

Configuration Manual

MSc Research Project
MSc in Cybersecurity

Richard Sosinski
Student ID: x22236520

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland
MSc Project Submission Sheet



School of Computing

Student Name: Richard Sosinski
Student ID: X22236520
Programme: MSc in Cybersecurity **Year:** 2023/2024
Module: Practicum 2
Lecturer: Michael Prior
Submission Due Date: 12/08/2024
Project Title: User Manual for the powerhouse security tool for a secure smart dwelling
Word Count: 2068 **Page Count:** 20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Richard Sosinski
Date: 11/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

User Manual for the Powerhouse Security Tool for a Secure Smart Dwelling

By Richard Sosinski
x22236520

1.0) Prerequisites:

1. Raspberry Pi
2. SD card 32-64 GB
3. SD card Reader
4. Network Switch
5. Home Router connecting to the internet
6. Mouse and Keyboard
7. USB (optional)
8. Monitor/TV for display
9. Ethernet Cable x1

2.0) Diagram of Network

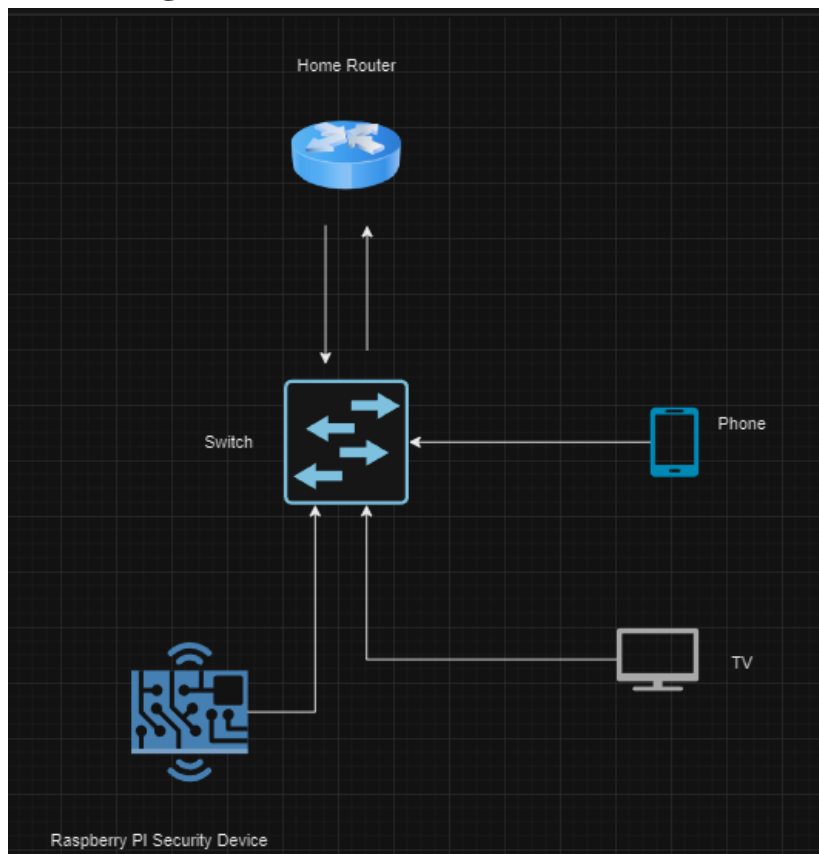


Image 2.1 Network Diagram

1. Connect Raspberry Pi to Switch
2. Connect Wired devices to the switch
3. Connect wireless devices to the main network
4. For all wireless devices set the default route and DNS settings as the Raspberry Pi's static IP
5. Set Raspberry Pi as the DHCP server on home router (unique to every router)
6. Connect Home router to the switch

DHCP should be working for everything on the network however, there was no testing done to try and see if the router's DHCP settings are changed they would comply with the Raspberry Pi's settings. There is no reason why it should not however, there are precautions there in case it does not work.

3.0) Setting up the Raspberry Pi

The setup of the Raspberry Pi should not take too long as most of the steps are not too complicated and require little to no technical knowledge. If the user is more advanced then they can modify these steps accordingly.

3.1) Step 1 Install the OS on the Raspberry Pi

This step requires the use of a computer to install the raspberry pi imager tool which helps in installation of the Raspbian image(Raspberry Pi Team, 2024a). This is a graphic tool meaning everything necessary is just buttons.

