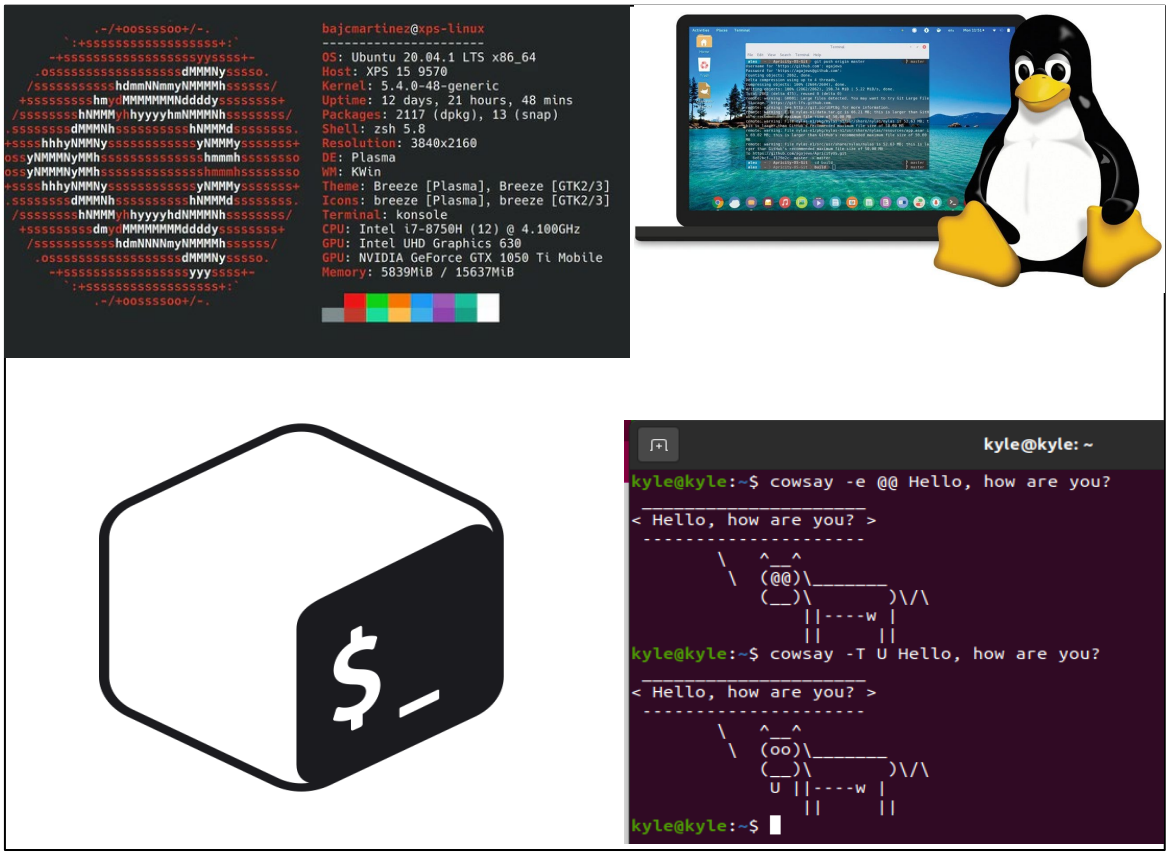


NETWORK RESEARCH PROJECT:
REMOTE CONTROL

Name: Muhd Fazil Istamar

Class: Centre for Cybersecurity (Batch – CFC240722)

Trainer Name: James Lim

Shell Script File Name: S11_NR_Proj.sh

Source:
https://livecodestream.dev/post/introduction-to-bash-for-beginners/
https://linuxhint.com/cowsay-linux-command/
https://www.opensourceforu.com/2020/03/reasons-to-use-linux/
https://linuxhint.com/cowsay-linux-command/

Objective

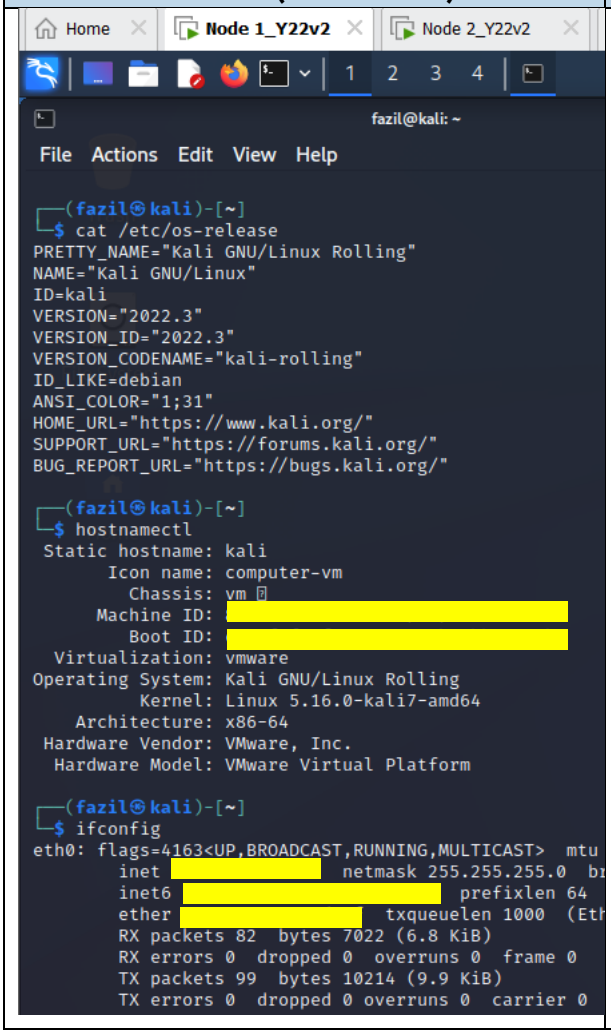
Create a script that automates the following tasks anonymously: -

I. Install relevant applications
II. Connect to a remote server via sshpass
III. Scan target remote server and collect information
IV. Store acquired information in local host

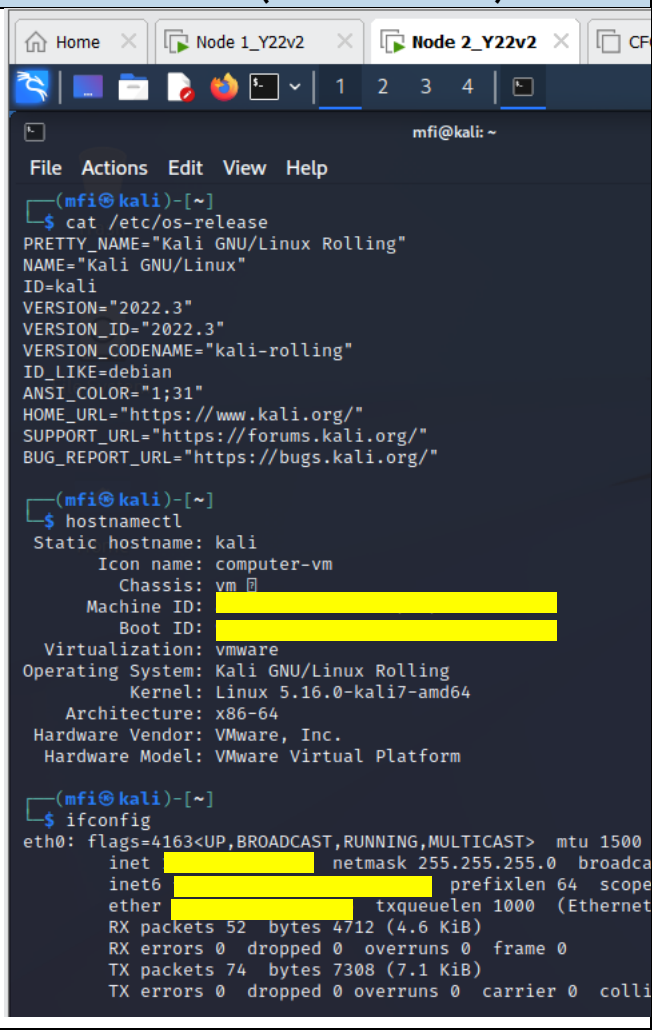
Project

- Creation of script is done by testing on two (2) Kali Linux of same Linux Kernel version. Refer to screen print below in the table on Page 3.

