

# VIT<sup>®</sup>

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

## **Network File Sharing Attack**

**NAME:** DHEVATHA S P

**REG NO.:** 22BCE0826

**NAME OF FACULTY:** DR. Satish C.J

**COURSE TITLE :** Penetration Testing and Vulnerability  
Analysis Lab

**COURSE CODE:** BCSE319P

**LAB SLOT:** L55+L56

**SEMESTER:** Winter Semester 2024-25

**CLASS NO.:** VL2024250505928

**Dhevatha S P**

**22BCE0826**

## 1. IP address of Kali Linux and Metasploitable2

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
pinkhacker@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.138.229 netmask 255.255.255.0 broadcast 192.168.138.255
    inet6 2401:4900:9240:b2f7:a00:27ff:feeb:2f9c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:feeb:2f9c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:eb:2f:9c txqueuelen 1000 (Ethernet)
    RX packets 88 bytes 7947 (7.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52 bytes 6043 (5.9 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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

pinkhacker@kali:~$ cd Desktop
pinkhacker@kali:~/Desktop$ nano lm_hash.txt

```

```

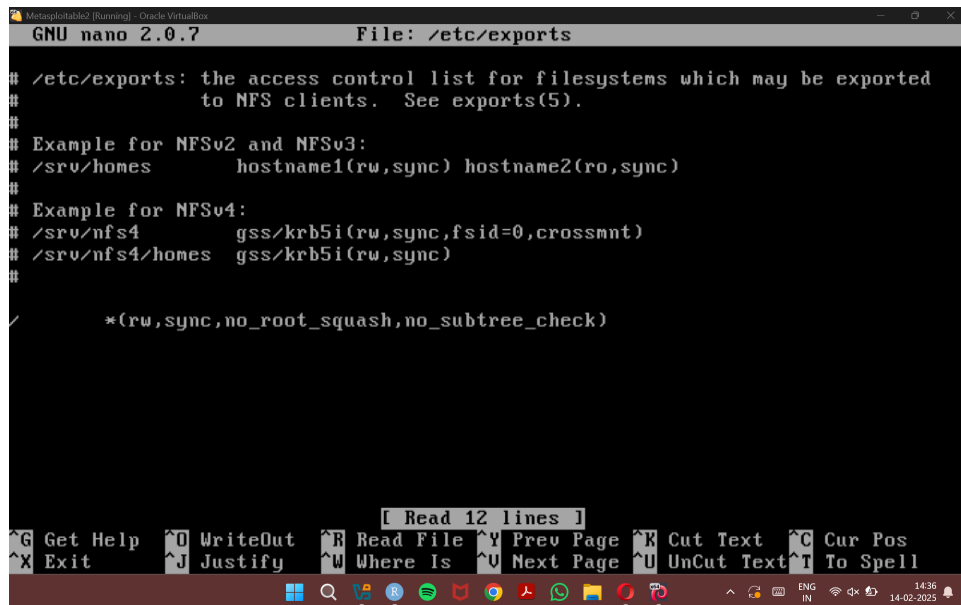
Metasploitable2 [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f7:56:85
          inet addr:192.168.138.1 Bcast:192.168.138.255 Mask:255.255.255.0
          inet6 addr: 2401:4900:9240:b2f7:a00:27ff:fef7:5685/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fef7:5685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3815 (3.7 KB) TX bytes:6266 (6.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:~$ _

```

## 2. Accessing the /etc/exports in Metasploitable2

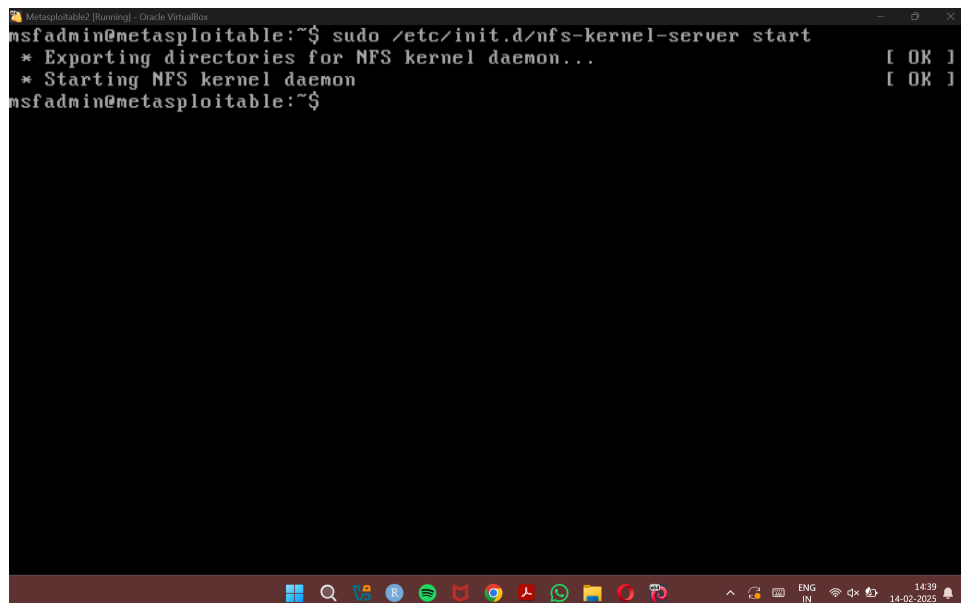


The screenshot shows a terminal window titled 'Metasploitable2 [Running] - Oracle VM VirtualBox'. The window displays the contents of the `/etc/exports` file using the `GNU nano 2.0.7` editor. The file content includes comments and export rules for NFSv2, NFSv3, and NFSv4. The terminal window has a standard Linux desktop environment at the bottom with various icons and a system tray showing the date and time as 14:36 on 14-02-2025.