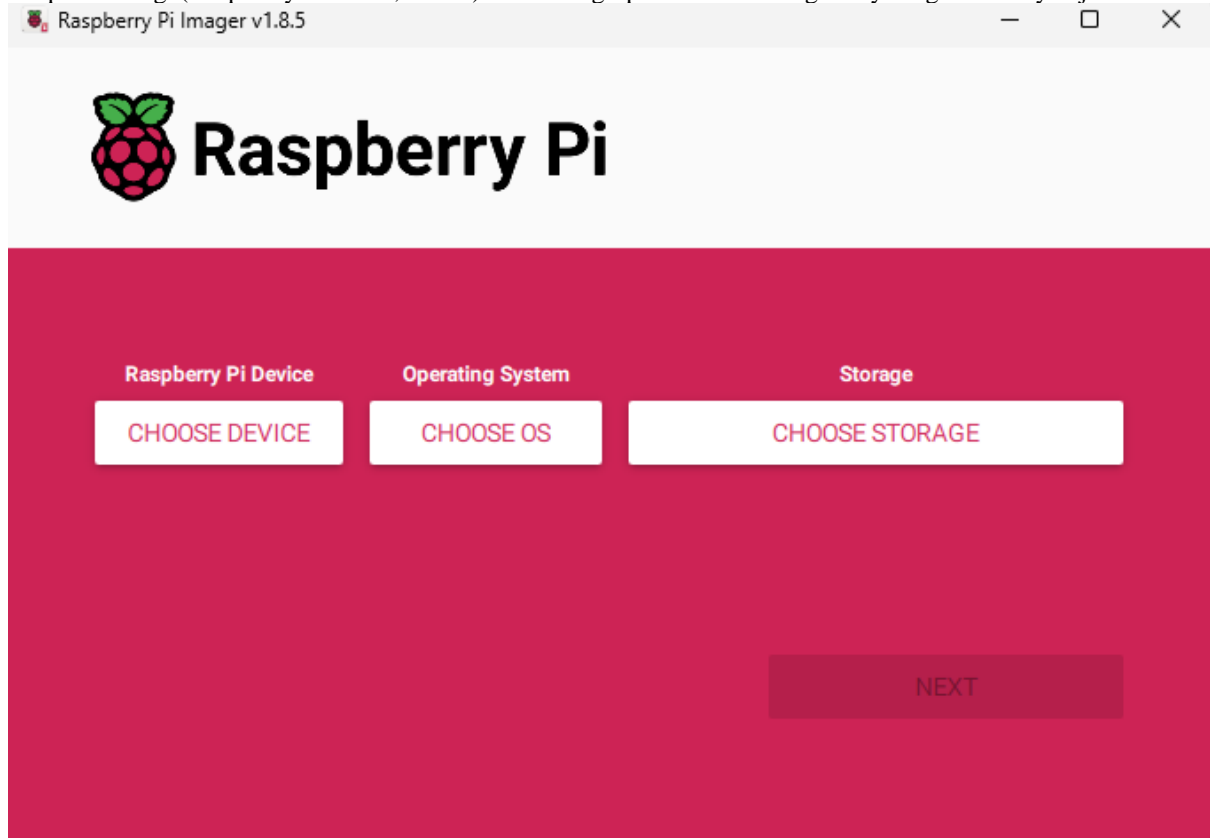


Image 3.1.1 Raspberry Pi imager first opening

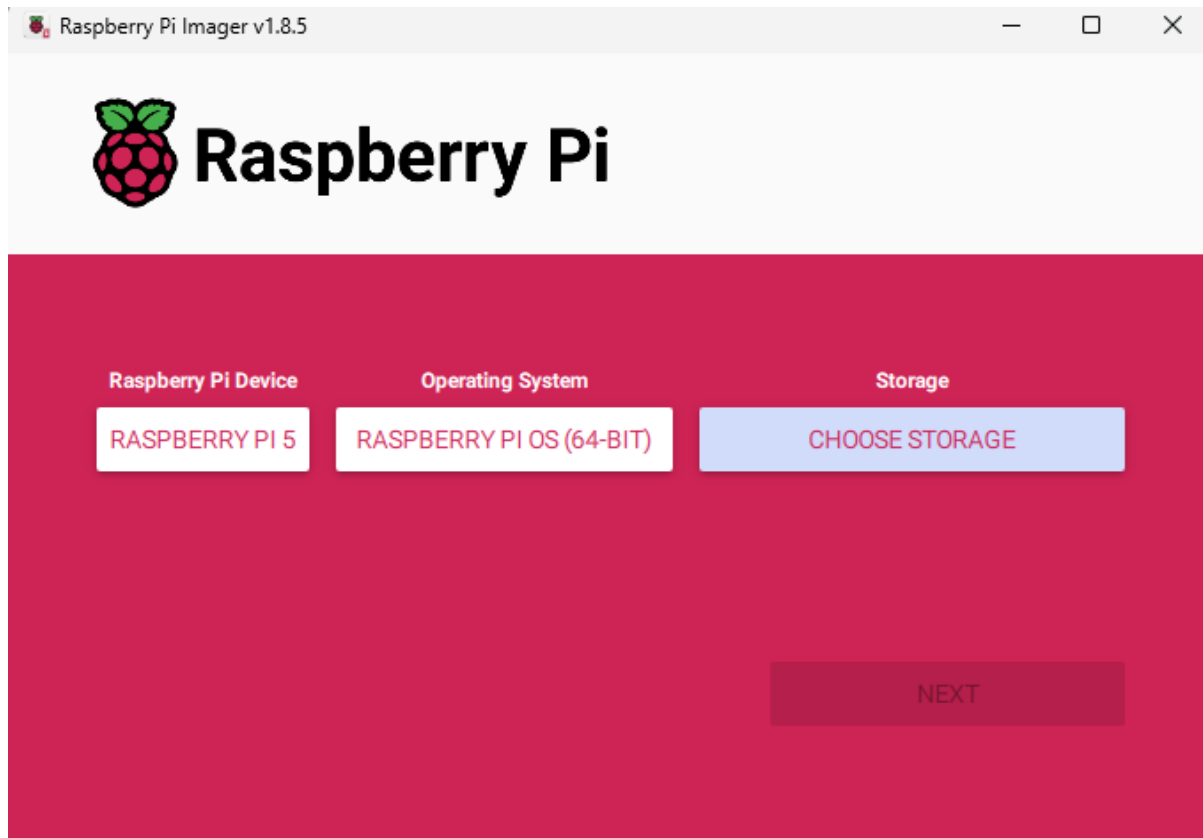


Image 3.1.2 Raspberry pi Imager chosen options

The operating system is suggested to be Raspberry Pi OS 64 bit, this is what this user manual will cover however, the raspberry pi device is the one the user has bought for themselves. After that the installer will prompt you to setup more settings, fill out the settings accordingly, these include settings like hostname, password, ssh, etc. These settings are user dependant however, they can be changed later if problems arise. Once this is completed eject the SD card and slide it into the Raspberry pi connect the Raspberry Pi correctly and turn it on. Make sure that before turning it on the keyboard and mouse are connected as well as the HDMI to the display otherwise the user will not be able to make any changes or continue with this manual. It is also recommended that the ethernet cable is connected to the Raspberry pi and the other end to the switch (Raspberry Pi Team, 2024b).

3.2) Step 2 Setting up the network settings

This step will cover how to setup a static IP address and turn on packet forwarding.

The first step is to setup the static IP address, this is done using the Network Manager tool built into Raspberry Pi OS (Raspbian as it will be called throughout this manual). To access the tool open the command prompt and type in "nmtui".

1. Open "nmtui"
2. Navigate to "Edit a connection" using the keyboard
3. Press enter to enter "Wired connection 1"
4. Change the setting of "IPv4 CONFIGURATION" from DHCP to Manual
5. Change the IP address to 192.168.1.x/24 assuming the network is running on that address range
6. Change the Gateway and DNS servers to the Router
7. Scroll down and press Exit
8. Navigate to "Activate a connection"
9. Press "Enter" once to turn off "Wired connection 1"
10. Press "Enter" once more to turn it back on

The static IP address has now been setup and it can be confirmed using the “ip address” command built into Linux.

The following images are the steps visualised:

