NMAP CHEATSHEET

Nmap Target Selection

|  |  |
| --- | --- |
| Scan a single IP | nmap 192.168.1.1 |
| Scan a host | nmap www.testhostname.com |
| Scan a range of IPs | nmap 192.168.1.1-20 |
| Scan a subnet | nmap 192.168.1.0/24 |
| Scan targets from a text file | nmap -iL list-of-ips.txt |

These are all default scans, which will scan 1000 TCP ports. Host discovery will take place.

Nmap Port Selection

|  |  |
| --- | --- |
| Scan a single Port | nmap -p 22 192.168.1.1 |
| Scan a range of ports | nmap -p 1-100 192.168.1.1 |
| Scan 100 most common ports (Fast) | nmap -F 192.168.1.1 |
| Scan all 65535 ports | nmap -p- 192.168.1.1 |

Nmap Port Scan types

|  |  |
| --- | --- |
| Scan using TCP connect | nmap -sT 192.168.1.1 |
| Scan using TCP SYN scan (default) | nmap -sS 192.168.1.1 |
| Scan UDP ports | nmap -sU -p 123,161,162 192.168.1.1 |
| Scan selected ports - ignore discovery | nmap -Pn -F 192.168.1.1 |

Privileged access is required to perform the default SYN scans. If privileges are insufficient a TCP connect scan will be used. A TCP connect requires a full TCP connection to be established and therefore is a slower scan. Ignoring discovery is often required as many firewalls or hosts will not respond to PING, so could be missed unless you select the -Pn parameter. Of course this can make scan times much longer as you could end up sending scan probes to hosts that are not there.

Take a look at the [Nmap Tutorial](https://hackertarget.com/nmap-tutorial/) for a detailed look at the scan process.

Service and OS Detection

|  |  |
| --- | --- |
| Detect OS and Services | nmap -A 192.168.1.1 |
| Standard service detection | nmap -sV 192.168.1.1 |
| More aggressive Service Detection | nmap -sV --version-intensity 5 192.168.1.1 |
| Lighter banner grabbing detection | nmap -sV --version-intensity 0 192.168.1.1 |

Service and OS detection rely on different methods to determine the operating system or service running on a particular port. The more aggressive service detection is often helpful if there are services running on unusual ports. On the other hand the lighter version of the service will be much faster as it does not really attempt to detect the service simply grabbing the banner of the open service.

Nmap Output Formats

|  |  |
| --- | --- |
| Save default output to file | nmap -oN outputfile.txt 192.168.1.1 |
| Save results as XML | nmap -oX outputfile.xml 192.168.1.1 |
| Save results in a format for grep | nmap -oG outputfile.txt 192.168.1.1 |
| Save in all formats | nmap -oA outputfile 192.168.1.1 |

The default format could also be saved to a file using a simple file redirect command > file. Using the -oN option allows the results to be saved but also can be monitored in the terminal as the scan is under way.

Digging deeper with NSE Scripts

|  |  |
| --- | --- |
| Scan using default safe scripts | nmap -sV -sC 192.168.1.1 |
| Get help for a script | nmap --script-help=ssl-heartbleed |
| Scan using a specific NSE script | nmap -sV -p 443 –script=ssl-heartbleed.nse 192.168.1.1 |
| Scan with a set of scripts | nmap -sV --script=smb\* 192.168.1.1 |

According to my Nmap install there are currently **471 NSE scripts**. The scripts are able to perform a wide range of security related testing and discovery functions. If you are serious about your network scanning you really should take the time to get familiar with some of them.

The option --script-help=$scriptname will display help for the individual scripts. To get an easy list of the installed scripts trylocate nse | grep script.

You will notice I have used the -sV service detection parameter. Generally most NSE scripts will be more effective and you will get better coverage by including service detection.

A scan to search for DDOS reflection UDP services

|  |  |
| --- | --- |
| Scan for UDP DDOS reflectors | nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr 192.168.1.0/24 |

UDP based DDOS reflection attacks are a common problem that network defenders come up against. This is a handy Nmap command that will scan a target list for systems with open UDP services that allow these attacks to take place. Full details of the command and the background can be found on the [Sans Institute Blog](https://isc.sans.edu/diary/Using+nmap+to+scan+for+DDOS+reflectors/18193) where it was first posted.

HTTP Service Information

|  |  |
| --- | --- |
| Gather page titles from HTTP services | nmap --script=http-title 192.168.1.0/24 |
| Get HTTP headers of web services | nmap --script=http-headers 192.168.1.0/24 |
| Find web apps from known paths | nmap --script=http-enum 192.168.1.0/24 |

There are many HTTP information gathering scripts, here are a few that are simple but helpful when examining larger networks. Helps in quickly identifying what the HTTP service is that is running on the open port. Note the http-enum script is particularly noisy. It is similar to [Nikto](https://hackertarget.com/nikto-website-scanner/) in that it will attempt to enumerate known paths of web applications and scripts. This will inevitably generated hundreds of404 HTTP responses in the web server error and access logs.

Detect Heartbleed SSL Vulnerability

|  |  |
| --- | --- |
| Heartbleed Testing | nmap -sV -p 443 --script=ssl-heartbleed 192.168.1.0/24 |

Heartbleed detection is one of the available SSL scripts. It will detect the presence of the well known Heartbleed vulnerability in SSL services. Specify alternative ports to test SSL on mail and other protocols *(Requires Nmap 6.46)*.

IP Address information

|  |  |
| --- | --- |
| Find Information about IP address | nmap --script=asn-query,whois,ip-geolocation-maxmind 192.168.1.0/24 |

Gather information related to the IP address and netblock owner of the IP address. Uses ASN, whois and geoip location lookups. See the [IP Tools](https://hackertarget.com/ip-tools/) for more information and similar IP address and DNS lookups.