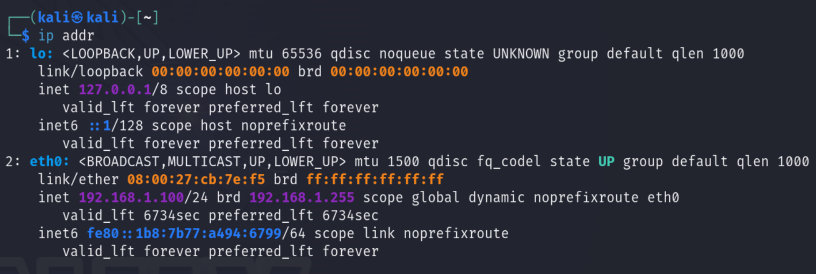
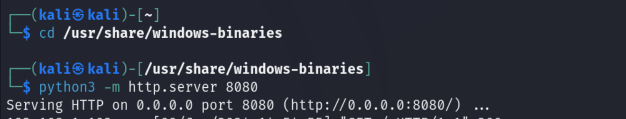
**Working with Bind & Reverse Shells**

# Section 1: Remote Shells using NetCat

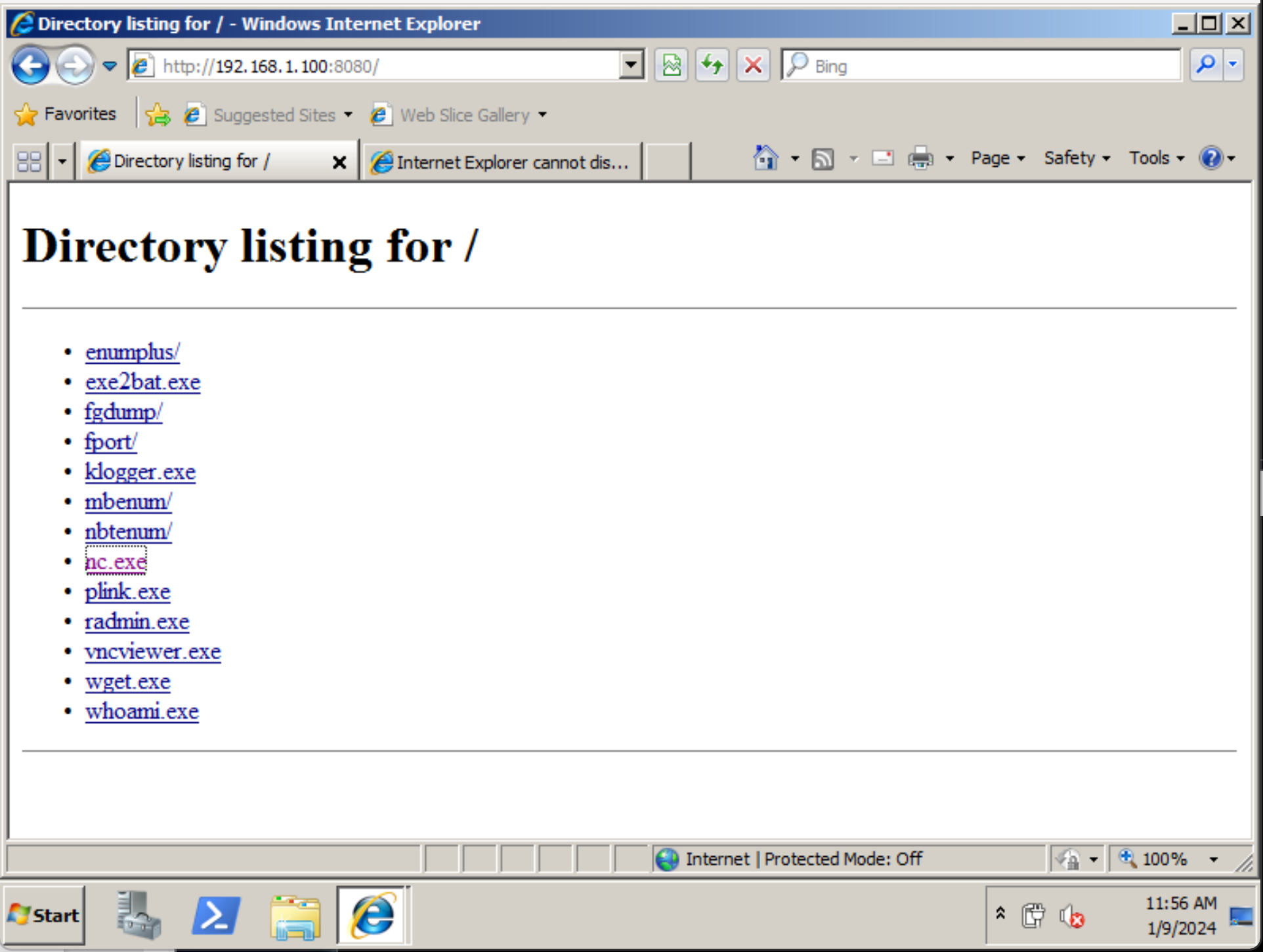
**Step 1:** Use the “ip addr” command to obtain its IP address on eth0.



