NETWORK RESEARCH PROJECT

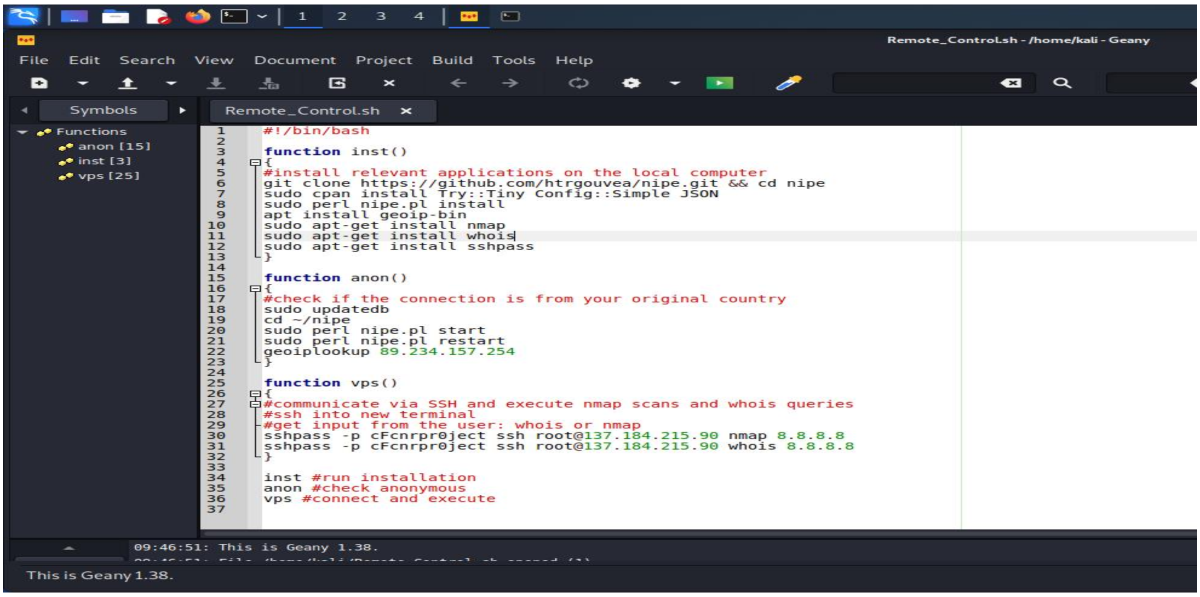
REMOTE CONTROL

Objective:

Create a script that communicates with a remote server and executes tasks anonymously.

Using geany to write a script to automate the process.

1) Function inst() to install all the necessary tools to run the script.
2) Function anon() to check if I am anonymous by using nipe.
   Nipe is to go anonymous.
   *Do sudo perl nipe.pl start and restart because there's a known bug.
3) Function vps() to ssh into new terminal and check nmap/ ssh
   *Format to do nmap/ whois inside the ssh terminal:
   "sshpass -p 'password' ssh user@host command"
   Use digital ocean to create a new project under ubuntu to get the IP address.



```bash
#!/bin/bash

function inst()
{
#install relevant applications on the local computer
git clone https://github.com/htrgouvea/nipe.git && cd nipe
sudo cpan install Try::Tiny Config::Simple JSON
sudo perl nipe.pl install
apt install geoip-bin
sudo apt-get install nmap
sudo apt-get install whois
sudo apt-get install sshpass
}

function anon()
{
#check if the connection is from your original country
sudo updatedb
cd ~/nipe
sudo perl nipe.pl start
sudo perl nipe.pl restart
geoiplookup 89.234.157.254
}

function vps()
{
#communicate via SSH and execute nmap scans and whois queries
#ssh into new terminal
#get input from the user: whois or nmap
sshpass -p cFcnrpr0ject ssh root@137.184.215.90 nmap 8.8.8.8
sshpass -p cFcnrpr0ject ssh root@137.184.215.90 whois 8.8.8.8
}

inst #run installation
anon #check anonymous
vps #connect and execute
```

