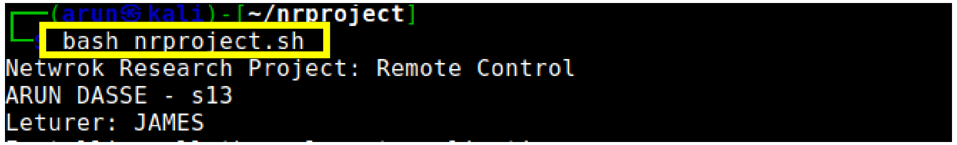
Network Research Project: Remote Control

ARUN DASSE - s13 - cfc2407
Lecturer name: James

Part1: Installing relevant applications (needed for the project) on the local computer

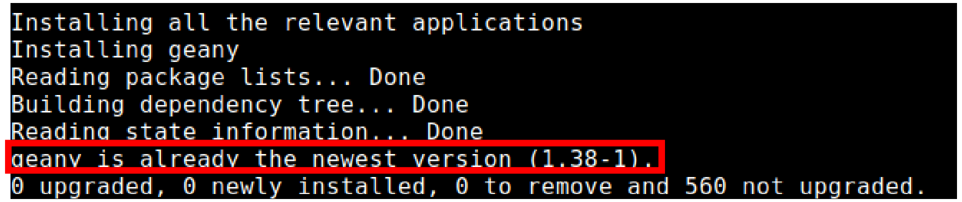
Note: Since all the applications are already installed on my Kali Linux,
when you do the command ‘sudo apt-get install <app/tool name>’ – it shows that it already installed

- used the bash cmd to run the nrproject.sh file



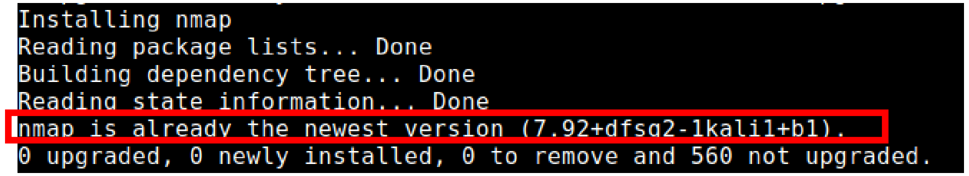
```
┌──(arun㉿kali)-[~/nrproject]
└─$ bash nrproject.sh
Netwrok Research Project: Remote Control
ARUN DASSE - s13
Leturer: JAMES
```

- Executed the command ‘sudo apt-get install geany’



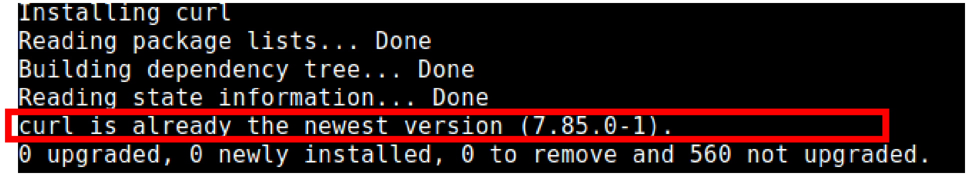
```
Installing all the relevant applications
Installing geany
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
geany is already the newest version (1.38-1).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

- Executed the command ‘sudo apt-get install nmap’



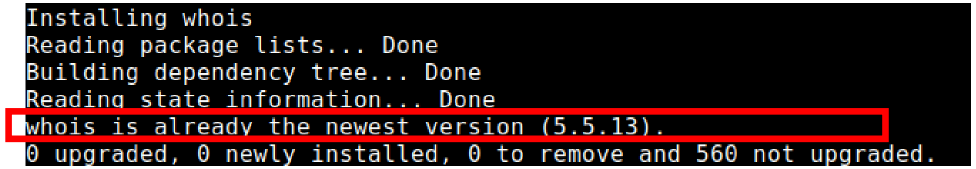
```
Installing nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.92+dfsg2-1kali1+b1).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

- Executed the command ‘sudo apt-get install curl’



