NETWORK RESEARCH PROJECT REMOTE CONTROL

Student: Dinie Haziq Bin Mohamad Raafe, S9

Class: CFC2407

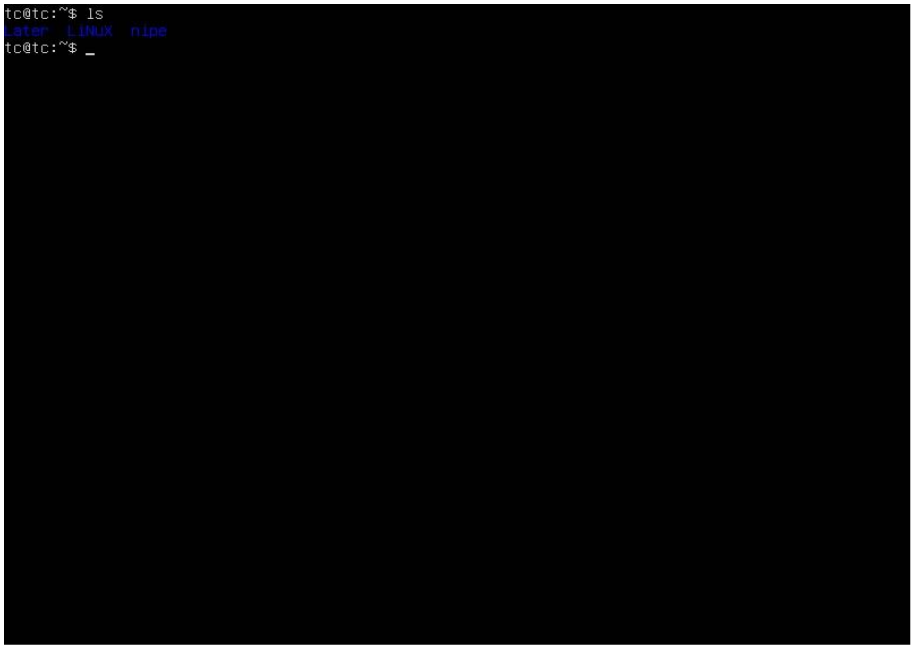
Lecturer: James

For this project, we are required to create a script that communicates with a remote server and executes task anonymously.

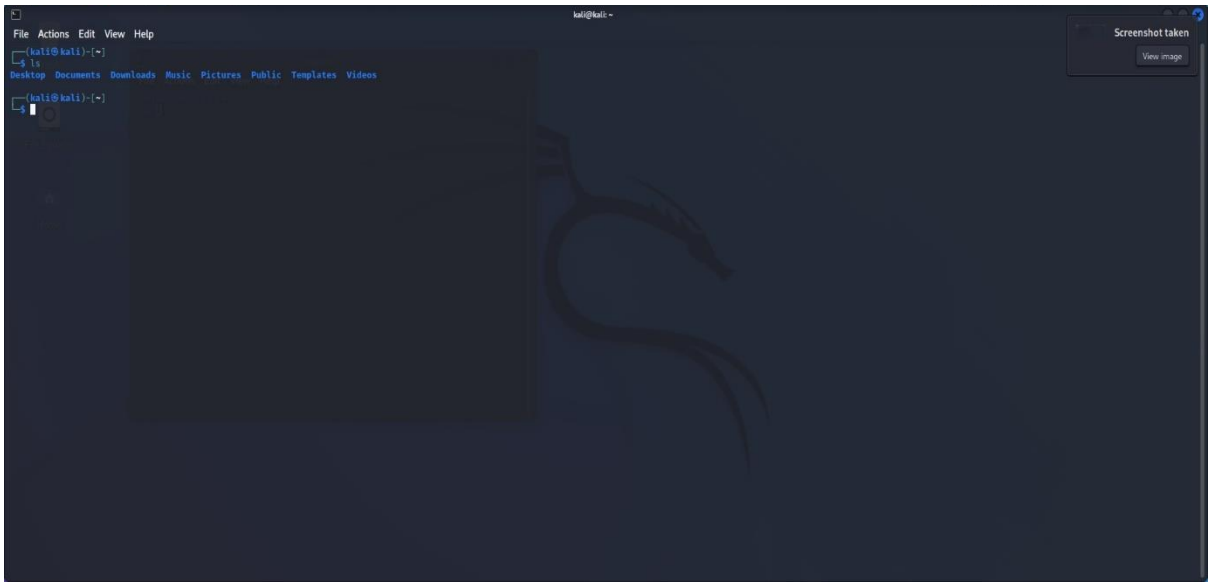
I will be using Ubuntu as my remote server and fresh kali machine to run this script. For the task that needs to be done on the remote server (Ubuntu) is to scan IP address with nmap and store the information on my local machine (Kali Linux). For anonymity, I will be using a tool called nipe.

