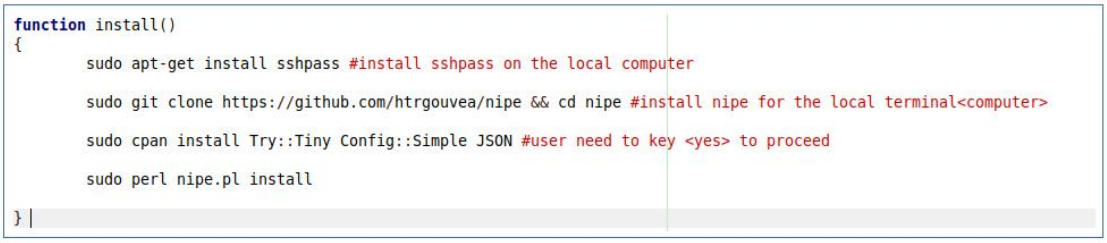
Network Research
Remote Control

CFC 240722

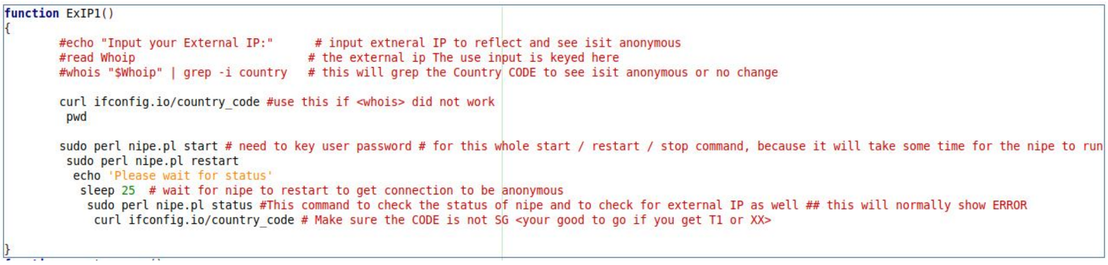
Leong Ming Zhou

10/8/2022



```
function install()
{
        sudo apt-get install sshpass #install sshpass on the local computer

        sudo git clone https://github.com/htrgouvea/nipe && cd nipe #install nipe for the local terminal<computer>

        sudo cpan install Try::Tiny Config::Simple JSON #user need to key <yes> to proceed

        sudo perl nipe.pl install

}
```

Function install above installs sshpass and nipe on the fresh computer/VM/terminal



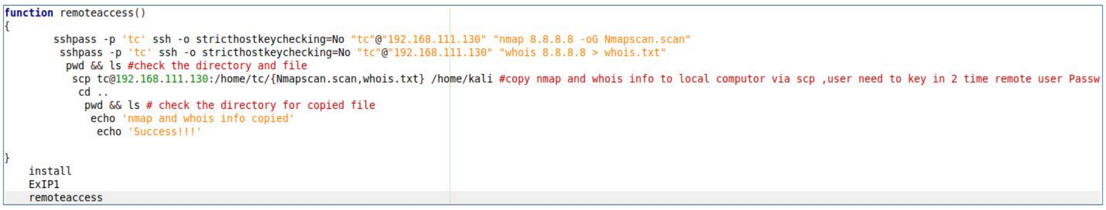
```
function ExIP1()
{
        #echo "Input your External IP:"      # input extneral IP to reflect and see isit anonymous
        #read Whoip                         # the external ip The use input is keyed here
        #whois "$Whoip" | grep -i country   # this will grep the Country CODE to see isit anonymous or no change

        curl ifconfig.io/country_code #use this if <whois> did not work
         pwd

        sudo perl nipe.pl start # need to key user password # for this whole start / restart / stop command, because it will take some time for the nipe to run
         sudo perl nipe.pl restart
          echo 'Please wait for status'
           sleep 25  # wait for nipe to restart to get connection to be anonymous
            sudo perl nipe.pl status #This command to check the status of nipe and to check for external IP as well ## this will normally show ERROR
             curl ifconfig.io/country_code # Make sure the CODE is not SG <your good to go if you get T1 or XX>

}
```

Function ExIP1 is to start and restart nipe, Echos "please wait for status" while nipe restarts.