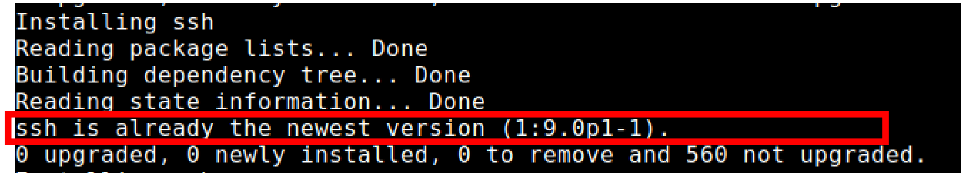
```
Installing curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.85.0-1).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

- Executed the command ‘sudo apt-get install whois’



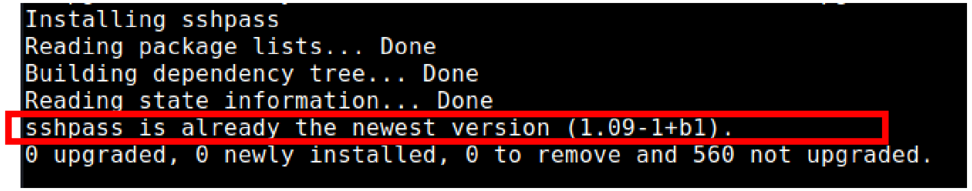
```
Installing whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.13).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

- Executed the command ‘sudo apt-get install ssh’



```
Installing ssh
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ssh is already the newest version (1:9.0p1-1).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

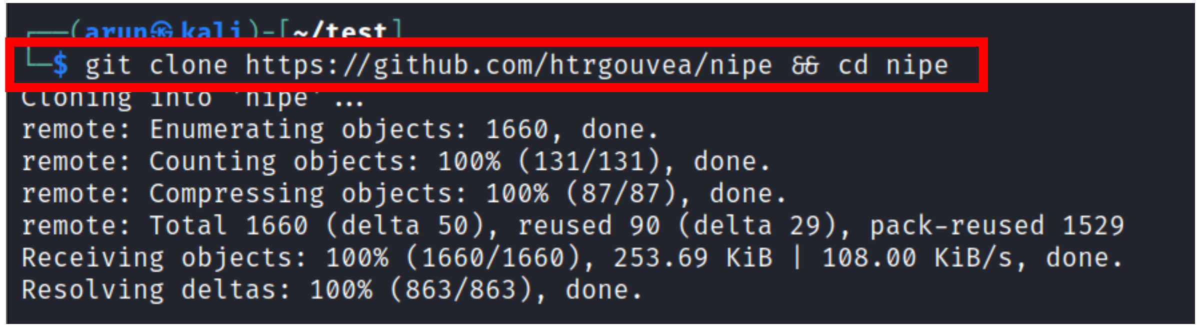
- Executed the command ‘sudo apt-get install sshpass’