```
GNU nano 2.0.7 File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

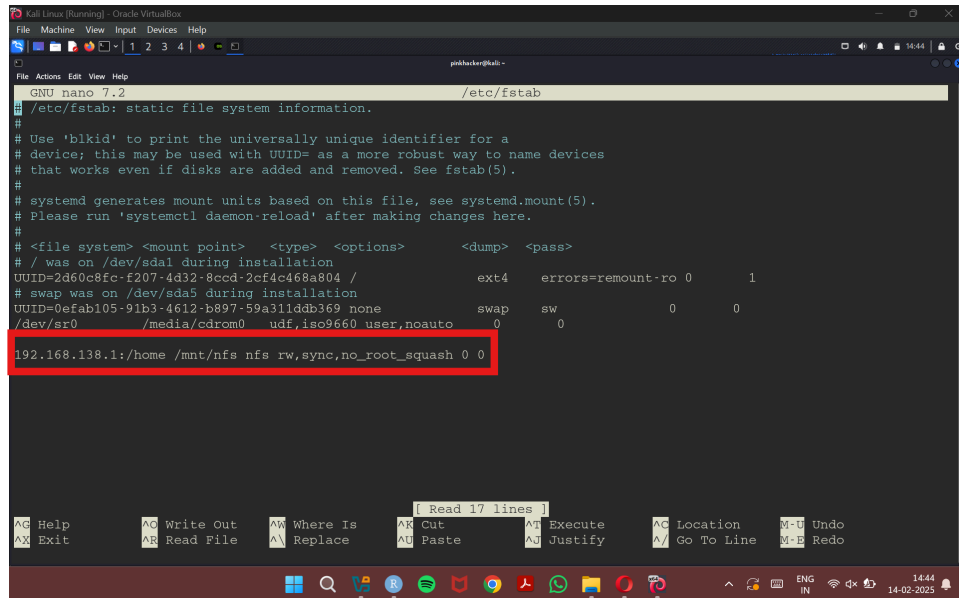
## 3. Starting the NFS server in Metasploitable2



The screenshot shows a terminal window titled 'Metasploitable2 [Running] - Oracle VM VirtualBox'. The window displays the command `sudo /etc/init.d/nfs-kernel-server start` being executed. The output shows two status messages: `* Exporting directories for NFS kernel daemon...` and `* Starting NFS kernel daemon`, both followed by `[ OK ]`. The terminal window has a standard Linux desktop environment at the bottom with various icons and a system tray showing the date and time as 14:39 on 14-02-2025.