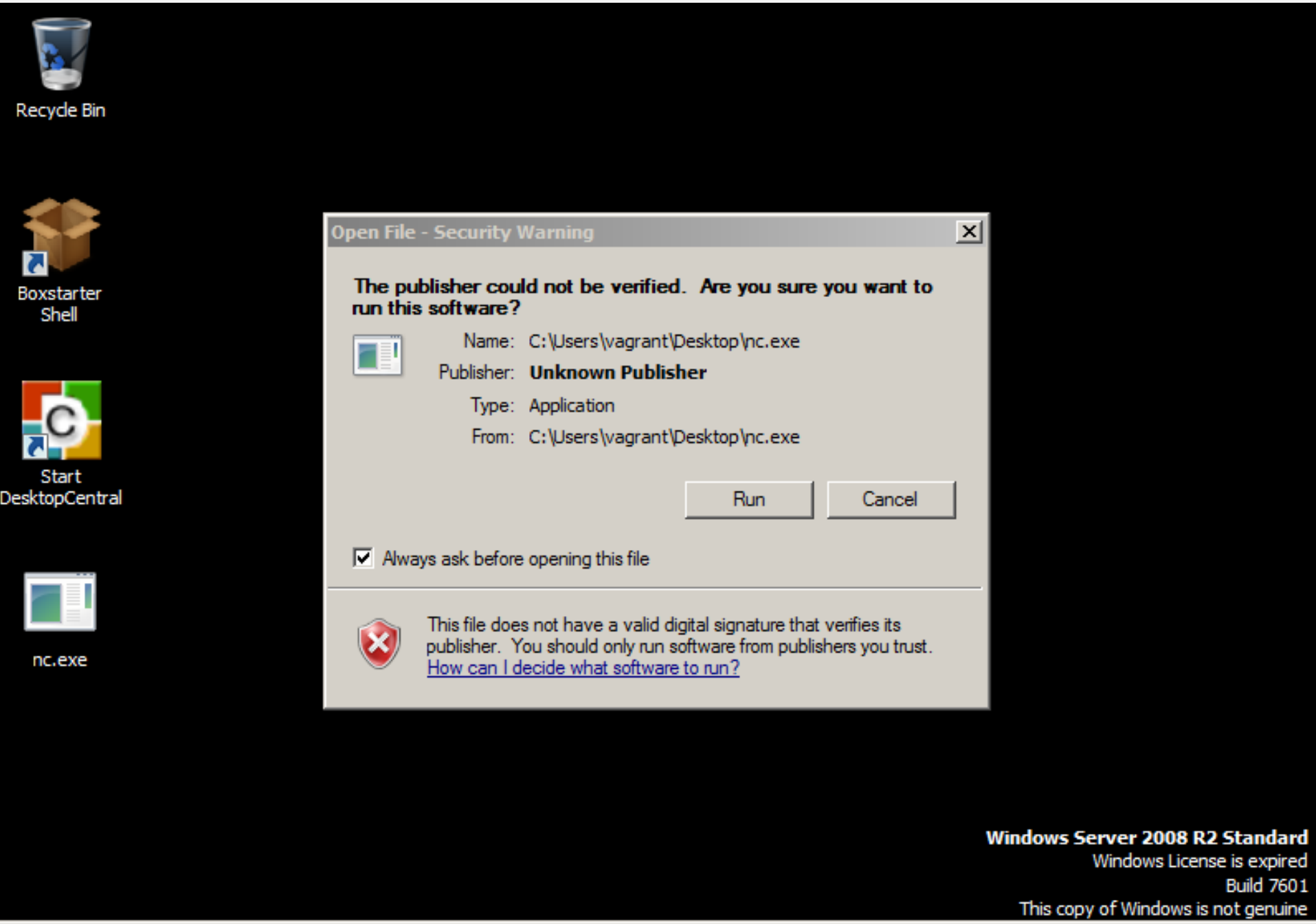
**Step 2:** Copy the Windows version of Netcat over to Metasploitable 3.



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



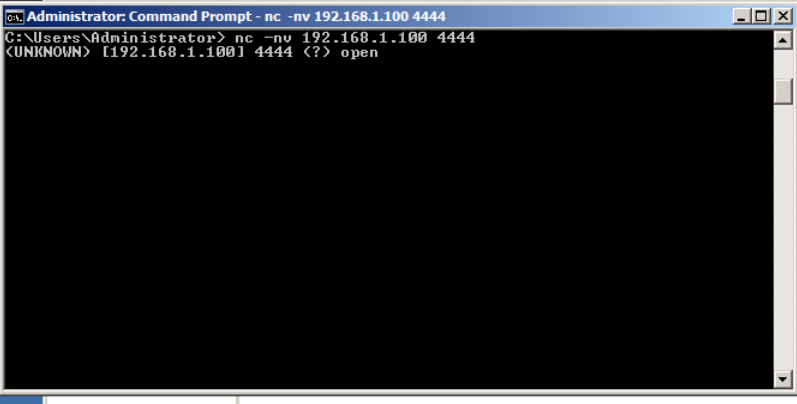
**Step 4:** Download the nc.exe file from Kali Linux.

