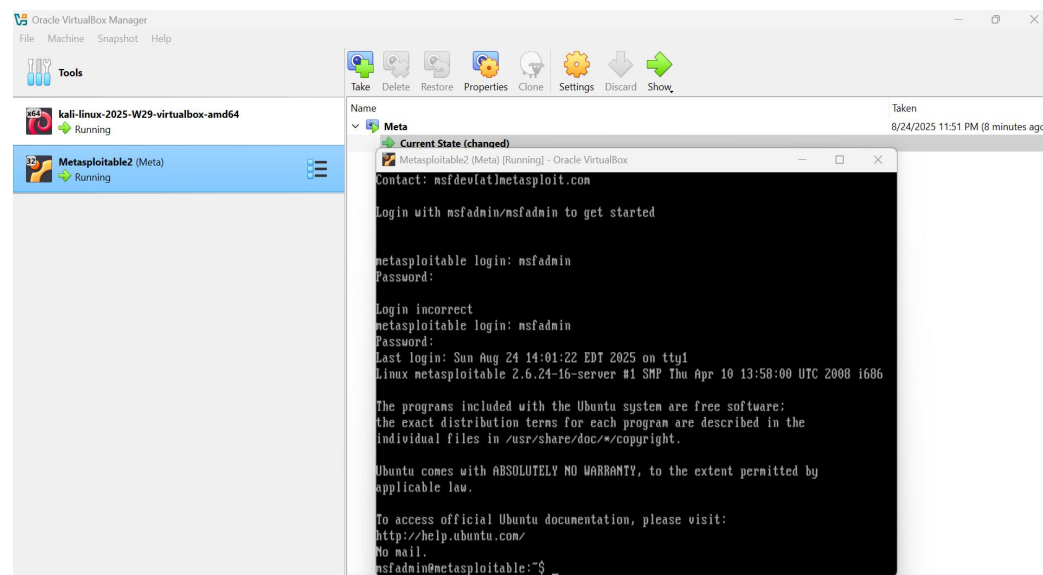


1. Metasploitable is successfully hosted inside Oracle VirtualBox



2. Created a File on Kali as Transfer.txt

There are different ways to create a file in Kali Linux:

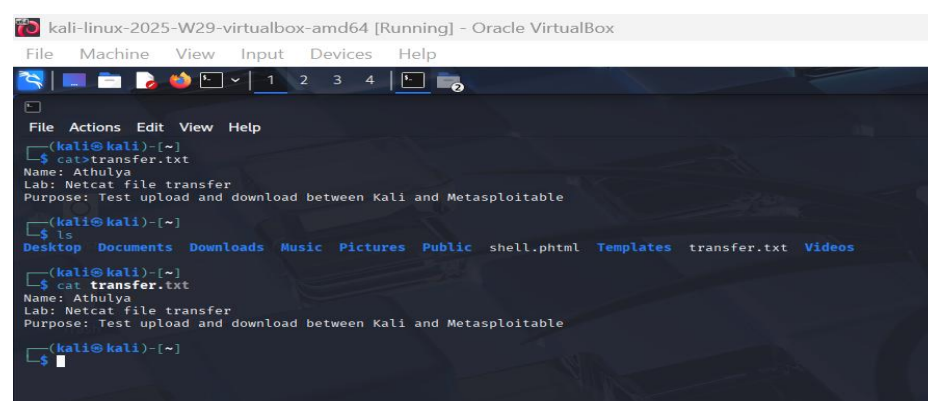
- ❖ Using the **echo** command – This allows us to create a file and directly insert text into it.
- ❖ Using the **touch** command – This simply creates an empty file.
- ❖ Using the **cat** command – This lets us create a file and type multiple lines of content. We finish by pressing CTRL+D.
- ❖ Using a text editor like **nano** – This opens a text editor inside the terminal. We can type content, then save and exit.

