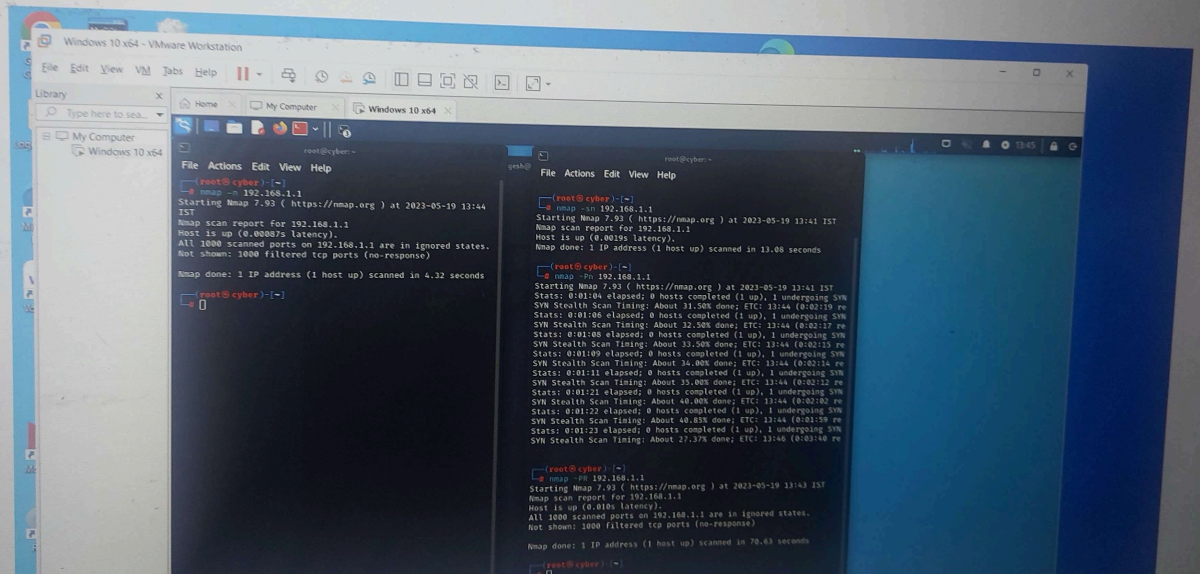
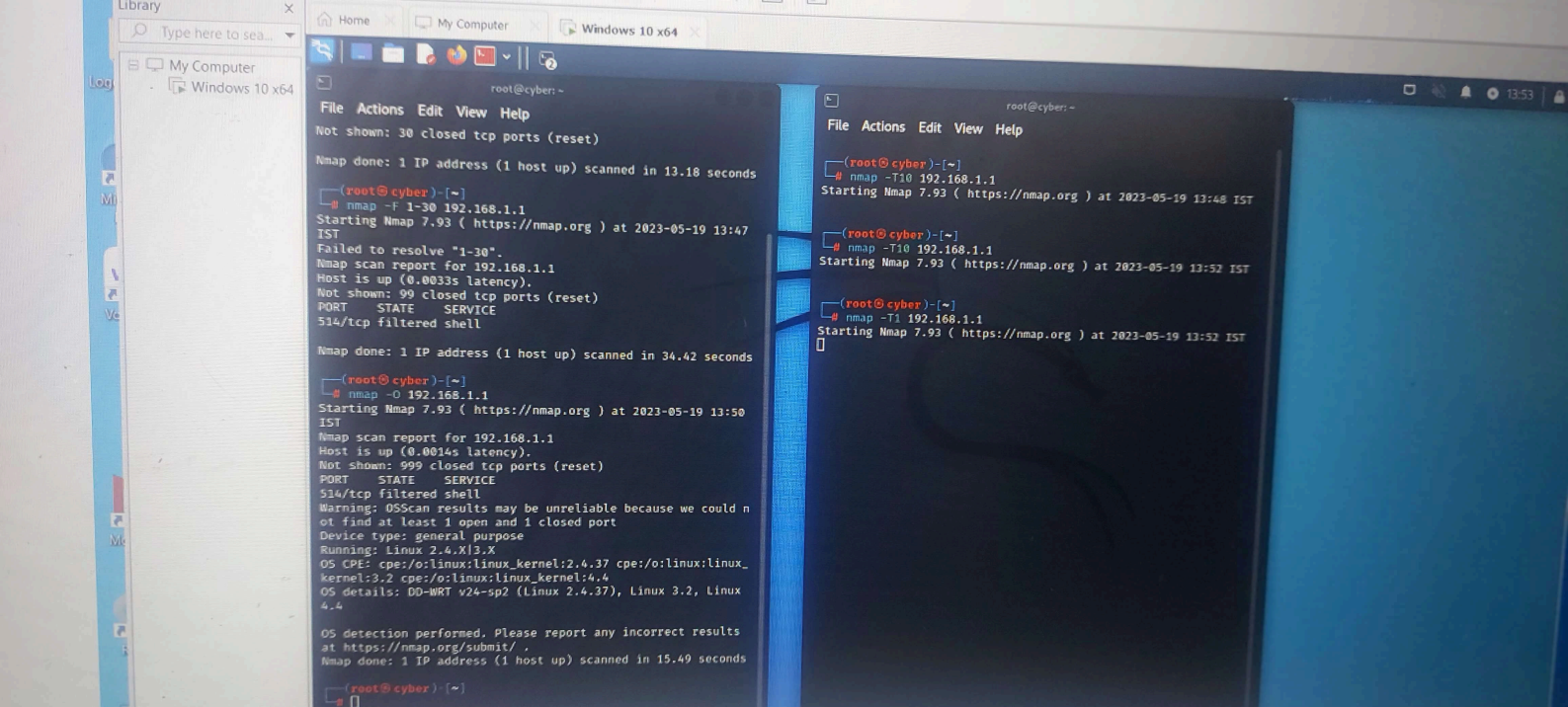
