Firewall Evasion Lab Report: Bypassing Firewalls using VPN

Table of Content

1. Overview

This lab report on Firewall Evasion: Bypassing Firewalls using VPN. Firewalls are a common security measure used to protect computer networks from external threats. However, these firewalls can be bypassed by attackers using various methods, such as using a Virtual Private Network (VPN). This lab report explores the concept of Firewall Evasion using VPN, and provides a practical demonstration of how to bypass firewalls using a VPN. The report provides step by step instructions for setting up a VPN connection and testing its effectiveness in bypassing a firewall.

2. Lab Tasks

2.1. Task 1: VM Setup

VM1 (VPN Client) IP address: 10.0.2.4
VM2 (VPN Server) IP address: 10.0.2.5
Target domain: telehack.com (64.13.139.230)
VirtualBox NAT Network setting as shown in the below figure (Figure. 01).

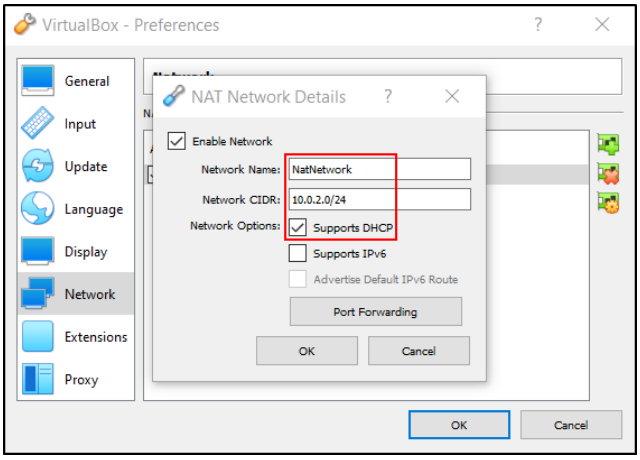

Figure. 01

Client and server network setting as shown in the below figures Figure. 02 and Figure. 03 respectively.

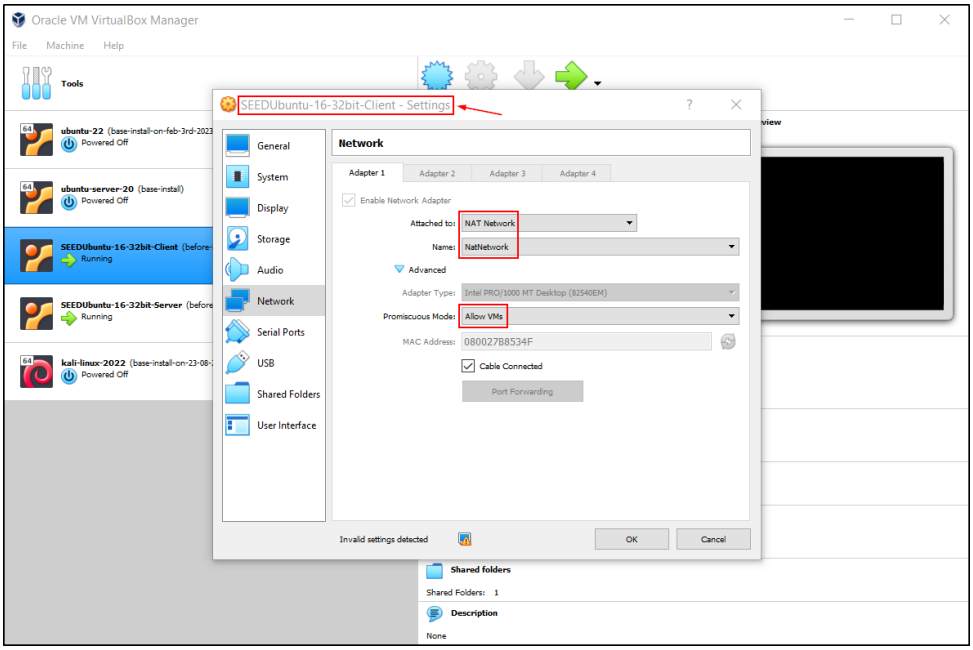

Figure. 02

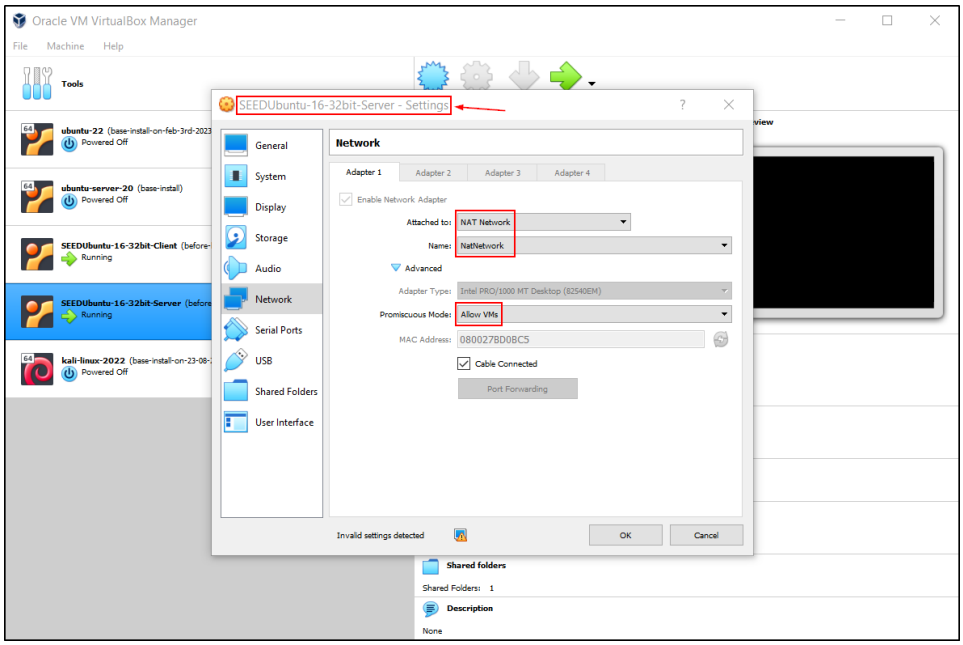

Figure. 03

Client and server ifconfig output and ping to google DNS (8.8.8.8) output as shown in the below figures Figure. 04 and Figure. 05 respectively. Client and server can reach to outside internet without any disruption.

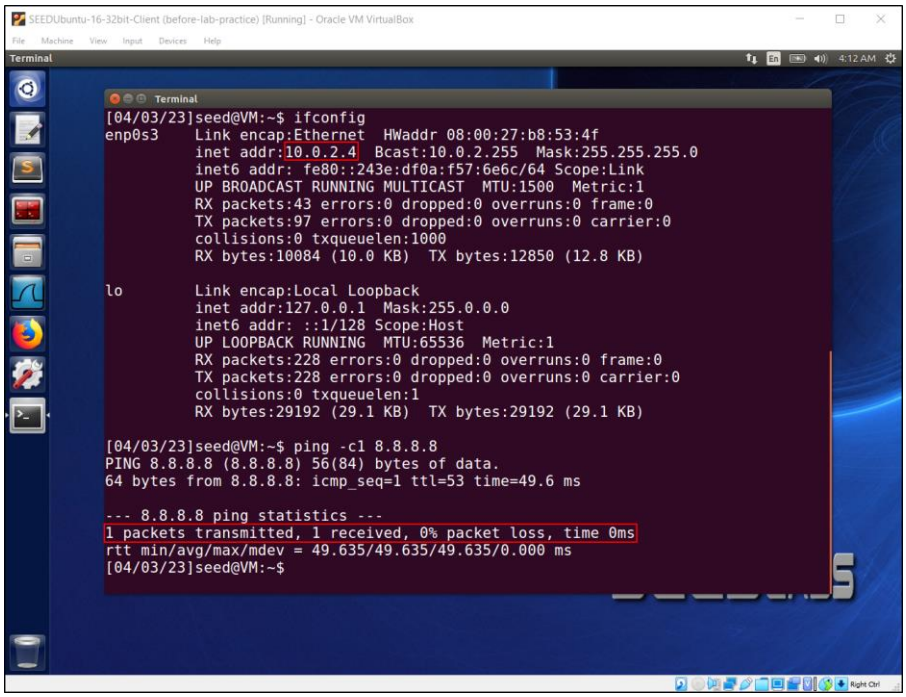

Figure. 04

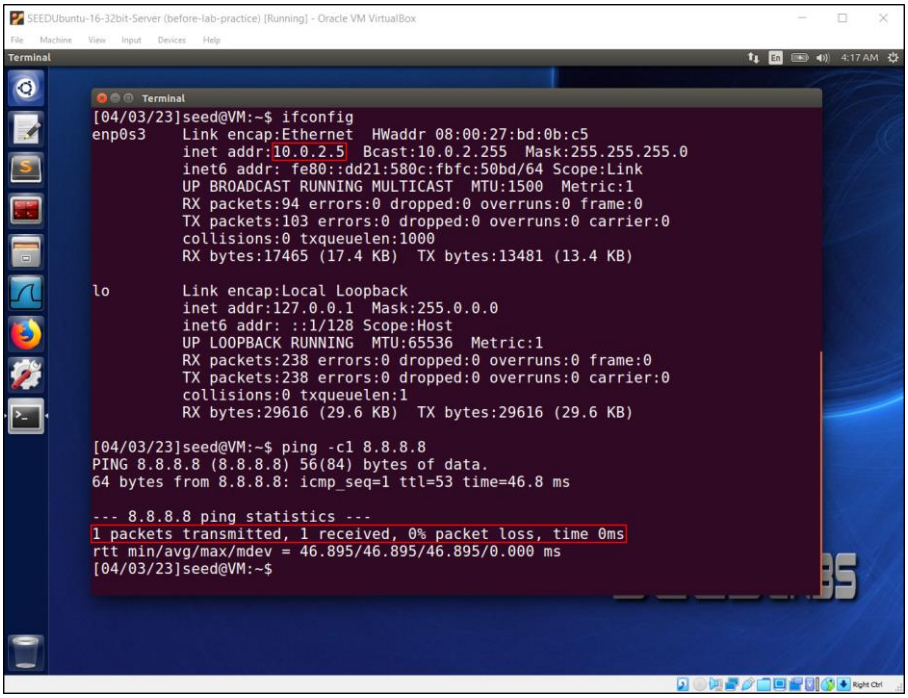

Figure. 05

Client and server can communicate (ping) each other as shown in the below figures Figure. 06 and Figure. 07 respectively.

