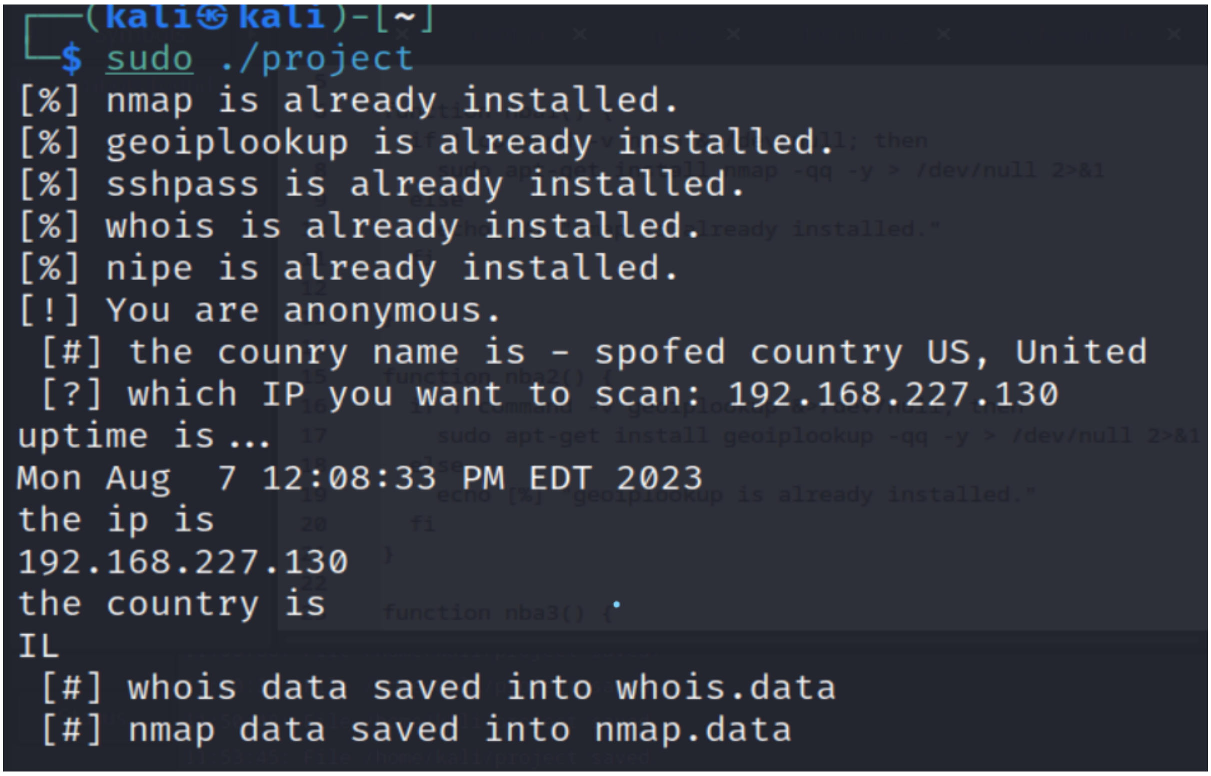
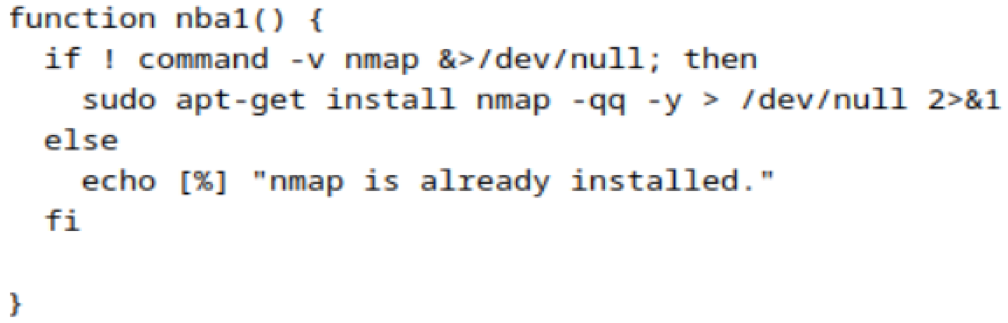
# project in network research

note: when you run the script pleas do it with sudo … ( sudo ./project)
note2: copy the script from the file and then paste Do not drag the file because after the script will not work

