NETWORK RESEARCH

Kyle Lim

1. Installing the relevant apps.
   code

```
function inst()
{
    #install ssh

    sudo apt-get install openssh-client

    #install nipe
    checknipe=$(cd nipe|grep -w no)
    if [ ! -z $checknipe ]
    then
        git clone https://github.com/htrgouvea/nipe && cd nipe
        sudo cpan install Try::Tiny Config::Simple JSON
        perl nipe.pl install
    else
        echo "You have nipe installed"
    fi

    #install sshpass

    sudo apt-get install sshpass

    #install nmap

    sudo apt-get install nmap
    clear
}
```

Testing out the code

```
Before we get started, let us check if we have the relevant applications first
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
openssh-client is already the newest version (1:9.0p1-1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
You have nipe installed
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
sshpass is already the newest version (1.09-1+b1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.92+dfsg2-1kali1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libllvm12 python3-ipaddr python3-singledispatch python3-twisted-bin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 232 not upgraded.
```

2. Checking if the connection is anonymous
   a) Checking the country (code)

```
function countrycheck()
{
    #check if the connection is from your origin country
    ip=$(curl -s ifconfig.io)
    country=$(curl -s https://ipinfo.io/$ip|grep -w country|awk '{print $2}'|tr -d '[:punct:]')
    echo "Is $country your origin country? (y/n)"
    read input
    if [ $input == "y" ]
    then
        echo "Please go anonymous before continuing"
    elif [ $input == "n" ]
    then
        echo "You are anonymous. Please proceed."
    else
        echo "Please try again"
    fi
}
```

   b) Checking if the user is anonymous (code)

```
function anon()
{
    #check if the connection is anonymous
    cd /home/kali/nipe

    stat_check=$(sudo perl nipe.pl status|grep -w activated)

    if [ ! -z "$stat_check" ]
    then
        echo "You are anonymous."
    else
        echo "Getting anonymity.Please wait"
    fi

}
```

   Testing the code out

```
Is SG your origin country? (y/n)
y
Please go anonymous before continuing
Getting anonymity.Please wait
Is DE your origin country? (y/n)
```

3. Connect to a VPS and execute scans.

Code

```
function vps()
{
    #connect to a vps via sshpass
    echo "Enter IP address to whois/nmap:"
    read ipadd
    #run nmap/whois on VPS
    sshpass -p 1 ssh ky@165.232.134.47 "nmap $ipadd > nmap.txt;whois $ipadd > whois.txt"
    #viewing the results
    sshpass -p 1 ssh ky@165.232.134.47 "cat nmap.txt"
    echo "press enter to view the whois result"
    read
    sshpass -p 1 ssh ky@165.232.134.47 "cat whois.txt"
```

```
function vps()
{
    #connect to a vps via sshpass
    echo "Enter IP address to whois/nmap:"
    read ipadd
    sshpass -p 1 ssh ky@165.232.134.47 "nmap $ipadd > nmap.txt;whois $ipadd > whois.txt"
    sshpass -p 1 ssh ky@165.232.134.47 "cat nmap.txt;cat whois.txt"

}
```

Testing it out

```
Enter IP address to whois/nmap:
8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-14 18:42 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0026s 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 4.03 seconds
press enter to view the whois result
```

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


OrgName:        Level 3 Parent, LLC
OrgId:          LPL-141
Address:        100 CenturyLink Drive
City:           Monroe
StateProv:      LA
PostalCode:     71203
Country:        US
RegDate:        2018-02-06
Updated:        2021-09-23
Comment:        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE ANY ISP ANNOUNCING OR TRANSITING PORTIONS WITHIN
Comment:
Comment:        Our looking glass is located at: https://lookingglass.centurylink.com/
Comment:
Comment:        For subpoena or court order please fax 844.254.5800 or refer to our Trust & Safety page:
Comment:        https://www.lumen.com/en-us/about/legal/trust-center/trust-and-safety.html
Comment:
Comment:        For abuse issues, please email abuse@aup.lumen.com
Comment:        All abuse reports MUST include:
```