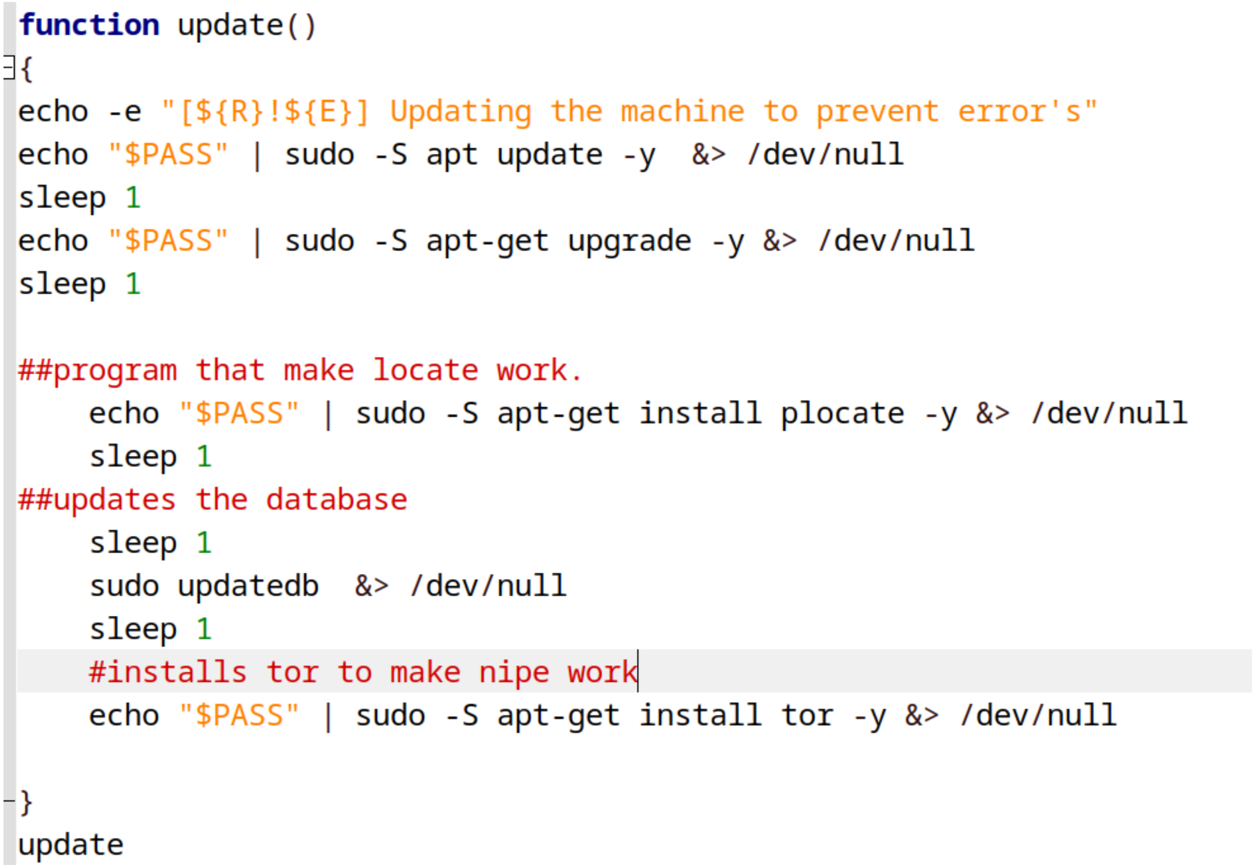
Network Research:Project

Project remote control : by daniel kovalevsky : student *8* teacher = arel
Class : 21 cybersecurity

#UPDATES

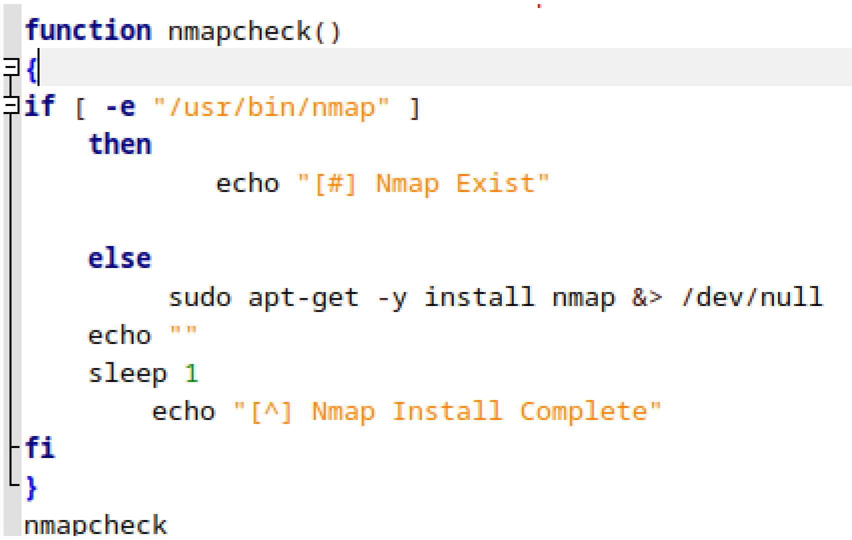
- updates the system , and installing placate [which make locate works] than updates the locate data base , and installing tor to make nipe work.



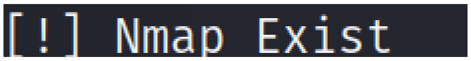
```
function update()
{
echo -e "[${R}!${E}] Updating the machine to prevent error's"
echo "$PASS" | sudo -S apt update -y  &> /dev/null
sleep 1
echo "$PASS" | sudo -S apt-get upgrade -y &> /dev/null
sleep 1

##program that make locate work.
    echo "$PASS" | sudo -S apt-get install plocate -y &> /dev/null
    sleep 1
##updates the database
    sleep 1
    sudo updatedb  &> /dev/null
    sleep 1
    #installs tor to make nipe work
    echo "$PASS" | sudo -S apt-get install tor -y &> /dev/null

}
update
```

#Nmap check

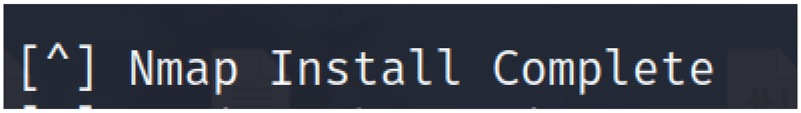
- this function with to check if the file nmap is in the system if unable to find than the function will install it.



```
function nmapcheck()
{
if [ -e "/usr/bin/nmap" ]
    then
            echo "[#] Nmap Exist"

    else
         sudo apt-get -y install nmap &> /dev/null
    echo ""
    sleep 1
        echo "[^] Nmap Install Complete"
fi
}
nmapcheck
```



