Internship – Day01 (Network Reconnaissance)

1. Title

Task: Scan Local Network for Open Ports
Name: Abhinav Tiwari
Date: 2025-09-22

2. Objective: Discover open ports on devices in the local lab network to evaluate exposure

3. Scope & Rules of Engagement

- **Scanned network(s)**: 192.168.197.0/24
- **Targets:** Metasploitable2 (192.168.197.131)
- **Tools used:** Nmap
- **Authorization**: Performed on owned VMs in isolated lab; no external scanning.

4. Methodology

4.1 Discover your IP / network range

Command: ip -4 addr show

```
┌──(kali㉿kali)-[~]
└─$ ip -4 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.197.128/24 brd 192.168.197.255 scope global dynamic noprefixroute eth0
       valid_lft 1718sec preferred_lft 1718sec
```

4.2 Quick host discovery (who's up?)

Command: nmap -sn 192.168.197.131 -oN nmap_hosts_up.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.197.131 -oN nmap_hosts_up.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:30 EDT
Nmap scan report for 192.168.197.131
Host is up (0.00079s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

4.3 Basic/top-ports reconnaissance

Command: nmap -sS --top-ports 100 -T4 -oN nmap.txt 192.168.197.131

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS --top-ports 100 -T4 -oN nmap.txt 192.168.197.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:31 EDT
Nmap scan report for 192.168.197.131
Host is up (0.0019s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

4.4 Full TCP port scan (all ports)

Command: nmap -sS -p- -T4 -oN all_ports.txt 192.168.197.131

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- -T4 -oN all_ports.txt 192.168.197.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:33 EDT
Nmap scan report for 192.168.197.131
Host is up (0.0020s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38618/tcp open  unknown
45332/tcp open  unknown
49534/tcp open  unknown
58325/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.63 seconds
```

4.5 Service/version & OS detection

Command: nmap -sS -sV -p21,80,443 -oA nmap_service_os.txt 192.168.197.131

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -p21,80,443 -oA nmap_service_os.txt 192.168.197.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:37 EDT
Nmap scan report for 192.168.197.131
Host is up (0.00095s latency).

PORT    STATE  SERVICE VERSION
21/tcp  open   ftp     vsftpd 2.3.4
80/tcp  open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp closed https
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix
```

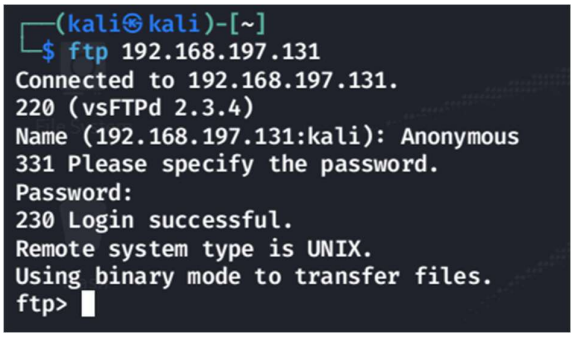
4.6 Save machine-readable output for parsing / reports

Command: nmap -sS -sV -O -p- -oA nmap_report 192.168.197.131

```
┌──(kali㉿kali)-[~]
└─$ cat nmap_report.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.95 scan initiated Mon Sep 22 07:42:35 2025 as: /usr/lib/nmap/nmap -&#45;privileged -sS -sV -O -p- -oA nmap_report 192.168.197.131 -->
<nmaprun scanner="nmap" args="/usr/lib/nmap/nmap -&#45;privileged -sS -sV -O -p- -oA nmap_report 192.168.197.131" start="1758541355" startstr="Mon Sep 22
 07:42:35 2025" version="7.95" xmloutputversion="1.05">
<scaninfo type="syn" protocol="tcp" numservices="65535" services="1-65535" />
<verbose level="0" />
<debugging level="0" />
<hosthint><status state="up" reason="arp-response" reason_ttl="0" />
<address addr="192.168.197.131" addrtype="ipv4" />
<address addr="00:0C:29:FA:DD:2A" addrtype="mac" vendor="VMware" />
<hostnames>
</hostnames>
</hosthint>
```

5. Findings

[Anonymous FTP allowed on target]
Target IP: 192.168.197.131
Hostname: metasploitable2
Port: 21/TCP
Service & Version: vsftpd 2.3.4 (detected via Nmap service scan)
Observed Output:
Nmap output: 21/tcp open ftp vsftpd 2.3.4
When connecting via ftp, anonymous login accepted: 230 Login successful.
Screenshot:



Vulnerability Issue:
The FTP service allows anonymous (unauthenticated) login, permitting unauthorised users to read/write files depending on configuration.

Risk Rating: High , *Reason:* Anonymous access allows data exposure or uploading of malicious files; vsftpd 2.3.4 is also historically associated with known exploits on deliberately vulnerable images.

Impact:
An attacker could download sensitive files from the FTP server.
An attacker may upload malicious scripts or backdoors if write permissions exist.
Could be used as pivot/storage for further attacks.

Remediation / Recommendation:

1. Disable anonymous FTP: set anonymous_enable=NO in /etc/vsftpd.conf.
2. Restart the service: sudo systemctl restart vsftpd (or /etc/init.d/vsftpd restart)
3. Ensure proper filesystem permissions — FTP directories should not be world-writable.
4. If FTP is not required, uninstall vsftpd: sudo apt remove --purge vsftpd
5. If FTP must be available, restrict access by firewall (allow only trusted IPs) and enable strong authentication (SFTP is preferable).

References / CVE

- CVE-2011-2523 (vsftpd 2.3.4 - Backdoor Command Execution)