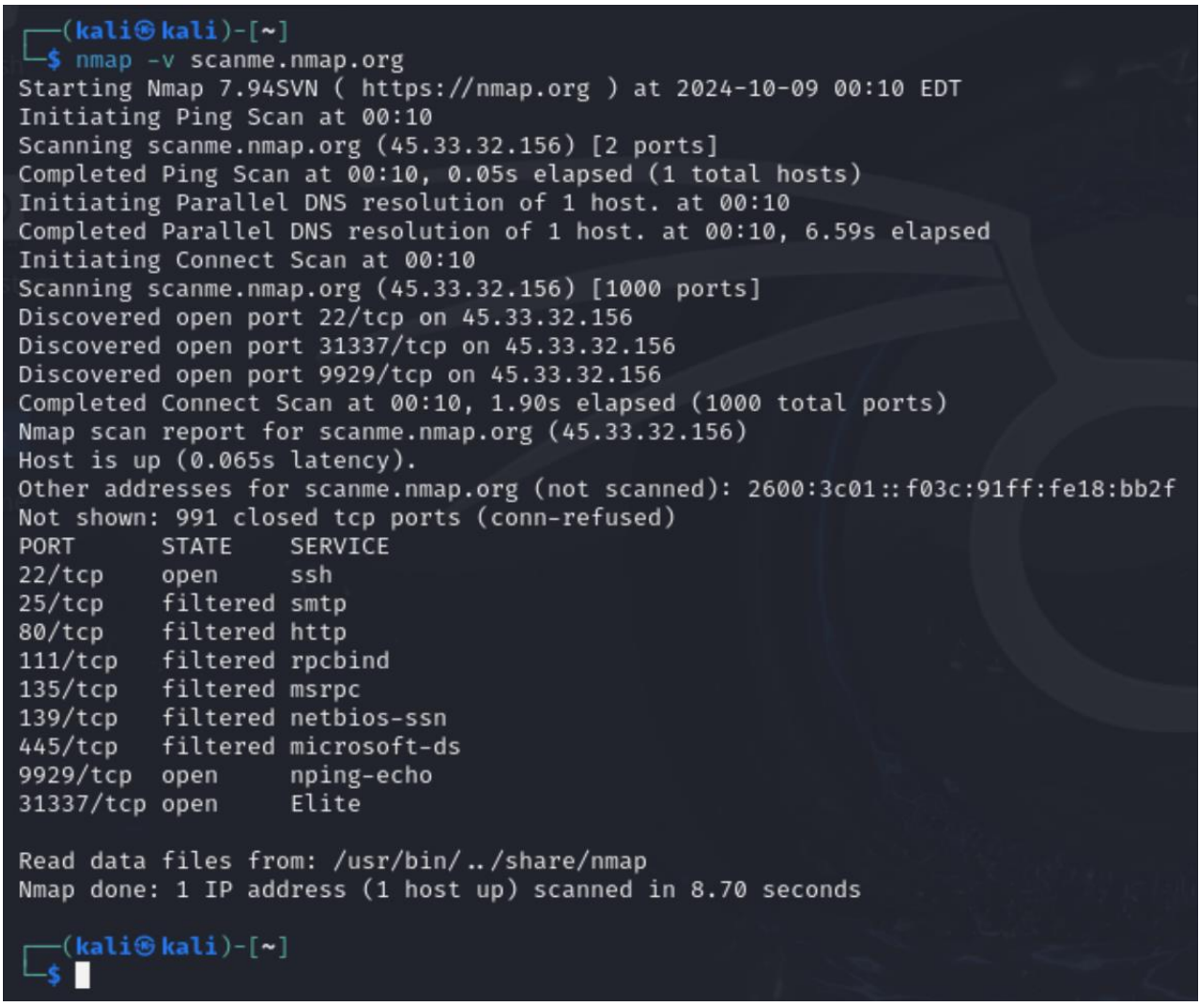
Karrington Hall
9 October 2024
COMP 2313 P01

nmap Lab

nmap -v scanme.nmap.org

- This option scans all reserved TCP ports on the machine scanme.nmap.org . The -v option enables verbose mode.



