

Lab Assignment 8

Aim: Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Lab Outcome Attainment: LO4

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts.

Nmap uses raw IP packets in novel ways to determine

- what hosts are available on the network,
- what services (application name and version) those hosts are offering,
- what operating systems (and OS versions) they are running,
- what type of packet filters/firewalls are in use etc.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". **That table lists the port number and protocol, service name, and state.**

The state is either open, filtered, closed, or unfiltered.

- **Open** means that an application on the target machine is listening for connections/packets on that port.
- **Filtered** means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it

is open or closed.

- **Closed** ports have no application listening on them, though they could open up at any time.
- Ports are classified as **unfiltered** when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed.
- Nmap reports the state combinations **open|filtered** and **closed|filtered** when it cannot determine which of the two states describe a port.

Nmap for typical scan :

1. TCP connect(0) scanning

nmap -sT ipaddress

These scans are so called because UNIX sockets programming uses a system call named `connect()` to begin a TCP connection to a remote site. If `connect()` succeeds, a connection was made. If it fails, the connection could not be made (the remote system is offline, the port is closed, or some other error occurred along the way). This allows a basic type of port scan, which **attempts to connect to every port in turn, and notes whether or not the connection succeeded. Once the scan is completed, ports to which a connection could be established are listed as *open*, the rest are said to be closed.**

This method of scanning is very effective, and provides a clear picture of the ports you can and cannot access. If a `connect()` scan lists a port as open, you can definitely connect to it - that is what the scanning computer just did! There is, however, a major drawback to this kind of scan; it is very easy to detect on the system being scanned. If a firewall or intrusion detection system is running on the victim, attempts to `connect()` to every port on the system will almost always trigger a warning. Indeed, with

modern firewalls, an attempt to connect to a single port which has been blocked or has not been specifically "opened" will usually result in the connection attempt being logged. Additionally, most servers will log connections and their source IP, so it would be easy to detect the source of a TCP connect() scan.

For this reason, the TCP Stealth Scan was developed.

```
root@tsec-H55M-S2V:/home/tsec# nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 00
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:34 IST
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.8
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:35 IST
Nmap scan report for 192.168.92.8
Host is up (0.090018s latency).
All 1000 scanned ports on 192.168.92.8 are closed
Nmap done: 1 IP address (1 host up) scanned in 2.82 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:35 IST
Nmap scan report for 192.168.92.1
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 90:8D:7B:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 72.41 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:45 IST
Nmap scan report for 192.168.92.1
Host is up (0.035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 90:8D:7B:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.6
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.7
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.64 seconds
root@tsec-H55M-S2V:/home/tsec#
```

2. TCP SYN scan

`#nmap -sS ipaddress`

SYN or Stealth scanning makes use of this procedure by sending a SYN packet and looking at the response. If SYN/ACK is sent back, the port is open and the remote end is trying to open a TCP connection. The scanner then sends an RST to tear down the connection before it can be established fully; often preventing the connection attempt appearing in application logs. If the port is closed, an RST will be sent. If it is filtered, the SYN packet will have been dropped and no response will be sent. In this way, Nmap can detect three port states - open, closed and filtered. Filtered ports may require further probing since they could be subject to firewall rules which render them open to some IPs or conditions, and closed to others.

Modern firewalls and Intrusion Detection Systems can detect SYN scans, but in combination with other features of Nmap, it is possible to create a virtually undetectable SYN scan by altering timing and other options.

```
root@tsec-H55M-S2V:/home/tsec#
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 18000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:34 IST
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.8

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:35 IST
Nmap scan report for 192.168.92.8
Host is up (0.000018s latency).
All 1000 scanned ports on 192.168.92.8 are closed
Nmap done: 1 IP address (1 host up) scanned in 2.82 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:35 IST
Nmap scan report for 192.168.92.1
Host is up (0.0011s latency).
Not shown: 997 closed ports.
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp  open  park-agent
MAC Address: 90:80:78:7E:5A:06 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 72.41 seconds
root@tsec-H55M-S2V:/home/tsec#
```

3. TCP FIN scan

#nmap -sF ipaddress

The idea behind these type of scans is that **a closed port should respond with an RST upon receiving packets, whereas an open port should just drop them** (it's listening for packets with SYN set). This way, you never make even part of a connection, and never send a SYN packet; which is what most IDS' look out for.

The FIN scan sends a packet with only the FIN flag set.