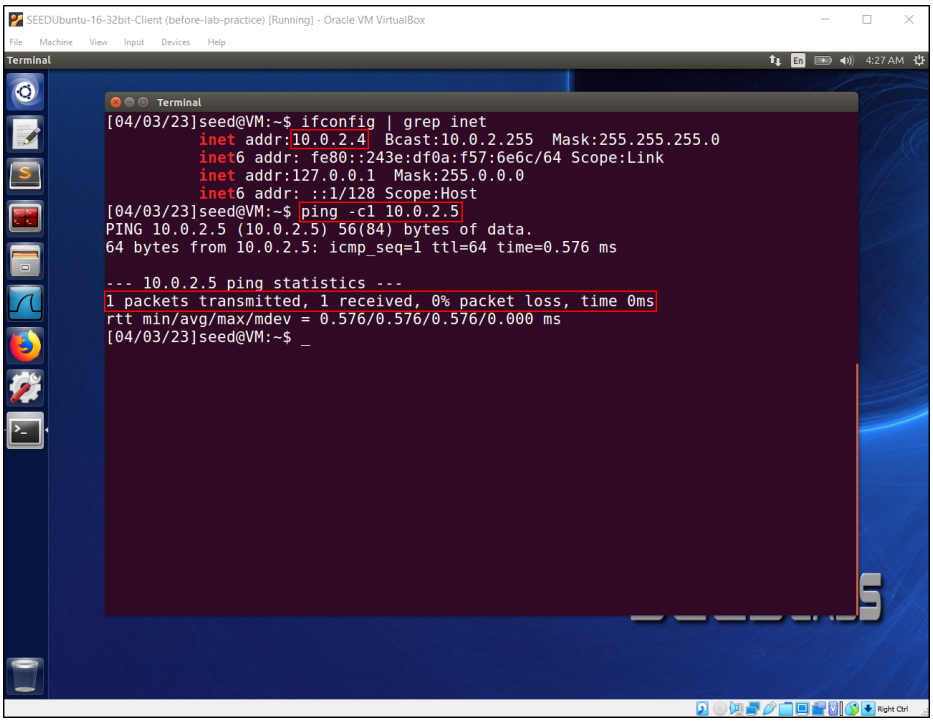

Figure. 06

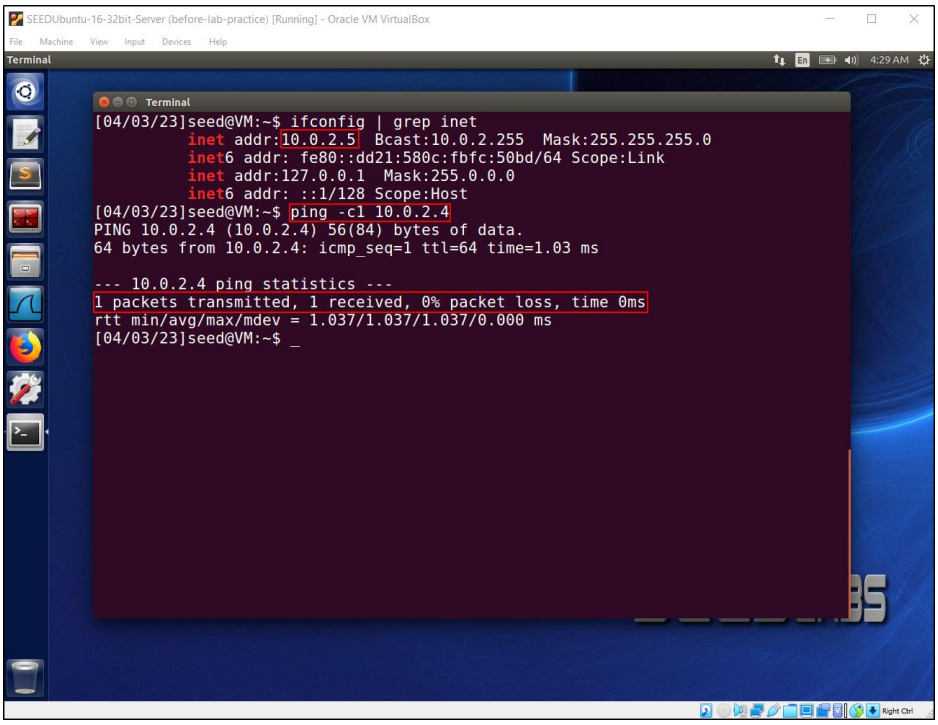

Figure. 07

Client and server communicate (ping) to telehack.com as shown in the below figures Figure. 08 and Figure. 09 respectively.

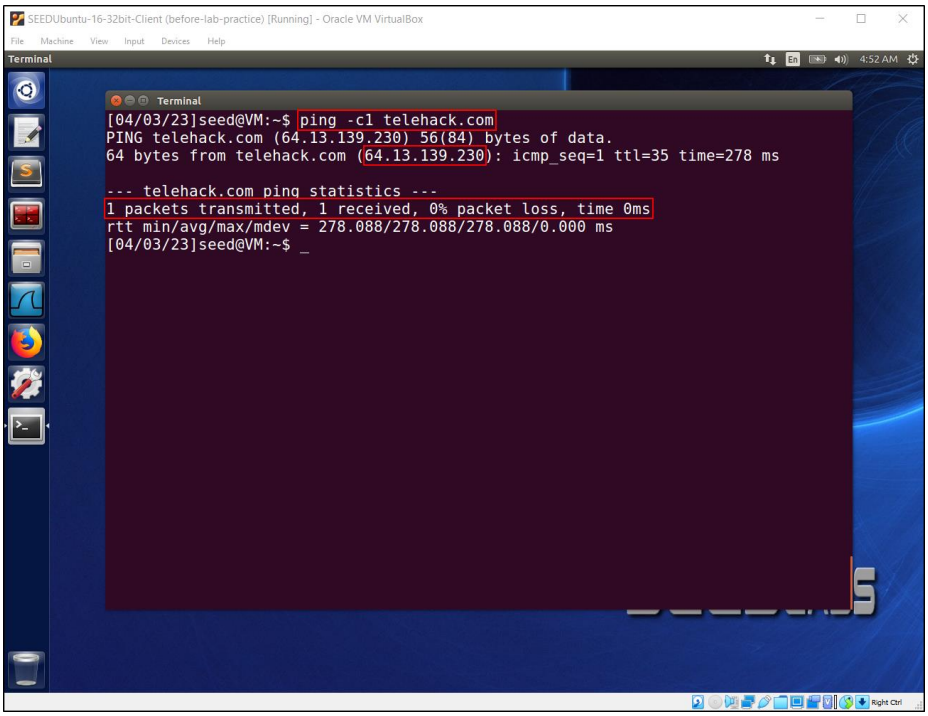

Figure. 08

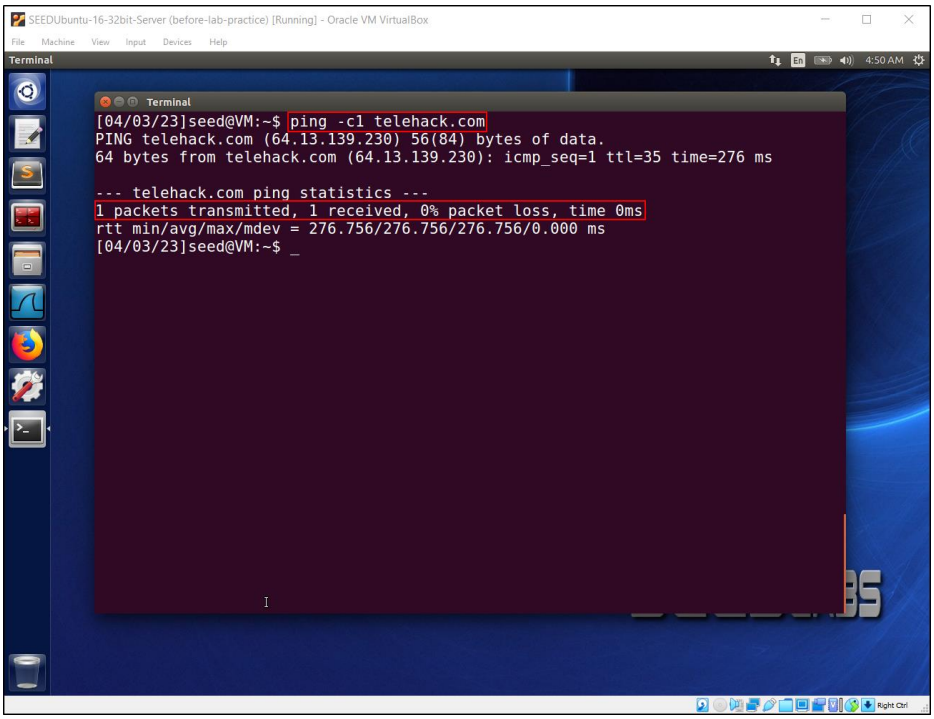

Figure. 09

2.2. Task 2: Set up Firewall

Client connection with target telehack.com via curl, ping and telnet tools with Wireshark packet capture as show in the below figures Figure. 10 and Figure. 11.

