Centre For Cybersecurity

Remote Control (S4)

15.04.2023

Muhammad Alif Anas Bin Ahmad

Overview

The project is meant to allow students to practice their knowledge of the Kali Linux system and aspects of network research and to code a bash script to program the necessary commands to probe information from a targeted IP address of an external system. This report will be documenting the different steps to reach the end product

Goals

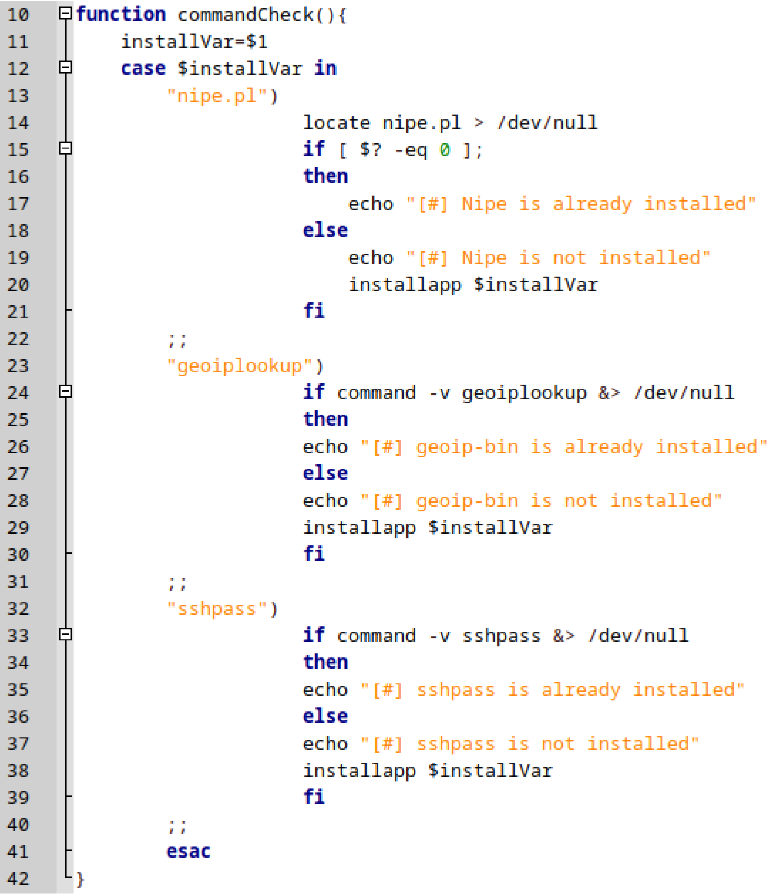
1. To script will be able to anonymously get information from a target IP address
2. Such information includes the nmap data and the whois data
3. The information gathered will then be output into a folder

