Objective

CREATE A SCRIPT THAT COMMUNICATES WITH A REMOTE SERVER AND EXECUTES TASKS ANONYMOUSLY.

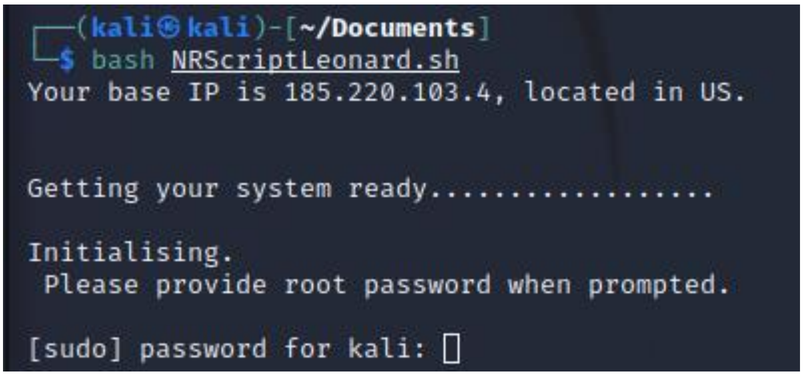
1. Installing applications

Install relevant applications on the local computer.

Tested on a fresh Kali VM. The script has also been tested with Nipe already running, as well as on a system that was already initialized with the necessary applications. All worked.

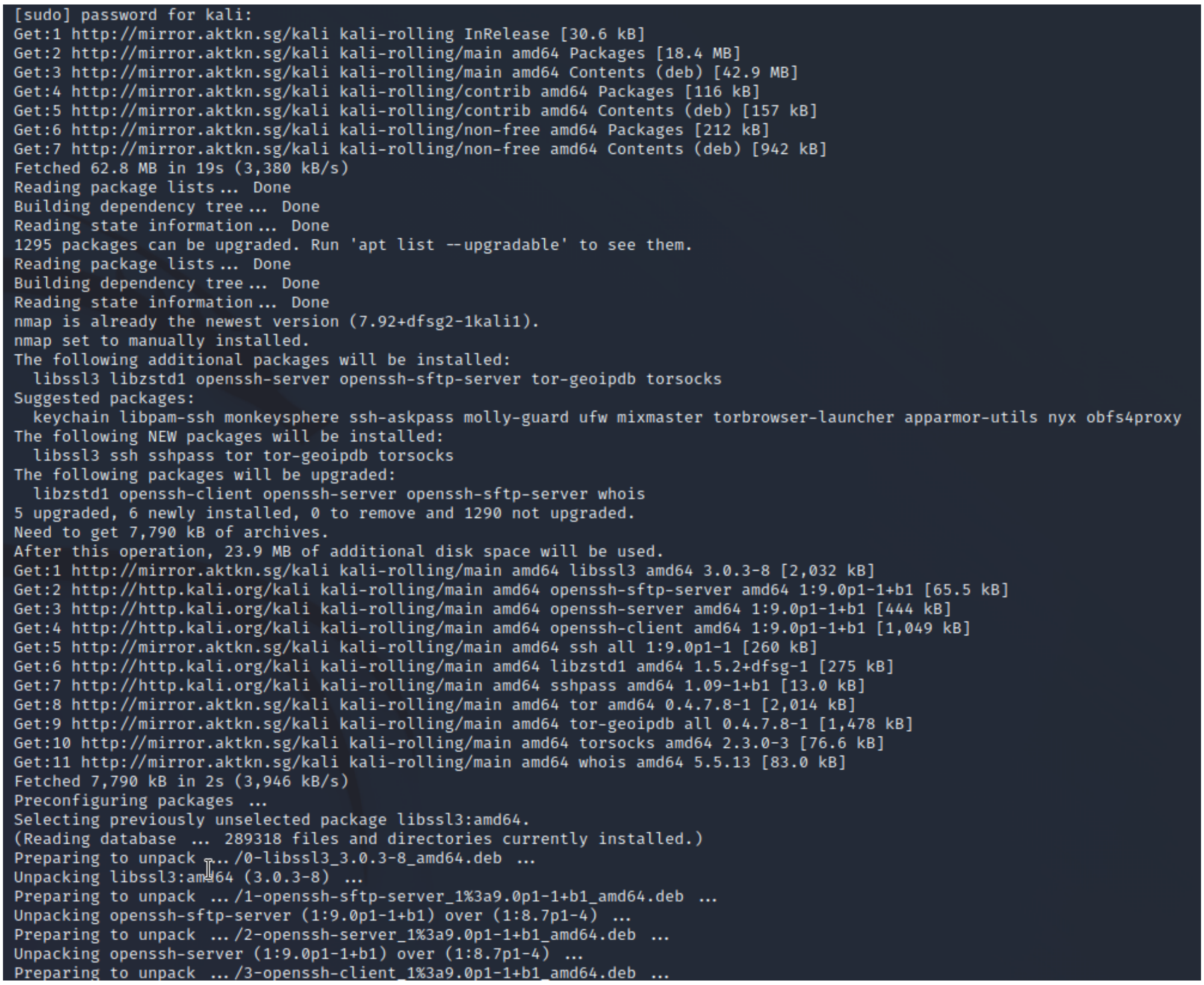
Comments in the script explain what the various segments are doing.

