

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

Network Research Project – Remote Control

Preamble

For this project, I will connect from virtual machine, kali to another virtual machine, ubuntu via ssh using the script I created and execute tasks (i.e. nmap scan and whois) anonymously. I will save the result of the each task and import back to my kali machine.

Snapshot of ubuntu machine info:

Ip address: 192.168.18.11

Username: tc

Password: tc

```
tion
System information as of Fri Jul 8 07:42:54 AM UTC 2022
System load: 0.02 Memory usage: 35% Processes: 244
Usage of /home: 0.0% of 250.00GB Swap usage: 0% Users logged in: 0
=> There were exceptions while processing one or more plugins. See
/var/log/landscape/sysinfo.log for more information.

0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Thu Jul 7 07:34:09 UTC 2022 from 192.168.18.8 on pts/0
tc@tc:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.18.11 netmask 255.255.255.0 broadcast 192.168.18.255
    inet6 2406:3003:2077:24c5:20c:29ff:fe57:c96c prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe57:c96c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:57:c9:6c txqueuelen 1000 (Ethernet)
    RX packets 220 bytes 52812 (52.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 220 bytes 20944 (20.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 96 bytes 7512 (7.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 96 bytes 7512 (7.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tc@tc:~$ _
```

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

Run the script "remotecontrol.sh".

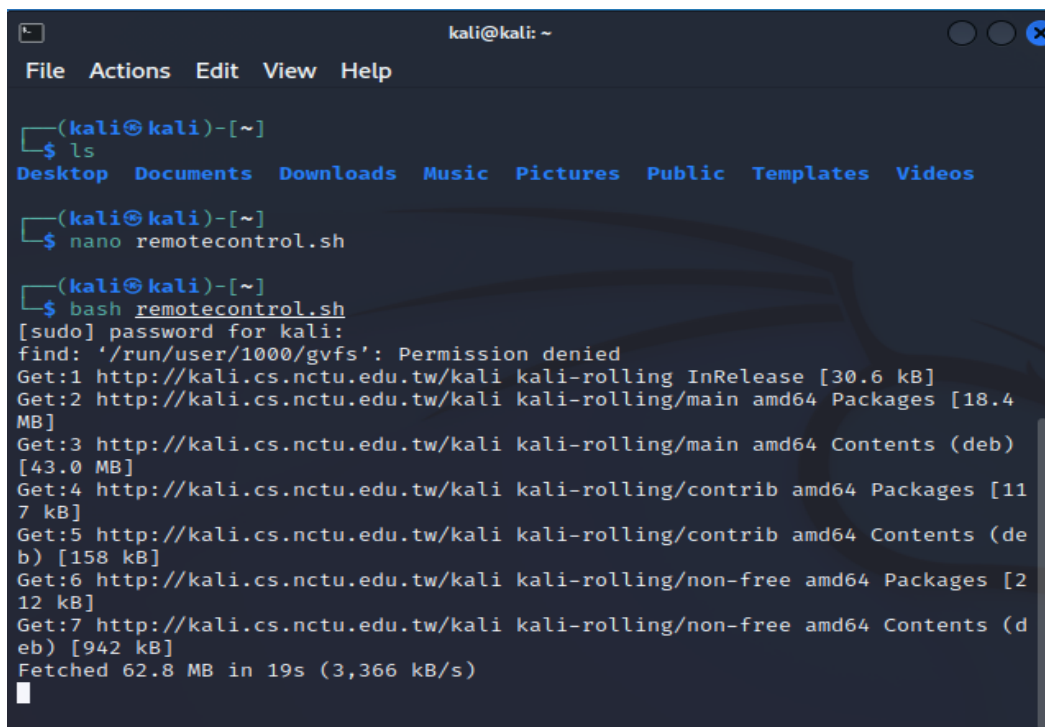
- i) As the virtual machine, kali is a new virtual machine, there is no Nipe tool install. The script will proceed to install the Nipe.
- ii) Before installing Nipe, the script will help to update and upgrade kali repository to avoid compilation error when installing nipe.

From script:

Command to update and upgrade the kali machine.

```
sudo apt-get update && sudo apt-get upgrade
```