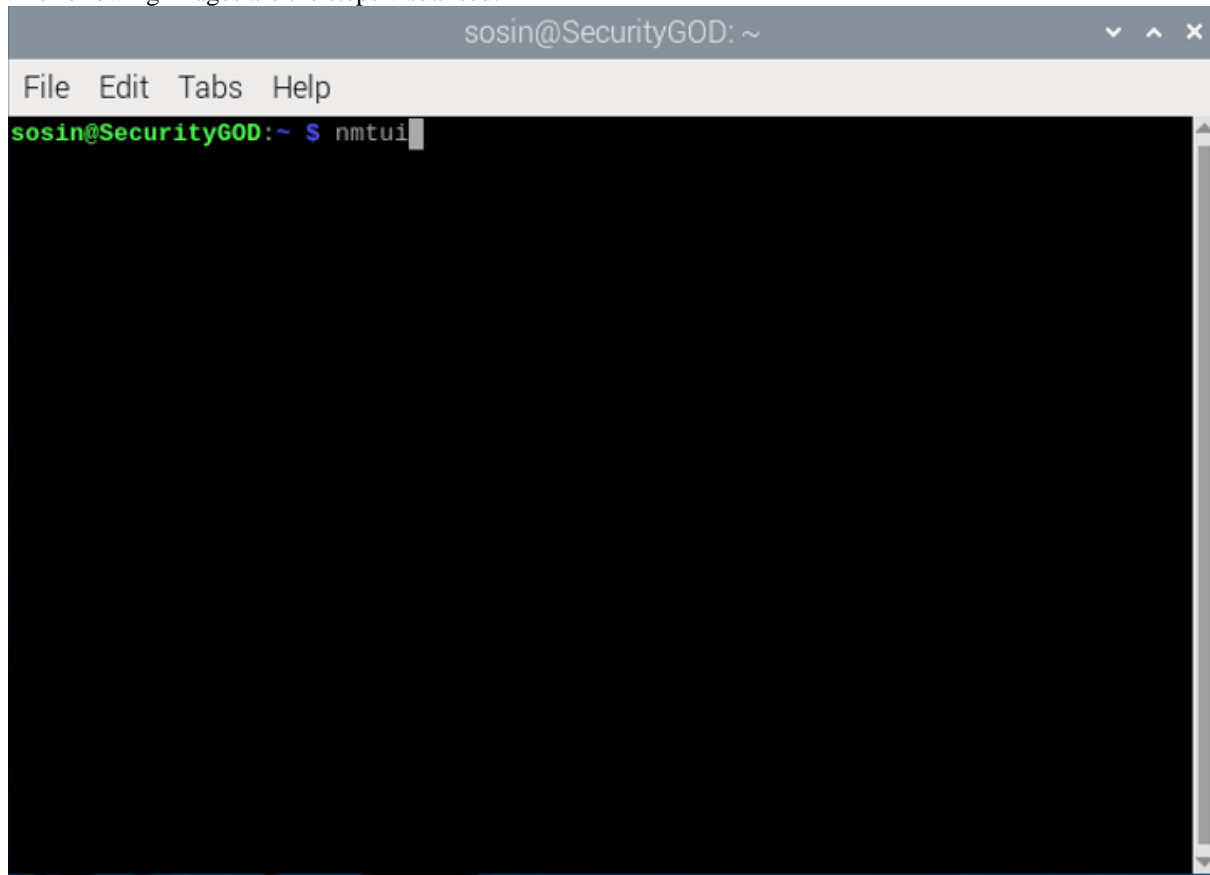


Image 3.2.1 entering network manager

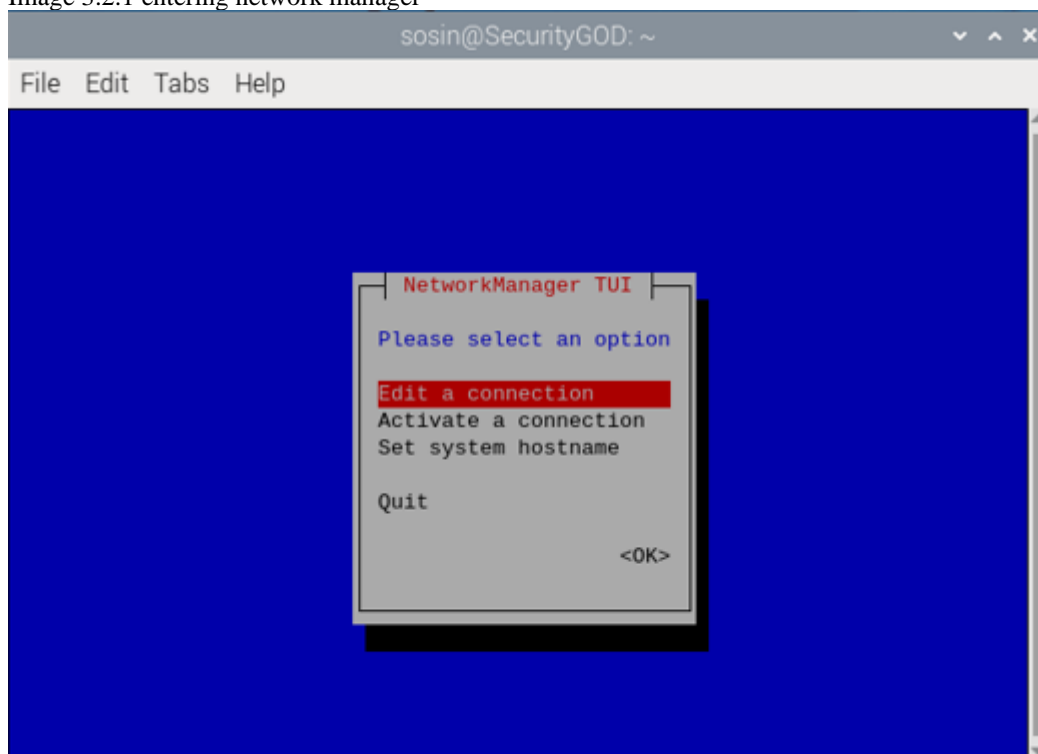


Image 3.2.2 Network manager user interface

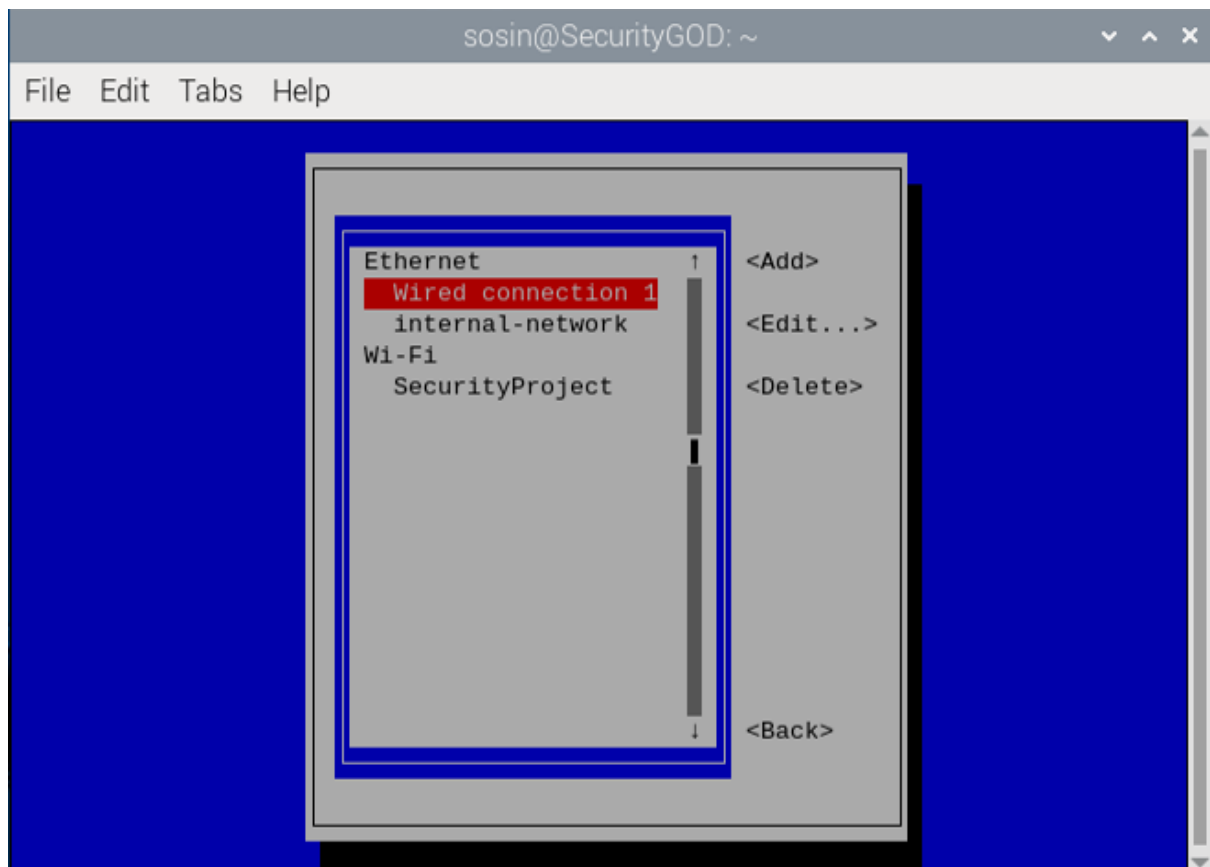


Image 3.2.3 Edit a connection options

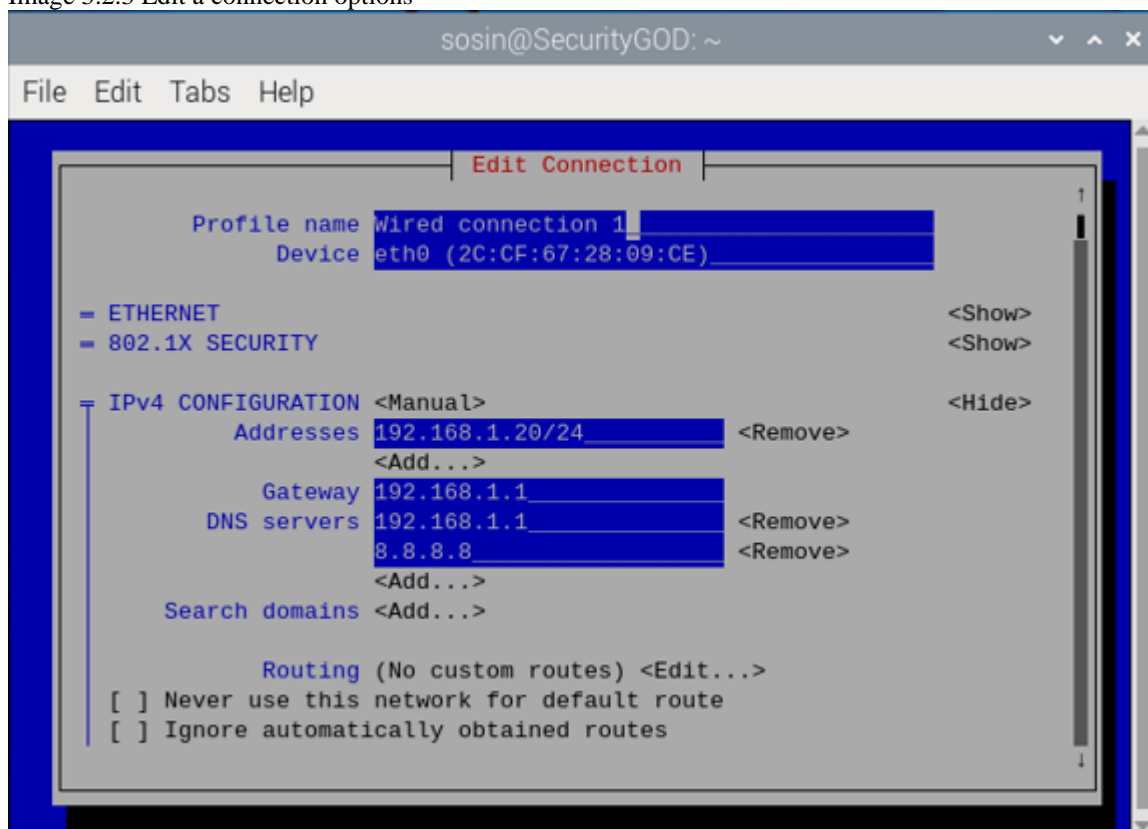


Image 3.2.4 Sample of settings for Wired Connection 1

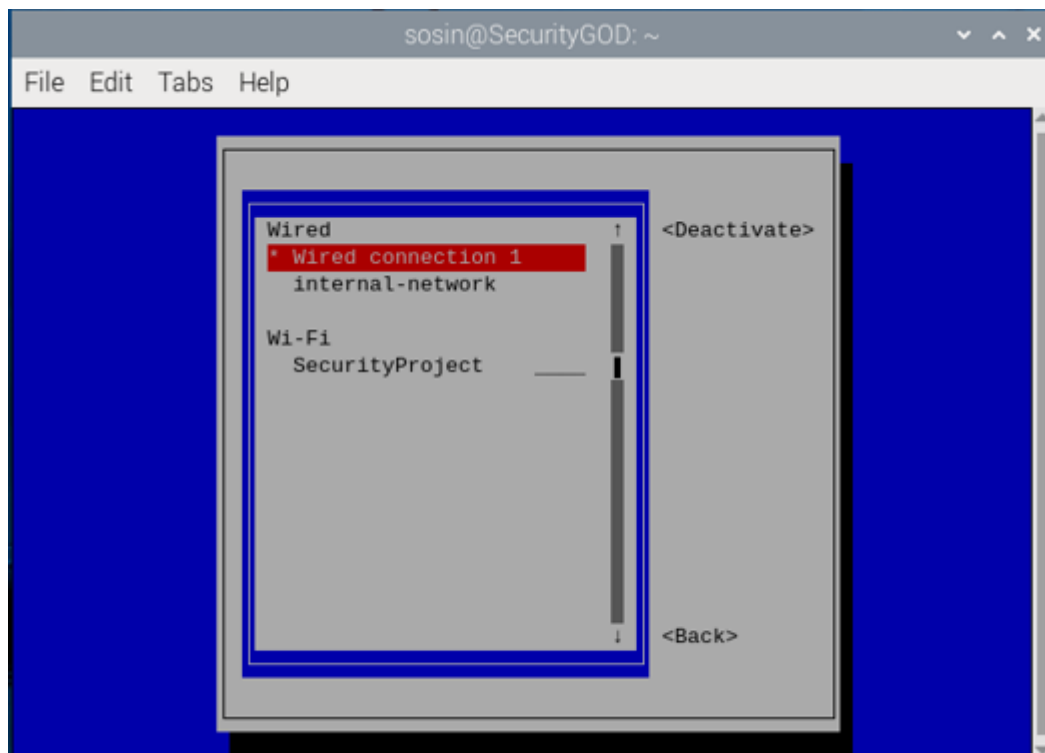


Image 3.2.5 Turning the network device off and on

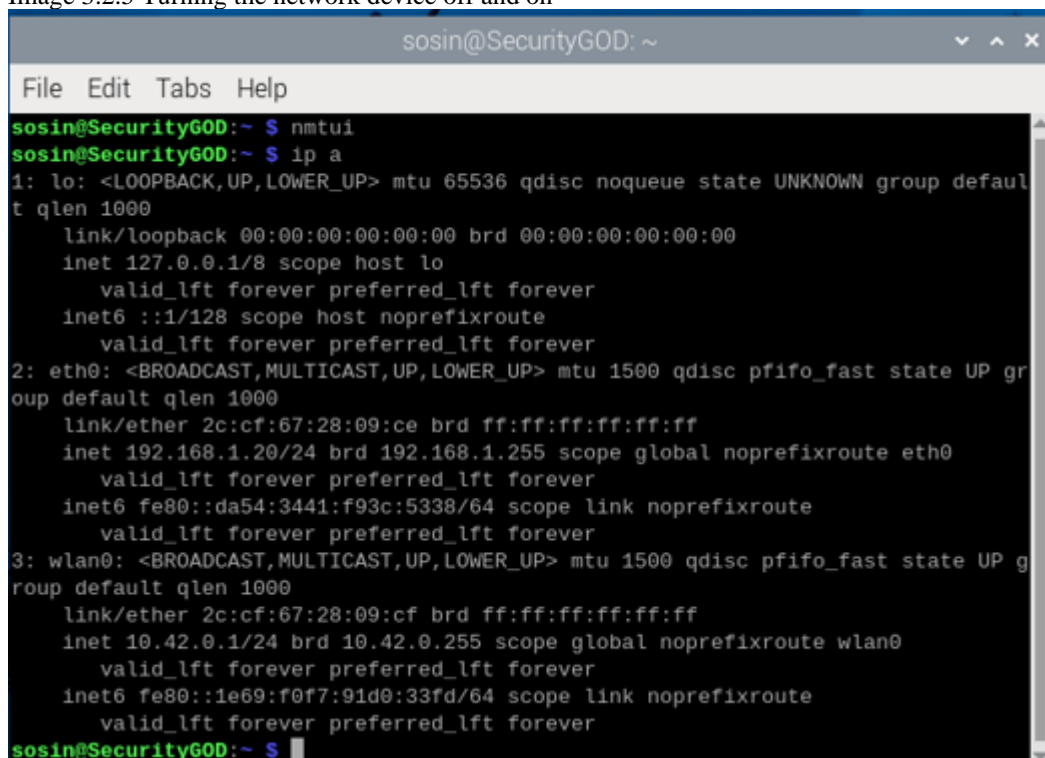
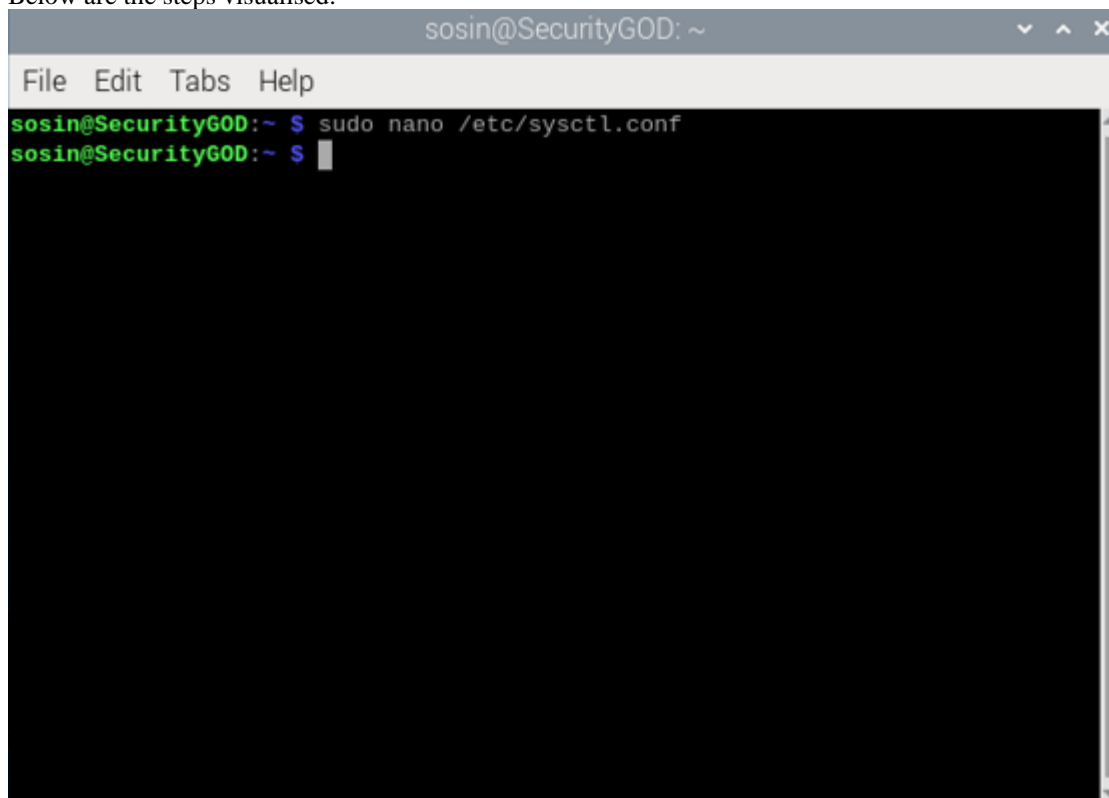


Image 3.2.6 Confirmation of the IP setup

The next series of steps will show how to setup packet forwarding (User Icarus_Radio, 2021).

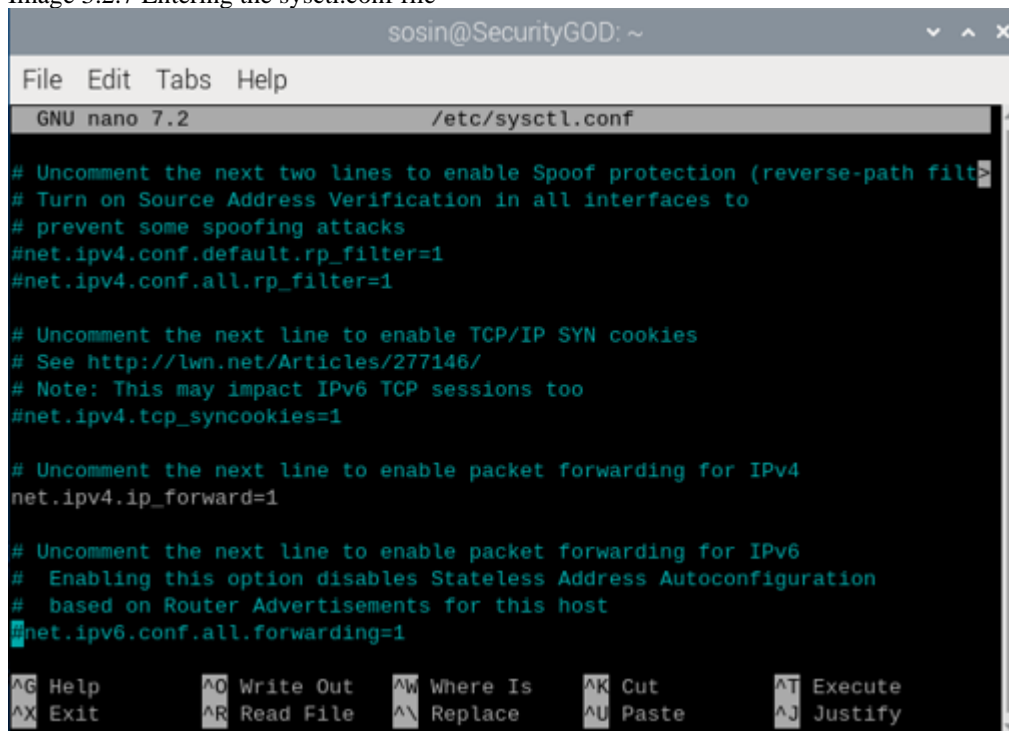
1. Open command prompt
2. Type in “sudo nano /etc/sysctl.conf”
3. Add the following argument “net.ipv4.ip_forward=1”
