Learning Metaslpoit 2

Yesterday I learnt how to scan the ssh port and learn / gather information about the target IP address. Today I will be looking into gathering the open ports of the target IP address.

use auxiliary/scanner/portscan/tcp

here we will be scanning the tcp ports of the target IP address for open ports

if we look at the options we will see that the host or the target IP is not set.

```
msf6 auxiliary(scanner/ssh/ssh_version) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per hos
   DELAY        0                yes       The delay between connections, per thread, in m
   JITTER       0                yes       The delay jitter factor (maximum value by which
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://docs.metasploit
   THREADS      1                yes       The number of concurrent threads (max one per h
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


View the full module info with the info, or info -d command.
```

So we set the host or the target IP address by the command ***set RHOSTS IP_address***

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.71.131
RHOSTS ⇒ 192.168.71.131
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 100
THREADS ⇒ 100
```

Then when we use the command ***run*** we will get all the tcp open ports in that target machine.

```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.71.131:       - 192.168.71.131:25 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:21 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:22 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:23 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:53 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:80 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:111 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:139 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:445 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:513 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:514 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:512 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:1099 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:1524 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:2049 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:2121 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:3306 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:3632 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:5432 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:5900 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:6000 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:6667 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:6697 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:8009 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:8180 - TCP OPEN
[+] 192.168.71.131:       - 192.168.71.131:8787 - TCP OPEN
[*] 192.168.71.131:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

If we use the command

use auxiliary/scanner/portscan/syn

this performs a SYN scan on the target which is much more stealthier.

Use auxiliary/scanner/portscan/ack

This command is used to perform ack scan to map out firewall rules and determine which ports are filtered.