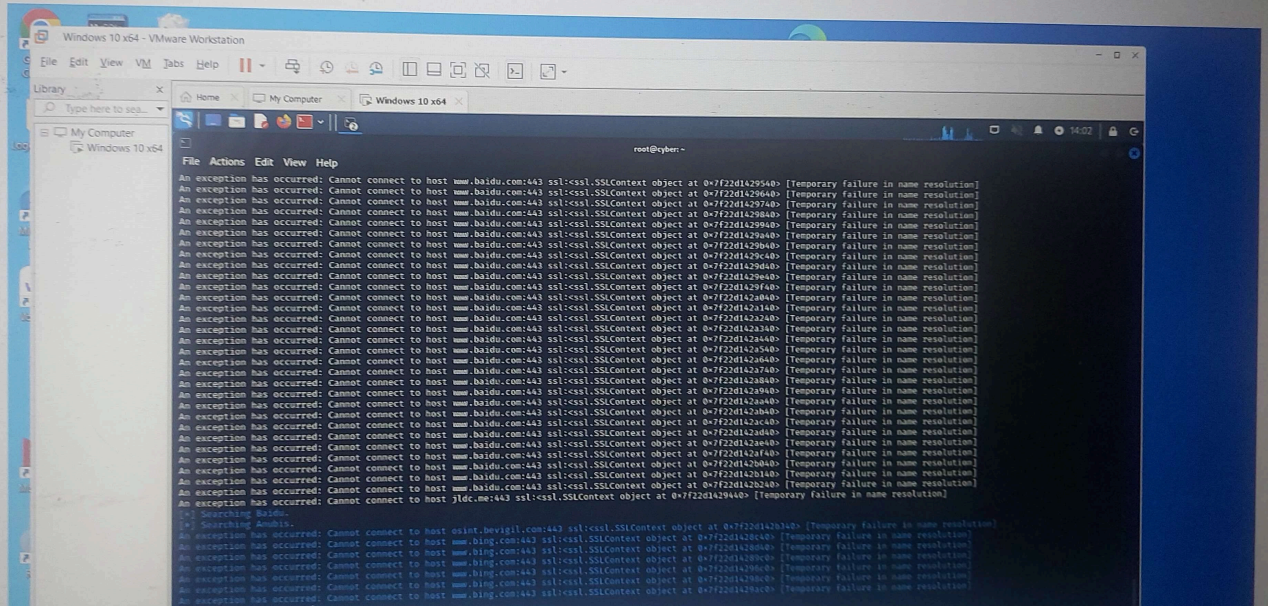
1. network map sacnning