Methods and Steps

I. Installation and anonymity check

Helper Functions

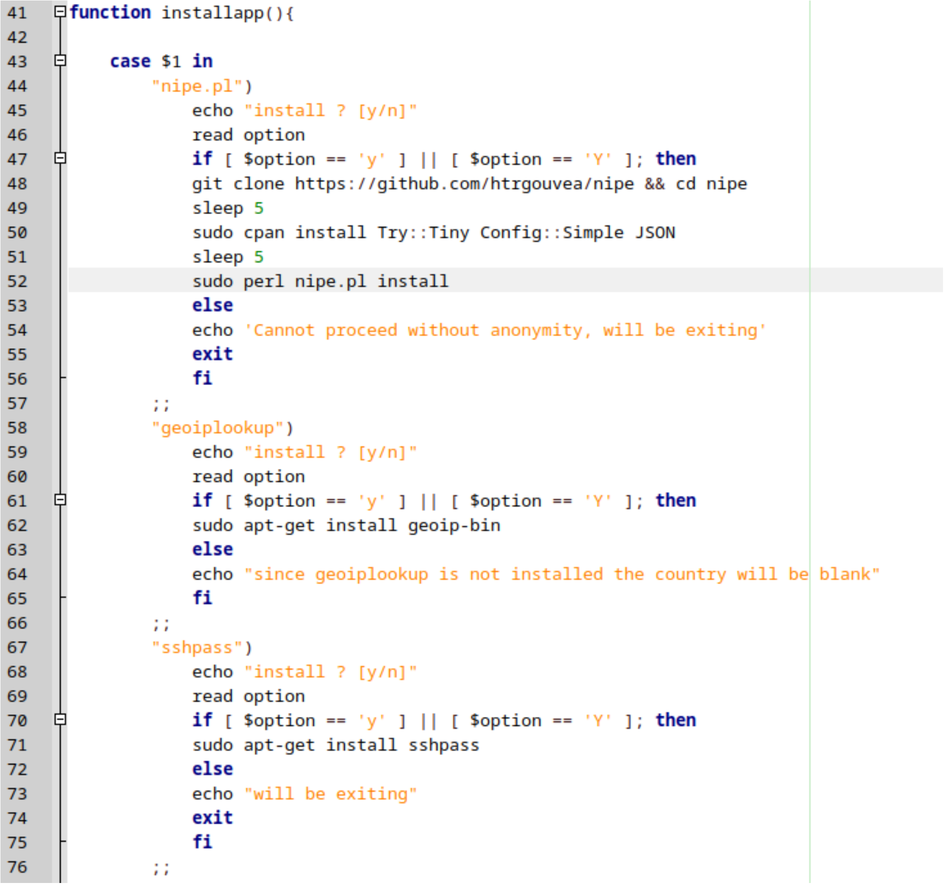
commandCheck()



```
function commandCheck(){
    installVar=$1
    case $installVar in
        "nipe.pl")
                    locate nipe.pl > /dev/null
                    if [ $? -eq 0 ];
                    then
                        echo "[#] Nipe is already installed"
                    else
                        echo "[#] Nipe is not installed"
                        installapp $installVar
                    fi
        ;;
        "geoiplookup")
                    if command -v geoiplookup &> /dev/null
                    then
                    echo "[#] geoip-bin is already installed"
                    else
                    echo "[#] geoip-bin is not installed"
                    installapp $installVar
                    fi
        ;;
        "sshpass")
                    if command -v sshpass &> /dev/null
                    then
                    echo "[#] sshpass is already installed"
                    else
                    echo "[#] sshpass is not installed"
                    installapp $installVar
                    fi
        ;;
        esac
}
```

This helper function will be in charge of the checking if the relevant apps have been installed, if the app such as Nipe is installed, then a message saying Nipe has been installed and will not proceed with installing Nipe.

installapp()

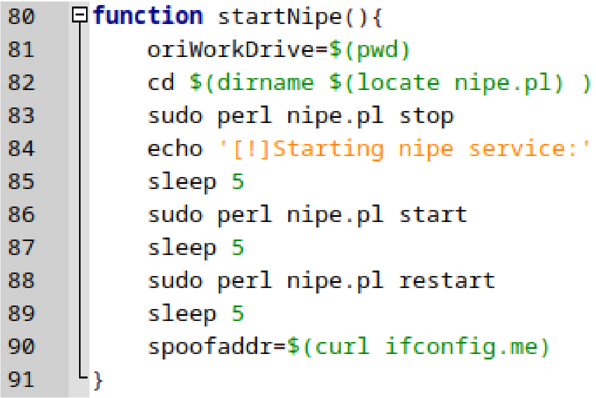


```
function installapp(){

    case $1 in
        "nipe.pl")
            echo "install ? [y/n]"
            read option
            if [ $option == 'y' ] || [ $option == 'Y' ]; then
            git clone https://github.com/htrgouvea/nipe && cd nipe
            sleep 5
            sudo cpan install Try::Tiny Config::Simple JSON
            sleep 5
            sudo perl nipe.pl install
            else
            echo 'Cannot proceed without anonymity, will be exiting'
            exit
            fi
        ;;
        "geoiplookup")
            echo "install ? [y/n]"
            read option
            if [ $option == 'y' ] || [ $option == 'Y' ]; then
            sudo apt-get install geoip-bin
            else
            echo "since geoiplookup is not installed the country will be blank"
            fi
        ;;
        "sshpass")
            echo "install ? [y/n]"
            read option
            if [ $option == 'y' ] || [ $option == 'Y' ]; then
            sudo apt-get install sshpass
            else
            echo "will be exiting"
            exit
            fi
        ;;
```