4. Press “CTRL S” to save
5. Press “CTRL X” to exit
6. Type “sudo sysctl -p”
7. Reboot the Raspberry Pi by typing in “reboot”

The packet forwarding has now been setup. This allows the Raspberry Pi to act as an intermediary between the host devices and the router, this is necessary otherwise the firewall, IPS and Zeek (if chosen to install) will not work correctly. As well as that if this setting is not setup the Raspberry Pi will not be able to work as a default route for the devices and the packets will be dropped and the hosts will not have a network connection. Below are the steps visualised:



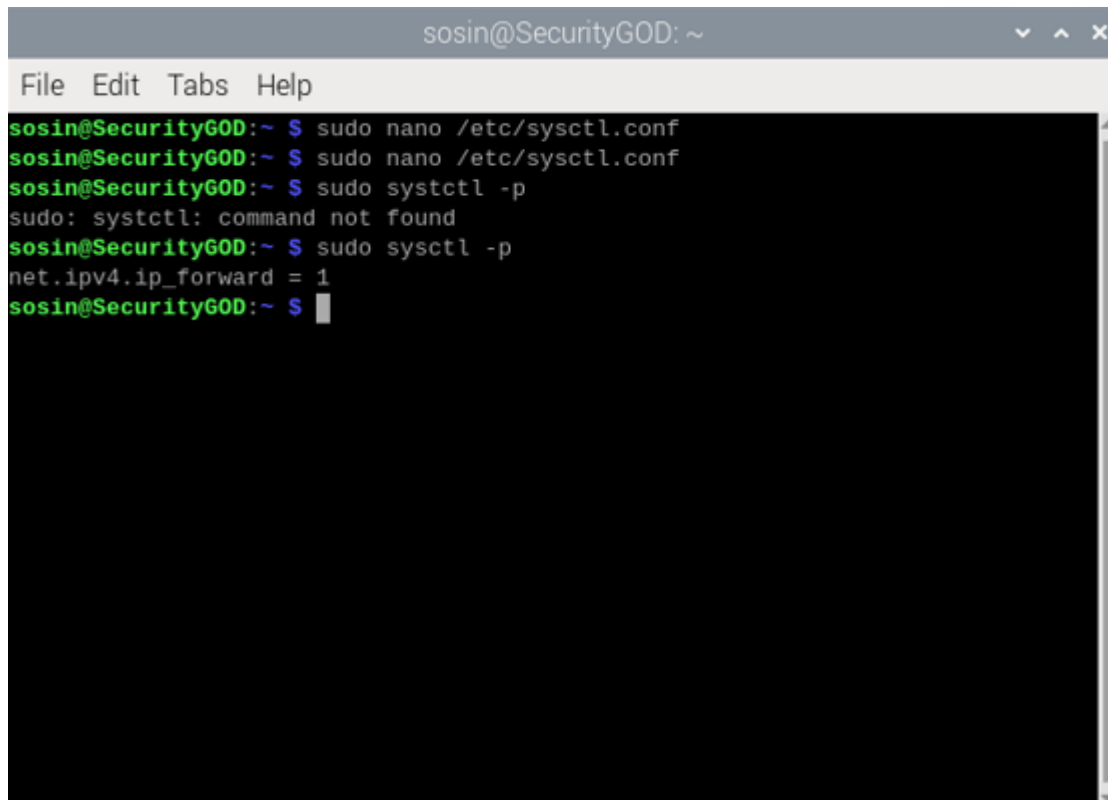
```
sosin@SecurityGOD: ~  
File Edit Tabs Help  
sosin@SecurityGOD:~$ sudo nano /etc/sysctl.conf  
sosin@SecurityGOD:~$
```

