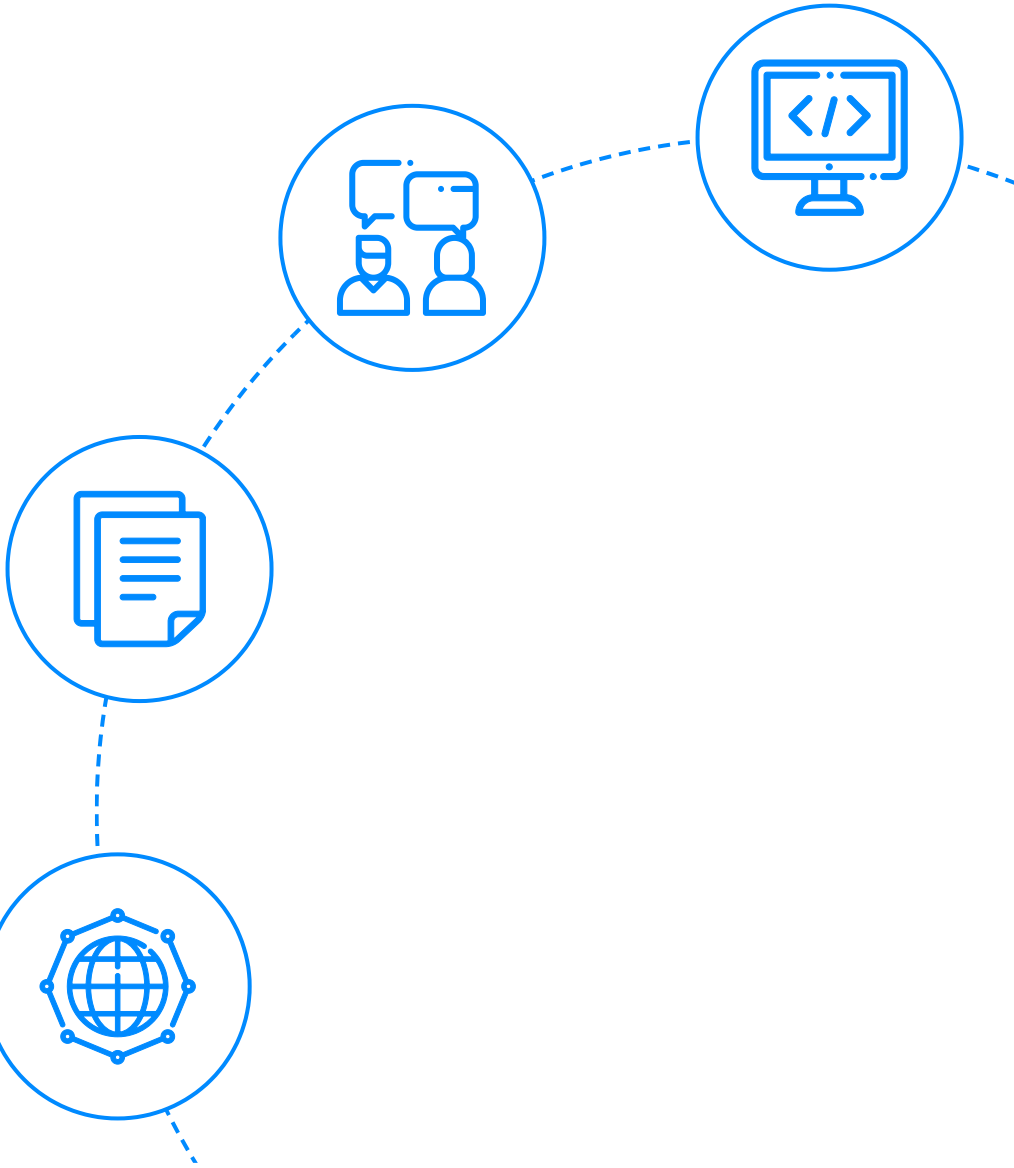
InterviewBit

NMAP Cheat Sheet



To view the live version of the page, click here.

Contents

NMAP Tutorial: Basics to Advanced

Let's get Started

Nmap("**Network Mapper**") is an open-source and free tool that's widely used for network discovery purposes. It's capable of performing both host discovery and service detection, as well as doing a content analysis of the traffic it receives. Common uses for Nmap include vulnerability discovery, system security auditing, and detecting cyber attacks. You can run Nmap on a command line or in a web browser. To get the most out of Nmap, you should familiarize yourself with its features and usage.

