Edwin’s Network research project

Contents

Step 1 Install relevant applications on the local computer

Step 2 Check if the connection is anonymous (not from your origin country)

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

Step 4 Save the result on your local computer.

Step 1 Install relevant applications on the local computer

Thought Process

1. To create a contained environment within the home folder to keep whatever we are doing in a single folder. This will facilitate easier location of files.
2. If we were to use this script on a whole new Kali or any system that can read bash, It auto update and upgrade the system. Otherwise, it will just check the versions.
3. After Identifying all the tools, just throw everything into a function and install it
4. I will be dealing with the installation of nipe separately as it requires more than a line of code.

Step 1 Install relevant applications on the local computer

1. To create a contained environment within the home folder to keep whatever we are doing in a single folder. This will facilitate easier locating of files.

```
function crefldr()
    {
        mkdir NRprobase
        cd NRprobase
    }
```

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  NRprobase  Public                Templates
Documents  Music      Pictures   RemoteControlEdwin.sh Videos
```

We CD into the Folder so that the script will be ran inside the Folder.

Step 1 Install relevant applications on the local computer

Force Update and upgrade.

```
## to have a sense of what we have, we just update and upgrade the kali to ensure that the kali is up to date
function forupdate()
    {
        sudo apt-get -y update
        sudo apt-get -y upgrade
    }
```

This function makes the system do its self update and upgrade every time it is ran.

The flag -y makes the sudo automatically assume that all the choices are ‘Yes’

```
Hit:1 http://mirror.aktkn.sg/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  cgpt faraday gstreamer1.0-plugins-bad ipython3 libgstreamer-plugins-bad1.0-0 python3-ipython
  vboot-kernel-utils vboot-utils
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

Step 1 Install relevant Tools on the local computer

After Identifying all the tools, just throw everything into a function and install it

```
Installing the tools for the job
-----Installing GEANY-----
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
geany is already the newest version (1.38-1+b1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
-----Installing NMAP-----
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.93+dfsg1-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
-----Installing CURL-----
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.86.0-2).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
-----Installing whois-----
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.14).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
-----Installing SSHPASS-----
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sshpass is already the newest version (1.09-1+b1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
```

```
function instools()
{
    echo "Installing the tools for the job"
    echo "-----Installing GEANY-----"
    sudo apt-get install -y geany
    echo "-----Installing NMAP-----"
    sudo apt-get install -y nmap
    echo "-----Installing CURL-----"
    sudo apt-get install curl
    echo "-----Installing whois-----"
    sudo apt-get install whois
    echo "-----Installing SSHPASS-----"
    sudo apt-get install sshpass
    echo "-----Installing net-tools-----"
    sudo apt-get install net-tools
    echo "-----Removing files that are not required-----"
    sudo apt autoremove
    echo "----------------------------------------------"

}
```

The idea is that when the script is ran, it will be ran on a new blank machine. But regardless, this portion will update the individual tools if its out of date.

The apt auto remove command is to remove all the old and unnecessary files for the system.

Step 1 Install relevant applications on the local computer

1. I will be dealing with the installation of nipe separately as it requires more than a line of code.

```
function insnipe()
{
    echo "INSTALLING NIPE"
    git clone https://github.com/htrgouvea/nipe
    #~ pwd
    cd nipe
    sudo cpan install Try::Tiny Config::Simple JSON
    sudo perl nipe.pl install
}
```

I could have just insert this function into the the instool function, to make it more effective. However, I decided to stick with my point on dealing with the nipe installation separately as, I feel that the nipe installation requires a bit more attention.

```
INSTALLING NIPE
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 | 407.00 KiB/s, done.
Resolving deltas: 100% (863/863), done.
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Sat, 08 Oct 2022 04:55:50 GMT
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.09).
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tor is already the newest version (0.4.7.10-1).
iptables is already the newest version (1.8.8-1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
```

Step 2 Check if the connection is anonymous (not from your origin country)

Thought Process

1. Start nipe, if the tor connection fail, the script will restart the connection.
2. Make a comparison between the things that would make a person anonymous: the IP address.