Nmap - "Network Mapper" is a free and open source utility for network discovery. We use this to scan for open ports, what kind of services are open, the version of services, and what operating system and version they are using.

Nipe – Is a script to make Tor Network our default gateway. Tor in short for The Onion Routing, is an open-source privacy network that enables anonymous web browsing.



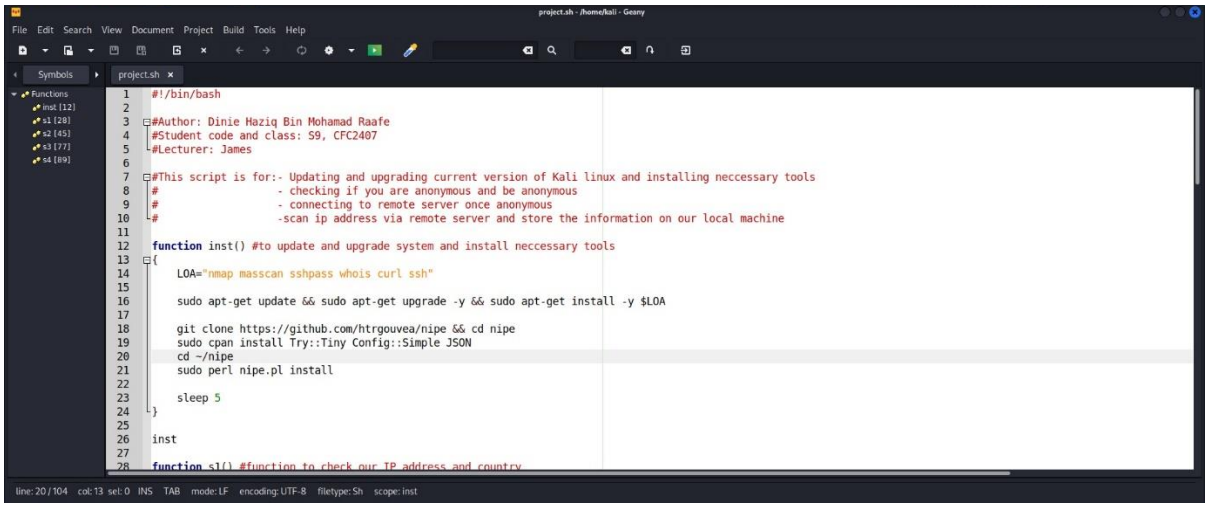
As you can see, there are no files in this ubuntu.



And this is a fresh kali machine just for this project.

So, for this script, I'm naming it **project.sh**

I will be showing the script and explain it before I show you how the script execute.



Script inst

This is the start of the script. We started off with **#!/bin/bash** .

#! – It's called shebang. The part after #! tells the system what program/language to use, for example, python, perl, ruby, etc. For this case, its bash.

- The hash is a comment in most languages, so the lines with # gets ignored in the subsequent execution.

function – It is a method to store commands in a block to make it reusable. Any commands written in between **{ }** will be stored. We give a name after **function** so we can call out the commands in that specific block, for this case, **inst**.

For this, I will be explaining the script function by function for easier understanding.

As you can see, the at start of **inst**, there is a line, **LOA=** "nmap masscan sshpass whois curl ssh"

LOA is a variable. It is a temporary store for a piece of information. We could use any words, alphabets, or numbers if it doesn't clash with a command. To read the variable, we place its name preceded by a **$** sign. So, for **LOA**, I have input the tools I need for this project.

Now the variable all set, we need to update and upgrade our system. We require root privileges. Instead of switching into root, I used **sudo** – "super user do", or "substitute user do". The **sudo** command elevates the current user to have root access. However, not all user has **sudo** access. Users need to be included in the **sudo** group in the system to have access to **sudo**.