The script should be run as normal user and will prompt for root password once. This is to execute all the commands that require superuser permissions, apt update and apt install and the nipe scripts. If the script is run with sudo, the nipe installation will occur in the /root directory and will not work as expected.



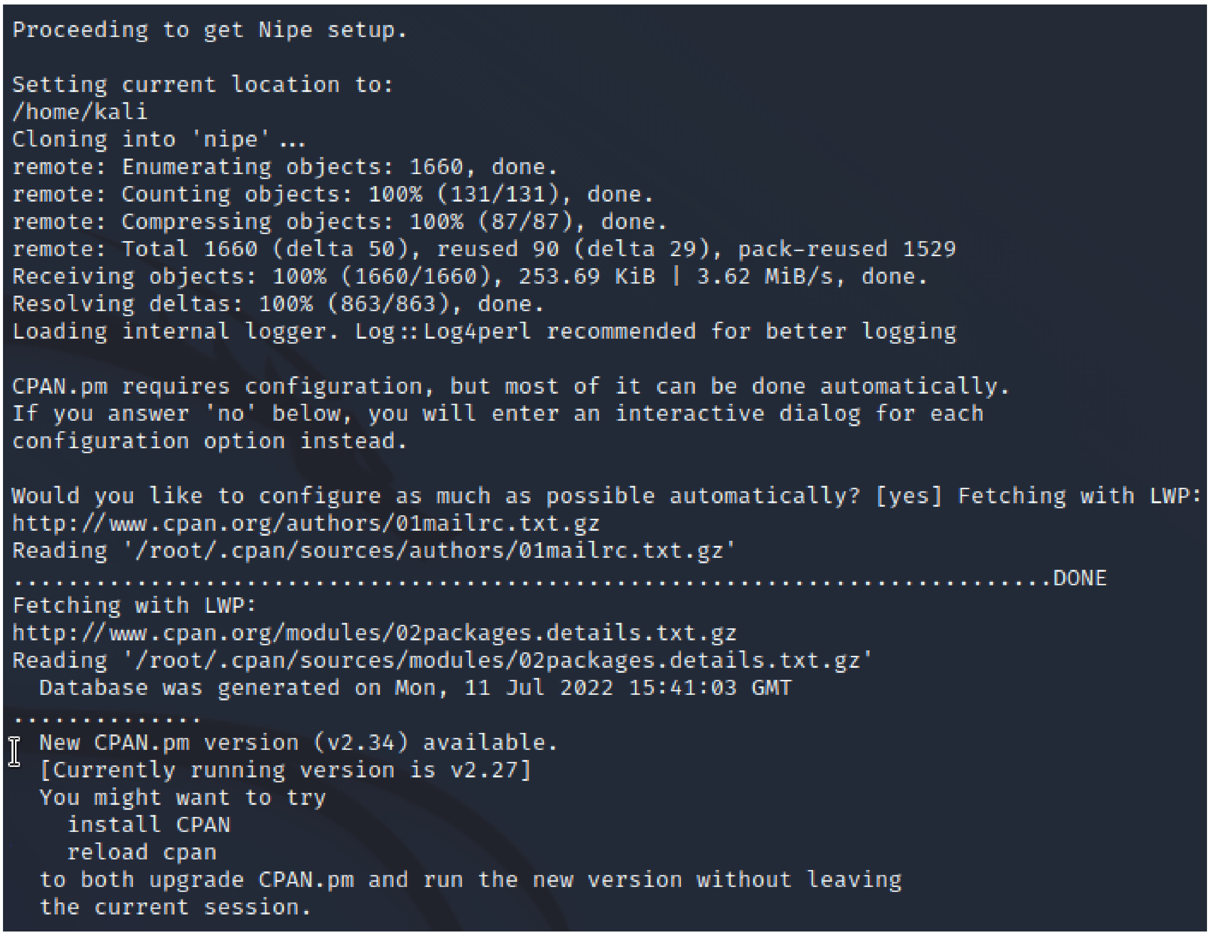
```
┌──(kali㉿kali)-[~/Documents]
└─$ bash NRScriptLeonard.sh
Your base IP is 185.220.103.4, located in US.


Getting your system ready.................

Initialising.
 Please provide root password when prompted.

[sudo] password for kali: ▯
```

