Nmap Syntax

1.Scanning an IP
Syntax: nmap <target-ip>

2.Scanning a HOST
Syntax: nmap <www.example.com>

3.Scanning a range of IPs
Syntax: nmap <ip-address-range>

4.Scanning a Subnet
Syntax: nmap <ip-address/24>

5.Scanning a Targets from a Text File
Syntax: nmap -iL <list.txt>

6.Scanning target & Ignore Discovery
Syntax: nmap -target-ip <-Pn>

7.Scanning target & Host Discovery
Syntax: nmap -target-ip <-sP>

8.Scan a Single Port
Syntax: nmap <target-ip> <-p port numbers>

9.Scan a range of ports
Syntax: nmap <target-ip> <-p firstport-lastport>

10.Scan all ports (65535)
Syntax: nmap <target-ip><-p->

11.Scan TCP or UDP Ports
Syntax: nmap <target-ip><-p U:port, T:port>

12.Fast Port Scan
Syntax: nmap <target-ip><-F> -v

13.No Randomise Port Scan
Syntax: nmap <target-ip><-r> -v

14.Nmap Top Ports Scan
Syntax: nmap <target-ip><—top-ports N> -v

15.Nmap Port Ratio Scan
Syntax: nmap <target-ip><—ports-ratio > -v

16.Port-knocking an obfuscation-as-security technique.
Syntax: for x in 1-10000; do nmap -Pn -p $x server_ip_address; done

17.Standard Service Detection
Syntax: nmap <target-ip><-sV>

18.Light Service Detection
Syntax: nmap <target-ip><-sV —version-intensity 0>

19.Aggressive Service Detection
Syntax: nmap <target-ip><-sV —version-intensity 5>

20.OS Detection
Syntax: nmap <target-ip> <-O >

21.OS Detection
Syntax: nmap <target-ip> <—max-os-tries>

22.OS Detection
Syntax: nmap <target-ip><—osscan-limit >

23.OS Detection
Syntax: nmap <target-ip><—osscan-guess; —fuzzy >

24.OS Detection
Syntax: nmap <target-ip><—script —smb-os-discovery >

25.Save Normal Output to File
Syntax: nmap <target-ip><-oN file.txt>

26.Save XML Output to File
Syntax: nmap <target-ip><-oX file.txt>

27.Save XML to CSV for Recon
Syntax: nmap <target-ip><-oX file.txt>
• Python parsey.py op.xml op.csv

28.Save "Grep"able Output to File
Syntax: nmap <target-ip><-oG file.txt>

29.ScRipT K1dd3 Output to File
Syntax: nmap <target-ip><-oS file.txt>

30.Save All Types Output to File
Syntax: nmap <target-ip><-oA file.txt>

31.Scan using Default Safe Scripts
Syntax: nmap <target-ip><-sC>

32.Getting Help for any Scripts
Syntax: nmap <target-ip><—script-help=scriptname>

33.Nmap Script Args
Syntax: nmap <target-ip><—script=scriptname —scriptargs>

34.Scan using specific Scripts
Syntax: nmap <target-ip><—script=script name.nse>

35.Scan using set of Scripts
Syntax: nmap <target-ip><—script="http-*">

36.Update Script Database
Syntax: nmap <target-ip><—script=updatedb>

37.Safe Scripts
Syntax: nmap <target-ip><—script=safe,default>

38.Vulnerability Scripts

Syntax: nmap <target-ip><—script=vuln>

39.DOS Scripts

Syntax: nmap <target-ip><—script=dos>

40.Exploit Scripts

Syntax: nmap <target-ip><—script=exploit>

41.Malware Scripts

Syntax: nmap <target-ip><—script=http-malware-host>

42.Intrusive Scripts

Syntax: nmap <target-ip><—script=intrusive>

43.NOT including Scripts

Syntax: nmap <target-ip><—script=not script type>

44.Boolean Expression Scan

Syntax: nmap <target-ip><—script=and or not script type>

45.Traceroute Scan

Syntax: nmap <target-ip><—traceroute>

46.Trace Traffic & Geo Resolution Scan

Syntax: nmap <target-ip><—script=traceroutegeolocation>

47.DNS BruteForce Scan

Syntax: nmap <target-ip><—script=dns-brute.nse>

48.Find Hosts on IP Scan

Syntax: nmap <target-ip> <—script=hostmap-bfk.nse>

49.Whois Scan

Syntax: nmap <target-ip><—script=whois-ip, whoisdomain>

50.Robots Scan

Syntax: nmap <target-ip><—script=http-robots.txt>

51.WAF Detect Scan

Syntax: nmap <target-ip><—script=http-waf-detect>

52.WAF Fingerprint Scan
Syntax: nmap <target-ip><—script=http-waf-fingerprint>

53.Wafw00f vs Nmap Scan
Syntax: wafw00f <target.com>
Syntax: nmap <target-ip><—script=http-waf-fingerprint>

54.Firewalk Scan
Syntax: nmap <target-ip><—script=firewalk —traceroute>

55.Shodan Scan
Syntax: nmap <target-ip><—script=shodan-api>

56.Email Enumeration
Syntax: nmap <target-ip><—script=http-grep>

57.Nmap Crawlers Scan
Syntax: nmap <target-ip><—script=http-useragent-tester>

58.Nmap Discovering Directories Scan
Syntax: nmap <target-ip><—script=http-enum>

59.Nmap Open Relay Scan
Syntax: nmap <target-ip><—script=smtp-open-relay>

60.Nmap SMTP User Enum Scan
Syntax: nmap <target-ip><—script=smtp-enum-users>

61.Nmap SMTP Password Attack Scan
Syntax: nmap <target-ip><—script=smtp-brute>

62.Nmap SMTP Backdoor Detect Scan
Syntax: nmap <target-ip><—script=smtp-strangeport>

63.Nmap POP3 Capabilities Scan
Syntax: nmap <target-ip><—script=pop3-capabilities>

64.Nmap IMAP Capabilities Scan

Syntax: nmap <target-ip><—script=imap-capabilities>

65.Nmap Cloak Scan with Decoy

Syntax: nmap <target-ip><-D>

66.Nmap Spoof Mac Address

Syntax: nmap <target-ip><—spoof-mac>

67.Nmap Select Interface

Syntax: nmap <target-ip><-e ethO>

68.Nmap Source Port Modify

Syntax: nmap <target-ip><—source-port 7890>

69.Nmap Fake TTL

Syntax: nmap <target-ip><—ttl 128>

70.Nmap Relay Proxies

Syntax: nmap <target-ip><—proxies proxy:port>

71.Nmap Bogus TCP/UDP Checksum

Syntax: nmap <target-ip><—badsum>

72.Nmap Bogus Fragment Scan

Syntax: nmap <target-ip> <-f>

73.Nmap MTU Scan

Syntax: nmap <target-ip><-mtu 8>