Nmap can be used to find open ports on a remote host or network, and check whether a host or network has been compromised. It can also be used to test your own server or network to identify weak spots. Another common use case is in vulnerability assessment: using Nmap to test the connection between your website and your users to see whether your application is open to exploitation.

When used properly, Nmap can be a very powerful tool. However, using it incorrectly can also cause problems. For example, sending a request with a Nmap scan that includes a lot of output will likely consume a lot of network bandwidth. This type of scan is called **promiscuous mode** and can cause network congestion if not used properly. Sending a request with a light Nmap scan may not cause any extra traffic but is still likely to return inaccurate results.

Nmap can also be used for malicious purposes. Connecting a vulnerable system to a large network of malicious systems can help spread infection. Using Nmap to scan networks for vulnerabilities is also a risky proposition. It is likely to return inaccurate or even misleading results. Nmap is an open-source tool and is widely used by Nessus and other security researchers. Therefore, it is likely to be well-regarded by the community.

NMAP Tutorial: Basics to Advanced

1. Nmap Scan Types

Scan Type	Details
TCP SCAN	A TCP scan is used to ensure that a three-way handshake has been completed between you and a selected target system. Even though it is very noisy, a TCP scan can be detected with little to no effort. This is because the services may log the sender's IP address and may trigger an intrusion detection system.
UDP SCAN	The UDP scan checks whether there is any UDP port open and listens for incoming connections on the target machine. Contrary to TCP, UDP does not offer any way to cure a positive result by sending a response with a positive acknowledgment. As a result, UDP scans may sometimes produce false positives. This type of scan is usually quite slow because computers, in general, slow down their responses to this kind of traffic in order to be on the safe side.
SYN SCAN	In a SYN scan, a TCP connection is established by first creating a SYN packet and sending it to the server. This is unlike a normal TCP scan, which just generates a SYN packet. The response to these specially crafted packets is also analyzed by Nmap to produce scan results.
ACK SCAN	To be able to monitor whether a particular port is filtered or not, ACK scans are employed. This guarantees to be very valuable when trying to spy on firewalls or their existing protocols. Simple packet filtering allows established connections, whereas a more complex firewall might not.

Category-wise diverse **NMAP commands** with examples are explained in the following section.

2. Target Specification

Switch	Example	Description
	`nmap 192.168.1.3`	Scan a specific IP address
	`nmap 192.168.1.2 192.168.2.3`	Scan specific IP addresses
	`nmap 192.168.1.7-254`	Scan specific range of IP addresses
	`nmap ramdom.doman.org`	Scans a domain
	`nmap 192.168.1.1/29`	Scans a single IP using CIDR notation
-iL	`nmap -iL text.txt`	Scans a target from a file
-iR	`nmap -iR 200`	Scans random 200 hosts
–exclude	`nmap -exclude 192.168.1.2`	Exclude the listed hosts

3. Scan Techniques

Switch	Example	Description
-sS	`nmap 192.167.1.2 -sS`	TCP SYN Scan
-sT	`nmap 192.168.1.1 -sT`	TCP Connect Scan
-sU	`nmap 192.168.1.1 -sU`	UDP scan
-sA	`nmap 192.168.1.1 -sA`	TCP ACK Scan
-sW	`nmap 192.168.1.1 -sW`	TCP Window scan
-sM	`nmap 192.168.1.1 -sM`	TCP Maimon scan

4. Host Discovery

Switch	Example	Description
-sL	`nmap 192.168.1.6-9 -sL`	Creates targets List only
-sn	`nmap 192.168.1.2/29 -sn`	This disables port scans and does host discovery only.
-Pn	`nmap 192.168.1.2-5 -Pn`	This disables host discovery and allows port scan only.
-PS	`nmap 192.168.1.2-5 -PS22-25,80`	TCP SYN ping on port x. Port 80 is by default
-PA	`nmap 192.168.1.2-5 -PA22-25,80`	TCP ACK ping on port x. Port 80 is by default
-PU	`nmap 192.168.1.3-7 -PU53`	Enables UDP ping on port x. Port 40125 is by default
-PR	`nmap 192.168.1.2-3/24 -PR`	ARP ping on the local network
-n	`nmap 192.168.1.2 -n`	Disables DNS resolution

