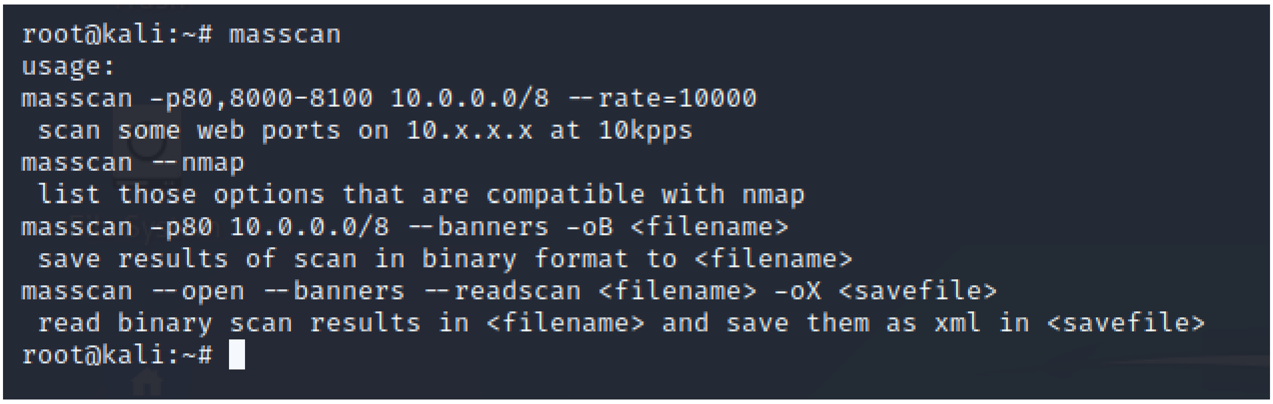
Scanning with Masscan

Masscan is a very fast port scanner.

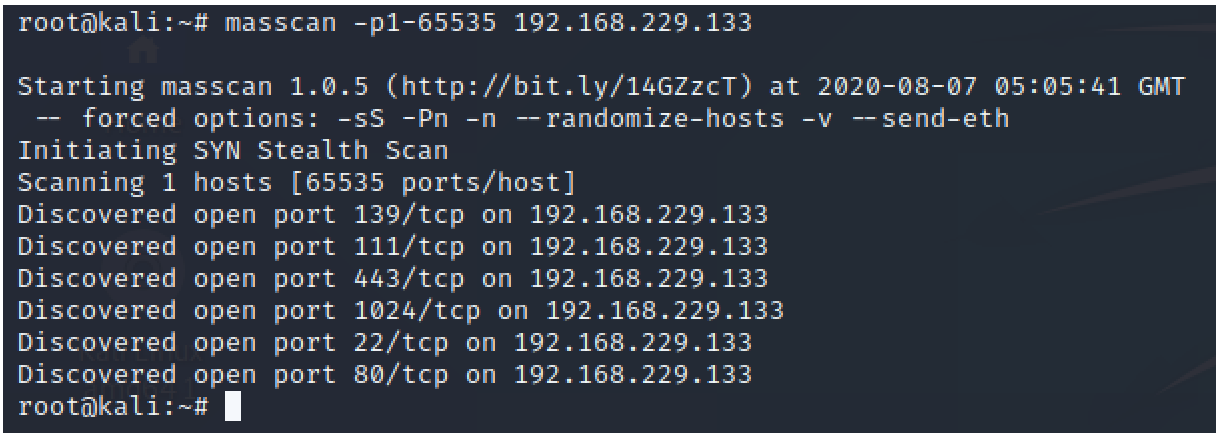
Fun fact: you can use this tool to scan a wide range of IP addresses

The following is a sample:



```
root@kali:~# masscan
usage:
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000
 scan some web ports on 10.x.x.x at 10kpps
masscan --nmap
 list those options that are compatible with nmap
masscan -p80 10.0.0.0/8 --banners -oB <filename>
 save results of scan in binary format to <filename>
masscan --open --banners --readscan <filename> -oX <savefile>
 read binary scan results in <filename> and save them as xml in <savefile>
root@kali:~# 
```

The following is a sample scan using this command `masscan -p1-65535 <IP_address>`:

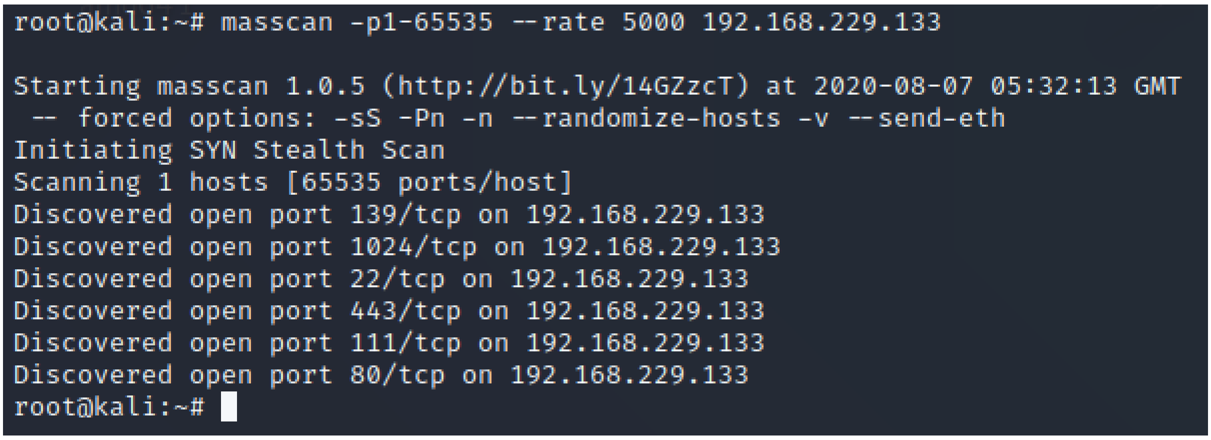


```
root@kali:~# masscan -p1-65535 192.168.229.133

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-08-07 05:05:41 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 139/tcp on 192.168.229.133
Discovered open port 111/tcp on 192.168.229.133
Discovered open port 443/tcp on 192.168.229.133
Discovered open port 1024/tcp on 192.168.229.133
Discovered open port 22/tcp on 192.168.229.133
Discovered open port 80/tcp on 192.168.229.133
root@kali:~# 
```

- `-p` is the port flag. Therefore `-p1-65535` refers to ports 1 to 65535.
- `-sS` is the Stealth scan flag
- `-Pn` makes the tool treat all ports like they are alive (active)

If we want to increase the scan speed, we can use the `--rate` flag as shown below:



```
root@kali:~# masscan -p1-65535 --rate 5000 192.168.229.133

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-08-07 05:32:13 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 139/tcp on 192.168.229.133
Discovered open port 1024/tcp on 192.168.229.133
Discovered open port 22/tcp on 192.168.229.133
Discovered open port 443/tcp on 192.168.229.133
Discovered open port 111/tcp on 192.168.229.133
Discovered open port 80/tcp on 192.168.229.133
root@kali:~# 
```
