Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 2: Enumeration

https://nmap.org/

GENERAL USAGE

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

NOTES

Scan techniques makes sense whan there is a firewall or similar solution preventing some types of scan (experimenting options may offer more information)

Increase service/version/OS detection "aggressiveness" if default methods do not return any useful result

TARGET SPECIFICATION

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

SERVICE/VERSION DETECTION

-sV: Probe open ports to determine service/version info (see Other Options cheatsheet for a detailed explanation, typical fist option to try)

--version-all: Try every single probe (intensity 9)

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-trace: Show detailed version scan activity (for debugging)

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

-sC: equivalent to --script=default

--script=<NSE scripts>: <NSE scripts> is a comma separated list of **directories, script-files or script-categories**

--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts (see each script documentation to consult argument names, number, and valid value types)

--script-args-file=filename: provide NSE script args in a file

--script-trace: Show all data sent and received

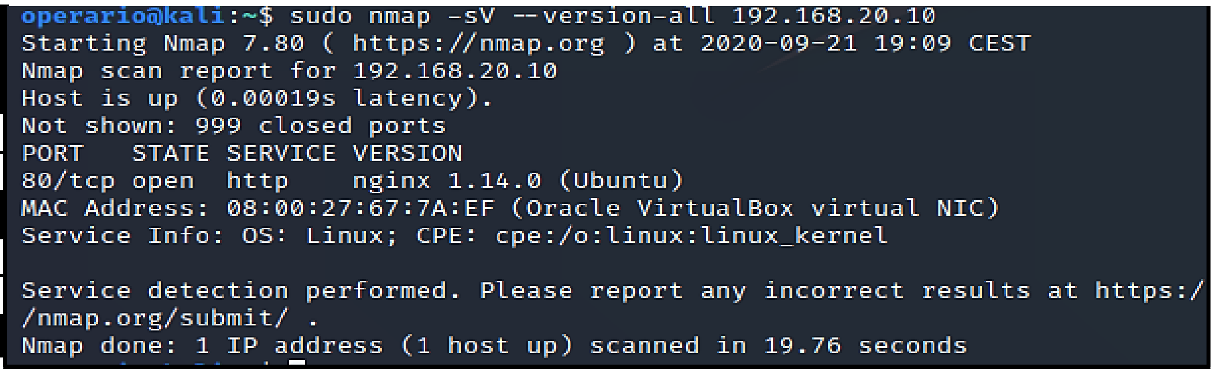
RECOMMENDED SCRIPT CATEGORIES FOR ENUMERATION (https://nmap.org/nsedoc/)

discovery: These scripts try to actively discover more about the network by querying public registries, SNMP-enabled devices, directory services, and the like. Examples include html-title (obtains the title of the root path of web sites), smb-enum-shares (enumerates Windows shares), and snmp-sysdescr (extracts system details via SNMP). See:

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

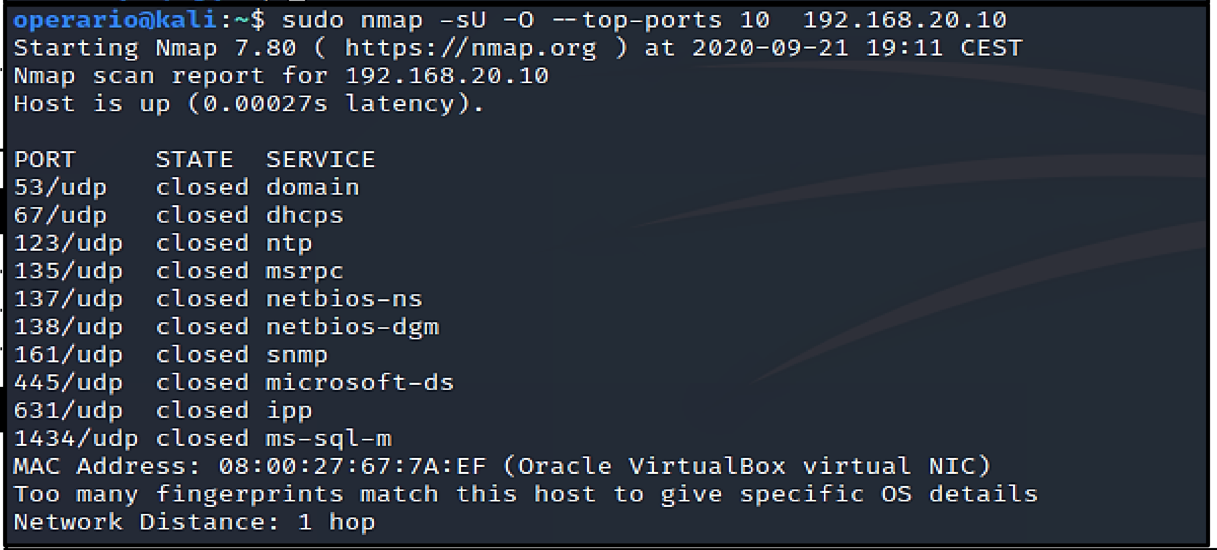
external: Scripts in this category may send data to a third-party database or other network resource. An example of this is whois-ip, which makes a connection to whois servers to learn about the address of the target. There is always the possibility that operators of the third-party database will record anything you send to them, which in many cases will include your IP address and the address of the target. Most scripts involve traffic strictly between the scanning computer and the client; any that do not are placed in this category. Services include IP Geolocalization, Shodan, SMTP, DNS, Whois...very useful for enumeration. See:

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



```
operario@kali:~$ sudo nmap -sV --version-all 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 19:09 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.76 seconds
```



```
operario@kali:~$ sudo nmap -sU -O --top-ports 10  192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 19:11 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00027s latency).

PORT     STATE  SERVICE
53/udp   closed domain
67/udp   closed dhcps
123/udp  closed ntp
135/udp  closed msrpc
137/udp  closed netbios-ns
138/udp  closed netbios-dgm
161/udp  closed snmp
445/udp  closed microsoft-ds
631/udp  closed ipp
1434/udp closed ms-sql-m
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

SCAN TECHNIQUES (WAYS TO CHECK PORTS AND RUNNING SERVICES)

-b <FTP relay host>: FTP bounce scan

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idle scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans

-sO: IP protocol scan

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sY/sZ: SCTP INIT/COOKIE-ECHO scans

PORT SPECIFICATION AND SCAN ORDER

--exclude-ports <port ranges>: Exclude the specified ports from scanning

-F: Fast mode - Scan fewer ports than the default scan

-p <port ranges>: Only scan specified ports. Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9

--port-ratio <ratio>: Scan ports more common than <ratio>

-r: Scan ports consecutively - don't randomize

--top-ports <number>: Scan <number> most common ports

OS DETECTION

-O: Enable OS detection

--osscan-guess: Guess OS more aggressively

--osscan-limit: Limit OS detection to promising targets

EXAMPLES

```
sudo nmap -sV --version-all 192.168.20.10
nmap -sS -A -sV -O -p - 192.168.20.10
```

version: The scripts in this special category are an extension to the version detection feature and cannot be selected explicitly. They are selected to run only if version detection (-sV) was requested. Their output cannot be distinguished from version detection output and they do not produce service or host script results. Examples are skypev2-version, pptp-version, and iax2-version. https://nmap.org/nsedoc/categories/version.html	*nmap -sS -A -sV -O -p - 192.168.20.10* *sudo nmap -sU -O --top-ports 10 192.168.20.10* *sudo nmap -p1-100 -sS 192.168.20.10* *sudo nmap -p-100 --script=banner 192.168.20.10* *sudo nmap --script=ip-geolocation-geoplugin www.ingenieriainformatica.uniovi.es* *sudo nmap --script=http-server-header www.ingenieriainformatica.uniovi.es*

by José Manuel Redondo López