I used cat command

Cat>transfer.txt

Used **ctrl+D** for save & exit Listed files in kali using command **ls**

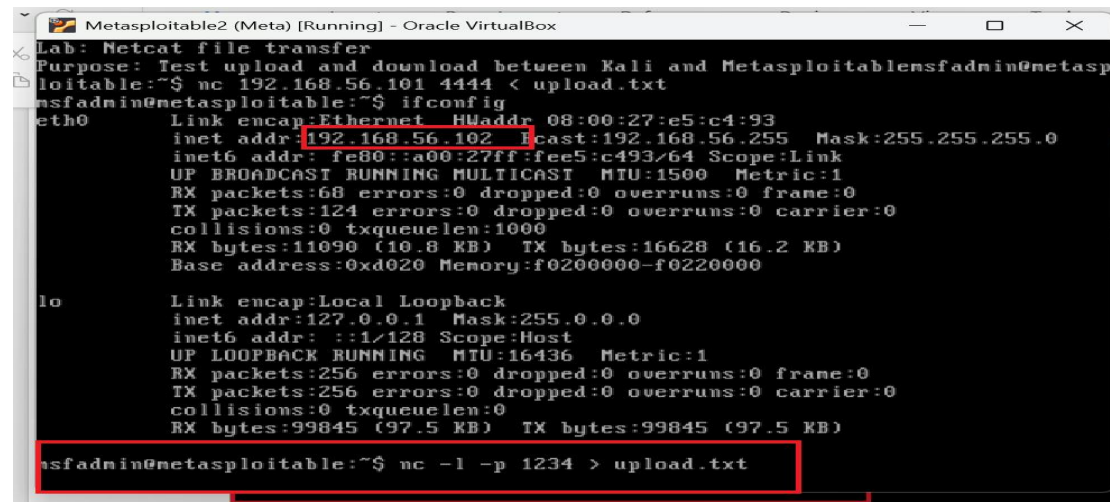
Listed entire content of the file using **cat transfer.txt**



3. Using Netcat – Uploading a File to Metasploitable and Downloading it Back to Kali

- Setting metasploitable to listening mode :

nc -l -p 1234 > upload.txt



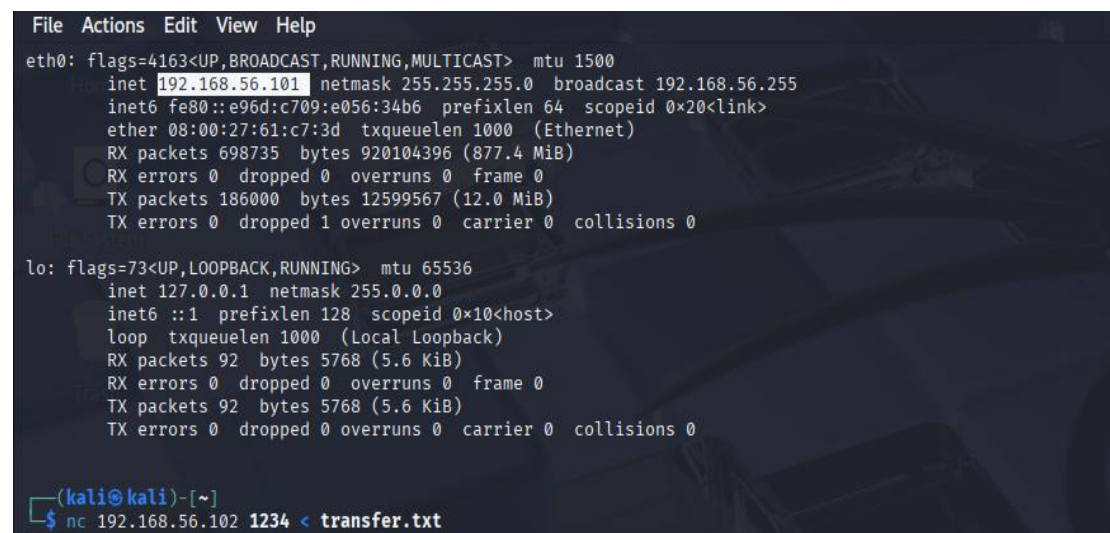
```
Metasploitable2 (Meta) [Running] - Oracle VirtualBox
Lab: Netcat file transfer
Purpose: Test upload and download between Kali and Metasploitable
nsfadmin@metasploitable:~$ nc 192.168.56.101 4444 < upload.txt
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:c4:93
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:c493/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68  errors:0  dropped:0  overruns:0  frame:0
          TX packets:124  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:11090 (10.8 KB)  TX bytes:16628 (16.2 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:256  errors:0  dropped:0  overruns:0  frame:0
          TX packets:256  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:99845 (97.5 KB)  TX bytes:99845 (97.5 KB)

nsfadmin@metasploitable:~$ nc -l -p 1234 > upload.txt
```

