26-3-21

Nmap

Nmap:

$ man nmap

↳ Scan the host, Find port status and services running on it

↳ Fingerprinting host/network.

Scan types:

When port scanning with Nmap, there are three basic scan types. These are:

TCP Connect Scans (-sT)
SYN "Half-open" Scans (-sS)
UDP Scans (-sU)
Additionally there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

TCP Null Scans (-sN)
TCP FIN Scans (-sF)
TCP Xmas Scans (-sX)

For more info refer THM nmap room on TCP, SYN, UDP scan types. https://www.tryhackme.com/room/furthernmap

NMAP Scripting engine : (NSE)

↳ different category of scripts available in NSE

↳ --script = <script category/script name>

, is used to run multiple scripts

↳ eg:) --script = ftp-anon → this script run on given target.

↳ --script-args = script name. arg1

some script requires additional arguments

, is used to run multiple scripts

↳ --script-help = script name

gets detail of the particular script

eg:)

```
nmap 192.168.0.1 -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'
```

Searching for Scripts :

↳ Stored in /usr/share/nmap/scripts

↳ There is a db stored we can search scripts using it.

/usr/share/nmap/scripts/script.db

↳ We can also grep the scripts which we looking for

grep "ftp" /usr/share/nmap/scripts/script.db

ls -l /usr/share/nmap/scripts/*ftp*

↳ We can also download NSE scripts from nmap offical site then put it under /usr/share/nmap/scripts

↳ Then run nmap --script-updatedb to update db.

Firewall evasion Technique :

- Pn switch treats the host is up & doesn't send ICMP packets, which is filtered by some IDS

-f :- Used to fragment the packets (i.e. split them into smaller pieces) making it less likely that the packets will be detected by a firewall or IDS. An alternative to -f, but providing more control over the size of the packets: --mtu <number>, accepts a maximum transmission unit size to use for the packets sent. This must be a multiple of 8.

--scan-delay <time in ms> :- used to add a delay between packets sent. This is very useful if the network is unstable, but also for evading any time-based firewall/IDS triggers which may be in place.

--badsum :- this is used to generate in invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a fire /IDS.