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$
```

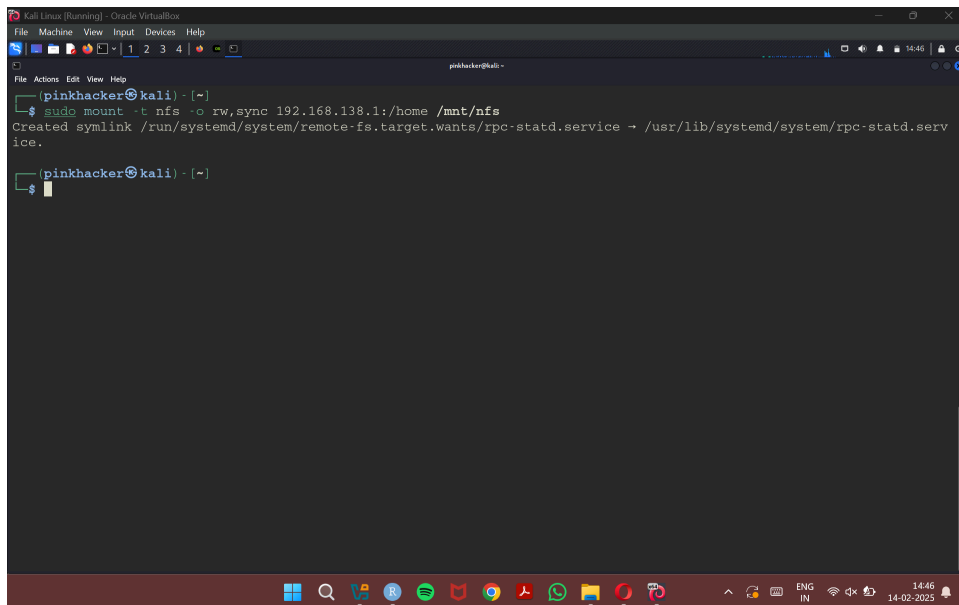
## 4. Modifying the /etc/fstab in Kali Linux



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 7.2 /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sdal during installation
UUID=2d60c8fc-f207-4d32-8ccd-2cf4c468a804 / ext4 errors=remount-ro 0 1
# swap was on /dev/sda5 during installation
UUID=0efab105-91b3-4612-b897-59a311d3b369 none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0
192.168.138.1:/home /mnt/nfs nfs rw,sync,no_root_squash 0 0
  