The script will run all the necessary repository updates and install required applications, just to be safe it installs **sshpass nmap ssh whois openssh-client tor**



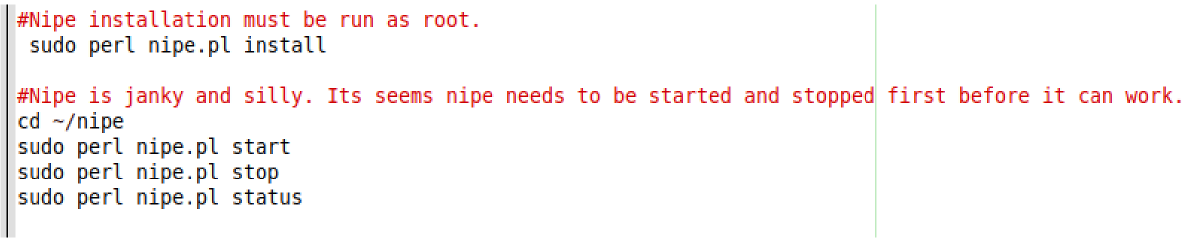
```
[sudo] password for kali:
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [30.6 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [18.4 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [42.9 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb) [157 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [212 kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb) [942 kB]
Fetched 62.8 MB in 19s (3,380 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1295 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.92+dfsg2-1kali1).
nmap set to manually installed.
The following additional packages will be installed:
  libssl3 libzstd1 openssh-server openssh-sftp-server tor-geoipdb torsocks
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw mixmaster torbrowser-launcher apparmor-utils nyx obfs4proxy
The following NEW packages will be installed:
  libssl3 ssh sshpass tor tor-geoipdb torsocks
The following packages will be upgraded:
  libzstd1 openssh-client openssh-server openssh-sftp-server whois
5 upgraded, 6 newly installed, 0 to remove and 1290 not upgraded.
Need to get 7,790 kB of archives.
After this operation, 23.9 MB of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libssl3 amd64 3.0.3-8 [2,032 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.0p1-1+b1 [65.5 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 openssh-server amd64 1:9.0p1-1+b1 [444 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 openssh-client amd64 1:9.0p1-1+b1 [1,049 kB]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/main amd64 ssh all 1:9.0p1-1 [260 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libzstd1 amd64 1.5.2+dfsg-1 [275 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 sshpass amd64 1.09-1+b1 [13.0 kB]
Get:8 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tor amd64 0.4.7.8-1 [2,014 kB]
Get:9 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tor-geoipdb all 0.4.7.8-1 [1,478 kB]
Get:10 http://mirror.aktkn.sg/kali kali-rolling/main amd64 torsocks amd64 2.3.0-3 [76.6 kB]
Get:11 http://mirror.aktkn.sg/kali kali-rolling/main amd64 whois amd64 5.5.13 [83.0 kB]
Fetched 7,790 kB in 2s (3,946 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libssl3:amd64.
(Reading database ... 289318 files and directories currently installed.)
Preparing to unpack .../0-libssl3_3.0.3-8_amd64.deb ...
Unpacking libssl3:amd64 (3.0.3-8) ...
Preparing to unpack .../1-openssh-sftp-server_1%3a9.0p1-1+b1_amd64.deb ...
Unpacking openssh-sftp-server (1:9.0p1-1+b1) over (1:8.7p1-4) ...
Preparing to unpack .../2-openssh-server_1%3a9.0p1-1+b1_amd64.deb ...
Unpacking openssh-server (1:9.0p1-1+b1) over (1:8.7p1-4) ...
Preparing to unpack .../3-openssh-client_1%3a9.0p1-1+b1_amd64.deb ...
```

Get Nipe installed and setup. This includes changing the directory and installing Nipe with sudo privileges.

