2023 CICT high quality class Group Project Report
Cyber Security

Project Title	How to install “telnet-ssl” Package on Ubuntu	
Project Area	Asian	
Students	ID	Name
	B2005850	Huỳnh Trần Tuấn Ngọc
	B2014926	Trần Đăng Khoa
	B2005850	Đinh Đông Phong
Reporting Date	12-12-2023	

Ⅰ. Project Outline

- **Title**

  HOW TO INSTALL “TELNET-SSL” PACKAGE ON UBUNTU

- Group Information

Team Name					
Team Composition		Name	Belong	Department	Position /year
Instructor		Noh	CICT	IT Department	
Student	Team Leader	Huỳnh Trần Tuấn Ngọc	CICT	Department of Computer Science	4
	Team member 2	Trần Đăng Khoa	CICT	Department of Computer Science	4
	Team member 3	Đinh Đông Phong	CICT	Department of Computer Science	4

Ⅱ. Project Information

- **Purpose of Project**

This project aims at checking and complementing security vulnerabilities of IT system, capturing the packets to prevent the movement of security attacks, and examines how to forward the packets to the system. We can analyze the data packets in detail to prevent unnecessary packet genera tion. This project is designed to train basic skill of detection of hacking ac ks under networking environment.

2. Project work flow(one model)

- Telnet to the telnet server from the client
- Attacker Fedora assigned IP address and virtual MAC address of t he target to attack
- Perform arp spoof and packet relay attacks on the victims
- Check Session Detection
- If session is detected, session hijacking is executed

Ⅲ. Action Plan

- **Environments & resource**

		Details
S/W	OS	CentOS 7, Ubuntu 20, Kali_Linux
	IDE	Redhat Linux, Debian Linux
	language	
	tool	Snort, WireShark, TCPdump, barnyard2,
H/W	device	Personal PC
	sensor	
	communica tion	

2. Role arrangements

Student	Division	role
1	Plan & design	
2	Analysis	
3	Implement & test	

3. Project Schedule

Division	Promotion contents	Schedule							
Plan	Role sharing and analysis software installation								
Analysis	Software option analysis								
Test	Analysis using Software function								
Finish	Create result document through analysis								
Offline meeting Plan	Information sharing and progress confirmation of each other								

Ⅳ. Expected Benefit

1. Performance Goals

- *Select Efficient Cipher Suites*: Telnet-SSL relies on SSL/TLS for encryption. Choose efficient and secure cipher suites to ensure the encryption process doesn't introduce unnecessary overhead. Consider prioritizing suites that offer a good balance between security and performance.
- *Optimize Network Latency:* Minimize network latency by ensuring that the Telnet-SSL server is located close to the clients, and that th

e network infrastructure is properly configured for efficient commun ication. This may include optimizing routing, reducing packet loss, and ensuring a reliable network connection.

- *Load Balancing:* If your Telnet-SSL server experiences high loads, consider implementing load balancing to distribute incoming conne ctions across multiple servers. This can help prevent a single serve r from becoming a bottleneck and improve overall system performa nce.
- *Hardware Acceleration***:** Utilize hardware acceleration features if yo ur server hardware supports them. Some systems have hardware modules specifically designed to accelerate SSL/TLS encryption, r educing the load on the CPU and improving overall performance.
- *Compression Considerations:* SSL/TLS supports data compression , but it may not always lead to improved performance. In some cas es, the overhead of compression and decompression may outweig h the benefits, especially on high-speed networks. Test and evalua te the impact of compression in your specific environment.
- *Session Resumption:* Implement session resumption mechanisms to reduce the overhead of SSL/TLS handshakes. Session resumpti on allows a client to reuse a previously established session, saving time and resources.
- *Optimize Server Configuration:* Fine-tune the Telnet-SSL server co nfiguration based on your specific use case. This may include adju sting the number of allowed connections, setting appropriate timeo uts, and configuring buffer sizes.
- *Monitor and Tune Resources:* Regularly monitor server resources such as CPU usage, memory, and network bandwidth. Adjust confi gurations based on resource utilization patterns to ensure optimal p erformance under varying workloads.
- *Regular Updates:* Keep your Telnet-SSL software and underlying o perating system up to date. Software updates often include perform ance improvements, bug fixes, and security enhancements.
- *Benchmarking:* Conduct benchmark tests to measure the performa nce of your Telnet-SSL implementation under different conditions. This will help identify potential bottlenecks and areas for improvem ent.