These scan types will work against any system where the TCP/IP implementation follows RFC 793. Microsoft Windows does not follow the RFC, and will ignore these packets even on closed ports. This technicality allows you to detect an MS Windows system by running SYN along with one of these scans. If the SYN scan shows open ports, and the FIN/NUL/XMAS does not, chances are you're looking at a Windows box


```
root@tsec-H55M-S2V:/home/tsec#
All 1800 scanned ports on 192.168.92.8 are closed
Nmap done: 1 IP address (1 host up) scanned in 2.82 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sS 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:35 IST
Nmap scan report for 192.168.92.1
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 72.41 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:45 IST
Nmap scan report for 192.168.92.1
Host is up (0.035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.6
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.7
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.64 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sF 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:47 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp   open|filtered park-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 92.08 seconds
root@tsec-H55M-S2V:/home/tsec#
```

4. TCP NULL scan

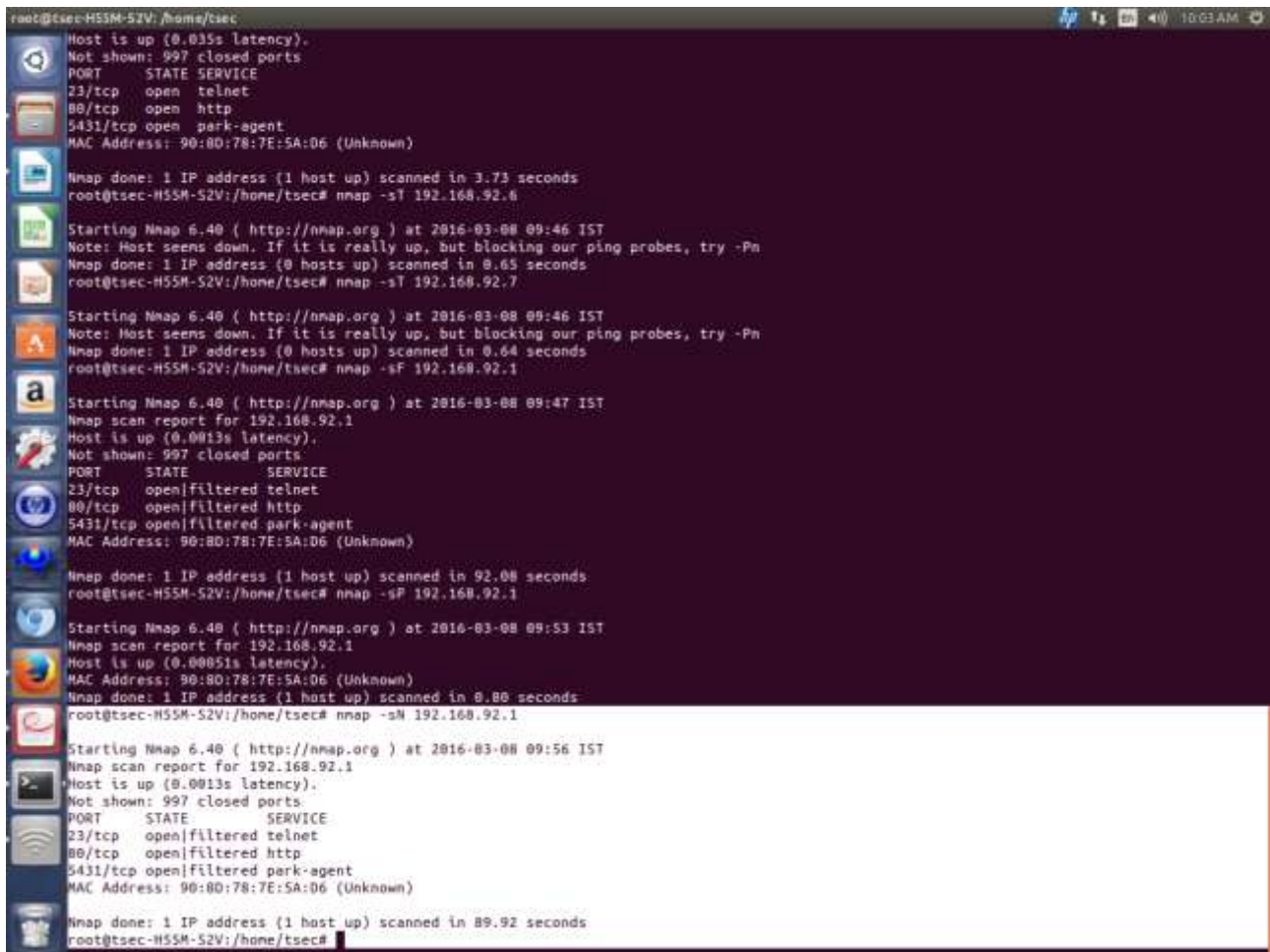
The Null Scan is a type of TCP scan that hackers — both ethical and malicious — use to identify listening TCP ports. In the right hands, a Null Scan can help identify potential holes for server hardening, but in the wrong hands, it is a reconnaissance tool. It is a pre-attack probe.