COMMANDS	WHAT DOES IT DO?
sudo	It allows programs or commands to be executed as super user or root user.
apt-get	apt – Advance Packaging Tool. It is a command line tool which helps in handling packages in Linux. It is task to retrieve information and packages from authenticated resources.
update	This command is used to synchronize the package index files from the source. This must be done before upgrade as to receive the most updated packages.
upgrade	It is used to install the latest versions of the updated packages.
install	It is used to install packages that the user wishes.
-y	This flag is used in the command line to specify that it should assume 'yes' for all prompts and should run without any interaction.
&&	It is used to execute multiple commands simultaneously.

So, from the table above, the second line in **inst**, it is telling the machine to update all its resources to the latest version and upgrade the machine to the latest version and install all the tools stated in **$LOA**.

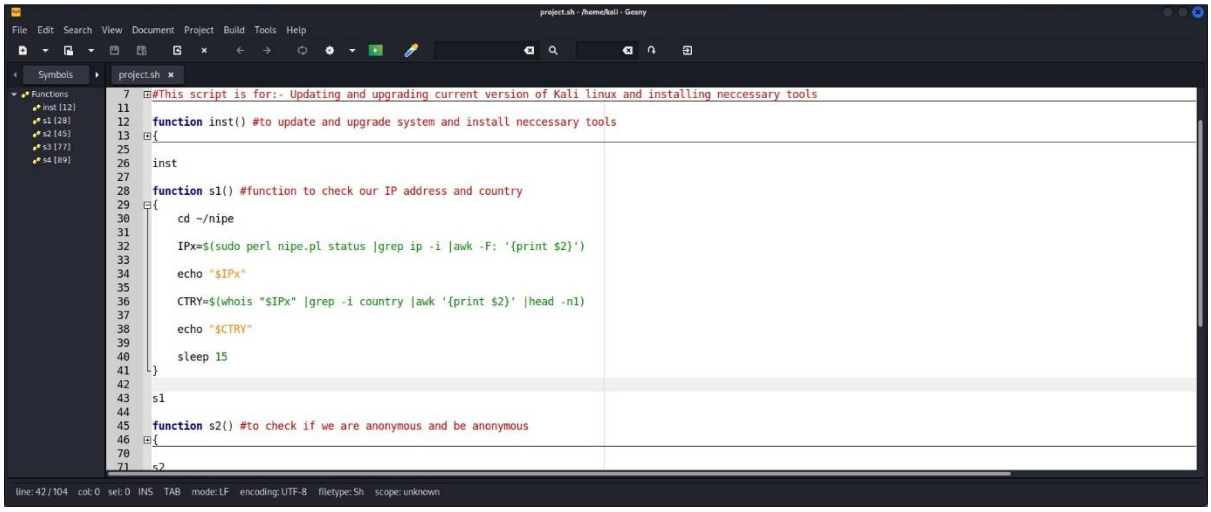
Next, we need to install **nipe.** However, **nipe** is not found in the apt library (/etc/apt/sources.list) as nipe is a project done by developer Heitor Gouvêa at github, thus we use **git clone.**

git clone is a Git command line utility which is used to target an existing repository and create a clone or copy of the target repository.

The instructions to download and install **nipe** can be found on his github page. (https://github.com/htrgouvea/nipe)

Right before the command line **sudo perl nipe.pl install**, there is a command line **cd ~/nipe.**

It means to change directory (**cd**) to **nipe** folder. We need to be in the folder to run the program. The **~** is the user home directory.



Script s1

For script s1, we use this function block to store command lines to display our IP address and which country this IP address is originating.

Like **LOA**, I will be storing the result of the variable in **IPx**.

IPx =$(<command>) – Reads the exit status of the command in the brackets and store it in **IPx.**

echo "$IPx"** – Is to read and display what is in **$IPx

An important thing to note, " " and ' ' does not produce the same result. ' ' will store is as it is and not as a variable, where as " " stores it as a variable.

For example, take it IP address as 192.168.29.130 stored in **IPx**

echo "$IPx" will show **192.168.29.130** in the terminal where as

echo '$IPx'** will show **$IPx in the terminal.

