Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 3: Exploiting

https://nmap.org/

GENERAL USAGE

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

NOTES

Using NSE scripts is mandatory to achieve proper exploiting capabilities. Choose wisely the type of exploiting technique you are going to use against the machine depending on what you want to achieve and the results of the Enumeration process (services located, available, versions...)

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

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

```
root@kali:~# nmap --script ftp-anon -p 21 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 15:46 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
root@kali:~#
```

```
root@kali:~# nmap --script smb-enum-shares -p445 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-03 15:49 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00074s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.14.2\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (server1804 server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.14.2\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
```

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

auth: These scripts deal with authentication credentials (or bypassing them) on the target system. Examples include x11-access, ftp-anon, and oracle-enum-users. Scripts which use brute force attacks to determine credentials are placed in the brute category instead.

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

brute: These scripts use brute force attacks to guess authentication credentials of a remote server. Nmap contains scripts for brute forcing dozens of protocols, including http-brute, oracle-brute, snmp-brute, etc.

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

dos: Scripts in this category may cause a denial of service. Sometimes this is done to test vulnerability to a denial of service method, but more commonly it is an undesired by necessary side effect of testing for a traditional vulnerability. These tests sometimes crash vulnerable services.

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

exploit: These scripts aim to actively exploit some vulnerability. Examples include jdwp-exec and http-shellshock.

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

fuzzer: This category contains scripts which are designed to send server software unexpected or randomized fields in each packet. While this technique can useful for finding undiscovered bugs and vulnerabilities in software, it is both a slow process and bandwidth intensive. An example of a script in this category is dns-fuzz, which bombards a DNS server with slightly flawed domain requests until either the server crashes or a user specified time limit elapses.

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

malware: These scripts test whether the target platform is infected by malware or backdoors. Examples include smtp-strangeport, which watches for SMTP servers running on unusual port numbers, and auth-spoof, which detects identd spoofing daemons which provide a fake answer before even receiving a query. Both of these behaviors are commonly associated with malware infections.

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

EXAMPLES

```
sudo nmap --script ftp-anon -p 21 192.168.20.10
sudo nmap --stript smb-enumshares -p445 192.168.20.10
sudo nmap --script ftp-brute -p 21 192.168.20.10
sudo nmap --script telnet-brute --script-args
userdb=users.lst,passdb=/usr/share/wordlists/nmap.lst 192.168.20.10
sudo nmap -sV --script=http-malware-host 192.168.20.10
nmap -sU --script dns-fuzz --script-args timelimit=2h 192.168.20.10
nmap -p80 --script http-csrf 192.168.20.10
```

```
|      Path: C:\var\lib\samba\printers
|      Anonymous access: <none>
|_     Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

```
sudo nmap -sU -sS --script smb-flood -p U:137,T:139 192.168.20.10
```

by José Manuel Redondo López