בס"ד

REMOTE CONTROL PROJECT

About the project:

obtaining information about a target by activating agents that obtain the information for you

if command to check if you are root if you are not root you access to root (For the next steps it will be necessary to be root to continue the script)

```bash
#!/bin/bash
#-----------------------------------------------------------------------------------------Network Research Project------------
#Checking if you are "root"
echo "-------------------------Network Research Project-------------------------" | lolcat -a -d 50
echo ""


if [ "$(whoami)" != "root" ]
then
    echo "You are not root! connecting as root" | lolcat
    sudo su
    exit
fi

```

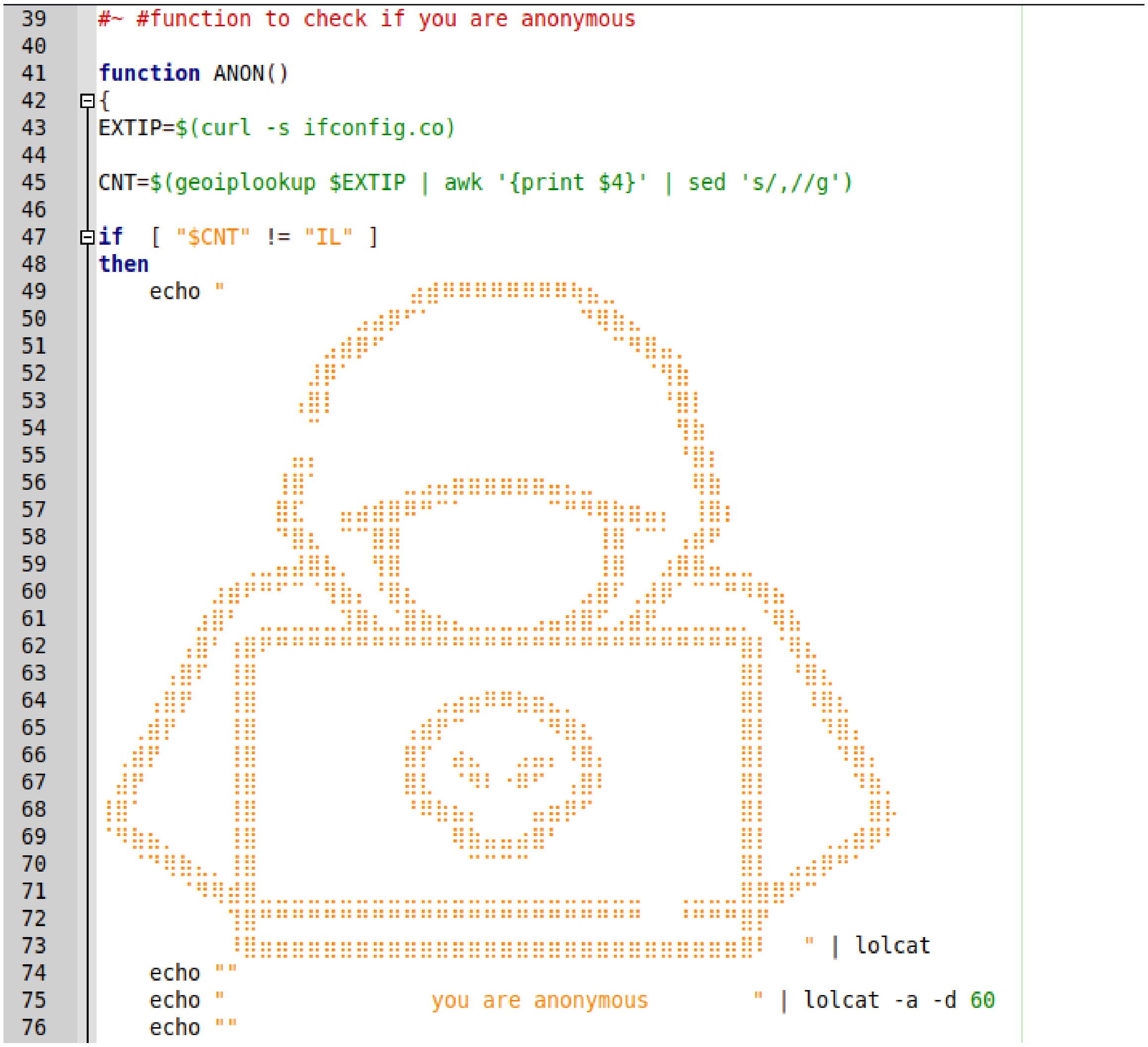
```
┌──(kali㉿KALI-SRV)-[~/Desktop]
└─$ bash project.sh
-------------------------Network Research Project-------------------------

You are not root! connecting as root
┌──(root㉿KALI-SRV)-[/home/kali/Desktop]
└─#
```