From terminal:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
(kali@kali)-[~]  
$ nano remotecontrol.sh  
(kali@kali)-[~]  
$ bash remotecontrol.sh  
[sudo] password for kali:  
find: '/run/user/1000/gvfs': Permission denied  
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]  
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [18.4 MB]  
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [43.0 MB]  
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [117 kB]  
Get:5 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Contents (deb) [158 kB]  
Get:6 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Packages [212 kB]  
Get:7 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Contents (deb) [942 kB]  
Fetched 62.8 MB in 19s (3,366 kB/s)
```

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

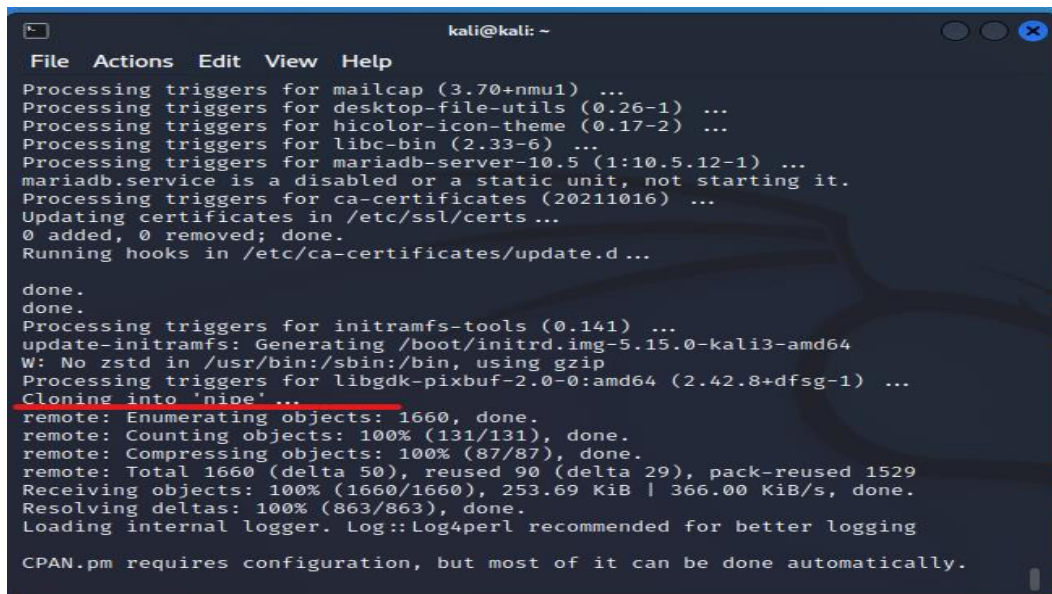
From script:

Commands to install the niipe. It will import from github htrgouvea.

```
git clone https://github.com/htrgouvea/niipe && cd niipe
sudo cpan install Try::Tiny Config::Simple JSON
sudo cpan install Switch JSON LWP::UserAgent Config::Simple
sudo perl niipe.pl install
```

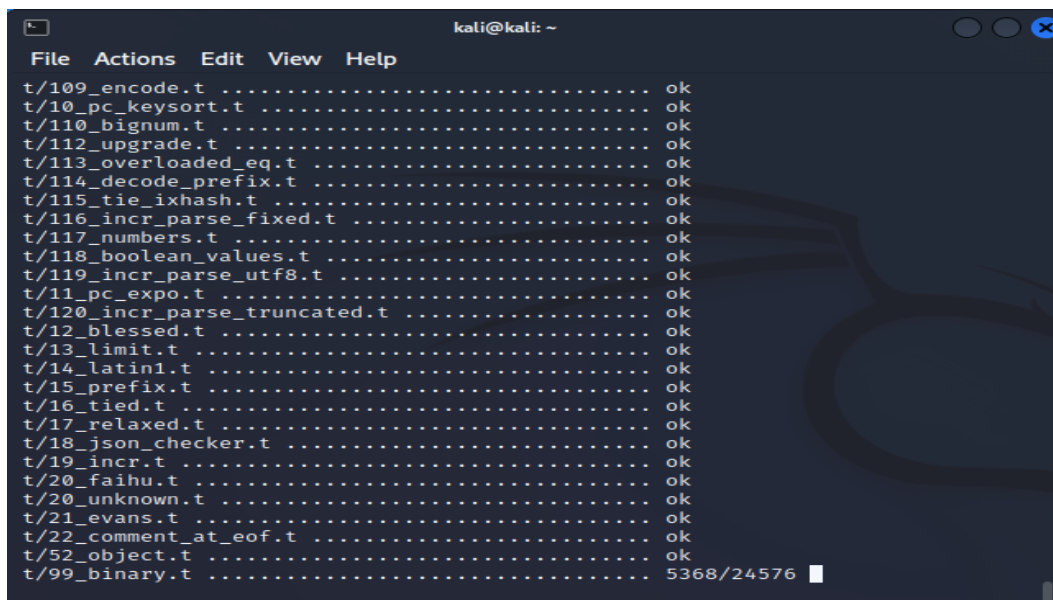
From terminal:

Highlighted red below the script has triggered the installation of Niipe process.