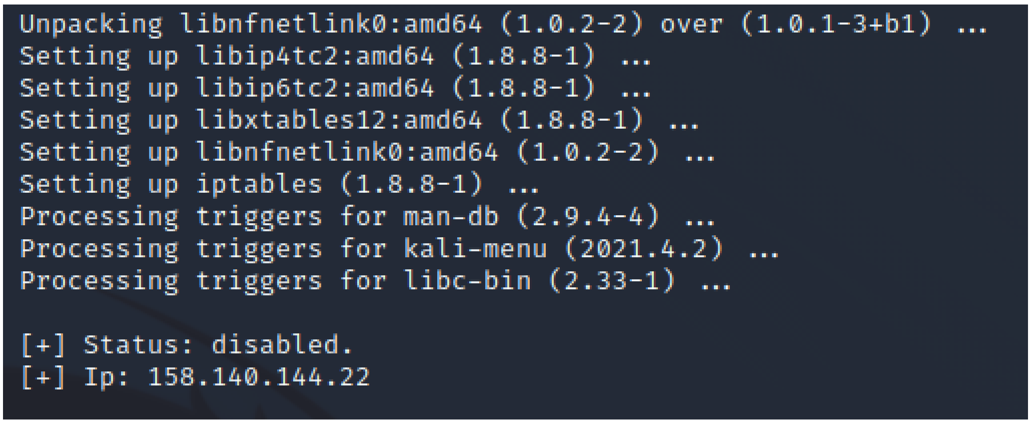


```
Proceeding to get Nipe setup.

Setting current location to:
/home/kali
Cloning into 'nipe'...
remote: Enumerating objects: 1660, done.
remote: Counting objects: 100% (131/131), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 1660 (delta 50), reused 90 (delta 29), pack-reused 1529
Receiving objects: 100% (1660/1660), 253.69 KiB | 3.62 MiB/s, done.
Resolving deltas: 100% (863/863), done.
Loading internal logger. Log::Log4perl recommended for better logging

CPAN.pm requires configuration, but most of it can be done automatically.
If you answer 'no' below, you will enter an interactive dialog for each
configuration option instead.

Would you like to configure as much as possible automatically? [yes] Fetching with LWP:
http://www.cpan.org/authors/01mailrc.txt.gz
Reading '/root/.cpan/sources/authors/01mailrc.txt.gz'
............................................................................DONE
Fetching with LWP:
http://www.cpan.org/modules/02packages.details.txt.gz
Reading '/root/.cpan/sources/modules/02packages.details.txt.gz'
  Database was generated on Mon, 11 Jul 2022 15:41:03 GMT
..............
  New CPAN.pm version (v2.34) available.
  [Currently running version is v2.27]
  You might want to try
    install CPAN
    reload cpan
  to both upgrade CPAN.pm and run the new version without leaving
  the current session.
```

I ran into some issues with Nipe failting to execute immediately after setup. To circumvent this nipe is started, stopped and status is viewed immediately after it is installed so that it will work properly when it is activated again later in the if statement.



```
#Nipe installation must be run as root.
 sudo perl nipe.pl install

#Nipe is janky and silly. Its seems nipe needs to be started and stopped first before it can work.
cd ~/nipe
sudo perl nipe.pl start
sudo perl nipe.pl stop
sudo perl nipe.pl status
```



```
Unpacking libnfnetlink0:amd64 (1.0.2-2) over (1.0.1-3+b1) ...
Setting up libip4tc2:amd64 (1.8.8-1) ...
Setting up libip6tc2:amd64 (1.8.8-1) ...
Setting up libxtables12:amd64 (1.8.8-1) ...
Setting up libnfnetlink0:amd64 (1.0.2-2) ...
Setting up iptables (1.8.8-1) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for libc-bin (2.33-1) ...

[+] Status: disabled.
[+] Ip: 158.140.144.22
```

