NMAP NETWORK SCANNER Software Guide

cloud academy
A QA COMPANY

NMAP NETWORK SCANNER

This guide covers the basics of using Nmap, the network scanner. As a network scanner, Nmap is often used at the beginning of penetration testing to find out basic information about the target website or web app.

Why use Nmap?

Nmap, or Network Mapper, is used in security and auditing for checking host or service uptime. It can tell us what's available on a given network, whether that's the applications that are in use or whether the network is running firewalls. It can even scan what operating systems are in use on the network.

Nmap works on all major operating systems and you can run it as command-line prompts or through the Nmap application called Zenmap. Nmap is incredibly popular with cybersecurity professionals because it is free, easy to use, well-supported and incredibly powerful and can allow you to scan huge computer networks, made up of thousands of machines.

Install and Get Help in Nmap

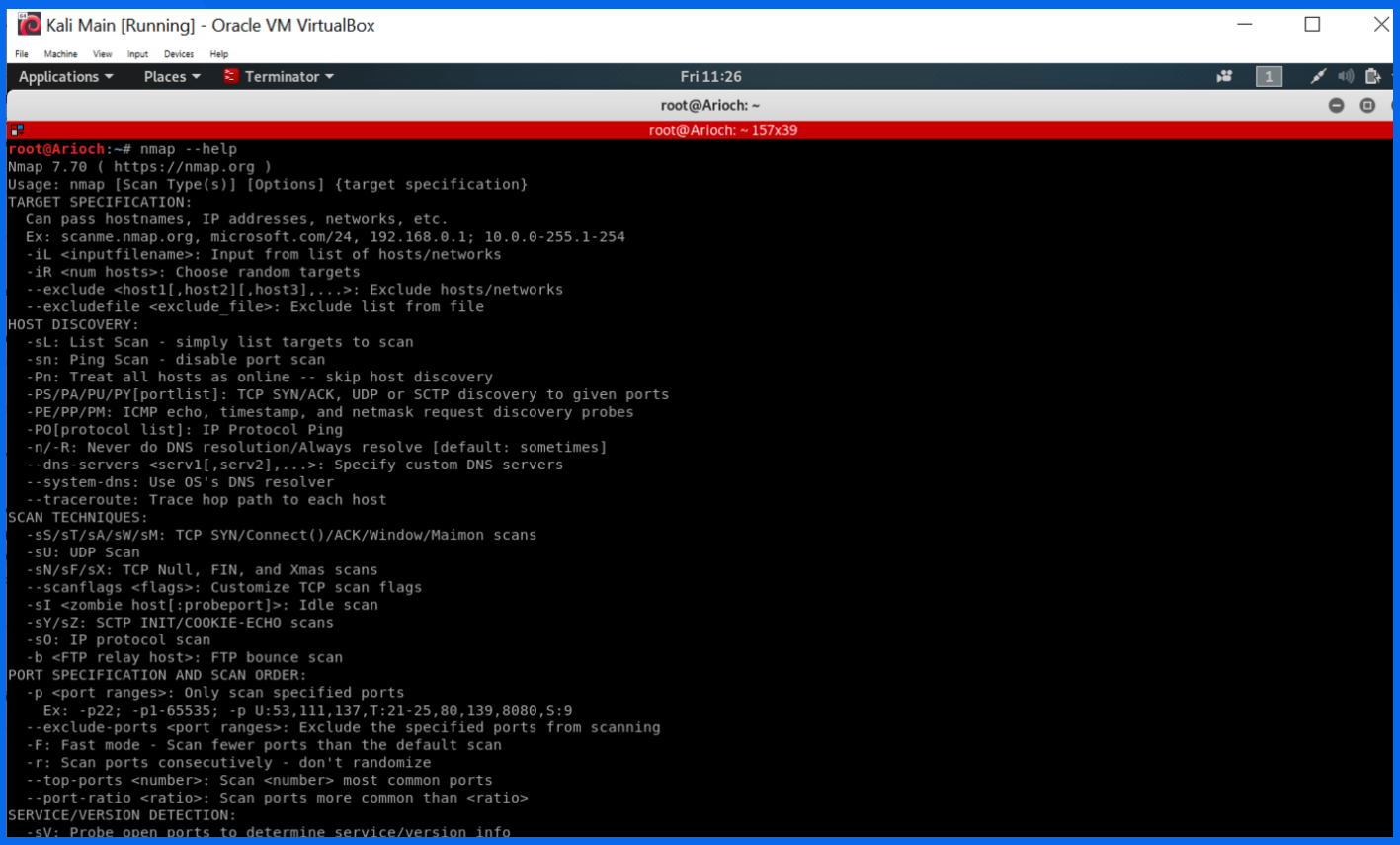
Nmap is pre-installed in Kali Linux. If you are using a different version of Linux, you will need to install Nmap.