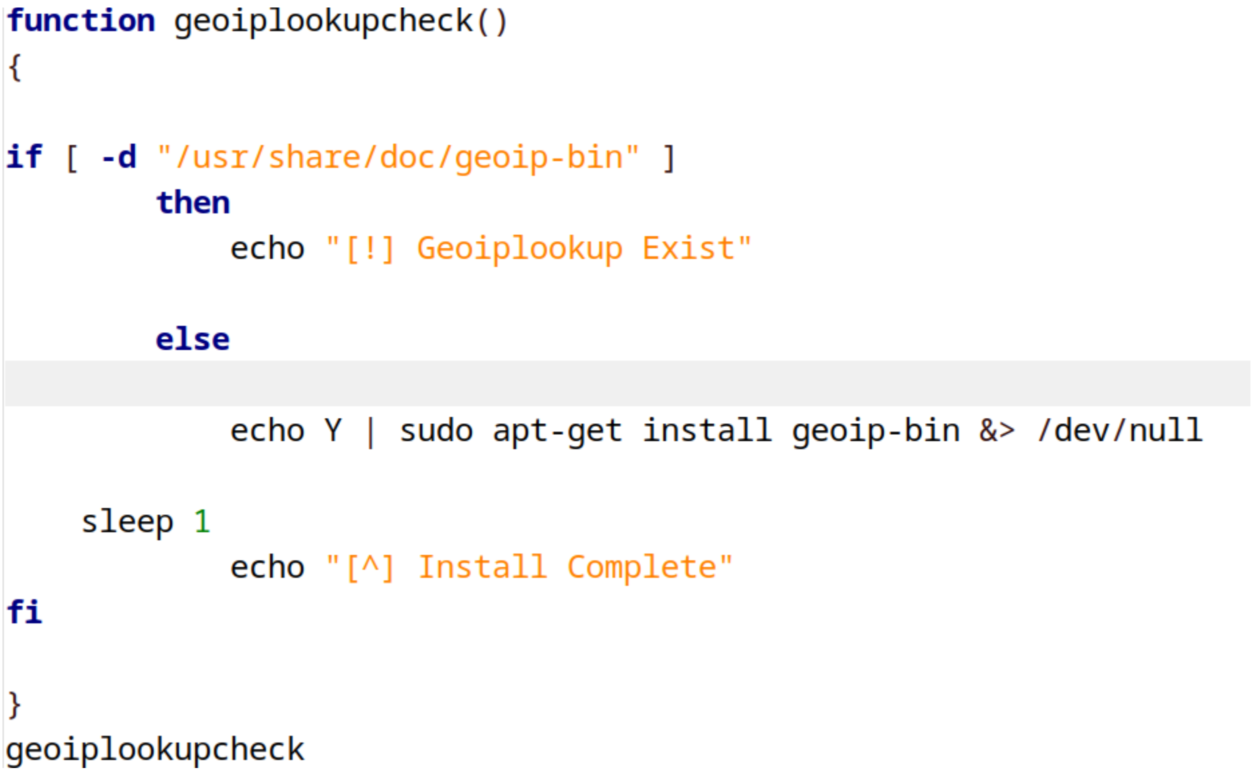
```
[!] Nmap Exist
```



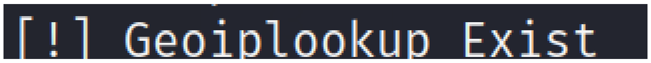
```
[^] Nmap Install Complete
```

#geoiplookup Check

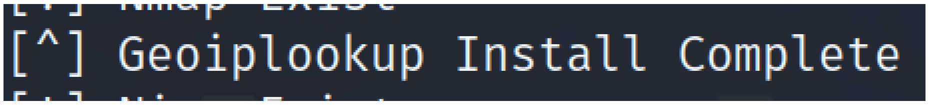
- by writing this function , we gave the function and option to find if geoiplookup (geoip-bin) is installed or not . if the program was in installed then it will say it exist , and if then it will download it and say the download was complete .



```
function geoiplookupcheck()
{

if [ -d "/usr/share/doc/geoip-bin" ]
        then
            echo "[!] Geoiplookup Exist"

        else

            echo Y | sudo apt-get install geoip-bin &> /dev/null

    sleep 1
            echo "[^] Install Complete"
fi

}
geoiplookupcheck
```



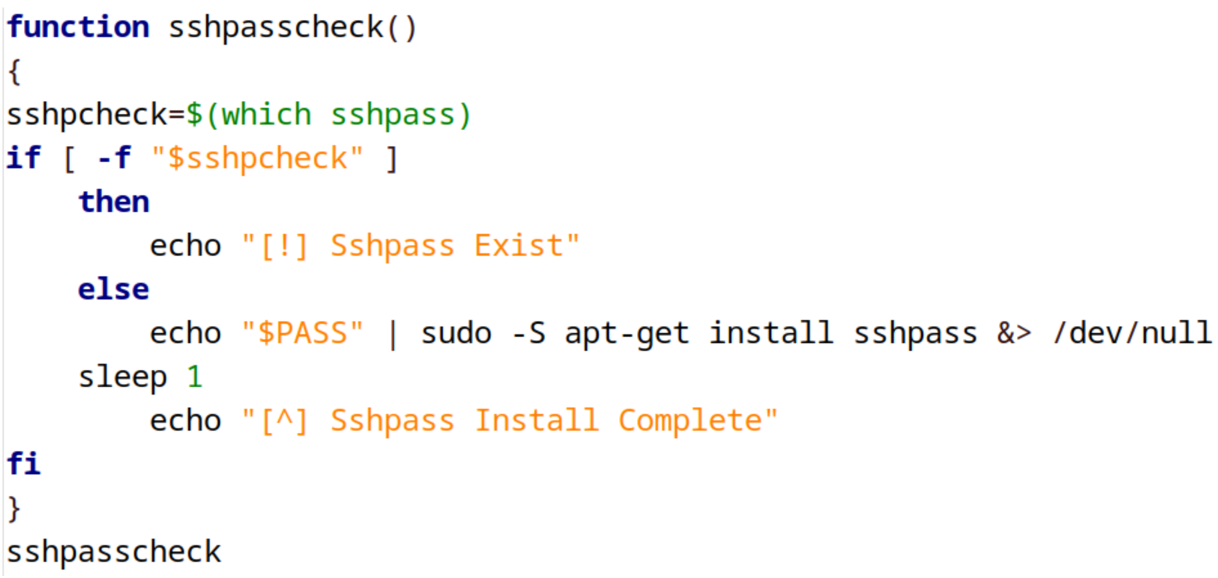
```
[!] Geoiplookup Exist
```



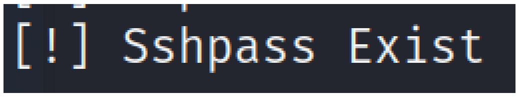
```
[^] Geoiplookup Install Complete
```

#Sshpasscheck

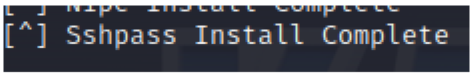
- by writing this function we used var to find the sshpass file if it exist
If not , it will install the sshpass



```
function sshpasscheck()
{
sshpcheck=$(which sshpass)
if [ -f "$sshpcheck" ]
    then
        echo "[!] Sshpass Exist"
    else
        echo "$PASS" | sudo -S apt-get install sshpass &> /dev/null
    sleep 1
        echo "[^] Sshpass Install Complete"
fi
}
sshpasscheck
```



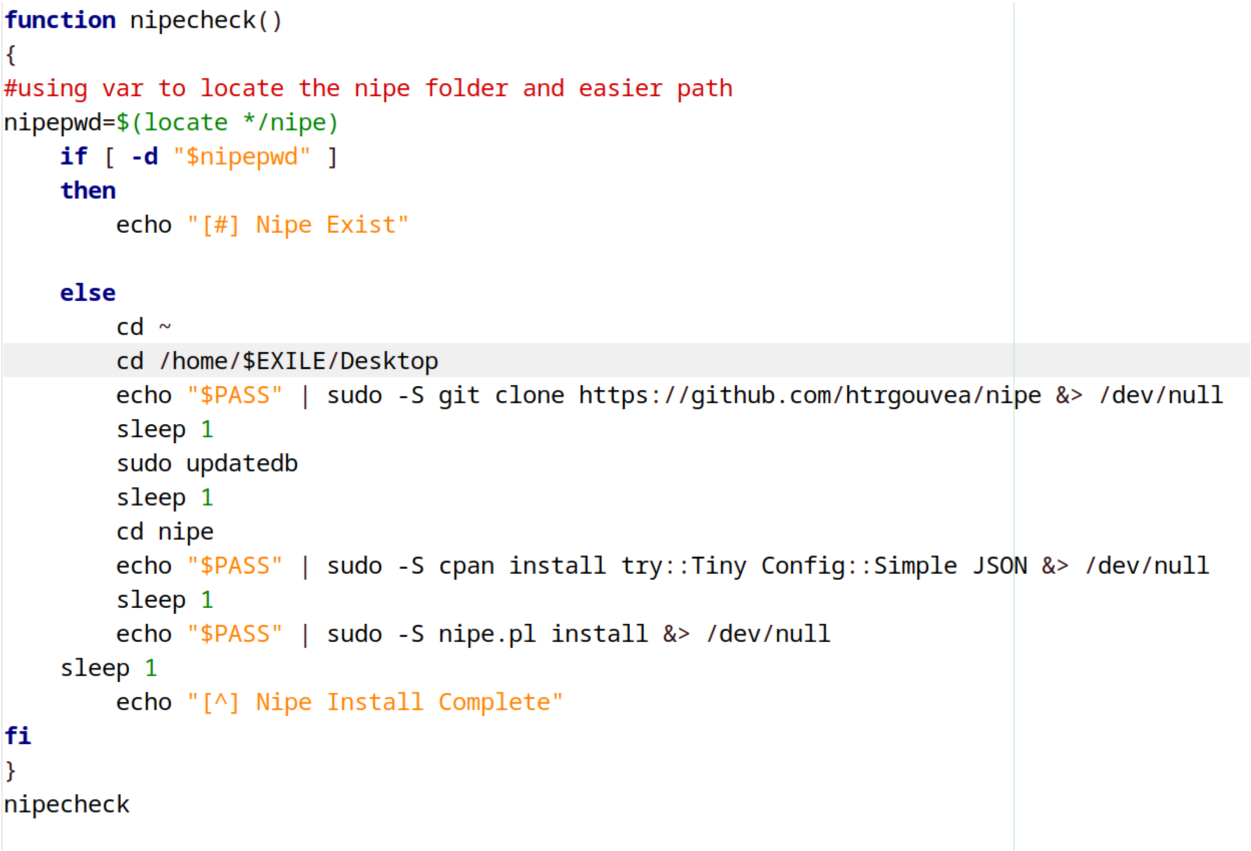
```
[!] Sshpass Exist
```



```
[^] Sshpass Install Complete
```