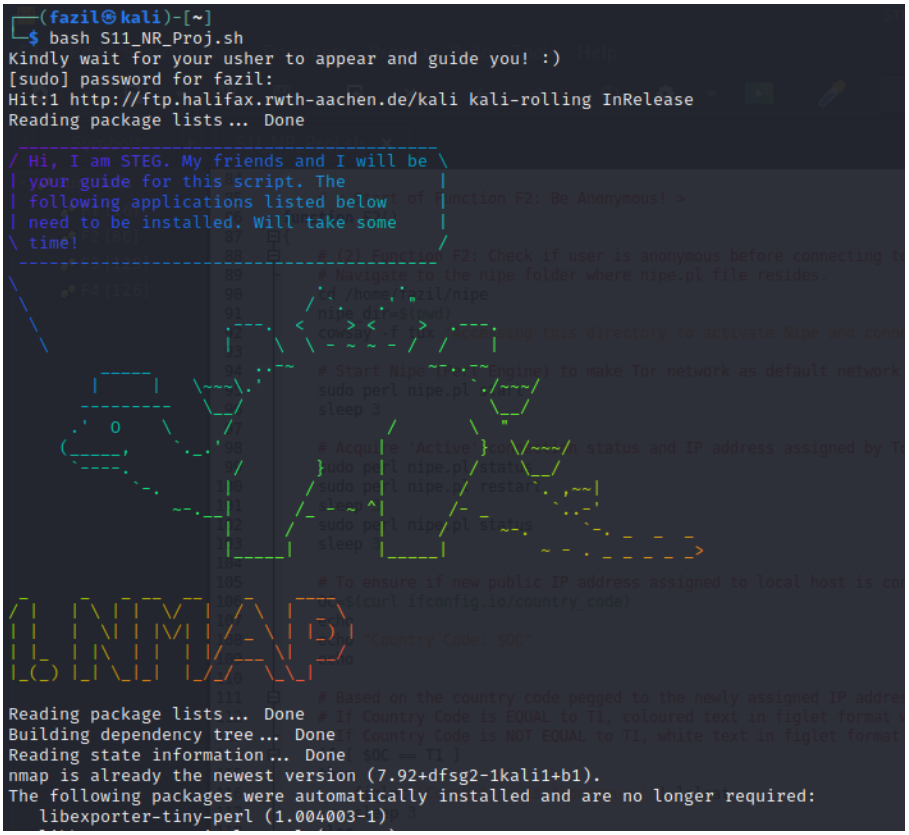
Node 1 (Local Host)



Node 2 (Remote Server)



A. Function 1 (F1): Get Ready!



- Above is an excerpt of the output for the installation of tools in Node 1 (Local Host).
- List of applications installed: cowsay, figlet, lolcat, nmap, masscan and sshpass.
- Colourful character illustration and headers were incorporated to provide the main key process that is ongoing while the bash shell script is running.
- Under this Function F1, the commands are scripted for the following sequence of activities:-
  1. Update list of packages from internet: sudo apt-get update
  2. Installation of fancy applications: sudo apt-get -y install cowsay lolcat figlet
  3. Installation of application tool (1): sudo apt-get -yV install nmap
  4. Installation of application tool (2): sudo apt-get -y install masscan
  5. Installation of application tool (3): sudo apt-get -y install sshpass
  6. Listing of application tools installed with version details using dpkg –list command
  7. Installation of Nipe; broken down into three (3) steps.
     i. Download of Nipe package
     ii. Installation of required libs and dependencies
     iii. Installation of Nipe
- 'sleep' command <syntax format: sleep number unit> is also used to delay the onset of next command as installation or task process(es) will complete within a few seconds. By default, if no value is provided for 'unit' in the syntax, it means seconds (s). This will allow users to follow through the script process and identify which stage the script is running.
- The objective of running the script in Function F1 is to install application tools in local host.
- Refer to Attachment 01 for full script of Function F1.

B. Function 2 (F2): Be Stealth!

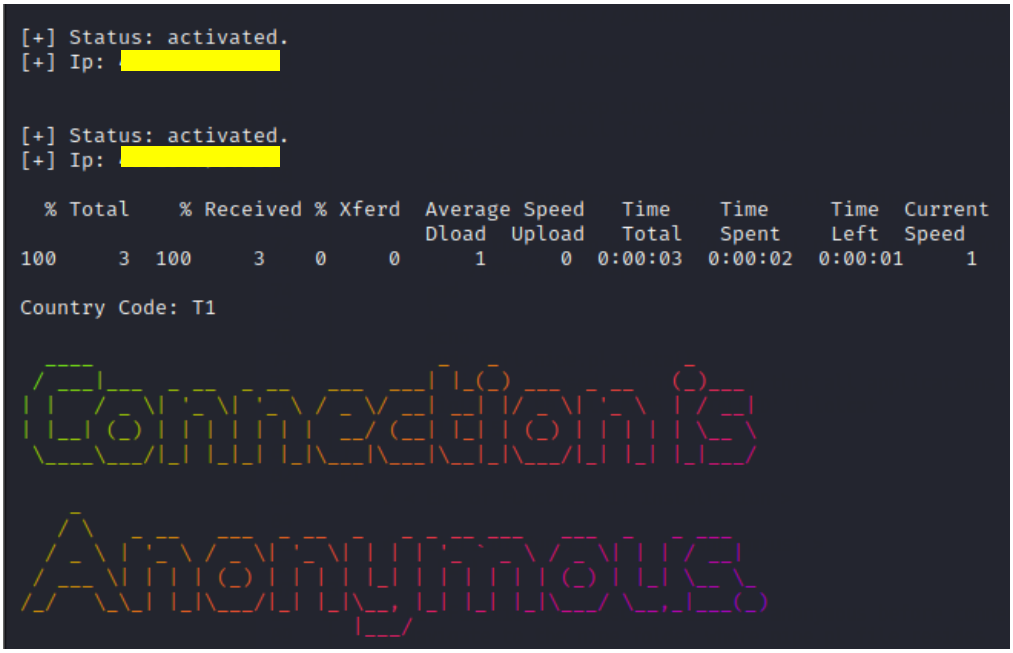
```
86  function F2()
87  {
88      # (2) Function F2: Check if user is anonymous before connecting to remote server
89      # Navigate to the nipe folder where nipe.pl file resides.
90      cd /home/fazil/nipe
91      nipe_dir=$(pwd)
92      cowsay -f tux "Accessing this directory to activate Nipe and connect to Tor network: $nipe_dir" | lolcat
93
94      # Start Nipe (Perl Engine) to make Tor network as default network gateway.
95      sudo perl nipe.pl start
96      sleep 3
97
98      # Acquire 'Active' connection status and IP address assigned by Tor network.
99      sudo perl nipe.pl status
100     sudo perl nipe.pl restart
101     sleep 3
102     sudo perl nipe.pl status
103     sleep 3
104
105     # To ensure if new public IP address assigned to local host is connected to Tor network through checking of country code = T1
106     OC=$(curl ifconfig.io/country_code)
107     echo
108     echo "Country Code: $OC"
109     echo
110
111     # Based on the country code pegged to the newly assigned IP address, it will determine whether user has establish anonymous connection.
112     # If Country Code is EQUAL to T1, coloured text in figlet format will be displayed.
113     # If Country Code is NOT EQUAL to T1, white text in figlet format will be displayed.
114     if [ $OC == T1 ]
115     then
116         figlet 'Connection is Anonymous.' | lolcat
117         sleep 3
118     else
119         figlet 'Connection is NOT Anonymous.'
120     fi
121 }
122 F2
123     # < End of Function F2: Be Anonymous! >
```

- Under this Function F2, the commands are scripted for the following sequence of activities:-
  1. Navigate to 'nipe' folder directory that has been created based on command line 62 when downloading Nipe package file. In this case, the nipe.pl file is residing in /home/fazil/nipe
  2. Establish an active connection to Tor network and assigned a unique anonymous IP address : sudo perl nipe.pl start.