```

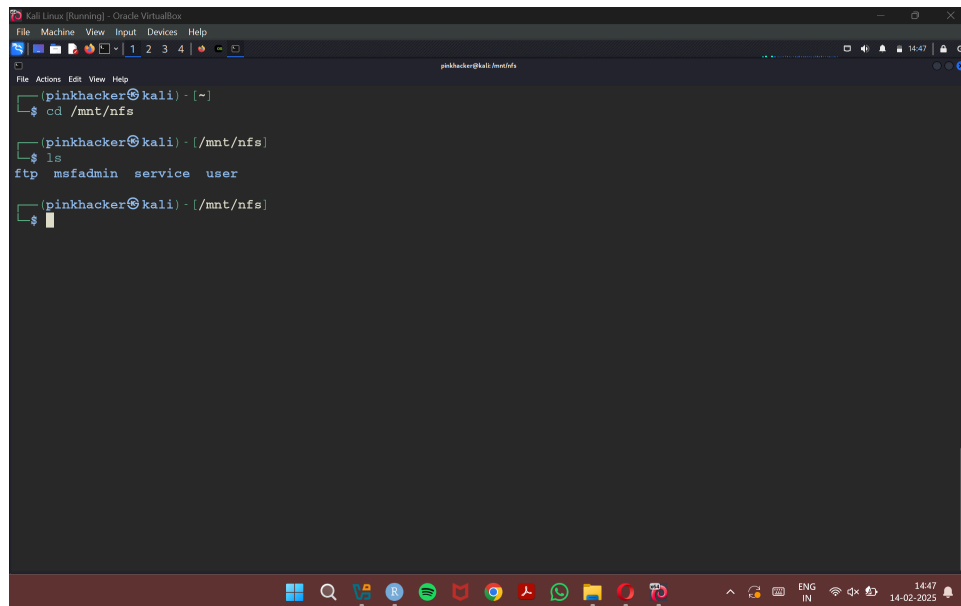
## 5. Mounting the NFS in Kali Linux



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
(pinkhacker@kali) ~
$ sudo mount -t nfs -o rw,sync 192.168.138.1:/home /mnt/nfs
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /usr/lib/systemd/system/rpc-statd.service.
(pinkhacker@kali) ~
$
  
```

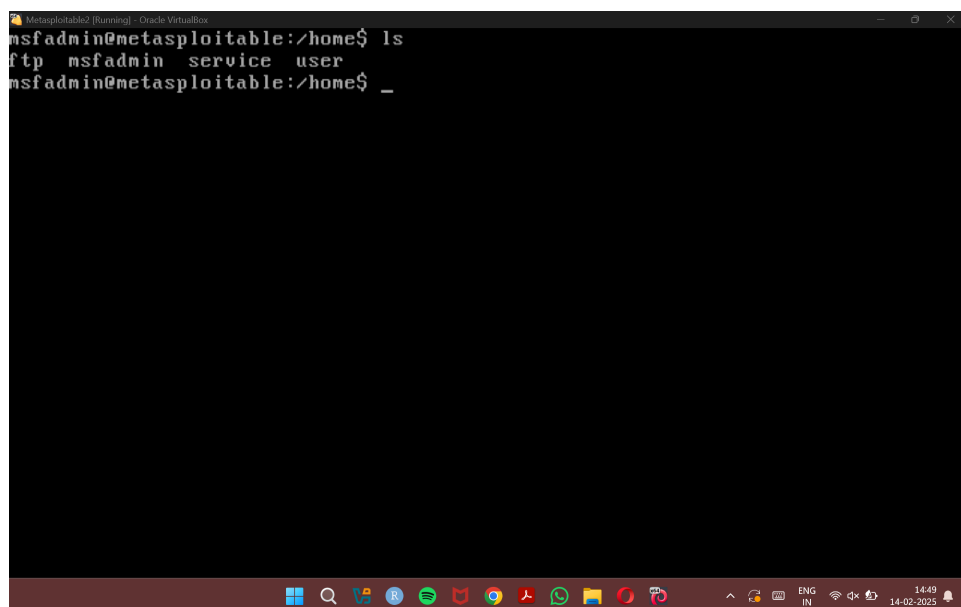
## 6. Locating the Metasploitable2 under /mnt/nfs in Kali Linux



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pinkhacker@kali: ~
$ cd /mnt/nfs

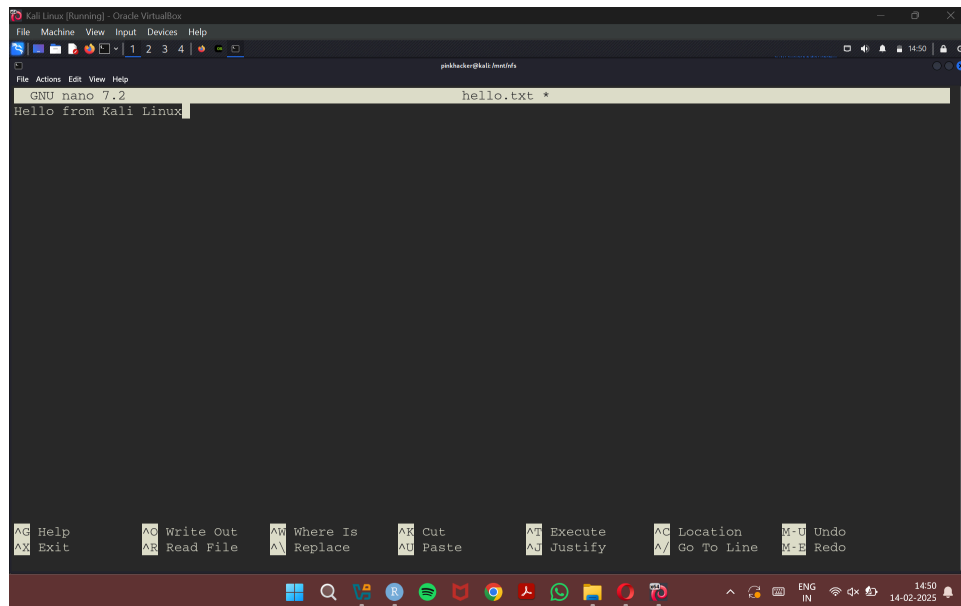
(pinkhacker@kali) - [/mnt/nfs]
$ ls
ftp  msfadmin  service  user

(pinkhacker@kali) - [/mnt/nfs]
$
```