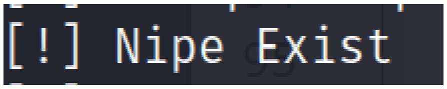
#Nipe check

- by writing this function we used var to locate nipe in the system.
And gave and option <if> nipe was installed then it will skip the process .
and if not it will download nipe on the desktop .



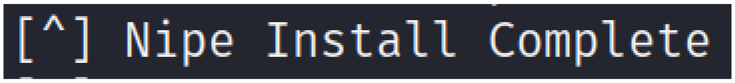
```
function nipecheck()
{
#using var to locate the nipe folder and easier path
nipepwd=$(locate */nipe)
    if [ -d "$nipepwd" ]
    then
        echo "[#] Nipe Exist"

    else
        cd ~
        cd /home/$EXILE/Desktop
        echo "$PASS" | sudo -S git clone https://github.com/htrgouvea/nipe &> /dev/null
        sleep 1
        sudo updatedb
        sleep 1
        cd nipe
        echo "$PASS" | sudo -S cpan install try::Tiny Config::Simple JSON &> /dev/null
        sleep 1
        echo "$PASS" | sudo -S nipe.pl install &> /dev/null
    sleep 1
        echo "[^] Nipe Install Complete"
fi
}
nipecheck
```

~if nipe already installed it will show this indicator



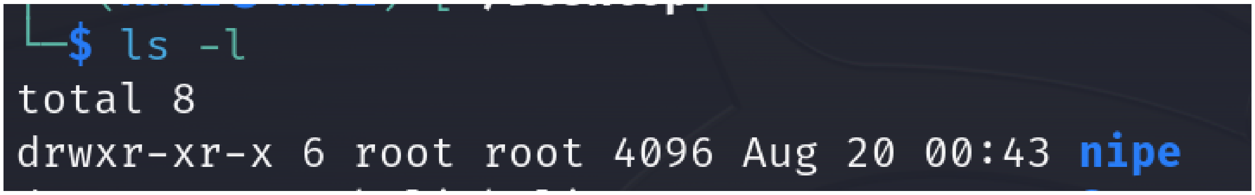
```
[!] Nipe Exist
```

~indicator of nipe begin installed



```
[^] Nipe Install Complete
```

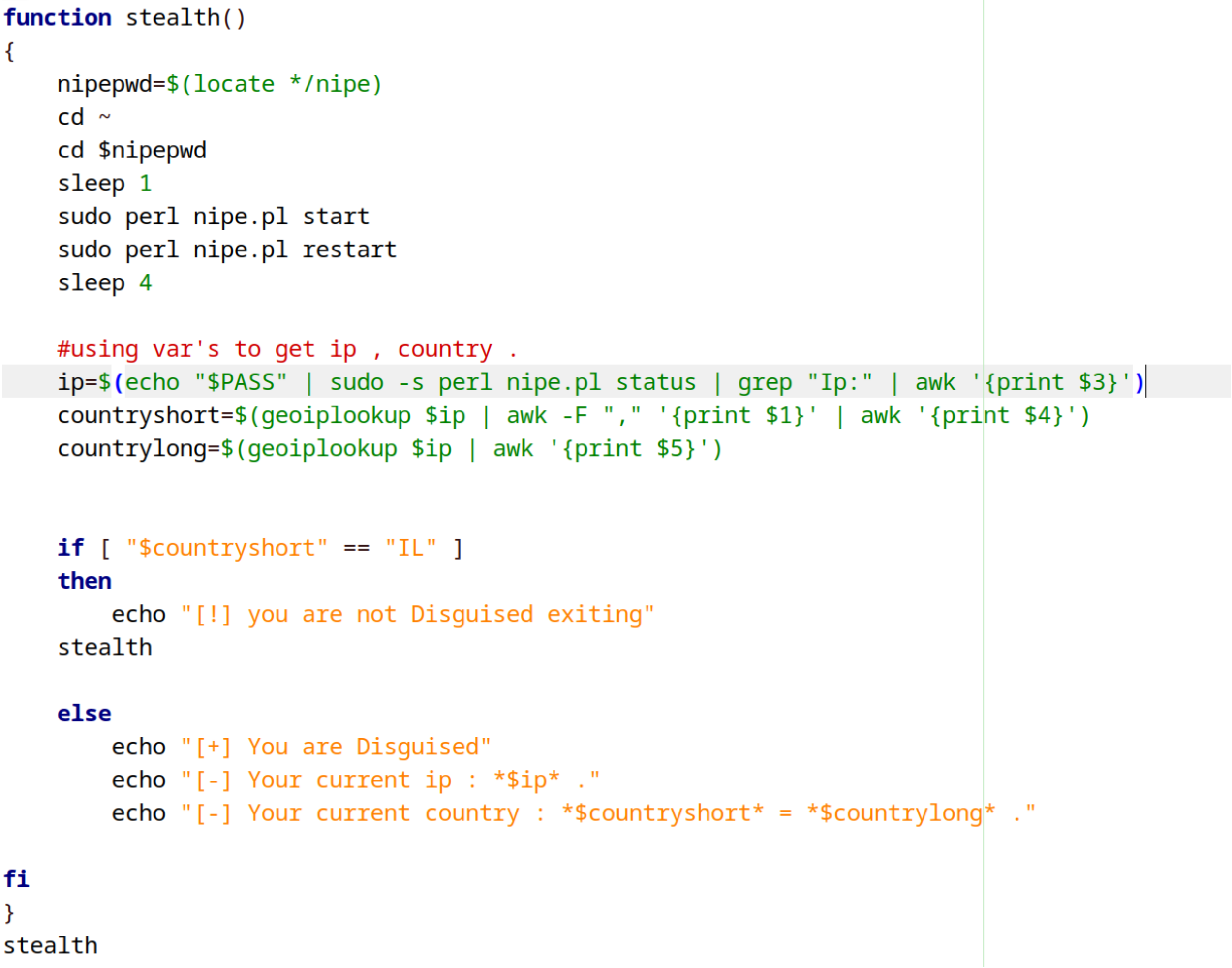
~ls -l where the nipe was installed



```
└─$ ls -l
total 8
drwxr-xr-x 6 root root 4096 Aug 20 00:43 nipe
```