```
kali@kali: ~
File Actions Edit View Help
Processing triggers for mailcap (3.70+nmul) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.33-6) ...
Processing triggers for mariadb-server-10.5 (1:10.5.12-1) ...
mariadb.service is a disabled or a static unit, not starting it.
Processing triggers for ca-certificates (20211016) ...
Updating certificates in /etc/ssl/certs ...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d ...
done.
done.
Processing triggers for initramfs-tools (0.141) ...
update-initramfs: Generating /boot/initrd.img-5.15.0-kali3-amd64
W: No zstd in /usr/bin:/sbin:/bin, using gzip
Processing triggers for libgdk-pixbuf-2.0-0:amd64 (2.42.8+dfsg-1) ...
Cloning into 'niipe' ...
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 | 366.00 KiB/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.
```



```
kali@kali: ~
File Actions Edit View Help
t/109_encode.t ..... ok
t/10_pc_keysort.t ..... ok
t/110_bignum.t ..... ok
t/112_upgrade.t ..... ok
t/113_overloaded_eq.t ..... ok
t/114_decode_prefix.t ..... ok
t/115_tie_ixhash.t ..... ok
t/116_incr_parse_fixed.t ..... ok
t/117_numbers.t ..... ok
t/118_boolean_values.t ..... ok
t/119_incr_parse_utf8.t ..... ok
t/11_pc_expo.t ..... ok
t/120_incr_parse_truncated.t ..... ok
t/12_blessed.t ..... ok
t/13_limit.t ..... ok
t/14_latin1.t ..... ok
t/15_prefix.t ..... ok
t/16_tied.t ..... ok
t/17_relaxed.t ..... ok
t/18_json_checker.t ..... ok
t/19_incr.t ..... ok
t/20_faihu.t ..... ok
t/20_unknown.t ..... ok
t/21_evans.t ..... ok
t/22_comment_at_eof.t ..... ok
t/52_object.t ..... ok
t/99_binary.t ..... 5368/24576
```

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

From script:

Commands below will check the status of nipe.

- If nipe is disabled, it means user is exposed (IP address will be user's current location)
- If nipe is activated, it means user is anonymous (IP address will be from foreign country, randomly assigned/connected via nipe)

```
checknipe=$(find / -type d -name nipe 2>/dev/null)
cd $checknipe
check=$(sudo perl nipe.pl status | grep -w activated)
ipadd=$(curl -s ifconfig.io)
country=$(geoiplookup $ipadd | awk '{print $5}')

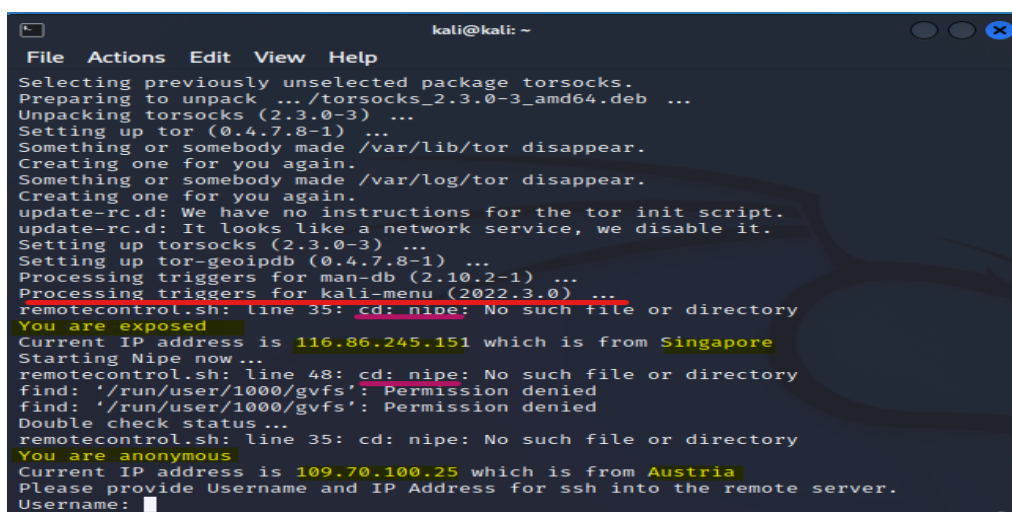
if [ ! -z "$check" ]
then
    echo "You are anonymous"
    echo "Current IP address is $ipadd which is from $country"
else
    echo "You are exposed"
    echo "Current IP address is $ipadd which is from $country"
    echo "Starting Nipe now..."
    cd nipe
    sudo perl nipe.pl start
    tornotfound
fi
```

From terminal:

Nipe tool is successfully downloaded (the last line is as shown red highlighted below.)

The script is starting to check for anonymously (as shown in yellow highlighted below.)

- Since user is exposed, the script will start nipe and if nipe is started successfully and user becomes anonymously, output will be "You are anonymously".