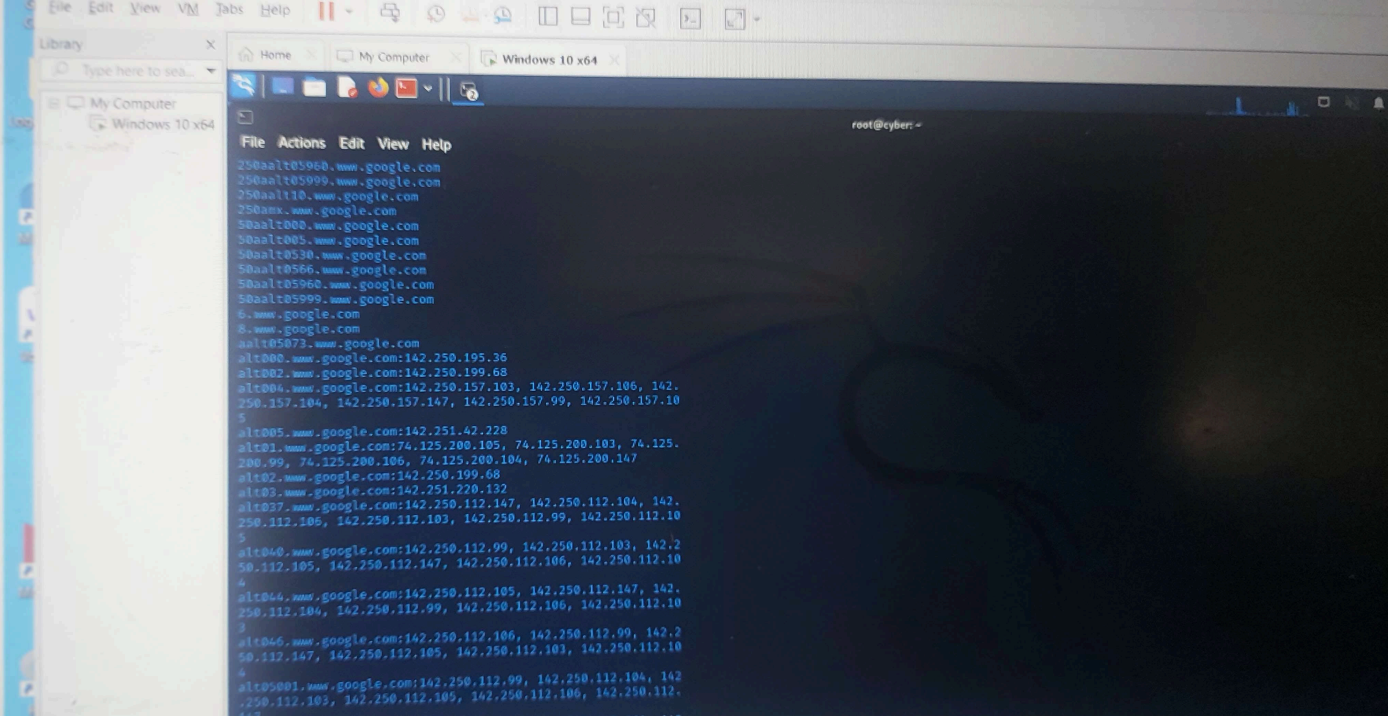


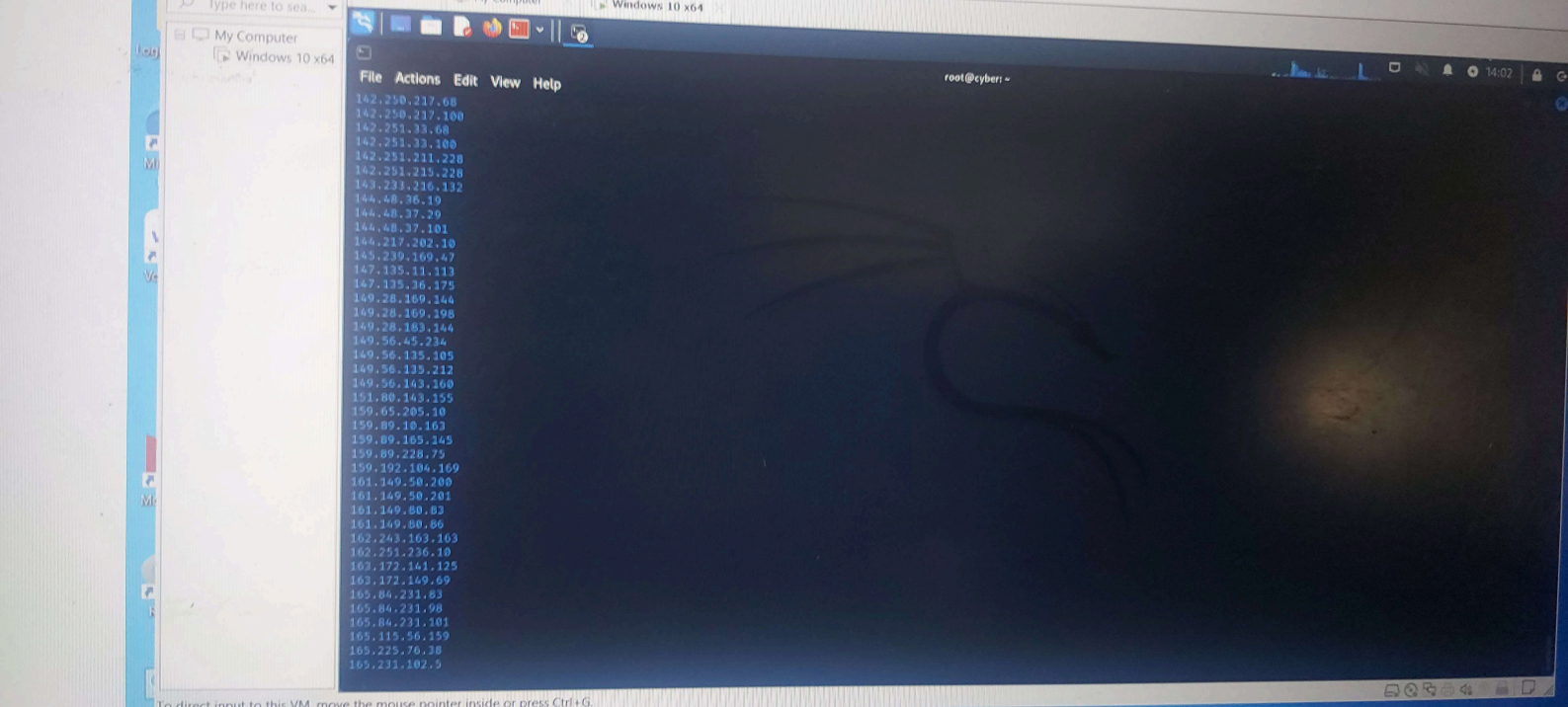

Library
Type here to sea...
My Computer
Windows 10 x64
Home
My Computer
Windows 10 x64
root@cyber: ~
File Actions Edit View Help
Not shown: 30 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
(root㉿cyber)-[~]
nmap -F 1-30 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-05-19 13:47 IST
Failed to resolve "1-30".
Nmap scan report for 192.168.1.1
Host is up (0.0033s latency).
Not shown: 99 closed tcp ports (reset)
PORT STATE SERVICE
514/tcp filtered shell
Nmap done: 1 IP address (1 host up) scanned in 34.42 seconds
(root㉿cyber)-[~]
nmap -O 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-05-19 13:50 IST
Nmap scan report for 192.168.1.1
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
(root㉿cyber)-[~]
#
root@cyber: ~
File Actions Edit View Help
(root㉿cyber)-[~]
nmap -T10 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-05-19 13:48 IST
(root㉿cyber)-[~]
nmap -T10 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-05-19 13:52 IST
(root㉿cyber)-[~]
nmap -T1 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-05-19 13:52 IST
13:53