This function will be called inside the earlier function commandCheck() and will trigger only when the said app is not yet installed on the system. The function is again using the Case statement to segregate the code into the three apps needed to run this script. Also, if the user does not want to install either SSHpass or Nipe, the program will exit. However, iff the Geoiplookup is not installed, then the program will continue but with some blanks in the data.

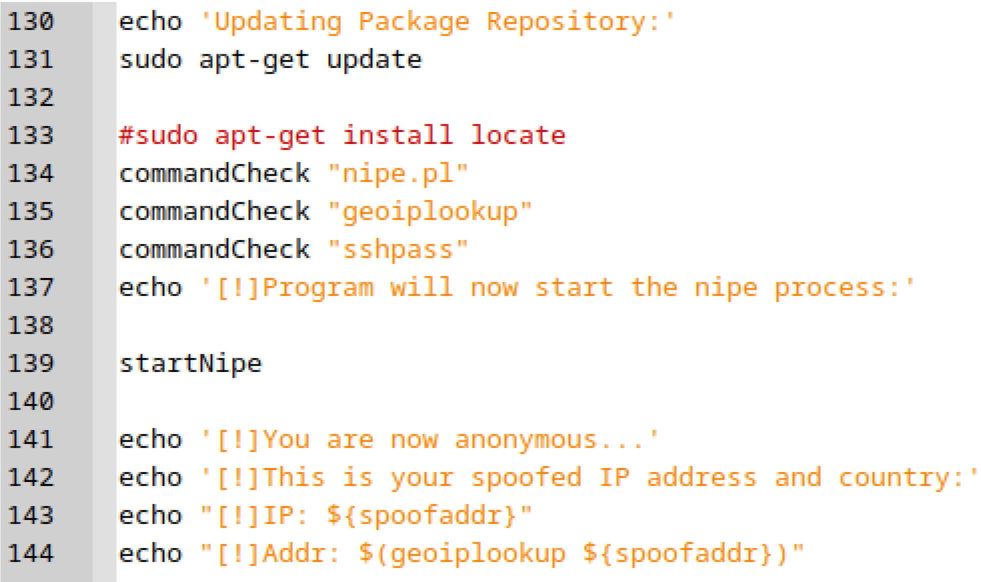
startNipe()



```
function startNipe(){
    oriWorkDrive=$(pwd)
    cd $(dirname $(locate nipe.pl) )
    sudo perl nipe.pl stop
    echo '[!]Starting nipe service:'
    sleep 5
    sudo perl nipe.pl start
    sleep 5
    sudo perl nipe.pl restart
    sleep 5
    spoofaddr=$(curl ifconfig.me)
}
```

The startNipe() function will change directory into where the nipe.pl is located so that the next commands will execute with no errors. It will then stop the nipe.pl service first in case the nipe.pl has already been started before running this script, then it will pause for 5 seconds before running the next command to give the Nipe time to execute properly.

Main Code



```
echo 'Updating Package Repository:'
sudo apt-get update

#sudo apt-get install locate
commandCheck "nipe.pl"
commandCheck "geoiplookup"
commandCheck "sshpass"
echo '[!]Program will now start the nipe process:'

startNipe

echo '[!]You are now anonymous...'
echo '[!]This is your spoofed IP address and country:'
echo "[!]IP: ${spoofaddr}"
echo "[!]Addr: $(geoiplookup ${spoofaddr})"
```

