Name - HARSHIL AMIT BUCH
Class - TY CSF-1
Roll Number - 14

Experiment No. 4

Title:

Perform a network scanning and vulnerability detection using tools like Nmap

Objective:

To learn how to scan a network using Nmap, identify live hosts, open ports, and detect possible vulnerabilities. This helps us understand the attack surface of a system.

Software/Tools Required:

- Kali Linux
- Terminal
- Nmap

Theory:

Nmap (Network Mapper) is a powerful tool for scanning networks. It detects active devices, services running on different ports, and possible vulnerabilities. Attackers use it for reconnaissance, while security professionals use it for defense and auditing.

Installation Commands:

Tool: zphisher

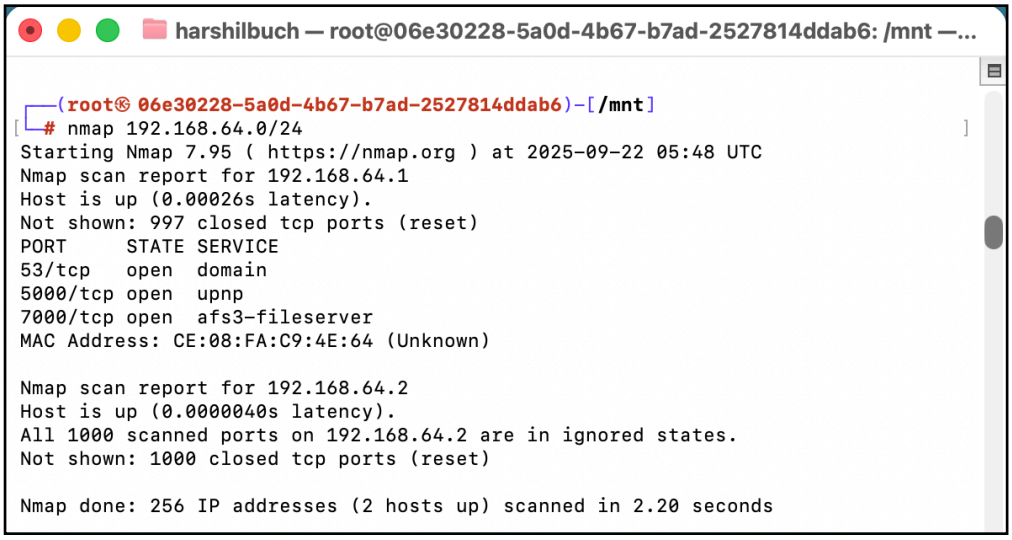
1. **Open Kali Linux Terminal Emulator**
2. **Commands:**

   sudo apt install nmap → (Install Nmap on Linux)

   Enter password and hit enter
3. **Once the installation is done,**
4. nmap <IP> → (Basic scan to find live host and open ports)
5. nmap -sV <IP> → (Detect services and versions running)

Note: In <IP> paste target IPv4 Address

Output Screenshots:



```
┌──(root㉿ 06e30228-5a0d-4b67-b7ad-2527814ddab6)-[/mnt]
└─# nmap -sV 192.168.64.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 05:48 UTC
Nmap scan report for 192.168.64.1
Host is up (0.00033s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
53/tcp   open  domain  (generic dns response: NXDOMAIN)
5000/tcp open  rtsp
7000/tcp open  rtsp
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.95%I=7%D=9/22%Time=68D0E354%P=aarch64-unknown-linux-gnu%
SF:r(DNSVersionBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\x01\0\0\x07ver
SF:sion\x04bind\0\0\x10\0\x03\0\x06\0\x01\0\0\x03\x84\0@\x01a\x0croot-se
SF:rvers\x03net\0\x05nstld\x0cverisign-grs\x03com\0x\xb4th\0\0\x07\x08\0\0
SF:\x03\x84\0\t:\x80\0\x01Q\x80");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.95%I=7%D=9/22%Time=68D0E351%P=aarch64-unknown-linux-gn
SF:uNr(GetRequest,8E,"HTTP/1\.1\x20403\x20Forbidden\r\nContent-Length:\x20
SF:0\r\nServer:\x20AirTunes/890\.79\.5\r\nX-Apple-ProcessingTime:\x203\r\n
SF:X-Apple-RequestReceivedTimestamp:\x202546388\r\n\r\n")%r(RTSPRequest,8E
SF:,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20A
SF:irTunes/890\.79\.5\r\nX-Apple-ProcessingTime:\x206\r\nX-Apple-RequestRe
SF:ceivedTimestamp:\x202546414\r\n\r\n")%r(HTTPOptions,8E,"HTTP/1\.1\x2040
SF:3\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/890\.79\.
SF:5\r\nX-Apple-ProcessingTime:\x208\r\nX-Apple-RequestReceivedTimestamp:\
SF:x202551424\r\n\r\n")%r(FourOhFourRequest,8E,"HTTP/1\.1\x20403\x20Forbid
SF:den\r\nContent-Length:\x200\r\nServer:\x20AirTunes/890\.79\.5\r\nX-Appl
SF:e-ProcessingTime:\x206\r\nX-Apple-RequestReceivedTimestamp:\x202551448\
SF:r\n\r\n")%r(SIPOptions,A0,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Len
SF:gth:\x200\r\nServer:\x20AirTunes/890\.79\.5\r\nCSeq:\x2042\x20OPTIONS\r
SF:\nX-Apple-ProcessingTime:\x204\r\nX-Apple-RequestReceivedTimestamp:\x20
SF:2551465\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7000-TCP:V=7.95%I=7%D=9/22%Time=68D0E356%P=aarch64-unknown-linux-gn
SF:uNr(RTSPRequest,8F,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Length:\x2
SF:00\r\nServer:\x20AirTunes/890\.79\.5\r\nX-Apple-ProcessingTime:\x2013\r
SF:\nX-Apple-RequestReceivedTimestamp:\x202546374\r\n\r\n")%r(GetRequest,8
SF:E,"HTTP/1\.1\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20
SF:AirTunes/890\.79\.5\r\nX-Apple-ProcessingTime:\x208\r\nX-Apple-RequestR
SF:eceivedTimestamp:\x202551384\r\n\r\n")%r(HTTPOptions,8E,"HTTP/1\.1\x204
SF:03\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/890\.79\
SF:.5\r\nX-Apple-ProcessingTime:\x207\r\nX-Apple-RequestReceivedTimestamp:
SF:\x202551405\r\n\r\n")%r(FourOhFourRequest,8E,"HTTP/1\.1\x20403\x20Forbi
SF:dden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/890\.79\.5\r\nX-App
SF:le-ProcessingTime:\x204\r\nX-Apple-RequestReceivedTimestamp:\x202551433
SF:\r\n\r\n")%r(SIPOptions,A0,"RTSP/1\.0\x20403\x20Forbidden\r\nContent-Le
SF:ngth:\x200\r\nServer:\x20AirTunes/890\.79\.5\r\nCSeq:\x2042\x20OPTIONS\
SF:r\nX-Apple-ProcessingTime:\x203\r\nX-Apple-RequestReceivedTimestamp:\x2
SF:02551456\r\n\r\n");
MAC Address: CE:08:FA:C9:4E:64 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```

Outcome:

We performed scanning with Nmap and found open ports and running services on the target system. Using service detection and vulnerability scripts, we identified potential weak points. This gave us practical exposure to reconnaissance and security auditing.

Conclusion:

The experiment shows the importance of Nmap in ethical hacking and cybersecurity. It highlights how attackers gather system details, but also how administrators can use the same tool to strengthen defenses.