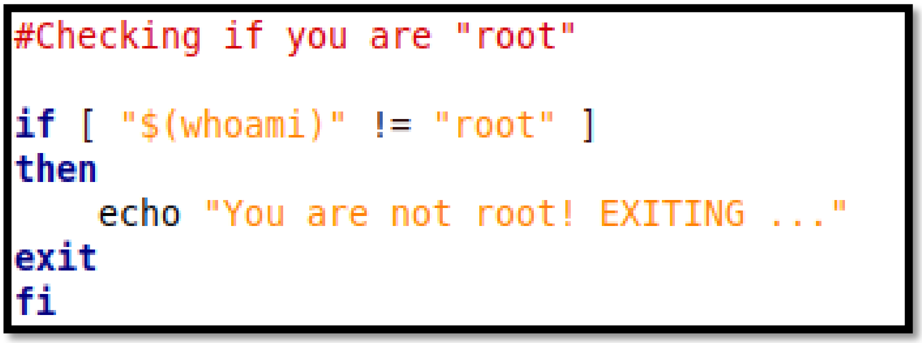
Project Network Research - Ofir Halfin

To start running the script you need to enter "root"!

This if statement check if the user is rooted or not!

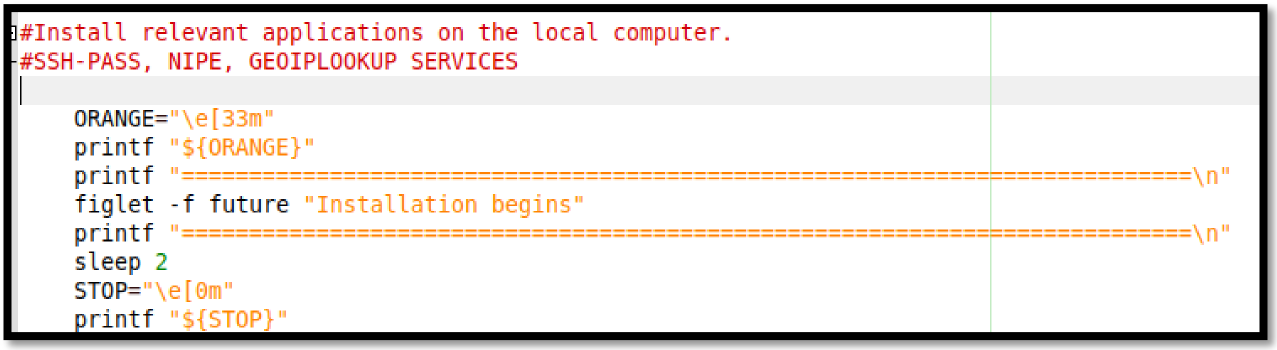
* Without enter "Root", the Script will exit immediately.



```
#Checking if you are "root"

if [ "$(whoami)" != "root" ]
then
	echo "You are not root! EXITING ..."
exit
fi
```

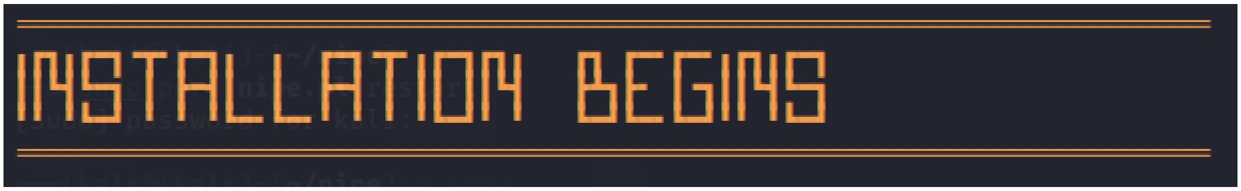
After entering "root", the script will continue and will start installing the following Tools/services:

input



```
#Install relevant applications on the local computer.
#SSH-PASS, NIPE, GEOIPLOOKUP SERVICES

	ORANGE="\e[33m"
	printf "${ORANGE}"
	printf "===========================================================================\n"
	figlet -f future "Installation begins"
	printf "===========================================================================\n"
	sleep 2
	STOP="\e[0m"
	printf "${STOP}"
```