2. Benefit

- *Encryption:* The primary benefit of Telnet-SSL is the ability to encry pt communication between the client and server. Traditional Telnet transmits data in plaintext, making it susceptible to eavesdropping. By using SSL, the data is encrypted, providing confidentiality and

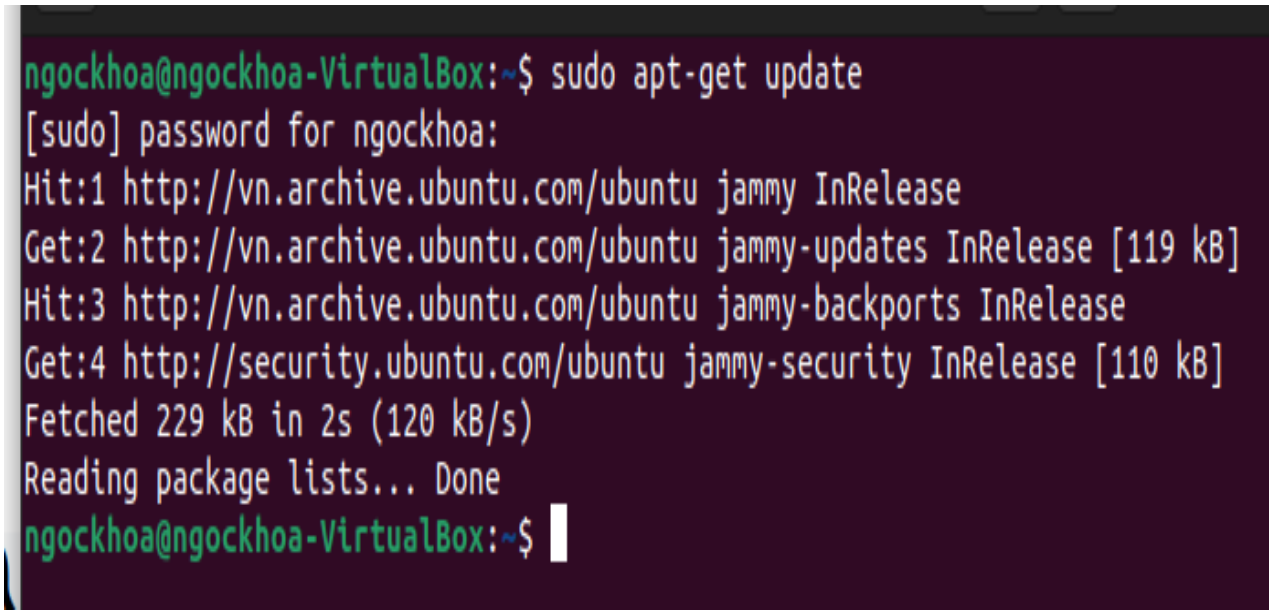
security.

- *Legacy Systems Compatibility:* In some cases, legacy systems or devices may only support Telnet for remote access, and adding SSL to Telnet might be a more feasible solution than transitioning to SSH. Telnet-SSL allows you to enhance security without necessarily changing the underlying protocol.
- *Authentication:* SSL provides a mechanism for authenticating the server to the client and vice versa. This helps ensure that the parties involved in the communication are who they claim to be, adding an extra layer of security to Telnet sessions.
- *Application Support*: If you have an application that relies on Telnet for communication and it supports SSL/TLS, using Telnet-SSL might be a way to secure the communication without modifying the application itself.

