Nmap Command in Linux

AIM:

To familiarize working of nmap in linux

DESCRIPTION:

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

- ✓ Real time information of a network
- ✓ Detailed information of all the IPs activated on your network
- ✓ Number of ports open in a network
- ✓ Provide the list of live hosts
- ✓ Port, OS and Host scanning

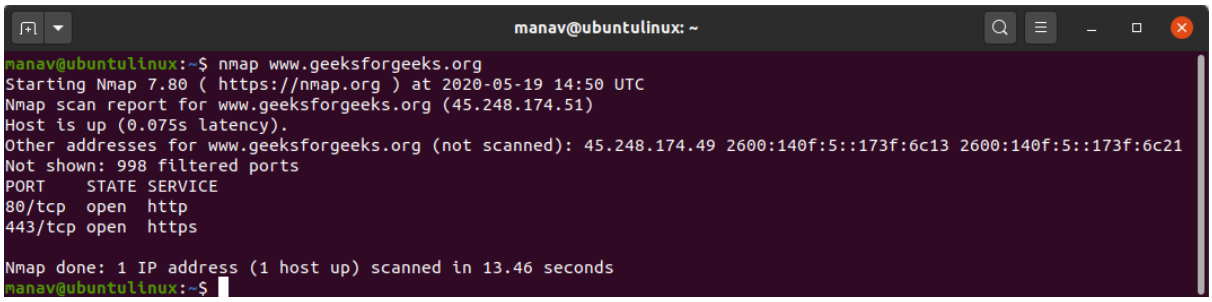
PROCEDURE:

- Installing Nmap

  sudo apt-get install nmap

- To scan a System with Hostname and IP address. First, Scan using Hostname

  nmap www.geeksforgeeks.org



- Now let's Scan using IP Address

  nmap 172.217.27.174

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ nmap 172.217.27.174
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 14:55 UTC
Nmap scan report for del11s03-in-f14.1e100.net (172.217.27.174)
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
manav@ubuntulinux:~$
```

The nmap command allows scanning a system in various ways. In this we are performing a scan using the hostname as “geeksforgeeks” and IP address “172.217.27.174”, to find all open ports, services, and MAC addresses on the system.

- To scan using “-v” option.

  nmap -v www.geeksforgeeks.org

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ nmap -v www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 16:53 UTC
Initiating Ping Scan at 16:53
Scanning www.geeksforgeeks.org (45.248.174.51) [2 ports]
Completed Ping Scan at 16:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:53
Completed Parallel DNS resolution of 1 host. at 16:53, 0.07s elapsed
Initiating Connect Scan at 16:53
Scanning www.geeksforgeeks.org (45.248.174.51) [1000 ports]
Discovered open port 80/tcp on 45.248.174.51
Discovered open port 443/tcp on 45.248.174.51
Completed Connect Scan at 16:53, 7.27s elapsed (1000 total ports)
Nmap scan report for www.geeksforgeeks.org (45.248.174.51)
Host is up (0.041s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 45.248.174.49 2600:140f
:5::173f:6c72 2600:140f:5::173f:6c73
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds
manav@ubuntulinux:~$
```

It is used to get more detailed information about the remote machines.

- To scan multiple hosts

nmap 103.76.228.244 157.240.198.35 172.217.27.174

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ nmap 103.76.228.244 157.240.198.35 172.217.27.174
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 16:57 UTC
Nmap scan report for bridgei2p.com (103.76.228.244)
Host is up (0.062s latency).
Not shown: 991 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s