     Syntax format

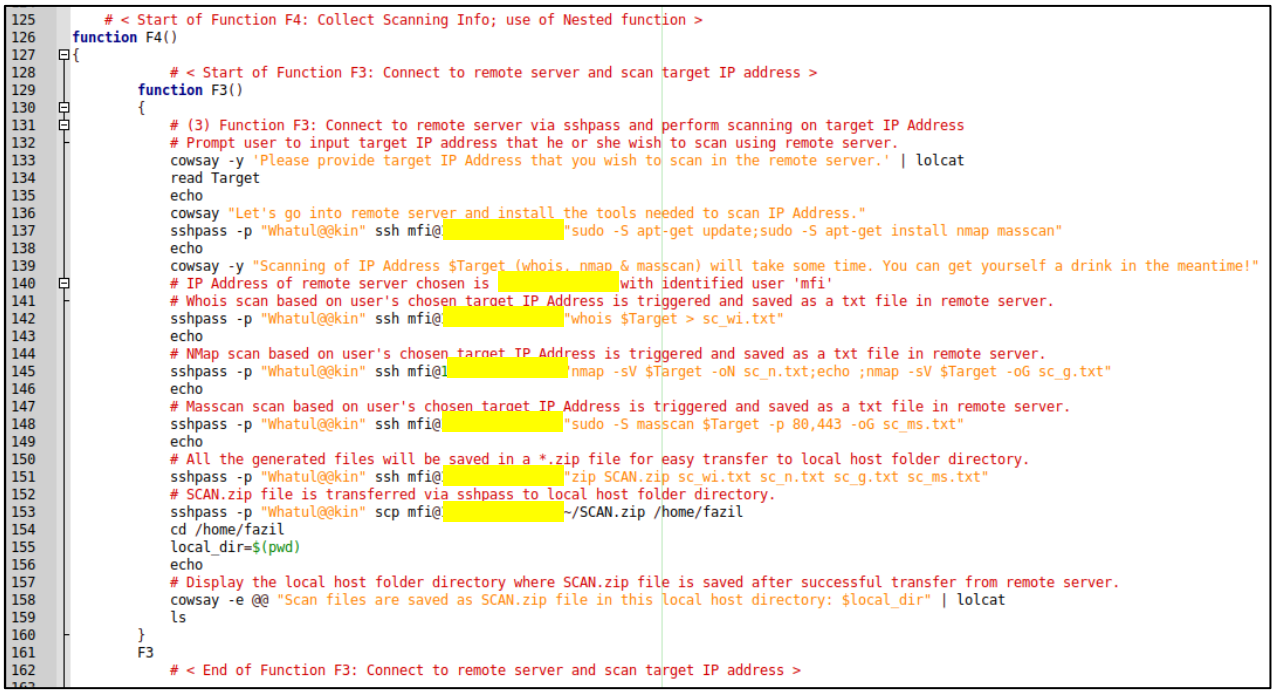
sudo	Acronym for superuser do which is a command that runs an elevated prompt without the need to change identity.
perl	Acronym for Practical Extraction and Report Language which is a language used to read nipe.pl script file.
nipe.pl	Script file to make Tor network (Darkweb) its Default Gateway (DG). At home, the DG is usually the router.
start	Action to start the script. Other options for this portion of syntax: **status** and **stop**

  3. Check the status of connection to Tor network (Activated /Disabled) and retrieve IP Address assignment. Below is a screenprint of the command output sudo perl nipe.pl status when running the script. For full script output screen prints, refer to Section E.



4. Verify IP address assigned to local host is unique and anonymous. Through verification of IP Address via curl ifconfig.io/country_code, the country origin of the IP address can be determined. Expected result is 'T1' as this will indicate the local host is connected to Tor network.
5. If-else command was used to set a condition based on the output from command Line 108.

C. Function 3 (F3): Let's Connect, Scan & Copy!



```
125     # < Start of Function F4: Collect Scanning Info; use of Nested function >
126 function F4()
127 {
128         # < Start of Function F3: Connect to remote server and scan target IP address >
129     function F3()
130     {
131         # (3) Function F3: Connect to remote server via sshpass and perform scanning on target IP Address
132         # Prompt user to input target IP address that he or she wish to scan using remote server.
133         cowsay -y 'Please provide target IP Address that you wish to scan in the remote server.' | lolcat
134         read Target
135         echo
136         cowsay "Let's go into remote server and install the tools needed to scan IP Address."
137         sshpass -p "Whatul@@kin" ssh mfi@[redacted]"sudo -S apt-get update;sudo -S apt-get install nmap masscan"
138         echo
139         cowsay -y "Scanning of IP Address $Target (whois, nmap & masscan) will take some time. You can get yourself a drink in the meantime!"
140         # IP Address of remote server chosen is [redacted] with identified user 'mfi'
141         # Whois scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
142         sshpass -p "Whatul@@kin" ssh mfi@[redacted]"whois $Target > sc_wi.txt"
143         echo
144         # NMap scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
145         sshpass -p "Whatul@@kin" ssh mfi@1[redacted]'nmap -sV $Target -oN sc_n.txt;echo ;nmap -sV $Target -oG sc_g.txt"
146         echo
147         # Masscan scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
148         sshpass -p "Whatul@@kin" ssh mfi@[redacted]"sudo -S masscan $Target -p 80,443 -oG sc_ms.txt"
149         echo
150         # All the generated files will be saved in a *.zip file for easy transfer to local host folder directory.
151         sshpass -p "Whatul@@kin" ssh mfi@[redacted]"zip SCAN.zip sc_wi.txt sc_n.txt sc_g.txt sc_ms.txt"
152         # SCAN.zip file is transferred via sshpass to local host folder directory.
153         sshpass -p "Whatul@@kin" scp mfi@[redacted]~/SCAN.zip /home/fazil
154         cd /home/fazil
155         local_dir=$(pwd)
156         echo
157         # Display the local host folder directory where SCAN.zip file is saved after successful transfer from remote server.
158         cowsay -e @@ "Scan files are saved as SCAN.zip file in this local host directory: $local_dir" | lolcat
159         ls
160     }
161     F3
162         # < End of Function F3: Connect to remote server and scan target IP address >
```

- Function F3 is nested in Function F4 so that it can be re-run if user choose to perform another scan of other target IP address. Refer to Section D for the use of 'case' command to allow user to have the 'finalsay' (variable) when all scans of the target IP Address have been completed.
- In the script shown above, Node 2 is the remote server (IP Address: [redacted]) and 'mfi' user's credentials have been defined in the script to allow remote non-interactive user access login via SSHPASS by local host Node 1 (IP Address: [redacted]). This offers great benefit if user access the remote server frequently and the time taken to input long secure password can be saved.
- Command line 134 will read user's input of target IP Address as per requested by the script in the previous command line. This allows flexibility for users who wish to scan other IP addresses. For this project, IP Address: 8.8.8.8 (Google) was chosen and tested for scanning.
- Under this Function F3, the commands are scripted for the following sequence of activities:-
  1. Prompt user to input target IP Address: read Target
  2. Install application tool (1) & (2): sudo apt-get install nmap masscan
  3. Based on user's chosen target IP Address, whois, nmap and masscan were triggered and generated individual text (*.txt) files that will be copied over to local host Node 1 directory:-

No.	Type of Scan	Scan File Name	Location (Node 2) - From	Location (Node 1) - To
i.	Whois	sc_wi.txt	/home/mfi	/home/fazil
ii.	Nmap (Normal)	sc_n.txt		
iii.	Nmap (Greppable)	sc_g.txt		
iv.	Masscan	sc_ms.txt		