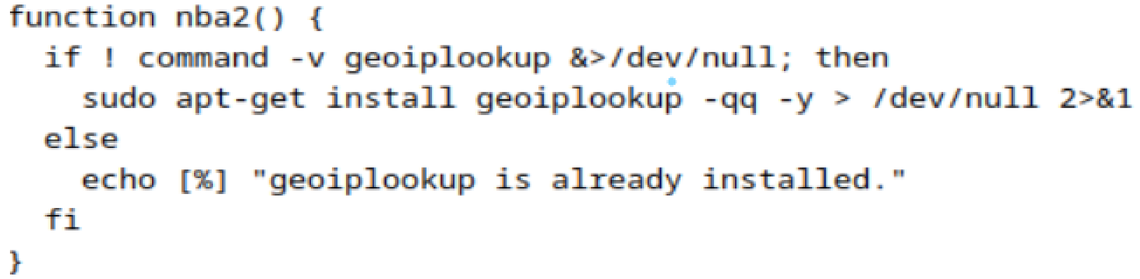


```
┌──(kali㉿kali)-[~]
└─$ sudo ./project
[%] nmap is already installed.
[%] geoiplookup is already installed.
[%] sshpass is already installed.
[%] whois is already installed.
[%] nipe is already installed.
[!] You are anonymous.
 [#] the counry name is - spofed country US, United
 [?] which IP you want to scan: 192.168.227.130
uptime is ...
Mon Aug  7 12:08:33 PM EDT 2023
the ip is
192.168.227.130
the country is
IL
 [#] whois data saved into whois.data
 [#] nmap data saved into nmap.data
```

this is how the script look like after he run

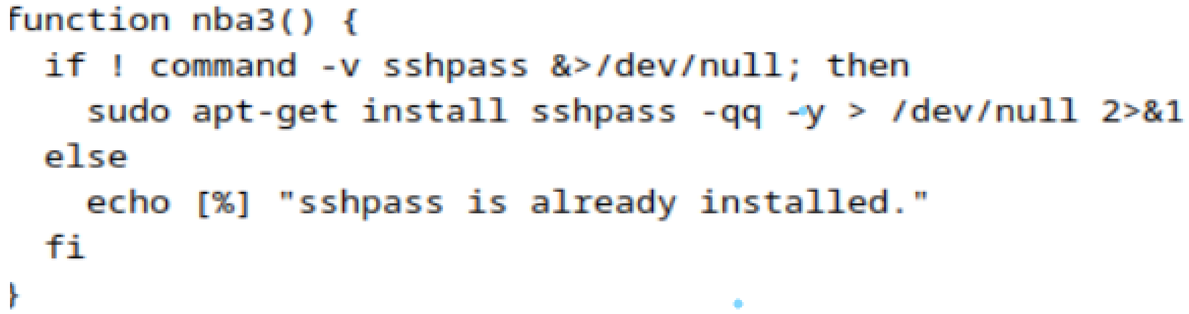


```
function nba1() {
  if ! command -v nmap &>/dev/null; then
    sudo apt-get install nmap -qq -y > /dev/null 2>&1
  else
    echo [%] "nmap is already installed."
  fi

}
```