Ⅴ. Practice Result

[step 1] For update the package list of available software packages

- $ sudo apt-get update:



[step 2] Install the telnet-ssl package with the following command:

- **$** sudo apt-get install telnet-ssl:

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo apt-get install telnet-ssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
telnet-ssl is already the newest version (0.17.41+0.2-3.3build2).
0 upgraded, 0 newly installed, 0 to remove and 134 not upgraded.
ngockhoa@ngockhoa-VirtualBox:~$
```

[step 3] Set up a static IP to be able to use telnet-ssl:

We use the "nmcli" command to configure a static IP for the Ubuntu mac hine, with this command you can access additional network information s uch as connection status, storage device name and general permissions in the network configuration.

- Addresses: 10.2.10.174
- Netmask: 255.255.255.0
- Gateway: 10.2.10.1

```
ngockhoa@ngockhoa-VirtualBox:~$ nmcli connection show
NAME                UUID                                  TYPE      DEVICE
Profile 1           16e97d77-d03e-4683-8c58-769fc73bcbc4  ethernet  enp0s3
Wired connection 1  8d37eed4-73a7-356c-b60d-5d560dc7887a  ethernet  --
```

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo nmcli con add type ethernet con-name 'stati
c' ifname enp0s3 ipv4.method manual ipv4.addresses 10.2.10.174/24 gw4 10.2.10.1
Connection 'static' (ccc9d1a3-8906-49dc-9de2-628bb754b0ff) successfully added.
```

Add the static connection you created to DNS IP:

- $ sudo nmcli con mod static ipv4.dns 10.2.10.174

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo nmcli con mod static ipv4.dns 10.2.10.174
```