I will be using the table below to explain the command line found within **$( )**

COMMANDS	WHAT DOES IT DO?
sudo	It allows programs or commands to be executed as super user or root user.
perl	It is a programming language. It specify the system what language to execute the programme. In this case is perl.
nipe.pl	The programme to execute.
status	To state the condition of the programme and its details.
|	The vertical bar connects the commands together making it possible to create a chain of related but separate processes.
grep ip -i	grep filter searches a file for a pattern of characters and displays all lines that contains that pattern. For in this case is **ip**. For **-i** flag, it tells the system to ignore upper case and lower case of the searched pattern.
awk	awk is a language for manipulation of data files, text retrieval and processing
-F:	it tells **awk** what field seperator to use. In this case, its **:**
'{print $2}'	it means print the second field seperated by **:**

So for this line of commands, **IPx =$(sudo perl nipe.pl status |grep ip -i |awk -F: '{print $2}')**

It is telling the system to run **nipe.pl**, display the status of the programme, search for **ip**, and display the second field of the result seperated by **:** and store it as **IPx**.

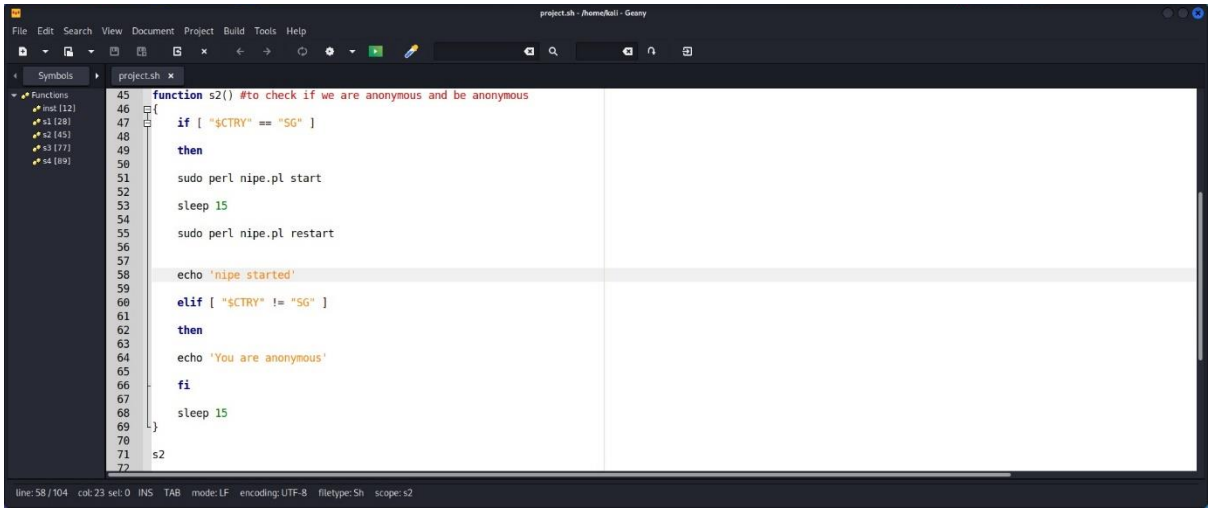
So for the next line of commands, it will be explained in the table below

COMMANDS	WHAT DOES IT DO?
whois	it is a query and response protocol that is used to search databases that store the registered users of an internet source, such as domain, ip address block, country and other information.
head -n1	the **head** command prints the first 10 line by default. **-n** flag followed by an interger (**1**)specify the number of lines to be shown.

CTRY=$(whois "$IPx" |grep -I country |awk '{print $2}' |head -n1 is telling the system to run **whois** on the ip address stored in **$IPx** and search for country and display the second row, first line and store the result as **CTRY**

echo "$CTRY" will display the result stored in **CTRY**

sleep 15 – means to wait 15 seconds before continuing to read the next line of commands.