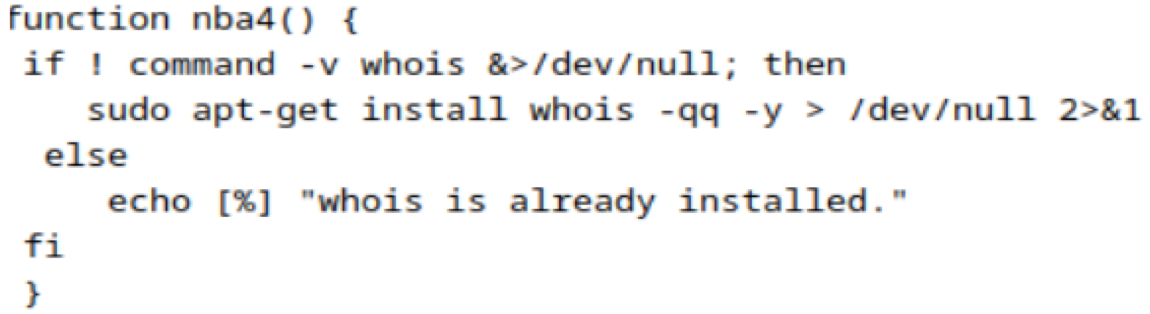


```
function nba2() {
  if ! command -v geoiplookup &>/dev/null; then
    sudo apt-get install geoiplookup -qq -y > /dev/null 2>&1
  else
    echo [%] "geoiplookup is already installed."
  fi
}
```

in the start i make shure that all the tool that i need would download

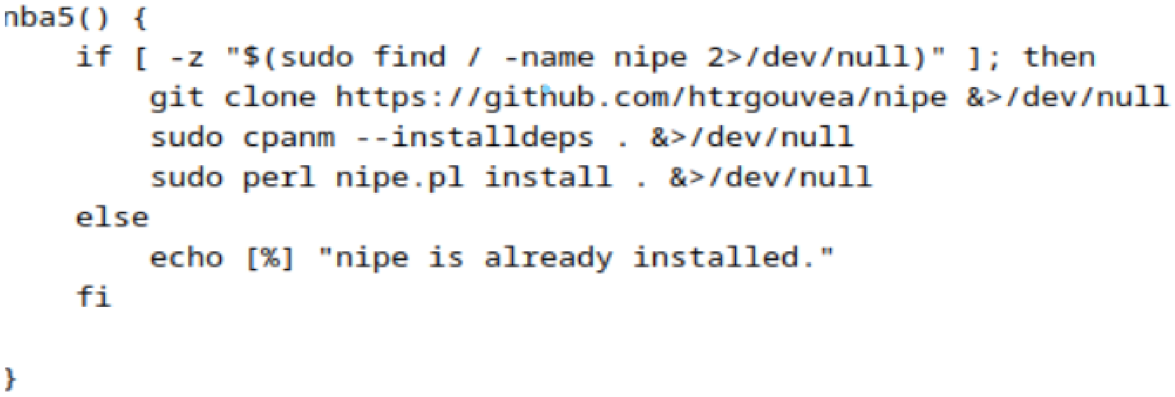


```
function nba3() {
  if ! command -v sshpass &>/dev/null; then
    sudo apt-get install sshpass -qq -y > /dev/null 2>&1
  else
    echo [%] "sshpass is already installed."
  fi
}
```



