20.12.2022 Reut Klaider Levy

Network Research Script

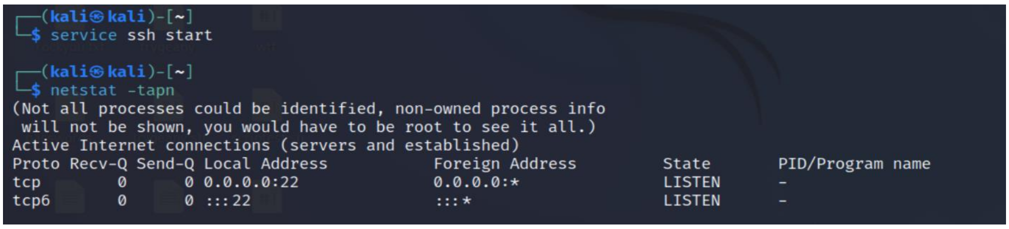
#This script will install needed tools,

#connect to remote server of your choose,

#will scan via nmap through the remote server for open ports on a given target.

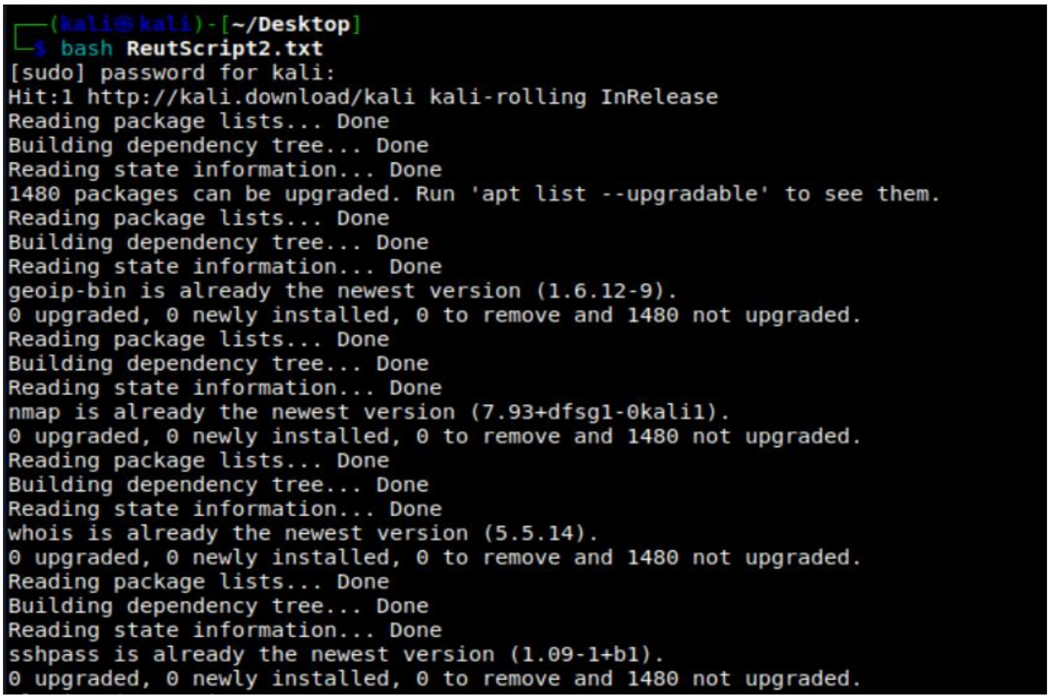
#Then the script will save all scanned data in a file, which you be able to read also on screen.