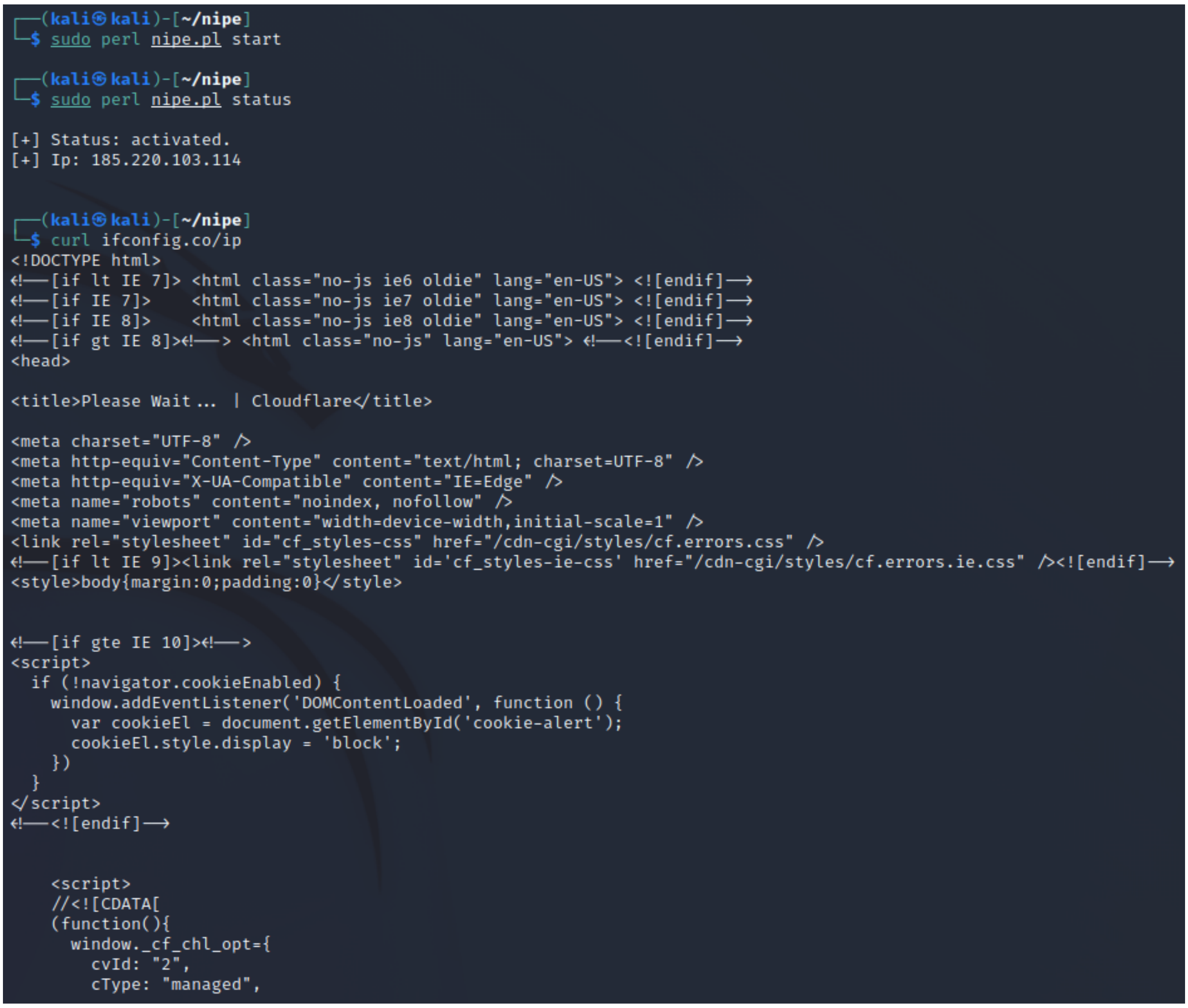
2. Check if the connection is anonymous

Check if the connection is from your origin country. If no, continue.

Available tools: curl, whois

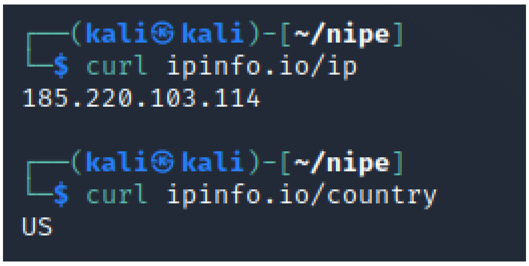
The script collects the IP and country before Nipe is installed and then again after Nipe has been started.

Originally I started with curl ifconfig.co/country but once nipe was active it would not return the correct info via command line. It turns out the better option / alternative was to curl ipinfo.io/ip and ipinfo.io/country



```
┌──(kali㉿kali)-[~/nipe]
└─$ sudo perl nipe.pl start

┌──(kali㉿kali)-[~/nipe]
└─$ sudo perl nipe.pl status

[+] Status: activated.
[+] Ip: 185.220.103.114


┌──(kali㉿kali)-[~/nipe]
└─$ curl ifconfig.co/ip
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>

<title>Please Wait... | Cloudflare</title>

<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" /><![endif]-->
<style>body{margin:0;padding:0}</style>


<!--[if gte IE 10]><!-->
<script>
  if (!navigator.cookieEnabled) {
    window.addEventListener('DOMContentLoaded', function () {
      var cookieEl = document.getElementById('cookie-alert');
      cookieEl.style.display = 'block';
    })
  }
</script>
<!--<![endif]-->


    <script>
    //<![CDATA[
    (function(){
      window._cf_chl_opt={
        cvId: "2",
        cType: "managed",
```

