Information Gathering & Assessment Report

Target: Metasploitable Virtual Machine
IP Address: 192.168.128.2
Testing Environment: Local VM network (Host-Only or NAT)
Date: March 24, 2025

1. Passive Reconnaissance

Methodology:

- Identified target IP using local virtual machine configuration.
- Attempted reverse DNS lookup using `nslookup`.

Command Executed:

nslookup 192.168.128.2

Result:

;; no servers could be reached

Conclusion: Reverse DNS lookup was unsuccessful due to the isolated lab environment and lack of DNS resolution. This is expected in local networks not connected to an external DNS server.

Ethical Note: Only passive techniques were used. No interaction with the target system occurred during this phase.

---

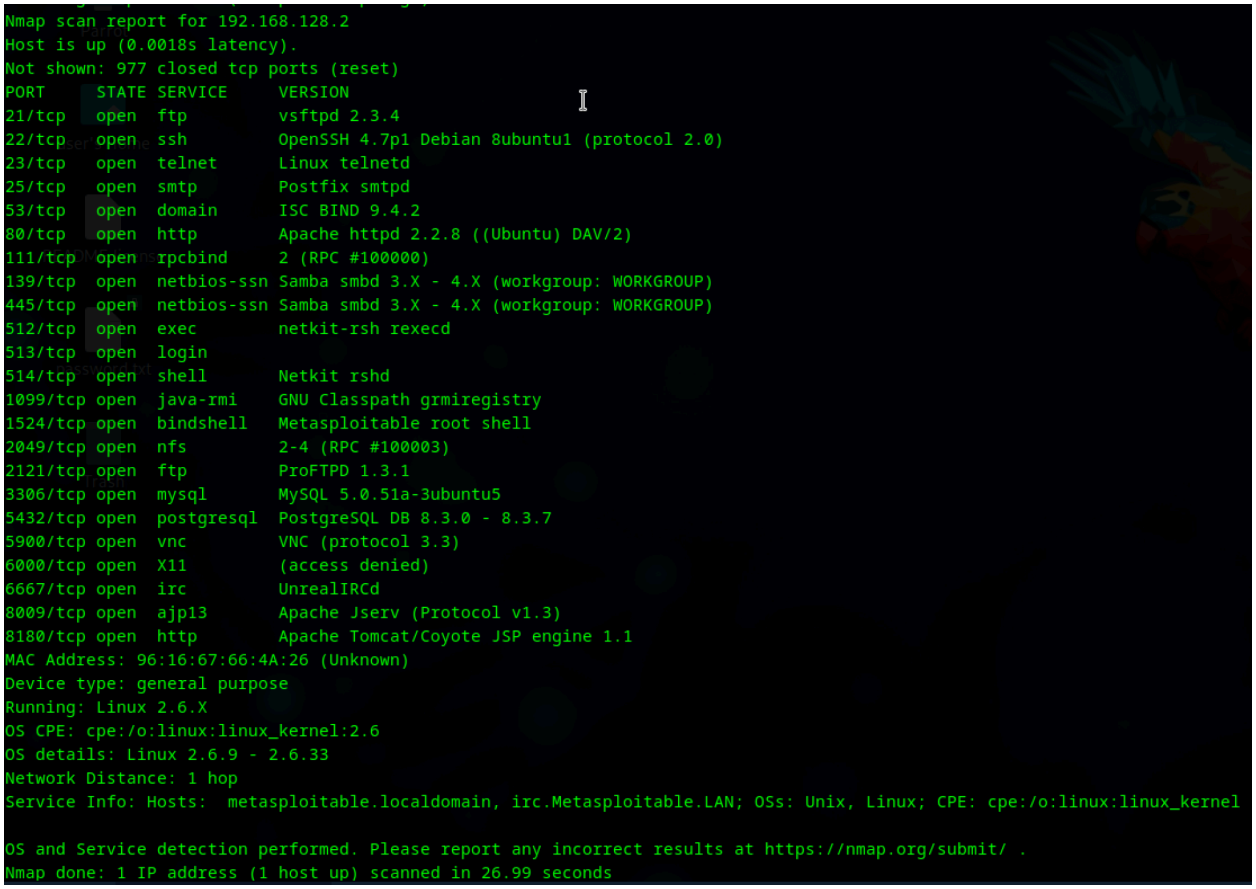
2. Network Enumeration

Tool Used: Nmap

Nmap Command Executed:

nmap -sS -sV -O 192.168.128.2

Key Findings:



```
Nmap scan report for 192.168.128.2
Host is up (0.0018s latency).
Not shown: 977 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  shell       Netkit rshd
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
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

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 26.99 seconds
```

- Host is up
- OS: Linux 2.6.X
- MAC Address: 96:16:67:66:44:26
- Distance: 1 hop

Open Ports and Services:

Port	State	Service	Version
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111	open	rpcbind	RPC
139	open	netbios-ssn	Samba smbd 3.X - 4.X
445	open	netbios-ssn	Samba smbd 3.X - 4.X
512	open	exec	netkit-rsh rexecd
513	open	login	-
514	open	shell	Netkit rshd
1099	open	java-rmi	GNU Classpath grmiregistry
1524	open	bindshell	Metasploitable root shell
2049	open	nfs	-
2121	open	ftp	ProFTPD 1.3.1
3306	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	open	vnc	VNC (protocol 3.3)
6000	open	X11	(access denied)
6667	open	irc	UnrealIRCd
8009	open	ajp13	Apache Jserv Protocol 1.3
8180	open	http	Apache Tomcat/Coyote JSP 1.1

3. Asset Discovery

Assets Identified:

- A single virtual machine with multiple exposed services
- Operating System: Linux 2.6.X
- Hostnames detected: `metasploitable.localdomain`, `irc.Metasploitable.LAN`

Technologies Observed:

- Web Servers: Apache 2.2.8, Tomcat/Coyote JSP

- Databases: MySQL, PostgreSQL
- File Transfer: FTP (vsftpd, ProFTPD)
- Remote Access: SSH, Telnet, VNC, RSH
- Email: Postfix (SMTP)
- Other: Samba, BIND DNS, Java RMI, Unreal IRC

---

4. Observations and Potential Vulnerabilities (To Be Investigated)

- **vsftpd 2.3.4** – Known backdoor vulnerability (CVE-2011-2523)
- **Open ports on insecure services** – Telnet, RSH, RPC, and VNC
- **Multiple remote access methods** – Suggests possible privilege escalation paths
- **Outdated Apache and Tomcat versions** – May be vulnerable to exploits

---

5. Ethical Compliance and Documentation

- All reconnaissance was performed within a controlled lab environment
- No unauthorized access was attempted
- All findings are used strictly for educational and ethical security purposes