- Send File from Kali to Metasploitable

nc 192.168.56.102 1234 < transfer.txt



```
File Actions Edit View Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
      inet6 fe80::e96d:c709:e056:34b6 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:61:c7:3d txqueuelen 1000 (Ethernet)
      RX packets 698735 bytes 920104396 (877.4 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 186000 bytes 12599567 (12.0 MiB)
      TX errors 0 dropped 1 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 92 bytes 5768 (5.6 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 92 bytes 5768 (5.6 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nc 192.168.56.102 1234 < transfer.txt
```

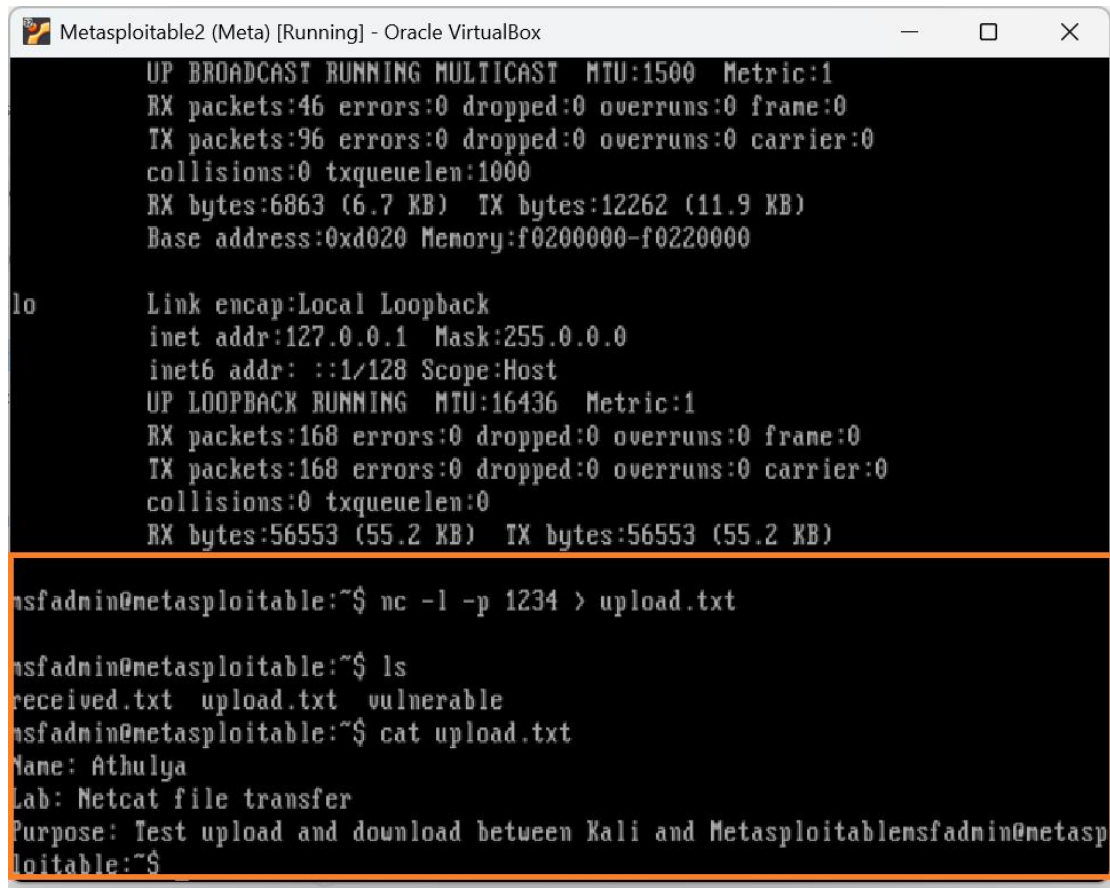
- 192.168.56.102 → Metasploitable IP
- 1234 → port matching the listener
- < transfer.txt → sends file content