Image 3.2.7 Entering the sysctl.conf file



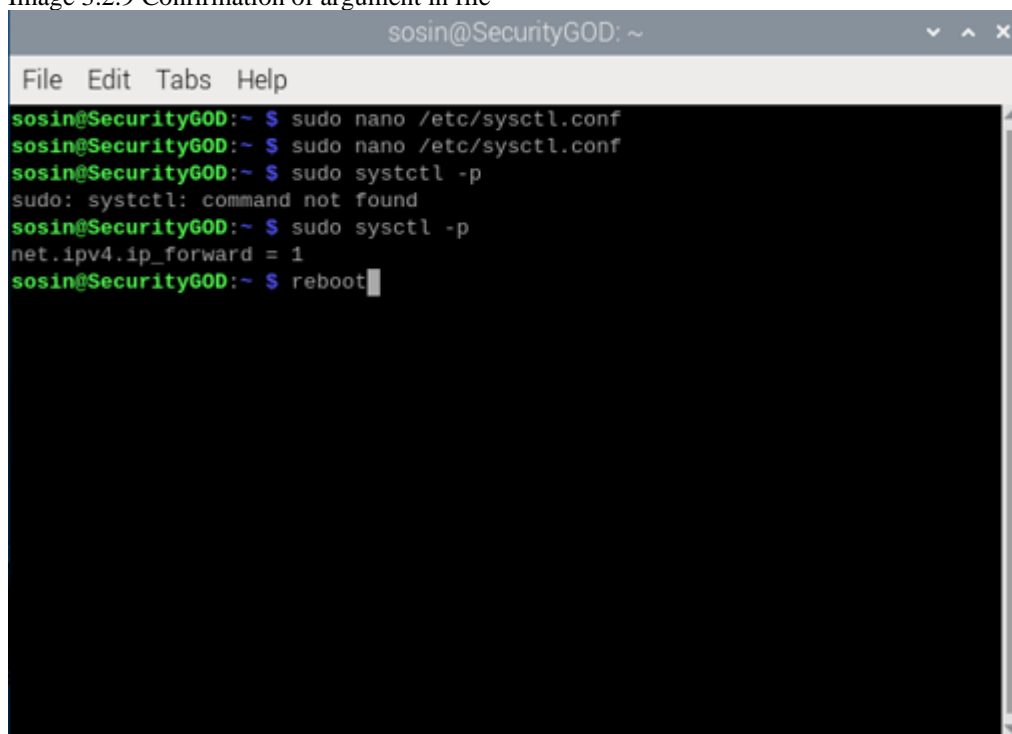
```
sosin@SecurityGOD: ~  
File Edit Tabs Help  
GNU nano 7.2 /etc/sysctl.conf  
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)  
# Turn on Source Address Verification in all interfaces to  
# prevent some spoofing attacks  
#net.ipv4.conf.default.rp_filter=1  
#net.ipv4.conf.all.rp_filter=1  
  
# Uncomment the next line to enable TCP/IP SYN cookies  
# See http://lwn.net/Articles/277146/  
# Note: This may impact IPv6 TCP sessions too  
#net.ipv4.tcp_syncookies=1  
  
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1  
  
# Uncomment the next line to enable packet forwarding for IPv6  
# Enabling this option disables Stateless Address Autoconfiguration  
# based on Router Advertisements for this host  
#net.ipv6.conf.all.forwarding=1  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Image 3.2.8 Adding the argument into the file

A terminal window titled 'sosin@SecurityGOD: ~' with a menu bar 'File Edit Tabs Help'. The terminal shows the following commands and output:

```
sosin@SecurityGOD:~ $ sudo nano /etc/sysctl.conf
sosin@SecurityGOD:~ $ sudo nano /etc/sysctl.conf
sosin@SecurityGOD:~ $ sudo sysctl -p
sudo: sysctl: command not found
sosin@SecurityGOD:~ $ sudo sysctl -p
net.ipv4.ip_forward = 1
sosin@SecurityGOD:~ $
```

Image 3.2.9 Confirmation of argument in file

A terminal window titled 'sosin@SecurityGOD: ~' with a menu bar 'File Edit Tabs Help'. The terminal shows the following commands and output:

```
sosin@SecurityGOD:~ $ sudo nano /etc/sysctl.conf
sosin@SecurityGOD:~ $ sudo nano /etc/sysctl.conf
sosin@SecurityGOD:~ $ sudo sysctl -p
sudo: sysctl: command not found
sosin@SecurityGOD:~ $ sudo sysctl -p
net.ipv4.ip_forward = 1
sosin@SecurityGOD:~ $ reboot
```

Image 3.2.10 system reboot

4.0) Setting up the Applications

It is highly recommended to use the easy installation script created and can be accessed by following this link: <https://github.com/Diickie/MSc-Degree-Project>. The files are compressed, and the user should download the file preferably on the desktop as that is where this user manual will show examples.

4.1) Using the easy install script to install Suricata and UFW with a basic configuration

1. Download the .zip file
2. Unzip the file on the Desktop
3. Open command terminal
4. Navigate into the folder on the desktop using the “cd” function
5. Run the script using the following command “sudo python3 installerSystem.py”
6. Wait for the script to finish and the Raspberry Pi to reboot
7. Ensure the applications are enabled by using “sudo systemctl status x” x being either Suricata or UFW

This step installs the firewall UFW and IPS Suricata. The installation provides a basic configuration, and it should work straight out of the box. To test attempt to ping outside of the network for example 8.8.8.8 or attempting to do a speed test. If there are any issues or if a more advanced user wants to create their own rules use these guides for more information:

1. <https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-debian> - UFW guide
2. <https://www.digitalocean.com/community/tutorials/how-to-install-suricata-on-debian-11> - Suricata guide
3. <https://www.digitalocean.com/community/tutorials/how-to-configure-suricata-as-an-intrusion-prevention-system-ips-on-debian-11> - Suricata as IPS guide

As well as that if there are any issues regarding connection check the NFQUEUE settings for both Suricata and UFW. For UFW this can be found in the file called “before” and for Suricata “/etc/systemd/system/suricata.service.d/override.conf”.

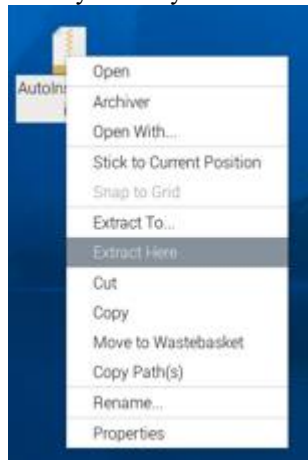


Image 4.1.1 Extraction of files to Desktop

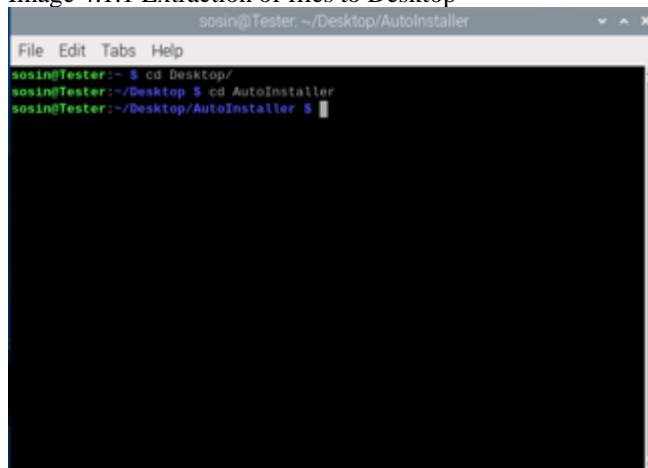


Image 4.1.2 Moving to “AutoInstaller” folder

```
sosin@Tester: ~/Desktop/AutoInstaller
File Edit Tabs Help
sosin@Tester:~$ cd Desktop/
sosin@Tester:~/Desktop$ cd AutoInstaller
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3
python3 python3.11 python3.11-config python3-config
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3
python3 python3.11 python3.11-config python3-config
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3 installerSystem.py
```

Image 4.1.3 Running the simple installer script