```
kali@kali: ~
File Actions Edit View Help
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.3.0-3_amd64.deb ...
Unpacking torsocks (2.3.0-3) ...
Setting up tor (0.4.7.8-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.3.0-3) ...
Setting up tor-geoipdb (0.4.7.8-1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.0) ...
remotecontrol.sh: line 35: cd: nipe: No such file or directory
You are exposed
Current IP address is 116.86.245.151 which is from Singapore
Starting Nipe now...
remotecontrol.sh: line 48: cd: nipe: No such file or directory
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/1000/gvfs': Permission denied
Double check status ...
remotecontrol.sh: line 35: cd: nipe: No such file or directory
You are anonymous
Current IP address is 109.70.100.25 which is from Austria
Please provide Username and IP Address for ssh into the remote server.
Username: 
```

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

From script:

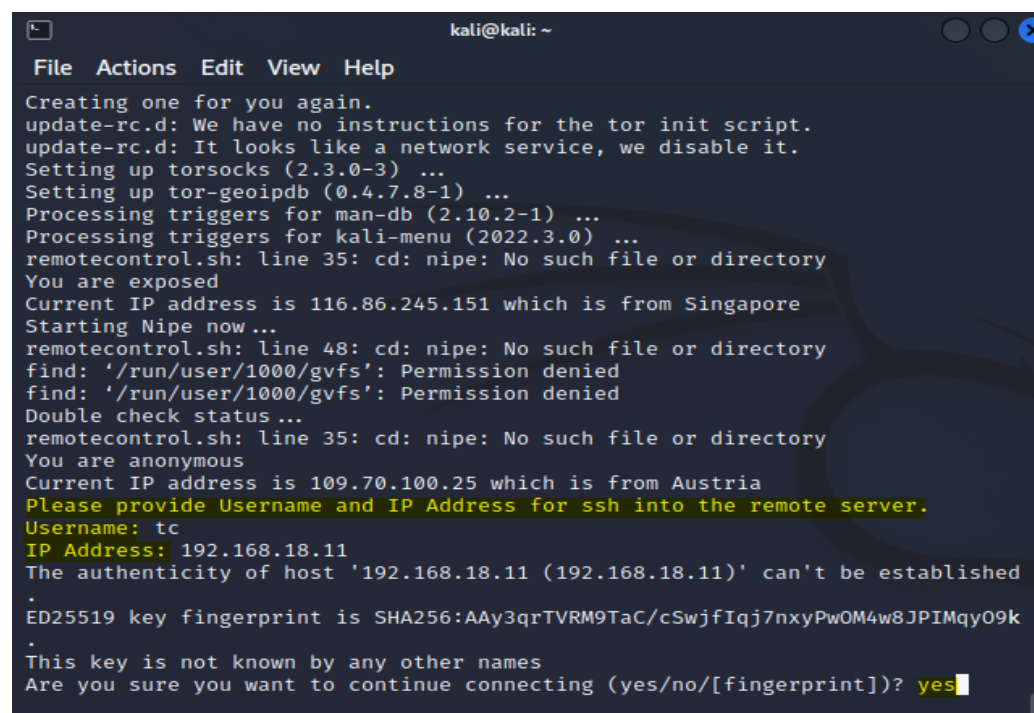
- The script will start to make connection to remote server, in this case is my virtual machine, ubuntu.

```
echo "Please provide Username and IP Address for ssh into the remote server."
read -p "Username: " user
read -p "IP Address: " ipssh

ssh "$user@"$ipssh "bash -s" <<'ENDSSH'
nmap 45.33.32.156 -oN nmap_whoisresult.txt
ipdetail=$(whois 45.33.32.156)
echo "$ipdetail" >> nmap_whoisresult.txt
exit
ENDSSH
echo " "
scp $user@$ipssh:/home/$user/nmap_whoisresult.txt .
```

- User will need to input username and password. In this example (refer to terminal screenshot below), my ubuntu will be using username of tc and ip address of 192.168.18.11
- Input "yes" to continue connecting.

From terminal:



```
kali@kali: ~
File Actions Edit View Help
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.3.0-3) ...
Setting up tor-geoipdb (0.4.7.8-1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.0) ...
remotecontrol.sh: line 35: cd: nipe: No such file or directory
You are exposed
Current IP address is 116.86.245.151 which is from Singapore
Starting Nipe now...
remotecontrol.sh: line 48: cd: nipe: No such file or directory
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/1000/gvfs': Permission denied
Double check status...
remotecontrol.sh: line 35: cd: nipe: No such file or directory
You are anonymous
Current IP address is 109.70.100.25 which is from Austria
Please provide Username and IP Address for ssh into the remote server.
Username: tc
IP Address: 192.168.18.11
The authenticity of host '192.168.18.11 (192.168.18.11)' can't be established
ED25519 key fingerprint is SHA256:AAy3qrTVRM9TaC/cSwjfIqj7nxyPwOM4w8JPIMqy09k
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```


Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

```
tc@192.168.18.11's password:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 07:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
139/tcp   filtered  netbios-ssn
161/tcp   filtered  snmp
179/tcp   filtered  bgp
646/tcp   filtered  ldap
4444/tcp  filtered  krb524
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 10.98 seconds

tc@192.168.18.11's password:
nmap_whoisresult.txt          100% 2599      1.2MB/s   00:00
```