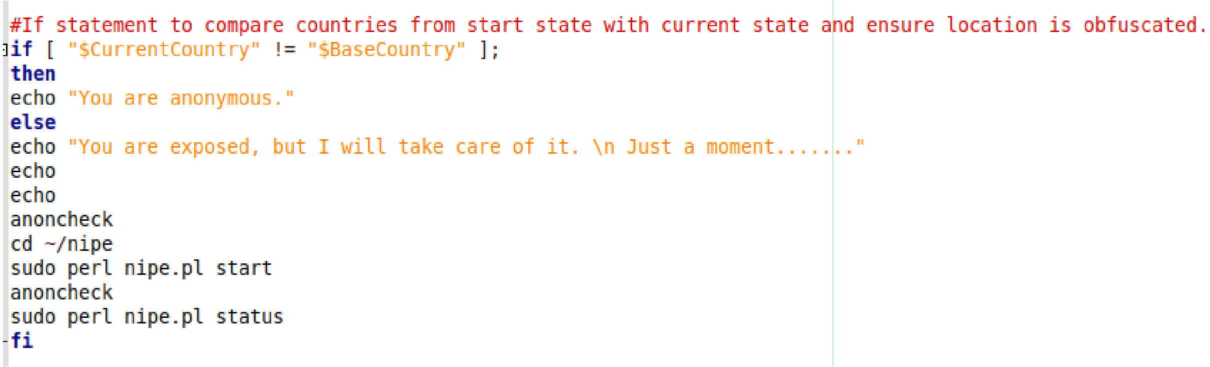
Trash output from ifconfig.co when nipe is active.



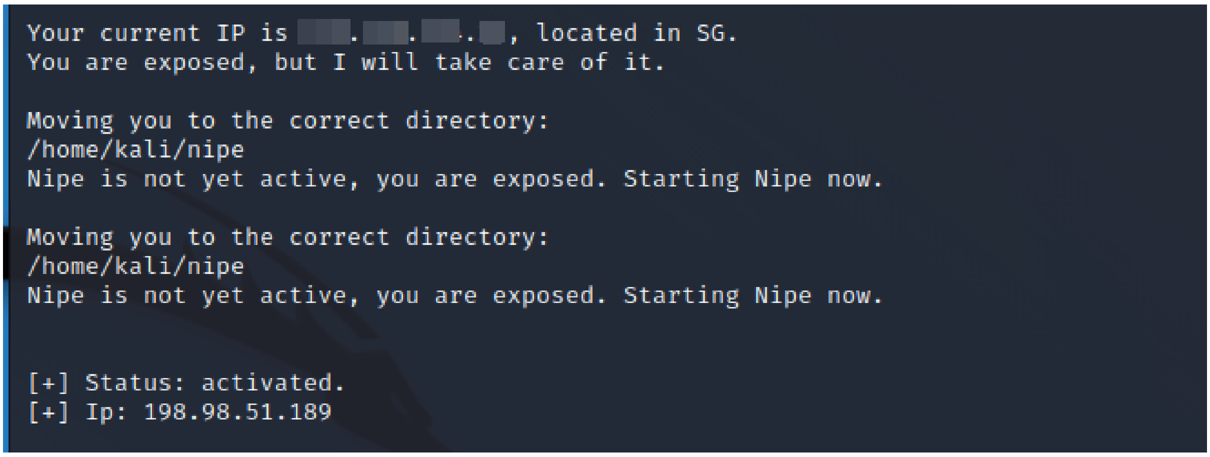
```
┌──(kali㉿kali)-[~/nipe]
└─$ curl ipinfo.io/ip
185.220.103.114

┌──(kali㉿kali)-[~/nipe]
└─$ curl ipinfo.io/country
US
```

Much more reliable output as can be seen above, from earlier testing. The required information is also pre-formatted. Ipinfo.io > ifconfig.co.

If exposed continue to check and run nipe until current country of origin of current IP is different from original country of origin.



```
#If statement to compare countries from start state with current state and ensure location is obfuscated.
if [ "$CurrentCountry" != "$BaseCountry" ];
then
echo "You are anonymous."
else
echo "You are exposed, but I will take care of it. \n Just a moment......."
echo
echo
anoncheck
cd ~/nipe
sudo perl nipe.pl start
anoncheck
sudo perl nipe.pl status
fi
```



```
Your current IP is [redacted], located in SG.
You are exposed, but I will take care of it.

Moving you to the correct directory:
/home/kali/nipe
Nipe is not yet active, you are exposed. Starting Nipe now.

Moving you to the correct directory:
/home/kali/nipe
Nipe is not yet active, you are exposed. Starting Nipe now.


[+] Status: activated.
[+] Ip: 198.98.51.189
```

3. Connect automatically to the VPS and execute tasks

Once the connection is anonymous, communicate via SSH and execute nmap scans and whois queries.