function to install applications by comparing whether the user has the relevant applications If the user has the file then the script continues and if not it downloads the apps for him.

```
#function to install applications
function INST()
{   if  [ -d "/etc/ssh" ]
    then
        echo "ssh already installed " | lolcat
    else
        echo "installing ssh" | lolcat
     apt-get install ssh 1>/dev/null
    fi

     apt-get install sshpass 1>/dev/null

     if [ -d "/usr/share/GeoIP" ]
     then
        echo ""
        echo "  geoip already installed " | lolcat
     else
        echo""
        echo "      installing geoip" | lolcat
        apt-get install geoip-bin 1>/dev/null
        echo""
     fi


     if [ -d "/home/kali/nipe" ]
     then
        echo""
        echo "      nipe already installed        " | lolcat
        echo""
        echo""
    else
        echo "                  connecting to nipe mode                 "
        git clone https://github.com/htrgouvea/nipe && cd nipe 1>/dev/null

        cpan install Try::Tiny Config::Simple JSON 1>/dev/null

        perl nipe.pl install 1>/dev/null


     fi

}
```

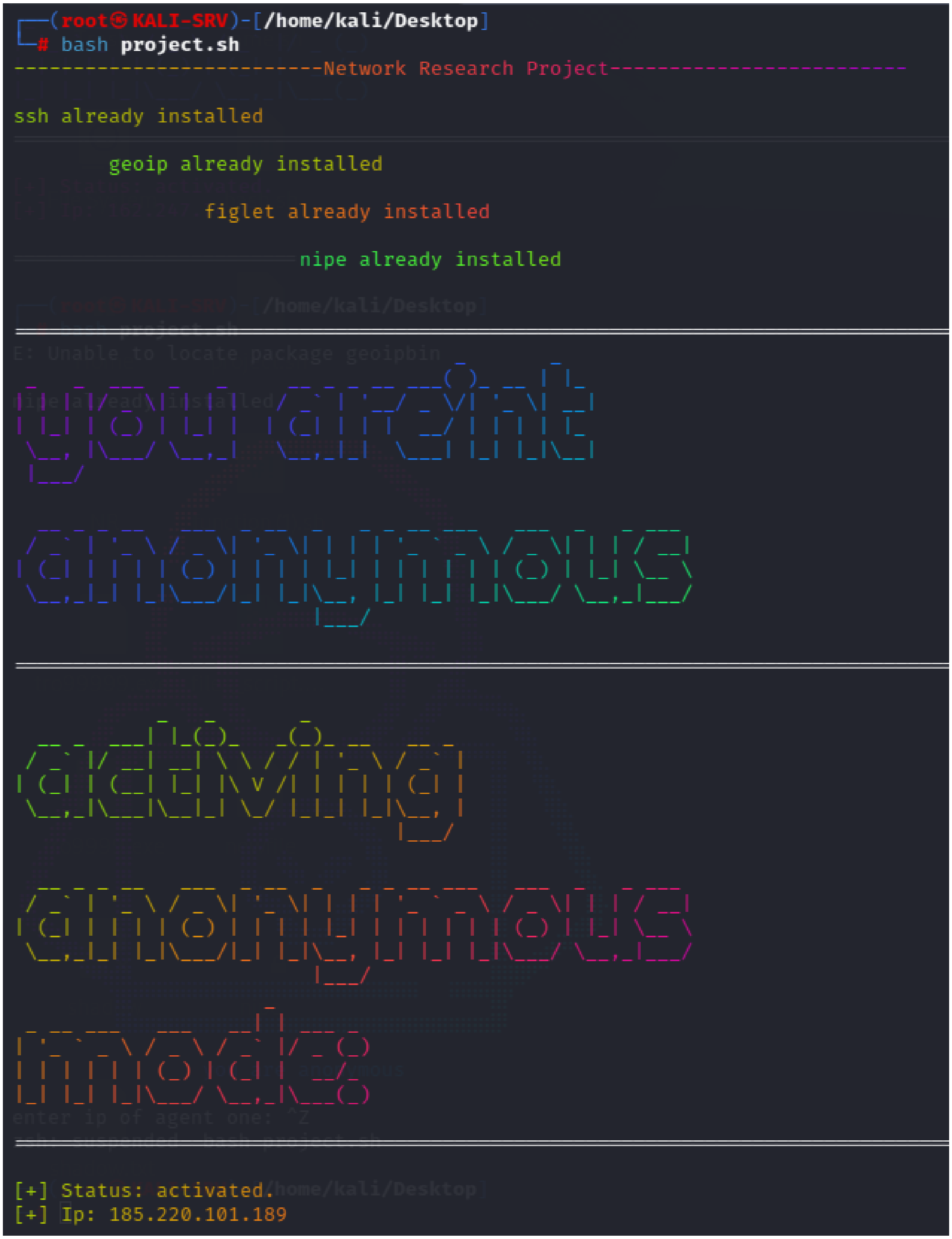
```
┌──(root㉿KALI-SRV)-[/home/kali/Desktop]
└─# bash project.sh
--------------------------Network Research Project-------------------------

ssh already installed

      geoip already installed

               nipe already installed
```