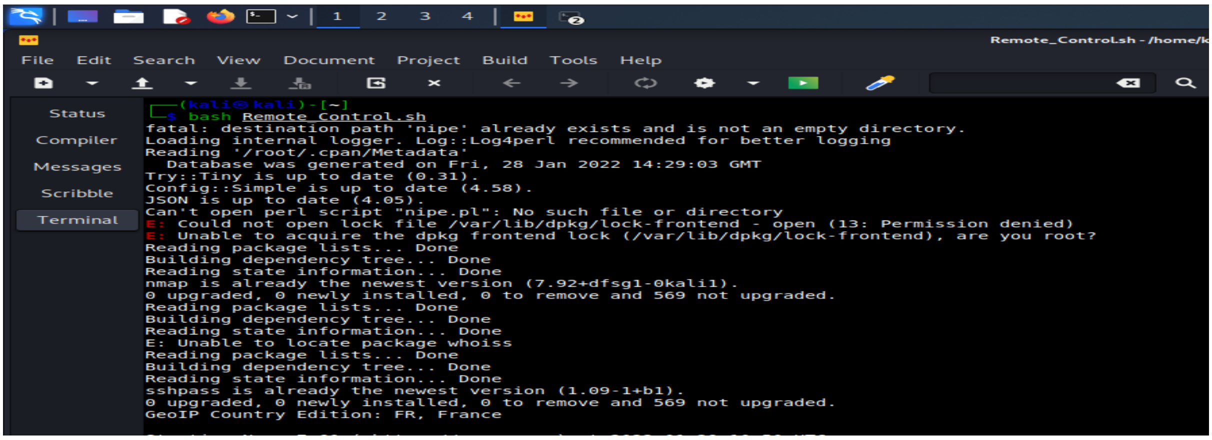
```
09:46:51: This is Geany 1.38.
```

```
This is Geany 1.38.
```

[Figure 1]

Script written using geany to automate the process.

Using 'curl ifconfig.me' to get the ip address in your terminal for geoiplookup.



```
┌──(kali㉿kali)-[~]
└─$ bash Remote_Control.sh
fatal: destination path 'nipe' already exists and is not an empty directory.
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Fri, 28 Jan 2022 14:29:03 GMT
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.05).
Can't open perl script "nipe.pl": No such file or directory
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.92+dfsg1-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 569 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package whois
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 569 not upgraded.
GeoIP Country Edition: FR, France
```

[Figure 2]

*Prove that the script works!

