🚀 60 DAYS OF NMAP – ONE COMMAND A DAY, ONE STEP CLOSER TO MASTERY 🔍

BY UMAR IQBAL

SWIPE

What is Nmap?

Nmap is an open-source network scanner used to discover hosts and services on a network. It provides detailed information about active systems, open ports, running services, and potential vulnerabilities.

Why Use Nmap?

1. Network inventory and management
2. Security assessment and vulnerability detection
3. Firewall evasion and penetration testing
4. Host and service discovery

SWIPE

Basic Nmap Commands:

1. “nmap –version” OR “nmap –v”
   check version of installed nmap.

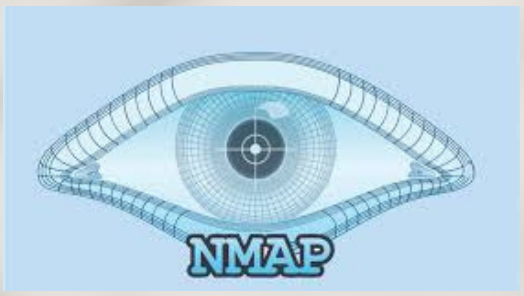
2. Nmap –h
   check help for nmap.

3. “nmap <target>”
   Basic scan for target without any flags, Nmap performs a SYN scan

4. nmap <target1> , <target2> , <target3>
   scan multiple Targets.

5. nmap -sn 192.168.1.0/24
   Determine if hosts are live. Means live/active hosts in your network.

SWIPE



6. nmap 192.168.1.1-50

scan a range of IPs/targets.

7. nmap 192.168.1.0/24

Scan an entire subnet.

8.nmap -p 22,80,443 <target>

Scan specific ports

9.nmap -p- <target>

Scan all ports

10.nmap -sV <target>

Service version detection

11.nmap -O <target>

Operating system Detection.

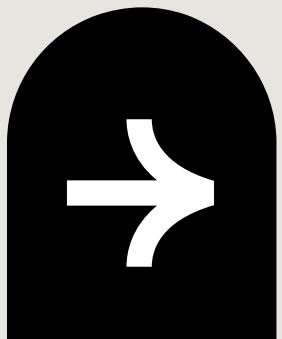
12.nmap -sT <target>

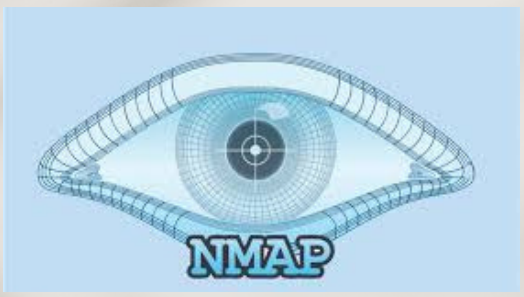
TCP connect scan (Full connection)

13.nmap -sS <target>

SYS scan (stealth scan).

SWIPE





14.nmap -sU <target>

UDP scan.

15.nmap -A <target>

Aggressive scan (version, OS, Scripts).

16.nmap -p 80 -sV <target>

Version Detection for a specific port.

17.nmap -Pn <target>

Disable Host Discovery (ping).

18.nmap -sL <target>

List targets without scanning.

19.nmap -sn <target>

ping scan to determine if hosts are live.

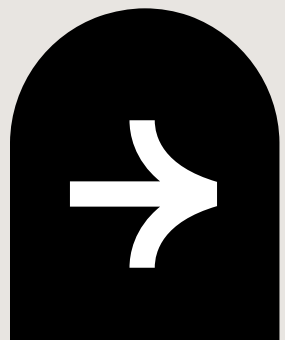
20.nmap -v <target>

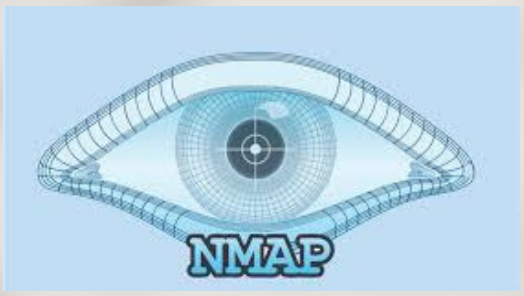
verbose mode (more details).

21.nmap -vv <target>

very verbose mode.

SWIPE





22.nmap -oX output.xml <target>

save output in XML format.

23.nmap -oG output.gnmap <target>

save output in grepable format.

24.nmap --script http-enum <target>

run specific scripts

25.nmap -sP 192.168.1.0/24

Ping scan for determining if hosts are up

26.nmap --top-ports <number>

Scan the most common ports.