Script s2

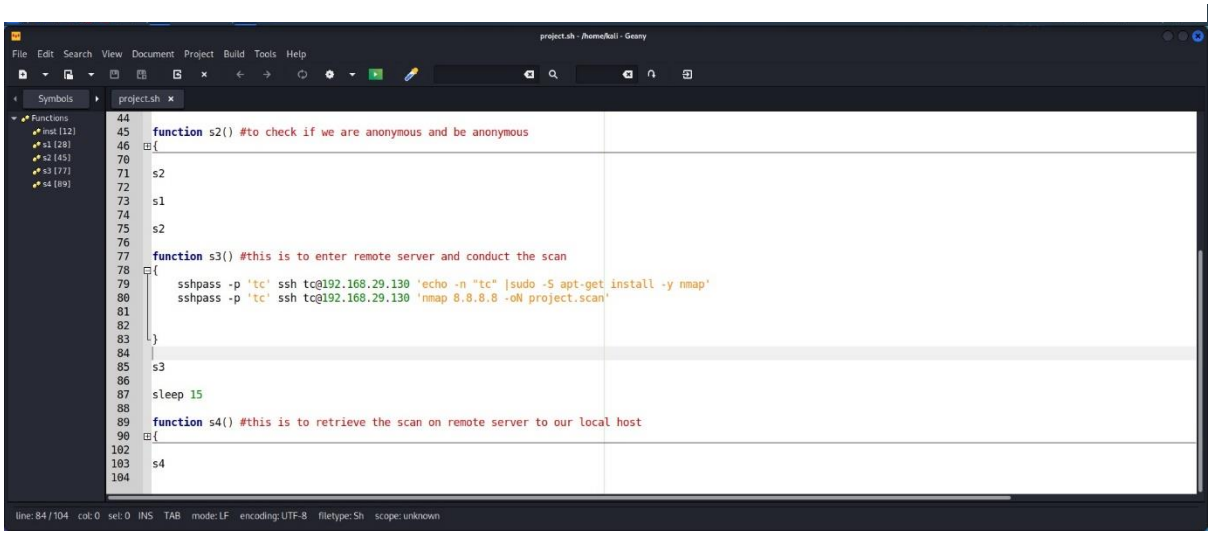
For **function s2**, we are checking if we are anonymous. By getting the variable we got from **s1**, **$CTRY**, we can check if our ip address is from my country of origin by comparing the result to our country short abbreviations, for in this caseis SG (Singapore).

By using **If statements**, it allows us to make decisions in our bash scripts. It tell the machine whther or not to run a piece of code based on the conditions that were set. And by using **elif**, we are able to set a series of conditions that may lead to different paths.

Example:

if [<condition>]
then
<commands>
elif [<condition>]
then
<different commands>
else
<other commands>
fi

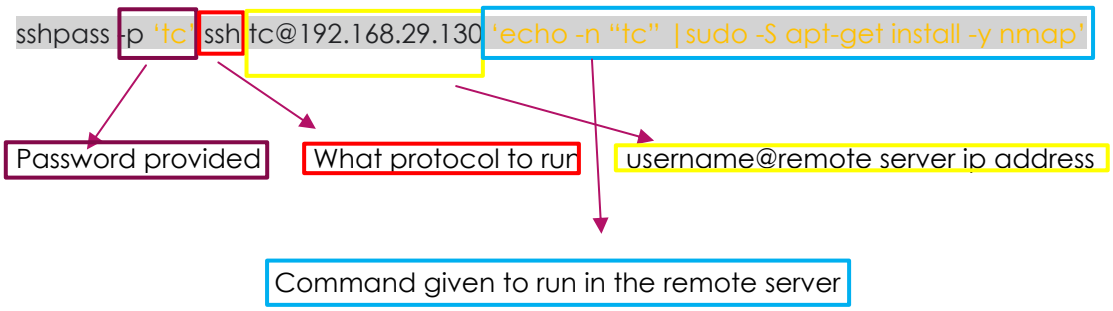
Thus for **s2**, we are telling the system that if **$CTRY** is equals **(==)**to **SG**, then run **sudo perl nipe.pl start** to run the nipe program, and **sudo perl nipe.pl restart** to restart the program. Else if **$CTRY** is not equals to **(!=)** **SG**, then display in the machine **'You are anonymous'**