A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags. In a production environment, there will never be a TCP packet that doesn't contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and edge routers that filter incoming packets with particular flags.

The expected result of a Null Scan on an open port is no response. Since there are no flags set, the target will not know how to handle the request. It will discard the packet and no reply will be sent. If the port

is closed, the target will send an RST packet in response.

Information about which ports are open can be useful to hackers, as it will identify active devices and their TCP-based application-layer protocol.



```
root@tsec-H55M-52V: /home/tsec
Host is up (0.035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp  open  park-agent
MAC Address: 90:80:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
root@tsec-H55M-52V: /home/tsec# nmap -sT 192.168.92.6

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@tsec-H55M-52V: /home/tsec# nmap -sT 192.168.92.7

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.64 seconds
root@tsec-H55M-52V: /home/tsec# nmap -sF 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:47 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 90:80:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 92.08 seconds
root@tsec-H55M-52V: /home/tsec# nmap -sP 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:53 IST
Nmap scan report for 192.168.92.1
Host is up (0.00051s latency).
MAC Address: 90:80:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
root@tsec-H55M-52V: /home/tsec# nmap -sN 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:56 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 90:80:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 89.92 seconds
root@tsec-H55M-52V: /home/tsec#
```

5. XMAS scan

The Xmas Tree scan sets the FIN, URG and PUSH flags are set. This scan will work on UNIX and related systems and cause the kernel to drop the packet if the receiving port is open.

```
root@tsec-H55M-S2V:/home/tsec#
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sT 192.168.92.7

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.64 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sF 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:47 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered perl-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 92.08 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sP 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:53 IST
Nmap scan report for 192.168.92.1
Host is up (0.00051s latency).
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sM 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:56 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered perl-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 89.92 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sX 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:07 IST
Nmap scan report for 192.168.92.1
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered perl-agent
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 92.73 seconds
root@tsec-H55M-S2V:/home/tsec#
```

6. Ping sweep

nmap -sP IP address of gateway

This scan type lists the hosts within the specified range that responded to a ping. It allows you to detect which computers are online, rather than which ports are open.


```
root@teco-H55N-S2V:/home/tsec#
Host is up (0.001s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 98:8D:7B:72:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 72.41 seconds
root@teco-H55N-S2V:/home/tsec# nmap -sT 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:45:15T
Nmap scan report for 192.168.92.1
Host is up (0.035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 98:8D:7B:72:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.73 seconds
root@teco-H55N-S2V:/home/tsec# nmap -sT 192.168.92.6

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46:15T
Note: Host seems down. If it is really up, but blocking our ping probes, try -fn
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@teco-H55N-S2V:/home/tsec# nmap -sT 192.168.92.7

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:46:15T
Note: Host seems down. If it is really up, but blocking our ping probes, try -fn
Nmap done: 1 IP address (0 hosts up) scanned in 0.64 seconds
root@teco-H55N-S2V:/home/tsec# nmap -sT 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:47:15T
Nmap scan report for 192.168.92.1
Host is up (0.0035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp   open|filtered park-agent
MAC Address: 98:8D:7B:72:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 92.08 seconds
root@teco-H55N-S2V:/home/tsec# nmap -sP 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:53:15T
Nmap scan report for 192.168.92.1
Host is up (0.00051s latency).
MAC Address: 98:8D:7B:72:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
root@teco-H55N-S2V:/home/tsec#
```

7. ACK scan

This scan type sends ACK packets to a host.

If an RST comes back, the port is classified "unfiltered" (that is, it was allowed to send its RST through whatever firewall was in place). If nothing comes back, the port is said to be "filtered", that is, the firewall prevented the RST coming back from the port. This scan type can help determine if a firewall is stateless (just blocks incoming SYN packets) or stateful (tracks connections and also blocks unsolicited ACK packets).