-Input password: tc. Once done, script will start running nmap scan. Once nmap is done, the result will save into nmap_whoisresult.txt. After nmap scan, whois is also conducted and the result is appended into nmap_whoisresult.txt. Finally, script will copy the nmap_whoisresult into local machine, kali (as shown in snapshot below). Up to this point, the script has done all the commands.

```
kali@kali: ~
File Actions Edit View Help
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
139/tcp   filtered  netbios-ssn
161/tcp   filtered  snmp
179/tcp   filtered  bgp
646/tcp   filtered  ldap
4444/tcp  filtered  krb524
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 10.98 seconds

tc@192.168.18.11's password:
nmap_whoisresult.txt          100% 2599      1.2MB/s   00:00

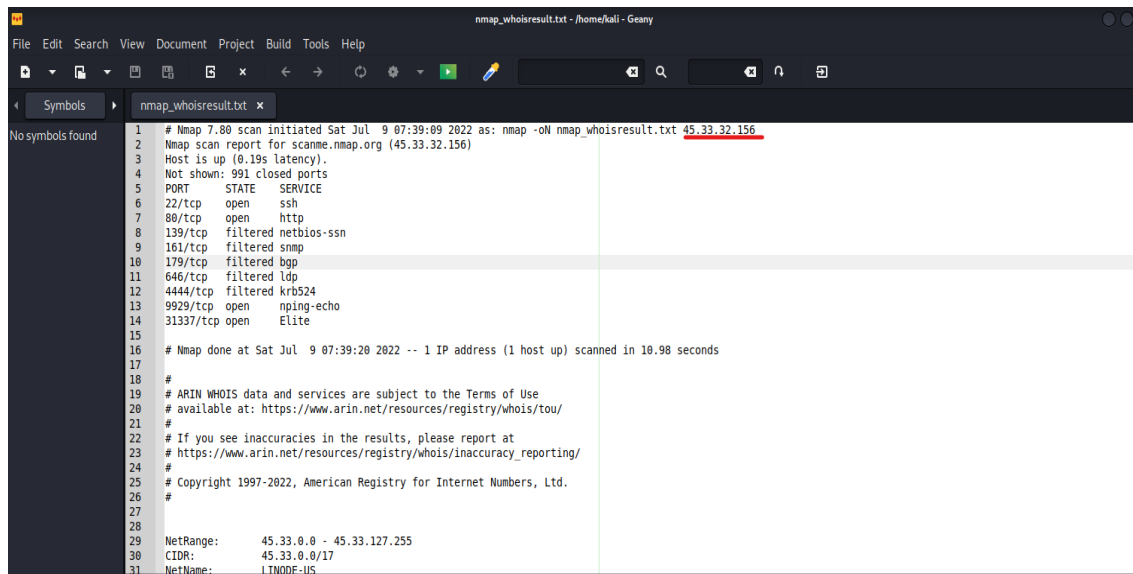
(kali@kali)-[~]
$ ls
Desktop  Music  Pictures  Templates
Documents  nipe  Public  Videos
Downloads  nmap_whoisresult.txt  remotecontrol.sh

(kali@kali)-[~]
$ geany nmap_whoisresult.txt

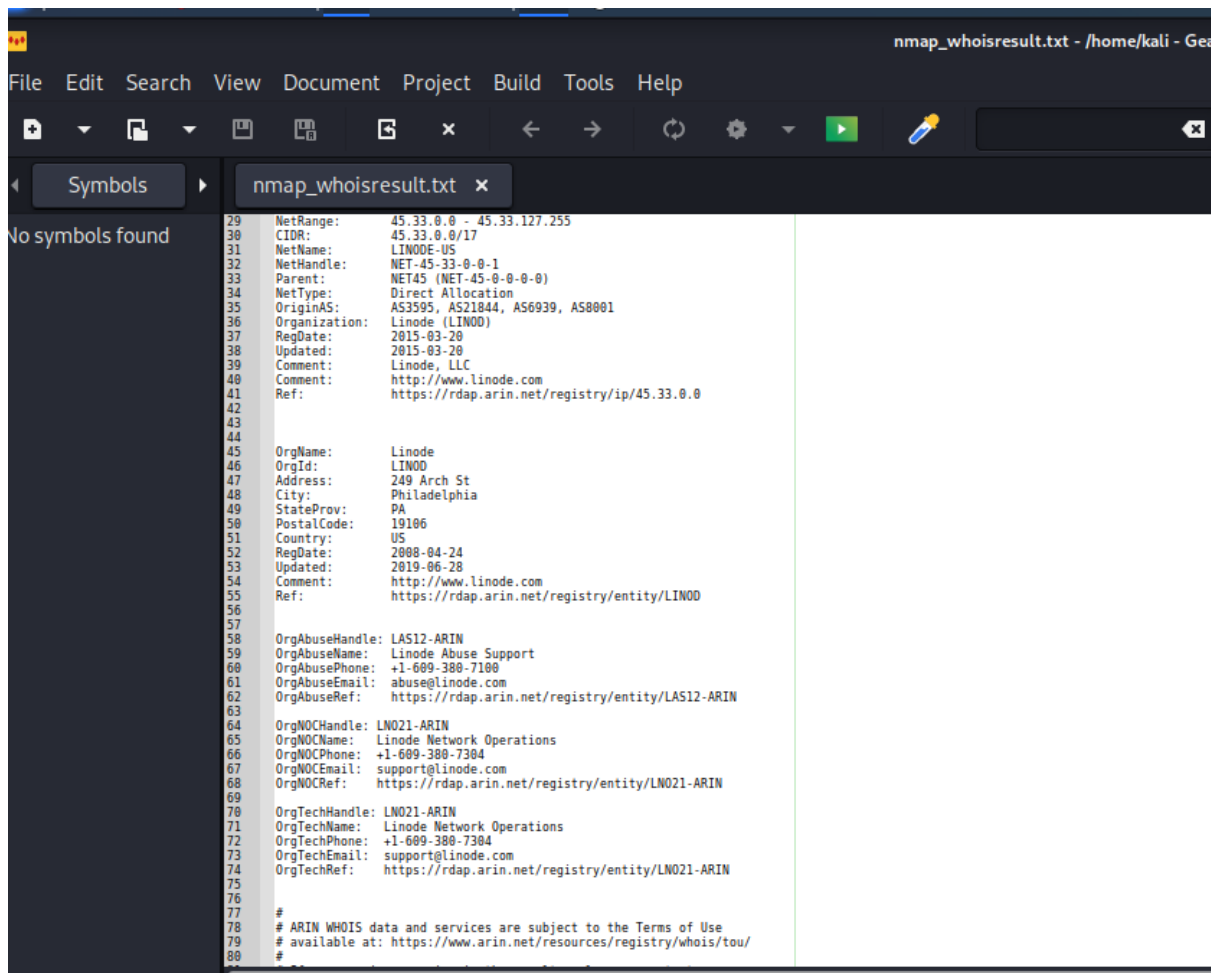
(kali@kali)-[~]
$
```

