Project Title: Network Testing Report

Scope and Objective: This report demonstrates a structured approach to network testing, service enumeration, and traffic analysis in a controlled lab environment. The activities were conducted against a Metasploitable2 virtual machine within a defined scope for educational and ethical penetration testing.

---

1. Network Mapping

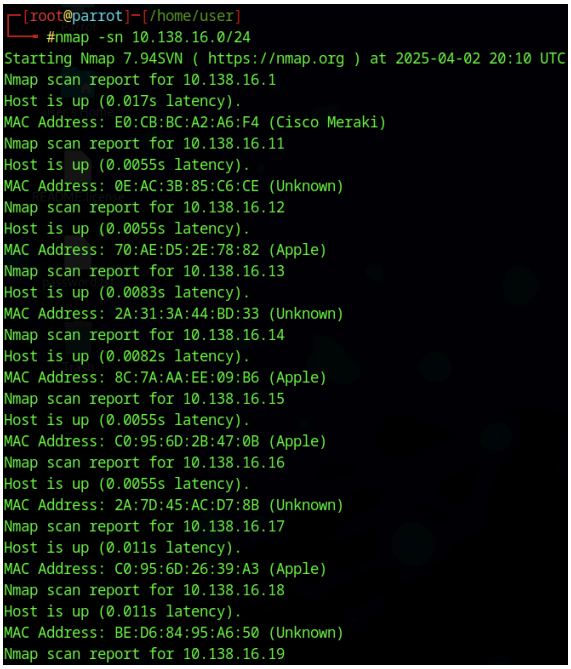
Tool Used: Nmap

Command:

nmap -sn 10.138.16.0/24

Result:

- Discovered active host: `10.138.16.138`
- Screenshot Reference:



```
┌──[root@parrot]─[/home/user]
└──╼ #nmap -sn 10.138.16.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 20:10 UTC
Nmap scan report for 10.138.16.1
Host is up (0.017s latency).
MAC Address: E0:CB:BC:A2:A6:F4 (Cisco Meraki)
Nmap scan report for 10.138.16.11
Host is up (0.0055s latency).
MAC Address: 0E:AC:3B:85:C6:CE (Unknown)
Nmap scan report for 10.138.16.12
Host is up (0.0055s latency).
MAC Address: 70:AE:D5:2E:78:82 (Apple)
Nmap scan report for 10.138.16.13
Host is up (0.0083s latency).
MAC Address: 2A:31:3A:44:BD:33 (Unknown)
Nmap scan report for 10.138.16.14
Host is up (0.0082s latency).
MAC Address: 8C:7A:AA:EE:09:B6 (Apple)
Nmap scan report for 10.138.16.15
Host is up (0.0055s latency).
MAC Address: C0:95:6D:2B:47:0B (Apple)
Nmap scan report for 10.138.16.16
Host is up (0.0055s latency).
MAC Address: 2A:7D:45:AC:D7:8B (Unknown)
Nmap scan report for 10.138.16.17
Host is up (0.011s latency).
MAC Address: C0:95:6D:26:39:A3 (Apple)
Nmap scan report for 10.138.16.18
Host is up (0.011s latency).
MAC Address: BE:D6:84:95:A6:50 (Unknown)
Nmap scan report for 10.138.16.19
```

```
Nmap scan report for 10.138.16.138
Host is up (0.00098s latency).
```

This step successfully identified the target machine as active on the local subnet.

---

2. Service Enumeration

Tool Used: Nmap

Command:

nmap -sV -O 10.138.16.138

Findings:

- Open services include FTP, SSH, Telnet, SMTP, HTTP, SMB, NFS, MySQL, PostgreSQL, VNC, and others
- OS fingerprint: Linux 2.6.X
- Screenshot Reference:

```
└──╼ #nmap -sV -O 10.138.16.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 20:15 UTC
Nmap scan report for 10.138.16.138
Host is up (0.0016s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 96:16:67:66:4A:26 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

This information identifies numerous vulnerable services and legacy software versions suitable for further analysis.

---

3. Protocol Analysis

Tested Protocol: FTP

Tool Used: FTP client

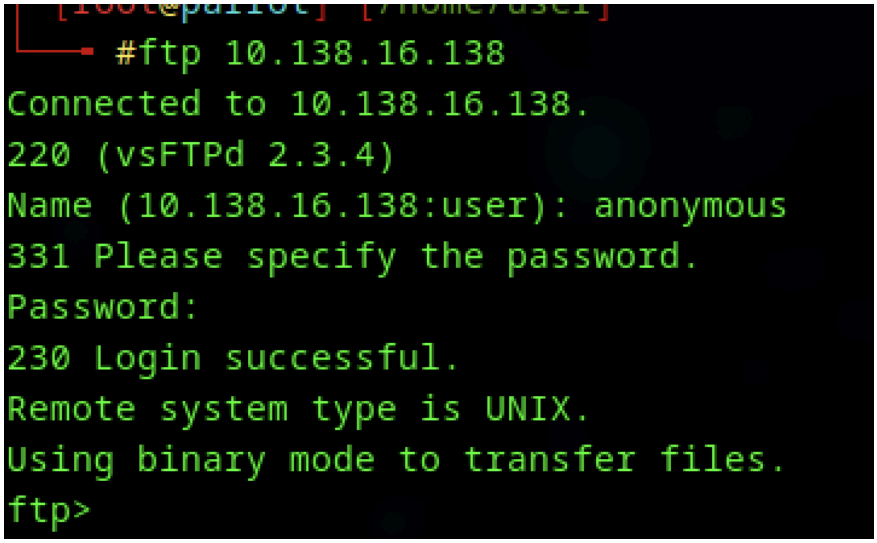
Command:

ftp 10.138.16.138

Action: Logged in using anonymous login

Result:

- Login successful without authentication
- Screenshot Reference:



This demonstrates a significant misconfiguration and security risk: anonymous access with upload/download capability.

---

4. Access Point Identification

Based on Nmap results:

- **FTP (21/tcp):** Anonymous login allowed ✅
- **Telnet (23/tcp):** Plaintext credentials likely ✅
- **SSH (22/tcp):** Old version, potential default creds ✅
- **HTTP (80/tcp / 8180/tcp):** Apache and Tomcat services exposed ✅

Each of these presents an entry point with potential for exploitation. Access points were identified strictly based on service enumeration without active exploitation beyond login testing.

---

5. Traffic Analysis

Tool Used: tcpdump

Command:

tcpdump -i enp0s1 port 21 -w capture.pcap

Screenshot Reference:

```
└──╼ #tcpdump -i enp0s1 port 21 -w capture.pcap
tcpdump: listening on enp0s1, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
^C36 packets captured
36 packets received by filter
0 packets dropped by kernel
```

Result:

- 36 FTP packets captured while anonymous FTP session was active
- Data exported to `capture.pcap`

Analysis (from Wireshark):

- Plaintext FTP authentication observed
- Command and response sequences visible
- No encryption in transport, revealing potential for credential sniffing

---

6. Summary of Key Findings

Service	Port	Vulnerability/Observation	Risk Level
FTP	21	Anonymous login allowed	High
SSH	22	Outdated OpenSSH version	Medium
Telnet	23	Plaintext communication	High
SMTP	25	VRFY/EXPN may be enabled	Medium
HTTP	80	Apache 2.2.8 exposed, possibly outdated	Medium
SMB	139/445	Samba 3.x with null sessions possible	High
VNC	5900	VNC 3.3 with no encryption	High

IRC	6667	UnrealIRCd potentially backdoored	High
Tomcat	8180	Coyote JSP engine exposed	Medium

---

7. Conclusion and Recommendations

This testing confirmed:

- Open and outdated services vulnerable to enumeration and misuse
- FTP misconfigured to allow anonymous login
- Cleartext protocols (FTP, Telnet) pose high risks
- Multiple access points should be secured or removed

Recommendations:

- Disable anonymous FTP or restrict it with permissions
- Replace Telnet with SSH and update SSH service
- Patch outdated services (Apache, MySQL, Samba, etc.)
- Apply encryption and firewall segmentation where appropriate