If you get stuck in Nmap, you can use the help menu to find basic commands. The example to the right is what the help section should look like in the terminal.

Use the code below to install Nmap and summon the help menu in the terminal.

```
Install NMap: apt-get install nmap

Get help in NMap: nmap --help
```



NMAP NETWORK SCANNER

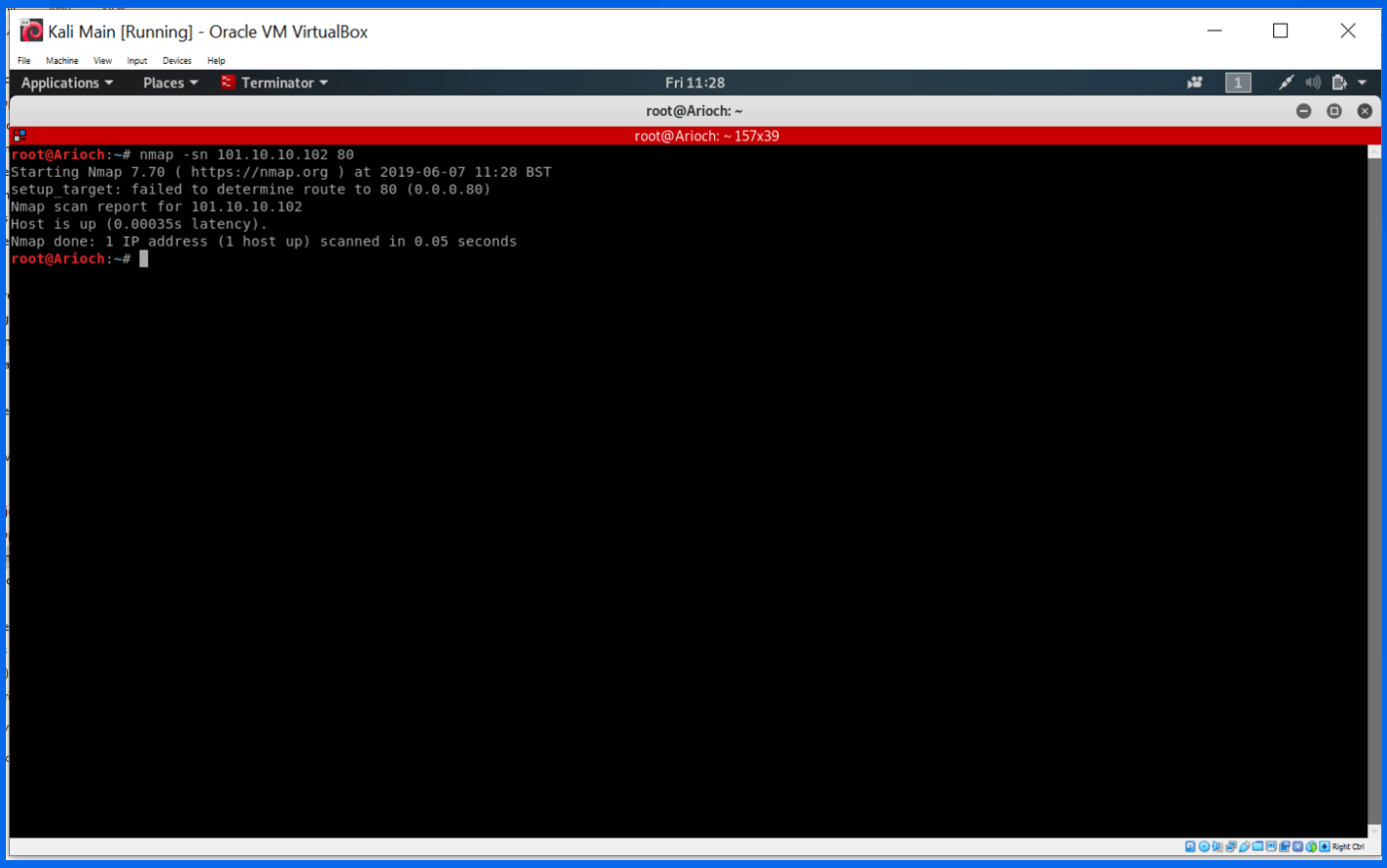
Conducting a Ping Sweep

A ping sweep is used to see if the target server that you're going to scan is up and running. It does this by sending an Internet Control Message Protocol request (or ICMP). To conduct a Ping Sweep in Nmap, you'll need to send out an ICMP request.