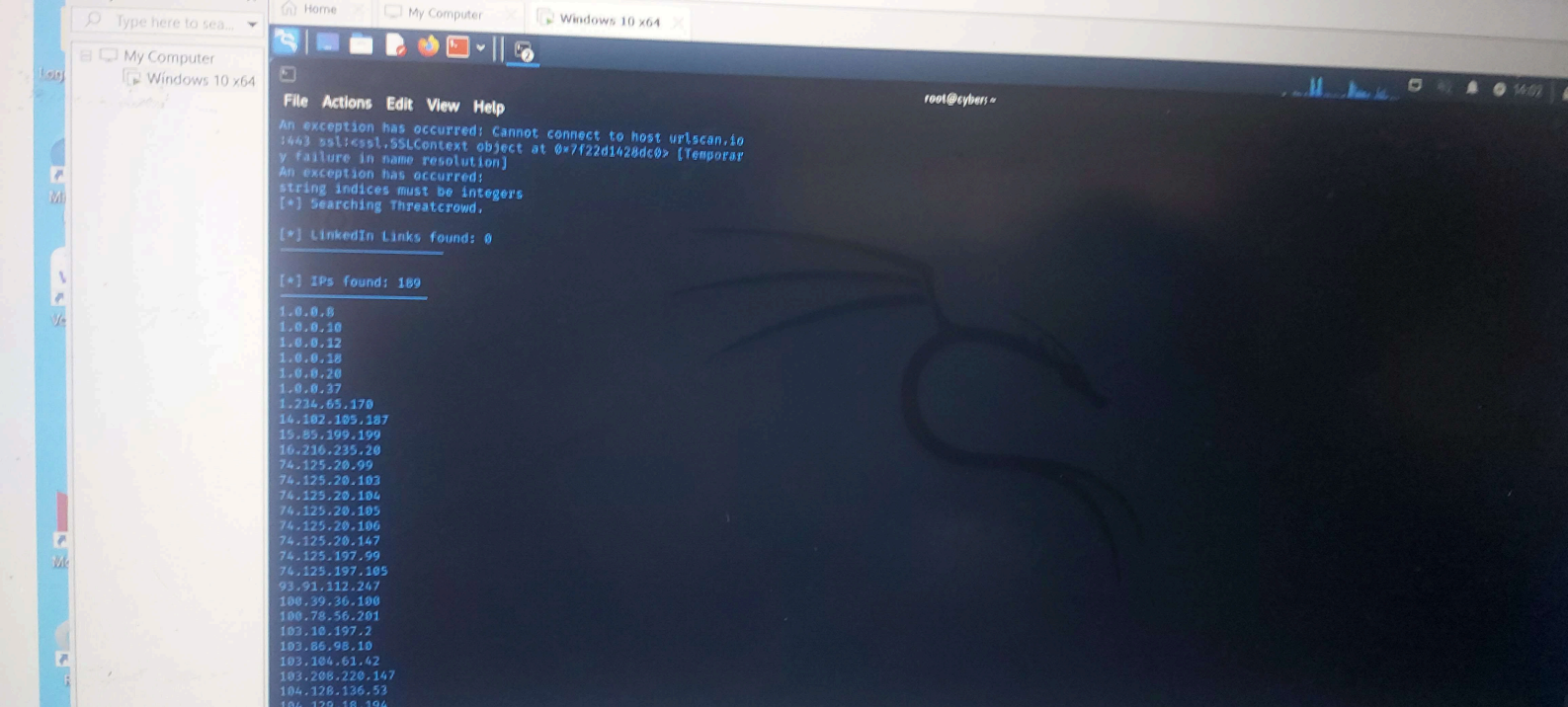
5. information gathering



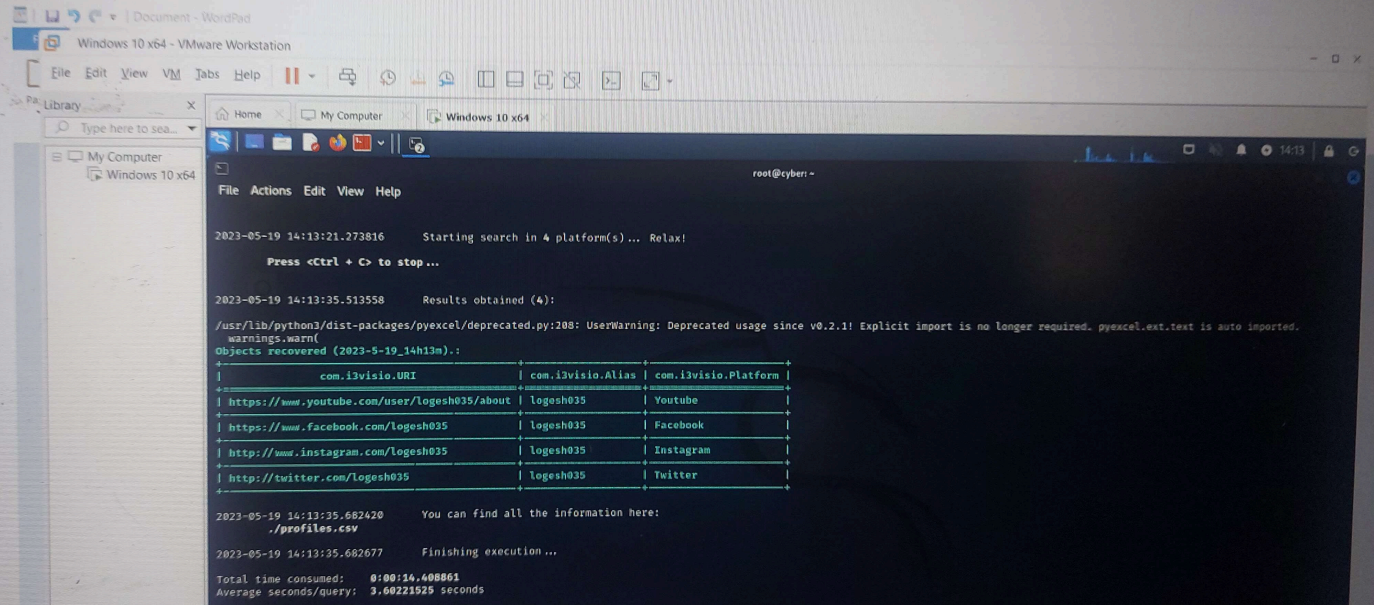
```
alt0541.www.google.com:142.250.112.105, 142.250.112.99, 142.
250.112.103, 142.250.112.147, 142.250.112.104, 142.250.112.1
06
alt0543.www.google.com:142.250.112.147, 142.250.112.99, 142.
250.112.105, 142.250.112.103, 142.250.112.104, 142.250.112.1
06
alt0553.www.google.com:142.250.112.106, 142.250.112.103, 142
.250.112.105, 142.250.112.99, 142.250.112.104, 142.250.112.1
47
alt05554.www.google.com:142.250.112.104, 142.250.112.147, 14
2.250.112.106, 142.250.112.105, 142.250.112.99, 142.250.112.
103
alt05556.www.google.com:142.250.112.147, 142.250.112.106, 14
2.250.112.105, 142.250.112.99, 142.250.112.103, 142.250.112.
104
alt0566.www.google.com:142.250.112.147, 142.250.112.106, 142
.250.112.103, 142.250.112.105, 142.250.112.99, 142.250.112.1
04
alt05960.www.google.com:142.250.112.104, 142.250.112.105, 14
2.250.112.99, 142.250.112.106, 142.250.112.147, 142.250.112.
103
alt05999.www.google.com:142.250.112.103, 142.250.112.99, 142
.250.112.105, 142.250.112.147, 142.250.112.104, 142.250.112.
106
alt10.www.google.com:142.250.188.4
alt953.www.google.com:142.250.112.99, 142.250.112.105, 142.2
50.112.103, 142.250.112.147, 142.250.112.104, 142.250.112.10
6
anuncios.www.google.com
eg.www.google.com
go.www.google.com
https.www.google.com
lt05071.www.google.com
mx.www.google.com
noticias.www.google.com
search.www.google.com
ubs.com.www.google.com
www.www.google.com

┌──(root㉿cyber)-[~]
```