```
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 560 not upgraded.
```

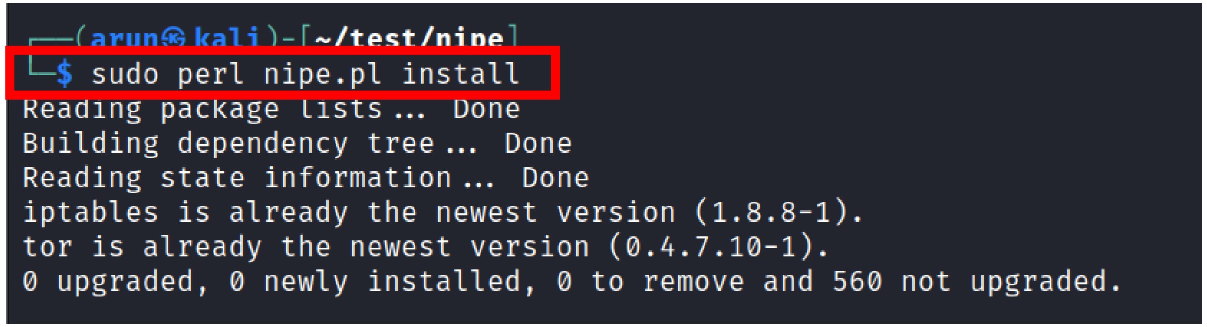
Part2a: Intall nipe to access TOR on the command line and scripting - [credit: https://github.com/htrgouvea/nipe]

- Download nipe from https://github.com/htrgouvea/nipe and move into the nipe directory



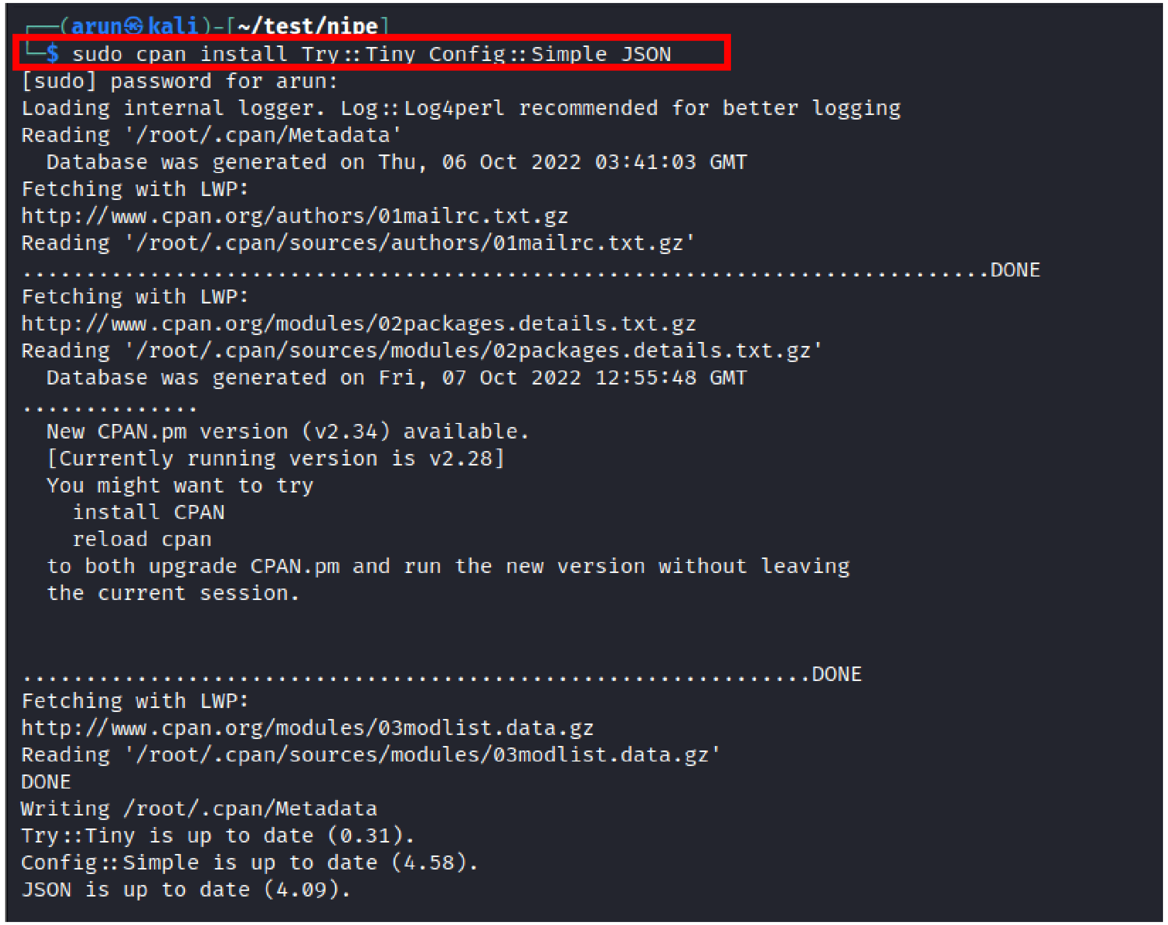
```
┌──(arun㉿kali)-[~/test]
└─$ git clone https://github.com/htrgouvea/nipe && cd nipe
Cloning into 'nipe'...
remote: Enumerating objects: 1660, done.
remote: Counting objects: 100% (131/131), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 1660 (delta 50), reused 90 (delta 29), pack-reused 1529
Receiving objects: 100% (1660/1660), 253.69 KiB | 108.00 KiB/s, done.
Resolving deltas: 100% (863/863), done.
```

- Nipe must be run as root, install the nipe.pl file



```
┌──(arun㉿kali)-[~/test/nipe]
└─$ sudo perl nipe.pl install
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 (0.4.7.10-1).
0 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
```

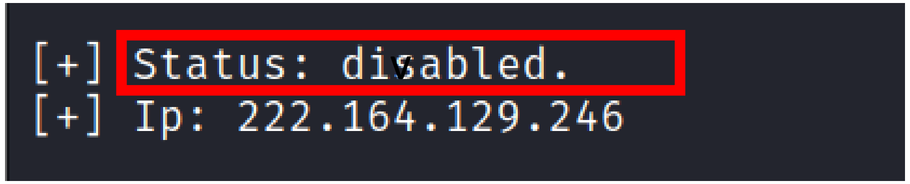
- Install libs and dependencies