If the Ping Sweep returns positively, you'll receive a return like the one in the example to the left. Enter *clear* to clear the terminal, and you'll then be able to begin scanning the target IP address.

To send out an ICMP request, use the following command, followed by the target IP address:

```
nmap -sn
```



NMAP NETWORK SCANNER

Port Scanning with Nmap

You can use Nmap to find a list of available port numbers available on the target website; this is one of the core purposes of Nmap.

This port number switch will present any available common ports that are open, shown in the example to the right.

To find out if any of the 100 most common port numbers are available on the web address, use:

```
nmap -F
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -A 10.1.1.*
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-07 09:10 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 59.41% done; ETC: 09:10 (0:00:01 remaining)
Stats: 0:01:23 elapsed; 252 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 09:12 (0:00:00 remaining)
Nmap scan report for 10.1.1.1
Host is up (0.00039s latency).
Not shown: 997 filtered 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 Windows 10 Enterprise 17134 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 0A:00:27:00:00:0D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: STUDENT16; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -19m58s, deviation: 34m37s, median: 0s
|_nbstat: NetBIOS name: STUDENT16, NetBIOS user: <unknown>, NetBIOS MAC: 0a:00:27:00:00:0d (unknown)
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: STUDENT16
|   NetBIOS computer name: STUDENT16\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-06-07T14:11:37+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
```

NMAP NETWORK SCANNER

Scan a Specific Port

If you already know which port number you wish to scan, such as port 80, you can use the following command to find it; make sure you always add the IP address:

```
nmap -p 80
```

Version Scanning

When you have found open ports, Nmap can use its default scripts to find out what software and script versions are being used by the target IP address. First, make a note of the open port numbers you want to scan, then enter the following command, followed by the port numbers. Make sure the port numbers are comma separated.

```
nmap -sv
```

Useful Scan Commands

Below are some useful scan commands in Nmap. Make sure you follow each command with the target IP address.

```
Scan a range of ports:  nmap -p 1-100
Scan all 65535 ports:   nmap -p-

Scan using TCP connect: nmap -sT
Scan using TCP SYN scan (default):      nmap -sS
Scan UDP ports: nmap -sU -p
Scan selected ports & ignore discovery: nmap -Pn -F
```

Set Scan Speed

Scan speed tells Nmap how quickly it should scan the target IP address; these are known as timing attacks. you can set the speed with following commands; Nmap is at Normal speed by default.

You can set the speed by typing the -T before setting what scan type you want to do.

```
Paranoid:   -T0
Sneaky:     -T1
Polite:     -T2
Normal:     -T3
Aggressive: -T4
Insane:     -T5
```