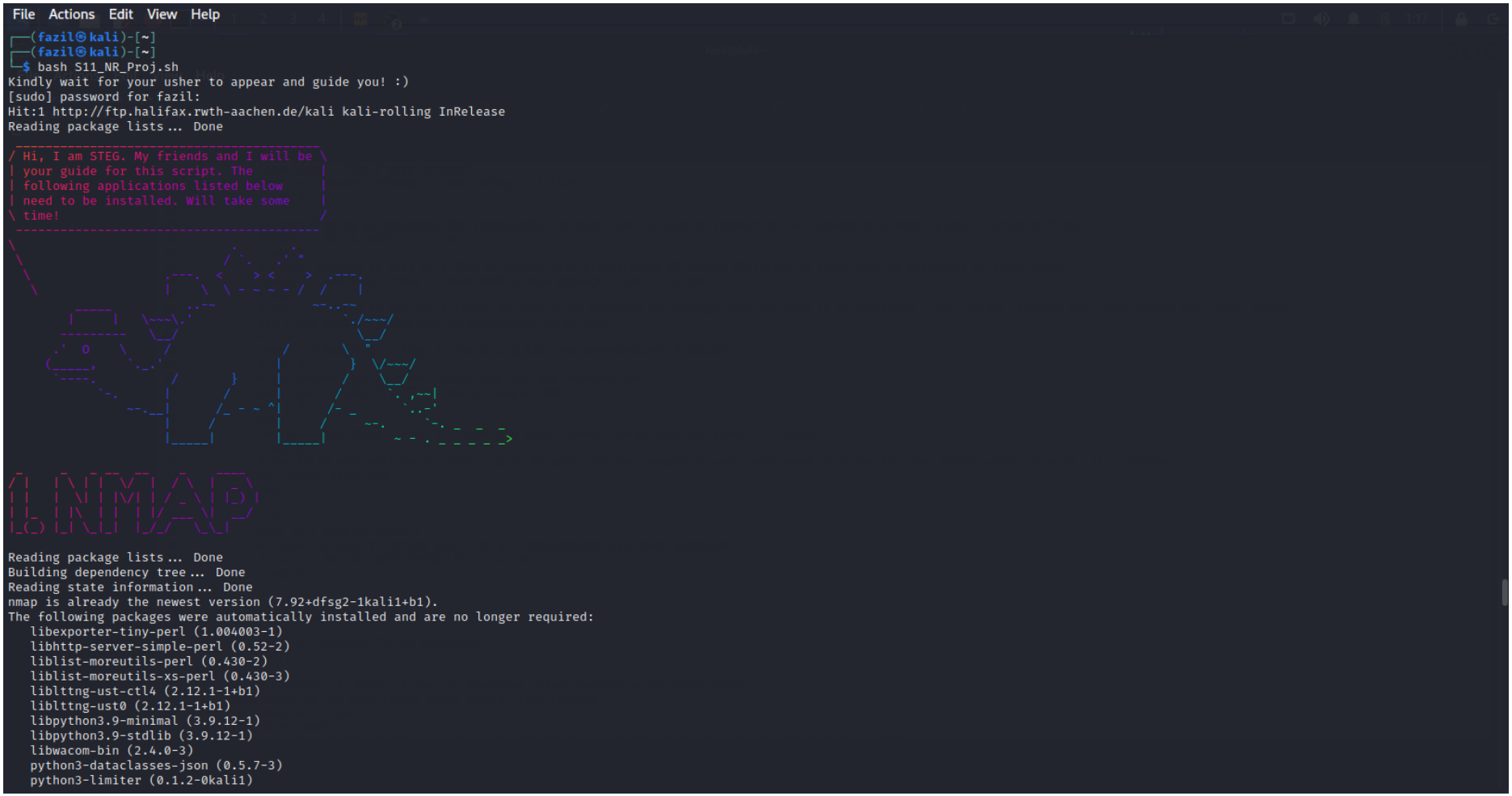
4. Upon completion of scanning IP Address 8.8.8.8, individual scan files will be archived to a *.zip file based on command line 151.
5. Command line 153: scp command is incorporated into sshpass syntax for the transfer of *.zip file to local host Node 1.

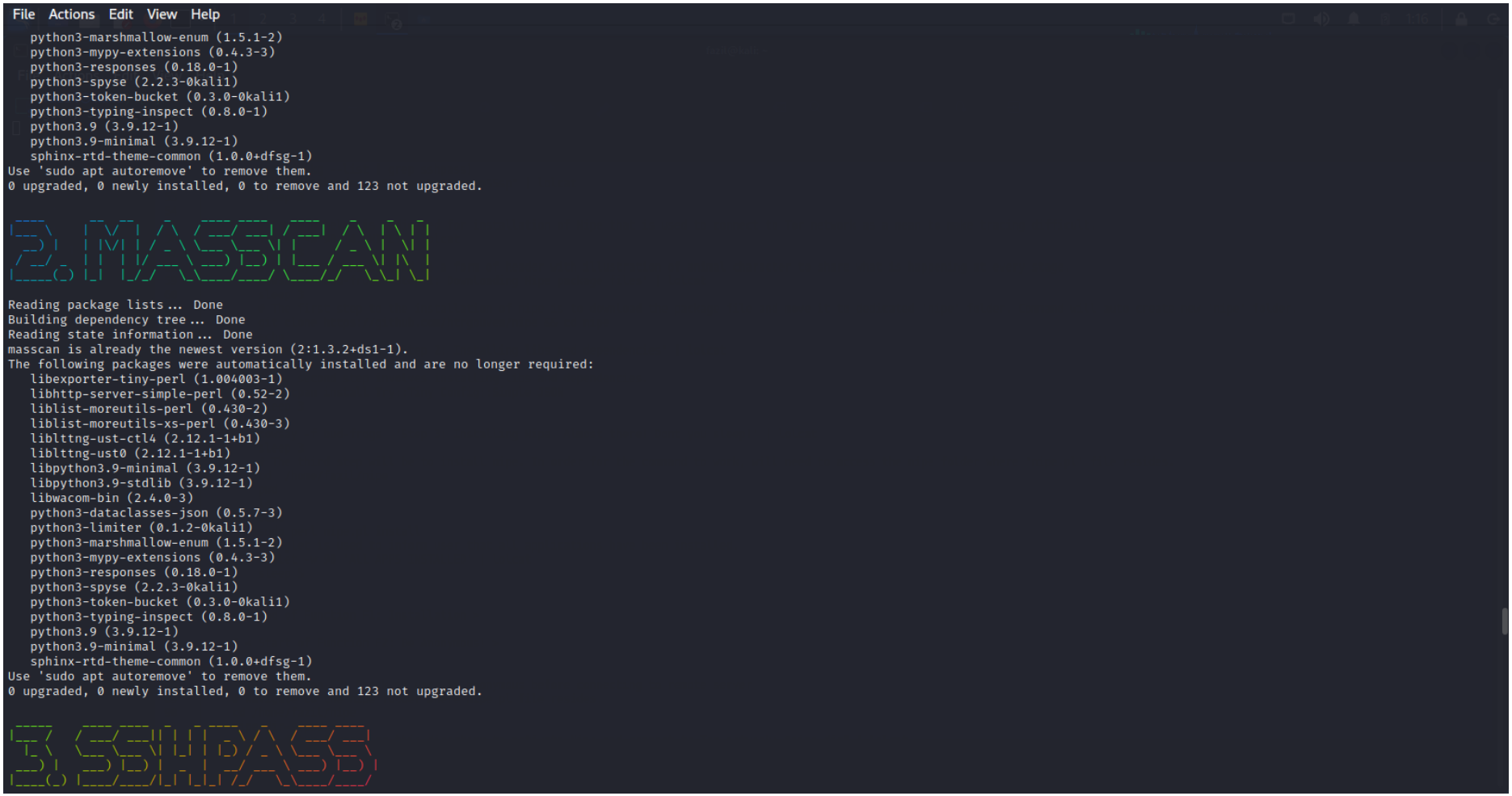
D. Function 4 (F4): Verify the scan locally!