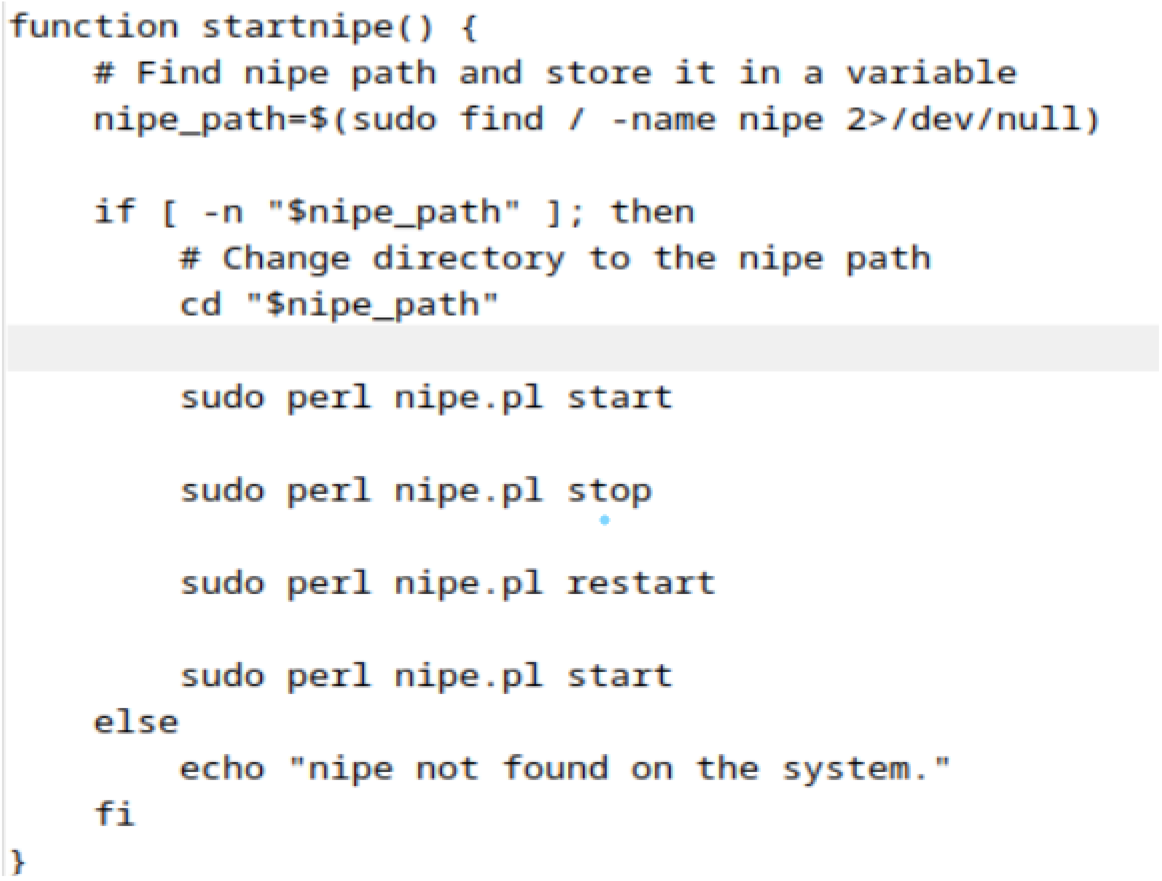
```
function nba4() {
 if ! command -v whois &>/dev/null; then
    sudo apt-get install whois -qq -y > /dev/null 2>&1
  else
     echo [%] "whois is already installed."
 fi
 }
```

all nba functions is use the same command for search and download



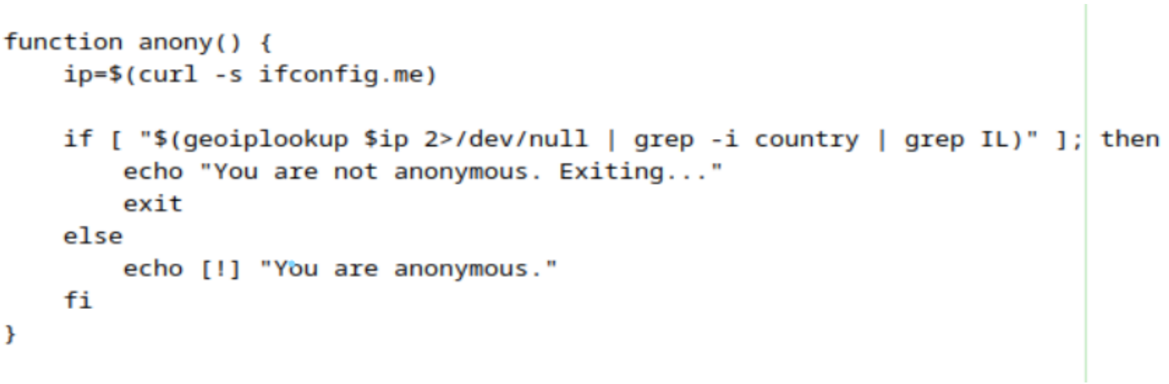
```
nba5() {
    if [ -z "$(sudo find / -name nipe 2>/dev/null)" ]; then
        git clone https://github.com/htrgouvea/nipe &>/dev/null
        sudo cpanm --installdeps . &>/dev/null
        sudo perl nipe.pl install . &>/dev/null
    else
        echo [%] "nipe is already installed."
    fi

}
```

nipe search and download is different  because nipe is a directory so i was needed to use command find but also the download is different so that function is more difficult



