Nmap Project

Tool: Kali Linux(Nmap)

Project-Site: scanme.nmap.org

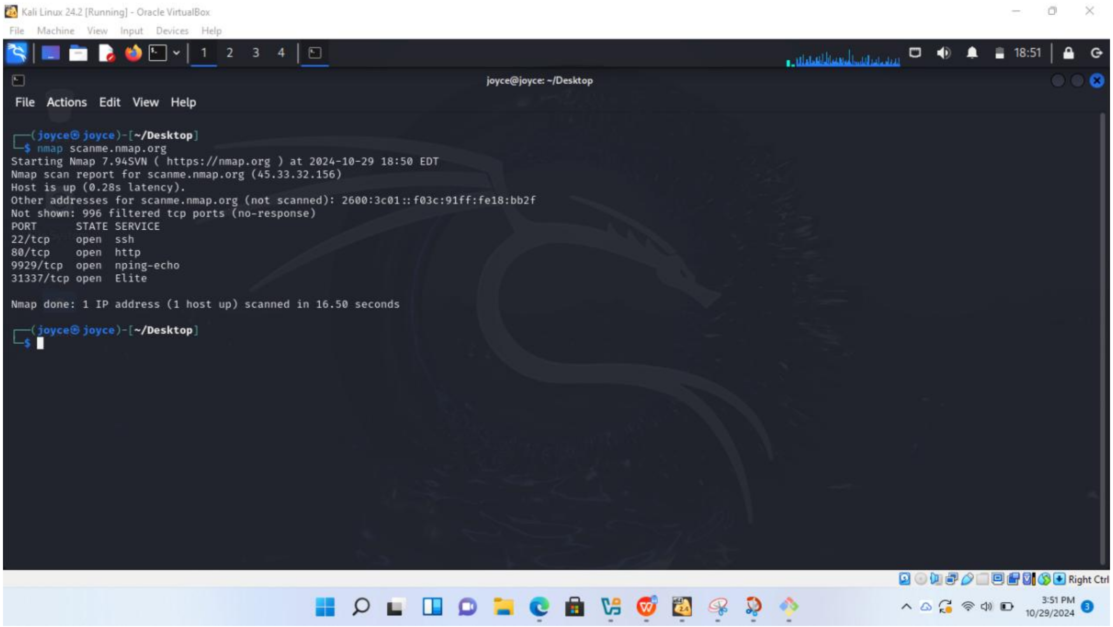
Project Objective: Learn Nmap and understand the results.

What is Nmap: Nmap (Network Mapper) is a an open source tool and software, used to scan for hosts and services, on a computer network. Its also used for security auditing, and information gathering(footprinting), and detection of vulnerabilities.

scanme.nmap.org

Scan Results:

This basic Nmap scan discovered four open ports, it also got the ipv4 address of the project-site(45.33 .32.156), and ipv6(2600:3c01:fe3c:91ff:fe18:bb2f)

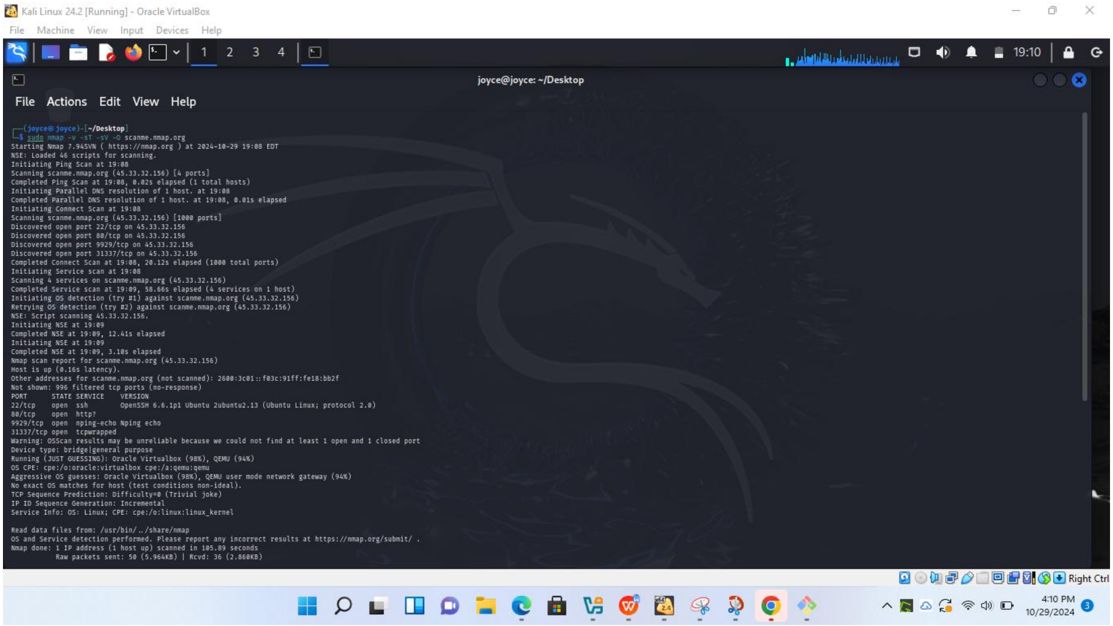

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:51
joyce@joyce: ~/Desktop
File Actions Edit View Help
Right Ctrl
3:51 PM
10/29/2024

```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 18:50 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s 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
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 16.50 seconds

┌──(joyce㉿joyce)-[~/Desktop]
└─$ 
```