5. Port Specification

Switch	Example	Description
-p	`nmap 192.168.1.9 -p 27`	Scan a specific port
-p	`nmap 192.168.1.9 -p 27-100`	Scan a port range
-p	`nmap 192.168.1.9 -p U:53,T:27-40,80`	Scans multiple TCP and UDP ports
-p-	`nmap 192.168.1.9 -p-`	Scan all ports
-p	`nmap 192.168.1.9 -p http,https`	Scans based on the service name
-F	`nmap 192.168.1.9 -F`	Scan 100 ports in fast manner
–top-ports	`nmap 192.168.1.9 -top-ports 1015`	Scans the top “x” ports
-p-65535	`nmap 192.168.1.8 -p 65535`	Skips the initial port in the range and starts the scan from port 1

6. Service and Version Detection

Switch	Example	Description
-sV	`nmap 192.168.1.9 -sV`	Helps in determining the version of the service
-sV –version-intensity	`nmap 192.168.1.9 -sV --version-intensity 9`	To increase the Intensity level between 0 to 9. The higher the number higher is possibility of correctness
-sV –version-light	`nmap 192.168.1.9 -sV --version-light`	This enables light mode. This has a lower possibility of correctness but is faster.
-sV –version-all	`nmap 192.168.1.9 -sV --version-all`	This enables an intensity level of 9. This has a higher possibility of correctness but is slower.
-A	`nmap 192.168.1.8 -A`	This enables OS detection, version detection, and script scanning.

7. OS Detection

Switch	Example	Description
-O	`nmap 192.168.1.8 -O`	TCP/IP stack fingerprinting is used for remote OS detection.
-O –osscan-limit	`nmap 192.168.1.8 -O -osscan-limit`	The TCP port scan will not attempt OS detection on those hosts that do not have at least one open and one closed port.
-O –osscan-guess	`nmap 192.168.1.8 -O -osscan-guess`	Makes Nmap guess more competently
-O –max-os-tries	`nmap 192.168.1.8 -O -max-os-tries 1`	This set the maximum number “x” of OS detection attempts against a target

8. Timing and Performance

Switch	Example	Description
-T0	`nmap 192.168.1.8 -T0`	Paranoid (0) Timing
-T1	`nmap 192.168.1.8 -T1`	Sneaky (1) Timing
-T2	`nmap 192.168.1.8 -T2`	Polite (2) Timing
-T3	`nmap 192.168.1.8 -T3`	Normal (3) Timing
-T4	`nmap 192.168.1.8 -T4`	Aggressive (4) Timing
-T5	`nmap 192.168.1.8 -T5`	Insane (5) Timing

Switch	Example input	Description
–host-timeout <time>	5s; 10m; 5h	After this long, give up on the target.
–min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	5s; 10m; 5h	How long it takes to return a probe round trip.
–min-hostgroup/max-hostgroup <size<size>	20; 512	Specifies host scan group sizes for parallelization
–min-parallelism/max-parallelism <numprobes>	10; 1	This probes parallelization
–scan-delay/–max-scan-delay <time>	10ms; 5s; 10m; 3h	This adjusts the delay between probes
–max-retries <tries>	5	Specifies the maximum number retries for port scan probe retransmissions

9. NSE Scripts

Switch	Example	Description
-sC	`nmap 192.168.1.9 -sC`	Default NSE scripts are used to scan.
–script default	`nmap 192.168.1.9 -script default`	This scans with default NSE scripts
–script	`nmap 192.168.1.9 -script=banner`	Single script scanning
–script	`nmap 192.168.1.9 -script=http*`	Wildcard scanning
–script	`nmap 192.168.1.9 -script=http,banner`	Two scripts scanning
–script	`nmap 192.168.1.9 -script "not intrusive"`	Default scanning without intrusive scripts
–script-args	`nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.9`	NSE script scanning with scipts

10. Useful NSE Script Examples

Command	Description
`nmap -Pn -script=http-sitemap-generator interviewbit.com`	Map generator for HTTP site
`nmap -n -Pn -p 80 -open -sV -vvv -script banner,http-title -iR 1000`	Search random web servers
`nmap -Pn -script=dns-brute interviewbit.com`	This gusses sub-domains by brute forcing on DNS hostnames
`nmap -n -Pn -vv -O -sV -script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1`	Run safe SMB scripts
`nmap -script whois* interviewbit.com`	Query for whois
`nmap -p80 -script http-unsafe-output-escaping interviewbit.com`	Vulnerabilities detection on cross websites
`nmap -p80 -script http-sql-injection interviewbit.com`	SQL injections detection