```
ngockhoa@ngockhoa-VirtualBox:~$ nmcli connection show
NAME                UUID                                  TYPE      DEVICE
Profile 1           16e97d77-d03e-4683-8c58-769fc73bcbc4  ethernet  enp0s3
static              ccc9d1a3-8906-49dc-9de2-628bb754b0ff  ethernet  --
Wired connection 1  8d37eed4-73a7-356c-b60d-5d560dc7887a  ethernet  --
```

Use the following command to connect

- Sudo nmcli con up id ‘static’

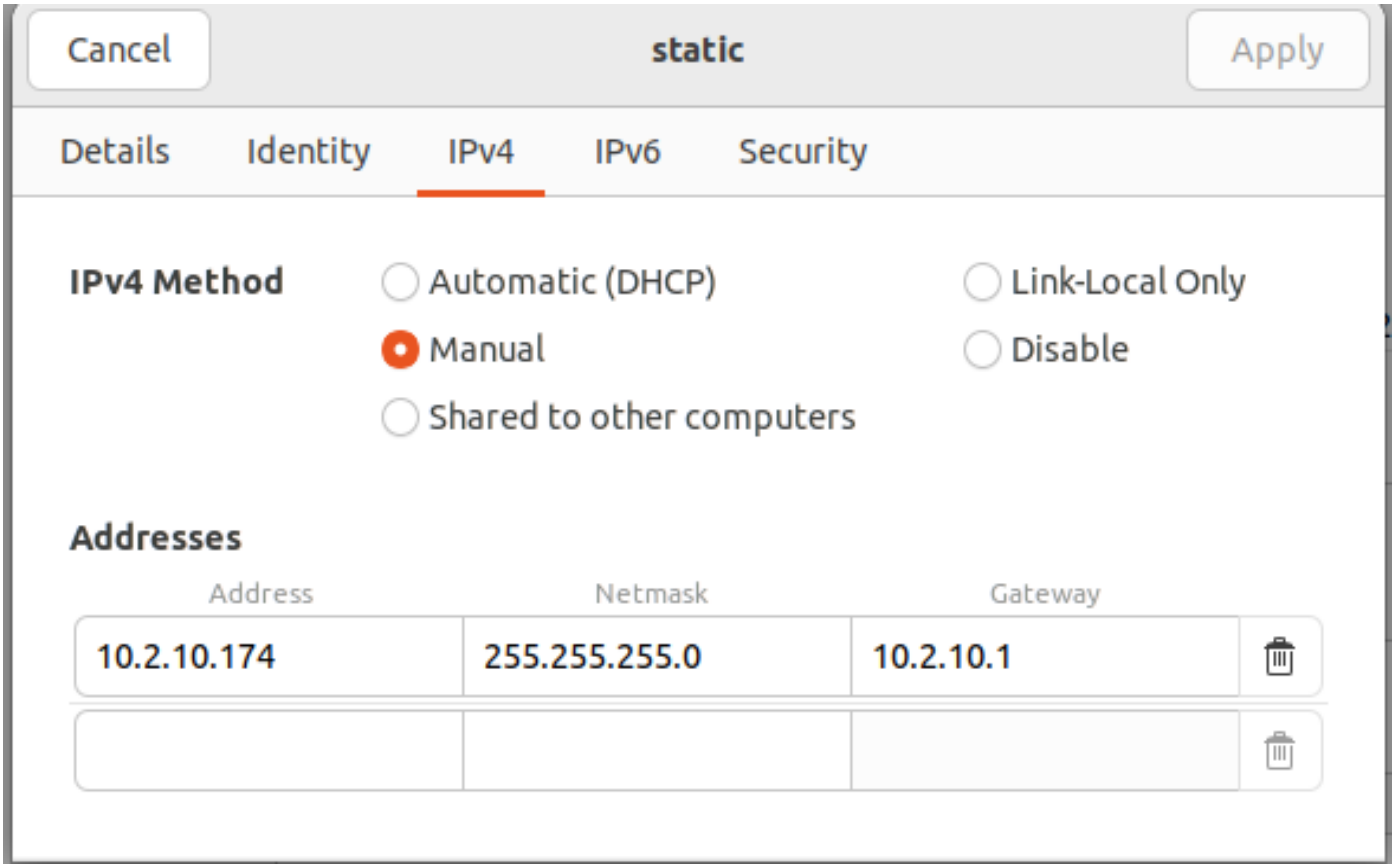
```
ngockhoa@ngockhoa-VirtualBox:~$ sudo nmcli con up id 'static'
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkMa
nager/ActiveConnection/33)
```

To determine the assigned static IP, we use the command:

- Ip route

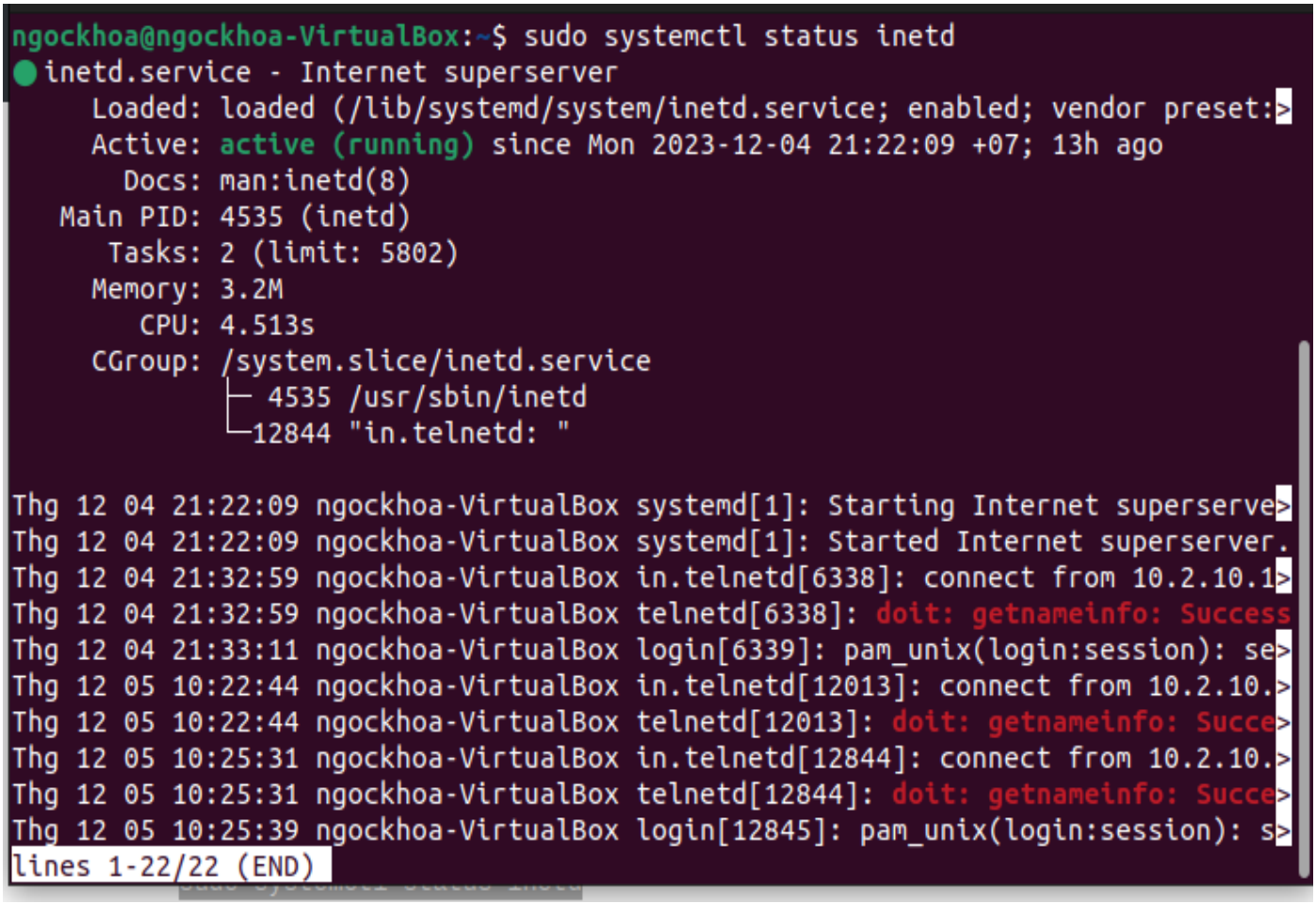
```
ngockhoa@ngockhoa-VirtualBox:~$ ip route
default via 10.2.10.1 dev enp0s3 proto static metric 20100
10.2.10.0/24 dev enp0s3 proto kernel scope link src 10.2.10.174 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
```

After completing the static IP configuration:



[step 4] Start it up to see if the status is working or not

$ sudo systemctl status inetd



[step 5] Check remote connection with static ip

Telnet 10.2.10.174