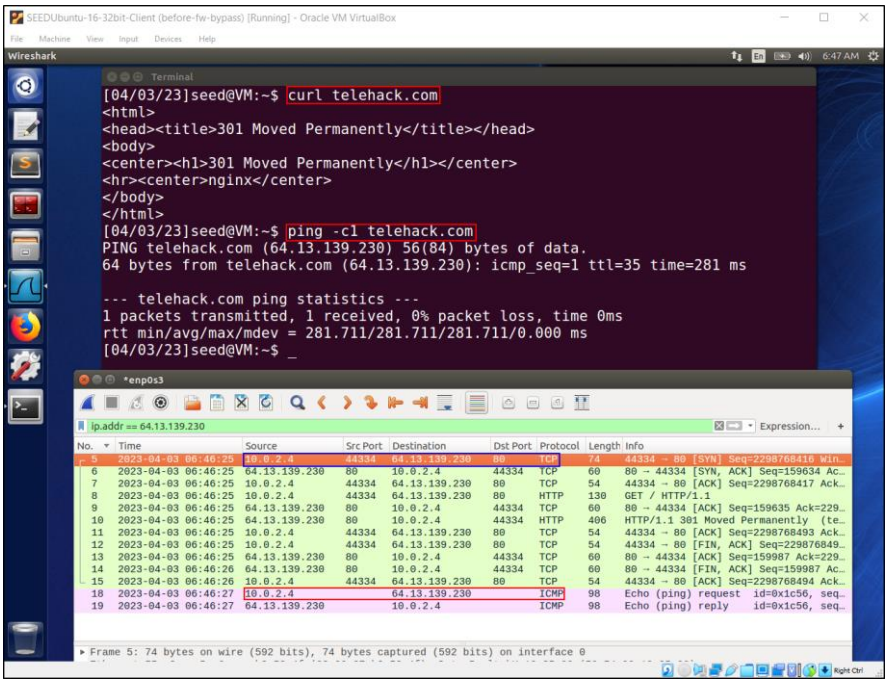

Figure. 10

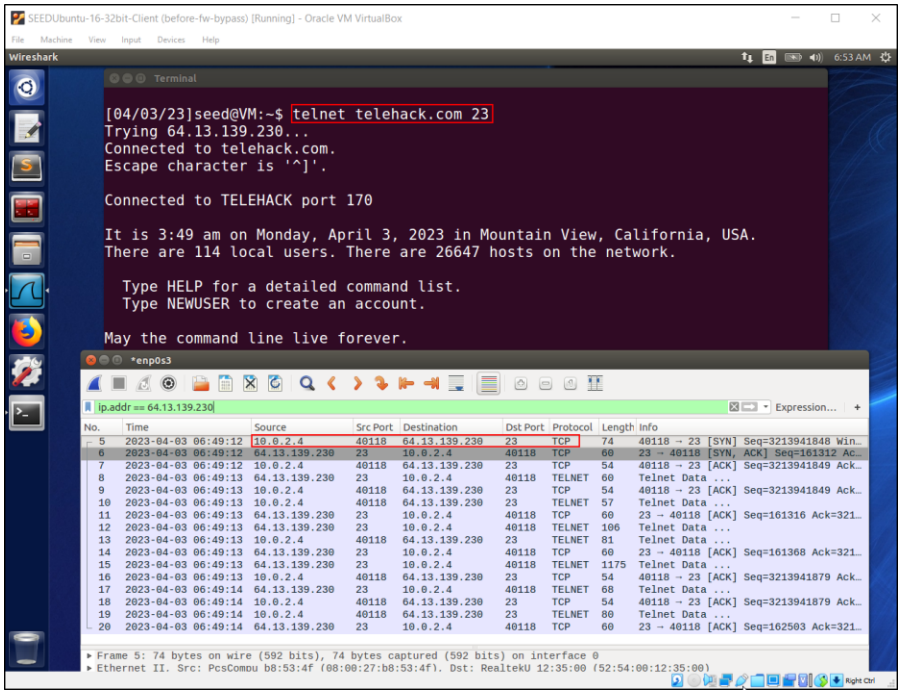

Figure. 11

Ufw tool used to set firewall rules as deny from client to access target domain telehack.com and try to connect via ping to target but 100% packet loss as shown below.

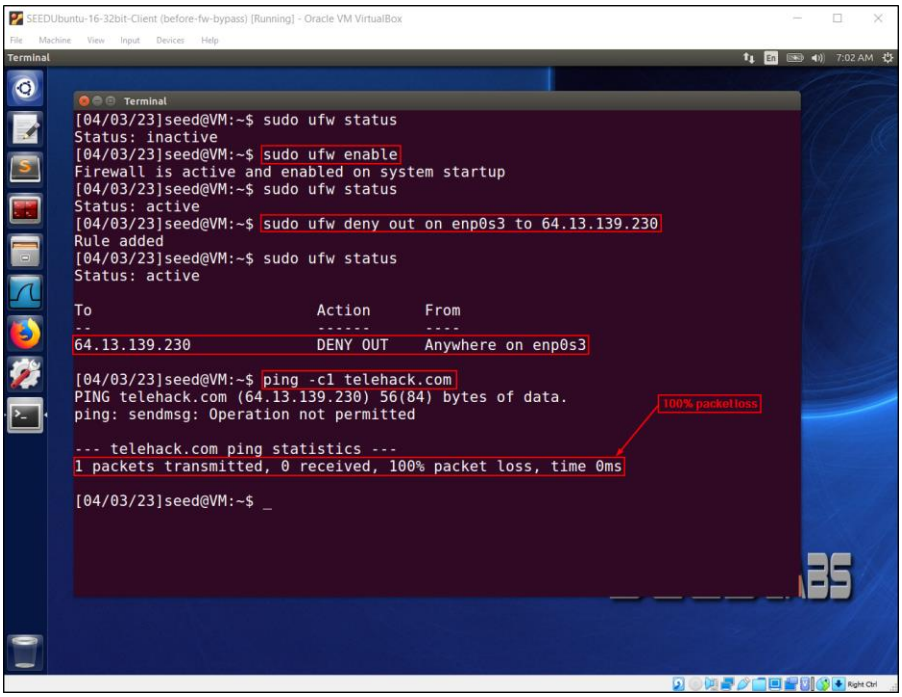

Figure. 12

Curl command used to check whether telehack.com can accessible from client or not. But network is unreachable as shown below.

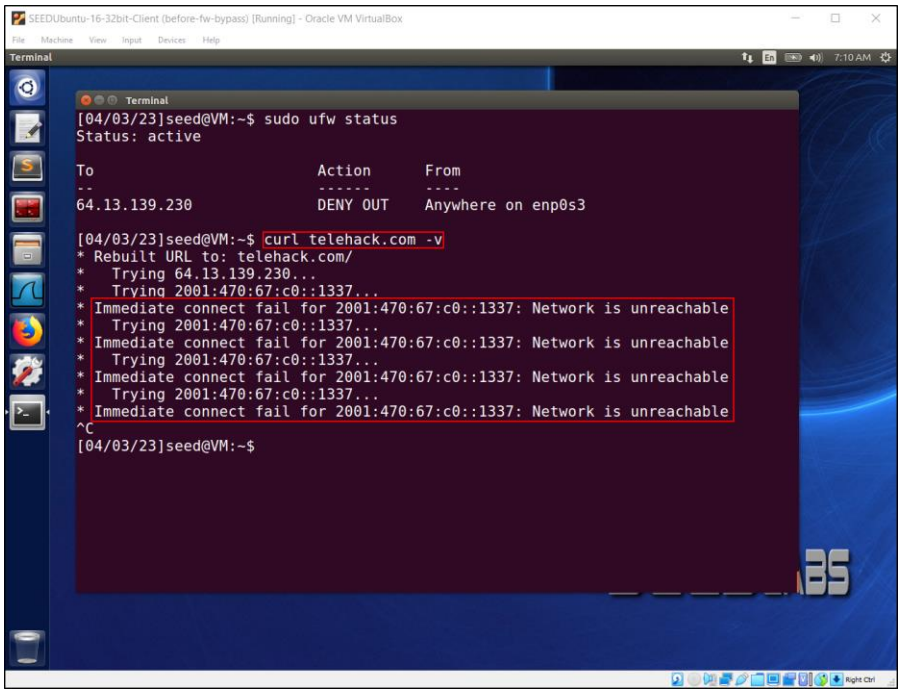

Figure. 13

2.3. Task 3: Bypassing Firewall using VPN

Step 1: Run VPN Server

Run VPN server program vpnserver.c in one terminal window on server as shown below.