Note that an ACK scan will never show ports in the "open" state, and so it should be used in conjunction with another scan type to gain more information about firewalls or packet filters between yourself and the victim.

```
root@tscc-H55H-S2V:/home/tsec#
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 02.08 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sP 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:53 IST
Nmap scan report for 192.168.92.1
Host is up (0.00051s latency).
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sN 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:56 IST
Nmap scan report for 192.168.92.1
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 09.92 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sX 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 09:56 IST
Nmap scan report for 192.168.92.1
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 02.73 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sA 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:10 IST
Nmap scan report for 192.168.92.1
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.92.1 are unfiltered
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 08.50 seconds
root@tscc-H55H-S2V:/home/tsec#
```

8. scanning range of ports

#nmap -p23 ipaddress scans specific port

#nmap -p23-443 ipaddress scans ports ranging from 23 to 443

```
root@tscc-H55H-S2V:/home/tsec#
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 05.92 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sX 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:07 IST
Nmap scan report for 192.168.92.1
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
80/tcp    open|filtered http
5431/tcp  open|filtered park-agent
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 02.73 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -sA 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:10 IST
Nmap scan report for 192.168.92.1
Host is up (0.0029s latency).
All 1000 scanned ports on 192.168.92.1 are unfiltered
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 08.50 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -p23 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:14 IST
Nmap scan report for 192.168.92.1
Host is up (0.0012s latency).
PORT      STATE      SERVICE
23/tcp    open      telnet
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
root@tscc-H55H-S2V:/home/tsec# nmap -p23-443 192.168.92.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-08 10:14 IST
Nmap scan report for 192.168.92.1
Host is up (0.0023s latency).
Not shown: 419 closed ports
PORT      STATE      SERVICE
23/tcp    open      telnet
80/tcp    open      http
MAC Address: 98:8D:78:7E:5A:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 19.15 seconds
root@tscc-H55H-S2V:/home/tsec#
```

9. Version Detection [-sV]

Version Detection collects information about the specific service running on an open port, including the product name and version number. This information can be critical in determining an entry point for an attack. The -sV option enables version detection, and the -A option enables both OS fingerprinting and version detection, as well as any other advanced features which may be added in future releases.

10. `nmap -sV -p 1-80 192.168.1.1/24`

This command will scan all of your local IP range (assuming you're in the 192.168.1.0-254 range), and will perform service identification (-sV) and will scan all ports (-p 1-80). Since you are running this as a normal user and not root it will be a TCP Connect based scan. If you run the command with `sudo` at the front it will run as a TCP SYN scan.

```

root@tsec-H55M-S2V:/home/tsec#
Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -sV -p 1-65535 192.168.92.1/24

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-09 18:26 IST

root@tsec-H55M-S2V:/home/tsec# nmap -sV -p 1-80 192.168.92.1/24

Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-09 18:32 IST
Nmap scan report for 192.168.92.1
Host is up (0.0014s latency).
Not shown: 78 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet?
80/tcp    open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port23-TCP:V=6.40NI=7XD=3/9NTine=560FAE93NP=i6B6-pc-linux-gnuKr(NULL,1B
SF:,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(GenericLines,1B,
SF:"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(GetRequest,1B,"Te
SF:lnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(HTTPOptions,1B,"Teln
SF:et\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(RTSPRequest,1B,"Telnet
SF:\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(RPCCheck,1B,"Telnet\x200
SF:isabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(DNSVersionBindReq,1B,"Telnet\
SF:x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(DNSStatusRequest,1B,"Teln
SF:et\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(Help,1B,"Telnet\x20Dis
SF:abled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(SSLSessionReq,1B,"Telnet\x20Dis
SF:abled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(Kerberos,1B,"Telnet\x20Disabled
SF:\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(SMBProgNeg,1B,"Telnet\x20Disabled\.\
SF:r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(X11Probe,1B,"Telnet\x20Disabled\.\r\n\0
SF:\0\0\0\0\03\0\03\01")Kr(FourOhFourRequest,1B,"Telnet\x20Disabled\.\r
SF:\n\0\0\0\0\0\0\0\03\0\03\01")Kr(LPDSstring,1B,"Telnet\x20Disabled\.\r\n\0
SF:\0\0\0\0\03\0\03\01")Kr(LDAPBindReq,1B,"Telnet\x20Disabled\.\r\n\0\0
SF:\0\0\0\0\03\0\03\01")Kr(SIPOptions,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0
SF:\0\0\03\0\03\01")Kr(LANDesk-RC,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0
SF:\x03\0\03\01")Kr(TerminalServer,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0
SF:\0\03\0\03\01")Kr(MCP,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\0
SF:3\01")Kr(NotesRPC,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01
SF:")Kr(WMSRequest,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")K
SF:r(oracle-tns,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(o
SF:fp,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01")Kr(kuno-server
SF:,1B,"Telnet\x20Disabled\.\r\n\0\0\0\0\0\0\0\03\0\03\01");
MAC Address: 90:8D:78:7E:5A:D6 (Unknown)

Nmap scan report for 192.168.92.2
Host is up (0.00029s latency).
All 80 scanned ports on 192.168.92.2 are filtered
MAC Address: 80:CB:02:12:35:89 (Secom)

Nmap scan report for 192.168.92.14
Host is up (0.00022s latency).
All 80 scanned ports on 192.168.92.14 are closed
MAC Address: 44:87:FC:EB:E5:EB (Elitegroup Computer System CO.)