```
ngockhoa@ngockhoa-VirtualBox:~$ telnet 10.2.10.174
Trying 10.2.10.174...
Connected to 10.2.10.174.
Escape character is '^]'.
[SSL not available]
Ubuntu 22.04.3 LTS
ngockhoa-VirtualBox login: ngockhoa
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

133 updates can be applied immediately.
96 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

[step 6] Use telnet to check open port 80

- telnet 10.2.10.174 80

```
 instead.
ngockhoa@ngockhoa-VirtualBox:~$ sudo netstat -tap | grep 80
ngockhoa@ngockhoa-VirtualBox:~$ telnet 10.2.10.174 80
Trying 10.2.10.174...
telnet: Unable to connect to remote host: Connection refused
```

[step 7] Use telnet to check the mail server

Telnet command is useful to test mail server, for this we need to run the following command

-$ telnet 10.2.10.174 25

```
ngockhoa@ngockhoa-VirtualBox:~$ telnet 10.2.10.174 25
Trying 10.2.10.174...
```

[step 8]

- Allow port 23 through the firewall on the remote machine

Reload the firewall

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo ufw allow 23/tcp
[sudo] password for ngockhoa:
Rules updated
Rules updated (v6)
ngockhoa@ngockhoa-VirtualBox:~$
```

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo ufw reload
Firewall reloaded
ngockhoa@ngockhoa-VirtualBox:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23/tcp                     ALLOW       Anywhere
23/tcp (v6)                ALLOW       Anywhere (v6)

ngockhoa@ngockhoa-VirtualBox:~$
```

[step 9]