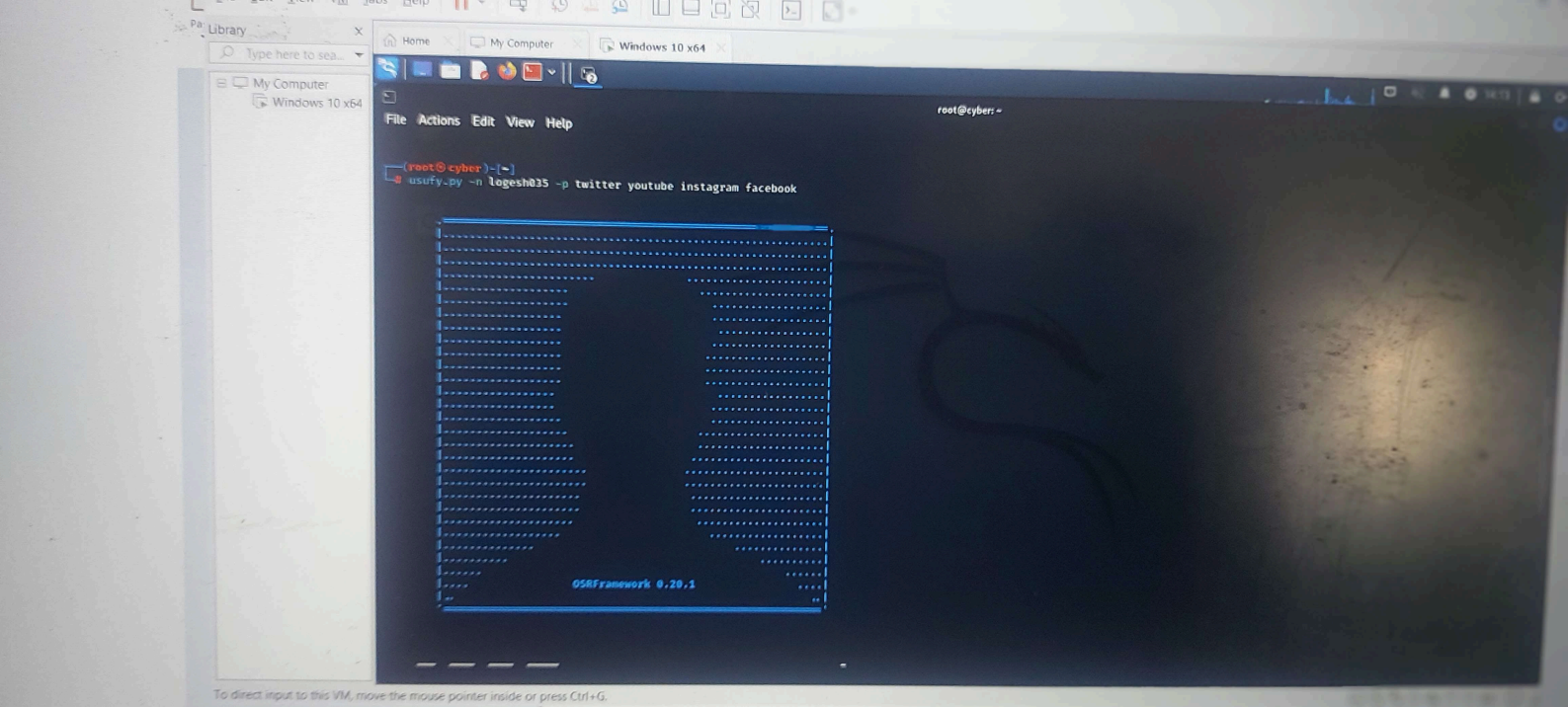

File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Home
My Computer
Windows 10 x64
root@cyber: ~
File Actions Edit View Help
250aalt05960.www.google.com
250aalt05999.www.google.com
250aalt10.www.google.com
250amx.www.google.com
50aalt000.www.google.com
50aalt005.www.google.com
50aalt0530.www.google.com
50aalt0566.www.google.com
50aalt05960.www.google.com
50aalt05999.www.google.com
6.www.google.com
8.www.google.com
aalt05073.www.google.com
alt000.www.google.com:142.250.195.36
alt002.www.google.com:142.250.199.68
alt004.www.google.com:142.250.157.103, 142.250.157.106, 142.
250.157.104, 142.250.157.147, 142.250.157.99, 142.250.157.10
5
alt005.www.google.com:142.251.42.228
alt01.www.google.com:74.125.200.105, 74.125.200.103, 74.125.
200.99, 74.125.200.106, 74.125.200.104, 74.125.200.147
alt02.www.google.com:142.250.199.68
alt03.www.google.com:142.251.220.132
alt037.www.google.com:142.250.112.147, 142.250.112.104, 142.
250.112.106, 142.250.112.103, 142.250.112.99, 142.250.112.10
5
alt040.www.google.com:142.250.112.99, 142.250.112.103, 142.2
50.112.105, 142.250.112.147, 142.250.112.106, 142.250.112.10
4
alt044.www.google.com:142.250.112.105, 142.250.112.147, 142.
250.112.104, 142.250.112.99, 142.250.112.106, 142.250.112.10
3
alt046.www.google.com:142.250.112.106, 142.250.112.99, 142.2
50.112.147, 142.250.112.105, 142.250.112.103, 142.250.112.10
4
alt05001.www.google.com:142.250.112.99, 142.250.112.104, 142
.250.112.103, 142.250.112.105, 142.250.112.106, 142.250.112.


Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
File Actions Edit View Help
root@cyber: ~
14:02
142.250.217.68
142.250.217.100
142.251.33.68
142.251.33.100
142.251.211.228
142.251.215.228
143.233.216.132
144.48.36.19
144.48.37.29
144.48.37.101
144.217.202.10
145.239.169.47
147.135.11.113
147.135.36.175
149.28.169.144
149.28.169.198
149.28.183.144
149.56.45.234
149.56.135.105
149.56.135.212
149.56.143.160
151.80.143.155
159.65.205.10
159.89.10.163
159.89.165.145
159.89.228.75
159.192.104.169
161.149.50.200
161.149.50.201
161.149.80.83
161.149.80.86
162.243.163.163
162.251.236.10
163.172.141.125
163.172.149.69
165.84.231.83
165.84.231.98
165.84.231.101
165.115.56.159
165.225.76.38
165.231.102.5
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