****

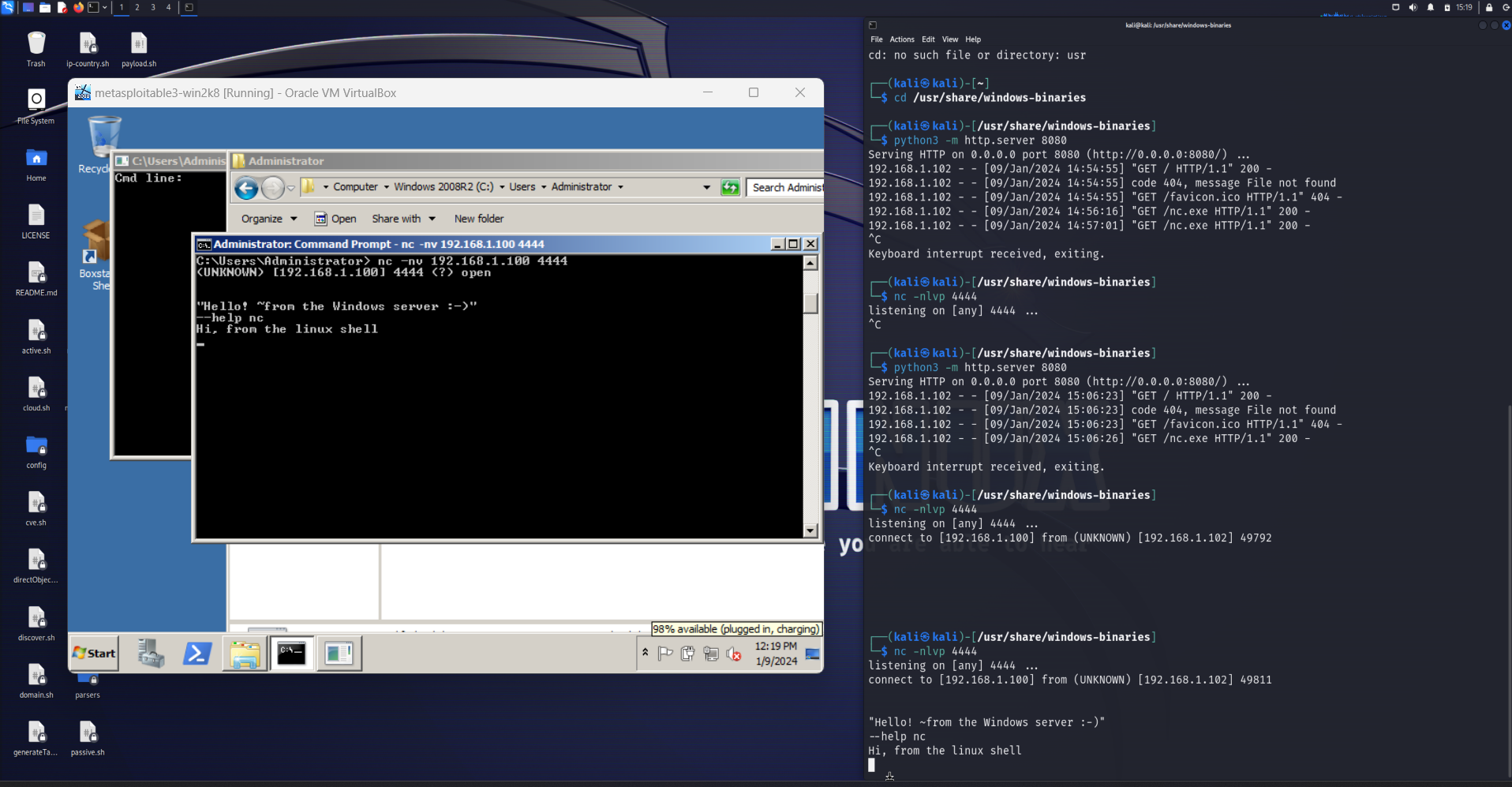
**Step 5:** Start a listener (server) on Kali Linux.