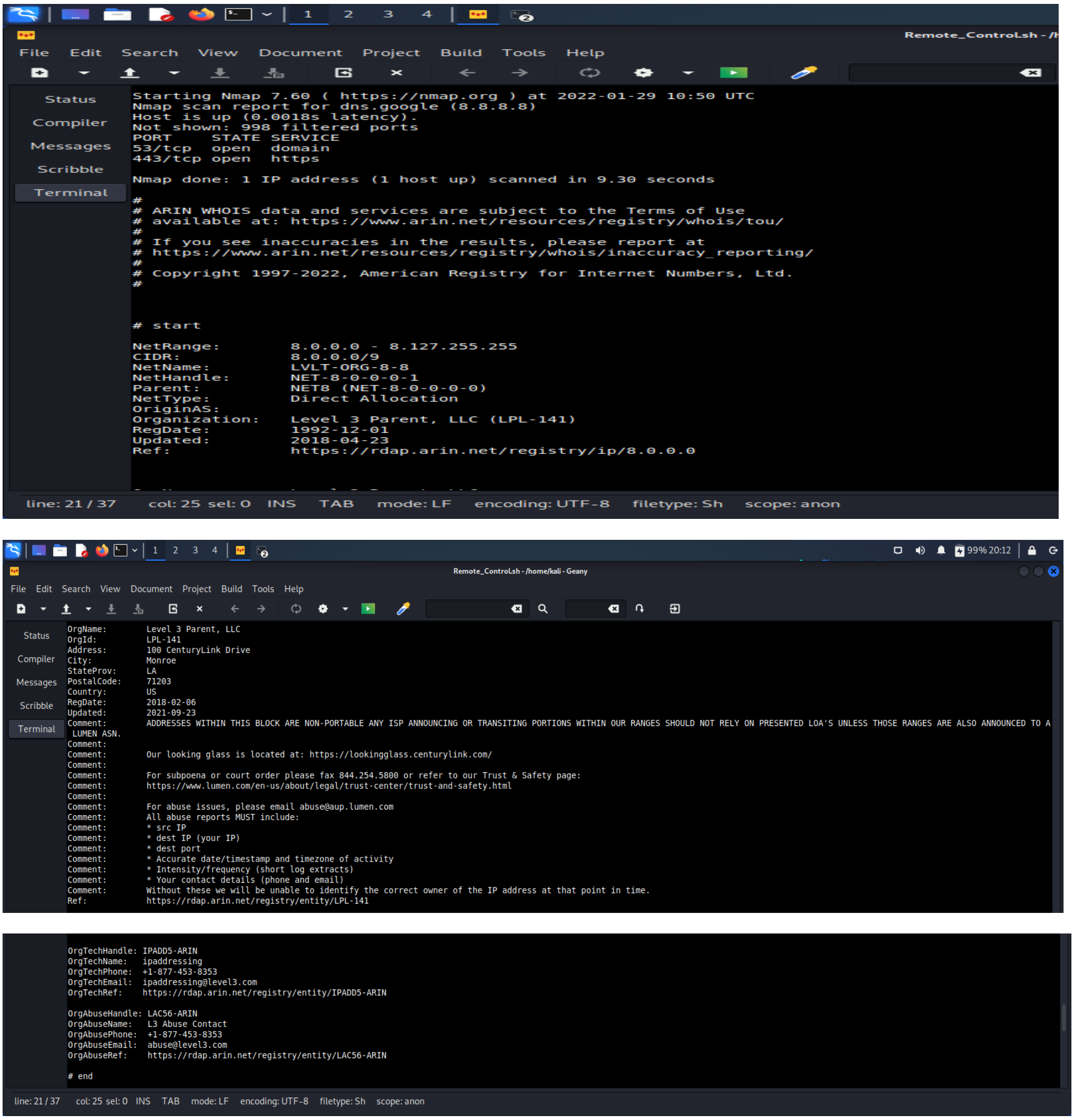
The system will detect for any un-install/ un-updated apps, and install it.

Once all the apps are downloaded, the script will run the next command to scan for location of ip.

Use digital ocean to create a new project under ubuntu to get the IP address.

Geoip result: France - Confirmed anonymous.

Nmap scan



```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-01-29 10:50 UTC
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0018s 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 9.30 seconds

#
# 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
```

line: 21 / 37   col: 25 sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: anon

```
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 OUR RANGES SHOULD NOT RELY ON PRESENTED LOA'S UNLESS THOSE RANGES ARE ALSO ANNOUNCED TO A
 LUMEN ASN.
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:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email)
Comment:        Without these we will be unable to identify the correct owner of the IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/LPL-141
```

```
OrgTechHandle: IPADD5-ARIN
OrgTechName:   ipaddressing
OrgTechPhone:  +1-877-453-8353
OrgTechEmail:  ipaddressing@level3.com
OrgTechRef:    https://rdap.arin.net/registry/entity/IPADD5-ARIN

OrgAbuseHandle: LAC56-ARIN
OrgAbuseName:   L3 Abuse Contact
OrgAbusePhone:  +1-877-453-8353
OrgAbuseEmail:  abuse@level3.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/LAC56-ARIN

# end
```

line: 21 / 37   col: 25 sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: anon