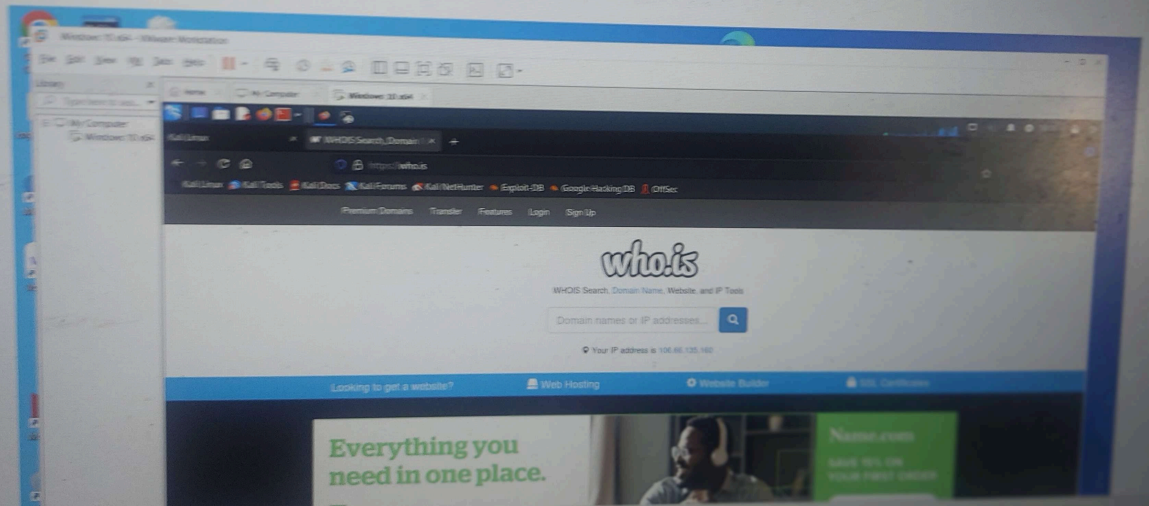

Type here to sea...
My Computer
Windows 10 x64
Home
My Computer
Windows 10 x64
File Actions Edit View Help
root@cybers: ~
An exception has occurred: Cannot connect to host urlscan.io
:443 ssl:<ssl.SSLContext object at 0x7f22d1428dc0> [Temporar
y failure in name resolution]
An exception has occurred:
string indices must be integers
[*] Searching Threatcrowd.
[*] LinkedIn Links found: 0
[*] IPs found: 189
1.0.0.8
1.0.0.10
1.0.0.12
1.0.0.18
1.0.0.20
1.0.0.37
1.234.65.170
14.102.105.187
15.85.199.199
16.216.235.20
74.125.20.99
74.125.20.103
74.125.20.104
74.125.20.105
74.125.20.106
74.125.20.147
74.125.197.99
74.125.197.105
93.91.112.247
100.39.36.100
100.78.56.201
103.10.197.2
103.86.98.10
103.104.61.42
103.208.220.147
104.128.136.53

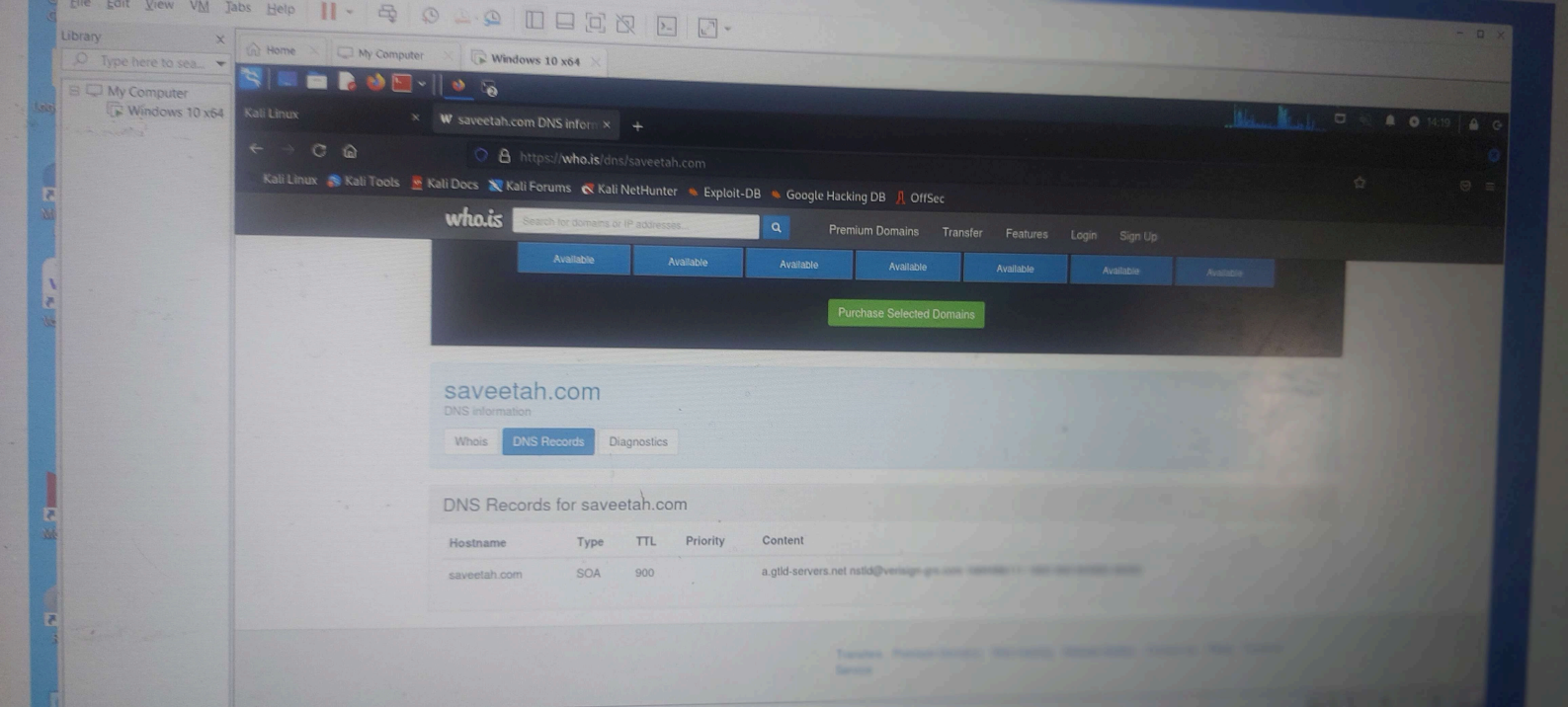
6. open source inteligence




Library
Type here to sea...
My Computer
Windows 10 x64
Home
My Computer
Windows 10 x64
File Actions Edit View Help
root@cyber: ~
root㉿cyber)-[~]
usufy.py -n logesh035 -p twitter youtube instagram facebook
OSRFramework 0.20.1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