****

**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.

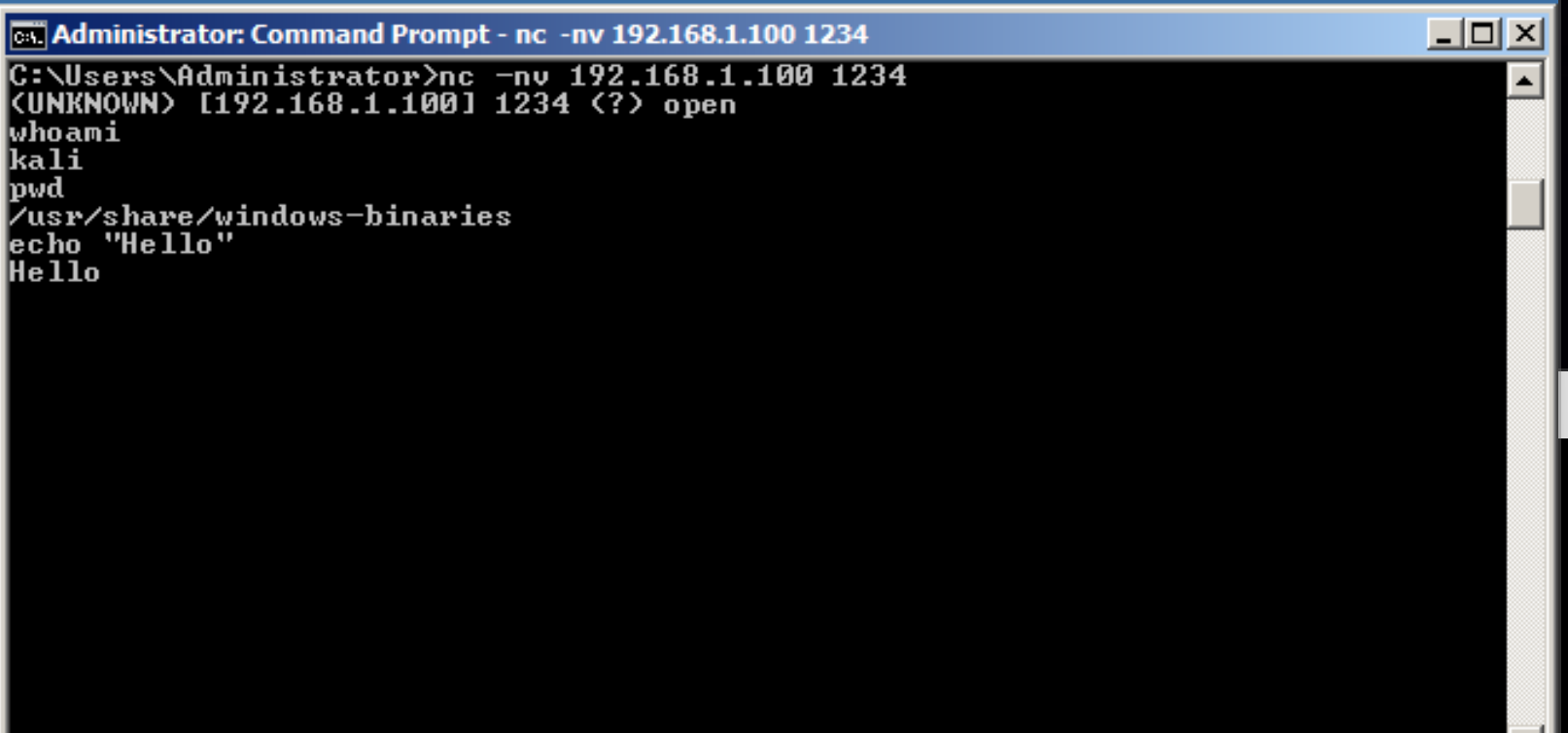


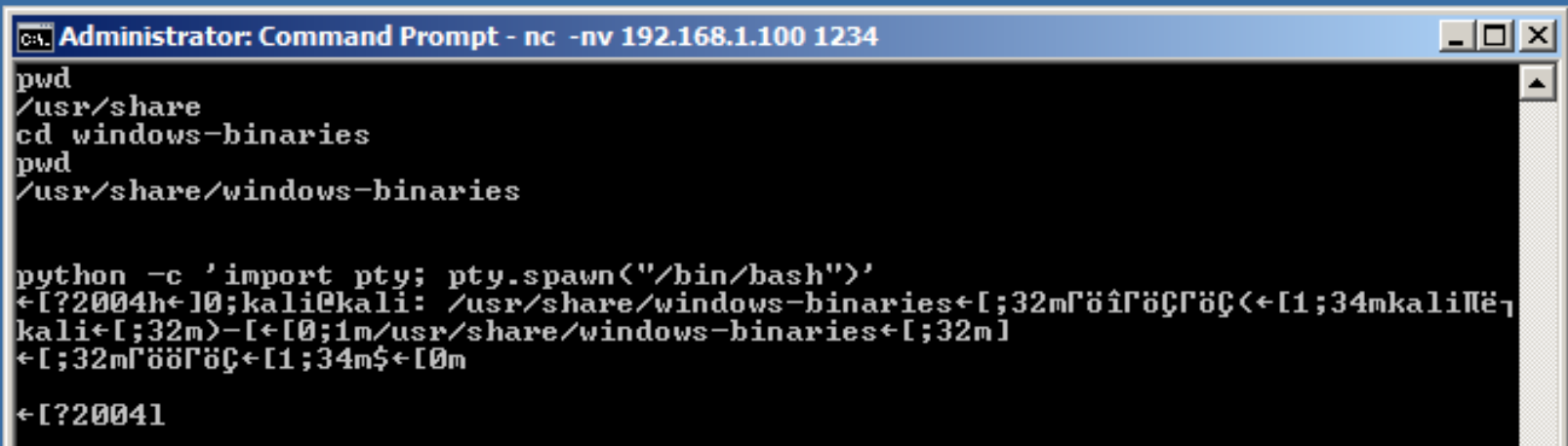
# Section 2: Creating a Bind Shell

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

****

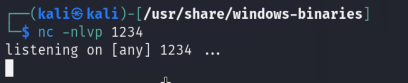
**Step 2:** Open the Windows Command Prompt and establish a Netcat connection to Kali Linux (listener).