output



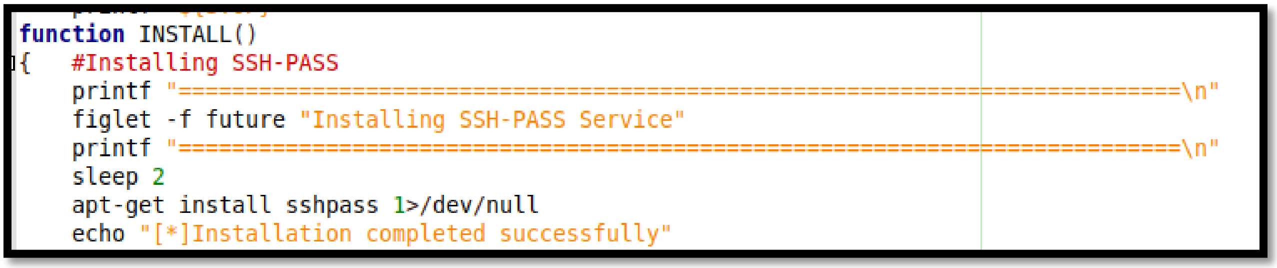
```
INSTALLATION BEGINS
```

Function 1 (INSTALL):

SSH-PASS Installation:

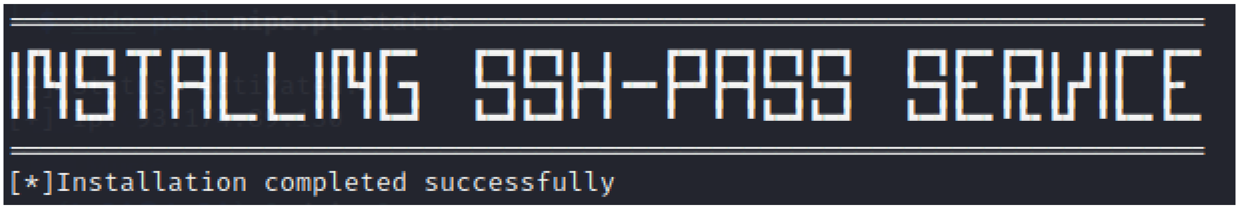
The ssh-pass utility is designed to run SSH using the keyboard-interactive password authentication mode, but in a non-interactive way.

input



```
function INSTALL()
{   #Installing SSH-PASS
    printf "===========================================================================\n"
    figlet -f future "Installing SSH-PASS Service"
    printf "===========================================================================\n"
    sleep 2
    apt-get install sshpass 1>/dev/null
    echo "[*]Installation completed successfully"
```

output



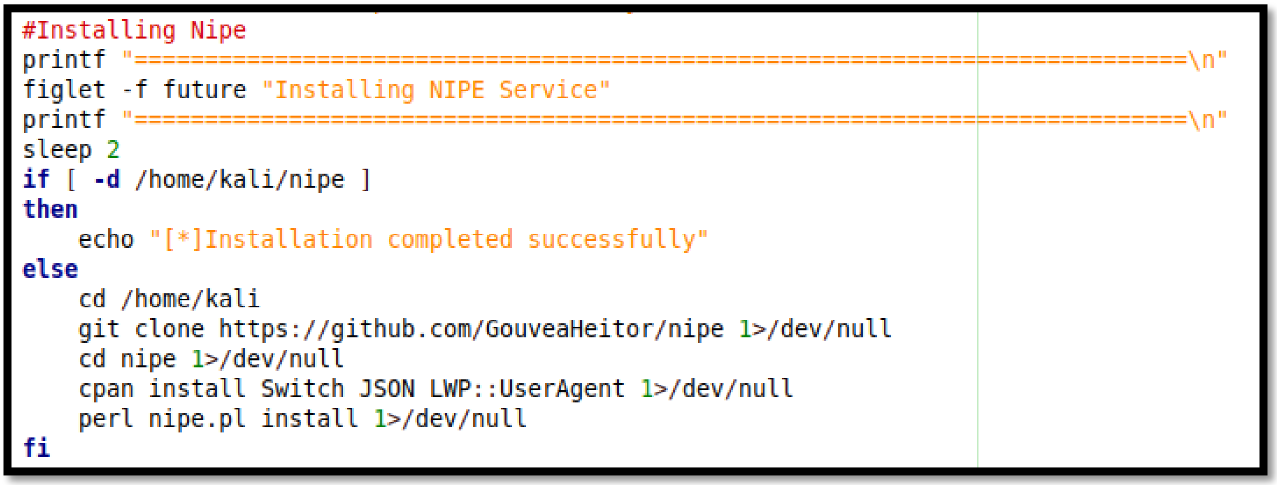
```
=====================================================================
INSTALLING SSH-PASS SERVICE
=====================================================================
[*]Installation completed successfully
```

NIPE Installation:

NIPE makes Tor network our default gateway. This is how we can anonymise our total Kali Linux system. This process is enough secure. Practically cracking Tor is close to impossible.