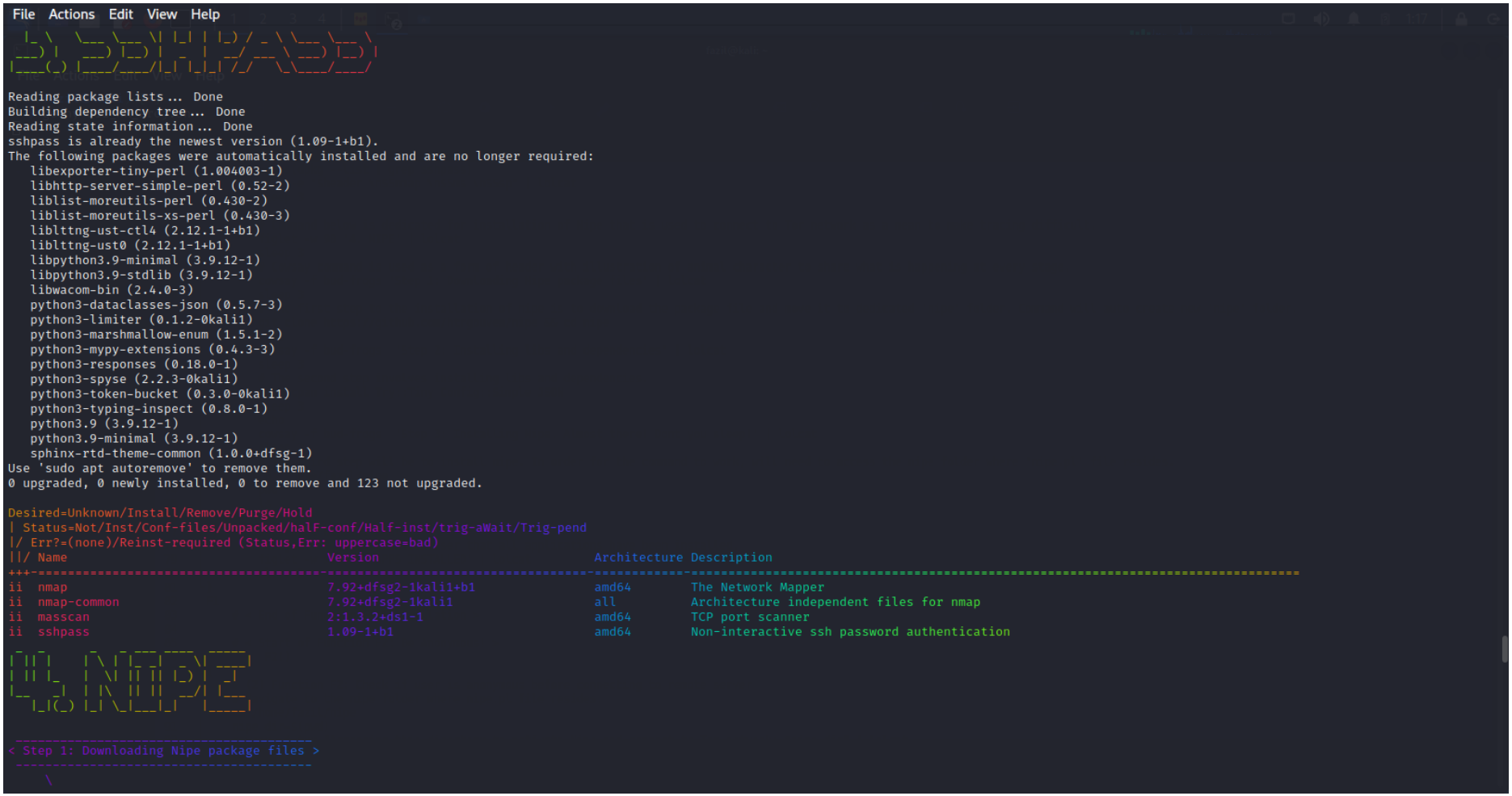
- 'case' command was used to allow user to choose what action to take:-
  A. Unzip the file that was transferred from Node 2 to Node 1.
  B. Perform another scan of target IP Address.
  C. Exit

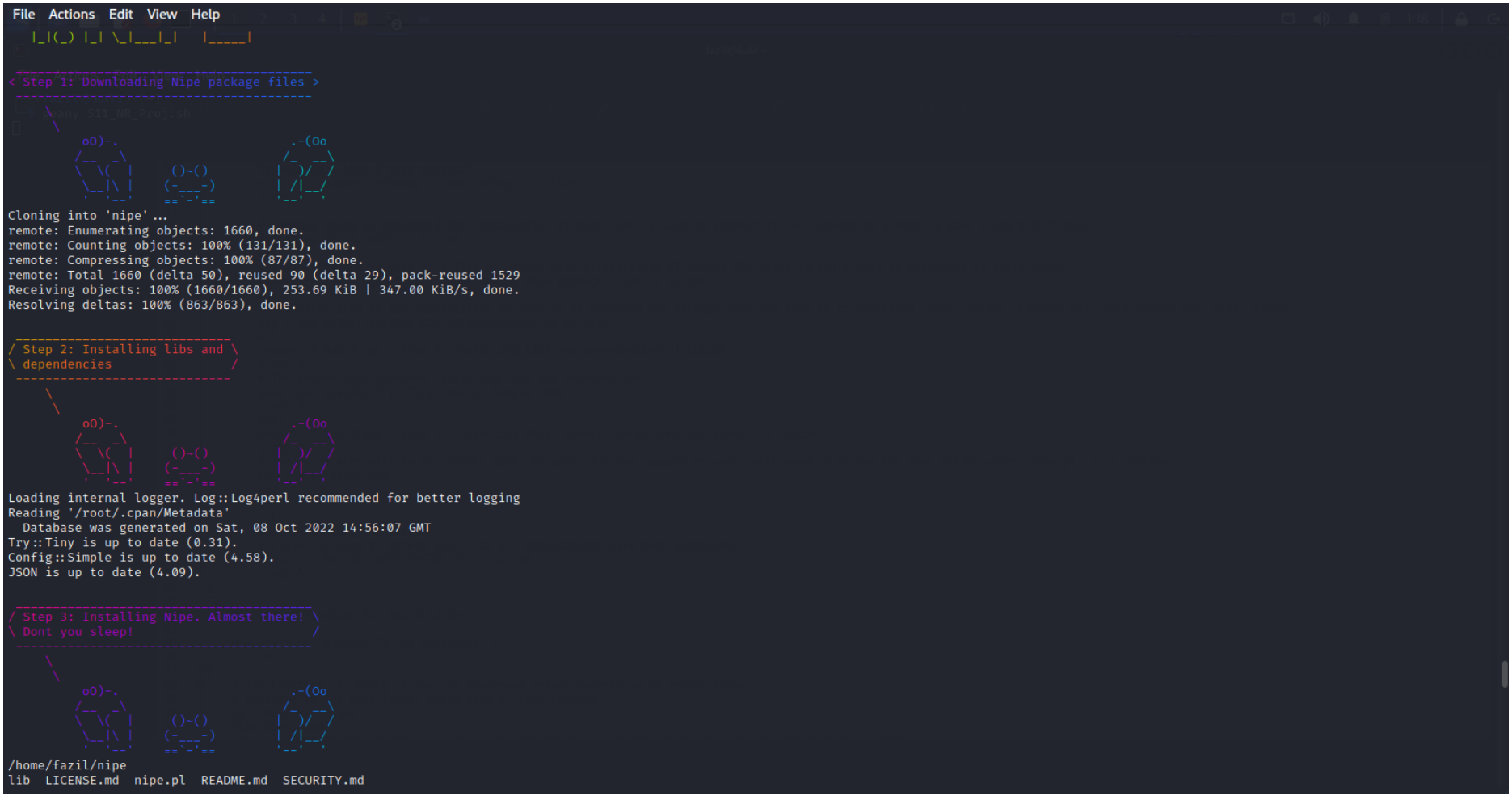
```
# < Prompt for user's next course of action. >
# User has three (3) options:-
##  [A] Unzip SCAN.zip file and view the individual scan files generated in remote server, exit script. User can then continue to open individual scan file.
##  [B] Perform another scan on other target IP Address. Revert to start Function F4 where user will be prompted to input new target IP Address.
##  [C] Exit from the script.
### 'finalsay' is the variable for this case script.
qn=$(cowsay "Your wish is my command. What would you like to do?(A)Unzip file (B)Scan another IP Add (C)Exit")
read -p "$qn" finalsay

case $finalsay in

(A)
    echo
    unzip SCAN.zip
    echo "Current working directory: $local_dir"
    ls
    sleep 3
    cowsay -T U 'Come see me again if you wish to scan another target IP Address! Mooo!' | lolcat
    sleep 3
;;

(B)
    F4
;;

(C)
    cowsay -T U 'Come see me again if you wish to scan another target IP Address! Mooo!' | lolcat
    sleep 3
    exit
;;
esac
```