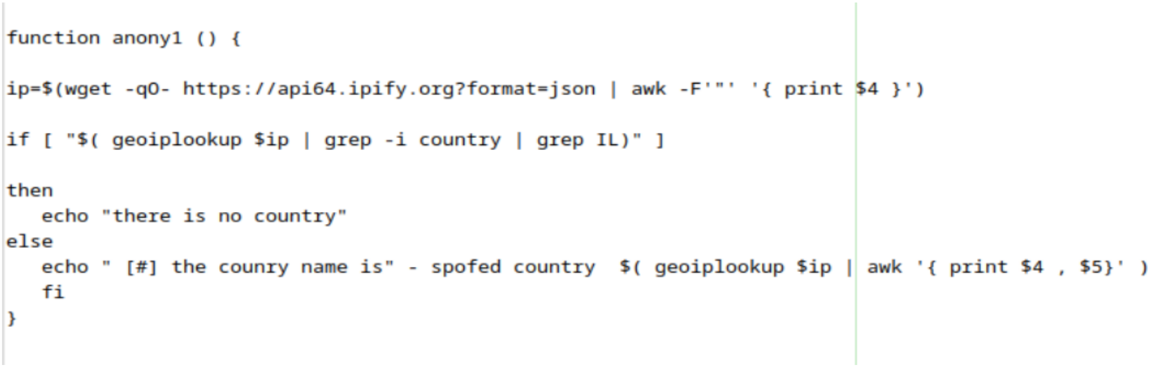
```
function startnipe() {
    # Find nipe path and store it in a variable
    nipe_path=$(sudo find / -name nipe 2>/dev/null)

    if [ -n "$nipe_path" ]; then
        # Change directory to the nipe path
        cd "$nipe_path"

        sudo perl nipe.pl start

        sudo perl nipe.pl stop

        sudo perl nipe.pl restart

        sudo perl nipe.pl start
    else
        echo "nipe not found on the system."
    fi
}
```

her i was make sure that after download nipe he would start to run



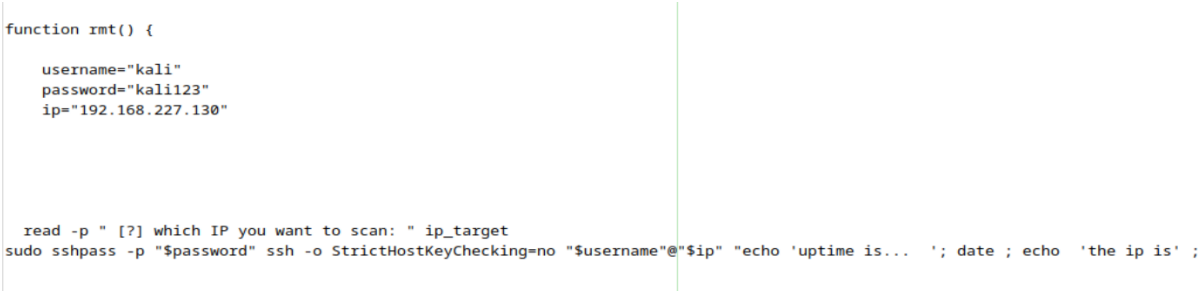
```
function anony() {
    ip=$(curl -s ifconfig.me)

    if [ "$(geoiplookup $ip 2>/dev/null | grep -i country | grep IL)" ]; then
        echo "You are not anonymous. Exiting..."
        exit
    else
        echo [!] "You are anonymous."
    fi
}
```

that function check if the function before her do her jobe and start nipe



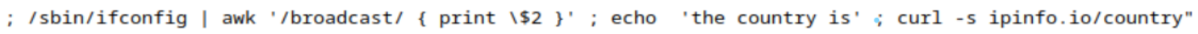
```
function anony1 () {

ip=$(wget -qO- https://api64.ipify.org?format=json | awk -F'"' '{ print $4 }')

if [ "$( geoiplookup $ip | grep -i country | grep IL)" ]

then
   echo "there is no country"
else
   echo " [#] the counry name is" - spofed country  $( geoiplookup $ip | awk '{ print $4 , $5}' )
   fi
}
```