# First, we will open a clone and start ssh service, so we will have a remote server to connect to via ssh.



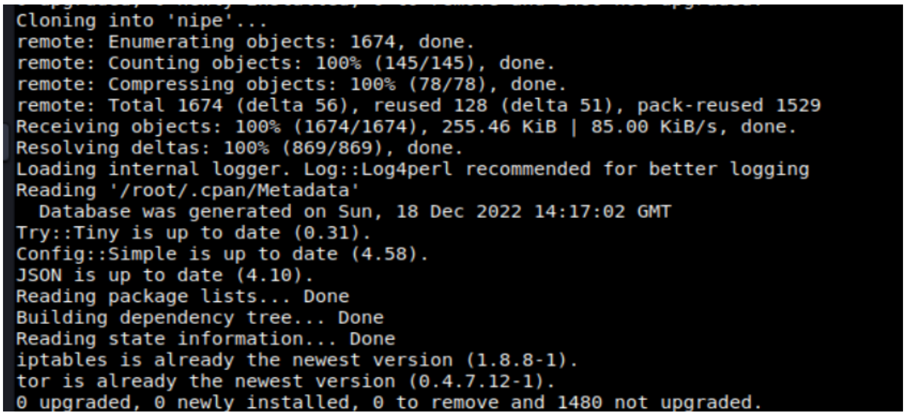
```
┌──(kali㉿kali)-[~]
└─$ service ssh start

┌──(kali㉿kali)-[~]
└─$ netstat -tapn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

# the script will install all needed tools with function INSTALL.



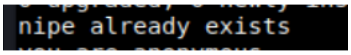
```
┌──(kali㉿kali)-[~/Desktop]
└─$ bash ReutScript2.txt
[sudo] password for kali:
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1480 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
geoip-bin is already the newest version (1.6.12-9).
0 upgraded, 0 newly installed, 0 to remove and 1480 not upgraded.
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 1480 not upgraded.
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 1480 not upgraded.
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 1480 not upgraded.
```

#Next, in same function - this script will check if you have NIPE tool installed, in case you don't - this function will install nipe tool on your machine.



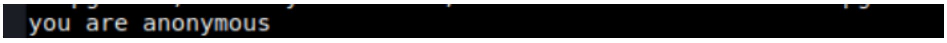
```
Cloning into 'nipe'...
remote: Enumerating objects: 1674, done.
remote: Counting objects: 100% (145/145), done.
remote: Compressing objects: 100% (78/78), done.
remote: Total 1674 (delta 56), reused 128 (delta 51), pack-reused 1529
Receiving objects: 100% (1674/1674), 255.46 KiB | 85.00 KiB/s, done.
Resolving deltas: 100% (869/869), done.
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Sun, 18 Dec 2022 14:17:02 GMT
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.10).
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.8-1).
tor is already the newest version (0.4.7.12-1).
0 upgraded, 0 newly installed, 0 to remove and 1480 not upgraded.
```

#In case nipe already exist – function will display



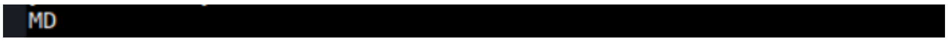
```
nipe already exists
```

#Next function – ANONYMOUSE - will start NIPE tool to make your connection anonymous. This function will check if nipe tool worked, if not – it will display "IL" and echo "You are not anonymous", if the tool work – the script will display "You are anonymous"



```
you are anonymous
```

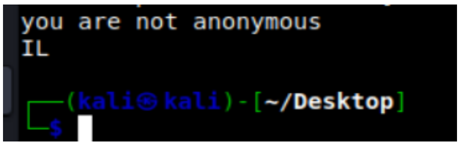
#Function ANONCOUNTRY will display which country your 'anonymous connect' connection.



```
MD
```

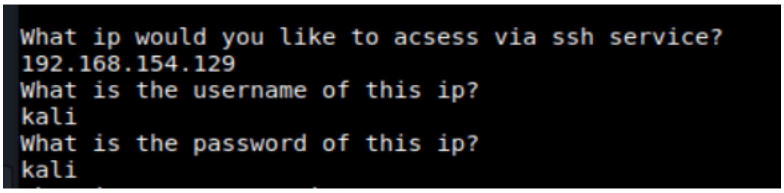
#Next function 'SSHDETAILS' will ask for needed details to access the remote server of your choose via ssh service. But it will only work if next function will be correct.

#function 'ILOREXIT' will check if your connection is anonymous – if so, the script will start function SSHDETAILS, if the connection is not anonymous – this function will display "IL" and exit script:



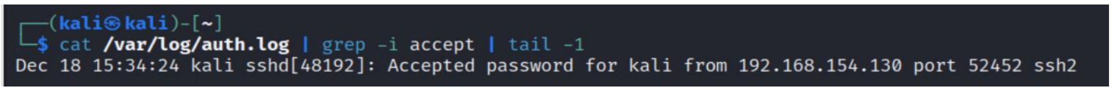
```
you are not anonymous
IL

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

#On shown case anonymous connection established, and SSHDETAILS function started, details were given.