#Nipe activation

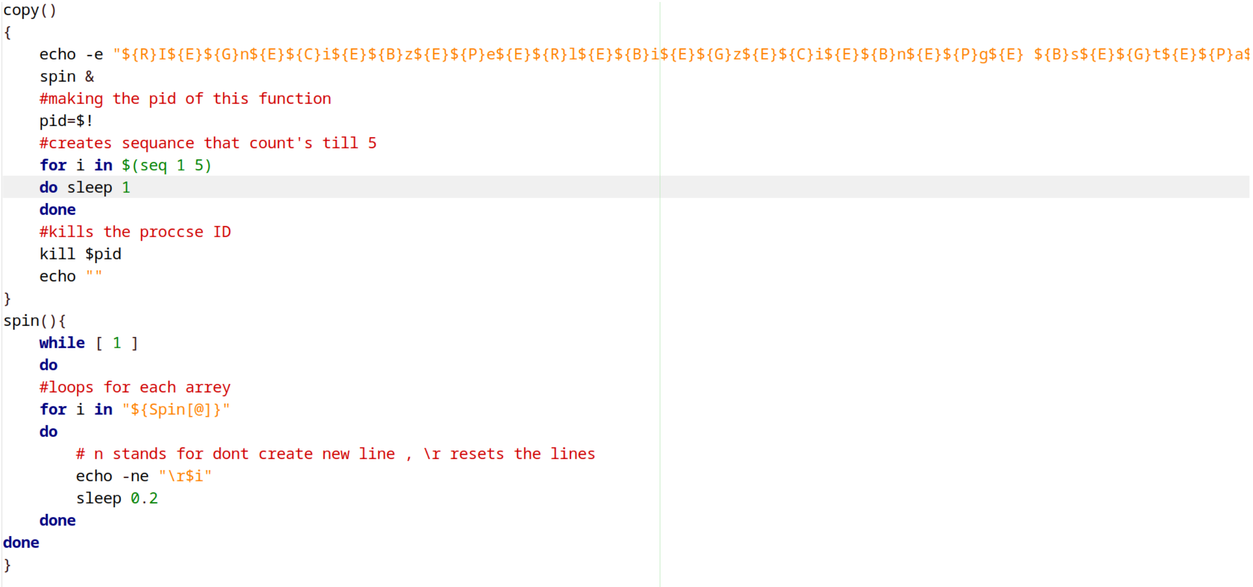
- using function named stealth to change folder to where nipe is located Than using nipe.pl start and restart to kick start the nipe.pl . giving it 4 sec sleep so that the restart will have time to do his magic. Than adding vars of commands like nipe.pl status and geoiplookup to tell the user the status of the ip ,



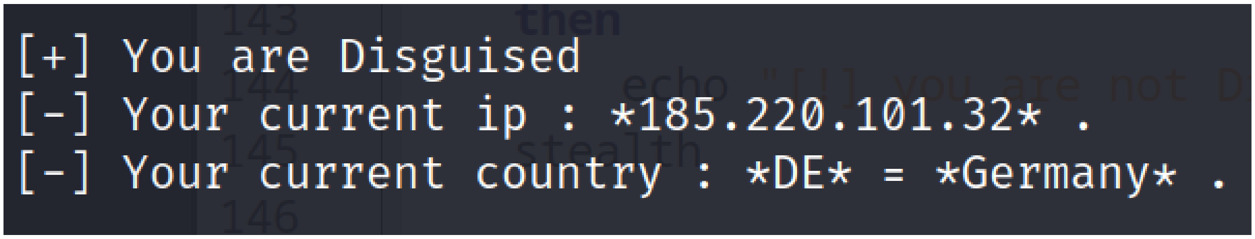
```
function stealth()
{
    nipepwd=$(locate */nipe)
    cd ~
    cd $nipepwd
    sleep 1
    sudo perl nipe.pl start
    sudo perl nipe.pl restart
    sleep 4

    #using var's to get ip , country .
    ip=$(echo "$PASS" | sudo -s perl nipe.pl status | grep "Ip:" | awk '{print $3}')
    countryshort=$(geoiplookup $ip | awk -F "," '{print $1}' | awk '{print $4}')
    countrylong=$(geoiplookup $ip | awk '{print $5}')


    if [ "$countryshort" == "IL" ]
    then
        echo "[!] you are not Disguised exiting"
    stealth

    else
        echo "[+] You are Disguised"
        echo "[-] Your current ip : *$ip* ."
        echo "[-] Your current country : *$countryshort* = *$countrylong* ."

fi
}
stealth
```

#Copy

- Creating a spinning animation , to substitute sleep while restarting nipe



```
copy()
{
    echo -e "${R}I${E}${G}n${E}${C}i${E}${B}z${E}${P}e${E}${R}l${E}${B}i${E}${G}z${E}${C}i${E}${B}n${E}${P}g${E} ${B}s${E}${G}t${E}${P}a$
    spin &
    #making the pid of this function
    pid=$!
    #creates sequance that count's till 5
    for i in $(seq 1 5)
    do sleep 1
    done
    #kills the proccse ID
    kill $pid
    echo ""
}
spin(){
    while [ 1 ]
    do
    #loops for each arrey
    for i in "${Spin[@]}"
    do
        # n stands for dont create new line , \r resets the lines
        echo -ne "\r$i"
        sleep 0.2
    done
done
}
```

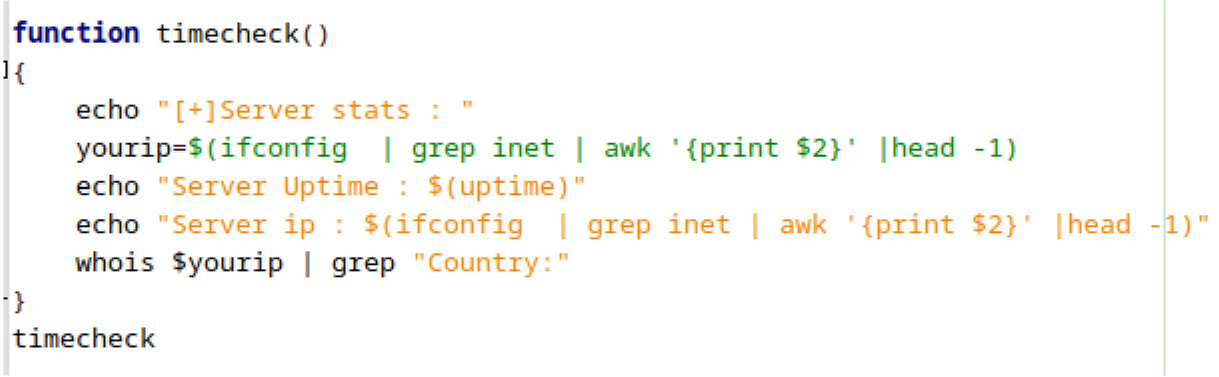


```
[+] You are Disguised
[-] Your current ip : *185.220.101.32* .
[-] Your current country : *DE* = *Germany* .
```