Step 2 Check if the connection is anonymous (not from your origin country)

1. Start nipe, if the tor connection fails, the script will restart the connection.

I shorten the nipe commands so that we can easily call it in to other functions later on.

```
## Function for checking Nipe Status
function nipestatus()
    {
        sudo perl nipe.pl status
    }
## Function for starting Nipe
function nipestart()
    {
        sudo perl nipe.pl start
    }
## Function for restarting Nipe
function niperestart()
    {
        sudo perl nipe.pl restart
    }

## Function for stopping Nipe
function nipestop()
    {
        sudo perl nipe.pl stop
    }

# Automating status script
function nstat()
    {
        nistat=$(nipestatus | grep Status | awk '{print $3}')
        echo "your Nipe is currently $nistat"
    }
```

Step 2 Check if the connection is anonymous (not from your origin country)

1. Start nipe, if the tor connection fails, the script will restart the connection.

   This script will ensure that the TOR is running correctly, by isolating the Status line of the output, as long as this output is not activated, it will run the restart command.

   The other 2 functions are used to ensure that the TOR's new IP and Location has been masked.

```
#Nipe start script
function nstart()
    {
        echo 'Starting Nipe'
        nipestart
        nistat=$(nipestatus | grep Status | awk '{print $3}')
        if [[ $nistat != activated ]]
            then
                echo "Restarting nipe"
                niperestart
        else
                echo "your Nipe is currently $nistat"
        fi
    }
```

```
Your Current IP : 192.168.75.138
Starting NIPE
NIPE started

[+] Status: activated.
[+] Ip: 185.220.101.29

Your Current IP : 185.220.101.29
you are anonymous
--------------------Nipe initialisation completed--------------------
```

```
function anoncheckip()
    {

        if [ $oip == $nip ]
        then
            echo ' you are not anonymous'
            nrestart
        else
            echo 'you are anonymous '
        fi
    }
```

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

Thought Process

1. Have the user of the script manually input his targets
2. Similar to the script at the beginning, to create a folder to contain the results of the scans.
3. Have the remote server install and run the 3 scans.
4. Ensure that the 3 files are saved in the predefined folder.

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

1. Have the user of the script manually input his targets.

Having it like this allows the user to

Use the script on different targets that

He has their information on

```
function getsvrinfo()
    {
        echo "Whats the IP to connect to?"
        read nrip
        echo "Who is the user?"
        read nrus
        echo "What is the password for this user?"
        read nrpwd
    }
```

```
sshpass into the NR droplet
Whats the IP to connect to?
137.184.75.13
Who is the user?
root
What is the password for this user?
RootR00t
Starting SHHPASS
```

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

1. Similar to the script at the beginning, to create a folder to contain the results of the scans.

```
sshpass -p $nrpwd ssh -o StrictHostKeyChecking=no $nrus@$nrip mkdir scanresults
```

By using the -o StrictHostKeyChecking=no I can skip the need to manually register the IP via a normal ssh

```
root@Test-test:~# ls
scanresults  snap
```

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

1. Have the remote server install and run the 3 scans.

```
function nmapinsp()
    {
    sshpass -p $nrpwd ssh $nrus@$nrip apt install nmap
    sshpass -p $nrpwd ssh $nrus@$nrip "cd scanresults && nmap 8.8.8.8 -oG nrsnmap.scan"
    }
function massinsp()
    {
    sshpass -p $nrpwd ssh $nrus@$nrip apt install masscan
    sshpass -p $nrpwd ssh $nrus@$nrip "cd scanresults && masscan 8.8.8.8 -p 20-80 -oG nrsmas.scan"
    }

function whoisinsp()
    {
    sshpass -p $nrpwd ssh $nrus@$nrip apt install whois
    #sshpass -p $nrpwd ssh $nrus@$nrip whoisrs.txt
    sshpass -p $nrpwd ssh $nrus@$nrip "cd scanresults && whois 8.8.8.8 >> whoisrs.txt"
    }
```

```
# Masscan 1.3.2 scan initiated Sat Oct  8 11:17:00 2022
# Ports scanned: TCP(61;20-80) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1665227820   Host: 8.8.8.8 ()        Ports: 53/open/tcp//domain//
# Masscan done at Sat Oct  8 11:17:12 2022
```

```
# 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)
RegDate:        1992-12-01
Updated:        2018-04-23
Ref:            https://rdap.arin.net/registry/ip/8.0.0.0
```

```
root@104.248.53.96's password:
nrsmas.scan                                           100%  229     0.2KB/s   00:00
nrsnmap.scan                                          100%  327     0.3KB/s   00:01
whoisrs.txt                                           100% 8493     8.3KB/s   00:01
stopping Nipe
your Nipe is currently disabled.
# Nmap 7.80 scan initiated Sat Oct  8 11:16:46 2022 as: nmap -oG nrsnmap.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 11:16:50 2022 -- 1 IP address (1 host up) scanned in 4.63 seconds
```