E. Screenprint of Bash Shell Script Output

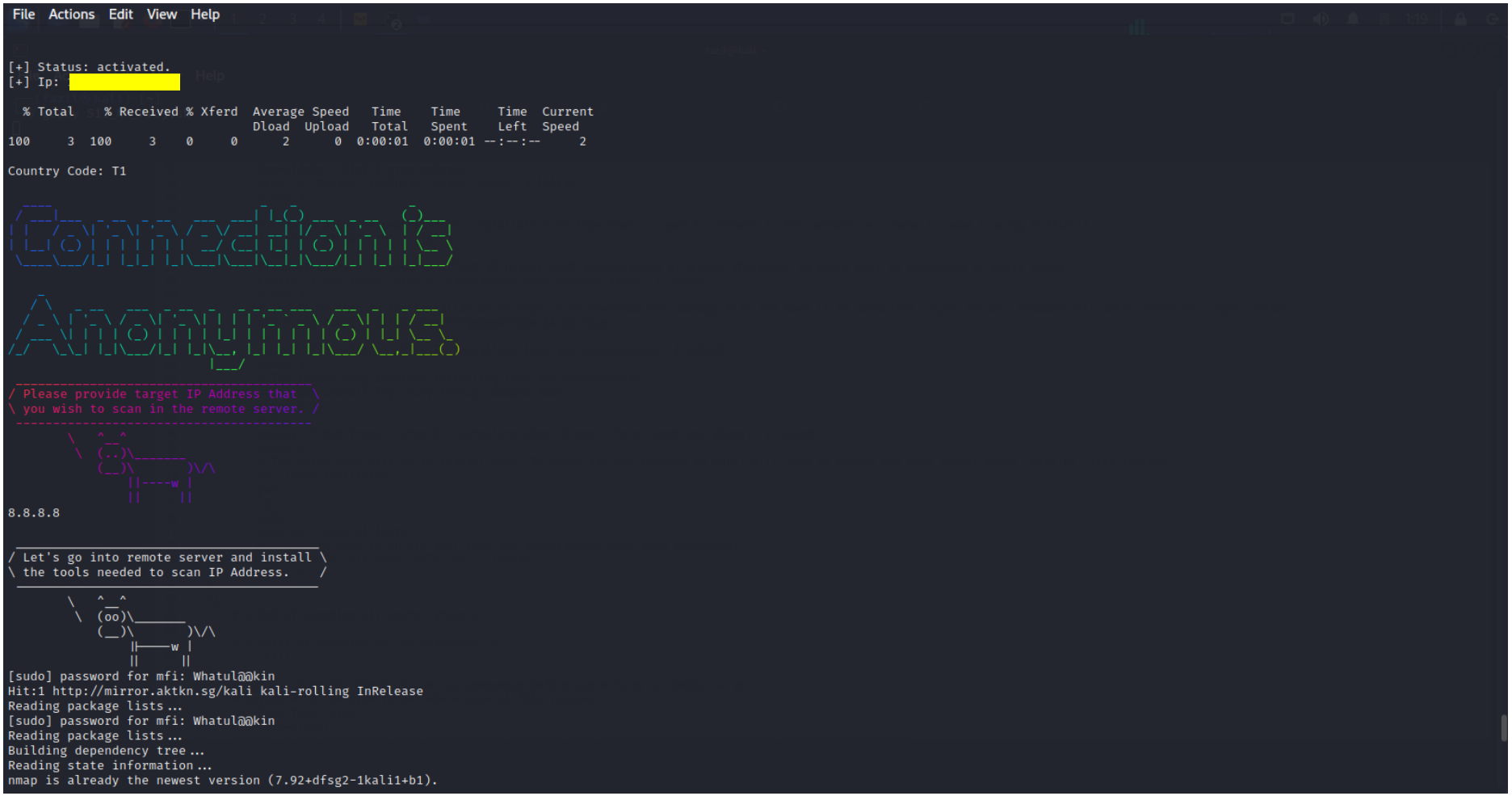



File Actions Edit View Help
python3-marshmallow-enum (1.5.1-2)
python3-mypy-extensions (0.4.3-3)
python3-responses (0.18.0-1)
python3-spyse (2.2.3-0kali1)
python3-token-bucket (0.3.0-0kali1)
python3-typing-inspect (0.8.0-1)
python3.9 (3.9.12-1)
python3.9-minimal (3.9.12-1)
sphinx-rtd-theme-common (1.0.0+dfsg-1)
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
masscan is already the newest version (2:1.3.2+ds1-1).
The following packages were automatically installed and are no longer required:
libexporter-tiny-perl (1.004003-1)
libhttp-server-simple-perl (0.52-2)
liblist-moreutils-perl (0.430-2)
liblist-moreutils-xs-perl (0.430-3)
liblttng-ust-ctl4 (2.12.1-1+b1)
liblttng-ust0 (2.12.1-1+b1)
libpython3.9-minimal (3.9.12-1)
libpython3.9-stdlib (3.9.12-1)
libwacom-bin (2.4.0-3)
python3-dataclasses-json (0.5.7-3)
python3-limiter (0.1.2-0kali1)
python3-marshmallow-enum (1.5.1-2)
python3-mypy-extensions (0.4.3-3)
python3-responses (0.18.0-1)
python3-spyse (2.2.3-0kali1)
python3-token-bucket (0.3.0-0kali1)
python3-typing-inspect (0.8.0-1)
python3.9 (3.9.12-1)
python3.9-minimal (3.9.12-1)
sphinx-rtd-theme-common (1.0.0+dfsg-1)
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.