function to check if you are anonymous by comparison with the user country if the user is from Israel then he’s not anonymous else he is anonymous

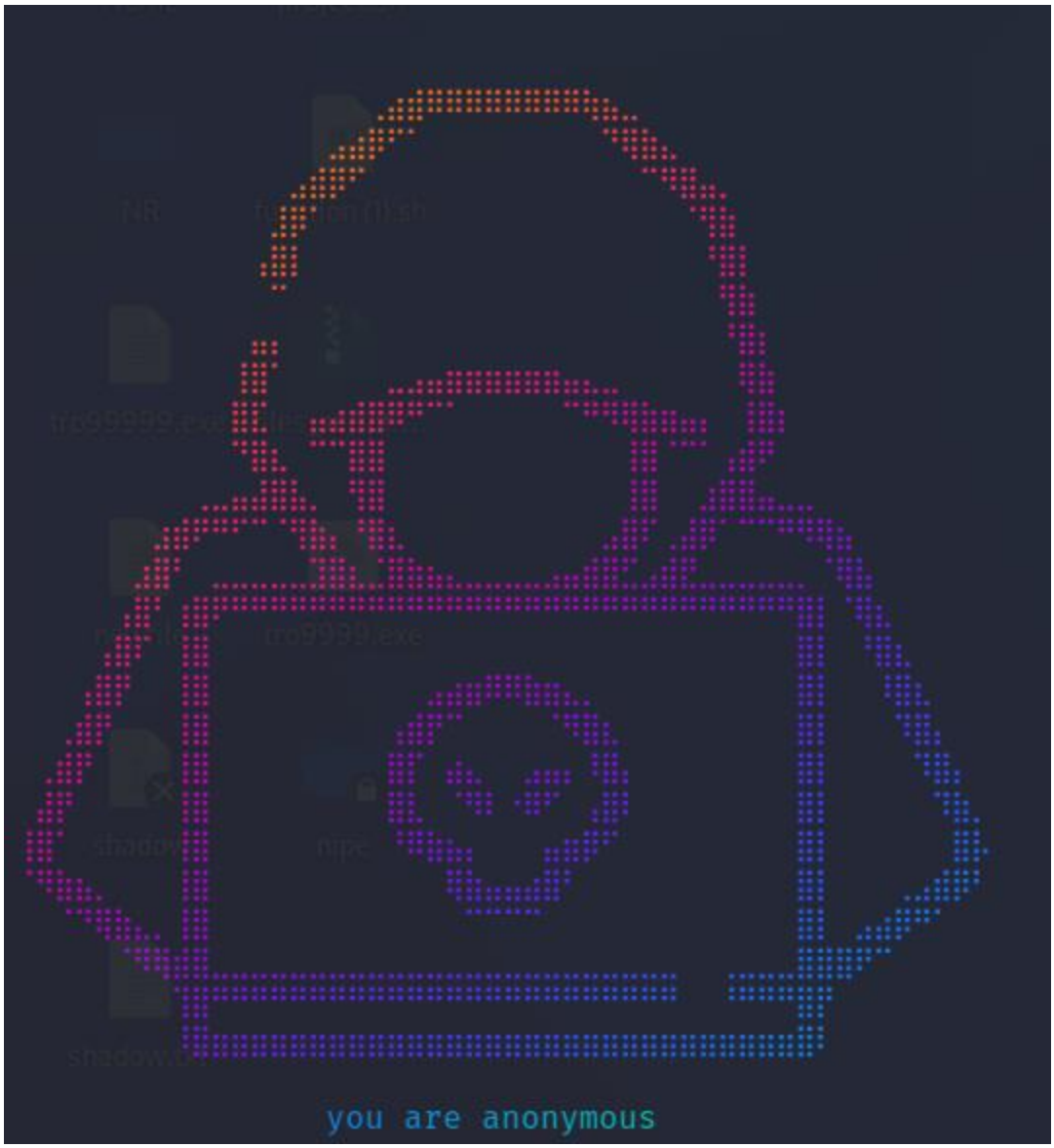


```
#~ #function to check if you are anonymous

function ANON()
{
EXTIP=$(curl -s ifconfig.co)

CNT=$(geoiplookup $EXTIP | awk '{print $4}' | sed 's/,//g')

if  [ "$CNT" != "IL" ]
then
    echo "
























                                                   " | lolcat
    echo ""
    echo "                you are anonymous         " | lolcat -a -d 60
    echo ""
```

```
else
    echo "================================================================================="
    figlet  "you  are'nt anonymous" | lolcat
    echo
    echo "================================================================================="
    echo
    figlet "activing anonymous mode: " | lolcat
    echo "================================================================================="
    cd /home/kali/nipe
    perl nipe.pl start 1>/dev/null
    perl nipe.pl restart 1>/dev/null
    perl nipe.pl start 1>/dev/null
    perl nipe.pl status | lolcat
    echo "========================="
    exit

fi
}
```



```
┌──(root㉿KALI-SRV)-[/home/kali/Desktop]
└─# bash project.sh
--------------------------Network Research Project-------------------------