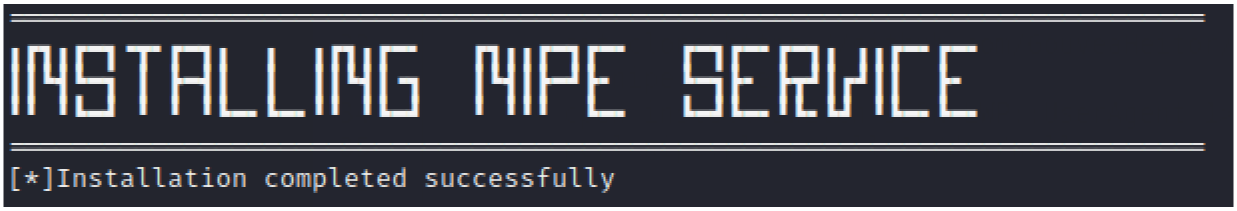
* In the script if the NIPE directory is exists, ignore installation again and it say the install completed.

Input



```
#Installing Nipe
printf "===========================================================================\n"
figlet -f future "Installing NIPE Service"
printf "===========================================================================\n"
sleep 2
if [ -d /home/kali/nipe ]
then
    echo "[*]Installation completed successfully"
else
    cd /home/kali
    git clone https://github.com/GouveaHeitor/nipe 1>/dev/null
    cd nipe 1>/dev/null
    cpan install Switch JSON LWP::UserAgent 1>/dev/null
    perl nipe.pl install 1>/dev/null
fi
```

output

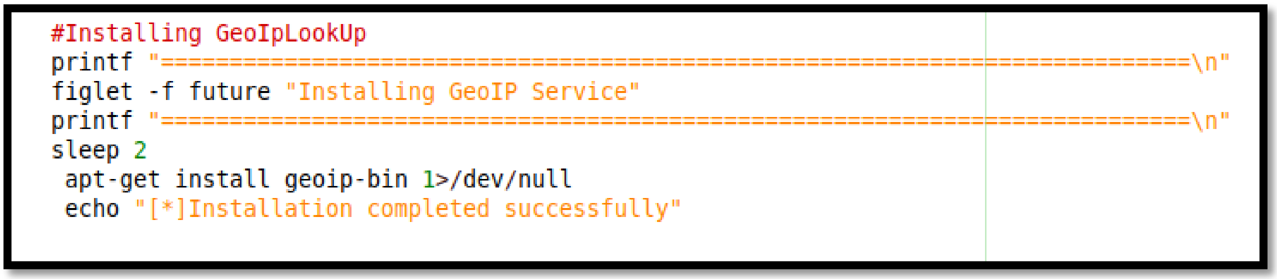


```
===========================================================================
INSTALLING NIPE SERVICE
===========================================================================
[*]Installation completed successfully
```

GeoIpLookUp Installation:

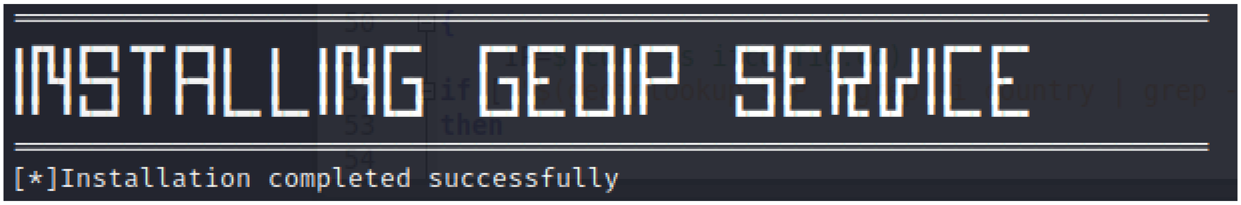
GeoIpLookUp uses the GeoIP library and database to find the Country that an IP address or hostname originates from.

input



```
#Installing GeoIpLookUp
printf "===========================================================================\n"
figlet -f future "Installing GeoIP Service"
printf "===========================================================================\n"
sleep 2
 apt-get install geoip-bin 1>/dev/null
 echo "[*]Installation completed successfully"
```

output



```
===========================================================================
INSTALLING GEOIP SERVICE
===========================================================================
[*]Installation completed successfully
```

Function 2 (CONNECTION):

After the Installation, need to change our IP ADDRESS by using “NIPE”.