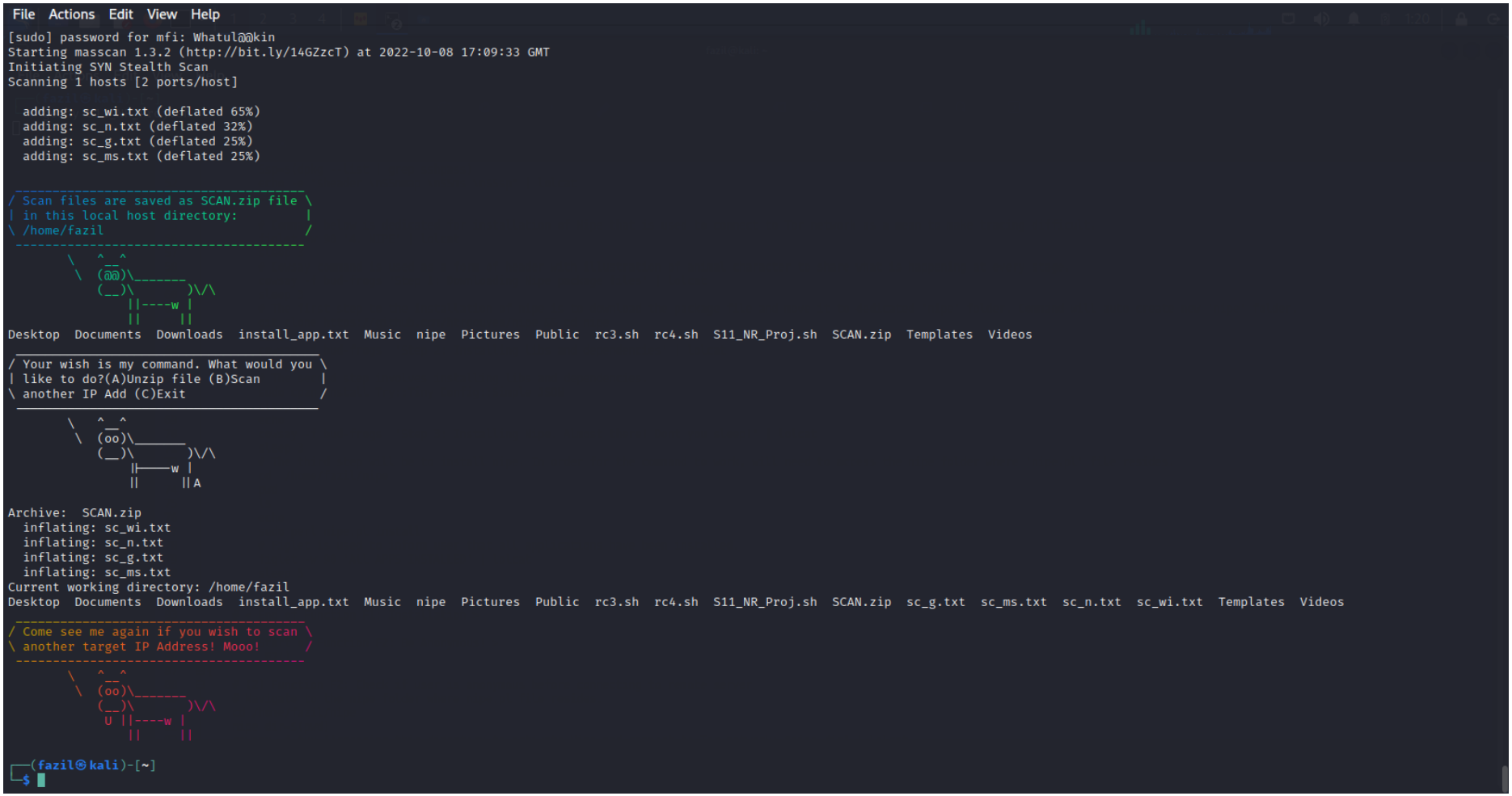

File Actions Edit View Help
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
sshpass is already the newest version (1.09-1+b1).
The following packages were automatically installed and are no longer required:
libexporter-tiny-perl (1.004003-1)
libhttp-server-simple-perl (0.52-2)
liblist-moreutils-perl (0.430-2)
liblist-moreutils-xs-perl (0.430-3)
liblttng-ust-ctl4 (2.12.1-1+b1)
liblttng-ust0 (2.12.1-1+b1)
libpython3.9-minimal (3.9.12-1)
libpython3.9-stdlib (3.9.12-1)
libwacom-bin (2.4.0-3)
python3-dataclasses-json (0.5.7-3)
python3-limiter (0.1.2-0kali1)
python3-marshmallow-enum (1.5.1-2)
python3-mypy-extensions (0.4.3-3)
python3-responses (0.18.0-1)
python3-spyse (2.2.3-0kali1)
python3-token-bucket (0.3.0-0kali1)
python3-typing-inspect (0.8.0-1)
python3.9 (3.9.12-1)
python3.9-minimal (3.9.12-1)
sphinx-rtd-theme-common (1.0.0+dfsg-1)
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Architecture Description
ii nmap 7.92+dfsg2-1kali1+b1 amd64 The Network Mapper
ii nmap-common 7.92+dfsg2-1kali1 all Architecture independent files for nmap
ii masscan 2:1.3.2+ds1-1 amd64 TCP port scanner
ii sshpass 1.09-1+b1 amd64 Non-interactive ssh password authentication
< Step 1: Downloading Nipe package files >


File Actions Edit View Help
|_|(_) |_| _|___|_| |_____|
< Step 1: Downloading Nipe package files >
Cloning into 'nipe' ...
remote: Enumerating objects: 1660, done.
remote: Counting objects: 100% (131/131), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 1660 (delta 50), reused 90 (delta 29), pack-reused 1529
Receiving objects: 100% (1660/1660), 253.69 KiB | 347.00 KiB/s, done.
Resolving deltas: 100% (863/863), done.
/ Step 2: Installing libs and \
\ dependencies /
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
Database was generated on Sat, 08 Oct 2022 14:56:07 GMT
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.09).
/ Step 3: Installing Nipe. Almost there! \
\ Dont you sleep! /
/home/fazil/nipe
lib LICENSE.md nipe.pl README.md SECURITY.md


File Actions Edit View Help
Reading package lists ... Done
Building dependency tree ... Done
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:
libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl liblttng-ust-ctl4 liblttng-ust0 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
sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.
Accessing this directory to activate
Nipe and connect to Tor network:
/home/fazil/nipe
[+] Status: activated.
[+] Ip:
[+] Status: activated.
[+] Ip:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 3 100 3 0 0 2 0 0:00:01 0:00:01 --:--:-- 2


File Actions Edit View Help
[+] Status: activated.
[+] Ip: [redacted]
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 3 100 3 0 0 2 0 0:00:01 0:00:01 --:--:-- 2
Country Code: T1
Please provide target IP Address that you wish to scan in the remote server.
8.8.8.8
Let's go into remote server and install the tools needed to scan IP Address.
[sudo] password for mfi: Whatul@@kin
Hit:1 http://mirror.aktkn.sg/kali kali-rolling InRelease
Reading package lists ...
[sudo] password for mfi: Whatul@@kin
Reading package lists ...
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.92+dfsg2-1kali1+b1).

```
File  Actions  Edit  View  Help
Building dependency tree ...
Reading state information ...
nmap is already the newest version (7.92+dfsg2-1kali1+b1).
masscan is already the newest version (2:1.3.2+ds1-1).
The following packages were automatically installed and are no longer required:
  libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl
  liblist-moreutils-xs-perl libltng-ust-ctl4 libltng-ust0
  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 sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 274 not upgraded.


 ____________________________________
/ Scanning of IP Address 8.8.8.8 (whois, \
| nmap & masscan) will take some time.   |
| You can get yourself a drink in the    |
\ meantime!                            /
 ------------------------------------
       \   ^__^
        \  (..)\_______
           (__)\       )\/\
               ||----w |
               ||     ||

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 13:08 EDT
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0067s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds

bash: line 1:  2924 Segmentation fault      nmap -sV 8.8.8.8 -oN sc_n.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-08 13:09 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.39 seconds

[sudo] password for mfi: Whatul@@kin
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-10-08 17:09:33 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [2 ports/host]

  adding: sc_wi.txt (deflated 65%)
  adding: sc_n.txt (deflated 32%)
  adding: sc_g.txt (deflated 25%)
  adding: sc_ms.txt (deflated 25%)
```


File Actions Edit View Help
[sudo] password for mfi: Whatul@@kin
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-10-08 17:09:33 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [2 ports/host]
adding: sc_wi.txt (deflated 65%)
adding: sc_n.txt (deflated 32%)
adding: sc_g.txt (deflated 25%)
adding: sc_ms.txt (deflated 25%)
/ Scan files are saved as SCAN.zip file \
| in this local host directory: |
\ /home/fazil /
Desktop Documents Downloads install_app.txt Music nipe Pictures Public rc3.sh rc4.sh S11_NR_Proj.sh SCAN.zip Templates Videos
/ Your wish is my command. What would you \
| like to do?(A)Unzip file (B)Scan |
\ another IP Add (C)Exit /
Archive: SCAN.zip
inflating: sc_wi.txt
inflating: sc_n.txt
inflating: sc_g.txt
inflating: sc_ms.txt
Current working directory: /home/fazil
Desktop Documents Downloads install_app.txt Music nipe Pictures Public rc3.sh rc4.sh S11_NR_Proj.sh SCAN.zip sc_g.txt sc_ms.txt sc_n.txt sc_wi.txt Templates Videos
/ Come see me again if you wish to scan \
\ another target IP Address! Mooo! /
(fazil㉿kali)-[~]
$

Attachment 01


```
#! /bin/bash

# Name of Student (Code): Muhd Fazil Istamar (S11)
# Class Code: CFC240722
# Name of Trainer: James Lim
# Filename: S11_NR_Proj.sh

## Description: This script is created to perform the tasks listed below.
## (1) Function F1: Install relevant applications to carry out tasks in remote server
## (2) Function F2: Check if user is anonymous before connecting to remote server
## (3) Function F3: Connect to remote server via sshpass and perform scanning of target IP Address
## (4) Function F4: Check if scanning files (.txt) have been copied over to local host successfully


    # < Start of Function F1: Installation >
function F1()
{
    # (1) Function F1: Install relevant applications to carry out tasks in remote server

        echo 'Kindly wait for your usher to appear and guide you! :)'
        # To get an updated list of packages from the internet
        sudo apt-get update
        # To install fancy tools for presentation of this script
        sudo apt-get -y install cowsay >> install_app.txt
        sudo apt-get -y install lolcat >> install_app.txt
        sudo apt-get -y install figlet >> install_app.txt

        # Introduction of the main task that will be executed in this function and trigger the installation of nmap, masscan and sshpass.
        # sleep command is used as a time delay before the start of next command.
        # figlet is used as a header to indicate what tool is installed.
```