Script s3

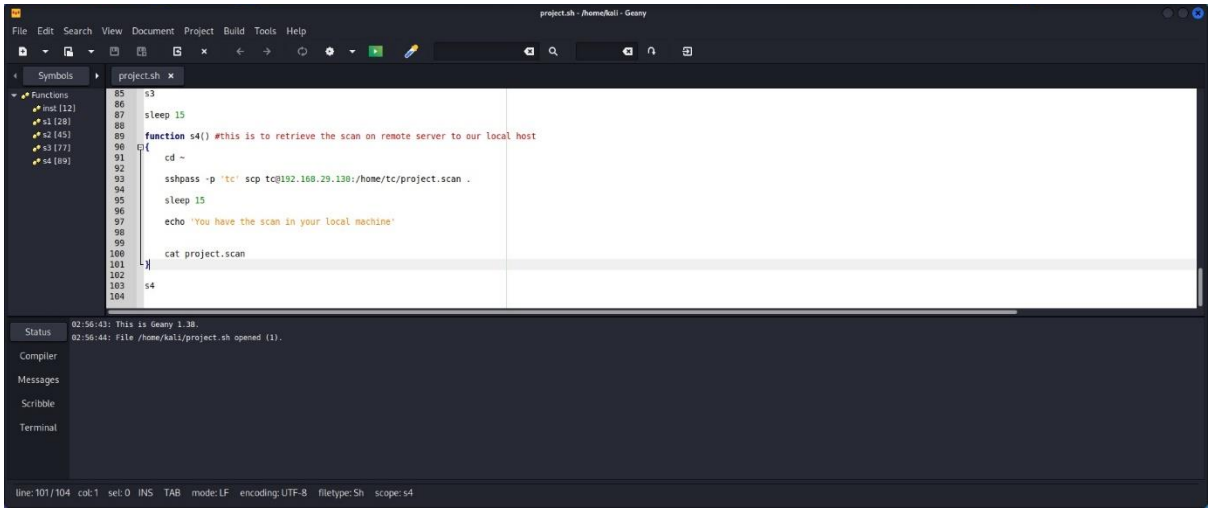
Once we anonymous, we connet to a remote server thru SSH protocol, also known as Secure Shell protocol. It is a network protocol that gives users, a secure way to access a computer over an unsecure network.

Using sshpass, which is a utility designed for running ssh using the mode referred to as "keyboard-interactive" password authentication, but in non-interactive mode. The -p flag in the command means password.



In the command, as **sudo** requires password to be typed in the terminal, the flag **-S** is used, to read the password from the standard input instead of the terminal to make the script run without asking for password. To prevent the password being displayed in the terminal the flag **-n** is used for echo. The **-n** flag prevents **echo** from displaying the password into the terminal.

For this project, I am going to scan IP address **8.8.8.8** and using **-oN** flag, it will save the output in **nmap**'s normal format, which is roughly the same as the standard interactive out of **nmap**. This file will be saved as **project.scan**



Script s4

Having run the commands needed to in the remote server, which is to run a scan of an IP address using nmap and saving it as **project.scan**, we need to retrieve the file by **SCP**. SCP is Secure Copy Protocol that enables secure transfer of computer files between a local host and a remote host.

Using **sshpass** to connect to the remote server, instead of using **ssh** as the protocol, we are using **scp** as the protocol to retrieve the file from the remote server.

sshpass -p 'tc' scp tc@192.168.29.130:/home/tc/project.scan .

Password provided

What protocol to run

username@remote server ip address

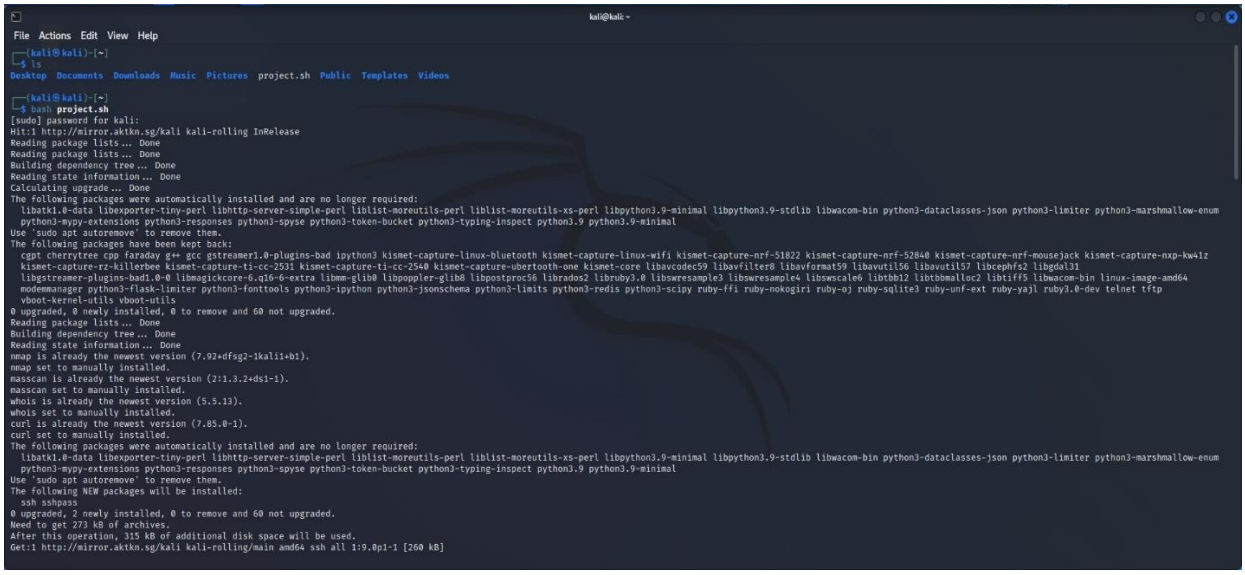
The directory of the file that needs to becopied (remote host) and the location the file needs to be saved (local host).