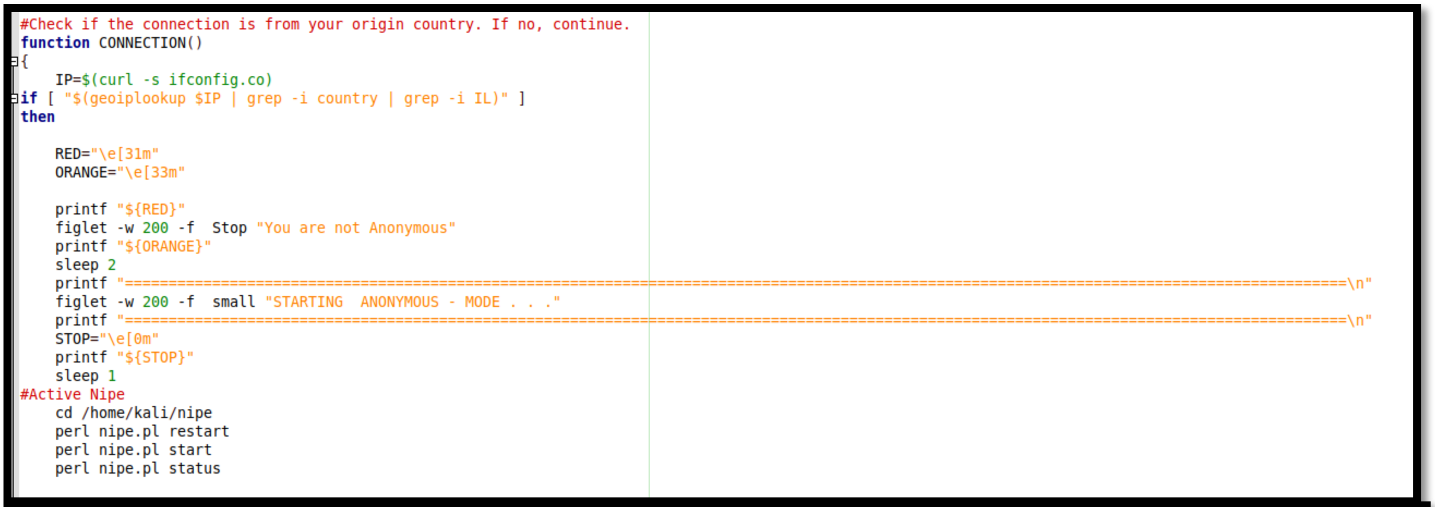
This Function checks if the user IP address = to his region(country).

If it is then, enter “anonymous mode” and continue!

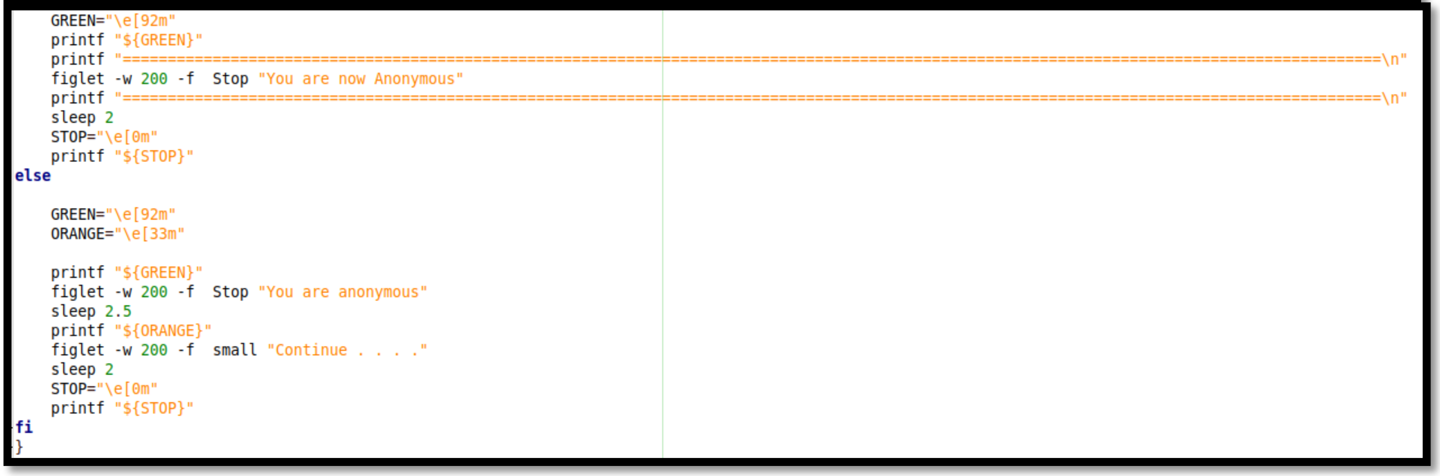
If its not, then continue without active “NIPE” again.