#Server status check

- using this function which will tell the user about the server status

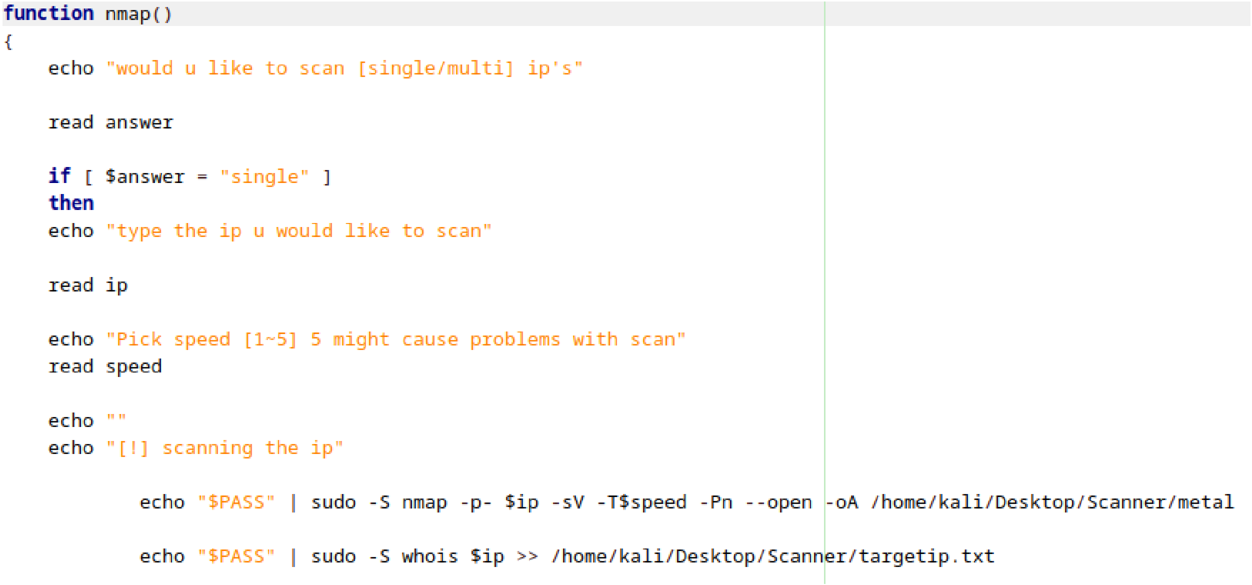
His uptime , his ip , and his ip country



```
function timecheck()
{
    echo "[+]Server stats : "
    yourip=$(ifconfig  | grep inet | awk '{print $2}' |head -1)
    echo "Server Uptime : $(uptime)"
    echo "Server ip : $(ifconfig  | grep inet | awk '{print $2}' |head -1)"
    whois $yourip | grep "Country:"
}
timecheck
```

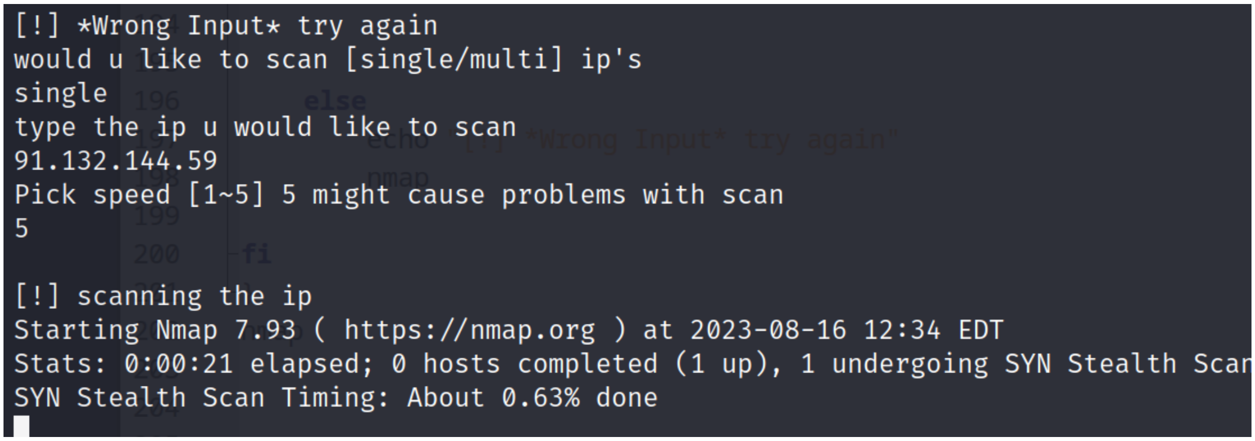
#Nmap + Whois Scan

With nmap i've tried so the user would be able to scan freely ip's of his choice and pick an ip also in this function i've added another option for the user to chose from a list of files , after the user finishes the scan the file saves into 3 file's xml,grepable,flat . to folder of the script.
#Nmap scanning multi from user's list of ip
#nmap scan



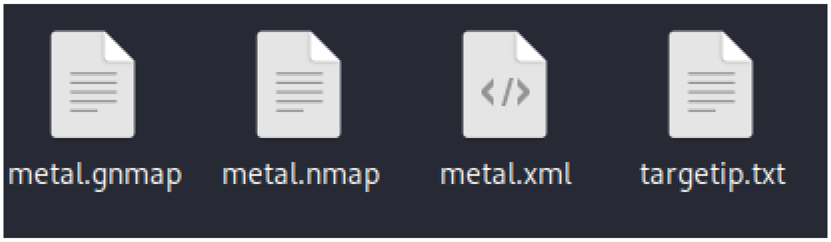
```
function nmap()
{
    echo "would u like to scan [single/multi] ip's"

    read answer

    if [ $answer = "single" ]
    then
    echo "type the ip u would like to scan"

    read ip

    echo "Pick speed [1~5] 5 might cause problems with scan"
    read speed

    echo ""
    echo "[!] scanning the ip"

            echo "$PASS" | sudo -S nmap -p- $ip -sV -T$speed -Pn --open -oA /home/kali/Desktop/Scanner/metal

            echo "$PASS" | sudo -S whois $ip >> /home/kali/Desktop/Scanner/targetip.txt
```