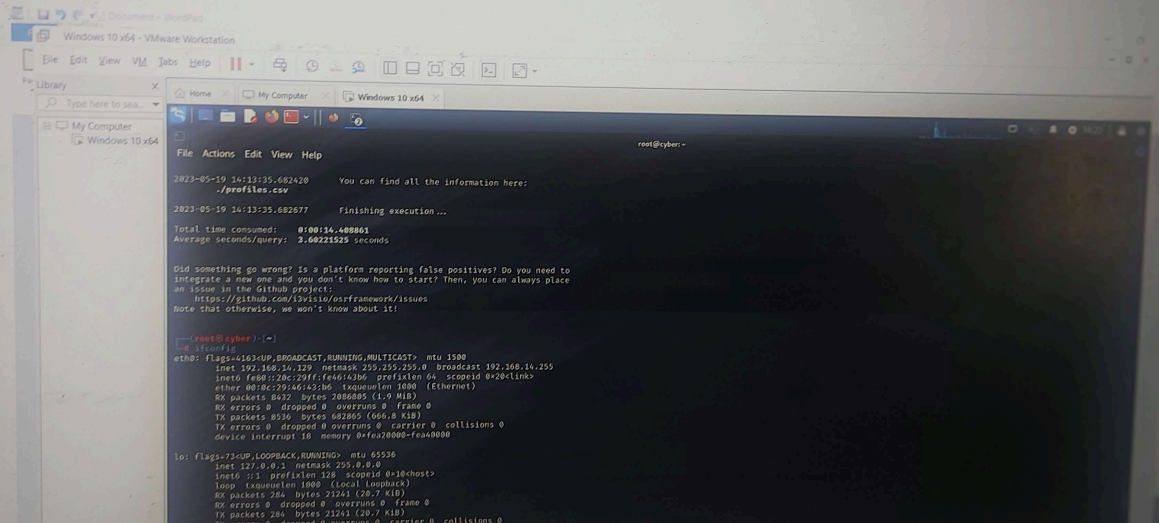
7 . use google whois for reconnaiasance



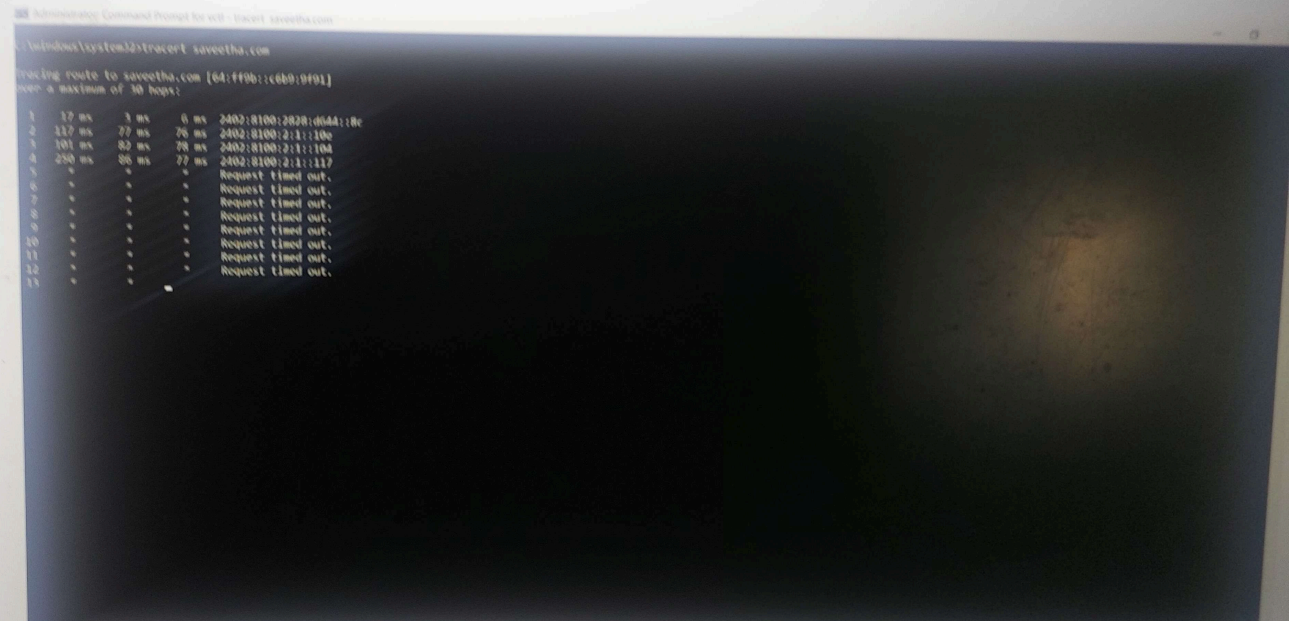

File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Home
My Computer
Windows 10 x64
Kali Linux
saveetah.com DNS inform
https://who.is/dns/saveetah.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
who.is
Search for domains or IP addresses...
Premium Domains Transfer Features Login Sign Up
Available Available Available Available Available Available Available
Purchase Selected Domains
saveetah.com
DNS information
Whois DNS Records Diagnostics
DNS Records for saveetah.com
Hostname Type TTL Priority Content
saveetah.com SOA 900
a.gtld-servers.net