```
┌──(arun㉿kali)-[~/test/nipe]
└─$ sudo cpan install Try::Tiny Config::Simple JSON
[sudo] password for arun:
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Thu, 06 Oct 2022 03:41:03 GMT
Fetching with LWP:
http://www.cpan.org/authors/01mailrc.txt.gz
Reading '/root/.cpan/sources/authors/01mailrc.txt.gz'
............................................................................DONE
Fetching with LWP:
http://www.cpan.org/modules/02packages.details.txt.gz
Reading '/root/.cpan/sources/modules/02packages.details.txt.gz'
  Database was generated on Fri, 07 Oct 2022 12:55:48 GMT
.............
  New CPAN.pm version (v2.34) available.
  [Currently running version is v2.28]
  You might want to try
    install CPAN
    reload cpan
  to both upgrade CPAN.pm and run the new version without leaving
  the current session.


..............................................................DONE
Fetching with LWP:
http://www.cpan.org/modules/03modlist.data.gz
Reading '/root/.cpan/sources/modules/03modlist.data.gz'
DONE
Writing /root/.cpan/Metadata
Try::Tiny is up to date (0.31).
Config::Simple is up to date (4.58).
JSON is up to date (4.09).
```

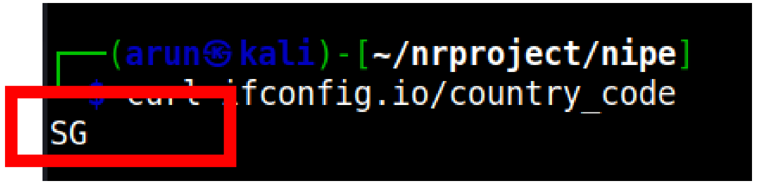
Part2b: To check if the connection is anonymous

- starting the nipe.pl service
- cmd: sudo perl nipe.pl start
- cmd: sudo perl nipe.pl status



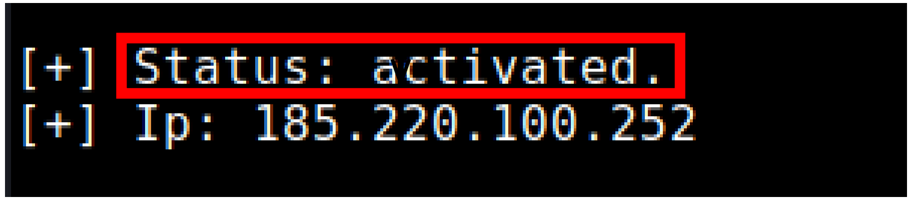
```
[+] Status: disabled.
[+] Ip: 222.164.129.246
```

- To check if the connection is anonymous/from the origin country
- cmd: curl ifconfig.io/country_code



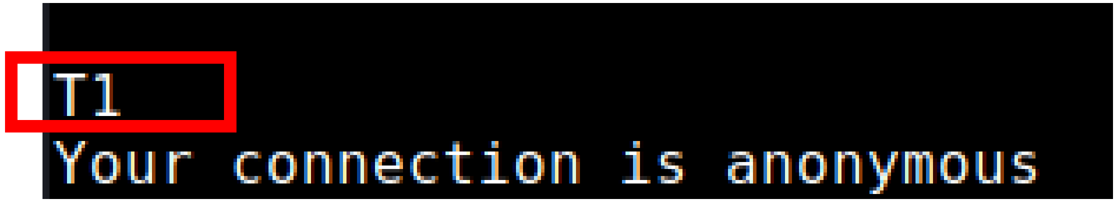
```
┌──(arun㉿kali)-[~/nrproject/nipe]
└─$ curl ifconfig.io/country_code
SG
```

- Restarting the nipe.pl service
- cmd: sudo perl nipe.pl restart
- cmd: sudo perl nipe.pl status