A delay is introduced based on trial and error; 25 seconds is found to be sufficient for nipe to boot up.(result may vary based on different system).

If the status showed ERROR but the country code is indicated T1(T1 consider as anonymous) you still can proceed.

After that the status will be activated and become anonymous.

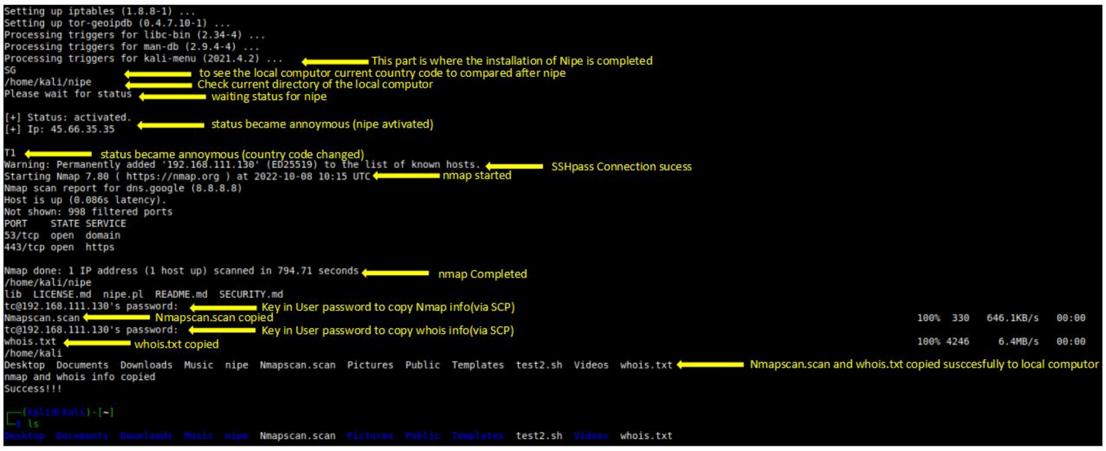


```
function remoteaccess()
{
       sshpass -p 'tc' ssh -o stricthostkeychecking=No "tc"@"192.168.111.130" "nmap 8.8.8.8 -oG Nmapscan.scan"
        sshpass -p 'tc' ssh -o stricthostkeychecking=No "tc"@"192.168.111.130" "whois 8.8.8.8 > whois.txt"
         pwd && ls #check the directory and file
          scp tc@192.168.111.130:/home/tc/{Nmapscan.scan,whois.txt} /home/kali #copy nmap and whois info to local computor via scp ,user need to key in 2 time remote user Passw
           cd ..
            pwd && ls # check the directory for copied file
             echo 'nmap and whois info copied'
              echo 'Success!!!'

}
    install
    ExIP1
    remoteaccess
```

Function remoteaccess to gain access into computer/VM/terminal via SSHpass.

Via sshpass to nmap into grepable format and copy back the file back to the local computer/VM/terminal.

and for whois via sshpass , I have choose to input the data in to “whois.txt” and copy back the file back to the local computer/VM/terminal.



```
Setting up iptables (1.8.8-1) ...
Setting up tor-geoipdb (0.4.7.10-1) ...
Processing triggers for libc-bin (2.34-4) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...
SG
/home/kali/nipe
Please wait for status

[+] Status: activated.
[+] Ip: 45.66.35.35

T1
Warning: Permanently added '192.168.111.130' (ED25519) to the list of known hosts.
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-08 10:15 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.086s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 794.71 seconds
/home/kali/nipe
lib  LICENSE.md  nipe.pl  README.md  SECURITY.md
tc@192.168.111.130's password:
Nmapscan.scan                                                                          100%  330   646.1KB/s   00:00
tc@192.168.111.130's password:
whois.txt                                                                              100% 4246     6.4MB/s   00:00
/home/kali
Desktop  Documents  Downloads  Music  nipe  Nmapscan.scan  Pictures  Public  Templates  test2.sh  Videos  whois.txt
nmap and whois info copied
Success!!!

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Nmapscan.scan  Pictures  Public  Templates  test2.sh  Videos  whois.txt
```

This part is where the installation of Nipe is completed

to see the local computor current country code to compared after nipe

Check current directory of the local computor

waiting status for nipe

status became annoymous (nipe avtivated)

status became annoymous (country code changed)

