Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 4: Other options applicable to all scans

https://nmap.org/

GENERAL USAGE

```
nmap [Scan Type(s)] [Options] {target specification}
```

NOTES

These options work with with most of the Reconaissance, Enumeration and Exploiting techniques of the other Cheatsheets and affects various aspects of the operations

Firewall / IDS evasion and Spoofing are useful to try to bypass certain network protections

Output formats change the data nmap shows to try to adapt it to different applications or result viewers

Misc options allow to use nmap in multiple contexts, for example networks with IPv6 addresses, or the special -A switch that enables a lot of options at the same time

Timing and performance are options to control scan speeds, so scan operations can finish faster (at the cost of potential less accuracy)

Script scan options list options to show each script help, update the script database (if we introduce a new custom one) and a description of the default scripts that are run when we use the -sV option in any nmap scan

FIREWALL/IDS EVASION AND SPOOFING TECHNIQUES (https://nmap.org/book/man-bypass-firewalls-ids.html)

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

--data <hex string>: Append a custom payload to sent packets

--data-length <num>: Append random data to sent packets

--data-string <string>: Append a custom ASCII string to sent packets

-e <iface>: Use specified interface

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-g/--source-port <portnum>: Use given port number

--ip-options <options>: Send packets with specified ip options

--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies

-S <IP_Address>: Spoof source address

--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--ttl <val>: Set IP time-to-live field

OUTPUT FORMATS (https://nmap.org/book/man-output.html)

--append-output: Append to rather than clobber specified output files

-d: Increase debugging level (use -dd or more for greater effect)

--iflist: Print host interfaces and routes (for debugging)

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

-oA <basename>: Output in the three major formats at once

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.

--open: Only show open (or possibly open) ports

--packet-trace: Show all packets sent and received

--reason: Display the reason a port is in a particular state

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

-v: Increase verbosity level (use -vv or more for greater effect)

--webxml: Reference stylesheet from Nmap.Org for more portable XML

MISC (https://nmap.org/book/man-misc-options.html)

SCRIPT SCANS (https://nmap.org/book/man-nse.html)

--script-updatedb: Update the script database.

--script-help=<NSE scripts>: Show help about scripts. <NSE scripts> is a comma-separated list of script-files or script-categories.

Additional useful script cathegories

default: These scripts are the default set and are run when using the -sC or -A options rather than listing scripts with --script. This category can also be specified explicitly like any other using --script=default. Many factors are considered in deciding whether a script should be run by default:

Speed: A default scan must finish quickly, which excludes brute force authentication crackers, web spiders, and any other scripts which can take minutes or hours to scan a single service.

Usefulness: Default scans need to produce valuable and actionable information. If even the script author has trouble explaining why an average networking or security professional would find the output valuable, the script should not run by default.

Verbosity: Nmap output is used for a wide variety of purposes and needs to be readable and concise. A script which frequently produces pages full of output should not be added to the default category. When there is no important information to report, NSE scripts (particularly default ones) should return nothing. Checking for an obscure vulnerability may be OK by default as long as it only produces output when that vulnerability is discovered.

Reliability: Many scripts use heuristics and fuzzy signature matching to reach conclusions about the target host or service. Examples include sniffer-detect and sql-injection. If the script is often wrong, it doesn't belong in the default category where it may confuse or mislead casual users. Users who specify a script or category directly are generally more advanced and likely know how the script works or at least where to find its documentation.

Intrusiveness: Some scripts are very intrusive because they use significant resources on the remote system, are likely to crash the system or service, or are likely to be perceived as an

-6: Enable IPv6 scanning

-A: Enable OS detection, version detection, script scanning, and traceroute

--datadir <dirname>: Specify custom Nmap data file location

-h: Print this help summary page.

--privileged: Assume that the user is fully privileged

--send-eth/--send-ip: Send using raw ethernet frames or IP packets

--unprivileged: Assume the user lacks raw socket privileges

-V: Print version number

TIMING AND PERFORMANCE (https://nmap.org/book/man-performance.html)

Options which take <time> are in seconds, or append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

--host-timeout <time>: Give up on target after this long

--max-rate <number>: Send packets no faster than <number> per second

--max-retries <tries>: Caps number of port scan probe retransmissions.

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <numprobes>: Probe parallelization

--min-rate <number>: Send packets no slower than <number> per second

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies probe round trip time.

--scan-delay/--max-scan-delay <time>: Adjust delay between probes

-T<0-5>: Set timing template (higher is faster)

EXAMPLES

```
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
```

SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

by José Manuel Redondo López

attack by the remote administrators. The more intrusive a script is, the less suitable it is for the default category. Default scripts are almost always in the safe category too, though we occasionally allow intrusive scripts by default when they are only mildly intrusive and score well in the other factors.

Privacy: Some scripts, particularly those in the external category described later, divulge information to third parties by their very nature. For example, the whois script must divulge the target IP address to regional whois registries. We have also considered (and decided against) adding scripts which check target SSH and SSL key fingerprints against Internet weak key databases. The more privacy-invasive a script is, the less suitable it is for default category inclusion.

We don't have exact thresholds for each of these criteria, and many of them are subjective. All of these factors are considered together when making a decision whether to promote a script into the default category. A few default scripts are identd-owners (determines the username running remote services using identd), http-auth (obtains authentication scheme and realm of web sites requiring authentication), and ftp-anon (tests whether an FTP server allows anonymous access).

https://nmap.org/nsedoc/categories/default.html

intrusive: These are scripts that cannot be classified in the safe category because the risks are too high that they will crash the target system, use up significant resources on the target host (such as bandwidth or CPU time), or otherwise be perceived as malicious by the target's system administrators. Examples are http-open-proxy (which attempts to use the target server as an HTTP proxy) and snmp-brute (which tries to guess a device's SNMP community string by sending common values such as public, private, and cisco). Unless a script is in the special version category, it should be categorized as either safe or intrusive.

https://nmap.org/nsedoc/categories/intrusive.html

https://nmap.org/nsedoc/categories/intrusive.html

safe: Scripts which weren't designed to crash services, use large amounts of network bandwidth or other resources, or exploit security holes are categorized as safe. These are less likely to offend remote administrators, though (as with all other Nmap features) we cannot guarantee that they won't ever cause adverse reactions. Most of these perform general network discovery. Examples are ssh-hostkey (retrieves an SSH host key) and html-title (grabs the title from a web page). Scripts in the version category are not categorized by safety, but any other scripts which aren't in safe should be placed in intrusive.

https://nmap.org/nsedoc/categories/safe.html