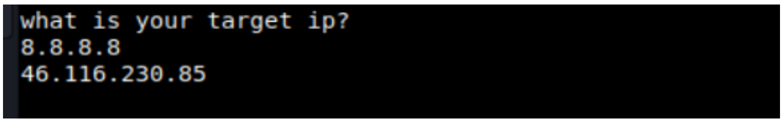
```
What ip would you like to acsess via ssh service?
192.168.154.129
What is the username of this ip?
kali
What is the password of this ip?
kali
```

#As you can see on the remote server – the connection is established



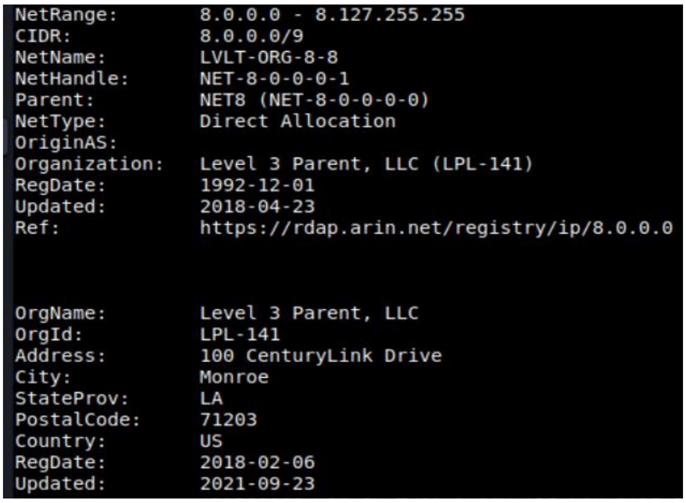
```
┌──(kali㉿kali)-[~]
└─$ cat /var/log/auth.log | grep -i accept | tail -1
Dec 18 15:34:24 kali sshd[48192]: Accepted password for kali from 192.168.154.130 port 52452 ssh2
```

#Function 'SSH1' will ask you for a target

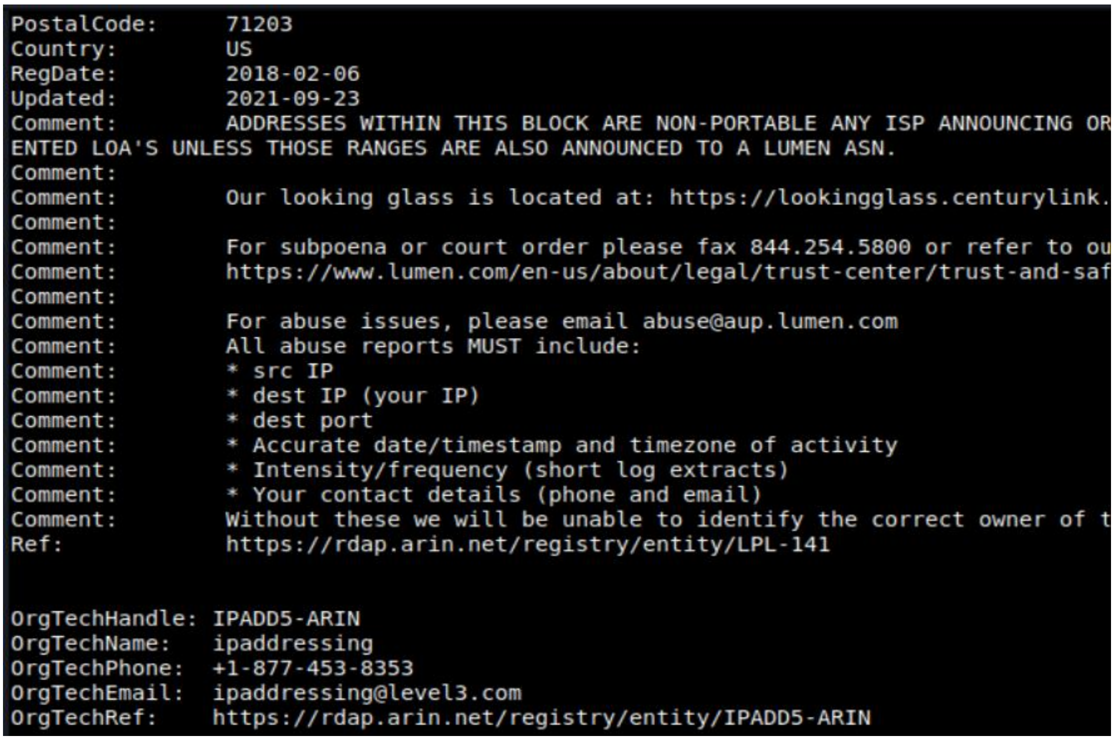


```
what is your target ip?
8.8.8.8
46.116.230.85
```

