Nmap Purpose	Nmap Commands	Wireshark Filters	Firewall Bypass Commands	Comments
Nmap TCP scan	nmap -sT -p 80,443 target_IP	ip.addr==ipaddress		
Nmap Syn Scan	nmap -sS -p 80,443 target_IP			
Nmap Null Scan	nmap -sN -p 80,443 target_IP		Bypass Firewall	Use only on the non-windows system to bypass the firewall
Nmap UDP scan (UDP ports)	nmap -sU -p 80,443 target_ip			For scanning the UDP ports
Nmap FIN scan	nmap -sF target_IP			It sets all the TCP packet header as FIN
Nmap XMAS scan	nmap -sX target_IP			Sends the packet with FIN, URG ,PUSH flag
Nmap ACK Scan	nmap -sA target_IP		Used to determine the state of the firewall	
Nmap Zombie Scan	Nmap -sI zombieIP -vv Target_IP		Used to bypass some Firewall rules on the internal system scan	
Nmap Normal Scan	Nmap target_IP			
nmap Range Scan	nmap target_IP/CIDR_value or Nmap target_IP-255			
Nmap Fast Scan	nmap -F target_IP			It scans only top 100 ports
Nmap Host Discovery scan	nmap -sn Target_subnet/24 netdiscover -r target_subnet/24 -I eth0 arpscan -l nmap -sP target_subnet/24			
Nmap scan through List	nmap -iL target_ip_list.txt			
Nmap random IP scanning	nmap -iR 20 -vv			This scan automatically picks 20 ipaddress from internet and it starts to scan that
Nmap exclude IP Scan	nmap -F target_subnet/24 --exclude IP_you_wanna_exclude			
Nmap exclude the List of IP	nmap -F target_subnet/24 --excludefile file.txt			
Nmap NO Host Discovery Scan	nmap -Pn target_subnet/24 -vv		Bypass the firewall based on the ICMP	It basically skips the ping scan and directly goes to the port scan
Nmap Scan using the port name & port Numbers	nmap target_IP -p ssh,ftp nmap target_IP -p 22,23			
Nmap scan only for open ports	nmap target_ip -vv --open			
Nmap to stop the random port scan	nmap -r target_IP			It scans the target system's port in ascending order.
Nmap top port scan	nmap target_IP --top-ports 10			It only scans the top 10 ports
Nmap service detection (Banner Grabbing)	nmap -sV target_IP -vv nmap -sV target_IP --version-intensity 0 nmap -sv -v target_IP --version-intensity 5			
Nmap OS detection with some scripts	nmap -O target_IP nmap -O target_IP --max-tries 5 -vv nmap -O target_IP --osscan-limit -vv			
Nmap OS detection with SMB script	nmap --script smb-os-discovery target_IP			
Nmap OUTPUT file formats	nmap -sV -T4 -oN filename.txt - Normal Output nmap -sV -T4 -oX filename.xml - XML output nmap -sV -T4 -oA filename - all file format.			
Running default nse script against the target server	nmap target_IP --script=default			
Nmap for ftp bruteforcing	Nmap target_ip -vv -Pn -p 9999 --script ftp-brute --script-args userdb=path_to_userdb.txt , passdb=path_to_password_db.txt			
Scanning the Target system with wildcard NSE scripts	Nmap target_system -vv --script http-* -p 80,443 -Pn			
How to update the nse script database	Nmap --script=updatedb or nmap --script updatedb -vv			
Nmap Vulnerability scan	Nmap --script vuln -p- -vv target_IP			
Check For DOS attack using Nmap	Nmap target_IP --script=dos -vv -Pn			It runs different scripts to detect whether the target system is vulnerable to DOS attack or not
Exploit scan against the target_IP	Nmap target_IP --script=exploit -vv -p- or nmap target_IP --script exploit -vv -p-			It basically runs all the exploits that are with nmap against the target server
How to check your target system is vulnerable for malw	nmap target_IP --script=http-malware-host			It basically checks for if the target system is afftected by any known malware attack.
Boolean nmap scripts scan	Nmap target_ip --script "(vulns and exploit) and not http-*" -vv			
Nmap Traceroute scan	Nmap target_IP --traceroute -vv			This to identify where the target system is hosted on.
How to find the geolocation of the target system	Nmap target_ip --traceroute --script=traceroute-geolocation -p 80			