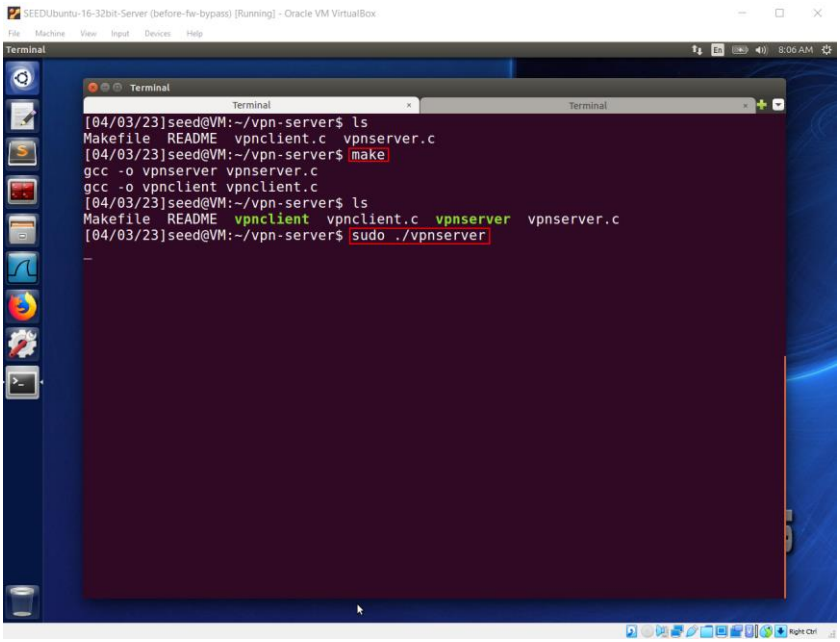

Figure. 14

While running above vpnserver.c program assign IP address 192.168.53.1 to tun0 interface in new terminal window on server as shown below.

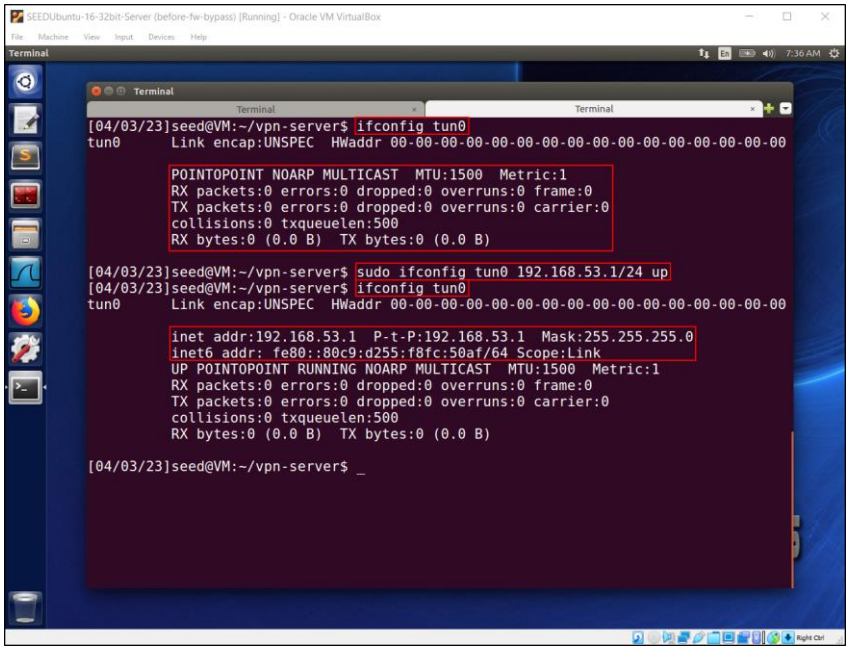

Figure. 15

Ifconfig command output on server after IP address assigned to tun0 interface as shown below.

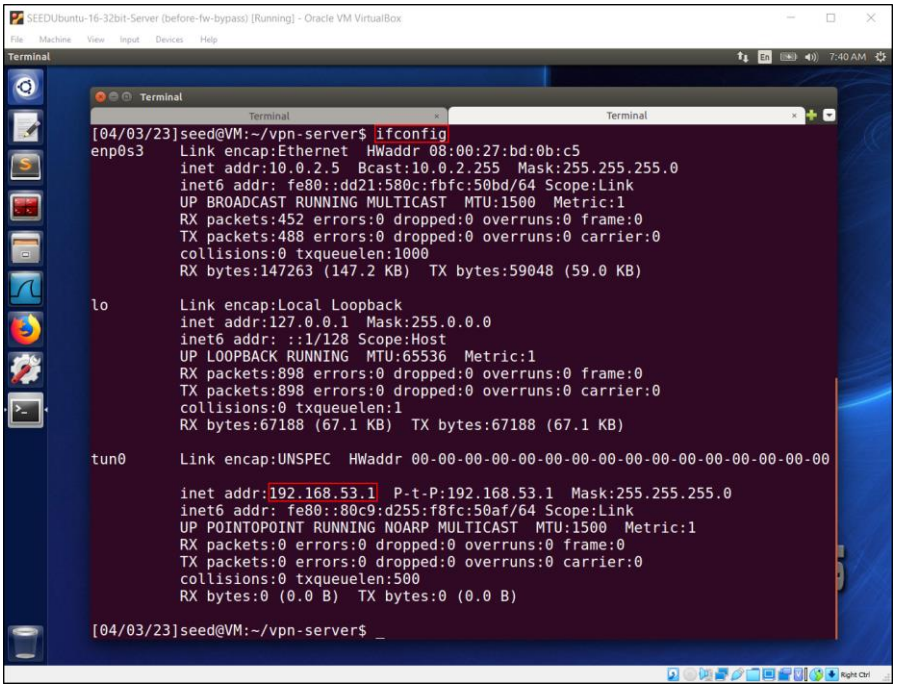

Figure. 16

IP forwarding enabled using the following command on server as shown below.

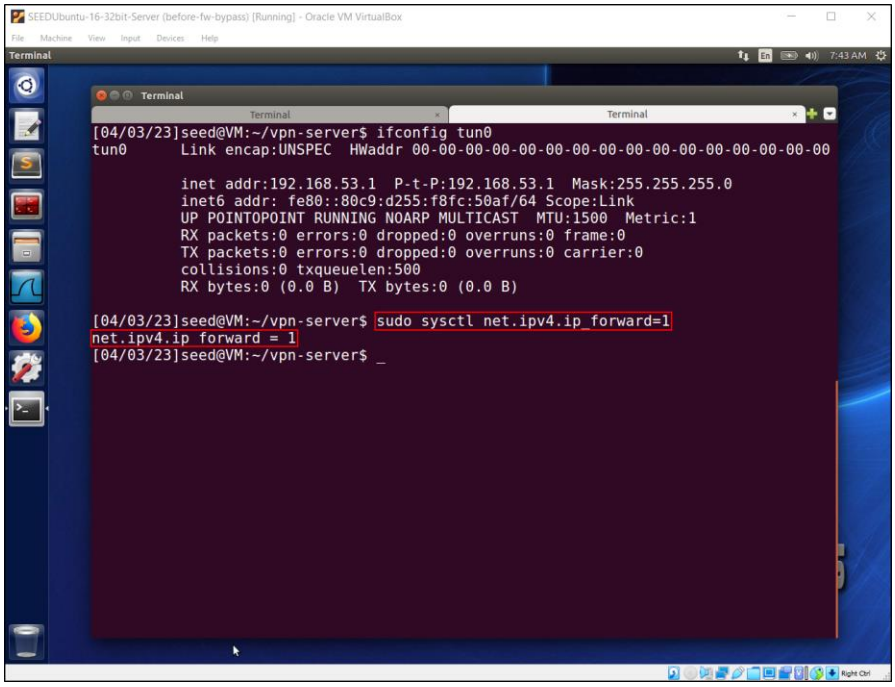

Figure. 17

Step 2: Run VPN Client

Change SERVER_IP address to server's IP address on vpnclient.c file as shown below.

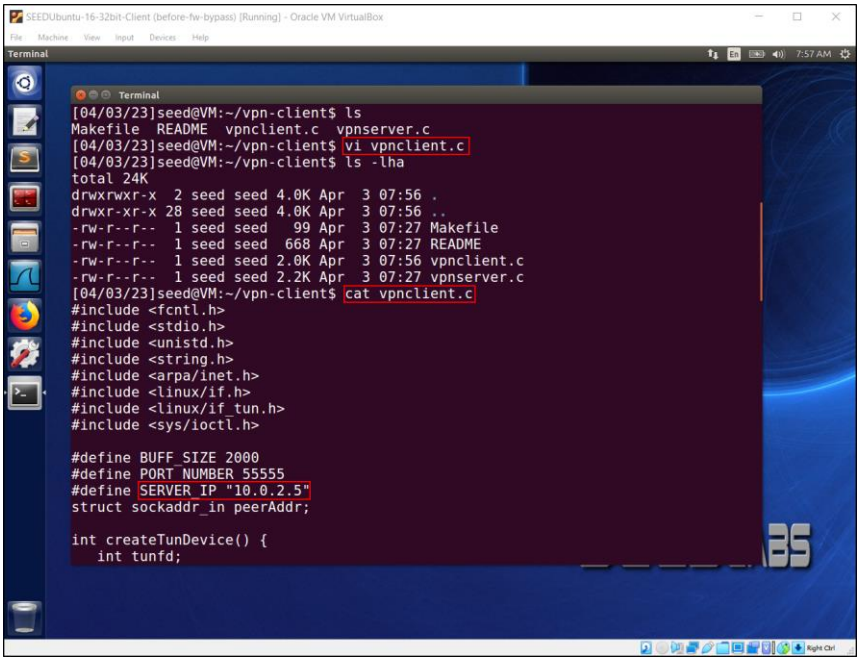

Figure. 18

Run VPN client program vpnclient.c in one terminal window on client as shown below.

