- Table of Contents
- NMAP Cheat Sheet
- Scan IP address (Targets)
- Port Related Commands
- Different Scan Types
- Identify Versions of Services and Operating Systems
- Scan Timings
- Output Types
- Discover Live Hosts
- NSE Scripts

Commands	Descriptions
nmap 10.0.0.1	Scan a single host IP
nmap 192.168.10.0/24	Scan a Class C subnet range
nmap 10.1.1.5-100	Scan the range of IPs between 10.1.1.5 up to 10.1.1.100
nmap -iL hosts.txt	Scan the IP addresses listed in text file "hosts.txt
nmap 10.1.1.3 10.1.1.6 10.1.1.8	Scan the 3 specified IPs only
nmap www.somedomain.com	First resolve the IP of the domain and then scan its IP address

Notes:-

Because we have not specified any other switches on the commands above (except the target IP address), the command will perform first host discovery by default and then scan the most common 1000 TCP ports by default.

Port Related Commands

On the section above we have not specified any ports which means the tool will scan the 1000 most common ports. However, in real engagements you should specify port numbers as well as shown below.

Commands	Descriptions
nmap -p80 10.1.1.1	Scan only port 80 for specified host
nmap -p20-23 10.1.1.1	Scan ports 20 up to 23 for specified host

nmap -p80,88,8000 10.1.1.1	*Scan ports 80,88,8000 only*
nmap -p- 10.1.1.1	*Scan ALL ports for specified host*
nmap -sS -sU -p U:53,T:22 10.1.1.1	*Scan ports UDP 53 and TCP 22*
nmap -p http,ssh 10.1.1.1	*Scan http and ssh ports for specified host*

Different Scan Types

Nmap is able to use various different techniques to identify live hosts, open ports etc. The following are the most popular scan types.

Commands	*Descriptions*
nmap -sS 10.1.1.1	*TCP SYN Scan (best option)*
nmap -sT 10.1.1.1	*Full TCP connect scan*
nmap -sU 10.1.1.1	*Scan UDP ports*
nmap -sP 10.1.1.0/24	*Do a Ping scan only*
nmap -Pn 10.1.1.1	*Don't ping the hosts, assume they are up*

There are some more scan types supported by nmap but we have listed the most useful ones above. Here is an overview of the most popular scan types:

-sS: This sends only a TCP SYN packet and waits for a TCP ACK. If it receives an ACK on the specific probed port, it means the port exist on the machine. This is fast and pretty accurate.

-sT: This creates a full TCP connection with the host (full TCP handshake). This is considered more accurate than SYN scan but slower and noisier.

-sP: This is for fast checking which hosts reply to ICMP ping packets (useful if you are on the same subnet as the scanned range and want a fast result about how many live hosts are connected).

Identify Versions of Services and Operating Systems

Another important feature of NMAP is to give you a wealth of information about what versions of services and Operating Systems are running on the remote hosts.

Commands	*Descriptions*
nmap -sV 10.1.1.1	*Version detection scan of open ports (services)*
nmap -O 10.1.1.1	*Identify Operating System version*

nmap -A 10.1.1.1	*This combines OS detection, service version detection, script scanning and traceroute.*

Scan Timings

Commands	*Descriptions*
nmap -T0 10.1.1.1	*Slowest scan (to avoid IDS)*
nmap -T1 10.1.1.1	*Sneaky (to avoid IDS)*
nmap -T2 10.1.1.1	*Polite (10 times slower than T3)*
nmap -T3 10.1.1.1	*Default scan timer (normal)*
nmap -T4 10.1.1.1	*Aggressive (fast and fairly accurate)*
nmap -T5 10.1.1.1	*Very Aggressive (might miss open ports)*

Output Types

For each scan we recommend outputting the results in a file for further evaluation later on. Nmap supports 3 main output formats as below:

Commands	*Descriptions*
nmap -oN [filename] [IP hosts]	*Normal text format*
nmap -oG [filename] [IP hosts]	*Grepable file (useful to search inside file)*
nmap -oX [filename] [IP hosts]	*XML file*
nmap -oA [filename] [IP hosts]	*Output in all 3 formats supported*

Example:

nmap -oN scan.txt 192.168.0.0/24 (this will scan the subnet and output the results in text file "scan.txt")

Discover Live Hosts

There are various techniques that can be used to discover live hosts in a network with nmap. Depending on whether you are scanning from the same LAN subnet or outside of a firewall, different live host identifications can be used (we will discuss this later)

Commands	*Descriptions*
nmap -PS22-25,80 10.1.1.0/24	*Discover hosts by TCP SYN packets to specified ports (in our example here the ports are 22 to 25 and 80)*
nmap -Pn 10.1.1.0/24	*Disable port discovery. Treat all hosts as online.*
nmap -PE 10.1.1.0/24	*Send ICMP Echo packets to discover hosts.*

nmap -sn 10.1.1.0/24	*Ping scan.*

NSE Scripts

Did you know that nmap is not only a port scanner? Actually, there are hundreds of included scripts that you can use with nmap to scan for all sorts of vulnerabilities, brute force login to services, check for well-known weaknesses on services etc.

Commands	*Descriptions*
nmap --script="name of script" 10.1.1.0/24	*Run the specified script towards the targets.*
nmap --script="name of script" --script-args="argument=arg" 10.1.1.0/24	*Run the script with the specified arguments.*
nmap --script-updatedb	*Update script database*

Other Useful Commands

Some other miscellaneous but useful commands:

Commands	*Descriptions*
nmap -6 [IP hosts]	*Scan IPv6 hosts*
nmap --proxies url1,url2	*Run the scan through proxies*
nmap --open	*Only show open ports*
nmap --script-help="script name"	*Get info and help for the specified script*
nmap -V	*Show currently installed version*
nmap -S [IP address]	*Spoof source IP*
nmap --max-parallelism [number]	*Maximum parallel probes/connections*
nmap --max-rate [number]	*Maximum packets per second*

Created by:- Vikram Solanki (Certified Ethical Hacker)