Once open the nmap_whoisresult.txt using geany, we will be able to view the result of nmap and whois on ip address: 45.33.32.156

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022



```
1 # Nmap 7.80 scan initiated Sat Jul  9 07:39:09 2022 as: nmap -oN nmap_whoisresult.txt 45.33.32.156
2 Nmap scan report for scanme.nmap.org (45.33.32.156)
3 Host is up (0.19s latency).
4 Not shown: 991 closed ports
5 PORT      STATE SERVICE
6 22/tcp    open  ssh
7 80/tcp    open  http
8 139/tcp   filtered netbios-ssn
9 161/tcp   filtered snmp
10 179/tcp   filtered bgp
11 646/tcp   filtered ldp
12 4444/tcp  filtered krb524
13 9929/tcp  open  nping-echo
14 31337/tcp open  Elite
15
16 # Nmap done at Sat Jul  9 07:39:20 2022 -- 1 IP address (1 host up) scanned in 10.98 seconds
17
18 #
19 # ARIN WHOIS data and services are subject to the Terms of Use
20 # available at: https://www.arin.net/resources/registry/whois/tou/
21 #
22 # If you see inaccuracies in the results, please report at
23 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
24 #
25 # Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
26 #
27
28
29 NetRange: 45.33.0.0 - 45.33.127.255
30 CIDR: 45.33.0.0/17
31 NetName: LINODE-US
32 NetHandle: NET-45-33-0-0-1
33 Parent: NET45 (NET-45-0-0-0)
34 NetType: Direct Allocation
35 OriginAS: AS3595, AS21844, AS6939, AS8001
36 Organization: Linode (LINOD)
37 RegDate: 2015-03-20
38 Updated: 2015-03-20
39 Comment: Linode, LLC
40 Comment: http://www.linode.com
41 Ref: https://rdap.arin.net/registry/ip/45.33.0.0
42
43
44
45 OrgName: Linode
46 OrgId: LINOD
47 Address: 249 Arch St
48 City: Philadelphia
49 StateProv: PA
50 PostalCode: 19106
51 Country: US
52 RegDate: 2008-04-24
53 Updated: 2019-06-28
54 Comment: http://www.linode.com
55 Ref: https://rdap.arin.net/registry/entity/LINOD
56
57
58 OrgAbuseHandle: LAS12-ARIN
59 OrgAbuseName: Linode Abuse Support
60 OrgAbusePhone: +1-609-380-7100
61 OrgAbuseEmail: abuse@linode.com
62 OrgAbuseRef: https://rdap.arin.net/registry/entity/LAS12-ARIN
63
64 OrgNOCHandle: LN021-ARIN
65 OrgNOCHandle: Linode Network Operations
66 OrgNOCPhone: +1-609-380-7304
67 OrgNOCEmail: support@linode.com
68 OrgNOCRef: https://rdap.arin.net/registry/entity/LN021-ARIN
69
70 OrgTechHandle: LN021-ARIN
71 OrgTechName: Linode Network Operations
72 OrgTechPhone: +1-609-380-7304
73 OrgTechEmail: support@linode.com
74 OrgTechRef: https://rdap.arin.net/registry/entity/LN021-ARIN
75
76
77 #
78 # ARIN WHOIS data and services are subject to the Terms of Use
79 # available at: https://www.arin.net/resources/registry/whois/tou/
80 #
```