```
sosin@Tester: ~/Desktop/AutoInstaller
File Edit Tabs Help
sosin@Tester:~$ cd Desktop/
sosin@Tester:~/Desktop$ cd AutoInstaller
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3
python3 python3.11 python3.11-config python3-config
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3
python3 python3.11 python3.11-config python3-config
sosin@Tester:~/Desktop/AutoInstaller$ sudo python3 installerSystem.py
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-1).
suricata is already the newest version (1:6.0.10-1).
0 upgraded, 0 newly installed, 0 to remove and 34 not upgraded.
None
[Installed UFW and Suricata...]
Beginning the copying and creation of base files...
Default outgoing policy changed to 'deny'
(Be sure to update your rules accordingly)
Default incoming policy changed to 'deny'
(Be sure to update your rules accordingly)
Beginning the reset of files to ensure they work correctly...
Firewall is active and enabled on system startup
Beginning Reboot in 10 seconds...
```

Image 4.1.4 Script running successfully

```
sosin@Tester: ~
File Edit Tabs Help
sosin@Tester:~$ sudo systemctl status ufw
● ufw.service - Uncomplicated Firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; preset: enabled)
   Active: active (exited) since Tue 2024-07-30 21:20:52 BST; 1min 30s ago
     Docs: man:ufw(8)
   Process: 593 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0)
   Main PID: 593 (code=exited, status=0/SUCCESS)
     CPU: 7ms

Jul 30 21:20:51 Tester systemd[1]: Starting ufw.service - Uncomplicated firewall.
Jul 30 21:20:52 Tester systemd[1]: Finished ufw.service - Uncomplicated firewall.
lines 1-10/10 (END)
sosin@Tester:~$ sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: ena
   Drop-In: /etc/systemd/system/suricata.service.d
            ↳ override.conf
   Active: active (running) since Tue 2024-07-30 21:20:59 BST; 1min 27s ago
     Docs: man:suricata(8)
            man:suricata-sc(8)
            https://suricata-ids.org/docs/
   Main PID: 1489 (Suricata-Main)
     Tasks: 12 (limit: 4439)
       CPU: 470ms
   CGroup: /system.slice/suricata.service
           ↳ 1489 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile

Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Perf> - Builti
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Perf> - Builti
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Config> - AutoF
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Info> - binding
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Info> - setting
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Info> - setting
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Config> - using
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Config> - using
Jul 30 21:20:59 Tester suricata[1489]: 30/7/2024 -- 21:20:59 - <Info> - Using v
lines 1-23
sosin@Tester:~$
```

Image 4.1.5 Checking if processes are running successfully

4.2) Installing Pi-Hole

The Pi-Hole installation is very nice to install. It is however not gotten through the “apt install” method rather the user has to install it using “curl -sSL https://install.pi-hole.net | bash” which is an automated installer other options are available on the official website (Pi-Hole Team, 2024)

The installation is done through a graphic interface and the screenshots below will show what the settings should look like for the sample network used in this user manual (Pi-Hole Team, 2024).

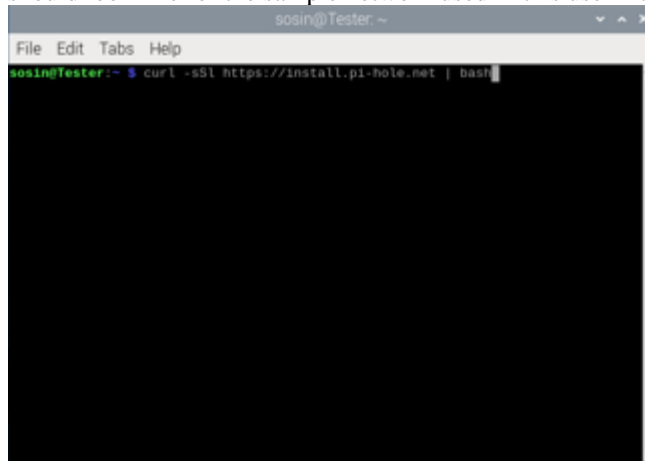


Image 4.2.1 Command used for installation

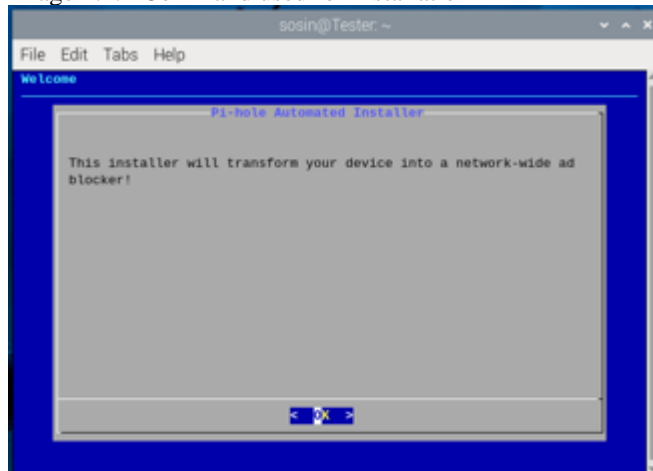


Image 4.2.2 Information first page of installer

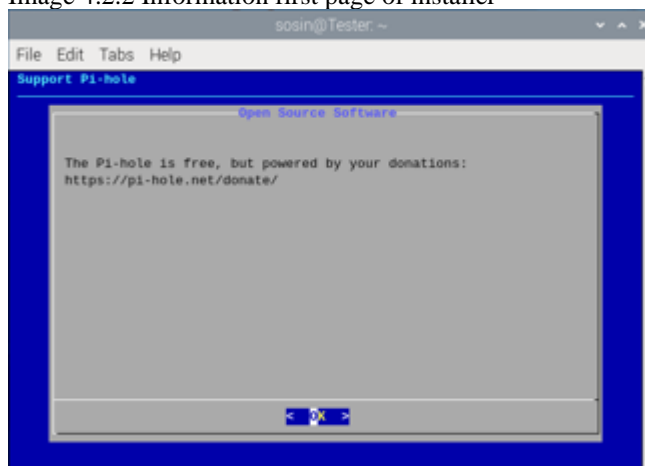


Image 4.2.3 Donation page can be ignored

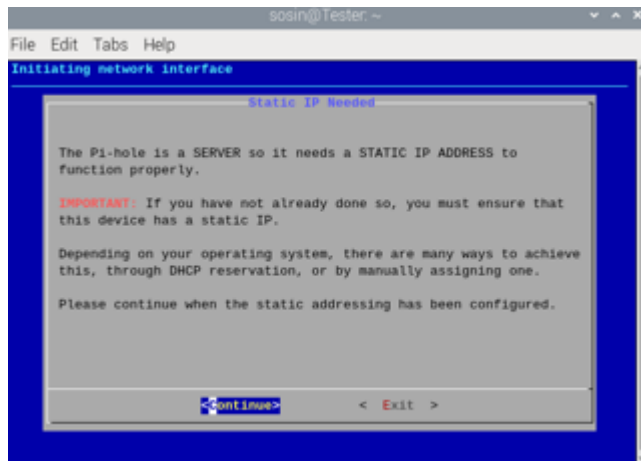


Image 4.2.4 Static IP has already been set continue

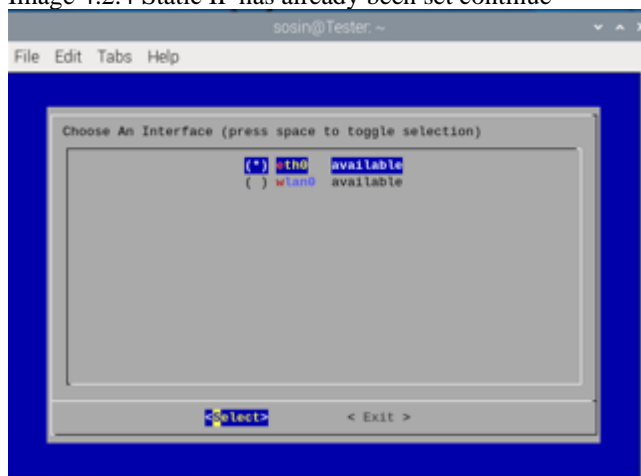


Image 4.2.5 Choosing interface

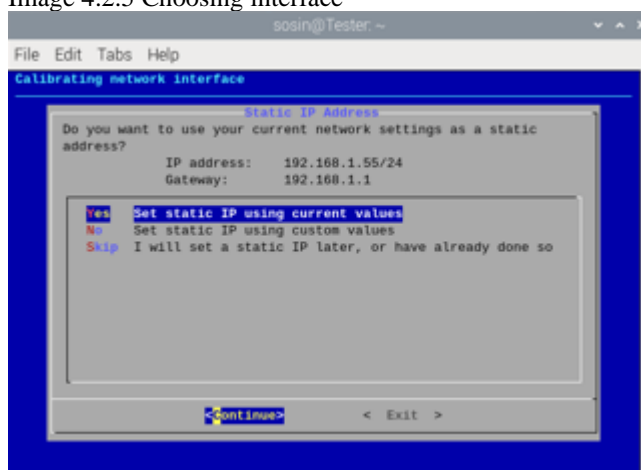


Image 4.2.6 Skip this step

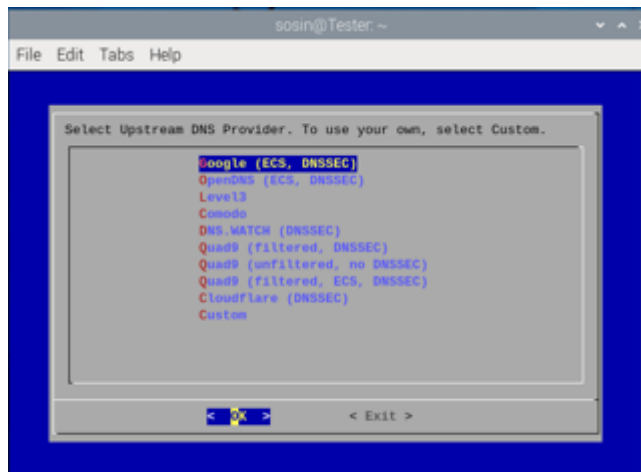


Image 4.2.7 Choose DNS this manual uses Google

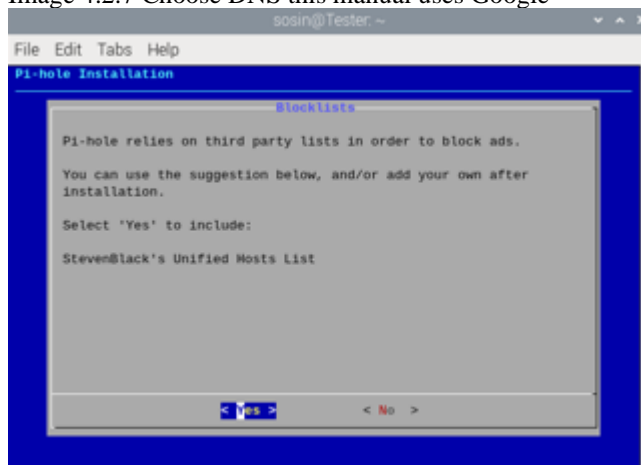


Image 4.2.8 Installing third party ad lists

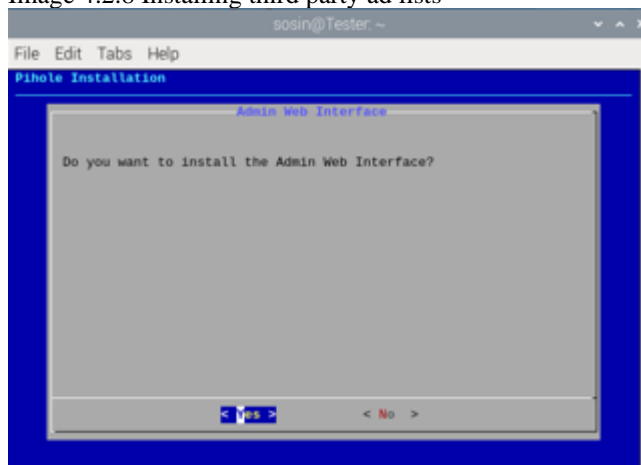


Image 4.2.9 Installing Graphic Interface through a browser

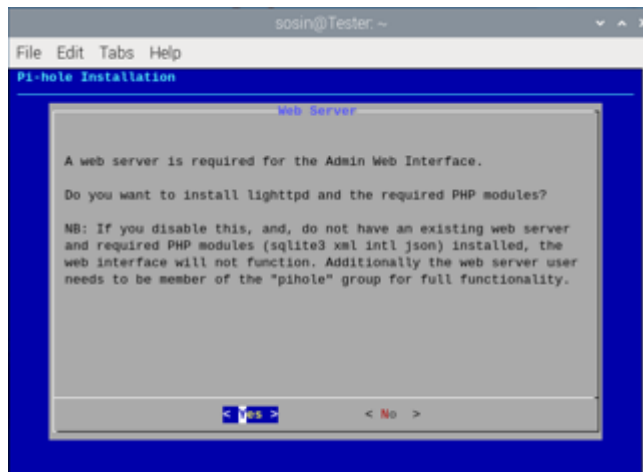


Image 4.2.10 Installing a web server to be able to run the graphic interface

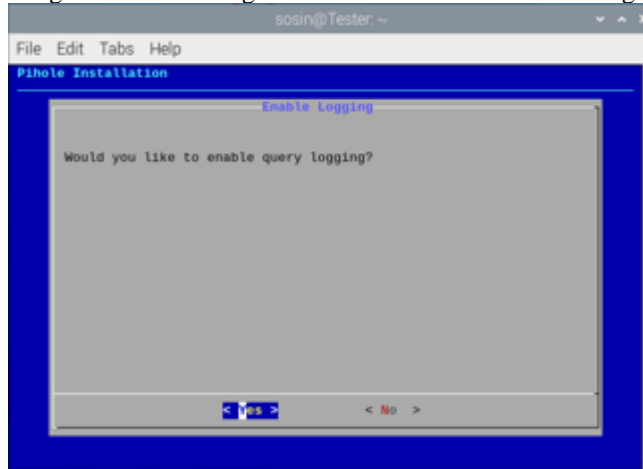


Image 4.2.11 Enable logging

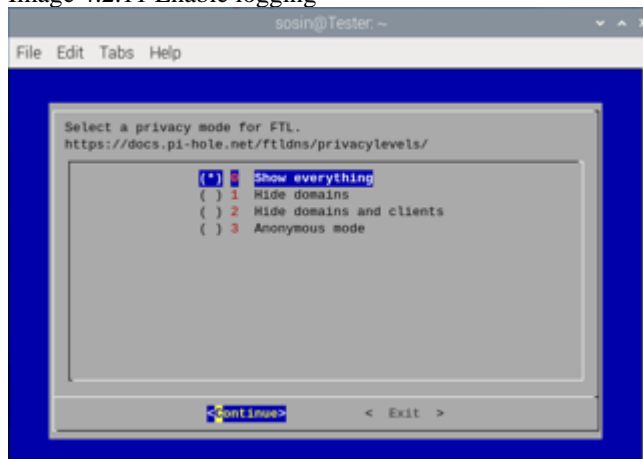


Image 4.2.12 Choosing the option to be able to see traffic (choosing which log to view)

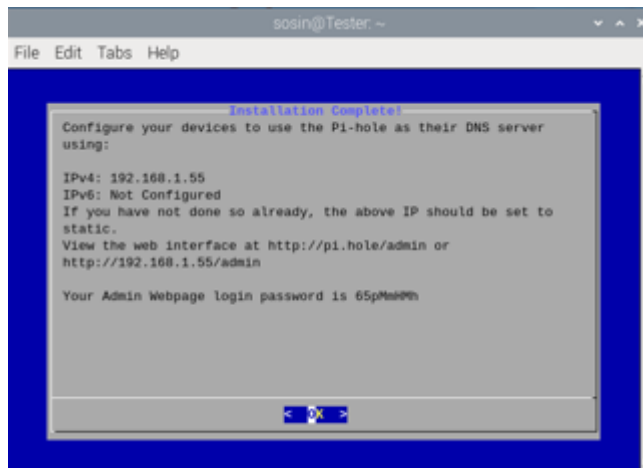


Image 4.2.13 Final page from setup showing how to login and what password to use

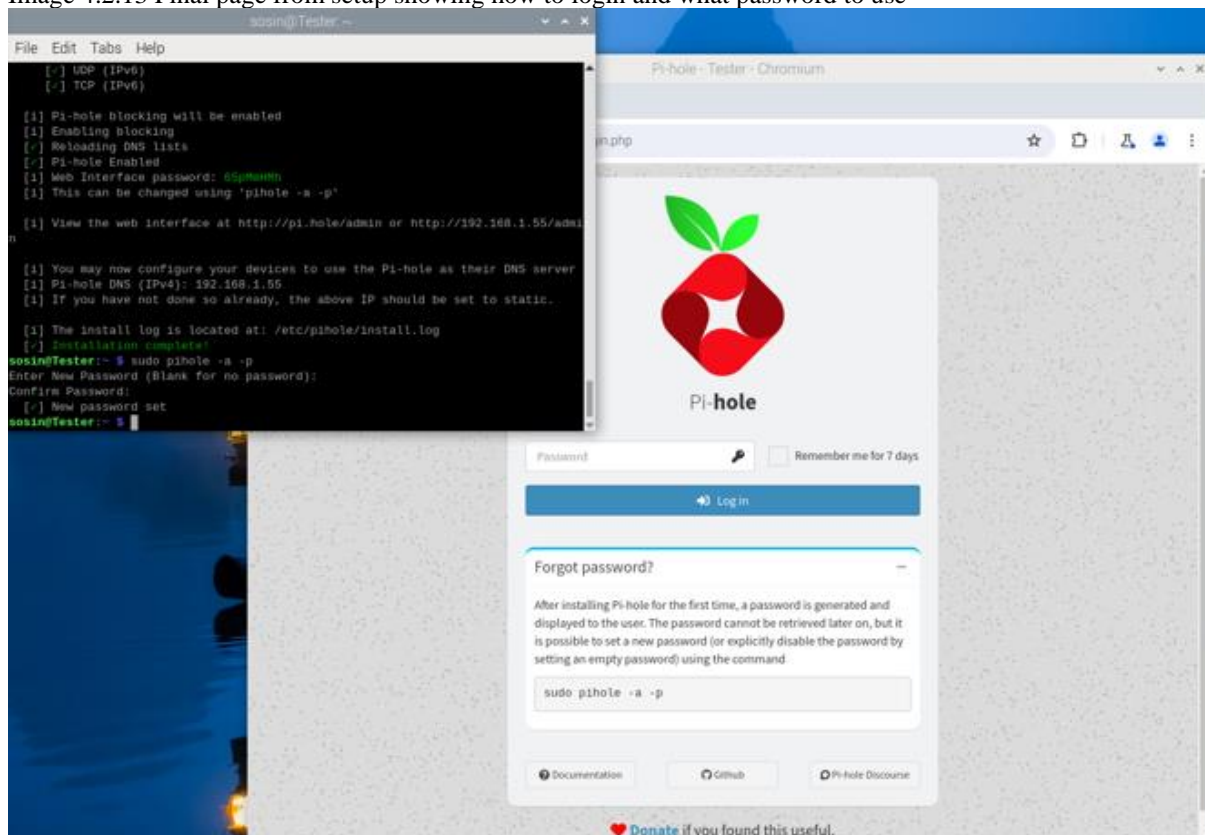


Image 4.2.14 Changing password for logging in

4.3) Installing Zeek

Zeek can be very temperamental and, when attempting to re-trace the steps taken to install the application but this time it failed. This step is not necessary for the final device, this is just an additional way of adding another layer of security. Zeek is an IDS so it would only inform the user that an attack is happening however, there is an IPS (Suricata) which will stop the attack from happening. What can be done instead could be running Wireshark as they both work as network analysers, but Zeek would be doing it without consuming too many resources rather than Wireshark looking at every packet coming in.