her i check for the country for the ip i get from  nipe

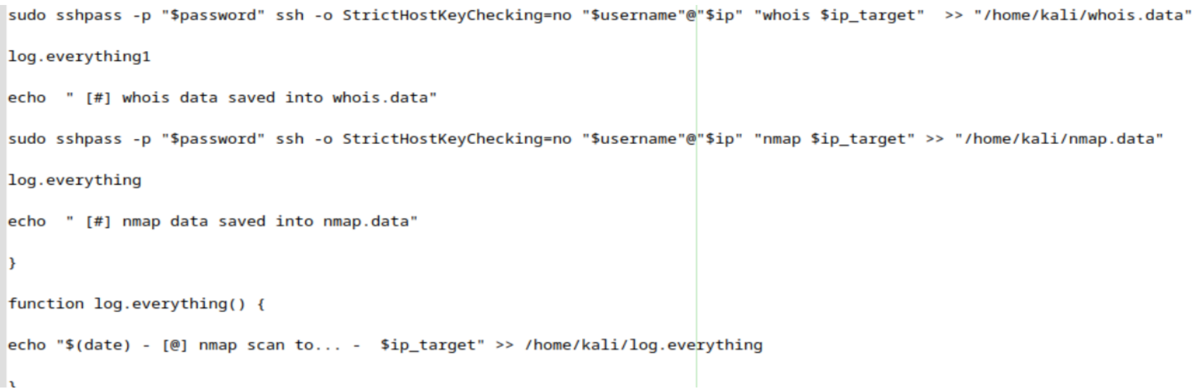


```
function rmt() {

    username="kali"
    password="kali123"
    ip="192.168.227.130"




  read -p " [?] which IP you want to scan: " ip_target
sudo sshpass -p "$password" ssh -o StrictHostKeyChecking=no "$username"@"$ip" "echo 'uptime is...  '; date ; echo  'the ip is' ;
```

her i connect to the remote server and the read command ask me to wich ip i want to scan but also check for uptime,country,ip

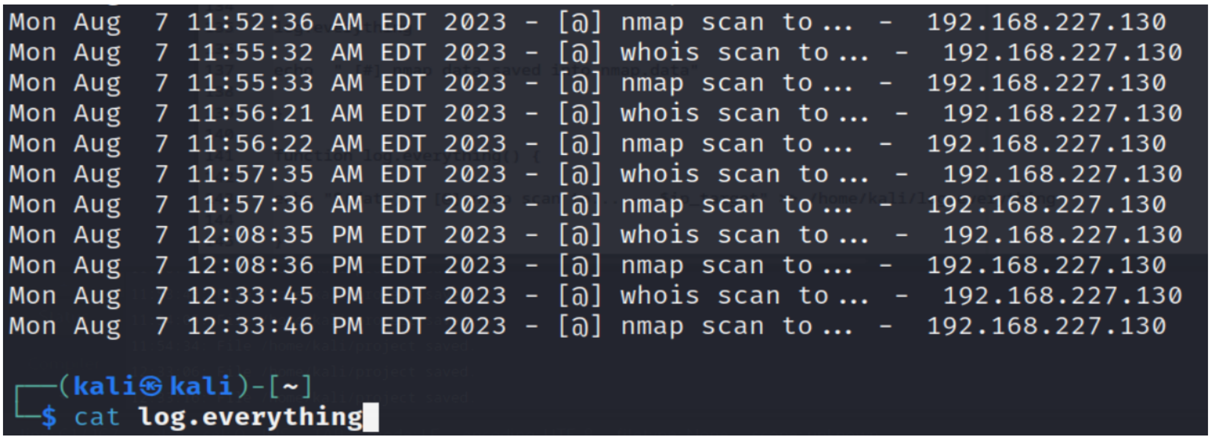


```
; /sbin/ifconfig | awk '/broadcast/ { print \$2 }' ; echo  'the country is' ; curl -s ipinfo.io/country"
```