* NIPE will show the new IP address and his status (activated, disabled)

input

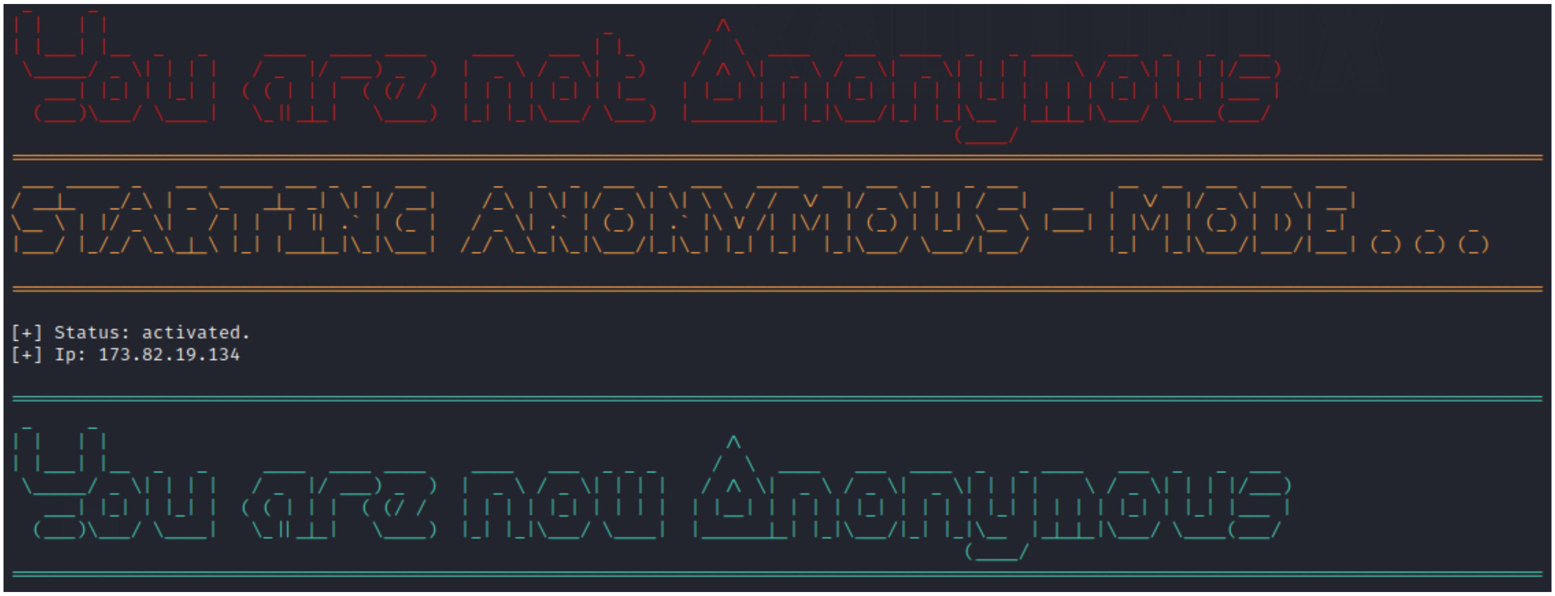


```
#Check if the connection is from your origin country. If no, continue.
function CONNECTION()
{
    IP=$(curl -s ifconfig.co)
if [ "$(geoiplookup $IP | grep -i country | grep -i IL)" ]
then

    RED="\e[31m"
    ORANGE="\e[33m"

    printf "${RED}"
    figlet -w 200 -f  Stop "You are not Anonymous"
    printf "${ORANGE}"
    sleep 2
    printf "==============================================================================================================================================\n"
    figlet -w 200 -f  small "STARTING  ANONYMOUS - MODE . . ."
    printf "==============================================================================================================================================\n"
    STOP="\e[0m"
    printf "${STOP}"
    sleep 1
#Active Nipe
    cd /home/kali/nipe
    perl nipe.pl restart
    perl nipe.pl start
    perl nipe.pl status
```



