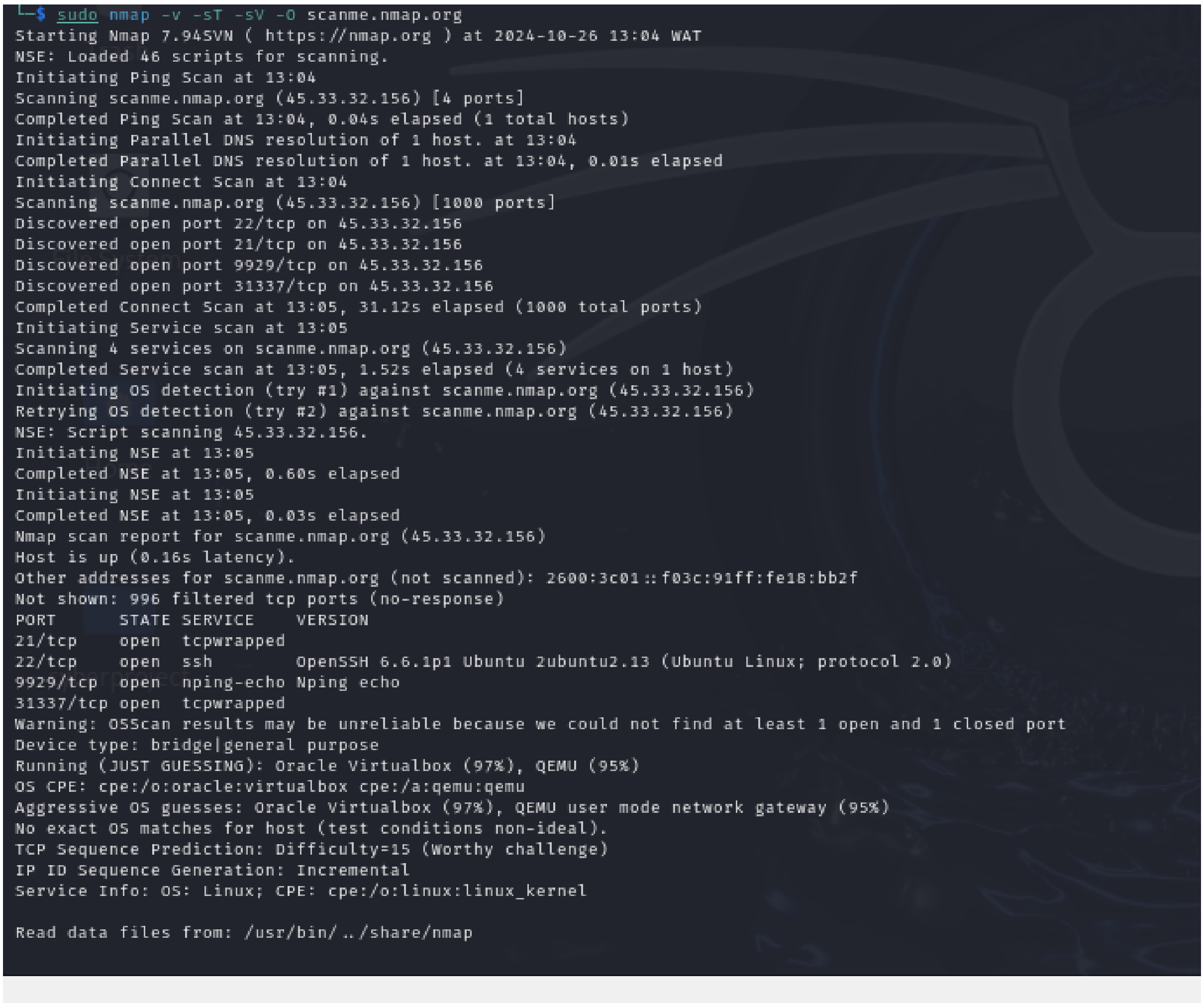
NMAP Assessment

Tool: Kali Linux (**Nmap)**

Lab Purpose: Nmap(Network Mapper) is an open-source security auditing and network scanning tool, it is used to discover and gather information on hosts and services on a network.