****

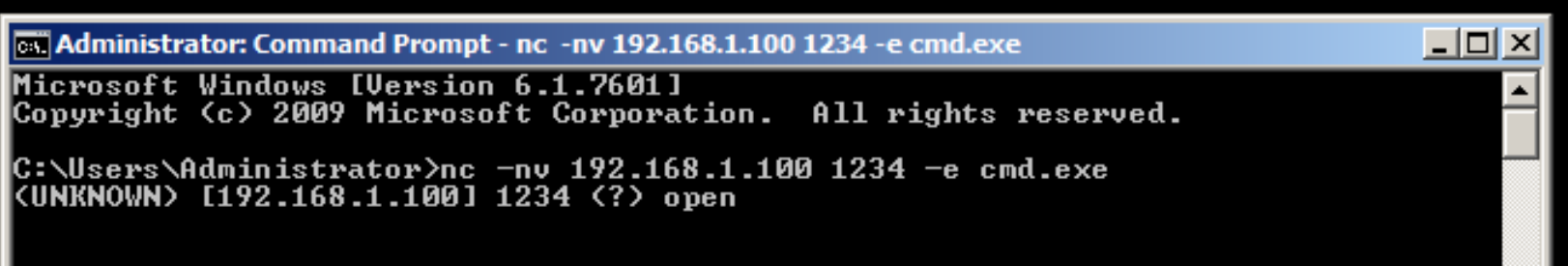
**Step 3:** Execute Linux-based commands from the Windows Command Prompt.****

