DC3
Cyber Training Academy

NMAP QUICK TIPS

WHAT IS IT?

Nmap is an open source utility for network discovery and security auditing

WHAT CAN IT DO?

Conduct a network inventory, manage service upgrade schedules, monitor host or service uptimes, and more

THE NMAP SUITE

The Nmap suite also contains these tools:

- **Zenmap:** Nmap's GUI frontend
- **Ncat:** used for data transfer, redirection and debugging
- **Ndiff:** used for comparing scan results
- **Nping:** used for packet generation and response analysis

NMAP OPTIONS

Type `nmap` to list the version and view the most common options.

MAPPING THE ENVIRONMENT

Discovering Hosts

Ping sweep and other discovery methods are used by Nmap to identify hosts. Discovery options include:

- **List Scan:** `(-sL)`
- **No port scan:** `(-sn)`
- **No ping:** `(-Pn)`
- **TCP SYN Ping:** `(-PS)`
- **TCP ACK Ping:** `(-PA)`
- **UDP Ping:** `(-PU)`
- **SCTP INIT Ping:** `(-PY)`
- **ICMP Ping Types:** `(-PE, -PP, -PM)`
- **IP Protocol Ping:** `(-PO)`
- **ARP Ping:** `(-PR)`

Outputting Results

Scans can be saved in the following formats:

- **Normal:** `(-oN)`
- **XML:** `(-oX)`
- **Scipt Kiddie:** `(-oS)`
- **Grepable:** `(-oG)`

Port Scanning

Ports states include the following:

- **Open:** a program is listening and responding to requests
- **Closed:** the system replies with an "error: no program listening on this port"
- **Filtered:** the system does not reply; this is typically caused by firewall rules which drop a packet without sending a reply

Scan types include the following:

- **Ping scan only:** `(-sn)`
- **TCP SYN:** `(-sS)`
- **TCP connect:** `(-sT)`
- **TCK ACK:** `(-sA)`
- **TCP NULL:** `(-sN)`
- **TCP FIN:** `(-sF)`
- **TCP Xmas:** `(-sX)`
- **TCP window:** `(-sW)`
- **TCP Maimon:** `(-sM)`
- **UDP:** `(-sU)`
- **Idle:** `(-sI)`
- **FTP bounce:** `(-b)`
- **IP protocol:** `(-sO)`

OS FINGERPRINTING

Each OS implements the TCP/IP stacks slightly differently which makes them distinguishable. OS detection is performed by Nmap using TCP/IP stack fingerprinting.

The `-O` option is used by Nmap for enabling OS detection:

- **Enable OS detection:** `(-O)`
- **Limit OS detection to promising targets :** `(--osscan-limit)`
- **Guess OS more aggressively:** `(-osscan -guess)`

SERVICE/VERSION DETECTION

Sometimes you will need to know the versions of Mail, DNS and Web servers running. Having an accurate version number will help dramatically in determining specific exploits a server is vulnerable to.

The `-sV` option is used by Nmap for enabling version detection:

- **Probe open ports to determine service/version info:** `(-sV)`
- **Set for 0 (light) to 9 (try all probes):** `(--version-intensity <level>)`
- **Limit to most likely probes (intensity 2):** `(--version-light)`
- **Try every single probe (intensity 9):** `(--version-all)`
- **Show detailed version of scan activity for debugging:** `(--version-trace)`

NMAP SCRIPTING ENGINE (NSE)

The NSE enables users to automate several networking tasks via scripting. NSE features four main types of scripts:

- **Prerule:** run before targets are scanned
- **Host:** executed following operations like as host discovery, port scanning, and version detection
- **Service:** run against specific services that are listening on the target systems
- **Postrule:** runs after targets are scanned

For a current list of all the NSE scripts, visit:
https://nmap.org/nsedoc/index.html

Locating and Selecting Scripts

Scripts are commonly located in the folders:
/usr/share/nmap/scripts or
/usr/local/share/nmap/scripts.

You can also search your file system for *.nse files.

- `locate *.nse`
- `find / -name “*.nse”`

The `-sC` option is used to activate the NSE.

```
nmap 192.168.229.80 -p 80 -sC
```

Or a custom set of scripts can be specified using --script.

```
nmap --script smb-brute
192.168.229.0/24
```

NCAT

Ncat can be installed with Nmap and can replace netcat or nc. Type `ncat` in the terminal to view its options.

NPING

Nping can be installed with Nmap and is capable of performing simple pings to detect systems in addition to generating packets, response analysis and response time measurement. Type `nping` in the terminal to view its modes and options.

Echo Mode

Nping’s “echo mode” allows users to see how the generated probes change in transit and reveals differences between transmitted packets and received packets.

```
nping -c 1 --tcp -p 80,433
192.168.229.13 192.168.229.80
```

In this example:

- `-c` specifies the number of times to probe each system
- `--tcp` specifies the TCP Probe Mode
- `-p 80,433` specifies the ports, followed by two target IP addresses (`192.168.229.13 192.168.229.80`)

Nping's output will be a list of the packets being sent and received. The level of detail will depend on options used.

NDIFF

Ndiff can be installed with Nmap and is used to compare Nmap scans. It can produce output in human-readable text or machine-readable XML formats

Ndiff will pick up on the following differences:

- Host states (up to down)
- Port states (open to closed)
- Service versions (from `-sV`)
- OS matches (from `-O`)
- Script output

EVASION TECHNIQUES

For the purposes of testing network defenses, Nmap offers functionality to detect and evade security devices. Some evasion techniques supported by Nmap include:

Fragmentation of IP Packets

```
nmap -f <ip_addr>
nmap --mtu 8 <ip_addr>
```

In the above example, `--mtu` specifies the offset size `8`

Decoy IP Addresses

```
nmap -D RND:10 <ip_addr>
```

In the above example, `RND` specifies the generation of `10` random, non-reserved IP addresses

Zombie or Idle Scans

```
nmap -sI <zombie_ip_addr>
<target_ip_addr>
```

Source Port Spoofing

```
nmap --source-port <port> <ip_addr>
nmap -g <portnumber>
```

Note that the `--source-port` and `-g` options are equivalent

IP Spoofing

```
nmap -sS -S <spoofed_source_ip_addr>
<ip_addr>
```

SYN-ACKs are sent back from the target to the spoofed address which does not exist

MAC Address Spoofing

```
nmap -sT -PN --spoof-mac <Mac_addr>
<ip_addr>
```

Randomizing Target Scan Order

```
nmap --randomize-hosts
<ip_addr_range>
```

Adding Random Data to Packets

```
nmap --data-length 25 <ip_addr>
```

In the above example, `--data-length` specifies appending `25` random bytes to the sent packet(s)

Manipulating the IP Time-to-Live Field

```
nmap --ttl <value>
```

Sending Packets with Invalid TCP, UDP or SCTP Checksums

```
nmap --badsums <ip_addr>
```

Firewalk

```
nmap --script=firewalk --traceroute
<ip_addr>
```

Firewalk is a script that attempts to disover firewall rules

Disguising the User Agent

```
nmap 192.168.229.80 -p 80 -sC
-script-args http.useragent
="Some other Browser"
```