Step 3 Once the connection is anonymous, communicate via SSH / SSHPASS and execute nmap scans / masscan and whois queries

1. Ensure that the 3 files are saved in the predefined folder.

```
# Checking that the saves are successfully saved in the scanresults folder
sshpass -p $nrpwd ssh -o StrictHostKeyChecking=no $nrus@$nrip "cd scanresults && ls"
```

```
nrsmas.scan
nrsnmap.scan
whoisrs.txt
---------------
```

In this case, I did it by running multiple commands using the &&

Step 4 Save the scan results your local computer.

Thought Process

- Using Secure Copy to copy the files back over to the local host and check that they are both can be read on the local host.
- After the copy is complete, we double check if the file are downloaded in the correct folder

Step 4 Save the scan results your local computer.

- Using Secure Copy to copy the files back over to the local host and check that they are both can be read on the local host.

```
function sendrs()
    {
    scp -r  $nrus@$nrip:~/scanresults ~/NRprobase
    }
```

Using this variation of the scp, it allows me to scp the whole folder instead of just 1 file, and which brings me back to the point on having everything in 1 folder

The -r command is used here to scp the folder's contents

```
kali@vulner's password:
nrsmas.scan                                                    100%  229   232.9K
B/s   00:00
whoisrs.txt                                                    100%   50KB  25.5M
B/s   00:00
nrsnmap.scan                                                   100%  328   387.4K
B/s   00:00
stopping Nipe
```

Step 4 Save the scan results your local computer.

- Using Secure Copy to copy the files back over to the local host and check that they are both can be read on the local host.

```
function gotoSdatafmnipe()
    {
        cd
        cd NRprobase/scanresults
    }
function rddlfiles()
    {
        echo "--------------------Nmap results--------------------"
        cat nrsnmap.scan
        echo "--------------------Masscan results-------
        cat nrsmas.scan
        echo "--------------------Whois Results---------
        cat whoisrs.txt
    }
```

Using the gotoSdatafmnipe function, basically moves me back to the home folder then cd into the exact location of the Scanresults folder that scp from.

```
--------------------Step 3 completed--------------------
root@104.248.53.96's password:
nrsmas.scan
nrsnmap.scan
whoisrs.txt
stopping Nipe
your Nipe is currently disabled.
nrsmas.scan  nrsnmap.scan  whoisrs.txt
--------------------Nmap results--------------------
# Nmap 7.80 scan initiated Sat Oct  8 11:16:46 2022 as: nmap -oG nrsnmap.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 11:16:50 2022 -- 1 IP address (1 host up) scanned in 4.63 seconds
--------------------Masscan results--------------------
# Masscan 1.3.2 scan initiated Sat Oct  8 11:17:00 2022
# Ports scanned: TCP(61;20-80) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1665227820   Host: 8.8.8.8 ()        Ports: 53/open/tcp//domain//
# Masscan done at Sat Oct  8 11:17:12 2022
--------------------Whois Results--------------------


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
```

And using cat to check the contents of the file to ensure that what was printed in the remote server is printed here in the local host.

Credits

SSHPASS

https://www.tecmint.com/sshpass-non-interactive-ssh-login-shell-script-ssh-password/

Instructor

Centre for Cybersecurity - James Lim

This Documentation is created by

Edwin Tan, Student code S5/2407