NMAP NETWORK SCANNER

General Nmap Commands

Below is a list of some useful commands and their functions in Nmap.

```
PROBE MODES:
  --tcp-connect                      : Unprivileged TCP connect probe mode.
  --tcp                              : TCP probe mode.
  --udp                              : UDP probe mode.
  --icmp                             : ICMP probe mode.
  --arp                              : ARP/RARP probe mode.
  --tr, --traceroute                 : Traceroute mode (can only be used with
                                       TCP/UDP/ICMP modes).
TCP CONNECT MODE:
   -p, --dest-port <port spec>       : Set destination port(s).
   -g, --source-port <portnumber>    : Try to use a custom source port.

TCP PROBE MODE:
   -g, --source-port <portnumber>    : Set source port.
   -p, --dest-port <port spec>       : Set destination port(s).
   --seq <seqnumber>                 : Set sequence number.
   --flags <flag list>               : Set TCP flags (ACK,PSH,RST,SYN,FIN...)
   --ack <acknumber>                 : Set ACK number.
   --win <size>                      : Set window size.
   --badsum                          : Use a random invalid checksum.

UDP PROBE MODE:
   -g, --source-port <portnumber>    : Set source port.
   -p, --dest-port <port spec>       : Set destination port(s).
   --badsum                          : Use a random invalid checksum.

ICMP PROBE MODE:
  --icmp-type <type>                 : ICMP type.
  --icmp-code <code>                 : ICMP code.
  --icmp-id <id>                     : Set identifier.
  --icmp-seq <n>                     : Set sequence number.
  --icmp-redirect-addr <addr>        : Set redirect address.
  --icmp-param-pointer <pnt>         : Set parameter problem pointer.
  --icmp-advert-lifetime <time>      : Set router advertisement lifetime.
  --icmp-advert-entry <IP,pref>      : Add router advertisement entry.
  --icmp-orig-time  <timestamp>      : Set originate timestamp.
  --icmp-recv-time  <timestamp>      : Set receive timestamp.
  --icmp-trans-time <timestamp>      : Set transmit timestamp.
ARP/RARP PROBE MODE:
  --arp-type <type>                  : Type: ARP, ARP-reply, RARP, RARP-reply.
  --arp-sender-mac <mac>             : Set sender MAC address.
  --arp-sender-ip  <addr>            : Set sender IP address.
  --arp-target-mac <mac>             : Set target MAC address.
  --arp-target-ip  <addr>            : Set target IP address.

IPv4 OPTIONS:
  -S, --source-ip                    : Set source IP address.
  --dest-ip <addr>                   : Set destination IP address (used as an alternative to {target specification} ).
  --tos <tos>                        : Set type of service field (8bits).
  --id  <id>                         : Set identification field (16 bits).
  --df                               : Set Don't Fragment flag.
  --mf                               : Set More Fragments flag.
  --ttl <hops>                       : Set time to live [0-255].
  --badsum-ip                        : Use a random invalid checksum.
  --ip-options <S|R [route]|L [route]|T|U ...> : Set IP options
  --ip-options <hex string>                    : Set IP options
  --mtu <size>                       : Set MTU. Packets get fragmented if MTU is small enough.
```

cloud academy
A QA COMPANY

NMAP NETWORK SCANNER

General Nmap Commands continued....

```
IPv6 OPTIONS:
  -6, --IPv6                        : Use IP version 6.
  --dest-ip                         : Set destination IP address (used as an alternative to {target specification}).
  --hop-limit                       : Set hop limit (same as IPv4 TTL).
  --traffic-class <class> :         : Set traffic class.
  --flow <label>                    : Set flow label.
ETHERNET OPTIONS:
  --dest-mac <mac>                  : Set destination mac address. (Disables ARP resolution)
  --source-mac <mac>                : Set source MAC address.
  --ether-type <type>               : Set EtherType value.
PAYLOAD OPTIONS:
  --data <hex string>               : Include a custom payload.
  --data-string <text>              : Include a custom ASCII text.
  --data-length <len>               : Include len random bytes as payload.
ECHO CLIENT/SERVER:
  --echo-client <passphrase>        : Run Nping in client mode.
  --echo-server <passphrase>        : Run Nping in server mode.
  --echo-port <port>                : Use custom <port> to listen or connect.
  --no-crypto                       : Disable encryption and authentication.
  --once                            : Stop the server after one connection.
  --safe-payloads                   : Erase application data in echoed packets.
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m, 0.25h).
  --delay <time>                    : Adjust delay between probes.
  --rate  <rate>                    : Send num packets per second.
MISC:
  -h, --help                        : Display help information.
  -V, --version                     : Display current version number.
  -c, --count <n>                   : Stop after <n> rounds.
  -e, --interface <name>            : Use supplied network interface.
  -H, --hide-sent                   : Do not display sent packets.
  -N, --no-capture                  : Do not try to capture replies.
  --privileged                      : Assume user is fully privileged.
  --unprivileged                    : Assume user lacks raw socket privileges.
  --send-eth                        : Send packets at the raw Ethernet layer.
  --send-ip                         : Send packets using raw IP sockets.
  --bpf-filter <filter spec>        : Specify custom BPF filter.

OUTPUT:
  -v                                : Increment verbosity level by one.
  -v[level]                         : Set verbosity level. E.g: -v4
  -d                                : Increment debugging level by one.
  -d[level]                         : Set debugging level. E.g: -d3
  -q                                : Decrease verbosity level by one.
  -q[N]                             : Decrease verbosity level N times
  --quiet                           : Set verbosity and debug level to minimum.
  --debug                           : Set verbosity and debug to the max level.
```