) (41 ) (42 ) (43 whois) (44 ) (45
 ) (46 ) (47 ) (48 ) (49 tacacs) (50 ) (51 ) (52 ) (53 domain) (54 ) (55 ) (56 ) (57 ) (58 ) (5
9 ) (60 )

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -8 20-80 -S 192.168.1.20
Scanning 192.168.1.20 (192.168.1.20), port 20-80
61 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   22 ssh        : .S..A... 128 12033 65535    46
   80 http       : .S..A... 128 12289  8192    46
   21 ftp        : .S..A... 128 12545  8192    46
```

Hping3 can further be refined to send packets covering a range of ports. Making it an invaluable tool for host discovery within a target organization.