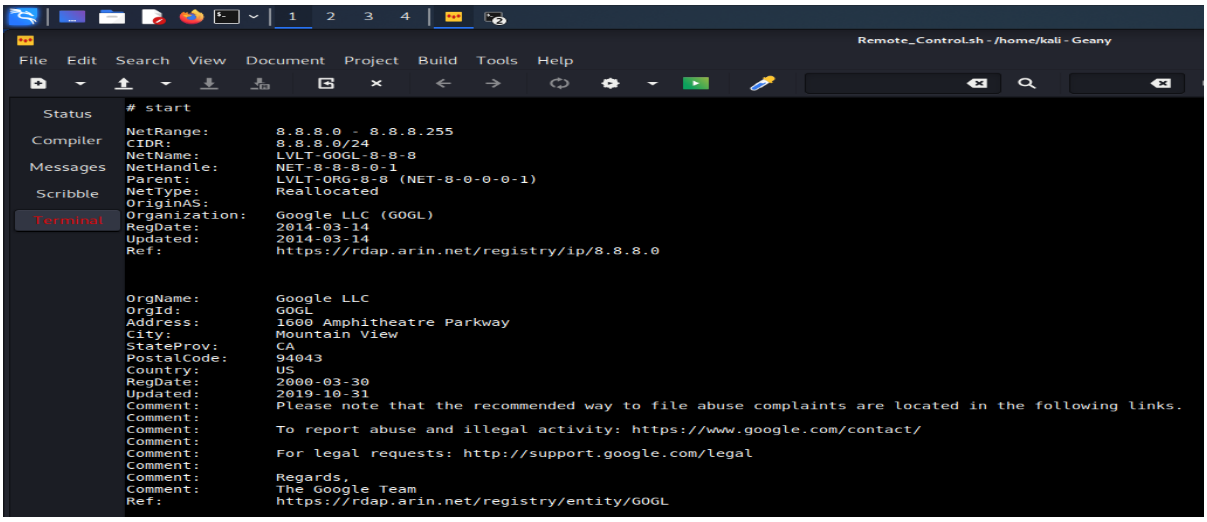
[Figure 3]

Following the format written in script, using ip 8.8.8.8 as default,

It will automatically SSH into a new terminal and do a nmap scan.

Scan for all open ports

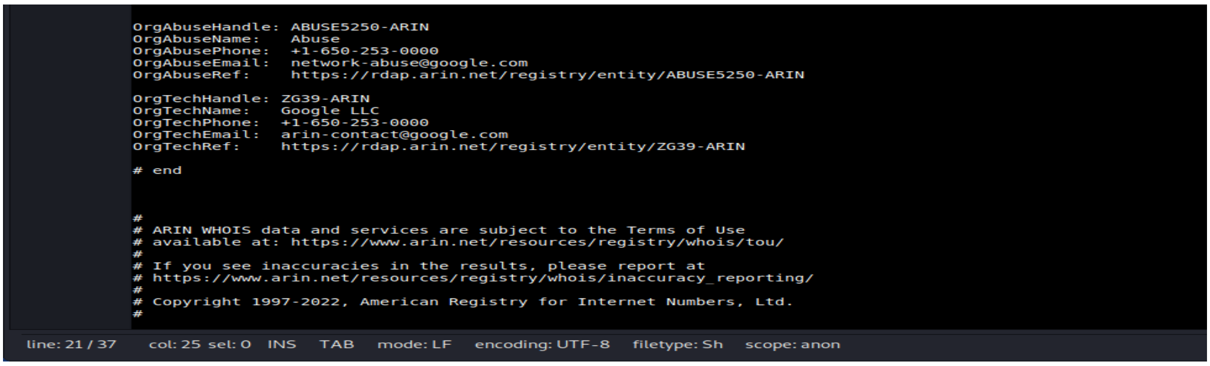
Whois scan



```
# start

NetRange:       8.8.8.0 - 8.8.8.255
CIDR:           8.8.8.0/24
NetName:        LVLT-GOGL-8-8-8
NetHandle:      NET-8-8-8-0-1
Parent:         LVLT-ORG-8-8 (NET-8-0-0-0-1)
NetType:        Reallocated
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2014-03-14
Updated:        2014-03-14
Ref:            https://rdap.arin.net/registry/ip/8.8.8.0


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL
```



```
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN

# end


#
# 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.
#
```