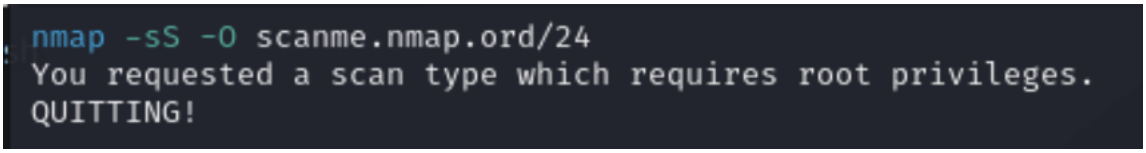
```
┌──(kali㉿kali)-[~]
└─$ nmap -v scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 00:10 EDT
Initiating Ping Scan at 00:10
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 00:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:10
Completed Parallel DNS resolution of 1 host. at 00:10, 6.59s elapsed
Initiating Connect Scan at 00:10
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 00:10, 1.90s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.065s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    filtered http
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.70 seconds

┌──(kali㉿kali)-[~]
└─$
```

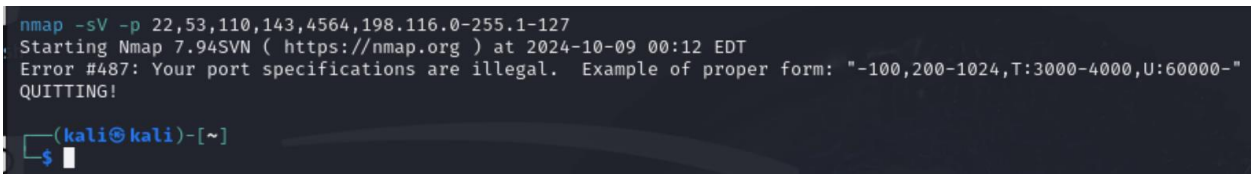
nmap -sS -O scanme.nmap.org/24

- Launches a stealth SYN scan against each machine that is up out of the 256 IPs on the /24 sized network where Scanme resides. It also tries to determine what operating system is running on each host that is up and running. This requires root privileges because of the SYN scan and OS detection.



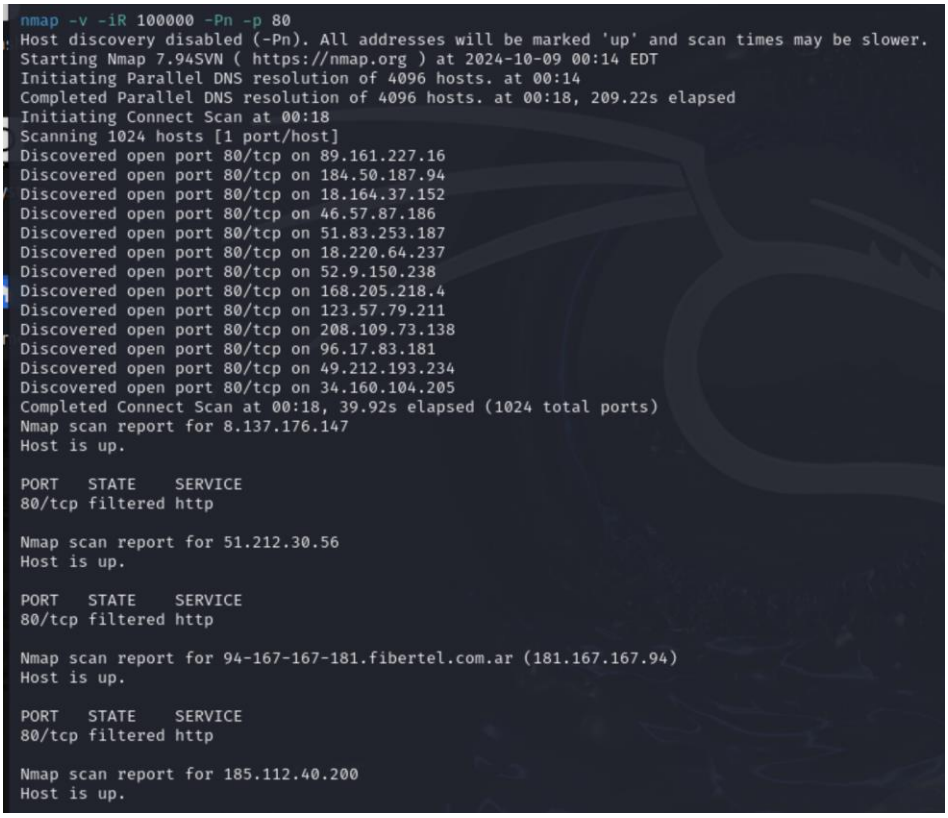
nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

- Launches host enumeration and a TCP scan at the first half of each of the 255 possible eight-bit subnets in the 198.116.0.0/16 address space. This tests whether the systems run SSH, DNS, POP3, or IMAP on their standard ports, or anything on port 4564. For any of these ports found open, version detection is used to determine what application is running.



nmap -v -iR 100000 -Pn -p 80

- Asks Nmap to choose 100,000 hosts at random and scan them for web servers (port 80). Host enumeration is disabled with -Pn since first sending a couple probes to determine whether a host is up is wasteful when you are only probing one port on each target host anyway.



nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

- This scans 4096 IPs for any web servers (without pinging them) and saves the output in grepable and XML formats.