|  |  |
| --- | --- |
| **Target Specification** |  |
| **Example** | **Description** |
| nmap 192.168.1.1 | Scan a single IP |
| nmap 192.168.1.1 192.168.1.2 | Scan specific IPs |
| nmap 192.168.1.1-254 | Scan a range IP |
| nmap sc.nmap.org | Scan domaain |
| nmap –iL target.txt | Scan targets from a file |
| nmap –iR 100 | Scan random 100 hosts |
| nmap –exclude 192.168.1.1 | Exclude listed hosts |
| **Nmap Scan Techniques** |  |
| nmap –sS 192.168.1.1 | TCP SYN port scan (Default) |
| nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| nmap 192.168.1.1 -sU | UDP port scan |
| nmap 192.168.1.1 -sW | TCP Window port scan |
| nmap 192.168.1.1 -sA | TCP ACK port scan |
| nmap 192.168.1.1 -sM | TCP Maimon port scan |
| Host Discovery |  |
| nmap 192.168.1.1-3 -sL | No Scan. List targets only |
| nmap 192.168.1.1/24 -sn | Disable port scanning. Host discovery only. |
| nmap 192.168.1.1-5 -Pn | Disable host discovery. Port scan only. |
| nmap 192.168.1.1-5 -PS22-25,80 | TCP SYN discovery on port x.Port 80 by default |
| nmap 192.168.1.1-5 -PA22-25,80 | TCP ACK discovery on port x.Port 80 by default |
| nmap 192.168.1.1-5 -PU53 | UDP discovery on port x.Port 40125 by default |
| nmap 192.168.1.1-1/24 -PR | ARP discovery on local network |
| nmap 192.168.1.1 -n | Never do DNS resolution |
| Port Specification |  |
| nmap 192.168.1.1 -p 21  nmap 192.168.1.1 -p 21-100  nmap 192.168.1.1 -p U:53,T:21-25,80  nmap 192.168.1.1 -p-  nmap 192.168.1.1 -p http,https | Port scan for port x  Port scan multiple TCP and UDP ports  nmap 192.168.1.1 -p-  Port scan from service name |
| nmap 192.168.1.1 -F | Fast port scan (100 ports) |
| nmap 192.168.1.1 -top-ports 2000 | Port scan the top x ports |
| nmap 192.168.1.1 -p-65535 | Leaving off initial port in range makes the scan start at port 1 |
| nmap 192.168.1.1 -p0- | Leaving off end port in rangemakes the scan go through to port 65535 |
| **Service and Version Detection** |  |
| nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |
| nmap 192.168.1.1 -sV -version-intensity 8 | Intensity level 0 to 9. Higher number increases possibility of correctness |
| nmap 192.168.1.1 -sV -version-light | Enable light mode. Lower possibility of correctness. Faster |
| nmap 192.168.1.1 -sV -version-all | Enable intensity level 9. Higher possibility of correctness. Slower |
| nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |
| **Timing and Performance** |  |
| nmap 192.168.1.1 -T0 | Paranoid (0) Intrusion Detection System evasion |
| Paranoid (0) Intrusion Detection System evasion | Sneaky (1) Intrusion Detection System evasion |
| nmap 192.168.1.1 -T2 | Polite (2) slows down the scan to use less bandwidth and use less target machine resources |
| nmap 192.168.1.1 -T3 | Normal (3) which is default speed |
| nmap 192.168.1.1 -T4 | Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network |
| nmap 192.168.1.1 -T5 | Insane (5) speeds scan; assumes you are on an extraordinarily fast network |
| **NSE Scripts** |  |
| nmap 192.168.1.1 -sC | Scan with default NSE scripts. Considered useful for discovery and safe |
| nmap 192.168.1.1 -script default | Scan with default NSE scripts. Considered useful for discovery and safe |
| nmap 192.168.1.1 -script=banner | Scan with a single script. Example banner |
| nmap 192.168.1.1 -script=http\* | Scan with a wildcard. Example http |
| nmap 192.168.1.1 -script=http,banner | Scan with two scripts. Example http and banner |
| nmap 192.168.1.1 -script "not intrusive" | Scan default, but remove intrusive scripts |
| nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.1 | NSE script with arguments |
| **Use NSE Script Examples** |  |
| nmap -Pn -script=http-sitemap-generator scanme.nmap.org | http site map generator |
| nmap -n -Pn -p 80 -open -sV -vvv -script banner,http-title -iR 1000 | Fast search for random web servers |
| nmap -Pn -script=dns-brute domain.com | Brute forces DNS hostnames guessing subdomains |
| 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 | Safe SMB scripts to run |
| nmap -script whois\* domain.com | Whois query |
| nmap -p80 -script http-unsafe-output-escaping scanme.nmap.org | Detect cross site scripting vulnerabilities |
| nmap -p80 -script http-sql-injection scanme.nmap.org | Check for SQL injections |
| **Firewall /IDS Evasion and Spoofing** |  |
| nmap 192.168.1.1 -f | Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters |
| nmap 192.168.1.1 -mtu 32 | Set your own offset size |
| nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1 | Send scans from spoofed IPs |
| nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip | Above example explained |
| nmap -S www.microsoft.com www.facebook.com | Scan Facebook from Microsoft (-e eth0 -Pn may be required) |
| nmap -g 53 192.168.1.1 | Use given source port number |
| nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1 | Relay connections through HTTP/SOCKS4 proxies |
| nmap -data-length 200 192.168.1.1 | Appends random data to sent packets |
| nmap 192.168.1.1 -oN normal.file | Normal output to the file normal.file |
| nmap 192.168.1.1 -oX xml.file | XML output to the file xml.file |
| nmap 192.168.1.1 -oG grep.file | Grepable output to the file grep.file |
| nmap 192.168.1.1 -oN file.file -append-output | Append a scan to a previous scan file |
| nmap 192.168.1.1 -v | Increase the verbosity level (use -vv or more for greater effect) |
| nmap 192.168.1.1 -d | Increase debugging level (use -dd or more for greater effect) |
| nmap 192.168.1.1 -reason | Display the reason a port is in a particular state, same output as -vv |
| nmap 192.168.1.1 -open | Only show open (or possibly open) ports |
| nmap 192.168.1.1 -T4 -packet-trace | Show all packets sent and received |
| nmap -iflist | Shows the host interfaces and routes |
| nmap -resume results.file | Resume a scan |