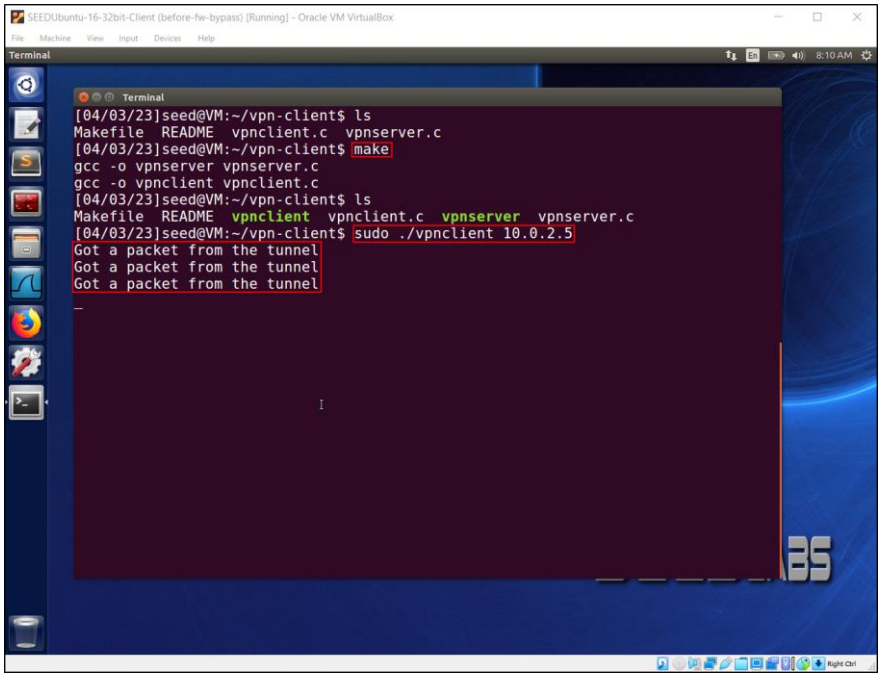

Figure. 19

Client connection message (Hello) on server as shown below.

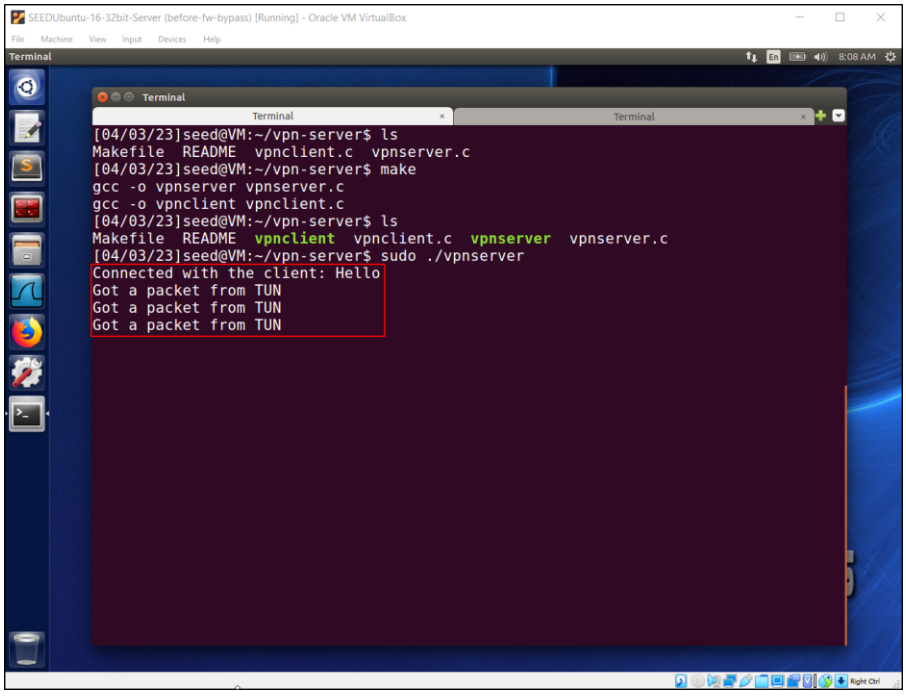

Figure. 20

While running above vpnclient.c program assign IP address 192.168.53.5 to tun0 interface in new terminal window on client as shown below.

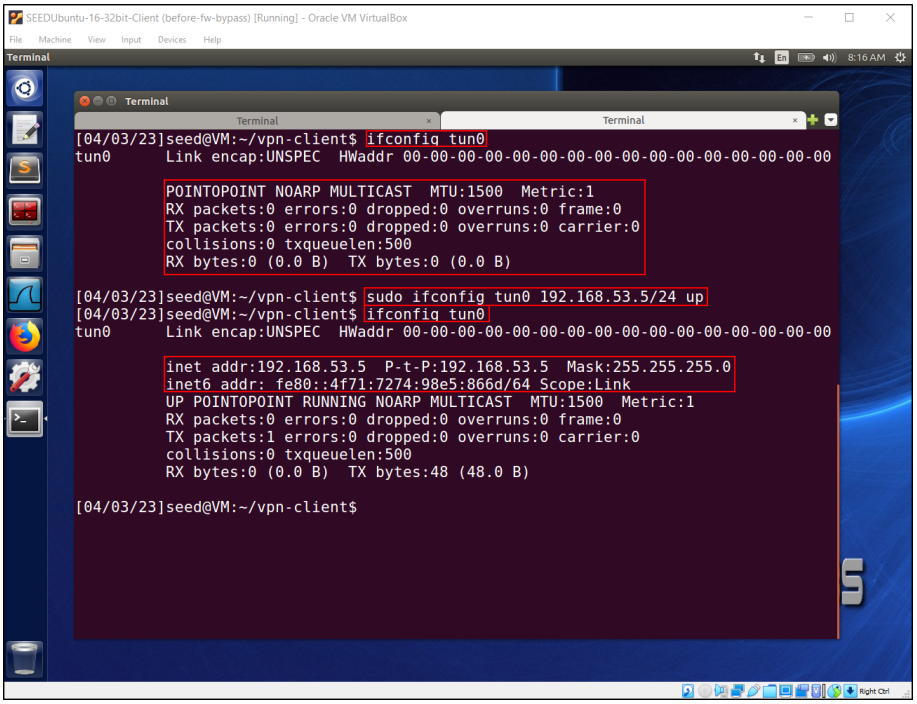

Figure. 21

Ifconfig command output on client after IP address assigned to tun0 interface as shown below.

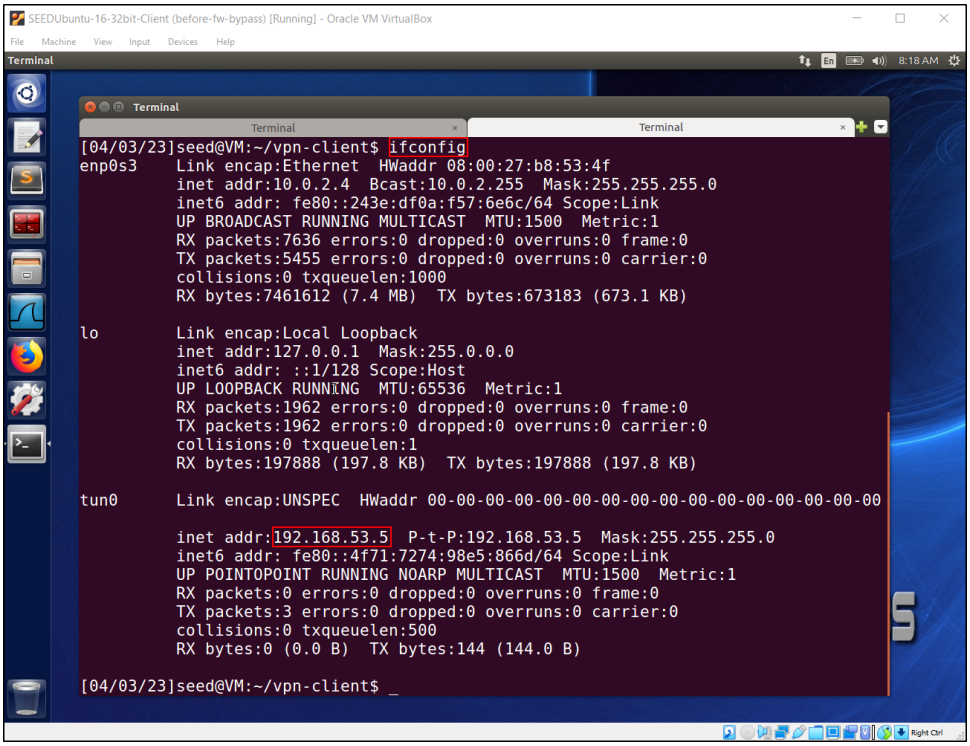

Figure. 22

Step 3: Set Up Routing on Client and Server VMs

VPN tunnel tun0 established between client and server after the above two steps. Set up routing paths on both client and server machines to direct the intended traffic through the tunnel as shown in the below figures Figure. 23 and Figure. 24 respectively.