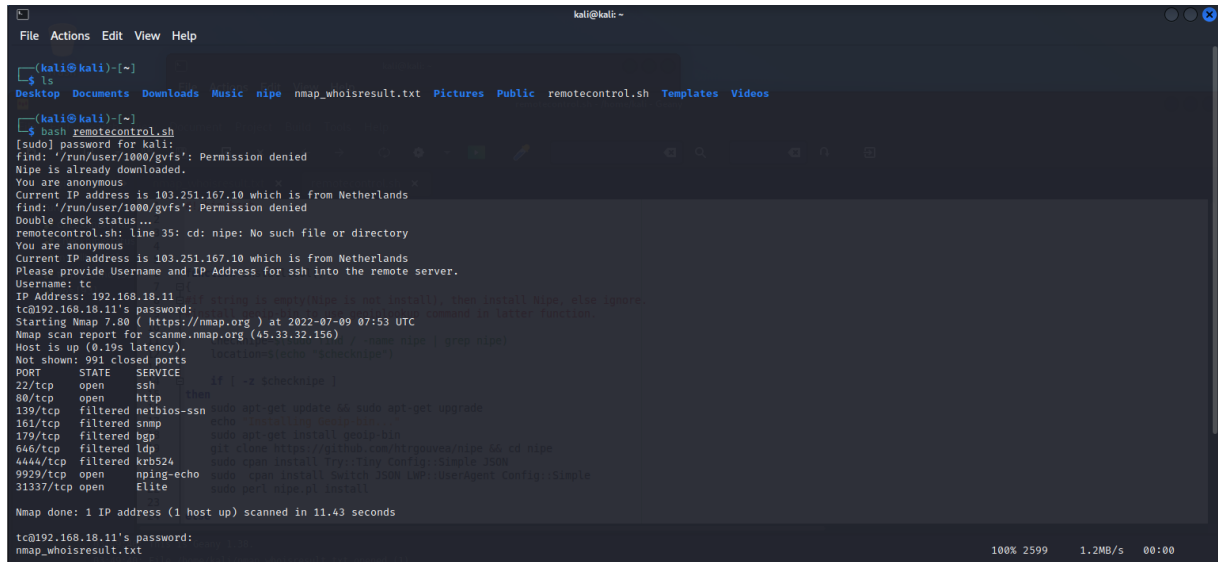


```
29 NetRange: 45.33.0.0 - 45.33.127.255
30 CIDR: 45.33.0.0/17
31 NetName: LINODE-US
32 NetHandle: NET-45-33-0-0-1
33 Parent: NET45 (NET-45-0-0-0)
34 NetType: Direct Allocation
35 OriginAS: AS3595, AS21844, AS6939, AS8001
36 Organization: Linode (LINOD)
37 RegDate: 2015-03-20
38 Updated: 2015-03-20
39 Comment: Linode, LLC
40 Comment: http://www.linode.com
41 Ref: https://rdap.arin.net/registry/ip/45.33.0.0
42
43
44
45 OrgName: Linode
46 OrgId: LINOD
47 Address: 249 Arch St
48 City: Philadelphia
49 StateProv: PA
50 PostalCode: 19106
51 Country: US
52 RegDate: 2008-04-24
53 Updated: 2019-06-28
54 Comment: http://www.linode.com
55 Ref: https://rdap.arin.net/registry/entity/LINOD
56
57
58 OrgAbuseHandle: LAS12-ARIN
59 OrgAbuseName: Linode Abuse Support
60 OrgAbusePhone: +1-609-380-7100
61 OrgAbuseEmail: abuse@linode.com
62 OrgAbuseRef: https://rdap.arin.net/registry/entity/LAS12-ARIN
63
64 OrgNOCHandle: LN021-ARIN
65 OrgNOCHandle: Linode Network Operations
66 OrgNOCPhone: +1-609-380-7304
67 OrgNOCEmail: support@linode.com
68 OrgNOCRef: https://rdap.arin.net/registry/entity/LN021-ARIN
69
70 OrgTechHandle: LN021-ARIN
71 OrgTechName: Linode Network Operations
72 OrgTechPhone: +1-609-380-7304
73 OrgTechEmail: support@linode.com
74 OrgTechRef: https://rdap.arin.net/registry/entity/LN021-ARIN
75
76
77 #
78 # ARIN WHOIS data and services are subject to the Terms of Use
79 # available at: https://www.arin.net/resources/registry/whois/tou/
80 #
```