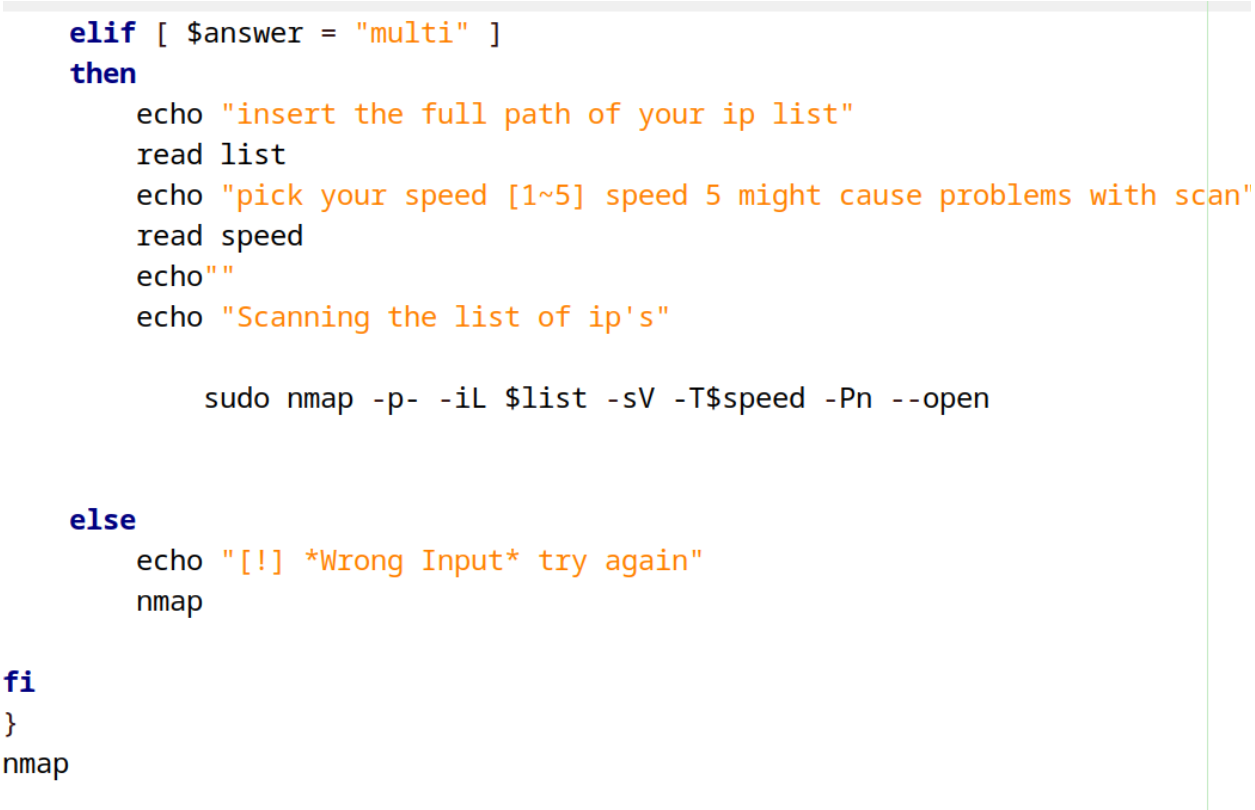
Single nmap scan =



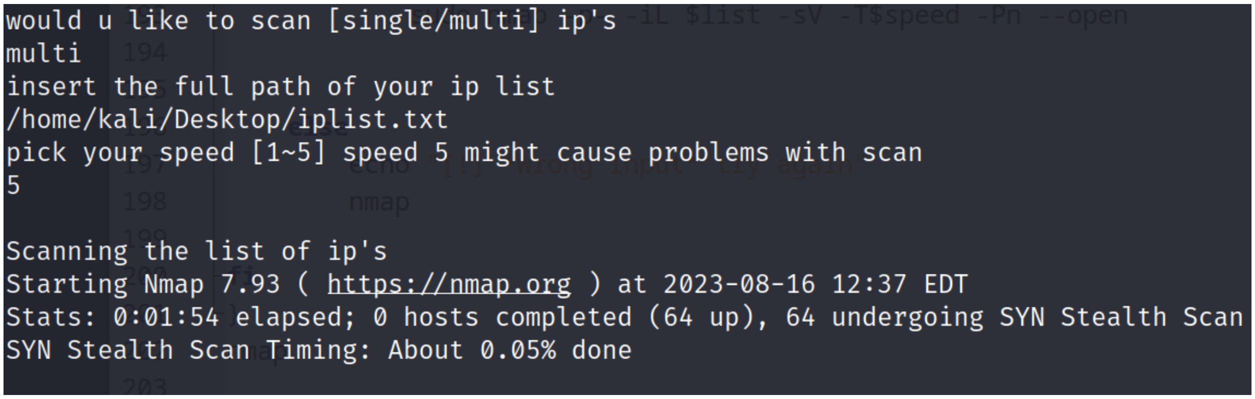
```
[!] *Wrong Input* try again
would u like to scan [single/multi] ip's
single
type the ip u would like to scan
91.132.144.59
Pick speed [1~5] 5 might cause problems with scan
5

[!] scanning the ip
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-16 12:34 EDT
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.63% done
```

The files from nmap + whois scan which created





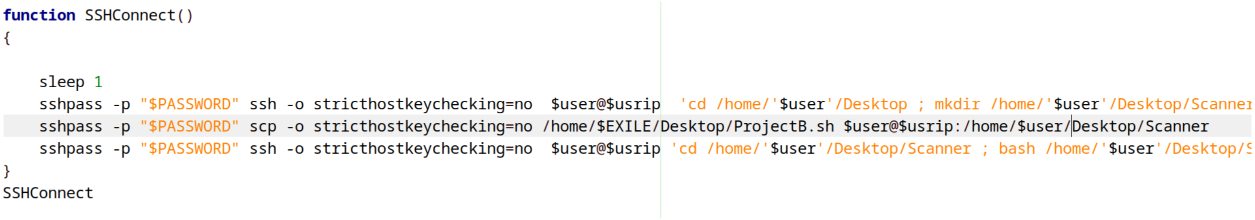
```
    elif [ $answer = "multi" ]
    then
        echo "insert the full path of your ip list"
        read list
        echo "pick your speed [1~5] speed 5 might cause problems with scan"
        read speed
        echo""
        echo "Scanning the list of ip's"

            sudo nmap -p- -iL $list -sV -T$speed -Pn --open


    else
        echo "[!] *Wrong Input* try again"
        nmap

fi
}
nmap
```



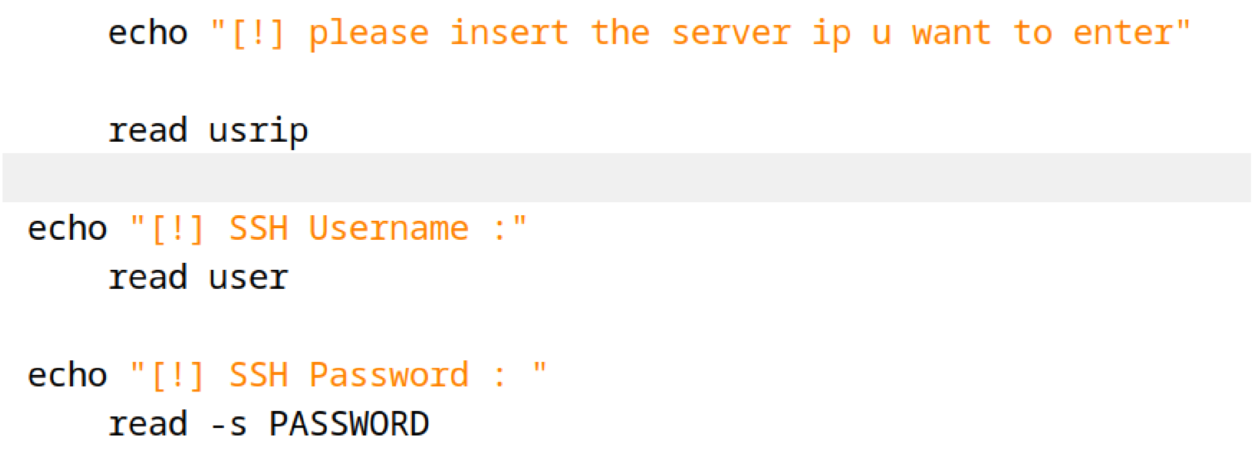
```
would u like to scan [single/multi] ip's
multi
insert the full path of your ip list
/home/kali/Desktop/iplist.txt
pick your speed [1~5] speed 5 might cause problems with scan
5

Scanning the list of ip's
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-16 12:37 EDT
Stats: 0:01:54 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.05% done
```

#SSHConnect

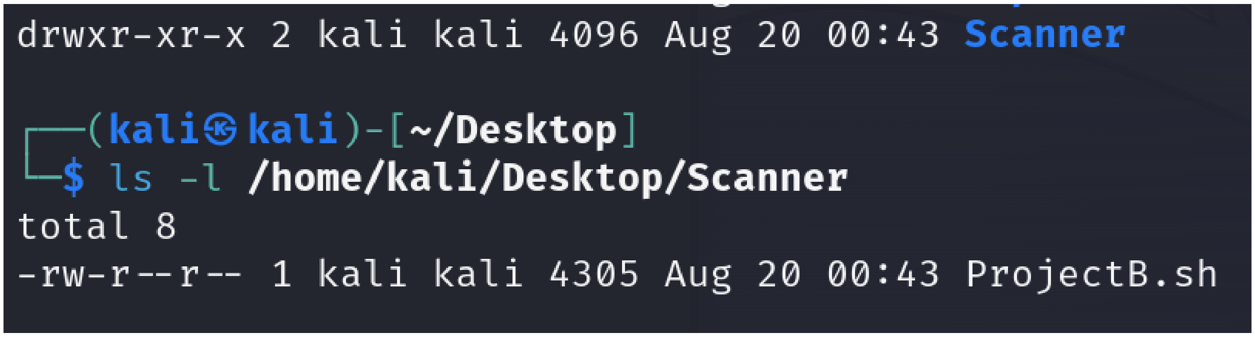
- by writing this function i gave the user the option to control the user , ip and password , in addition it will create a directory in the dedicated server where the first script will send the second script that will run in the server.



```
function SSHConnect()
{

    sleep 1
    sshpass -p "$PASSWORD" ssh -o stricthostkeychecking=no  $user@$usrip  'cd /home/'$user'/Desktop ; mkdir /home/'$user'/Desktop/Scanner
    sshpass -p "$PASSWORD" scp -o stricthostkeychecking=no /home/$EXILE/Desktop/ProjectB.sh $user@$usrip:/home/$user/Desktop/Scanner
    sshpass -p "$PASSWORD" ssh -o stricthostkeychecking=no  $user@$usrip 'cd /home/'$user'/Desktop/Scanner ; bash /home/'$user'/Desktop/S
}
SSHConnect
```