The guide which should be used for this installation if wanted to and it is recommended for more advanced users can be found here (Github user devnull-hub, 2023) .

4.4) Using the Backup System Script

The backup system script works as a way to backup the whole raspberry pi into one file (Ubuntu Team, 2024). This is recommended to be done once after all test to make sure everything is working is done and after that it should be done monthly.

1. Make the directory/folder where the backups are going to be stored for example “/home/x/backups”
2. Change the value of “DEST_FOLDER” in the “backup.sh” file so that it reflects the directory of the backups
3. Check permissions of the backup file using “ls -la” it should come with “rwxrwxrwx”
4. If permissions are incorrect run “sudo chmod 777 backup.sh”
5. Once that is completed run the script by using the following “sudo ./backup.sh”
6. The file will be created in the format of “hostname-day.tar”
7. It is highly suggested that the file is then exported to a USB as well as a cloud storage service like OneDrive or Google Drive

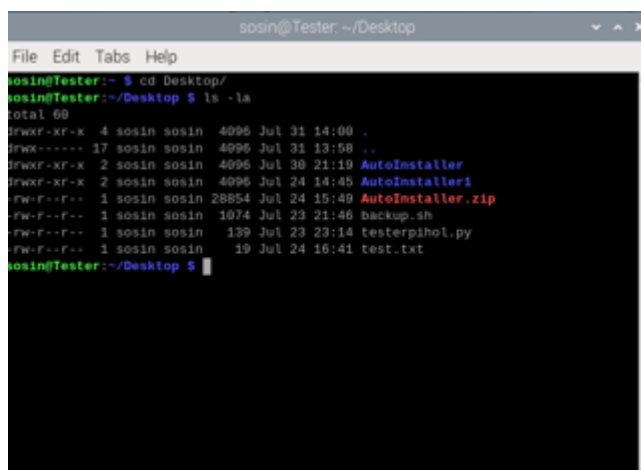
A terminal window titled 'sosin@Tester ~/Desktop' showing the output of the 'ls -la' command. The output lists several files and directories with their permissions, owner, group, size, and timestamps. The file 'backup.sh' is highlighted with a red background and shows permissions '-rwxr-xr-x'.

Image 4.4.1 Checking permissions of backup.sh

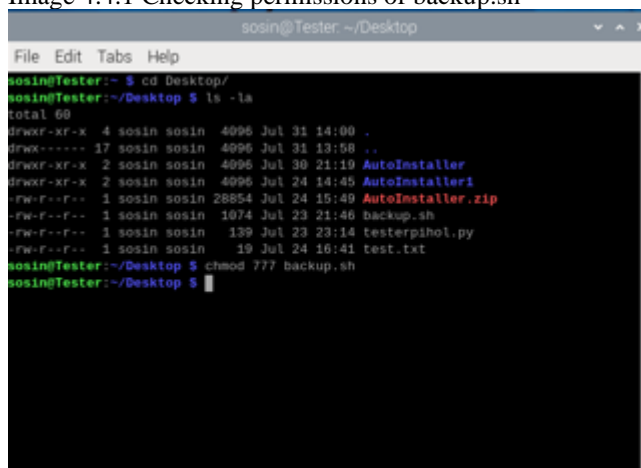
A terminal window titled 'sosin@Tester ~/Desktop' showing the output of the 'ls -la' command followed by the execution of the 'chmod 777 backup.sh' command. The output of 'ls -la' is the same as in the previous image. The 'chmod' command is executed successfully, and the prompt returns to the user.

Image 4.4.2 Adding permissions to backup.sh

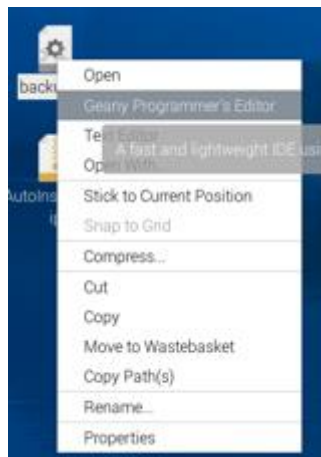


Image 4.4.3 How to access text editor

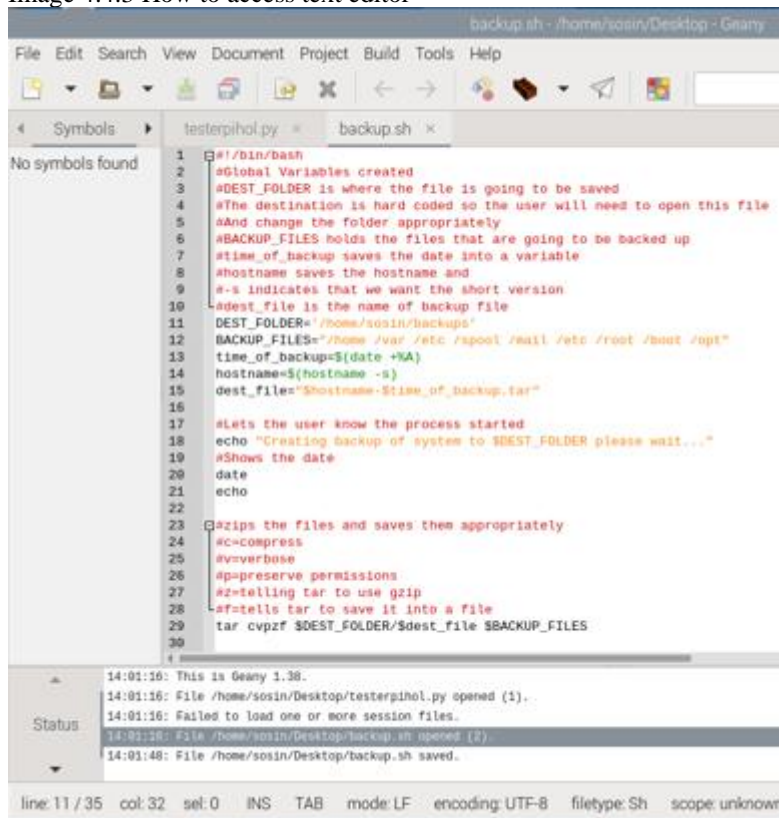


Image 4.4.4 Adding correct value to DEST_FOLDER

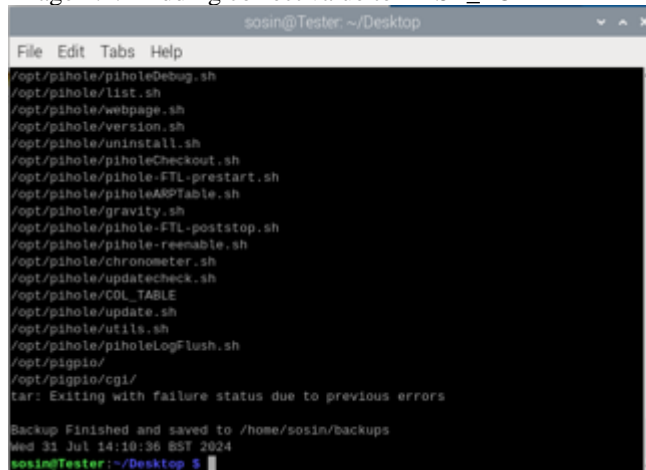


Image 4.4.5 Backup script finished running the error can be ignored

References

Github user devnull-hub (2023) How to use a Raspberry PI 4 as a Network Sensor with Zeek and Rita, How to use a Raspberry PI 4 as a Network Sensor with Zeek and Rita. Available at: <https://github.com/devnull-hub/rita-zeek-rpi4> (Accessed: 8 August 2024).

Pi-Hole Team (2024) Installation, One-Step Automated Install¶. Available at: <https://docs.pi-hole.net/main/basic-install/> (Accessed: 8 August 2024).

Raspberry Pi Team (2024a) Raspberry Imager installer, Software. Available at: <https://www.raspberrypi.com/software/>.

Raspberry Pi Team (2024b) Raspberry Pi Documentation, Getting Started. Available at: <https://www.raspberrypi.com/documentation/computers/getting-started.html> (Accessed: 8 August 2024).

Ubuntu Team (2024) Basic backup shell script, Basic backup shell script. Available at: <https://ubuntu.com/server/docs/basic-backup-shell-script> (Accessed: 5 August 2024).

User Icarus_Radio (2021) ‘Cannot enable IP forwarding on 64-bit Pi OS’, Raspberry Pi Forum. Available at: <https://forums.raspberrypi.com/viewtopic.php?t=313116> (Accessed: 8 August 2024).