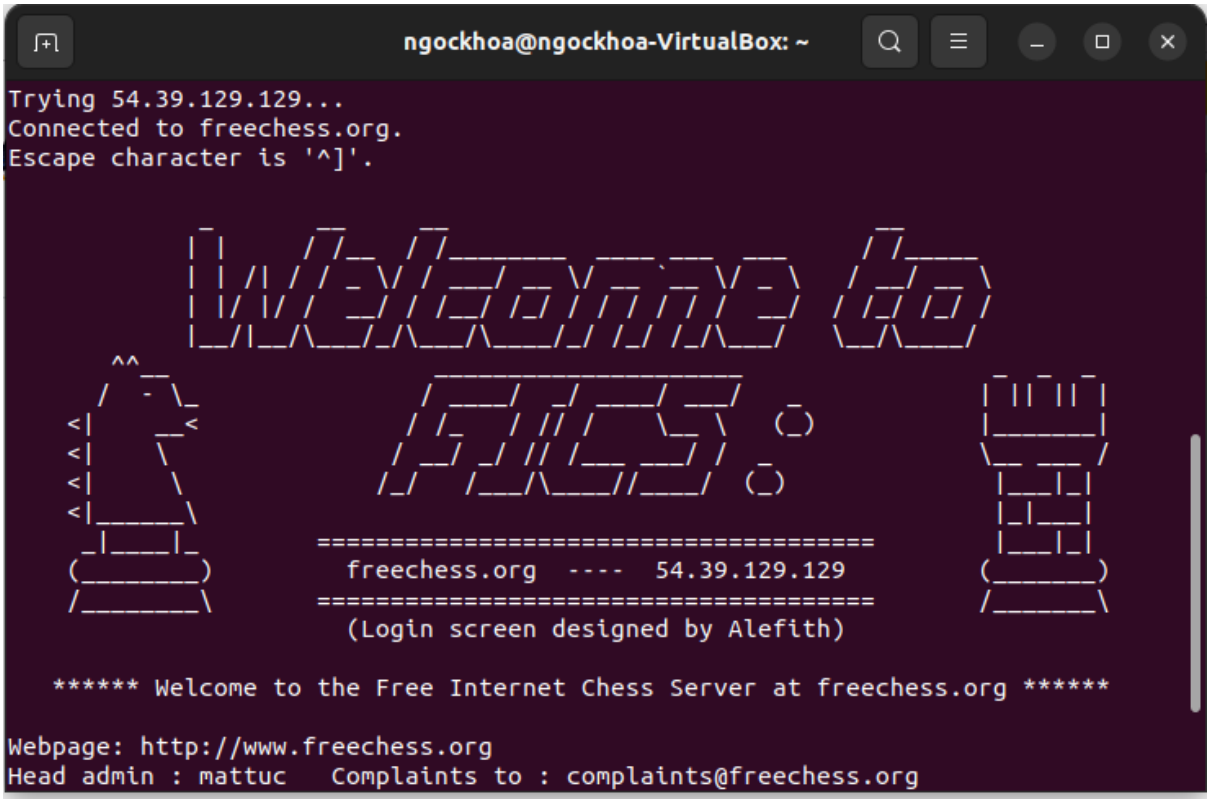
Using Telnet to check the network

```
ngockhoa@ngockhoa-VirtualBox:~$ telnet google.com 80
Trying 142.251.220.78...
Connected to google.com.
Escape character is '^]'.
```

telnet is a great way to check if a specific port is open on a server. Check if a certain port
is answering any calls by specifying the port number in the command. Do ing so
allows you to see what's going on in a network and if a port is responsive or not.

[step 10]

Telnet allows you to connect the website with the right [server_address] and [port]