- **Verify Upload on Metasploitable**

Cntrl+C

ls

cat upload.txt



```
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:46 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6863 (6.7 KB) TX bytes:12262 (11.9 KB)
Base address:0xd020 Memory:f0200000-f0220000

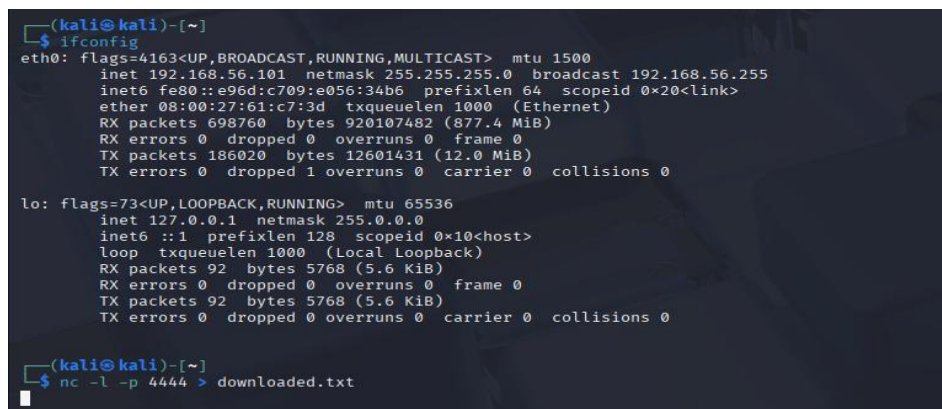
lo:
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:168 errors:0 dropped:0 overruns:0 frame:0
TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:56553 (55.2 KB) TX bytes:56553 (55.2 KB)

nsfadmin@metasploitable:~$ nc -l -p 1234 > upload.txt

nsfadmin@metasploitable:~$ ls
received.txt upload.txt vulnerable
nsfadmin@metasploitable:~$ cat upload.txt
Name: Athulya
Lab: Netcat file transfer
Purpose: Test upload and download between Kali and Metasploitable
nsfadmin@metasploitable:~$
```

- **Prepare Kali to Receive File Back (Download)**

nc -l -p 4444 > downloaded.txt



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::e96d:c709:e056:34b6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:61:c7:3d txqueuelen 1000 (Ethernet)
    RX packets 698760 bytes 920107482 (877.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 186020 bytes 12601431 (12.0 MiB)
    TX errors 0 dropped 1 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 92 bytes 5768 (5.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 92 bytes 5768 (5.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nc -l -p 4444 > downloaded.txt
```

- **Send File Back from Metasploitable to Kali**

nc 192.168.56.101 4444 < received.txt

```
RX bytes:56553 (55.2 KB) TX bytes:56553 (55.2 KB)

msfadmin@metasploitable:~$ nc -l -p 1234 > upload.txt

msfadmin@metasploitable:~$ ls
received.txt  upload.txt  vulnerable
msfadmin@metasploitable:~$ cat upload.txt
Name: Athulya
Lab: Netcat file transfer
Purpose: Test upload and download between Kali and Metasploitable
msfadmin@metasploitable:~$ nc 192.168.56.101 4444 < upload.txt
```

- **Verify download on kali**

Cntrl+C

ls

cat upload.txt

```
(kali@kali)-[~]
└─$ nc -l -p 4444 > downloaded.txt
^C

(kali@kali)-[~]
└─$ ls
1234 Desktop Documents downloaded.txt Downloads Music Pictures Public shell.phtml Templates transfer.txt Videos

(kali@kali)-[~]
└─$ cat downloaded.txt
Name: Athulya
Lab: Netcat file transfer
Purpose: Test upload and download between Kali and Metasploitable

(kali@kali)-[~]
└─$
```