Attachment 01


```
31          cowsay -f stegosaurus 'Hi, I am STEG. My friends and I will be your guide for this script. The following
            applications listed below need to be installed. Will take some time!' | lolcat
32          echo
33          figlet '1. NMAP' | lolcat
34          sleep 4
35          sudo apt-get -yV install nmap
36          echo
37          figlet '2. MASSCAN' | lolcat
38          sleep 4
39          sudo apt-get -yV install masscan
40          echo
41          figlet '3. SSHPASS' | lolcat
42          sleep 4
43          sudo apt-get -yV install sshpass
44          echo
45          sleep 3
46
47          # List of the applications installed with its version detail.
48          header=$(dpkg --list | head -n 5)
49          Snmap=$(dpkg --list | grep nmap)
50          Sms=$(dpkg --list | grep masscan)
51          Ssp=$(dpkg --list | grep sshpass)
52          echo -e "$header \n$Snmap \n$Sms \n$Ssp" | lolcat
53          sleep 3
54
55          # Command below is dedicated for installation of Nipe that is used to connect to Tor network as a mean to make
            tracing difficult.
56          figlet -w 90 '4. NIPE' | lolcat
57          sleep 3
58          # Cowsay command is used as a form of header with illustration of animal character to share what is happening
            at every stage.
```

Attachment 01


```
59          cowsay -f bud-frogs 'Step 1: Downloading Nipe package files' | lolcat
60          sleep 3
61          # The first step to the installation of nipe is to download the package file and move it to dedicated 'nipe'
            folder. Command will auto create new 'nipe' folder.
62          git clone https://github.com/htrgouvea/nipe && cd nipe
63          echo
64          cowsay -f bud-frogs  'Step 2: Installing libs and dependencies' | lolcat
65          sleep 3
66          # The second step involves installing libs and dependencies.
67          sudo cpan install Try::Tiny Config::Simple JSON
68          sleep 3
69          echo
70          cowsay -f bud-frogs  'Step 3: Installing Nipe. Almost there! Dont you sleep!' | lolcat
71          sleep 3
72          # The third step will be to install nipe. In order for the command to work, will need to access the nipe folder
            where 'nipe.pl' file resides.
73          cd  /home/fazil/nipe
74          pwd
75          ls
76          echo
77          sudo perl nipe.pl install
78          # Figlet is used to inform user that all applications have been installed.
79          figlet -w 90 'All APPS INSTALLED' | lolcat
80          sleep 5
81  }
82  F1
83      # < End of Function F1: Installation >
84
85      # < Start of Function F2: Be Anonymous! >
86  function F2()
87  {
```

```
88      # (2) Function F2: Check if user is anonymous before connecting to remote server
89      # Navigate to the nipe folder where nipe.pl file resides.
90      cd /home/fazil/nipe
91      nipe_dir=$(pwd)
92      cowsay -f tux "Accessing this directory to activate Nipe and connect to Tor network: $nipe_dir" | lolcat
93
94      # Start Nipe (Perl Engine) to make Tor network as default network gateway.
95      sudo perl nipe.pl start
96      sleep 3
97
98      # Acquire 'Active' connection status and IP address assigned by Tor network.
99      sudo perl nipe.pl status
100     sudo perl nipe.pl restart
101     sleep 3
102     sudo perl nipe.pl status
103     sleep 3
104
105     # To ensure if new public IP address assigned to local host is connected to Tor network through checking of country
        code = T1
106     OC=$(curl ifconfig.io/country_code)
107     echo
108     echo "Country Code: $OC"
109     echo
110
111     # Based on the country code pegged to the newly assigned IP address, it will determine whether user has establish
        anonymous connection.
112     # If Country Code is EQUAL to T1, coloured text in figlet format will be displayed.
113     # If Country Code is NOT EQUAL to T1, white text in figlet format will be displayed.
114     if [ $OC == T1 ]
115     then
116         figlet 'Connection is Anonymous.' | lolcat
```

```
117             sleep 3
118         else
119             figlet 'Connection is NOT Anonymous.'
120         fi
121     }
122     F2
123         # < End of Function F2: Be Anonymous! >
124
125         # < Start of Function F4: Collect Scanning Info; use of Nested function >
126     function F4()
127     {
128                 # < Start of Function F3: Connect to remote server and scan target IP address >
129             function F3()
130             {
131                 # (3) Function F3: Connect to remote server via sshpass and perform scanning on target IP Address
132                 # Prompt user to input target IP address that he or she wish to scan using remote server.
133                 cowsay -y 'Please provide target IP Address that you wish to scan in the remote server.' | lolcat
134                 read Target
135                 echo
136                 cowsay "Let's go into remote server and install the tools needed to scan IP Address."
137                 sshpass -p "Whatul@@kin" ssh mfi@<IP Address> "sudo -S apt-get update;sudo -S apt-get install nmap masscan"
138                 echo
139                 cowsay -y "Scanning of IP Address $Target (whois, nmap & masscan) will take some time. You can get yourself
                    a drink in the meantime!"
140                 # IP Address of remote server chosen is <IP Address> with identified user 'mfi'
141                 # Whois scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
142                 sshpass -p "Whatul@@kin" ssh mfi@<IP Address> "whois $Target > sc_wi.txt"
143                 echo
144                 # NMap scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
145                 sshpass -p "Whatul@@kin" ssh mfi@<IP Address> "nmap -sV $Target -oN sc_n.txt;echo ;nmap -sV $Target -oG
                    sc_g.txt"
```

```
146             echo
147             # Masscan scan based on user's chosen target IP Address is triggered and saved as a txt file in remote server.
148             sshpass -p "Whatul@@kin" ssh mfi@<IP Address> "sudo -S masscan $Target -p 80,443 -oG sc_ms.txt"
149             echo
150             # All the generated files will be saved in a *.zip file for easy transfer to local host folder directory.
151             sshpass -p "Whatul@@kin" ssh mfi@<IP Address>"zip SCAN.zip sc_wi.txt sc_n.txt sc_g.txt sc_ms.txt"
152             # SCAN.zip file is transferred via sshpass to local host folder directory.
153             sshpass -p "Whatul@@kin" scp mfi@<IP Address>:~/SCAN.zip /home/fazil
154             cd /home/fazil
155             local_dir=$(pwd)
156             echo
157             # Display the local host folder directory where SCAN.zip file is saved after successful transfer from
                remote server.
158             cowsay -e @@ "Scan files are saved as SCAN.zip file in this local host directory: $local_dir" | lolcat
159             ls
160         }
161         F3
162             # < End of Function F3: Connect to remote server and scan target IP address >
163
164             # < Prompt for user's next course of action. >
165             # User has three (3) options:-
166             ##  [A] Unzip SCAN.zip file and view the individual scan files generated in remote server, exit script.
                User can then continue to open individual scan file.
167             ##  [B] Perform another scan on other target IP Address. Revert to start Function F4 where user will be
                prompted to input new target IP Address.
168             ##  [C] Exit from the script.
169             ### 'finalsay' is the variable for this case script.
170             qn=$(cowsay "Your wish is my command. What would you like to do?(A)Unzip file (B)Scan another IP Add (C)Exit")
171             read -p "$qn" finalsay
172
173             case $finalsay in
```

```
174
175             (A)
176                 echo
177                 unzip SCAN.zip
178                 echo "Current working directory: $local_dir"
179                 ls
180                 sleep 3
181                 cowsay -T U 'Come see me again if you wish to scan another target IP Address! Mooo!' | lolcat
182                 sleep 3
183             ;;
184
185             (B)
186                 F4
187             ;;
188
189             (C)
190                 cowsay -T U 'Come see me again if you wish to scan another target IP Address! Mooo!' | lolcat
191                 sleep 3
192                 exit
193             ;;
194             esac
195 }
196 F4
197     # < End of Function F4: Collect Scanning Info; use of Nested function Case>
198
```