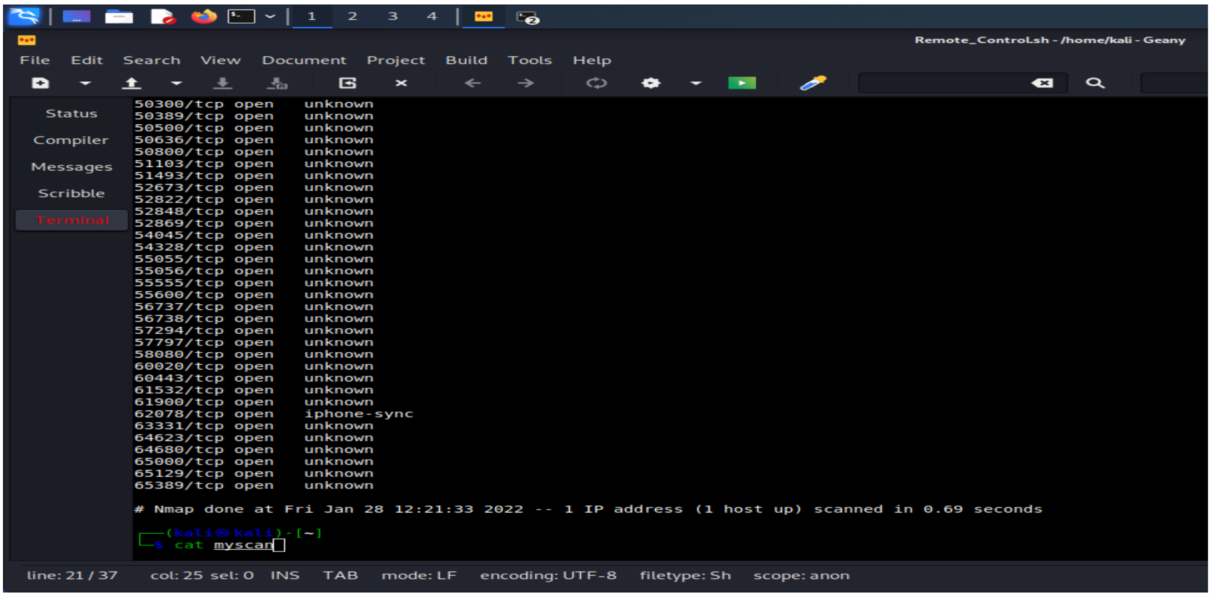
line: 21 / 37   col: 25 sel: 0   INS   TAB   mode: LF   encoding: UTF-8   filetype: Sh   scope: anon

[Figure 4]

Following the format written in script, using ip 8.8.8.8 as default,

It will automatically SSH into a new terminal and do a whois scan.

Found the company to be Google.



```
50300/tcp open   unknown
50389/tcp open   unknown
50500/tcp open   unknown
50636/tcp open   unknown
50800/tcp open   unknown
51103/tcp open   unknown
51493/tcp open   unknown
52673/tcp open   unknown
52822/tcp open   unknown
52848/tcp open   unknown
52869/tcp open   unknown
54045/tcp open   unknown
54328/tcp open   unknown
55055/tcp open   unknown
55056/tcp open   unknown
55555/tcp open   unknown
55600/tcp open   unknown
56737/tcp open   unknown
56738/tcp open   unknown
57294/tcp open   unknown
57797/tcp open   unknown
58080/tcp open   unknown
60020/tcp open   unknown
60443/tcp open   unknown
61532/tcp open   unknown
61900/tcp open   unknown
62078/tcp open   iphone-sync
63331/tcp open   unknown
64623/tcp open   unknown
64680/tcp open   unknown
65000/tcp open   unknown
65129/tcp open   unknown
65389/tcp open   unknown

# Nmap done at Fri Jan 28 12:21:33 2022 -- 1 IP address (1 host up) scanned in 0.69 seconds

┌──(kali㉿kali)-[~]
└─$ cat myscan
```

[Figure 5]

After Geany script is run successfully, save the output and run it on terminal.

Format: nmap -oN <file name> <localhost>

Used: nmap -oN myscan 8.8.8.8

Once saved, run cat myscan on terminal to see the output.

Success: Output shows all open port!