. in this command means in my current directory. Thus it is telling to save the file in my current directory.

cat project.scan means to display what is in that file in the terminal.

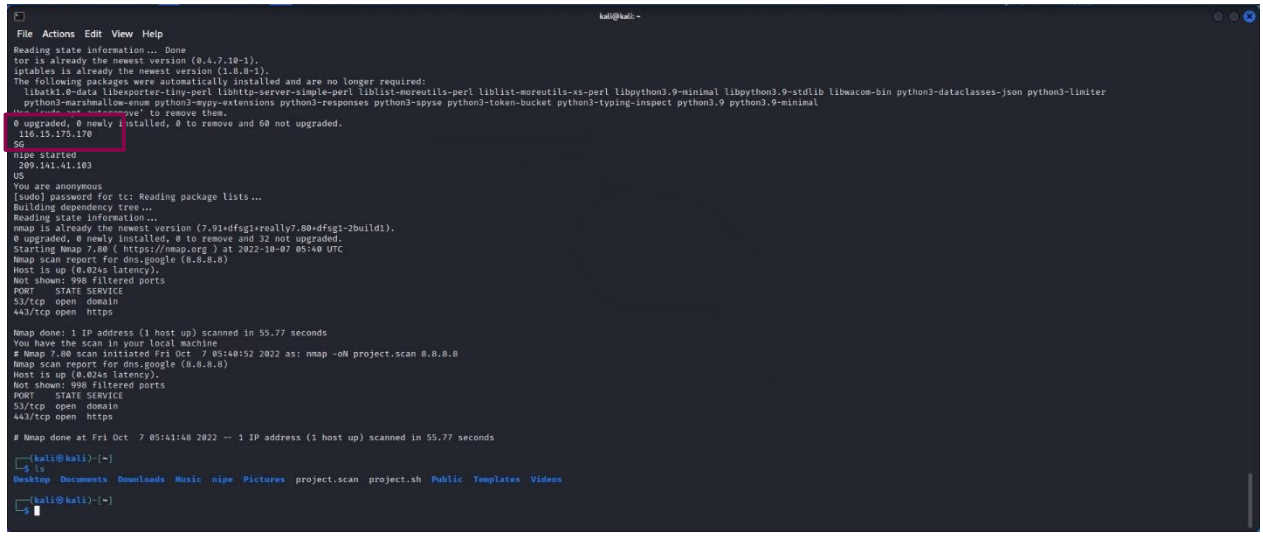
So the flow of the script is running this blocks of functions in this sequence

inst -> s1 -> s2 -> s1 ->s2 -> s3 -> s4



Running the script

As you can see in the picture above, the script is running the installationof the necessary tools written in **function inst**.



The highlighted box displayed results from $IPx and $CTRY from **function s1.** Our current IP address is **116.15.175.170** and our country is **SG**.

```
kali@kali: ~
File  Actions  Edit  View  Help
Reading state information ... Done
tor is already the newest version (0.4.7.10-1).
iptables is already the newest version (1.8.8-1).
The following packages were automatically installed and are no longer required:
  libatk1.0-data libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin python3-dataclasses-json python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
 116.15.175.170
SG
nipe started
 209.141.41.103
US
You are anonymous
[sudo] password for tc: Reading package lists ...
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2build1).
0 upgraded, 0 newly installed, 0 to remove and 32 not upgraded.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-07 05:40 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 55.77 seconds
You have the scan in your local machine
# Nmap 7.80 scan initiated Fri Oct  7 05:40:52 2022 as: nmap -oN project.scan 8.8.8.8
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

# Nmap done at Fri Oct  7 05:41:48 2022 -- 1 IP address (1 host up) scanned in 55.77 seconds

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Pictures  project.scan  project.sh  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$
```

This highlighted box is telling us that because we are not anonymous from the result above, **function s2** has started to run **nipe**. After running **nipe**, the script goes back to **function s1** to check our IP address and country location.