11. Firewall / IDS Evasion and Spoofing

Switch	Example	Description
-f	`nmap 192.168.1.9 -f`	Small fragmented IP packets are used in requested scans (including ping scans). More difficult for packet filters
–mtu	`nmap 192.168.1.9 -mtu 32`	Set the offset size yourself
-D	`nmap -D 192.168.9.102, 192.168.9.103, 192.168.9.104, 192.168.9.523`	Scans from the spoofed IPs are send via this
-S	`nmap -S www.interviewbit.com www.scaler.com`	Scans Scaler from InterviewBit
-g	`nmap -g 53 192.168.1.9`	Uses the given port number
–proxies	`nmap -proxies http://192.168.1.9:8080, http://192.168.9.2:8080 192.168.1.9`	This relays connections via HTTP or SOCKS4 proxy
–data-length	`nmap -data-length 200 192.168.1.9`	This adds random data to the sent packets

12. Output

Switch	Example	Description
-oN	`nmap 192.168.1.9 -oN result.file`	Adds the output to the result.file that is in normal format
-oX	`nmap 192.168.1.9 -oX result.file`	Adds the output to the result.file that is in XML format
-oG	`nmap 192.168.1.9 -oG result.file`	Adds the output to the result.file that can be grepable
-oA	`nmap 192.168.1.9 -oA results`	All three major formats are displayed via this
-oG –	`nmap 192.168.1.9 -oG -`	Shows grepable output on the screen
–append-output	`nmap 192.168.1.9 -oN file.file -append-output`	Adds a scan to the previous scanned file
-v	`nmap 192.168.1.9 -v`	Verbosity level is increase via this
-d	`nmap 192.168.1.9 -d`	Debugging level is increase via this
–reason	`nmap 192.168.1.9 -reason`	Shows the reason for the given state of the port
–open	`nmap 192.168.1.9 -open`	Open ports are shown

13. Other Useful NMAP Commands

Command	Description
`nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn`	Only ports x are scanned, no ports are discovered.
`nmap 192.168.1.9-1/25 -PR -sn -vv`	Only show ARP discovery on the local network, no port scan.
`nmap -iR 20 -sn -traceroute`	No port scan - just traceroute to specific targets.
`nmap 192.168.1.9-40 -sL -dns-server 192.168.1.9`	Queries the Internal DNS for detecting hosts and then lists targets

Conclusion

In this document, we've covered the basics of Network Mapper (NMAP), its features and some of the important cheat sheets. NMAP is the supreme source of port scan information, the foundation for most security enumeration during the initial phases of a penetration test. It has a number of settings and when you first start out using it it may be difficult to figure out. You can follow the guide for running Nmap on a Mac OS X or Linux machine. The beauty of the Nmap tool is that it's designed to work with text output. This means that you do not have to be an expert in Linux or Bash Scripting in order to use this amazing tool. The code examples are very easy to follow and you will be up and running with Nmap in no time.

Now, it's time for you to head out and try what we've covered here and more. More than memorizing syntax, do pay attention to practising them and solving problems.

Links to More Interview Questions

C Interview Questions	Php Interview Questions	C Sharp Interview Questions
Web Api Interview Questions	Hibernate Interview Questions	Node Js Interview Questions
Cpp Interview Questions	Oops Interview Questions	Devops Interview Questions
Machine Learning Interview Questions	Docker Interview Questions	Mysql Interview Questions
Css Interview Questions	Laravel Interview Questions	Asp Net Interview Questions
Django Interview Questions	Dot Net Interview Questions	Kubernetes Interview Questions
Operating System Interview Questions	React Native Interview Questions	Aws Interview Questions
Git Interview Questions	Java 8 Interview Questions	Mongodb Interview Questions
Dbms Interview Questions	Spring Boot Interview Questions	Power Bi Interview Questions
Pl Sql Interview Questions	Tableau Interview Questions	Linux Interview Questions
Ansible Interview Questions	Java Interview Questions	Jenkins Interview Questions