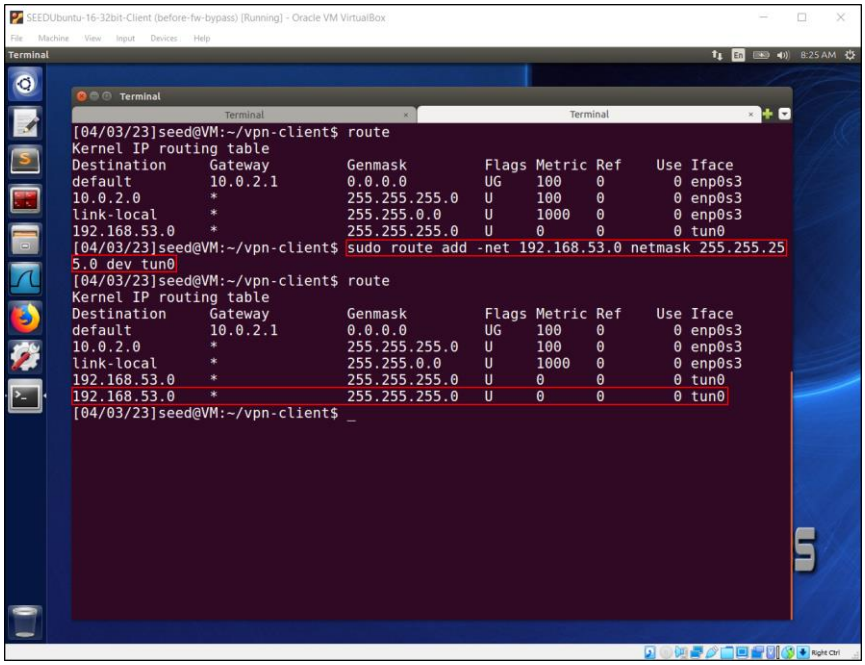

Figure. 23

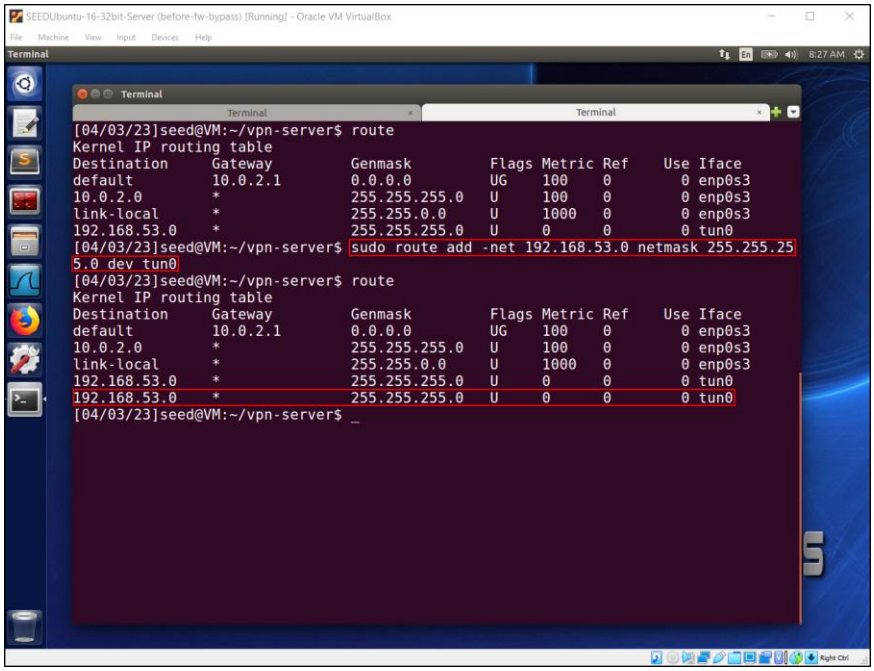

Figure. 24

Client and server communicate (ping) each other using tun0 IP address after tun0 interface created as shown in the below figures Figure. 25 and Figure. 26 respectively.

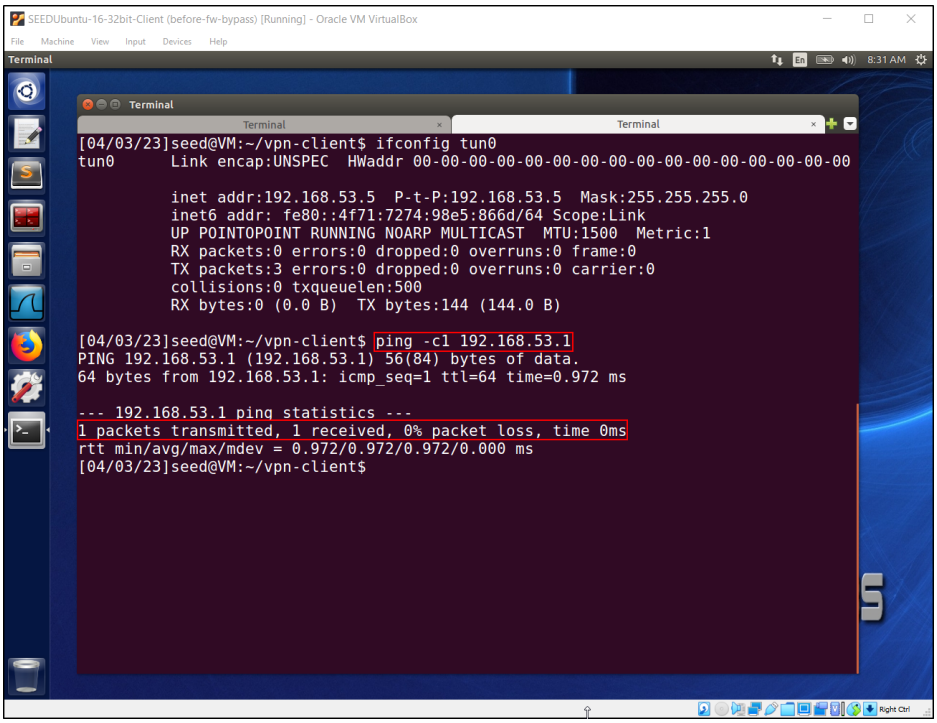

Figure. 25

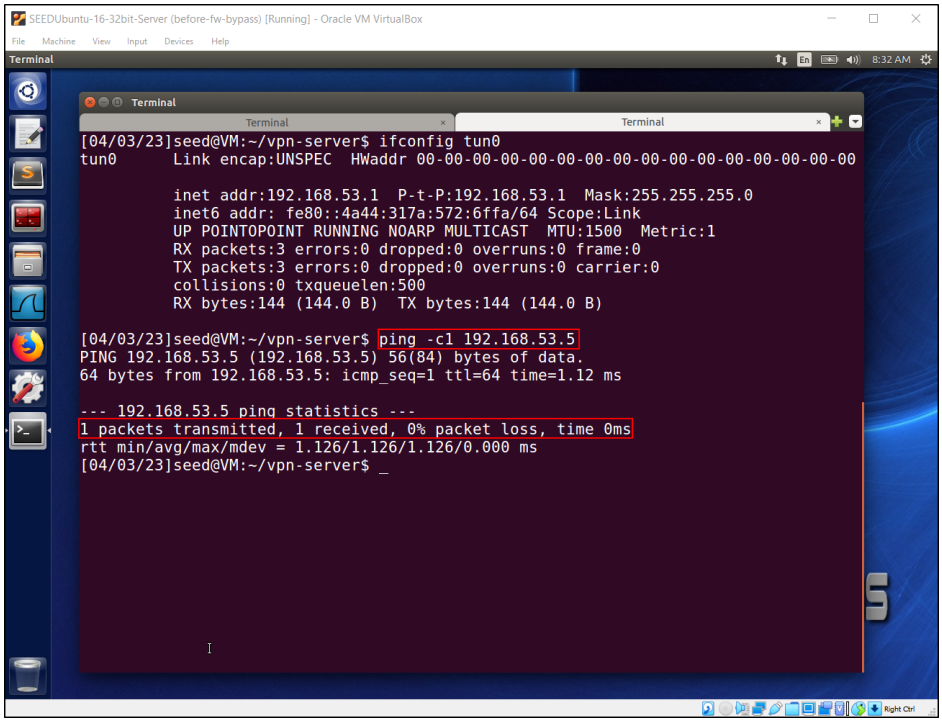

Figure. 26

Ssh connection between client and server using tun0 interface IP address as shown in the below figures Figure. 27 and Figure. 28 respectively.

