LAB

10

Linux (Metasploitable 2) Hacking

By the end of this section, you should be able to:

- Identify vulnerabilities in Linux (Metasploitable 2).
- Demonstrate the use of Metasploit in exploiting vulnerability
- Exploit the vulnerability on Linux (Metasploitable 2).

10.1 Introduction

Generally, success in Hacking a system depending on the vulnerability the target possesses. The vulnerability can come from many aspect such as a weak configured system, an old services that have a well-known vulnerability, unpatched system or it can cause by a user is that is not considering a good security measures during using a system. In order to identify a vulnerability, an attacker will run a lot of scanning and enumeration activity for getting as much information as possible about the target infrastructure and services. A weak security countermeasure might be revealed through the scanning and enumeration phase. This information is then used by the attacker to plan for the next step in system hacking.

Task 1: Scanning Linux (Metasploitable 2) target

1. To start the Lab activity you need :-
    a. A Kali linux VM
    b. A Metasploitable 2 linux (ML2) VM

   Both VM should be set to A NAT network setting
2. Login into ML2 and check the IP address, this ML2 VM will become the victim/target
3. Login to Kali VM, open a terminal and check the IP address. The Kali VM will become the attacker in this lab activity.
4. On the same terminal on Kali VM, open a Metasploit console using the command

```
>msfconsole
```

5. Once the Metasploit console appear start the scanning on the windows machine by using the nmap command

```
msf> nmap -T4 -A -v [ML2 IP address]
```

6. From the result of the scanning identify the open port and do some research on each service available on ML2.
7. Generally, you will get port 21 is open, these ports indicate that ML2 have FTP services available. The FTP service is implemented using VSFTPD 2.3.4 and this ftp services have a known vulnerability that is provided in the Metasploit framework.

Task 2 : Exploiting VSFTPD 2.3.4 vulnerability

1. Once you have identified the vulnerability on ML2 machine, the next phase is to search for the exploit for the vulnerability. Most well-known vulnerability have an exploit script already available to be used especially in the Metasploit framework.
2. In order to search the suitable exploit script for a vulnerability, Metasploit user's can use the search command with the of use the exploit option type and the right keyword. For example to search for the VSFTPD vulnerability you can type the command:-

```
msf> search type:exploit vsftpd
```

3. Any exploit related to vsftpd will be displayed on the msfconsole, to get further description on the exploit, user can used the command info and the specified exploit index.

```
msf>info
exploit/unix/ftp/vsftpd_234_backdoor
```

4. The information displayed contain the required setting for executing the exploits as well the detail description of the exploit including the specified target of the exploit.
5. To use the exploit, you can type the command use and followed with the reference index of the exploit.

```
msf>use
exploit/unix/ftp/vsftpd_234_backdoor
```

6. You will see the prompt change to the name of the exploit, now type in the command

   ```
   …>show options
   ```

   To get the required setting to start the exploit.
7. There are few setting need to be set into the exploit before the exploit can be executed, the setting is the Remote target (RHOST). This exploit will initiate a remote shell even though we not specifying the payload.
8. To set all the setting requirement, you need to type the command

   ```
   …>set RHOST [the target VM IP (ML2 address)]
   …>show options (to check the setting)
   ```

9. Once the exploit requirement has been set, the exploit can be executed using the command

   ```
   …>exploit
   ```

10. During the exploit you will see some information displayed on the msfconsole, this information show the exploit responses an if the exploit success, you will see a session is created and you can type any shell command on the display.
11. You now have overtaken the ML2 machine remotely and are able to do some malicious activity to the ML2 machine. To

get the option you can do towards the target, type in the command

- **This Lab manual come with a video demonstration, please refer to the video for extra exploitation features**
- **All the activities done in this Lab are very intrusive in nature and it is a crime to hack into anyone machine unless it is an official penetration test**
- **PLEASE DO THIS EXERCISE IN A CONTROL ENVIRONMENT AND FOR THE PURPOSE OF LEARNING ONLY**

Review Question

Do a research on other vulnerability on the ML2 machine have.

1. List at least 5 other exploits can be use in attacking a ML2. Specify the services and the suitable exploit available in Metasploit Framework.