Nmap scan report for edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)
Host is up (0.040s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap scan report for kix05s07-in-f174.1e100.net (172.217.27.174)
Host is up (0.041s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 12.96 seconds
manav@ubuntulinux:~$
```

We can scan multiple hosts by writing IP addresses or hostnames with nmap.

- To scan whole subnet

nmap 103.76.228.*

We can scan a whole subnet or IP range with nmap by providing "*" with it. It will scan a whole subnet and give the information about those hosts which are Up in the Network.

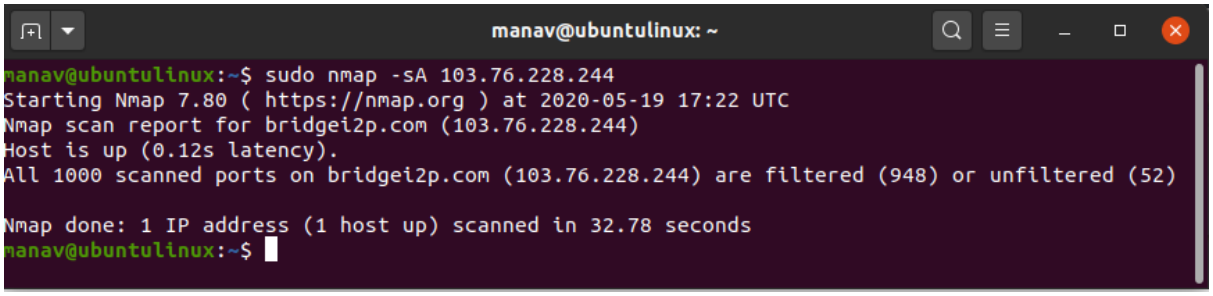
- To scan specific range of IP address

nmap 192.168.29.1-20

We can specify the range of IP addresses. This command will scan IP address 192.168.29.1 to 192.168.29.20 .

- To scan to detect firewall settings.

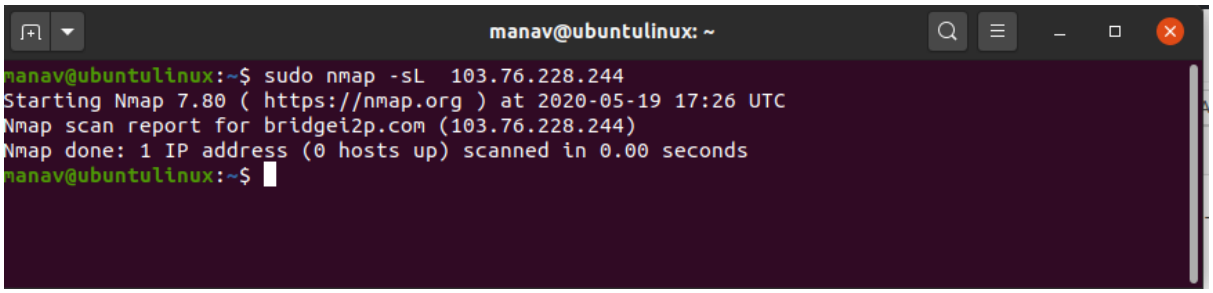
sudo nmap -sA 103.76.228.244



Detecting firewall settings can be useful during penetration testing and vulnerability scans. To detect it we use "-sA" option. This will provide you with information about firewall being active on the host. It uses an ACK scan to receive the information.

- To identify Hostnames

sudo nmap -sL 103.76.228.244



We use "sL" option to find hostnames for the given host by completing a DNS query for each one. In addition to this "-n" command can be used to skip DNS resolution, while the "-R" command can be used to always resolve DNS.

- To scan from a file

nmap -iL input.txt

```
manav@ubuntulinux: ~/gfg
manav@ubuntulinux:~/gfg$ nmap -iL input.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 17:52 UTC
Nmap scan report for bridgei2p.com (103.76.228.244)
Host is up (0.095s latency).
Not shown: 954 filtered ports, 32 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 25.60 seconds
manav@ubuntulinux:~/gfg$
```

If we have a long list of addresses that we need to scan, we can directly import a file through the command line. It will produce a scan for the given IP addresses.

- To get some help

nmap -h

```
manav@ubuntulinux: ~
manav@ubuntulinux:~$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
```

```
manav@ubuntulinux: ~
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -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)
  --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 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
manav@ubuntulinux:~$
```

We use the “-h” option if we have any questions about nmap or any of the given commands. It shows the help section for nmap command, including giving information regarding the available flags.

- Here -sS flag is used for TCP SYN Scan, which is a stealthy and efficient method of scanning for open ports on a target system.

nmap -sS <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous/Desktop]
└─# nmap -sS www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:10 IST
Nmap scan report for www.geeksforgeeks.org (49.44.192.41)
Host is up (0.012s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c09a 2405:200:1609:1731::312c:c0ca 49.44.112.188
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

- Here “-oG” flag can be used to store the nmap result in to specific file.

nmap -sS <Domain Name> -oG <file-path>

```
┌──(root㉿Anonymous)-[/home/anonymous/Desktop]
└─# nmap -sS www.geeksforgeeks.org -oG nmap_result
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:11 IST
Nmap scan report for www.geeksforgeeks.org (23.64.140.209)
Host is up (0.013s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c09a 2405:200:1609:1731::312c:c0ca 23.64.140.218
rDNS record for 23.64.140.209: a23-64-140-209.deploy.static.akamaitechnologies.com
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

- The "-sU" flag is used with nmap to perform a UDP scan, which allows the user to discover open UDP ports and services on a target system.

nmap -sU <Domain Name>

- The "-sn" flag is used with nmap to perform a ping scan, which sends ICMP requests to a target host or network to determine hosts is up or not.