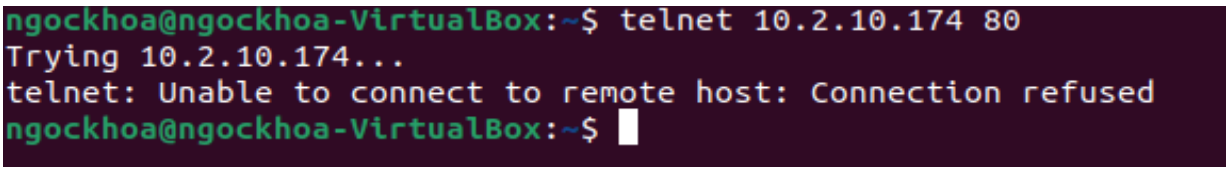


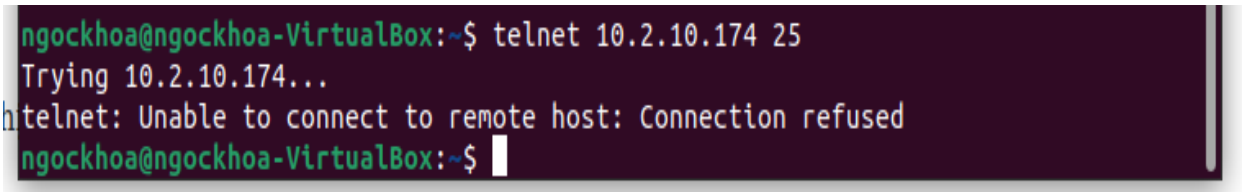
It will show an ASCII version of the website do action on it

Ⅵ. Problem and Solution

1. Technical issues during project development

- **Unable to connect to remote host**: Unable to connect to remote port 80, due to unable to connect to remote host.





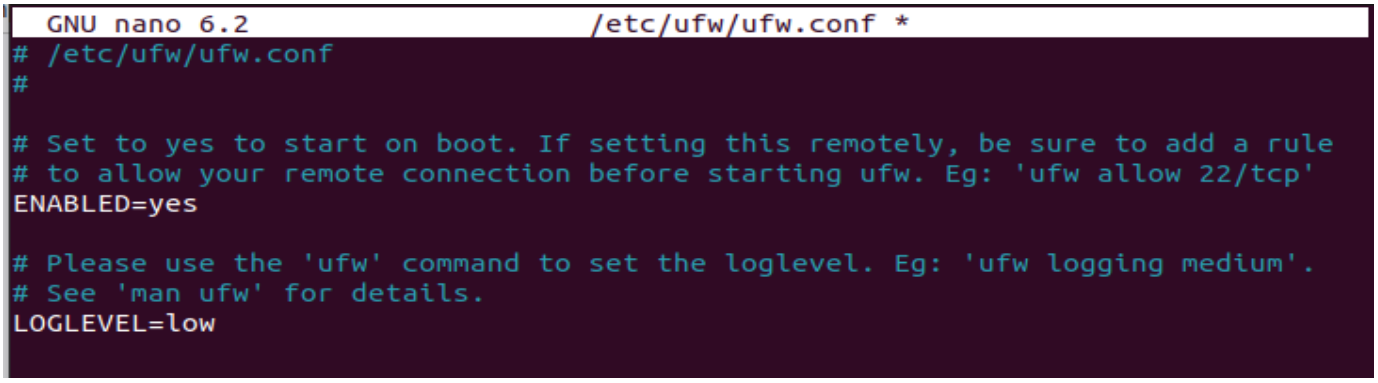
- Firewall not enabled (skipping reload):

```
ngockhoa@ngockhoa-VirtualBox:~$ sudo ufw reload
[sudo] password for ngockhoa:
Firewall not enabled (skipping reload)
ngockhoa@ngockhoa-VirtualBox:~$
```

2. Solution(how to solve the problems)

- Unalbe to connect to remote host: Ensure that the service you are trying to connect to on the remote host is running and accepting connections. For example, if you are trying to connect via SSH, make sure the SSH serve r is running on the remote host.

- Firewall not enabled (skipping reload): If this error appears, we can check it with the command "sudo nano /etc/ufw/ufw.com". And search for “EN ABLED= yes” to edit “yes” to “no” to fix the above error.



Ⅶ. References

[ONLINE] : https://zoomadmin.com/HowToInstall/UbuntuPackage/telnet-ssl

[ONLINE]: https://funix.edu.vn/chia-se-kien-thuc/cach-dinh-cau-hinh-dia-chi-ip-tinh-tren-ubuntu-22-04-lts/

[ONLINE]: https://vi.linux-console.net/?p=5215#google_vignette

==========