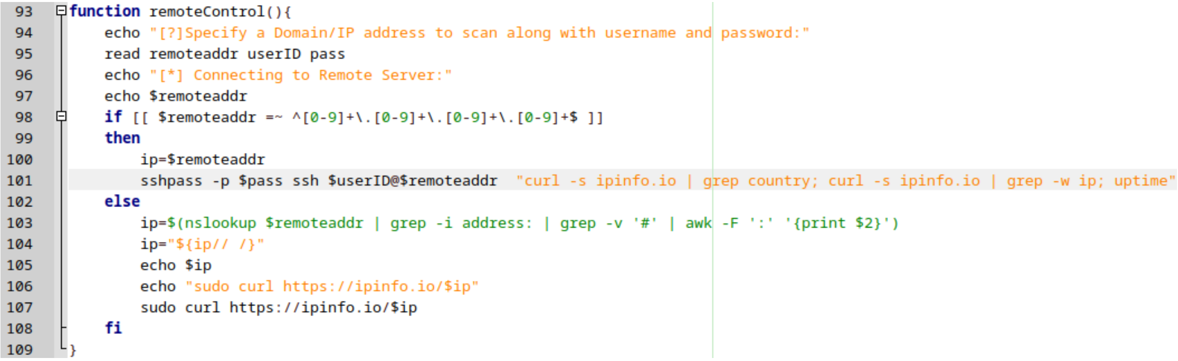
With the use of the helper functions, the main code for the initial part of the script is easy to manage, the first command will be to update the package repository, then it will check if the needed commands have been installed on the system, after installing the commands, the program will start Nipe to give the anonymity before the rest of the program runs.

It will also provide the IP address of the spoofed IP as well as the address of the IP.

II. Auto Connect and execute commands on Remote Server via SSH

Helper Functions

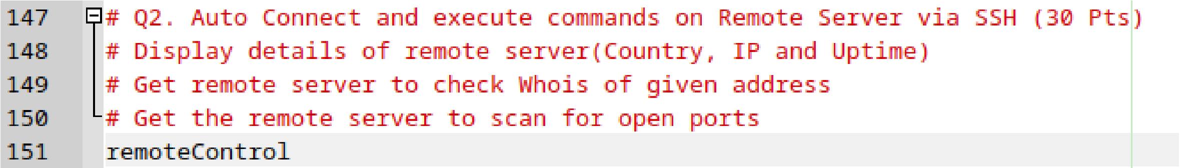
remoteControl()



```
function remoteControl(){
    echo "[?]Specify a Domain/IP address to scan along with username and password:"
    read remoteaddr userID pass
    echo "[*] Connecting to Remote Server:"
    echo $remoteaddr
    if [[ $remoteaddr =~ ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$ ]]
    then
        ip=$remoteaddr
        sshpass -p $pass ssh $userID@$remoteaddr  "curl -s ipinfo.io | grep country; curl -s ipinfo.io | grep -w ip; uptime"
    else
        ip=$(nslookup $remoteaddr | grep -i address: | grep -v '#' | awk -F ':' '{print $2}')
        ip="${ip// /}"
        echo $ip
        echo "sudo curl https://ipinfo.io/$ip"
        sudo curl https://ipinfo.io/$ip
    fi
}
```

This helper function will mainly check and see if the user has entered an IP or the name of a website, then it will segregate the code using a IF ELSE statement, if user has entered an IP, it will also need the username and password of the target address so that sshpass will be used to get the details of the target. If the name of the website is used, then the IP address will be extracted using the nslookup and grep commands. Then it will make use of the API of Ipinfo website to get the information from the extracted IP address.