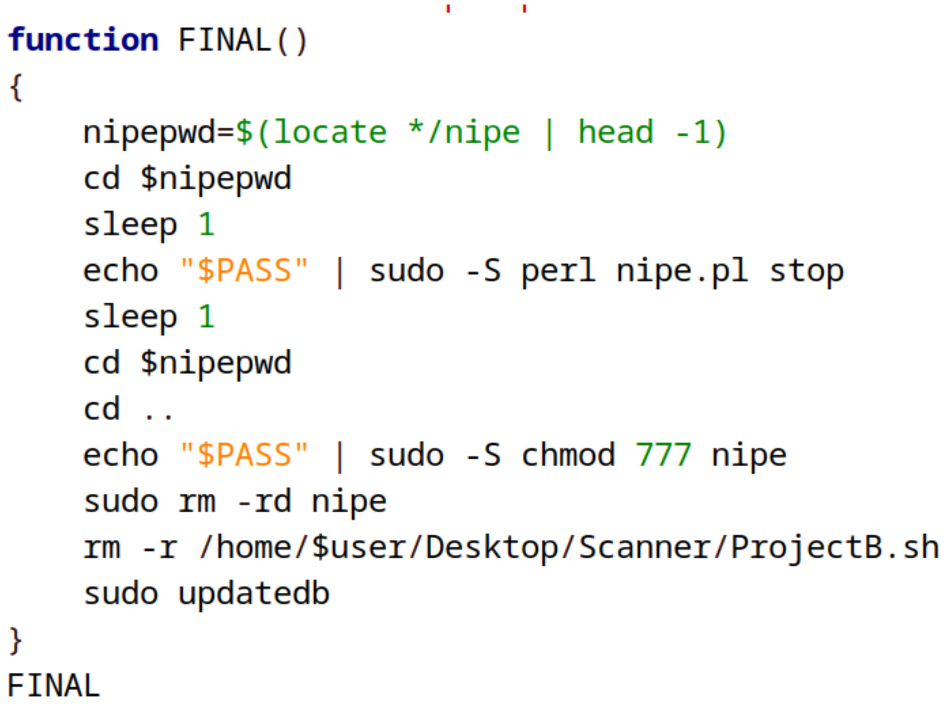


```
        echo "[!] please insert the server ip u want to enter"

        read usrip


  echo "[!] SSH Username :"
        read user

  echo "[!] SSH Password :  "
        read -s PASSWORD
```



```
drwxr-xr-x 2 kali kali 4096 Aug 20 00:43 Scanner

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l /home/kali/Desktop/Scanner
total 8
-rw-r--r-- 1 kali kali 4305 Aug 20 00:43 ProjectB.sh
```

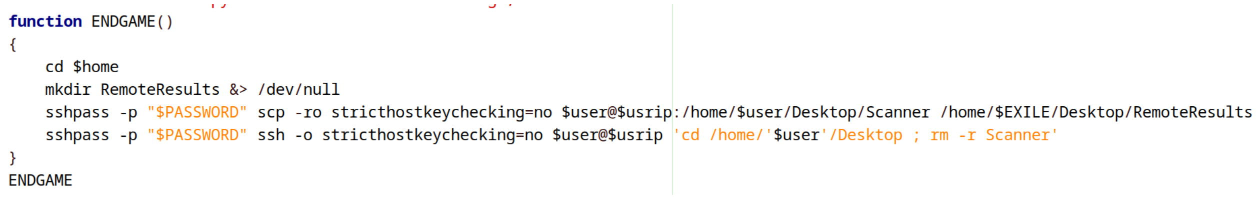
#FINAL
- by using this function in second script , we stop the nipe service , we change to permissions of the nipe folder so we will be able to delete it from the desktop we downloaded , also will delete the script we transfered



```
function FINAL()
{
    nipepwd=$(locate */nipe | head -1)
    cd $nipepwd
    sleep 1
    echo "$PASS" | sudo -S perl nipe.pl stop
    sleep 1
    cd $nipepwd
    cd ..
    echo "$PASS" | sudo -S chmod 777 nipe
    sudo rm -rd nipe
    rm -r /home/$user/Desktop/Scanner/ProjectB.sh
    sudo updatedb
}
FINAL
```

#ENDGAME

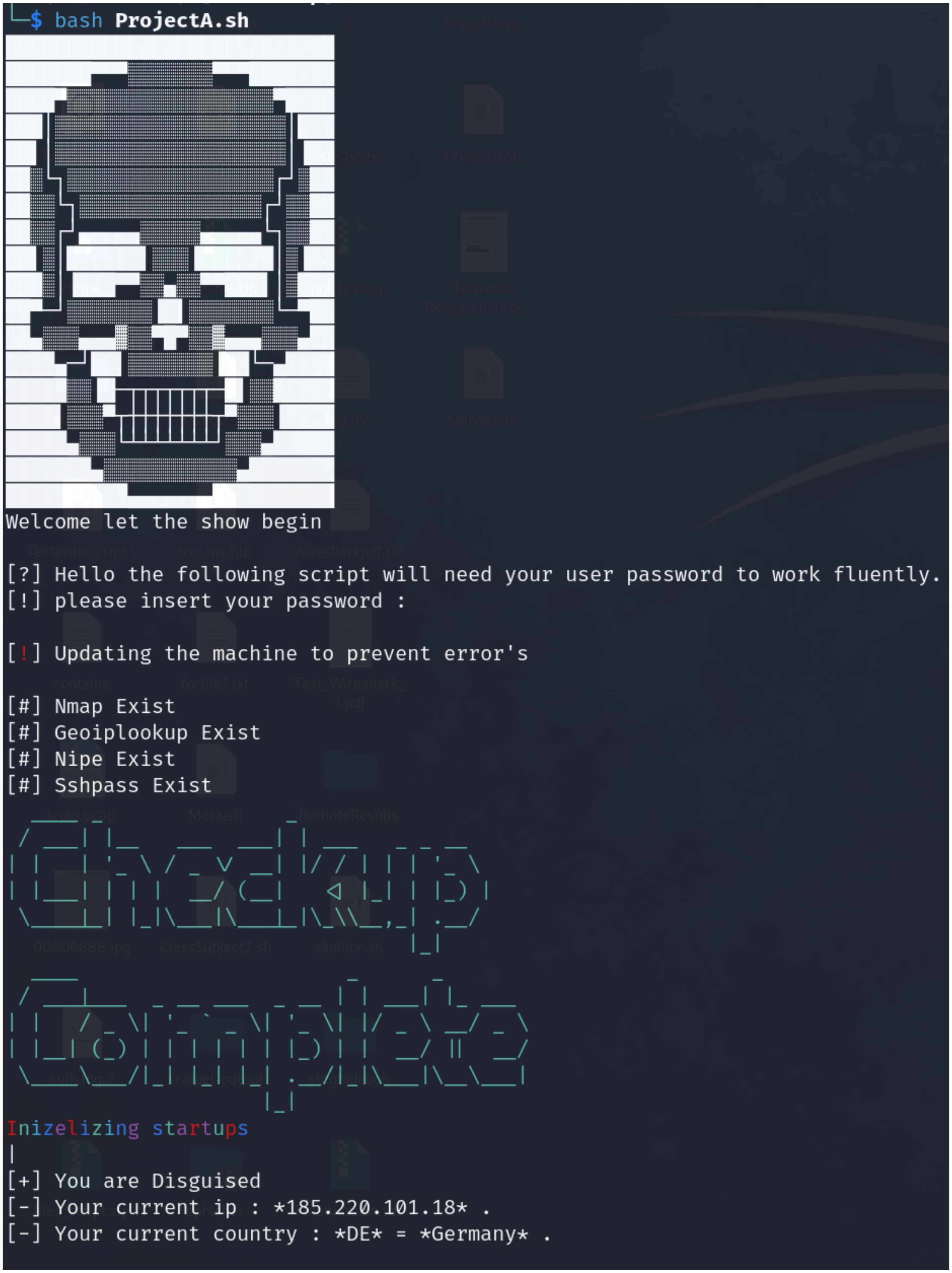
- By writing this function we create directory in our local kali and grab the Scanned files from nmap [grepable xml and flat] , and then we delete log folder from the server.



```
function ENDGAME()
{
    cd $home
    mkdir RemoteResults &> /dev/null
    sshpass -p "$PASSWORD" scp -ro stricthostkeychecking=no $user@$usrip:/home/$user/Desktop/Scanner /home/$EXILE/Desktop/RemoteResults
    sshpass -p "$PASSWORD" ssh -o stricthostkeychecking=no $user@$usrip 'cd /home/'$user'/Desktop ; rm -r Scanner'
}
ENDGAME
```