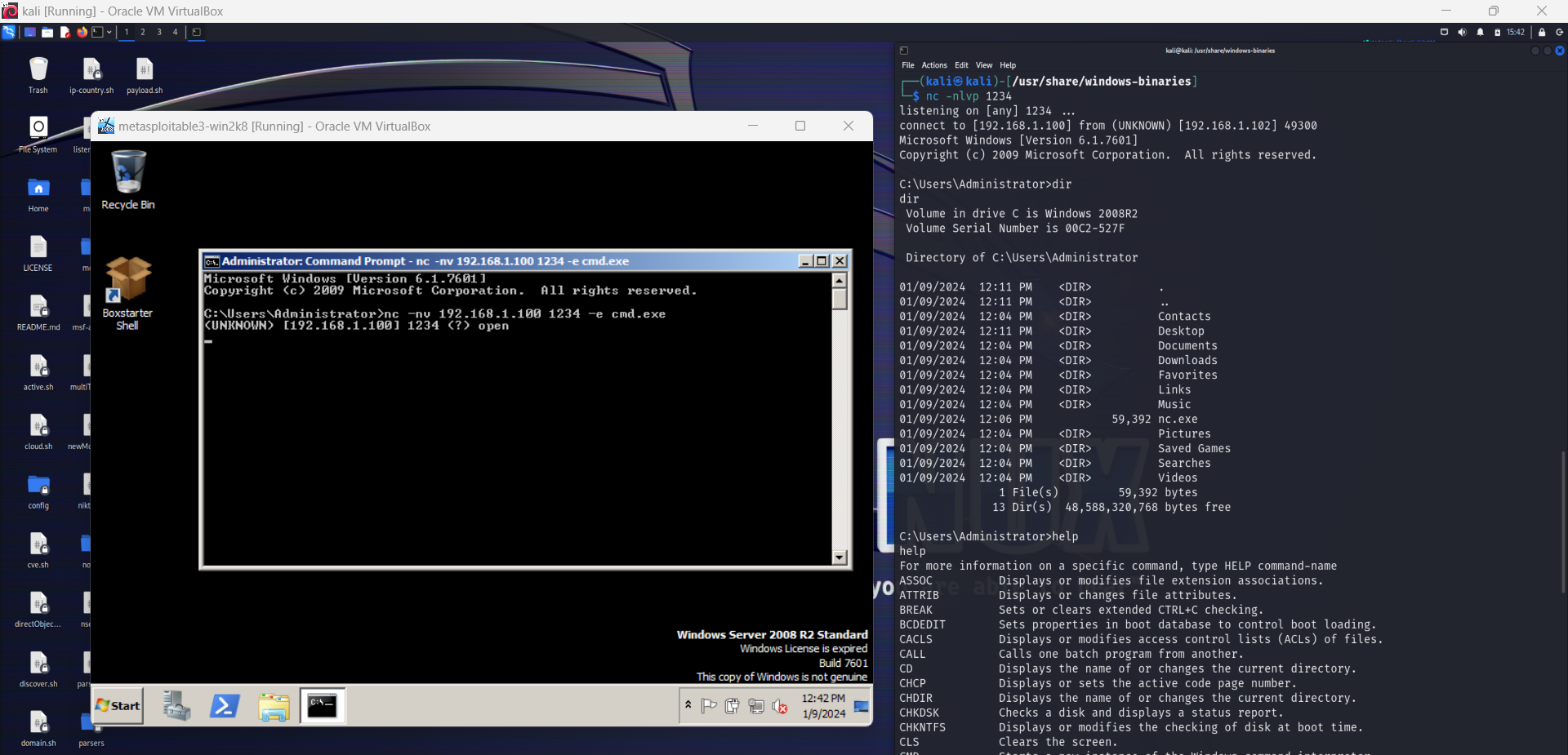
# Section 3: Creating a Reverse Shell

**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.

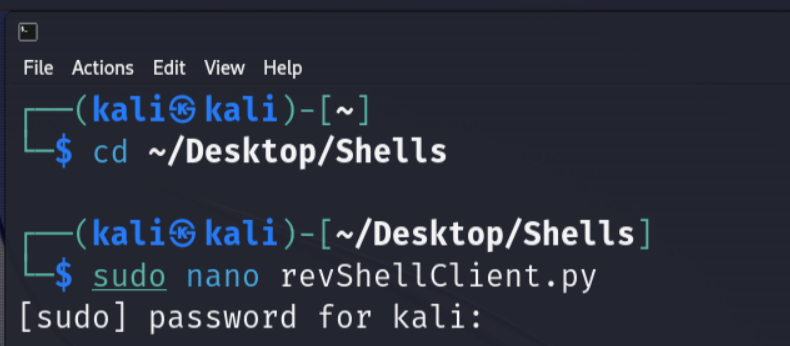
****

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

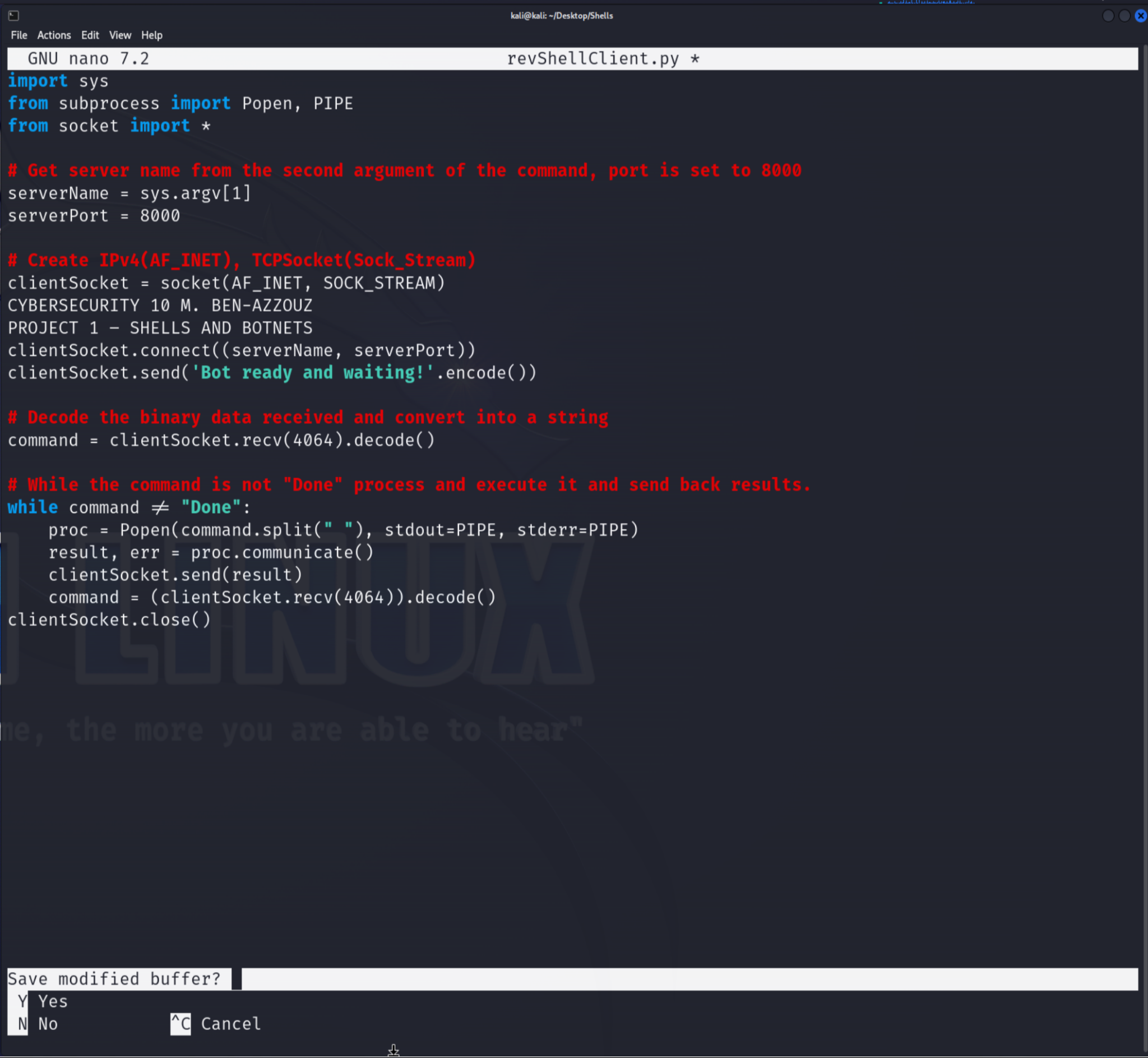