As the result is shown, our IP address after running **nipe** is **209.141.41.103** and our country is **US**

And because of this, the terminal echoed **'You are anonymous'**.

```
kali@kali: ~
File  Actions  Edit  View  Help
Reading state information ... Done
tor is already the newest version (0.4.7.10-1).
iptables is already the newest version (1.8.8-1).
The following packages were automatically installed and are no longer required:
  libatk1.0-data libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin python3-dataclasses-json python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
 116.15.175.170
SG
nipe started
 209.141.41.103
US
You are anonymous
[sudo] password for tc: Reading package lists ...
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2build1).
0 upgraded, 0 newly installed, 0 to remove and 32 not upgraded.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-07 05:40 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 55.77 seconds
You have the scan in your local machine
# Nmap 7.80 scan initiated Fri Oct  7 05:40:52 2022 as: nmap -oN project.scan 8.8.8.8
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

# Nmap done at Fri Oct  7 05:41:48 2022 -- 1 IP address (1 host up) scanned in 55.77 seconds

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Pictures  project.scan  project.sh  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$
```

This highlighted box represents **function s3**. It is downloading the tools needed which is nmap into the remote server and started the scan and saving the output into a file.

```
tc@tc:~$ ls
Later  LINUX  nipe
tc@tc:~$ ls
Later  LINUX  nipe
tc@tc:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2022-10-04 12:32:21 UTC; 2h 51min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 859 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 897 (sshd)
      Tasks: 1 (limit: 911)
     Memory: 1.6M
        CPU: 657ms
     CGroup: /system.slice/ssh.service
             └─897 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
tc@tc:~$ ls
Later  LINUX  nipe  project.scan
tc@tc:~$
```

As you can see above, the file project.scan is in the remote server (Ubuntu).

```
kali@kali: ~
File  Actions  Edit  View  Help
Reading state information ... Done
tor is already the newest version (0.4.7.10-1).
iptables is already the newest version (1.8.8-1).
The following packages were automatically installed and are no longer required:
  libatk1.0-data libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin python3-dataclasses-json python3-limiter
  python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
116.15.175.170
SG
nipe started
209.141.41.103
US
You are anonymous
[sudo] password for tc: Reading package lists ...
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2build1).
0 upgraded, 0 newly installed, 0 to remove and 32 not upgraded.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-07 05:40 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 55.77 seconds
You have the scan in your local machine
# Nmap 7.80 scan initiated Fri Oct  7 05:40:52 2022 as: nmap -oN project.scan 8.8.8.8
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

# Nmap done at Fri Oct  7 05:41:48 2022 -- 1 IP address (1 host up) scanned in 55.77 seconds

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Pictures  project.scan  project.sh  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$
```

This box represents **function s4**. Where I downloaded the file **project.scan** from remote server to my local machine.

As you can see, the copied file **project.scan** is being displayed from the command

cat project.scan in the script and is the same as the output found in the remote server, and the filed is available in my current directory.

So in conclusion, the script is running fine, and does what it needs to be done for the project, which is to be anonymous, connect to a remote server and does scan of ip address, and save the file to my local machine.

Resources:

https://linuxhint.com/bash-logical-and-operator/#:~:text=The%20Bash%20logical%20(%26%26)%20operator,or%20execute%20multiple%20commands%20simultaneously.

https://www.geeksforgeeks.org/apt-get-command-in-linux-with-examples/

https://itsfoss.com/apt-update-vs-upgrade/#:~:text=Difference%20between%20apt%20update%20and%20upgrade&text=The%20update%20command%20only%20gets,package%20to%20the%20new%20version.

https://acloudguru.com/blog/engineering/linux-commands-for-beginners-sudo

https://www.simplilearn.com/tutorials/git-tutorial/what-is-git

https://github.com/htrgouvea/nipe

https://www.computerhope.com/unix/uwhois.htm#:~:text=WHOIS%20is%20a%20query%20and,wider%20range%20of%20other%20information.

https://ryanstutorials.net/bash-scripting-tutorial/bash-if-statements.php

https://www.techtarget.com/searchsecurity/definition/Secure-Shell

https://linux.die.net/man/1/sshpass

https://nmap.org/book/port-scanning-options.html