How to perform the dns bruteforce scan	Nmap target_ip --script=dns-brute -vv			It is used to enumerate all the DNS records of the target domain.
Whois scan for the targetIP	Nmap --script=whois-domain target_IP			
How to detect the WAF using nmap	nmap --script=http-waf-detect target_IP -p 80,443 -vv			This command used for firewall Detection
Fingerprinting the WAF	nmap --script=http-waf-fingerprint target_IP -p 80,443, -vv			
Nmap to find the firewalled ports	Nmap target_ip --script=firewalk --traceroute -vv			It basically finds what are the ports are filtered
Enumerating emails by spidering the target website an	Nmap target_ip --script=http-grep --script-args http-grep.builtins=e-mail -vv			
Sitemap generation using the Nmap command	Nmap -vv target_ip --script http-sitemap-generator -p 80			It basically give the sitempa, Which looks like the tree structure of the files that are presented on the webpages of the target website
Website Crawler scan	Nmap --script=http-useragent-tester target_IP -vv -p 80			It is used to identify the what are the HTTP crawlers are allowed to crawl against the target website
Nmap HTTP directory scan	Nmap --script=http-enum target_IP -vv -p 80			It is just trying to enumerate the sensitive directories against the target webserver
SMTP Open Relay Attack Scan	Nmap --script=smtp-open-relay target_IP -vv -p 25			It is basically check for the target system is vulnerable to SMTP open Relay Attack or not
SMTP username Enumeration	nmap --script=smtp-enum-users target_IP -vv -p 25			It is basically enumerates the SMTP usernames of the target server
SMTP password Bruteforcing	Nmap --script smtp-brute target_IP -vv -p 25			It bruteforce the password for the SMTP service
SMTP backdoor Detection Scan	Nmap target_ip --script=smtp-strangeport -vv			It basically checks the target server's smtp service, If the SMTP service is running on the target server apart from the defautl port, Then there is a possibility of running the SMTP backdoor on that server
POP3 Enumeration	nmap --script=pop3-capabilities target_IP -vv -p 25			It basically tells us the what are the supported commands from the POP3 service
IMAP Enumeration	nmap --script=imap-capabilities target_IP -vv -p 25			It basically tells us the what are the supported commands from the IMAP service
Nmap Decoy Scan	Nmap -D spoofed_ip target_IP -vv		Firewall Bypassing	
Nmap Scan with Customized Interface	Nmap target_IP -e eth0 -sV -Pn -vv			We can manually select the interface to perform the scan against the target system
Scan with spoosed Mac address	Nmap target_IP --spoof-mac mac_address -vv -Pn		Firewall Bypassing	We can spoof the mac address while doing the scan against the target IP
Spoofing the source port	Nmap target_IP --source-port 3555 -vv		Firewall Bypassing	
Spoofing TTL to confuse the target person	Nmap target_IP -p 80,443 -vv --ttl 64			By using this scan we can prevent the OS detection.
How to use Proxy for scanning the system	Nmap target_IP --proxies proxy:portno -vv			
Nmap Bogus Scan	Nmap target_IP -vv --badsum -p 21,22,23			By using this scan we can come to whether the target system is behind the IDS or Firewall. If the target system has the firewall or IDS -> for this scan you will get the reply. Else you will not get the reply for this scan.
Nmap Fragementation Scan	nmap target_IP -f -vv -p 21,22,23		Firewall Bypassing	By using this scan we can fragement the size of the packet, Basically default TCP packet size is 16 bytes. But by using this scan we can reduce the fragment size of the of the packet to bypass the firewalls. This can be works on only on the old firewalls

Note:

Red Box indicates the firewall Bypassing Scripts

Blue Box indicates the service based enumeration and attack based scripts

Green Box indicates the vulnerability Scanning related scripts.