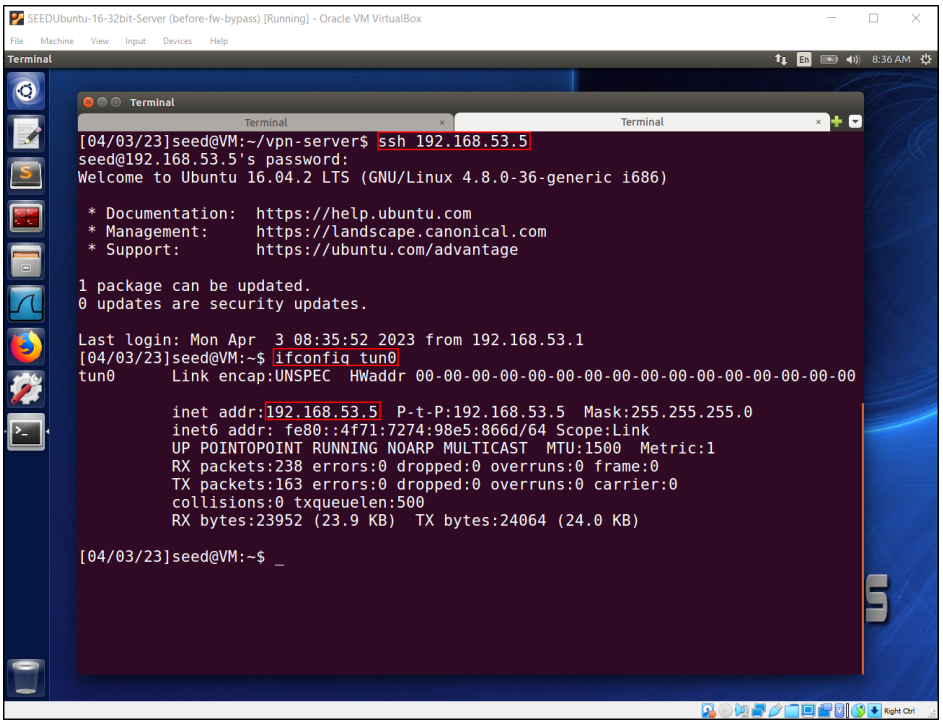

Figure. 27

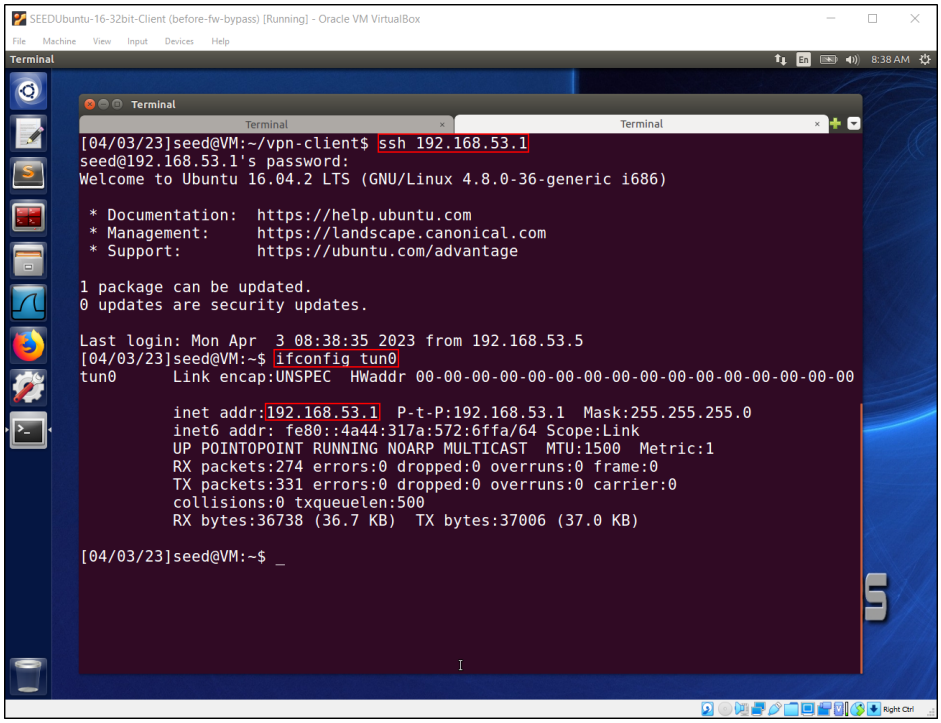

Figure. 28

Step 4: Set Up NAT on Server VM

Enable the NAT Network on server as shown below.

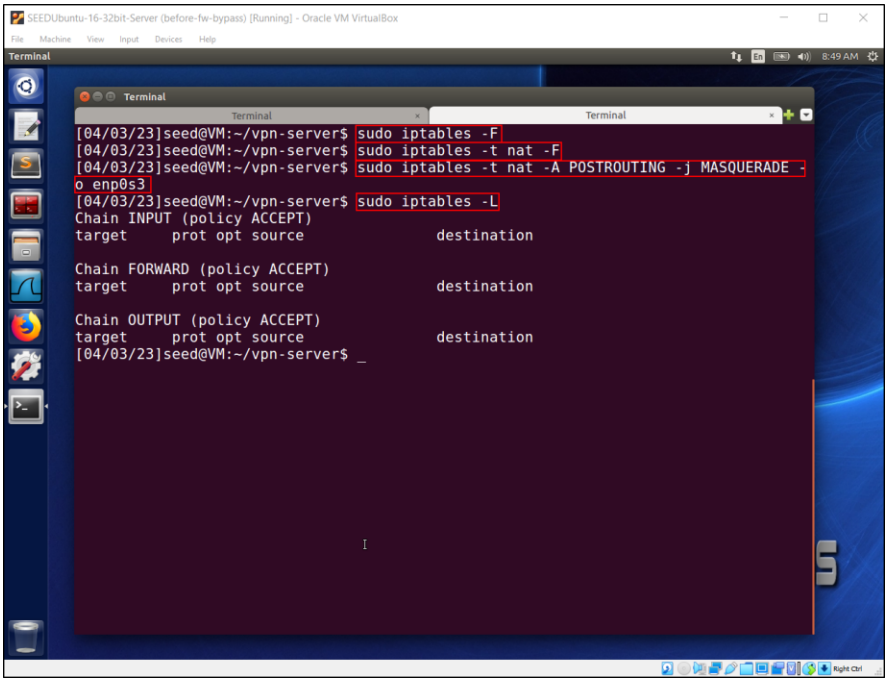

Figure. 29

Client can connect with target telehack.com via ping tool with Wireshark packet capture as shown below.

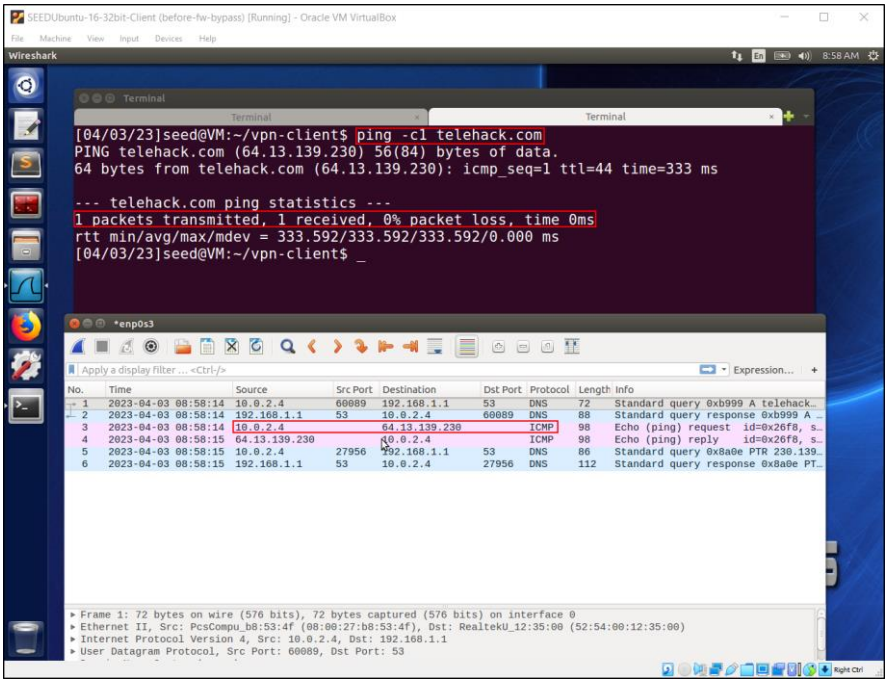

Figure. 30

Step 5: Bypass firewall with VPN tunnel tun0

Ufw tool used to set firewall rules as deny from client to access target domain telehack.com and try to connect via ping to target but 100% packet loss as shown below.

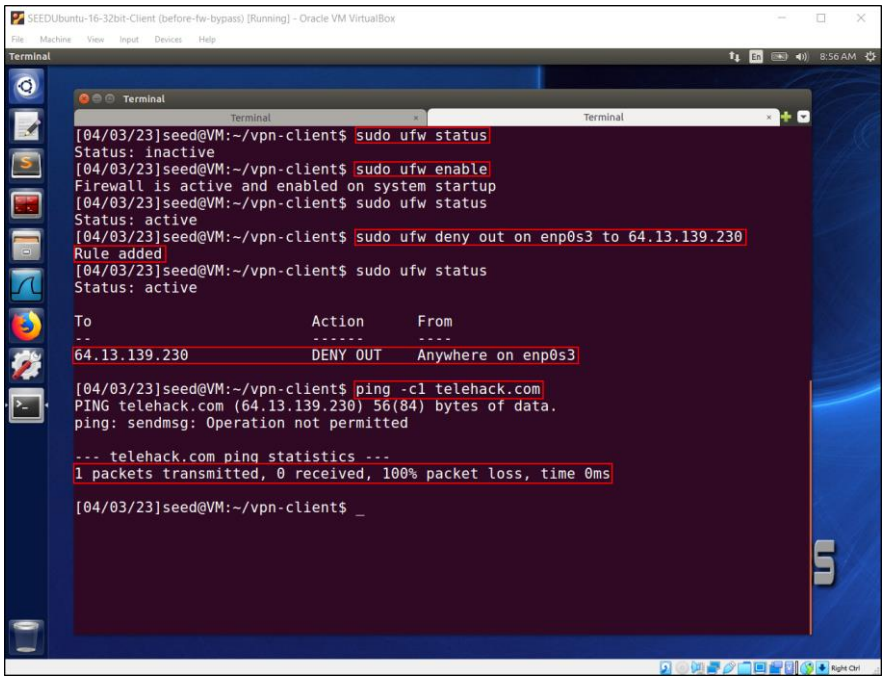

Figure. 31

Routing entry added accordingly to bypass firewall on the client as shown below.