```

```
root@tsec-HSSM-S2V: /home/tsec
SF: x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(DNSStatusRequest,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(Help,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(SSLSessionReq,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(Kerberos,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(SMBProgNeg,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(X11Probe,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(FourOhFourRequest,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(LPDString,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(LDAPBindReq,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(SIPOptions,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(LANDesk-RC,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(TerminalServer,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(NCP,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(NotesRPC,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(NMSRequest,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(Oracle-tns,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(aSF:fp,1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01")\r(kuno-serverSF:1B,"Telnet\x200isabled\.\r\n\0\0\0\0\03\0\03\01");
MAC Address: 90:80:78:7E:5A:06 (Unknown)

Nmap scan report for 192.168.92.2
Host is up (0.00029s latency).
All 80 scanned ports on 192.168.92.2 are filtered
MAC Address: 00:C0:02:12:35:89 (Sercomm)

Nmap scan report for 192.168.92.14
Host is up (0.00022s latency).
All 80 scanned ports on 192.168.92.14 are closed
MAC Address: 44:87:FC:EB:E5:EB (Elitegroup Computer System CO.)

Nmap scan report for 192.168.92.16
Host is up (0.00021s latency).
All 80 scanned ports on 192.168.92.16 are closed
MAC Address: 44:87:FC:EB:E5:7B (Elitegroup Computer System CO.)

Nmap scan report for 192.168.92.37
Host is up (0.00028s latency).
All 80 scanned ports on 192.168.92.37 are closed
MAC Address: D4:BE:D9:CB:E1:D4 (Dell)

Nmap scan report for 192.168.92.197
Host is up (-0.099s latency).
All 80 scanned ports on 192.168.92.197 are filtered
MAC Address: 1C:6F:65:D1:3F:AA (Giga-byte Technology Co.)

Nmap scan report for 192.168.92.8
Host is up (0.00019s latency).
All 80 scanned ports on 192.168.92.8 are closed

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 30.36 seconds
root@tsec-HSSM-S2V: /home/tsec#
```

11. Operating system fingerprinting

#nmap -O ipaddress

Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its `nmap-os-db` database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match.


```
root@tsec-H55M-S2V: /home/tsec
OS: (R=YXDF=YNT=40%W=0%S=Z%N=S+NF=AR%O=SRD=0%Q=)T6(R=YXDF=YNT=40%W=0%S=AXA=Z
OS:XF=RXO=NRD=0%Q=)T7(R=YXDF=YNT=40%W=0%S=Z%N=S+NF=AR%O=SRD=0%Q=)U1(R=YXDF=
OS:NKT=40%IPL=164NUN=0%RIPL=GNRID=GNRIPCK=GNRUCK=GNRUD=C)IE(R=YXDFI=NNT=40%
OS:CD=5)
Network Distance: 1 hop
Nmap scan report for 192.168.92.197
Host is up (-0.099s latency).
All 1000 scanned ports on 192.168.92.197 are filtered
MAC Address: 1C:6F:65:D1:3F:AA (Giga-byte Technology Co.)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 192.168.92.8
Host is up (0.000012s latency).
All 1000 scanned ports on 192.168.92.8 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 239.01 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -O 192.168.92.8
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-09 11:07 IST
Nmap scan report for 192.168.92.8
Host is up (0.000021s latency).
All 1000 scanned ports on 192.168.92.8 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.33 seconds
root@tsec-H55M-S2V:/home/tsec# nmap -O 192.168.92.1
Starting Nmap 6.40 ( http://nmap.org ) at 2016-03-09 11:08 IST
Nmap scan report for 192.168.92.1
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
5431/tcp   open  park-agent
MAC Address: 98:BD:78:7E:5A:D6 (Unknown)
Device type: switch
Running: Allied Telesyn embedded, D-Link embedded
OS CPE: cpe:/h:alliedtelesyn:at-gs950 cpe:/h:dlink:des-3226l
OS details: Allied Telesyn AT-GS950 or D-Link DES-3226L switch
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.07 seconds
root@tsec-H55M-S2V:/home/tsec#
```

12. Idle scan - self study