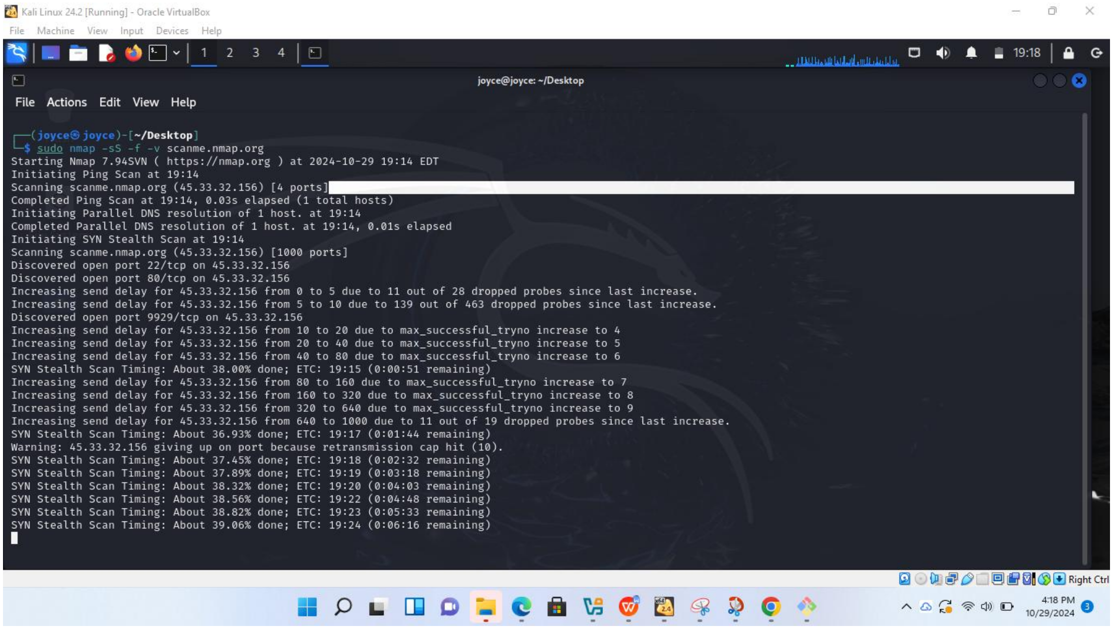
Scan Results: Using the -v -sT -sV -O flags: With the -v(verbose mode), -sT(Tcp connect scan), -sV (scan version) -O (Osscan) flags. It discovered four ports open, and services, it also discovered the ipv4 address, and the ipv6 address, version detection, device type and OS(Operating System)


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
19:10
joyce@joyce: ~/Desktop
File Actions Edit View Help
Right Ctrl
4:10 PM
10/29/2024

```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ sudo nmap -v -sT -sV -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 19:08 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 19:08
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 19:08, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:08
Completed Parallel DNS resolution of 1 host. at 19:08, 0.01s elapsed
Initiating Connect Scan at 19:08
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/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 19:08, 20.12s elapsed (1000 total ports)
Initiating Service scan at 19:08
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 19:09, 58.66s 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 19:09
Completed NSE at 19:09, 12.41s elapsed
Initiating NSE at 19:09
Completed NSE at 19:09, 3.10s 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
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http?
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 (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).
TCP Sequence Prediction: Difficulty=0 (Trivial joke)
IP ID Sequence Generation: Incremental
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 105.89 seconds
           Raw packets sent: 50 (5.964KB) | Rcvd: 36 (2.860KB)
```

Scan Results: With the -sS(Stealthy mode), -f(fast), -v(verbose mode) fags. It Perfomed a fast stealthy, verbose scan:


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
19:18
joyce@joyce: ~/Desktop
File Actions Edit View Help
Right Ctrl
4:18 PM
10/29/2024

```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ sudo nmap -sS -f -v scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 19:14 EDT
Initiating Ping Scan at 19:14
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 19:14, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:14
Completed Parallel DNS resolution of 1 host. at 19:14, 0.01s elapsed
Initiating SYN Stealth Scan at 19:14
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 28 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 139 out of 463 dropped probes since last increase.
Discovered open port 9929/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 38.00% done; ETC: 19:15 (0:00:51 remaining)
Increasing send delay for 45.33.32.156 from 80 to 160 due to max_successful_tryno increase to 7
Increasing send delay for 45.33.32.156 from 160 to 320 due to max_successful_tryno increase to 8
Increasing send delay for 45.33.32.156 from 320 to 640 due to max_successful_tryno increase to 9
Increasing send delay for 45.33.32.156 from 640 to 1000 due to 11 out of 19 dropped probes since last increase.
SYN Stealth Scan Timing: About 36.93% done; ETC: 19:17 (0:01:44 remaining)
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 37.45% done; ETC: 19:18 (0:02:32 remaining)
SYN Stealth Scan Timing: About 37.89% done; ETC: 19:19 (0:03:18 remaining)
SYN Stealth Scan Timing: About 38.32% done; ETC: 19:20 (0:04:03 remaining)
SYN Stealth Scan Timing: About 38.56% done; ETC: 19:22 (0:04:48 remaining)
SYN Stealth Scan Timing: About 38.82% done; ETC: 19:23 (0:05:33 remaining)
SYN Stealth Scan Timing: About 39.06% done; ETC: 19:24 (0:06:16 remaining)
█
```

Perfoming a fast stealthy, verbosity scan: -sS -f -v flags