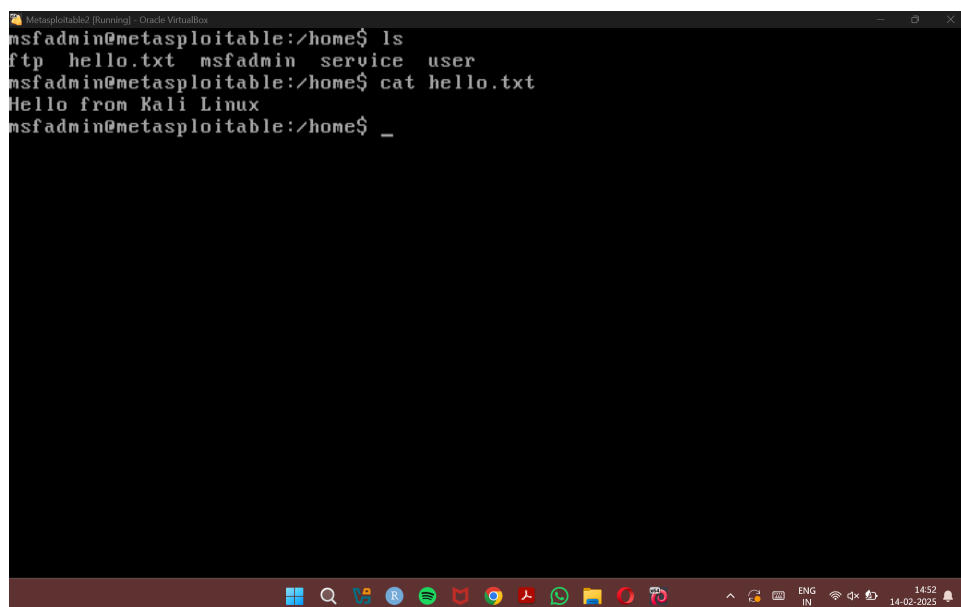


```
Metasploitable2 [Running] - Oracle VM VirtualBox
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ _
```

## 7. Creating a file in Kali Linux which will in parallel create the same in Metasploitable2



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
GNU nano 7.2 hello.txt *
Hello from Kali Linux
```



```
Metasploitable2 [Running] - Oracle VM VirtualBox
msfadmin@metasploitable:/home$ ls
ftp hello.txt msfadmin service user
msfadmin@metasploitable:/home$ cat hello.txt
Hello from Kali Linux
msfadmin@metasploitable:/home$ _
```