**Crafting Your Own Reverse Shell**

# Section 1: Writing a Reverse Shell Client

**Step 1:** Create a Python file using Nano:

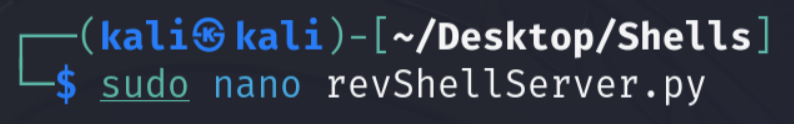


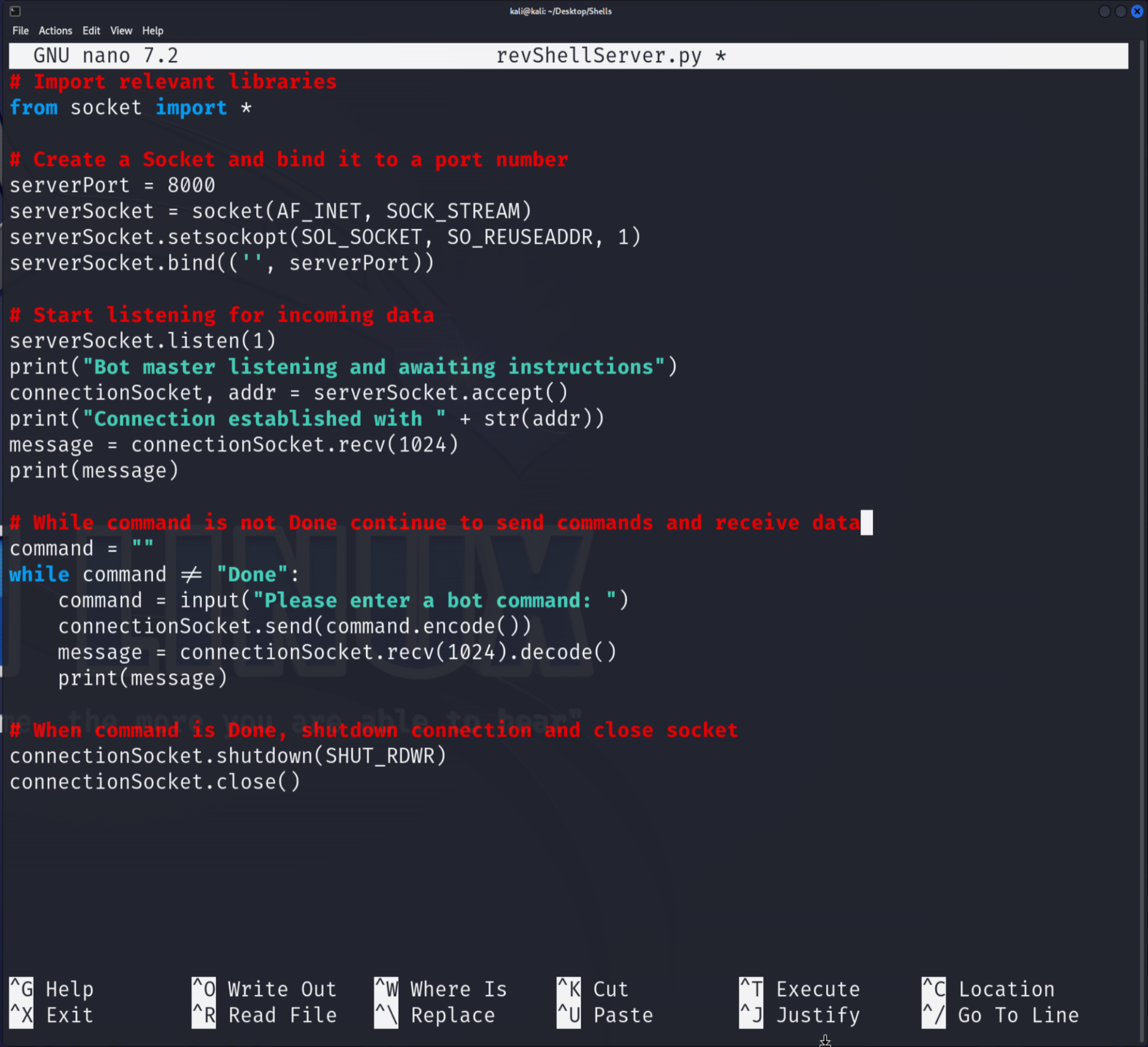
**Step 2:** Add the Python code to the nano program.