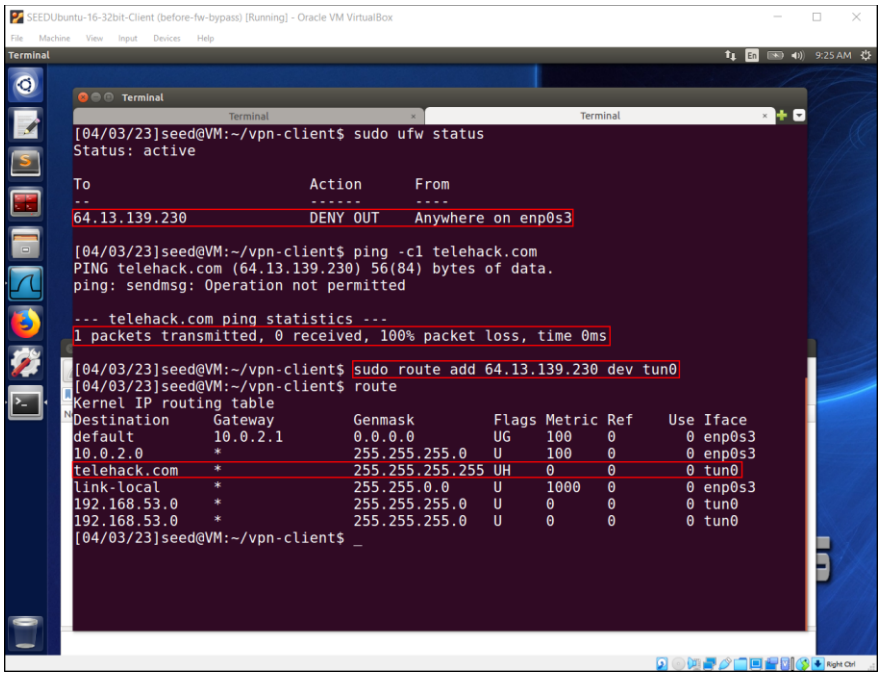

Figure. 32

Able to bypass the firewall and ping to telehack.com with the help of VPN tunnel tun0 with Wireshark packet capture as shown below.

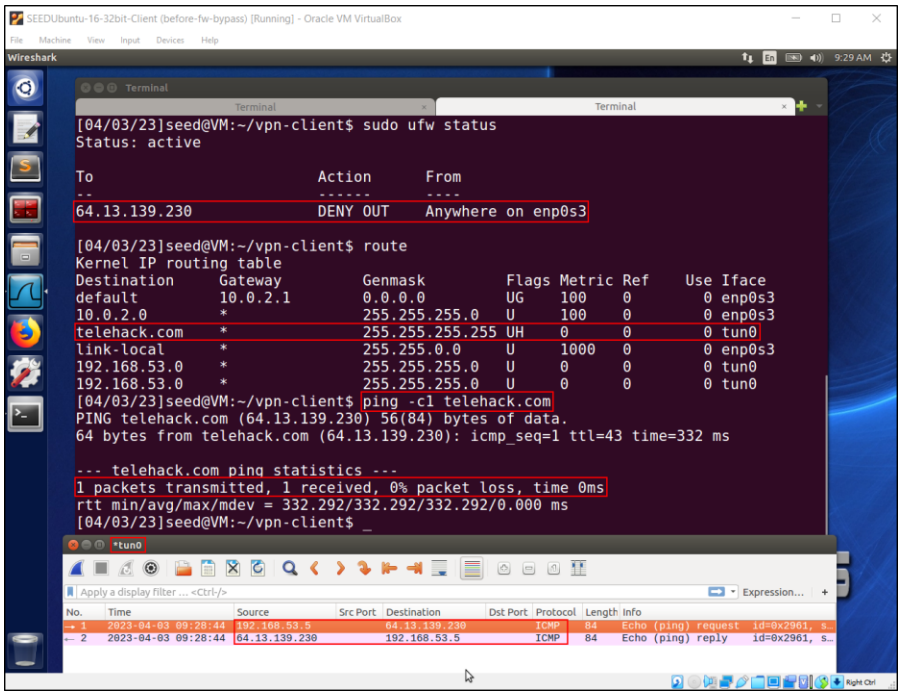

Figure. 33

Now, client can connect to target telehack.com via VPN tunnel tun0 interface IP address. As, evidence curl (port 80) and telnet (port 23) tools with Wireshark packet capture shown in the below figures Figure. 34 and Figure. 35.

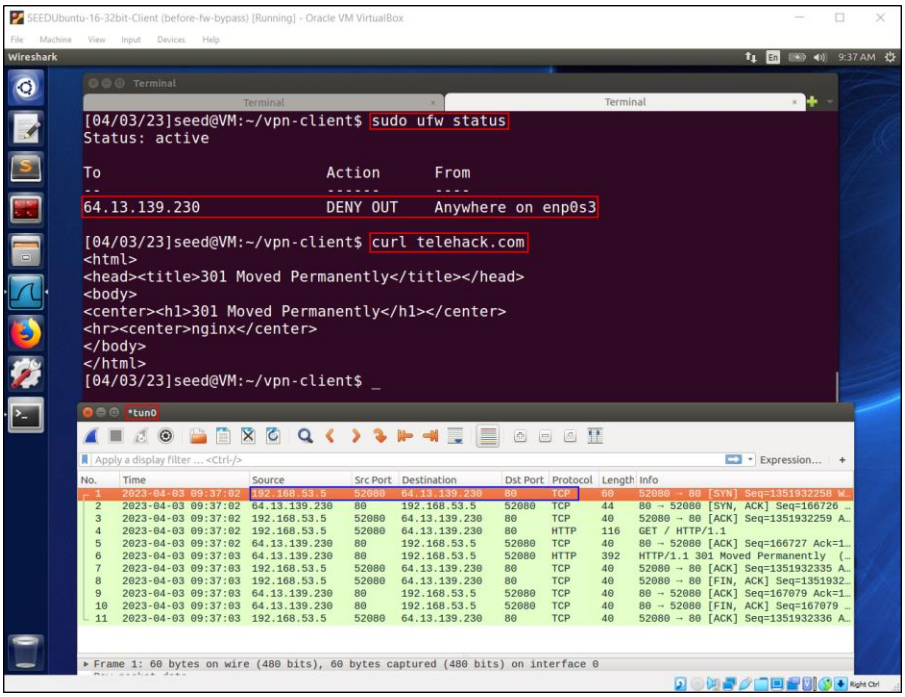

Figure. 34

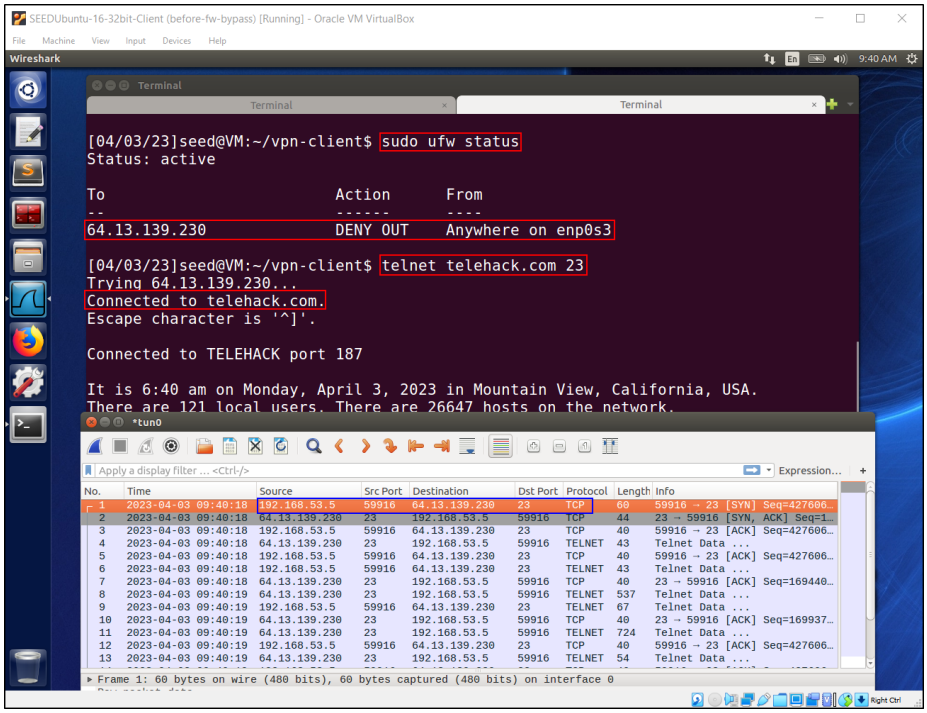

Figure. 35

3. References

1. "Firewall Evasion Techniques and Countermeasures" by SANS Institute: https://www.sans.org/reading-room/whitepapers/firewalls/firewall-evasion-techniques-countermeasures-33098
2. "VPN Evasion Techniques: A Deep Dive" by Infosec Institute: https://resources.infosecinstitute.com/vpn-evasion-techniques-a-deep-dive/
3. "Bypassing firewalls using VPNs" by Help Net Security: https://www.helpnetsecurity.com/2018/09/13/bypassing-firewalls-vpns/
4. "The Dangers of Using a VPN" by Norton: https://us.norton.com/internetsecurity-privacy-the-dangers-of-using-a-vpn.html