```
[+] Status: activated.
[+] Ip: 185.220.100.252
```

- To check if the connection is anonymous
- cmd: curl ifconfig.io/country_code

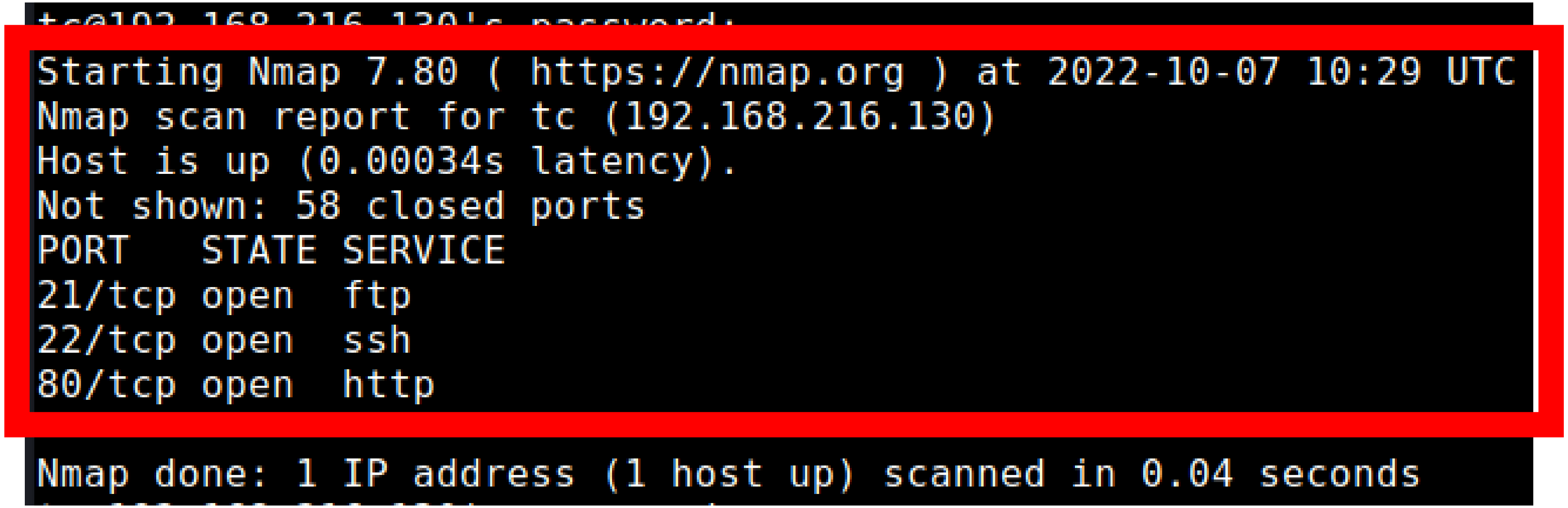


```
T1
Your connection is anonymous
```

Part3: Communicate via SSH / SSHPASS and execute nmap scans / masscan and whois/curl queries

cmd: `ssh tc@192.168.216.130 'nmap 192.168.216.130 -p20-80 -oN result1.txt’`

- ssh - ssh command provides a secure encrypted connection between the remote server (ubuntu) and the local machine
- tc – remote server username
- 192.168.216.130 – remote server ip address
- nmap – to scan the network
- 192.168.216.130 - remote server ip address
- -p20-80 – scan for the specific ports from 20 to 80
- -oN – normal way to save the nmap results, as how we see on the terminal
- result1.txt - save the nmap results in the result1.txt (filename)

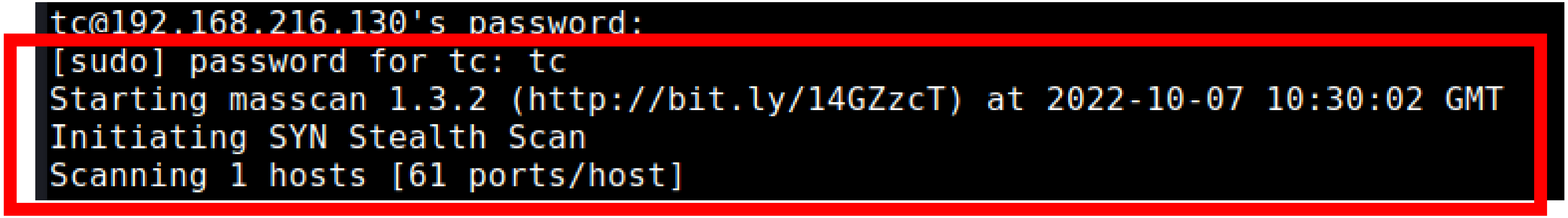


