

Scanning With Metasploit

Start up metasploit by using the `msfconsole` command, and use the `search portscan` command as shown below to search for port scanning modules:

```

root@kali:~# msfconsole
# cowsay++
< metasploit >

      \
      \ (oo)_____)
        (_____) \
          ||----|| *

      =[ metasploit v5.0.101-dev ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Use the resource command to run commands from a file

msf5 > search portscan

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/http/wordpress_pingback_access                  normal        No    Wordpress Pingback Locator
1  auxiliary/scanner/natpmp/natpmp_portscan                          normal        No    NAT-PMP External Port Scanner
2  auxiliary/scanner/portscan/ack                                    normal        No    TCP ACK Firewall Scanner
3  auxiliary/scanner/portscan/ftpbounce                             normal        No    FTP Bounce Port Scanner
4  auxiliary/scanner/portscan/syn                                    normal        No    TCP SYN Port Scanner
5  auxiliary/scanner/portscan/tcp                                   normal        No    TCP Port Scanner
6  auxiliary/scanner/portscan/xmas                                  normal        No    TCP "XMas" Port Scanner
7  auxiliary/scanner/sap/sap_router_portscanner                     normal        No    SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf5 >

```

We'll use the `syn` module by entering this command `use 4` or `use auxiliary/scanner/portscan/syn`. Next, we will use the `options` command to view the available options. In this case we will only set the `rhosts` (target IP address) using the `set rhosts <IP_address>` command. We can also increase the port range by using the `set ports 1-65535` command. Finally, we will use the `run` command to start the scan as shown below:

```

msf5 > use 4
msf5 auxiliary(scanner/portscan/syn) > options

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



| Name      | Current Setting | Required | Description                                                                        |
|-----------|-----------------|----------|------------------------------------------------------------------------------------|
| BATCHSIZE | 256             | yes      | The number of hosts to scan per set                                                |
| DELAY     | 0               | yes      | The delay between connections, per thread, in milliseconds                         |
| INTERFACE |                 | no       | The name of the interface                                                          |
| JITTER    | 0               | yes      | The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.     |
| PORTS     | 1-10000         | yes      | Ports to scan (e.g. 22-25,80,110-900)                                              |
| RHOSTS    |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| SNAPLEN   | 65535           | yes      | The number of bytes to capture                                                     |
| THREADS   | 1               | yes      | The number of concurrent threads (max one per host)                                |
| TIMEOUT   | 500             | yes      | The reply read timeout in milliseconds                                             |



msf5 auxiliary(scanner/portscan/syn) > set rhosts 192.168.229.133
rhosts => 192.168.229.133
msf5 auxiliary(scanner/portscan/syn) > set ports 1-65535
ports => 1-65535
msf5 auxiliary(scanner/portscan/syn) > run

[+] TCP OPEN 192.168.229.133:22
[+] TCP OPEN 192.168.229.133:80
[+] TCP OPEN 192.168.229.133:111
[+] TCP OPEN 192.168.229.133:139
[+] TCP OPEN 192.168.229.133:443

```

We could also increase the scanning speed by using the `set threads <number>` command.