27.nmap -p <port> --open <target>

Show only open ports

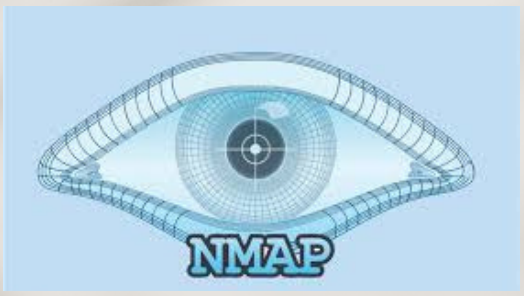
28.nmap --max-retries <num> <target>

Set the maximum number of retries

29.nmap --min-rate <rate> <target>

Set minimum packet rate per second.

SWIPE



30.nmap -p 1-1000 <target>

Scan the first 1000 ports

31.nmap --scan-delay <time> <target>

Set wait time between packets

32.nmap -sT -p 80 <target>

TCP connect scan for a specific port

33.nmap --script vuln <target>

Run vulnerability detection scripts

34.nmap -sR <target>

Scan ports recording responses

35.nmap -6 <target>

IPv6 scanning

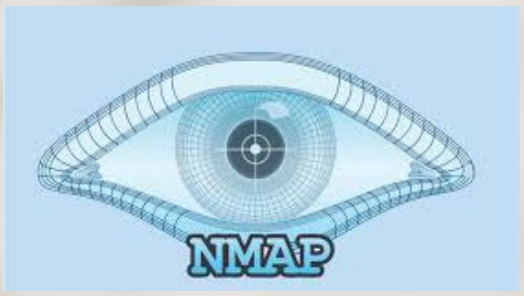
36.nmap -T4 <target>

Adjust scan speed

37.nmap --version-all <target>

Detailed version detection

SWIPE



38.nmap --script=http-* <target>

Run specific HTTP scripts

39.nmap --source-port <port> <target>

Scan using a specific source port

40.nmap --data-length <length> <target>

Send given length packets

41.nmap --badsum <target>

Send packets with incorrect checksum

42.nmap --script-args <args>

Pass arguments to scripts

43.nmap --script-timeout <time> <target>

Set timeout for scripts

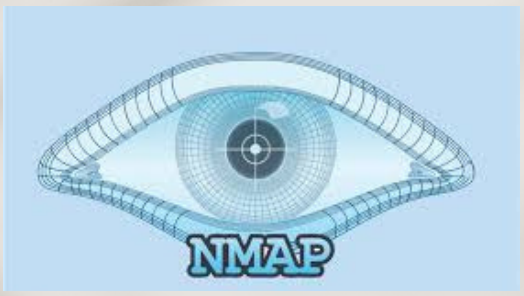
44.nmap --datagram-length <length> <target>

Adjust datagram length

45.nmap -sV --script=default <target>

Run Nmap default scripts

SWIPE



46.nmap --traceroute <target>

Perform a traceroute to determine the route

47.nmap -sA <target>

TCP port scan with analysis flags

48.nmap --packet-trace <target>

Show details of packets sent and received

49.nmap -p 0-65535 <target>

Scan all ports

50.nmap -p 1-1000 --open <target>

Scan first 1000 ports that are open

51.nmap -sS -p <port> <target>

SYN scan for a specific port

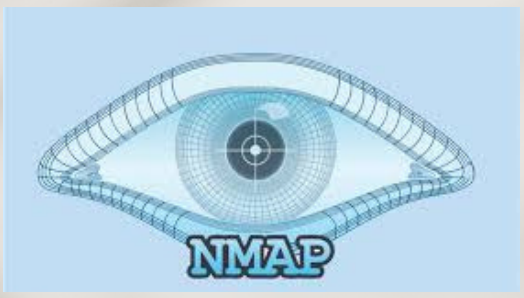
52.nmap -sC <target>

Run default category scripts

53.nmap -oA <basename> <target>

Save output in all formats

SWIPE



54.nmap --script http-methods <target>

Detect supported HTTP methods

55.nmap -sV --version-intensity <level> <target>

Adjust version detection intensity

56.nmap --top-ports 100 <target>

Scan the top 100 most common ports

57.nmap -p <port> --script <script> <target>

Run a specific script on a specific port

58.nmap -sS -p 443 <target>

Stealth scan on port 443 (HTTPS)

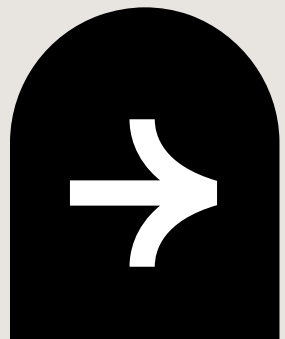
59.nmap --dns-servers <DNS_IP> <target>

Use a specific DNS server for name resolution

60.nmap -iR <num>

Scan a random set of IP addresses

SWIPE



FOLLOW ME ON LINKEDIN:

www.linkedin.com/in/umar-iqbal-901b892b7

✅ That’s 60 Nmap commands!
Thanks to everyone who followed along the journey.
From basic scans to advanced scripting, this series was all about learning and sharing.
If you found it helpful — feel free to connect, comment your favorite command, or suggest what tool I should cover next. 🚀

@UMAR-IQBAL