Prepared by:
Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
9 July 2022

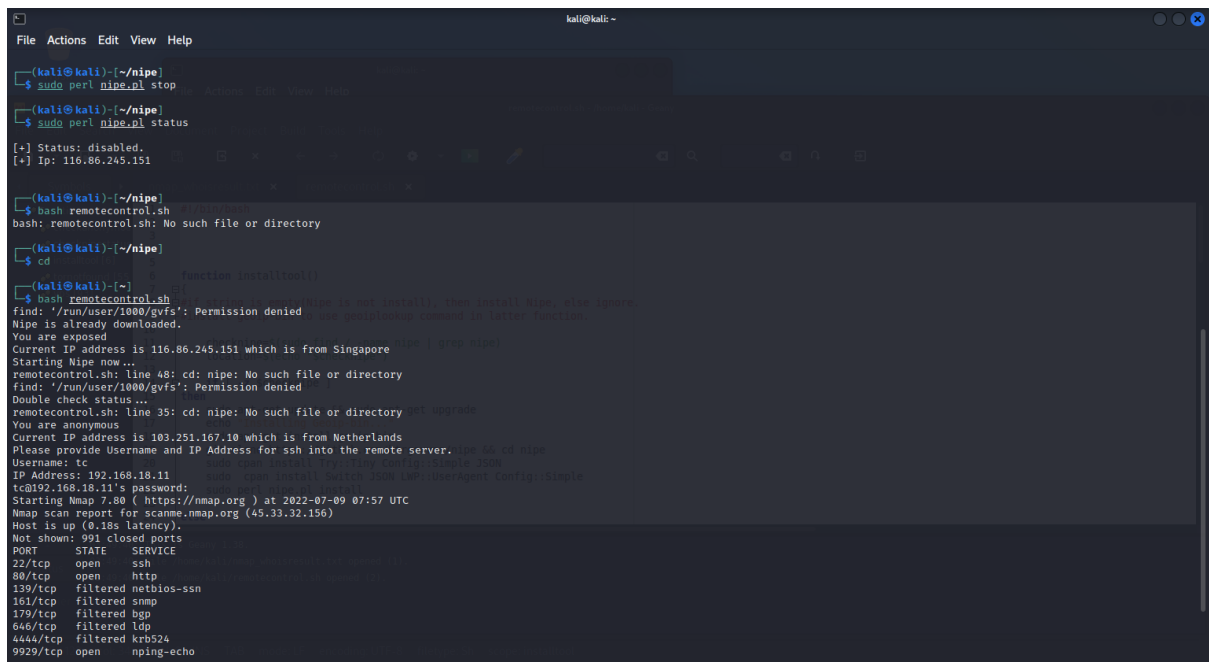
Below snapshot show the script is working even if niipe is already installed.

Scenario 1: Niipe is installed and Niipe status is activated.



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ ls  
Desktop Documents Downloads Music niipe nmap_whoisresult.txt Pictures Public remotecontrol.sh Templates Videos  
[kali@kali]~  
$ bash remotecontrol.sh  
[sudo] password for kali:  
find: '/run/user/1000/gvfs': Permission denied  
Niipe is already downloaded.  
You are anonymous  
Current IP address is 103.251.167.10 which is from Netherlands  
find: '/run/user/1000/gvfs': Permission denied  
Double check status...  
remotecontrol.sh: line 35: cd: niipe: No such file or directory  
You are anonymous  
Current IP address is 103.251.167.10 which is from Netherlands  
Please provide Username and IP Address for ssh into the remote server.  
Username: tc  
IP Address: 192.168.18.11  
tc@192.168.18.11's password:  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 07:53 UTC  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.19s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   filtered netbios-ssn  
161/tcp   filtered snmp  
179/tcp   filtered bgp  
646/tcp   filtered ldp  
4444/tcp  filtered krb524  
9929/tcp  open  nping-echo  
31337/tcp open  elite  
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds  
tc@192.168.18.11's password:  
nmap_whoisresult.txt 100% 2599 1.2MB/s 00:00
```

Scenario 2: Niipe is installed and Niipe status is disabled.



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~/niipe  
$ sudo perl niipe.pl stop  
[kali@kali]~/niipe  
$ sudo perl niipe.pl status  
[+] Status: disabled.  
[+] Ip: 116.86.245.151  
[kali@kali]~/niipe  
$ bash remotecontrol.sh  
bash: remotecontrol.sh: No such file or directory  
[kali@kali]~/niipe  
$ cd  
[kali@kali]~  
$ bash remotecontrol.sh  
find: '/run/user/1000/gvfs': Permission denied  
Niipe is already downloaded.  
You are exposed  
Current IP address is 116.86.245.151 which is from Singapore  
Starting Niipe now...  
remotecontrol.sh: line 48: cd: niipe: No such file or directory  
find: '/run/user/1000/gvfs': Permission denied  
Double check status...  
remotecontrol.sh: line 35: cd: niipe: No such file or directory  
You are anonymous  
Current IP address is 103.251.167.10 which is from Netherlands  
Please provide Username and IP Address for ssh into the remote server.  
Username: tc  
IP Address: 192.168.18.11  
tc@192.168.18.11's password:  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 07:57 UTC  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.18s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   filtered netbios-ssn  
161/tcp   filtered snmp  
179/tcp   filtered bgp  
646/tcp   filtered ldp  
4444/tcp  filtered krb524  
9929/tcp  open  nping-echo
```