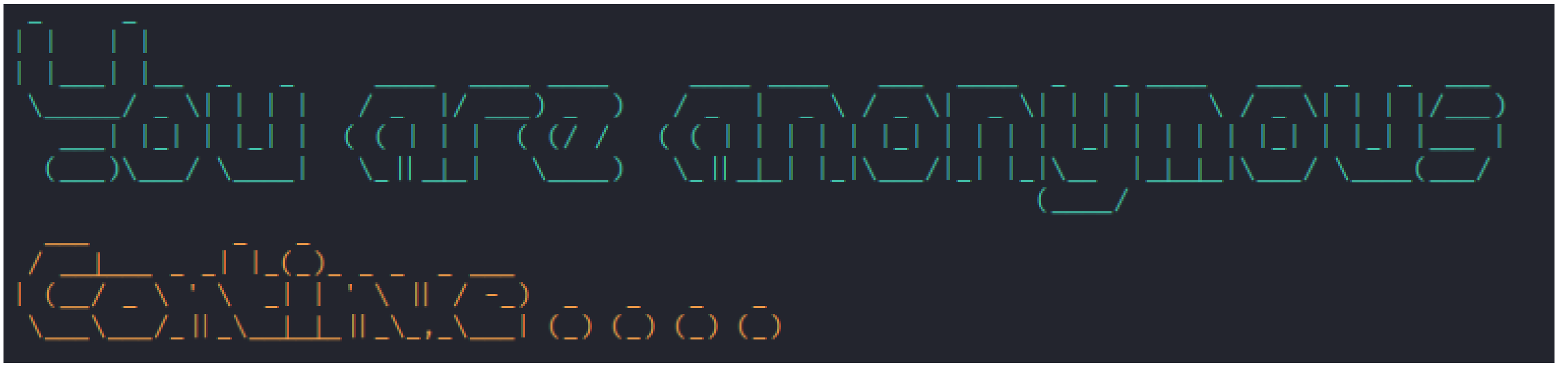
```
    GREEN="\e[92m"
    printf "${GREEN}"
    printf "==============================================================================================================================================\n"
    figlet -w 200 -f  Stop "You are now Anonymous"
    printf "==============================================================================================================================================\n"
    sleep 2
    STOP="\e[0m"
    printf "${STOP}"
else

    GREEN="\e[92m"
    ORANGE="\e[33m"

    printf "${GREEN}"
    figlet -w 200 -f  Stop "You are anonymous"
    sleep 2.5
    printf "${ORANGE}"
    figlet -w 200 -f  small "Continue . . . ."
    sleep 2
    STOP="\e[0m"
    printf "${STOP}"
fi
}
```

output - when the user not anonymous!



```
[+] Status: activated.
[+] Ip: 173.82.19.134
```

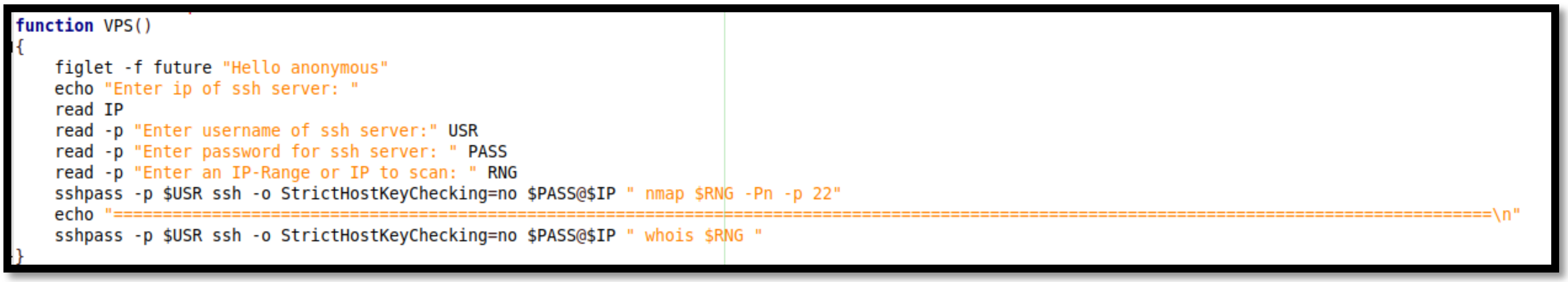
output – when the user anonymous!