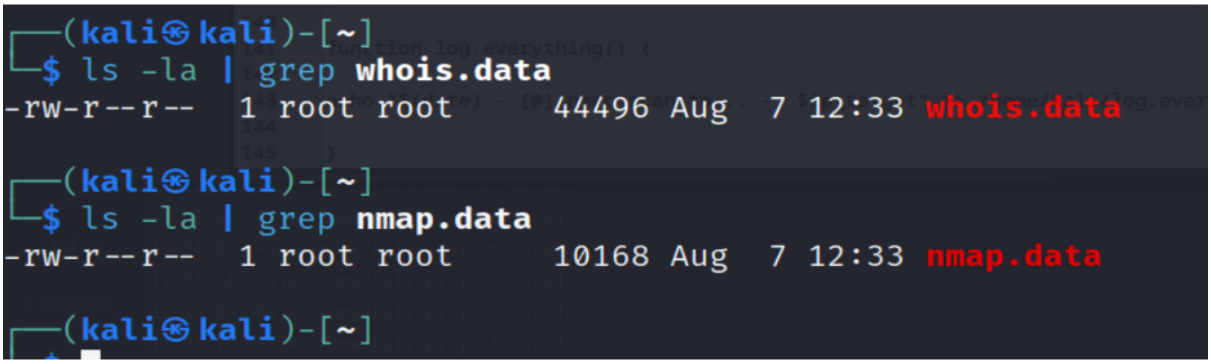
```
sudo sshpass -p "$password" ssh -o StrictHostKeyChecking=no "$username"@"$ip" "whois $ip_target"  >> "/home/kali/whois.data"

log.everything1

echo  " [#] whois data saved into whois.data"

sudo sshpass -p "$password" ssh -o StrictHostKeyChecking=no "$username"@"$ip" "nmap $ip_target" >> "/home/kali/nmap.data"

log.everything

echo  " [#] nmap data saved into nmap.data"

}

function log.everything() {

echo "$(date) - [@] nmap scan to... -  $ip_target" >> /home/kali/log.everything

}
```

her i do whois and nmap to the given address and saved all into the files and in the and of the two lines i call the logs



```
Mon Aug  7 11:52:36 AM EDT 2023 - [@] nmap scan to... -  192.168.227.130
Mon Aug  7 11:55:32 AM EDT 2023 - [@] whois scan to... -  192.168.227.130
Mon Aug  7 11:55:33 AM EDT 2023 - [@] nmap scan to... -  192.168.227.130
Mon Aug  7 11:56:21 AM EDT 2023 - [@] whois scan to... -  192.168.227.130
Mon Aug  7 11:56:22 AM EDT 2023 - [@] nmap scan to... -  192.168.227.130
Mon Aug  7 11:57:35 AM EDT 2023 - [@] whois scan to... -  192.168.227.130
Mon Aug  7 11:57:36 AM EDT 2023 - [@] nmap scan to... -  192.168.227.130
Mon Aug  7 12:08:35 PM EDT 2023 - [@] whois scan to... -  192.168.227.130
Mon Aug  7 12:08:36 PM EDT 2023 - [@] nmap scan to... -  192.168.227.130
Mon Aug  7 12:33:45 PM EDT 2023 - [@] whois scan to... -  192.168.227.130
Mon Aug  7 12:33:46 PM EDT 2023 - [@] nmap scan to... -  192.168.227.130

┌──(kali㉿kali)-[~]
└─$ cat log.everything
```

this is how the log locks like



```
┌──(kali㉿kali)-[~]
└─$ ls -la | grep whois.data
-rw-r--r--   1 root root     44496 Aug  7 12:33 whois.data

┌──(kali㉿kali)-[~]
└─$ ls -la | grep nmap.data
-rw-r--r--   1 root root     10168 Aug  7 12:33 nmap.data

┌──(kali㉿kali)-[~]
```

and the files