```
tc@192.168.216.130's password:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-07 10:29 UTC
Nmap scan report for tc (192.168.216.130)
Host is up (0.00034s latency).
Not shown: 58 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Part3: Communicate via SSH / SSHPASS and execute nmap scans / masscan and whois/curl queries

cmd: ssh tc@192.168.216.130 "sudo -S masscan 8.8.8.8 -p20-80 > result2.txt“

- ssh - ssh command provides a secure encrypted connection between the remote server (ubuntu) and the local machine
- tc – remote server username
- 192.168.216.130 – remote server ip address
- masscan – to scan the network
- 8.8.8.8 - ip address of a google.com
- -p20-80 – scan for the specific ports from 20 to 80
- result2.txt - save the masscan results in the result2.txt (filename)

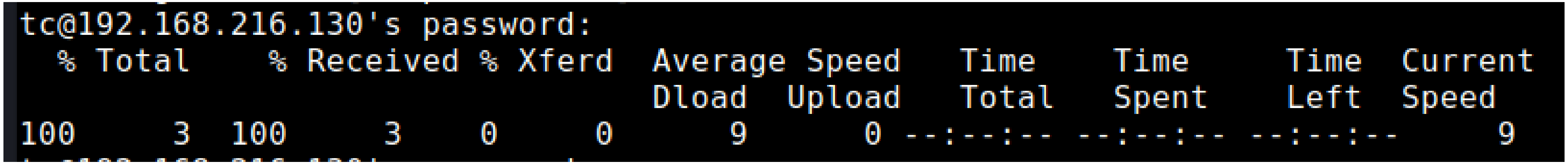


```
tc@192.168.216.130's password:
[sudo] password for tc: tc
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-10-07 10:30:02 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [61 ports/host]
```

Part3: Communicate via SSH / SSHPASS and execute nmap scans / masscan and whois/curl queries

cmd: `ssh tc@192.168.216.130 'curl ifconfig.io/country_code > result3.txt’`

- ssh - ssh command provides a secure encrypted connection between the remote server (ubuntu) and the local machine
- tc – remote server username
- 192.168.216.130 – remote server ip address
- curl ifconfig.io/country_code – this command line wil give the information of the origin country.
- result3.txt - save the results in the result3.txt (filename)

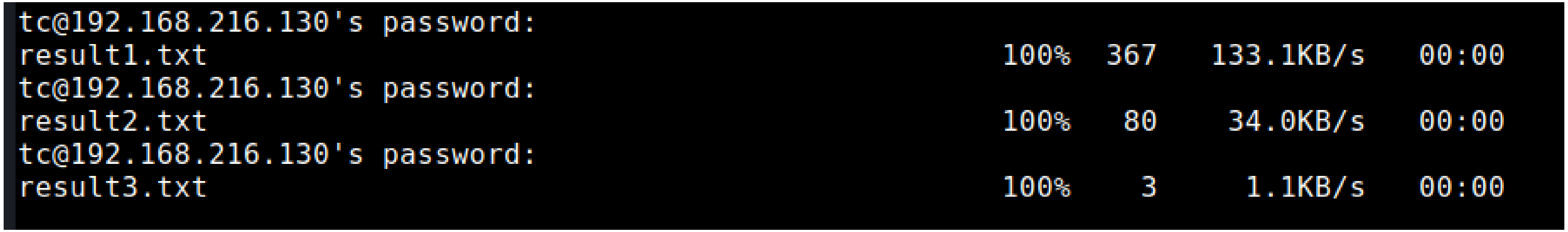


```
tc@192.168.216.130's password:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100     3  100     3    0     0      9      0 --:--:-- --:--:-- --:--:--     9
```

Part4a: Copy the scan result files from the remote server to the local computer using scp

```
cmd: scp tc@192.168.216.130:~/result1.txt ~/nrproject
cmd: scp tc@192.168.216.130:~/result2.txt ~/nrproject
cmd: scp tc@192.168.216.130:~/result3.txt ~/nrproject
```

- scp – (secure copy) is a command help you to securely copy files and directories between two locations.
- tc – userame (remote server)
- 192.168.216.130 – ipaddress of the remote server
- ~/result1.txt – file location
- ~/nrproject – destination