ssh already installed

        geoip already installed

                figlet already installed

                        nipe already installed

                                    _       _
 _   _  ___  _   _    __ _ _ __ ___( )_ __ | |_
| | | |/ _ \| | | |  / _` | '__/ _ \/| '_ \| __|
| |_| | (_) | |_| | | (_| | | |  __/ | | | | |_
 \__, |\___/ \__,_|  \__,_|_|  \___| |_| |_|\__|
 |___/

  __ _ _ __   ___  _ __  _   _ _ __ ___   ___  _   _ ___
 / _` | '_ \ / _ \| '_ \| | | | '_ ` _ \ / _ \| | | / __|
| (_| | | | | (_) | | | | |_| | | | | | | (_) | |_| \__ \
 \__,_|_| |_|\___/|_| |_|\__, |_| |_| |_|\___/ \__,_|___/
                         |___/


            _   _       _
  __ _  ___| |_(_)_   _(_)_ __   __ _
 / _` |/ __| __| \ \ / / | '_ \ / _` |
| (_| | (__| |_| |\ V /| | | | | (_| |
 \__,_|\___|\__|_| \_/ |_|_| |_|\__, |
                                |___/

  __ _ _ __   ___  _ __  _   _ _ __ ___   ___  _   _ ___
 / _` | '_ \ / _ \| '_ \| | | | '_ ` _ \ / _ \| | | / __|
| (_| | | | | (_) | | | | |_| | | | | | | (_) | |_| \__ \
 \__,_|_| |_|\___/|_| |_|\__, |_| |_| |_|\___/ \__,_|___/
                         |___/
                     _
 _ __ ___   ___   __| | ___ _
| '_ ` _ \ / _ \ / _` |/ _ (_)
| | | | | | (_) | (_| |  __/_
|_| |_| |_|\___/ \__,_|\___(_)


[+] Status: activated.
[+] Ip: 185.220.101.189
```