SSHpass Connection sucess

nmap started

nmap Completed

Key in User password to copy Nmap info(via SCP)

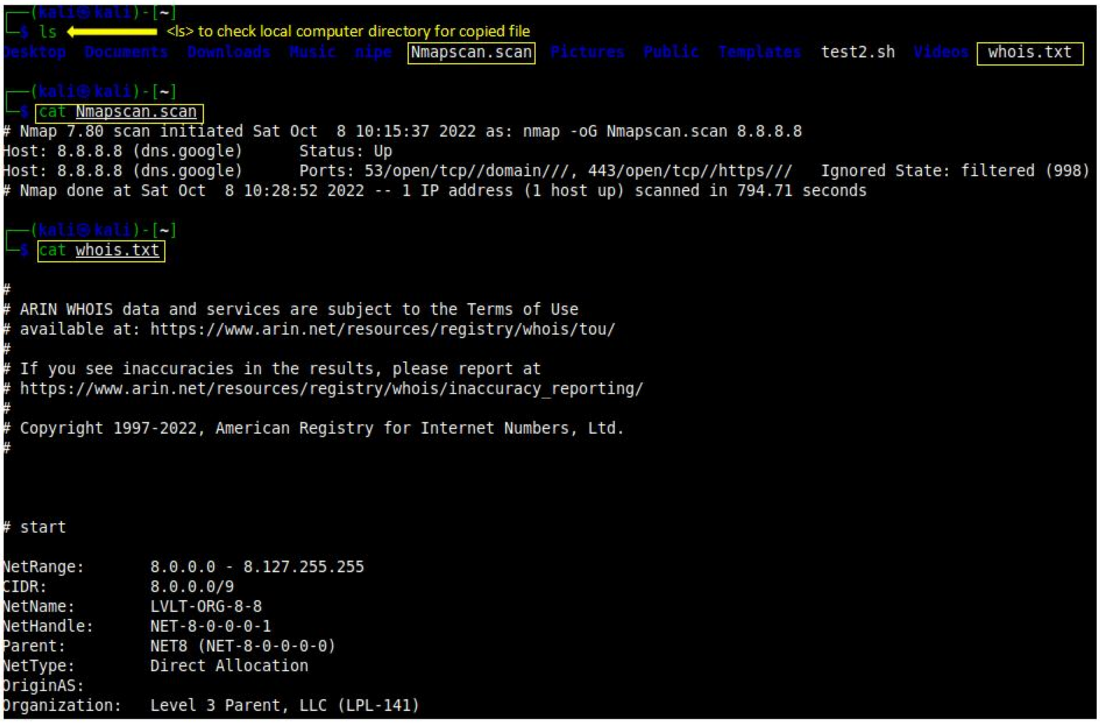
Nmapscan.scan copied

Key in User password to copy whois info(via SCP)

whois.txt copied

Nmapscan.scan and whois.txt copied succesfully to local computor

Above snapshot is the result after running the script



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nipe  Nmapscan.scan  Pictures  Public  Templates  test2.sh  Videos  whois.txt

┌──(kali㉿kali)-[~]
└─$ cat Nmapscan.scan
# Nmap 7.80 scan initiated Sat Oct  8 10:15:37 2022 as: nmap -oG Nmapscan.scan 8.8.8.8
Host: 8.8.8.8 (dns.google)      Status: Up
Host: 8.8.8.8 (dns.google)      Ports: 53/open/tcp//domain///, 443/open/tcp//https///   Ignored State: filtered (998)
# Nmap done at Sat Oct  8 10:28:52 2022 -- 1 IP address (1 host up) scanned in 794.71 seconds

┌──(kali㉿kali)-[~]
└─$ cat whois.txt

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       8.0.0.0 - 8.127.255.255
CIDR:           8.0.0.0/9
NetName:        LVLT-ORG-8-8
NetHandle:      NET-8-0-0-0-1
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Level 3 Parent, LLC (LPL-141)
```

<ls> to check local computer directory for copied file

Above snapshot is the Copied file to confirm the content inside of each file.

From this coding/script I'm trying to achieve to remote access from local machine to source machine via being anonymous and nmap/whois into a file.

After nmap/whois into a file then copy the file to the local machine.