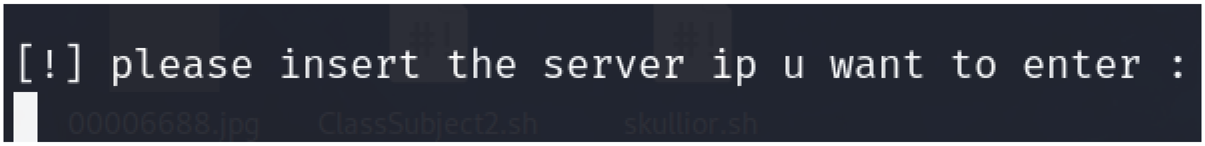
#Proof in 1 go that it works :

First script ~



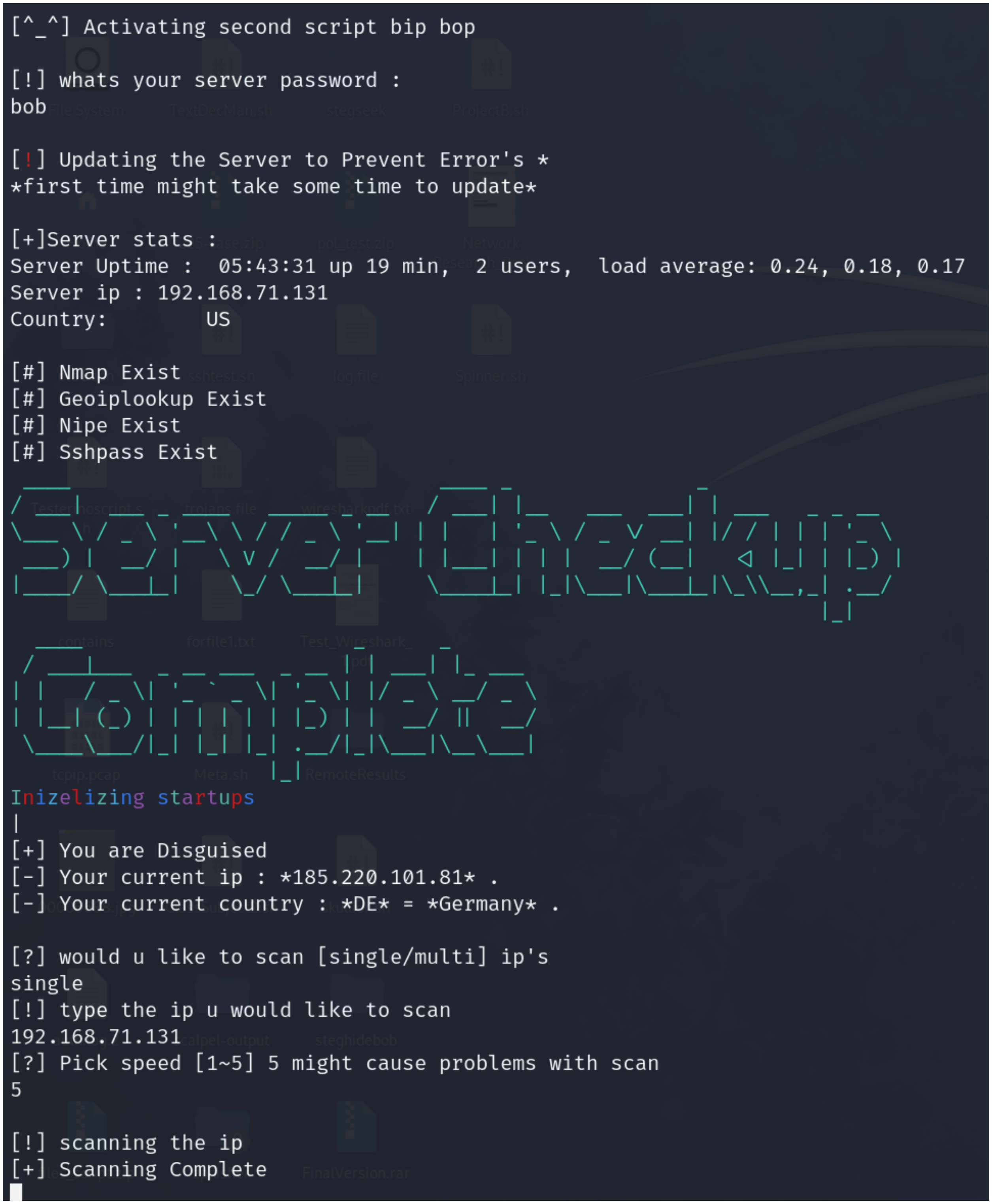
```
└─$ bash ProjectA.sh
```

```
Welcome let the show begin

[?] Hello the following script will need your user password to work fluently.
[!] please insert your password :

[!] Updating the machine to prevent error's

[#] Nmap Exist
[#] Geoiplookup Exist
[#] Nipe Exist
[#] Sshpass Exist
  ____ _               _
 / ___| |__   ___  ___| | ___   _ _ __
| |   | '_ \ / _ \/ __| |/ / | | | '_ \
| |___| | | |  __/ (__|   <| |_| | |_) |
 \____|_| |_|\___|\___|_|\_\\__,_| .__/
                                 |_|
  ____                      _      _
 / ___|___  _ __ ___  _ __ | | ___| |_ ___
| |   / _ \| '_ ` _ \| '_ \| |/ _ \ __/ _ \
| |__| (_) | | | | | | |_) | |  __/ ||  __/
 \____\___/|_| |_| |_| .__/|_|\___|\__\___|
                     |_|
Inizelizing startups
|
[+] You are Disguised
[-] Your current ip : *185.220.101.18* .
[-] Your current country : *DE* = *Germany* .
```



```
[!] please insert the server ip u want to enter :
```

- Second Script



```
[^_^] Activating second script bip bop

[!] whats your server password :
bob

[!] Updating the Server to Prevent Error's *
*first time might take some time to update*

[+]Server stats :
Server Uptime :  05:43:31 up 19 min,  2 users,  load average: 0.24, 0.18, 0.17
Server ip : 192.168.71.131
Country:        US

[#] Nmap Exist
[#] Geoiplookup Exist
[#] Nipe Exist
[#] Sshpass Exist
 ____                              ____ _               _
/ ___|  ___ _ ____   _____ _ __   / ___| |__   ___  ___| | ___   _ _ __
\___ \ / _ \ '__\ \ / / _ \ '__| | |   | '_ \ / _ \/ __| |/ / | | | '_ \
 ___) |  __/ |   \ V /  __/ |    | |___| | | |  __/ (__|   <| |_| | |_) |
|____/ \___|_|    \_/ \___|_|     \____|_| |_|\___|\___|_|\_\\__,_| .__/
                                                                  |_|

  ____                      _      _
 / ___|___  _ __ ___  _ __ | | ___| |_ ___
| |   / _ \| '_ ` _ \| '_ \| |/ _ \ __/ _ \
| |__| (_) | | | | | | |_) | |  __/ ||  __/
 \____\___/|_| |_| |_| .__/|_|\___|\__\___|
                     |_|
Inizelizing startups
|
[+] You are Disguised
[-] Your current ip : *185.220.101.81* .
[-] Your current country : *DE* = *Germany* .

[?] would u like to scan [single/multi] ip's
single
[!] type the ip u would like to scan
192.168.71.131
[?] Pick speed [1~5] 5 might cause problems with scan
5

[!] scanning the ip
[+] Scanning Complete
```