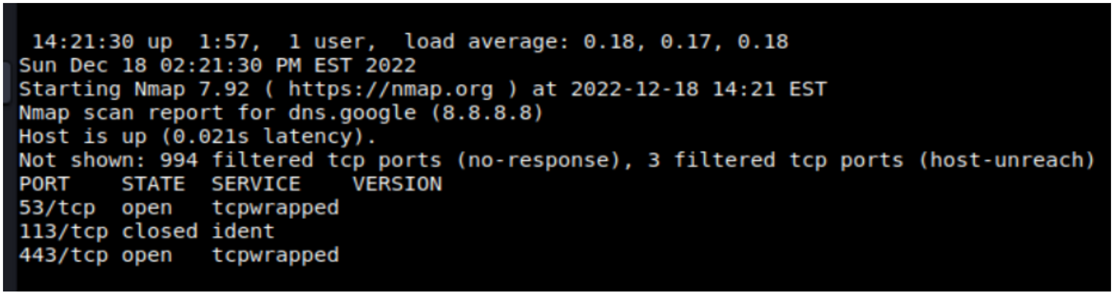
#As given a target the function 'SSH1' will scan that target for open ports via nmap tool through remote server, this function will also retrieve public ip, scan for who is your target, his Date info, time info and country info.



```
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
```



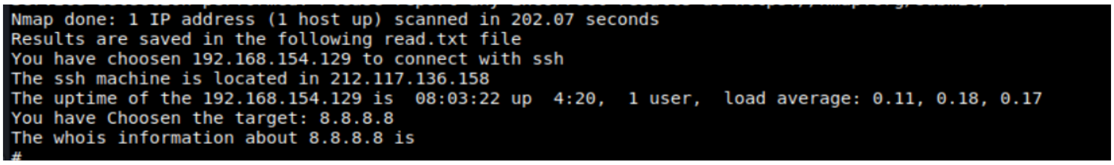
```
PostalCode:     71203
Country:        US
RegDate:        2018-02-06
Updated:        2021-09-23
Comment:        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE ANY ISP ANNOUNCING OR
ENTED LOA'S UNLESS THOSE RANGES ARE ALSO ANNOUNCED TO A LUMEN ASN.
Comment:
Comment:        Our looking glass is located at: https://lookingglass.centurylink.
Comment:
Comment:        For subpoena or court order please fax 844.254.5800 or refer to ou
Comment:        https://www.lumen.com/en-us/about/legal/trust-center/trust-and-saf
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 t
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
```



```
 14:21:30 up  1:57,  1 user,  load average: 0.18, 0.17, 0.18
Sun Dec 18 02:21:30 PM EST 2022
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-18 14:21 EST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.021s latency).
Not shown: 994 filtered tcp ports (no-response), 3 filtered tcp ports (host-unreach)
PORT    STATE  SERVICE    VERSION
53/tcp  open   tcpwrapped
113/tcp closed ident
443/tcp open   tcpwrapped
```

#On this 'SSH1' function all data displayed will be saved on host computer, and will be available from host computer in any given time.

#At the last function 'SSHREAD' – all data will save at a file named read.txt and all information will display on screen.



```
Nmap done: 1 IP address (1 host up) scanned in 202.07 seconds
Results are saved in the following read.txt file
You have choosen 192.168.154.129 to connect with ssh
The ssh machine is located in 212.117.136.158
The uptime of the 192.168.154.129 is  08:03:22 up  4:20,  1 user,  load average: 0.11, 0.18, 0.17
You have Choosen the target: 8.8.8.8
The whois information about 8.8.8.8 is
#
```

Hope you enjoyed my script.