Function 3 (VPS):

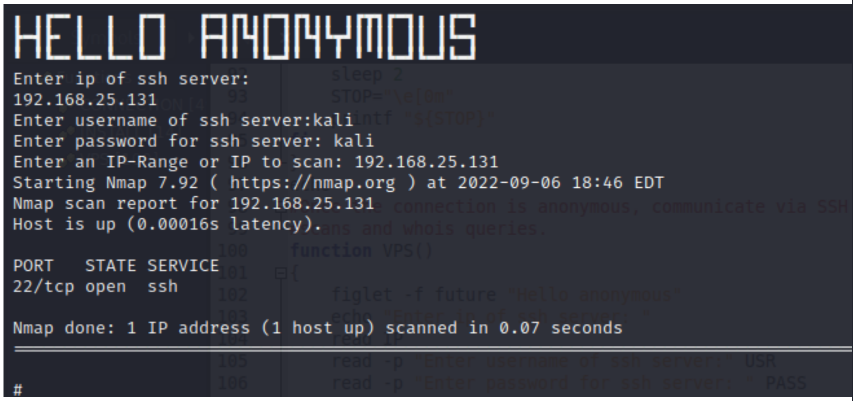
Once the connection is anonymous, communicate via SSH and execute Nmap scans and Whois queries.

input

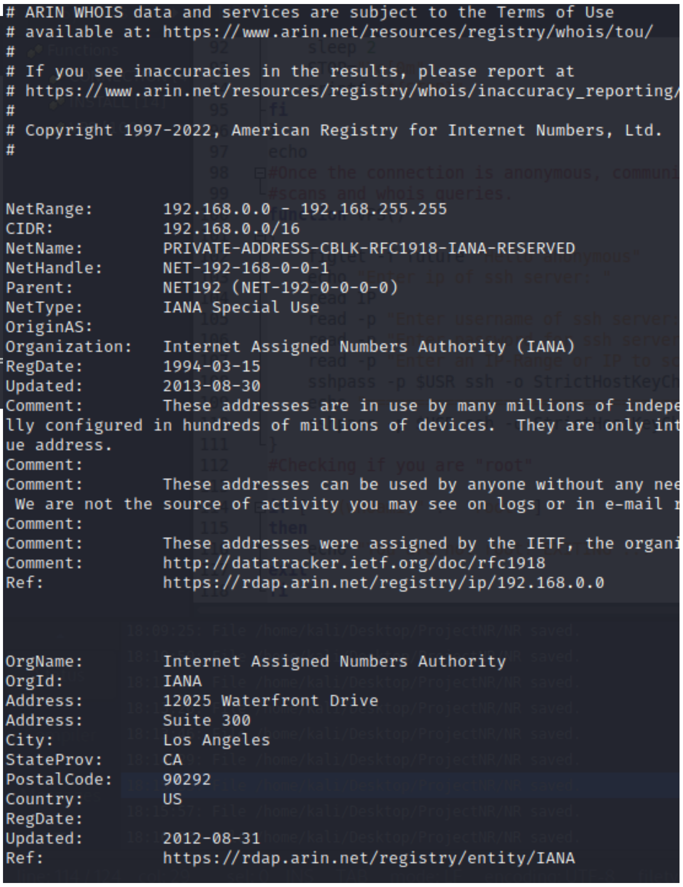


```
function VPS()
{
    figlet -f future "Hello anonymous"
    echo "Enter ip of ssh server: "
    read IP
    read -p "Enter username of ssh server:" USR
    read -p "Enter password for ssh server: " PASS
    read -p "Enter an IP-Range or IP to scan: " RNG
    sshpass -p $USR ssh -o StrictHostKeyChecking=no $PASS@$IP " nmap $RNG -Pn -p 22"
    echo "==============================================================================================================================================\n"
    sshpass -p $USR ssh -o StrictHostKeyChecking=no $PASS@$IP " whois $RNG "
}
```

output

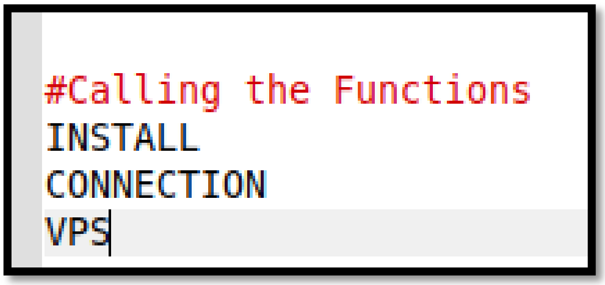


```
HELLO ANONYMOUS
Enter ip of ssh server:
192.168.25.131
Enter username of ssh server:kali
Enter password for ssh server: kali
Enter an IP-Range or IP to scan: 192.168.25.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-06 18:46 EDT
Nmap scan report for 192.168.25.131
Host is up (0.00016s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
=======================================================================
#
```



```
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of indepe
lly configured in hundreds of millions of devices.  They are only int
ue address.
Comment:
Comment:        These addresses can be used by anyone without any nee
 We are not the source of activity you may see on logs or in e-mail r
Comment:
Comment:        These addresses were assigned by the IETF, the organi
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA
```

AT THE END OF THE INPUT - CALLING ALL THE 3 FUNCTIONS TO ACTIVE THEM!!