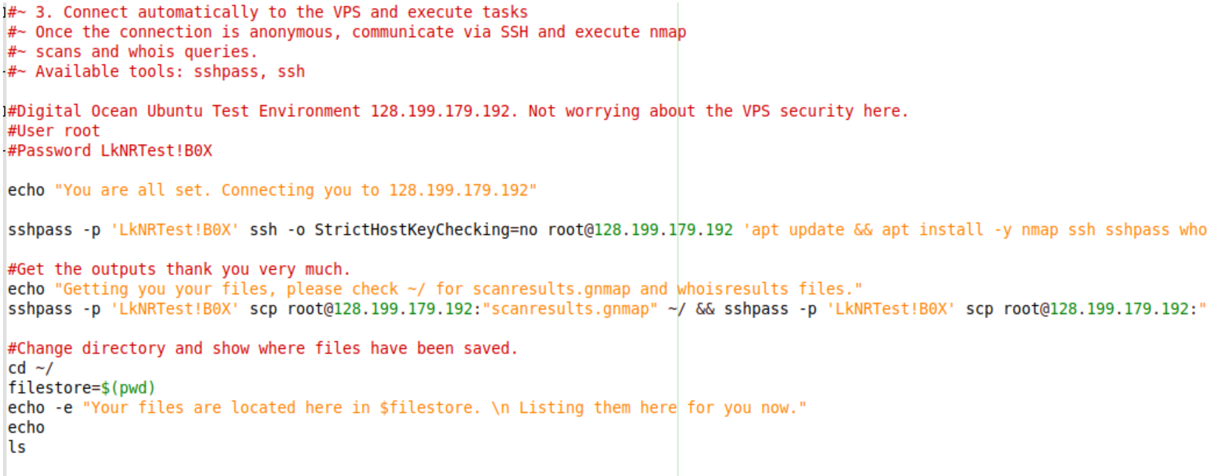
Available tools: sshpass, ssh

Using a Digital Ocean Ubuntu VPS with password and username inline for the script.