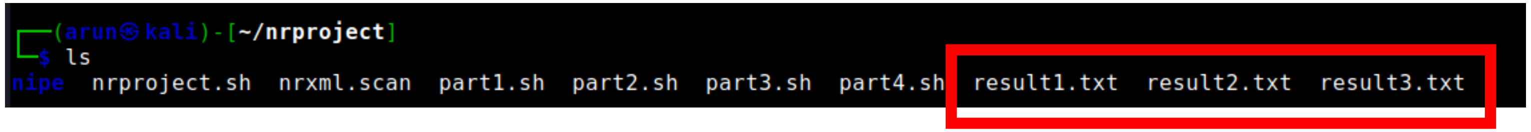


```
tc@192.168.216.130's password:
result1.txt                                          100%  367   133.1KB/s   00:00
tc@192.168.216.130's password:
result2.txt                                          100%   80    34.0KB/s   00:00
tc@192.168.216.130's password:
result3.txt                                          100%    3     1.1KB/s   00:00
```

Part4b: Make sure all the files has been copied to your local machine and read the files

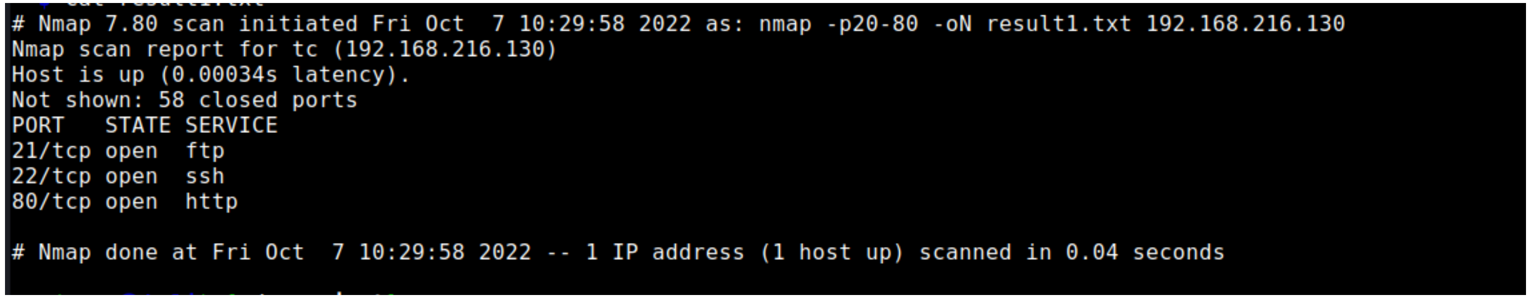
cmd: ls
cmd: cat result1.txt
cmd: cat result2.txt
cmd: cat result3.txt

- do ls command to checl all the files are located in the respective directory
- execute cat filename.extension to read the files



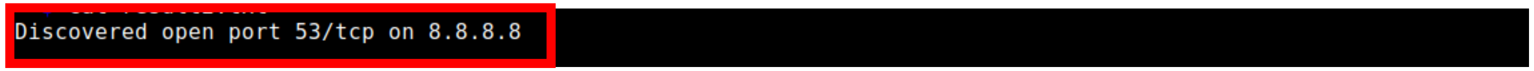
```
┌──(arun㉿kali)-[~/nrproject]
└─$ ls
nipe  nrproject.sh  nrxml.scan  part1.sh  part2.sh  part3.sh  part4.sh  result1.txt  result2.txt  result3.txt
```

All the three result files are copied into the local machine



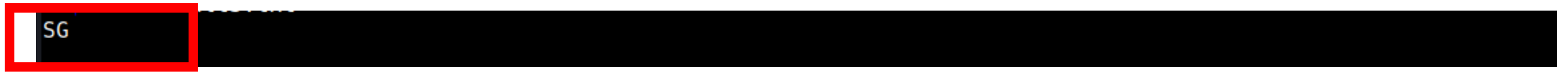
```
# Nmap 7.80 scan initiated Fri Oct  7 10:29:58 2022 as: nmap -p20-80 -oN result1.txt 192.168.216.130
Nmap scan report for tc (192.168.216.130)
Host is up (0.00034s latency).
Not shown: 58 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

# Nmap done at Fri Oct  7 10:29:58 2022 -- 1 IP address (1 host up) scanned in 0.04 seconds
```

Nmap scan – result1.txt



```
Discovered open port 53/tcp on 8.8.8.8
```

Masscan – result2.txt



```
SG
```

curl ifconfig.io/country_code – result3.txt