nmap -sn <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -sn www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:18 IST
Nmap scan report for www.geeksforgeeks.org (49.44.112.188)
Host is up (0.018s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c0ca 2405:200:1609:1731::312c:c09a 49.44.192.41
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

- The "-p" flag is used with nmap to perform scan on a specific port or range of ports. (In our case it will scan port 80,443 and 21)

nmap -p 80 443 21 <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -p 80 443 21 www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:16 IST
Nmap scan report for www.geeksforgeeks.org (23.64.140.209)
Host is up (0.016s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c09a 2405:200:1609:1731::312c:c0ca 23.64.140.218
rDNS record for 23.64.140.209: a23-64-140-209.deploy.static.akamaitechnologies.com

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 3 IP addresses (1 host up) scanned in 1.48 seconds
```

- We can also specify the range of ports to scan on a network. (In this case it will scan all the ports in the range of 1 to 80)

nmap -p 1-80 <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -p 1-80 www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:17 IST
Nmap scan report for www.geeksforgeeks.org (49.44.192.41)
Host is up (0.0098s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c0ca 2405:200:1609:1731::312c:c09a 49.44.112.188
Not shown: 78 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
```

- Here -A indicates aggressive, it will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (–traceroute). It even provides a lot of valuable information about the host.

nmap -A <Domain Name>

```
root@kali:~# nmap -A www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 04:59 EST
Nmap scan report for www.geeksforgeeks.org (23.199.69.251)
Host is up (0.027s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 23.199.69.248 2405:200:1630:a03::312c:c5c0 2405:200:1630:a03::312c:c5a9
rDNS record for 23.199.69.251: a23-199-69-251.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE        VERSION
80/tcp  open  tcpwrapped
|_http-server-header: AkamaiGHost
|_http-title: Access Denied
443/tcp open  ssl/tcpwrapped
| http-server-header:
|   AkamaiGHost
|_  Apache
|_http-title: Access Denied
| ssl-cert: Subject: commonName=www.geeksforgeeks.org
| Subject Alternative Name: DNS:api.geeksforgeeks.org, DNS:auth.geeksforgeeks.org, DNS:authcdn.geeksforgeeks.org, DNS:cdncontribute.geeksforgeeks.org, DNS:cdnpractice.geeksforgeeks.org, DNS:cdnvideos.geeksforgeeks.org, DNS:contribute.g
eeksforgeeks.org, DNS:ide.geeksforgeeks.org, DNS:media.geeksforgeeks.org, DNS:practice.geeksforgeeks.org, DNS:www.geeksforgeeks.org
| Not valid before: 2020-12-28T11:43:53
|_Not valid after:  2021-03-28T11:43:53
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|   http/1.1
|_  http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: QEMU user mode network gateway (94%), Konica Minolta 7035 printer (89%), GNU Hurd 0.3 (87%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%), Bay Networks BayStack 450 switch (software version
4.2.0.16) (86%), Tyco 24 Port SNMP Managed Switch (86%), Cabletron ELS100-24TXM Switch or Icom IC-7800 radio transceiver (86%), HP 9100c Digital Sender printer (J3113A) (85%), Minolta Di550 laser printer (85%), NEC SuperScript printer
(85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.78 ms 10.0.2.2
2   1.90 ms a23-199-69-251.deploy.static.akamaitechnologies.com (23.199.69.251)

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 57.45 seconds
```

- Using this command we can discover the target hosting service or identify additional targets according to our needs for quickly tracing the path.

nmap --trace out <Domain Name>

```
root@kali:~# nmap --trace out  www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 05:10 EST
Failed to resolve "out".
Nmap scan report for www.geeksforgeeks.org (23.199.69.251)
Host is up (0.0047s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 23.199.69.248 2405:200:1630:a03::312c:c5a9 2405:200:1630:a03::312c:c5c0
rDNS record for 23.199.69.251: a23-199-69-251.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.75 ms 10.0.2.2
2   1.86 ms a23-199-69-251.deploy.static.akamaitechnologies.com (23.199.69.251)

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds
```

- Here it will display the operating system where the domain or ip address is running, but will not display the exact operating system available on the computer. It will display only the chance of operating system available in the computer. The command will just guess the running operating system (OS) on the host.

nmap -O <Domain Name>

```
root@kali:~# nmap -O  www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 04:57 EST
Nmap scan report for www.geeksforgeeks.org (23.199.69.248)
Host is up (0.029s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 23.199.69.251 2405:200:1630:a03::312c:c5a9 2405:200:1630:a03::312c:c5c0
rDNS record for 23.199.69.248: a23-199-69-248.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (99%), QEMU (96%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (99%), QEMU user mode network gateway (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
```