Server IP: 128.199.179.192

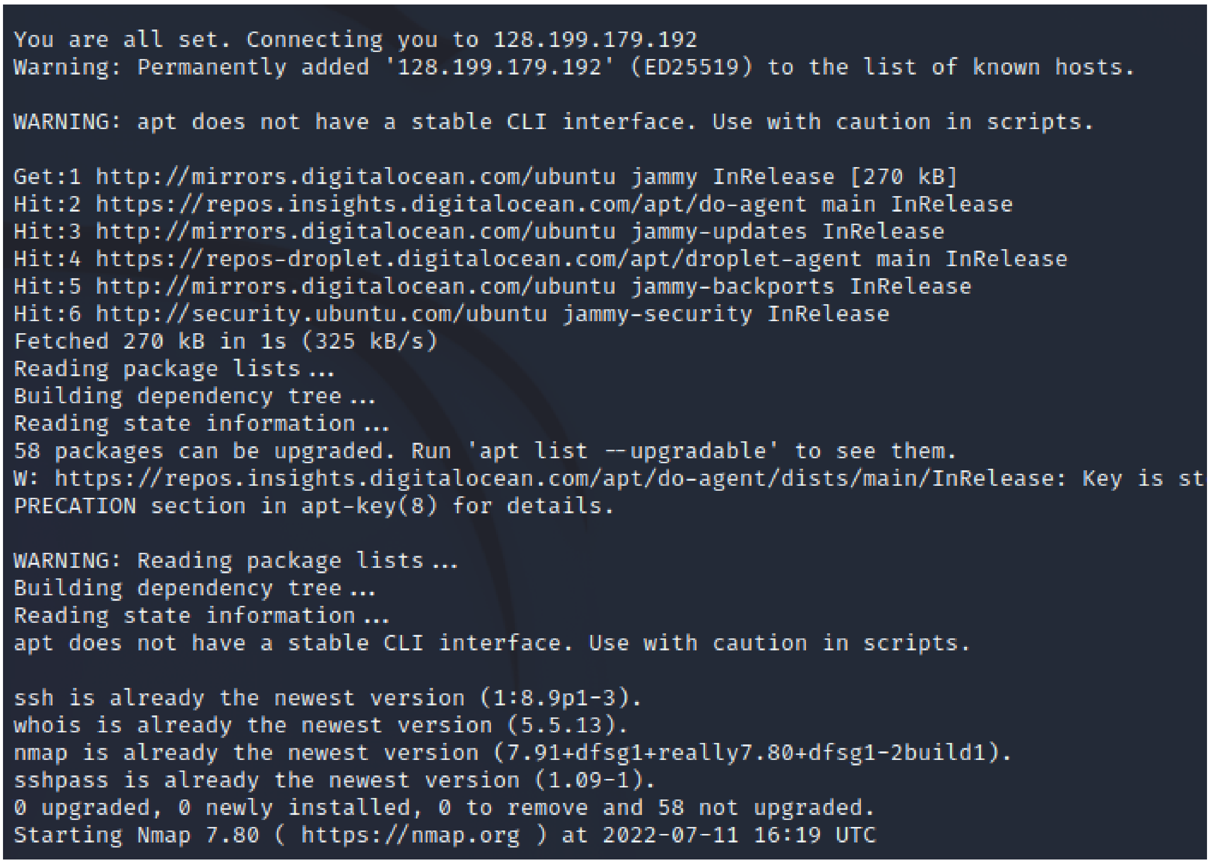
User:root

Password:LkNRTest!B0X



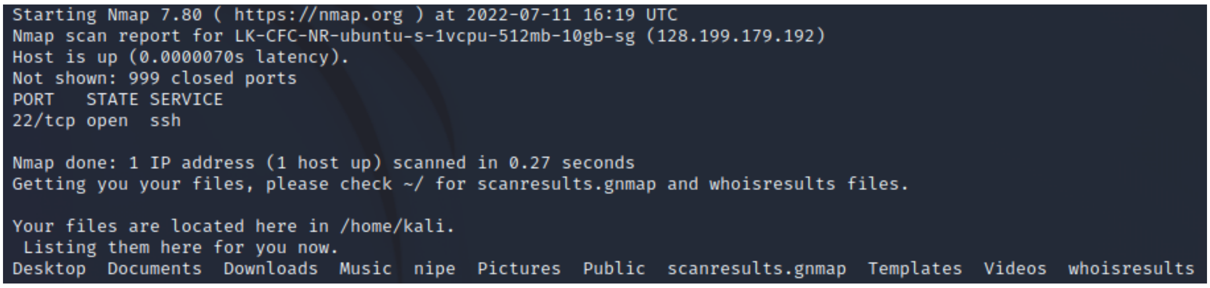
```
#~ 3. Connect automatically to the VPS and execute tasks
#~ Once the connection is anonymous, communicate via SSH and execute nmap
#~ scans and whois queries.
#~ Available tools: sshpass, ssh

#Digital Ocean Ubuntu Test Environment 128.199.179.192. Not worrying about the VPS security here.
#User root
#Password LkNRTest!B0X

echo "You are all set. Connecting you to 128.199.179.192"

sshpass -p 'LkNRTest!B0X' ssh -o StrictHostKeyChecking=no root@128.199.179.192 'apt update && apt install -y nmap ssh sshpass who

#Get the outputs thank you very much.
echo "Getting you your files, please check ~/ for scanresults.gnmap and whoisresults files."
sshpass -p 'LkNRTest!B0X' scp root@128.199.179.192:"scanresults.gnmap" ~/ && sshpass -p 'LkNRTest!B0X' scp root@128.199.179.192:"

#Change directory and show where files have been saved.
cd ~/
filestore=$(pwd)
echo -e "Your files are located here in $filestore. \n Listing them here for you now."
echo
ls
```

Automatically SSH in run an apt update and install the required programs **nmap ssh sshpass whois**



```
You are all set. Connecting you to 128.199.179.192
Warning: Permanently added '128.199.179.192' (ED25519) to the list of known hosts.

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Get:1 http://mirrors.digitalocean.com/ubuntu jammy InRelease [270 kB]
Hit:2 https://repos.insights.digitalocean.com/apt/do-agent main InRelease
Hit:3 http://mirrors.digitalocean.com/ubuntu jammy-updates InRelease
Hit:4 https://repos-droplet.digitalocean.com/apt/droplet-agent main InRelease
Hit:5 http://mirrors.digitalocean.com/ubuntu jammy-backports InRelease
Hit:6 http://security.ubuntu.com/ubuntu jammy-security InRelease
Fetched 270 kB in 1s (325 kB/s)
Reading package lists ...
Building dependency tree ...
Reading state information ...
58 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://repos.insights.digitalocean.com/apt/do-agent/dists/main/InRelease: Key is st
PRECATION section in apt-key(8) for details.

WARNING: Reading package lists ...
Building dependency tree ...
Reading state information ...
apt does not have a stable CLI interface. Use with caution in scripts.

ssh is already the newest version (1:8.9p1-3).
whois is already the newest version (5.5.13).
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2build1).
sshpass is already the newest version (1.09-1).
0 upgraded, 0 newly installed, 0 to remove and 58 not upgraded.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-11 16:19 UTC
```

The nmap scan and whois results are exported to files and then downloaded via scp to the local computer's home directory.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-11 16:19 UTC
Nmap scan report for LK-CFC-NR-ubuntu-s-1vcpu-512mb-10gb-sg (128.199.179.192)
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
Getting you your files, please check ~/ for scanresults.gnmap and whoisresults files.

Your files are located here in /home/kali.
 Listing them here for you now.
Desktop  Documents  Downloads  Music  nipe  Pictures  Public  scanresults.gnmap  Templates  Videos  whoisresults
```