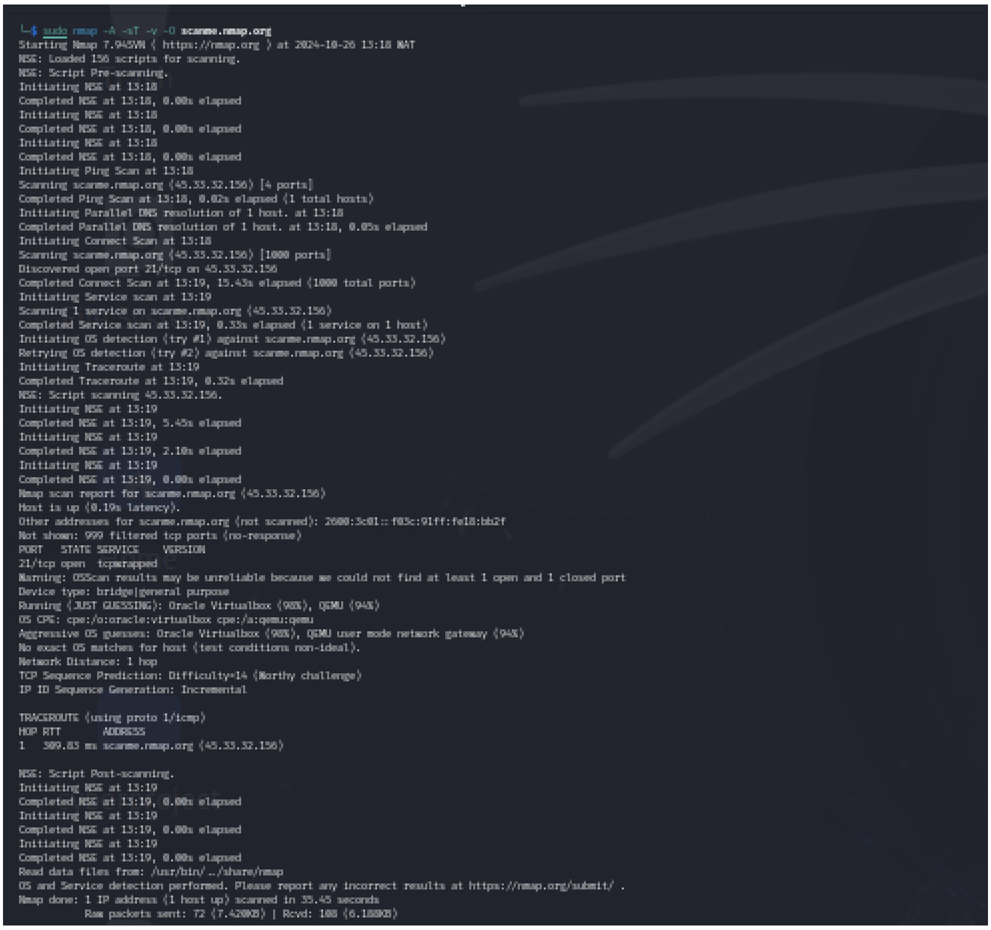
Project Objective: Learn how to scan a host using Nmap, and understand the results.

Project-Site: scanme.nmap.org



```
└─$ sudo nmap -v -sT -sV -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 13:04 WAT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 13:04
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 13:04, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.01s elapsed
Initiating Connect Scan at 13:04
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 21/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 13:05, 31.12s elapsed (1000 total ports)
Initiating Service scan at 13:05
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:05, 1.52s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 13:05
Completed NSE at 13:05, 0.60s elapsed
Initiating NSE at 13:05
Completed NSE at 13:05, 0.03s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
21/tcp    open  tcpwrapped
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (95%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (95%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=15 (Worthy challenge)
IP ID Sequence Generation: Incremental
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
```



```
└─$ sudo nmap -A -sT -v -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 13:18 WAT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:18
Completed NSE at 13:18, 0.00s elapsed
Initiating NSE at 13:18
Completed NSE at 13:18, 0.00s elapsed
Initiating NSE at 13:18
Completed NSE at 13:18, 0.00s elapsed
Initiating Ping Scan at 13:18
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 13:18, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:18
Completed Parallel DNS resolution of 1 host. at 13:18, 0.05s elapsed
Initiating Connect Scan at 13:18
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 21/tcp on 45.33.32.156
Completed Connect Scan at 13:19, 15.43s elapsed (1000 total ports)
Initiating Service scan at 13:19
Scanning 1 service on scanme.nmap.org (45.33.32.156)
Completed Service scan at 13:19, 0.33s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 13:19
Completed Traceroute at 13:19, 0.32s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 13:19
Completed NSE at 13:19, 5.45s elapsed
Initiating NSE at 13:19
Completed NSE at 13:19, 2.10s elapsed
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=14 (Worthy challenge)
IP ID Sequence Generation: Incremental

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   309.83 ms scanme.nmap.org (45.33.32.156)

NSE: Script Post-scanning.
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
Initiating NSE at 13:19
Completed NSE at 13:19, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.45 seconds
           Raw packets sent: 72 (7.420KB) | Rcvd: 108 (6.180KB)
```

SCAN RESULTS 1

Using the Sudo nmap, and -v -sT -sV -O flags, it discovered four open ports; On Ip Address (45.33.32.156) scanme.nmap.org

-Port 21(FTP)

-Port 22(SSH)

-Port 9929(Nping echo)

-Port 31337(TCP wrapped)

-v flag: This enables Verbosity, and causes Nmap to gather more information about the scan in progress, such as open ports found in real time, and time estimates for scan.

-sT flag: This is the TCP Connect Scan flag, it establishes full connection to the target, by using the three way handshake to, it sends SYN packets to the target port, and waits for SYN-ACK packets, to see if the ports are open, the last handshake is the ACK packet that acknowledges the connection established.

-sV flag: This Scans Version detection on specified ports.

-O flag: This used to detect the OS, such as the device type, the OS details, and Network distance.

Using the -O (Osscan), it detected the Hypervisor (Oracle Virtual Box).

Finally, it also detected the Service Info;

The Operating System (OS Linux)

The CPE (Common Platform Enumeration)

SCAN 2: Using the Sudo Nmap and -A -sT -v -O flags,;

With the -A flag in this scan, it gathers full information on the target site.