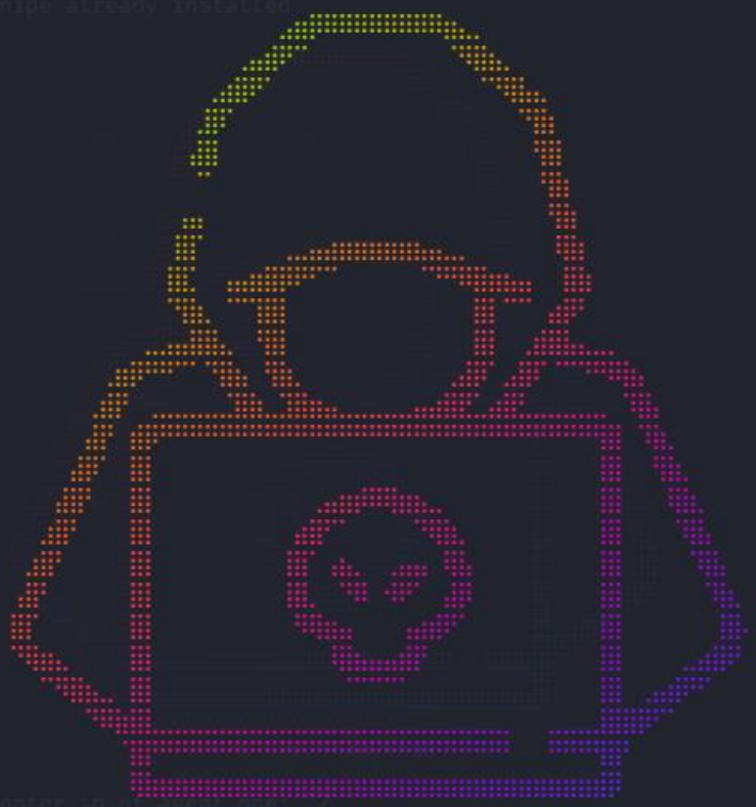

you are anonymous

Queries function

After you become anonymous you controlling your agents by queries to obtain information on the target

```
#~ A function for obtaining information about the target by agents
function VPS()
{
    read -p "enter ip of agent one: " IP

    read -p "enter username of agent one: " USER

    read -p "enter ip range to scan: " RNG
    echo ""
    echo "scaning for open ports" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "nmap  $RNG -Pn -p22,80,443 | grep open " #namp query for port scan
    echo ""
    echo "scaning for hosts in the network" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "nmap -sn  $RNG | grep -i scan" #namp scan for hosts in the network
    echo ""
    echo "scaning for operating systems" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "nmap -sV -F  $RNG | grep -i service | grep -i info" #namp scan for Operating Systems
    echo ""
    read -p "enter ip of agent two: " IP
    read -p "enter username of agent two: " USER
    read -p "enter ip range to scan: " RNG
    echo "scaning country of the target" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "whois  $RNG | grep -i country " #whois query for country
    echo ""
    echo "scaning city of the target" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP " whois  $RNG | grep -i city " #whois query for city
    echo ""
    echo "scaning Phone number of the target" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "whois  $RNG |grep -i OrgTechPhone | awk '{print $2}'" #whois query for phone number of the target
    echo ""
    echo "scaning Email of the target" | lolcat
    sshpass -p "$USER" ssh -o StrictHostKeyChecking=no $USER@$IP "whois  $RNG |grep -i OrgTechemail " #whois query for the email of the target


}
INST
ANON
VPS
```

```
┌──(root㉿KALI-SRV)-[/home/kali/Desktop]
└─# bash project.sh
-------------------------Network Research Project-------------------------

ssh already installed

        geoip already installed

                figlet already installed

                        nipe already installed
```



```
                you are anonymous

enter ip of agent one:
```

```
enter ip of agent one: 192.168.188.139
enter username of agent one: kali
enter ip range to scan: 18.198.103.184

scaning for open ports
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

scaning for hosts in the network
Nmap scan report for ec2-18-198-103-184.eu-central-1.compute.amazonaws.com (18.198.103.184)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

scaning for operating systems
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

enter ip of agent two: 192.168.188.138
enter username of agent two: tc
enter ip range to scan: 18.198.103.184
scaning country of the target
Country:        US
Country:        DE

scaning city of the target
City:           Seattle
City:           Munchen

scaning Phone number of the target
OrgTechPhone:  +1-206-555-0000
OrgTechPhone:  +1-206-555-0000

scaning Email of the target
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechEmail:  amzn-noc-contact@amazon.com

┌──(root㉿KALI-SRV)-[/home/kali/Desktop]
└─#
```

To run the script, you must have lolcat plugin

- Sudo apt-get install lolcat

Yair Solomon

Remote control project

Lecturer: Natalie Erez