****

# Section 2: Writing a TCP Server (Listener)

**Step 1:** Create a Python file using Nano:

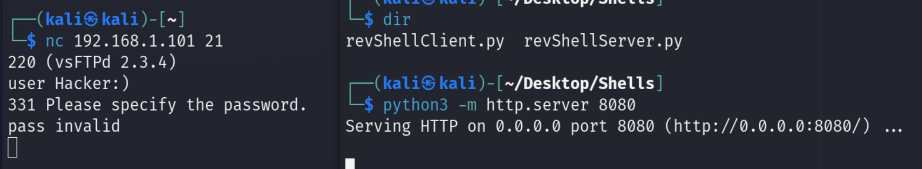


**Step 2:** Add the Python code to the nano program.

# Section 3: Load Reverse Shell onto the Target

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

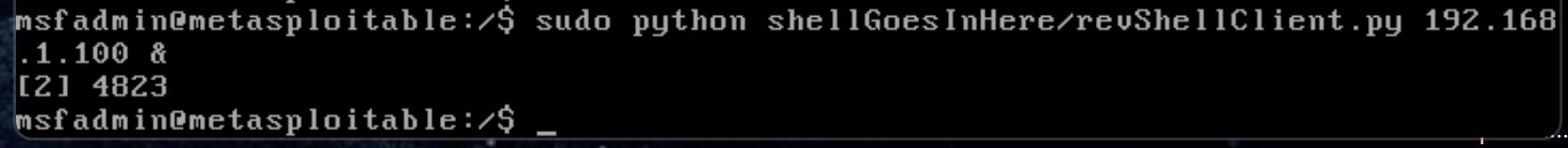
****

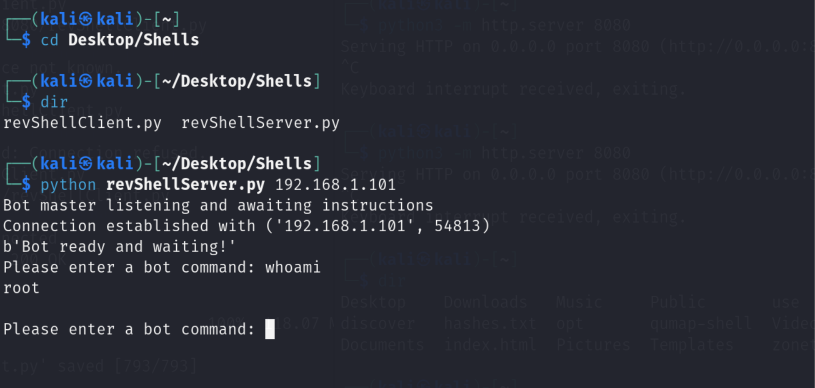
****

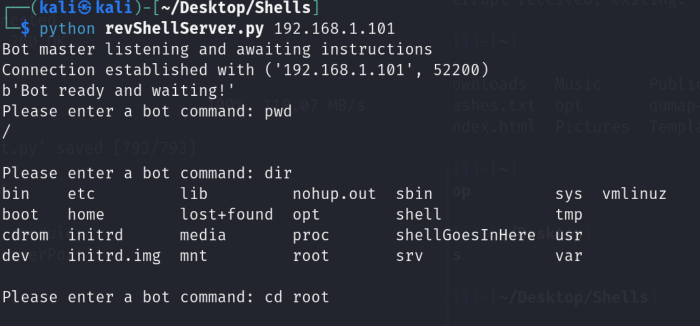
**Step 2:** Create a folder on the Metasploitable device and send the Python file to that device.

****

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

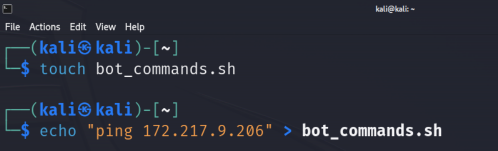
****

****

****

# Section 4: Botnets

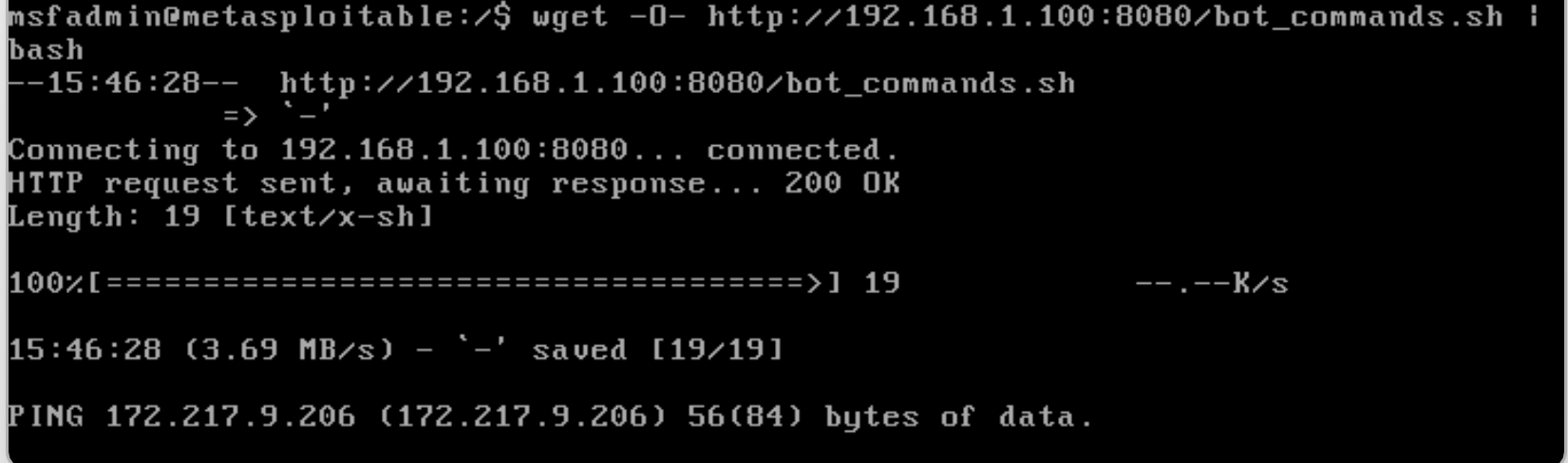
**Step 1:** Create a file and insert the text “ping 172.217.9.206” in the file.



**Step 2:** Create a bot client.

****

**Step 3:** Use the client to ping a server.

****

****