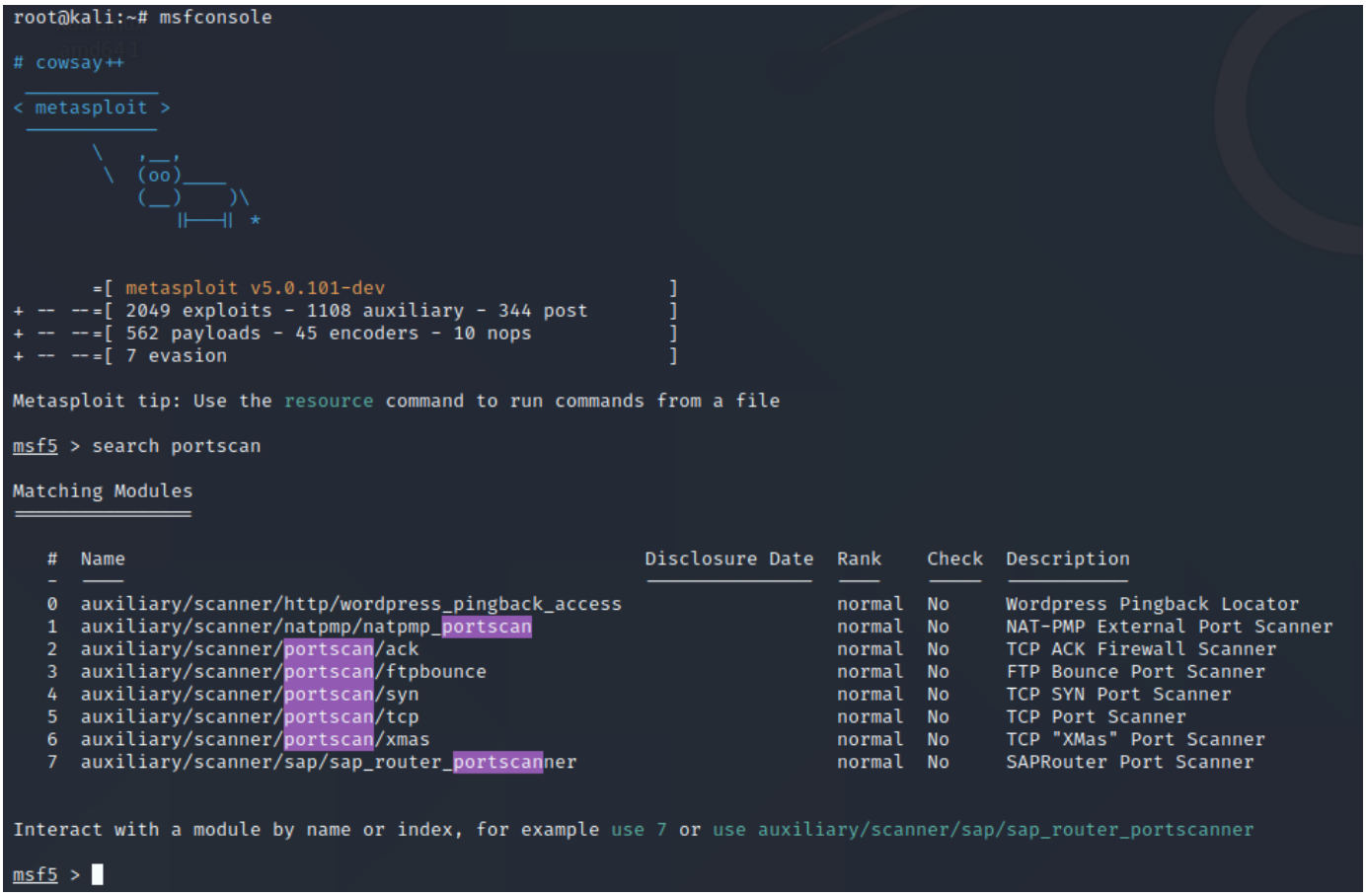
Scanning With Metasploit

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



We'll use the `syn` module by entering this command `use 4` or `use auxiliary/scaner/portscan/syn`. Next, we will use the `options` command to view the available options. In this casee 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.