Main Code



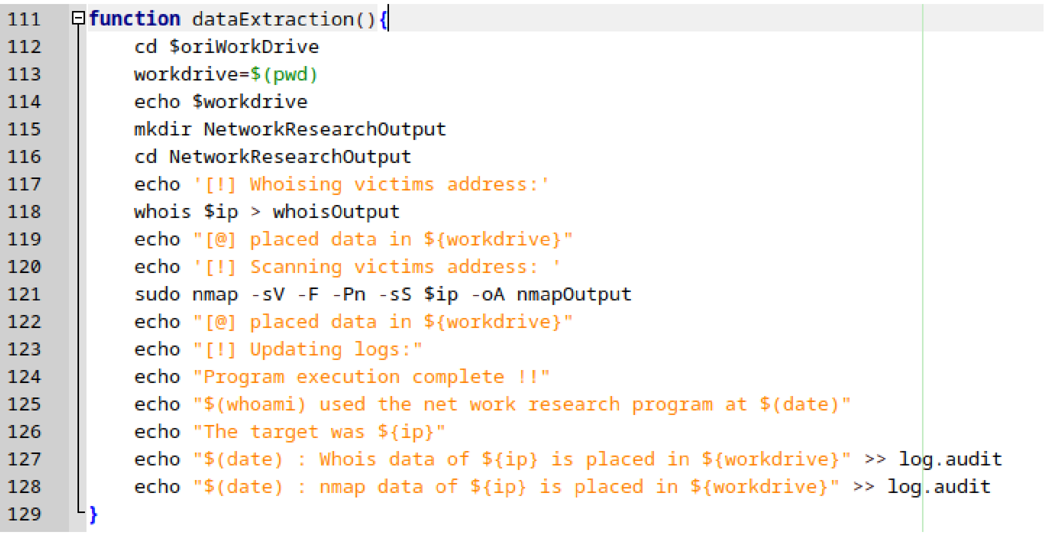
```
# Q2. Auto Connect and execute commands on Remote Server via SSH (30 Pts)
# Display details of remote server(Country, IP and Uptime)
# Get remote server to check Whois of given address
# Get the remote server to scan for open ports
remoteControl
```

Since the functionality of the second part of the script is already in the helper function, the main code only contains the calling of said helper function

III. Results

Helper Functions

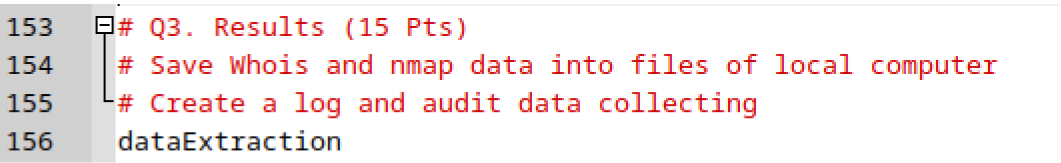
dataExtraction()



```
function dataExtraction(){
    cd $oriWorkDrive
    workdrive=$(pwd)
    echo $workdrive
    mkdir NetworkResearchOutput
    cd NetworkResearchOutput
    echo '[!] Whoising victims address:'
    whois $ip > whoisOutput
    echo "[@] placed data in ${workdrive}"
    echo '[!] Scanning victims address: '
    sudo nmap -sV -F -Pn -sS $ip -oA nmapOutput
    echo "[@] placed data in ${workdrive}"
    echo "[!] Updating logs:"
    echo "Program execution complete !!"
    echo "$(whoami) used the net work research program at $(date)"
    echo "The target was ${ip}"
    echo "$(date) : Whois data of ${ip} is placed in ${workdrive}" >> log.audit
    echo "$(date) : nmap data of ${ip} is placed in ${workdrive}" >> log.audit
}
```

This helper function will extract the needed data from both the whois as well as the nmap outputs into the newly created directory in the same folder where the program is executed. Then the logs will be updated with information such as the user who executed the script, the time and the target IP address

Main code



```
# Q3. Results (15 Pts)
# Save Whois and nmap data into files of local computer
# Create a log and audit data collecting
dataExtraction
```

Same with the previous part of the script, the helper function already has all the functionalities coded inside it and the main code will only need to call the helper function.

References

Nmap. (n.d.). Retrieved April 14, 2023, from https://nmap.org/

Htrgouvea. (n.d.). HTRGOUVEA/NIPE: An engine to make Tor Network your default gateway. GitHub. Retrieved April 15, 2023, from https://github.com/htrgouvea/nipe

Radu RădeanuRadu Rădeanu Get my country by IP in Bash. Unix &amp; Linux Stack Exchange. Retrieved April 15, 2023, from https://unix.stackexchange.com/questions/83473/get-my-country-by-ip-in-bash