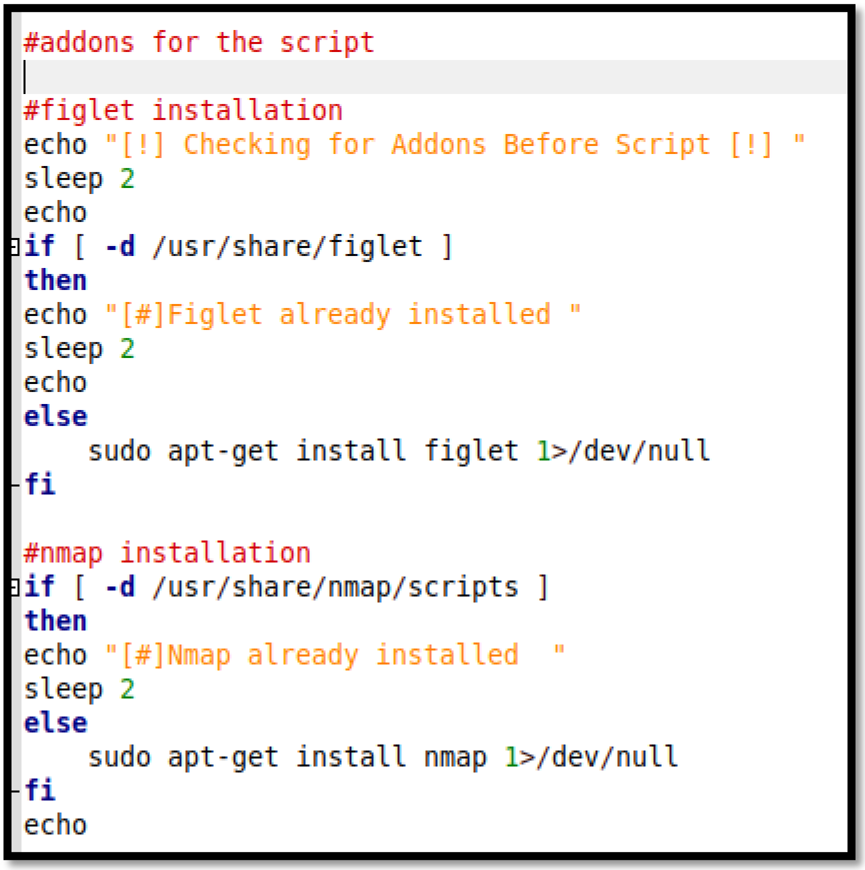


```
#Calling the Functions
INSTALL
CONNECTION
VPS
```

“Addons” I used:

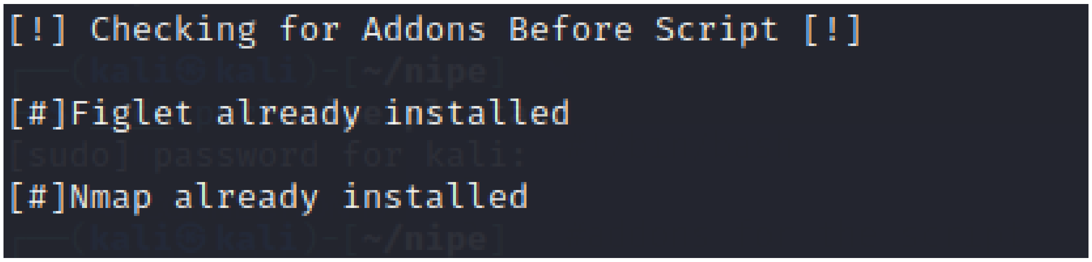
- Figlet program
- Figlet Color text: https://unix.stackexchange.com/questions/444017/color-variables-on-figlet
- Nmap

input



```
#addons for the script

#figlet installation
echo "[!] Checking for Addons Before Script [!] "
sleep 2
echo
if [ -d /usr/share/figlet ]
then
echo "[#]Figlet already installed "
sleep 2
echo
else
    sudo apt-get install figlet 1>/dev/null
fi

#nmap installation
if [ -d /usr/share/nmap/scripts ]
then
echo "[#]Nmap already installed  "
sleep 2
else
    sudo apt-get install nmap 1>/dev/null
fi
echo
```

output



```
[!] Checking for Addons Before Script [!]

[#]Figlet already installed

[#]Nmap already installed
```