8. tracert , pin g ,ipconfig if config

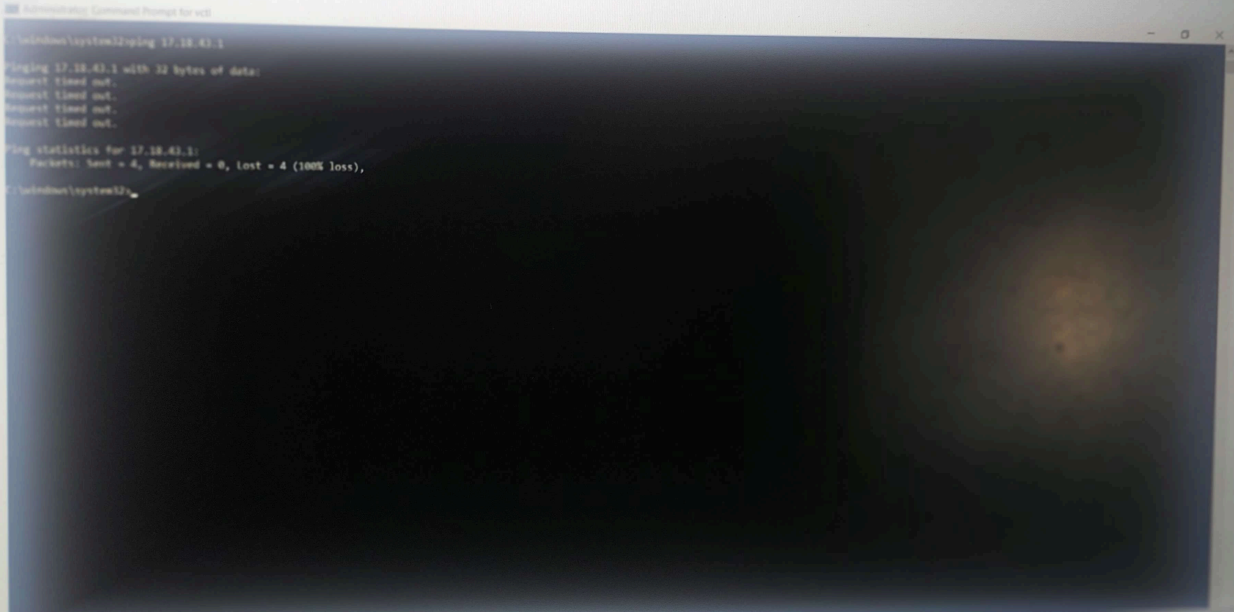
ifconfig



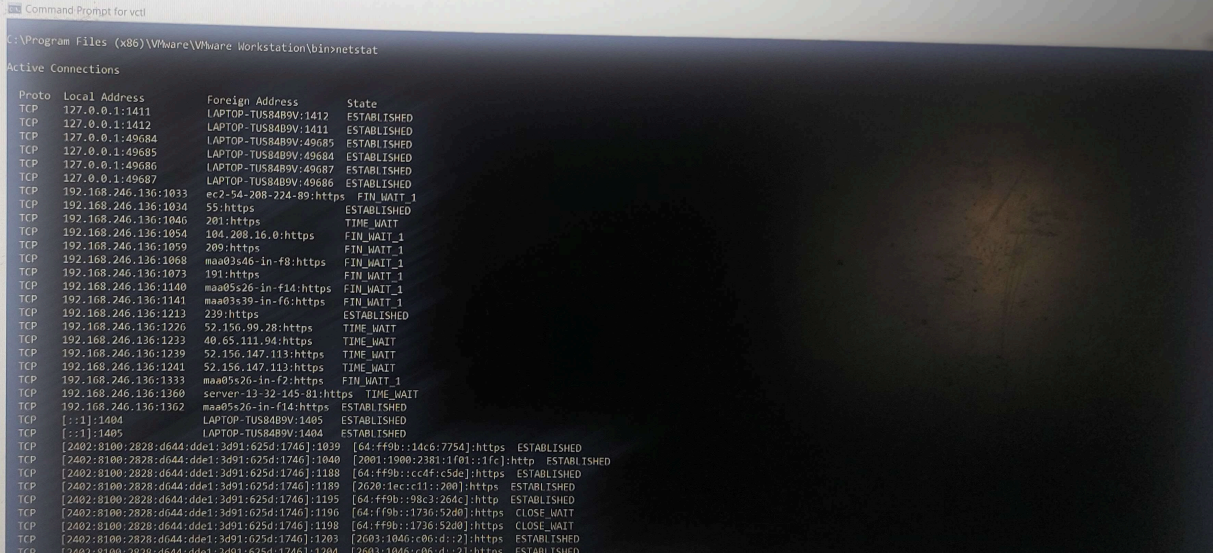
tracert


Administrator: Command Prompt for vcll - tracert saveetha.com
C:\Windows\system32>tracert saveetha.com
Tracing route to saveetha.com [64:ff9b::c6b9:9f01]
over a maximum of 30 hops:
1 17 ms 3 ms 6 ms 2402:8100:2828:d644::8c
2 117 ms 77 ms 76 ms 2402:8100:2:1::10e
3 101 ms 82 ms 78 ms 2402:8100:2:1::104
4 250 ms 86 ms 77 ms 2402:8100:2:1::117
5 * * * Request timed out.
6 * * * Request timed out.
7 * * * Request timed out.
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 * * * Request timed out.
12 * * * Request timed out.
13 * * *

ping


Administrator: Command Prompt for vcll
C:\windows\system32>ping 17.18.43.1
Pinging 17.18.43.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 17.18.43.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\windows\system32>

netstat



Command Prompt for vctl

```
C:\Program Files (x86)\VMware\VMware Workstation\bin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1411         LAPTOP-TUS84B9V:1412   ESTABLISHED
  TCP    127.0.0.1:1412         LAPTOP-TUS84B9V:1411   ESTABLISHED
  TCP    127.0.0.1:49684        LAPTOP-TUS84B9V:49685  ESTABLISHED
  TCP    127.0.0.1:49685        LAPTOP-TUS84B9V:49684  ESTABLISHED
  TCP    127.0.0.1:49686        LAPTOP-TUS84B9V:49687  ESTABLISHED
  TCP    127.0.0.1:49687        LAPTOP-TUS84B9V:49686  ESTABLISHED
  TCP    192.168.246.136:1033   ec2-54-208-224-89:https  FIN_WAIT_1
  TCP    192.168.246.136:1034   55:https               ESTABLISHED
  TCP    192.168.246.136:1046   201:https              TIME_WAIT
  TCP    192.168.246.136:1054   104.208.16.0:https     FIN_WAIT_1
  TCP    192.168.246.136:1059   209:https              FIN_WAIT_1
  TCP    192.168.246.136:1068   maa03s46-in-f8:https   FIN_WAIT_1
  TCP    192.168.246.136:1073   191:https              FIN_WAIT_1
  TCP    192.168.246.136:1140   maa05s26-in-f14:https  FIN_WAIT_1
  TCP    192.168.246.136:1141   maa03s39-in-f6:https   FIN_WAIT_1
  TCP    192.168.246.136:1213   239:https              ESTABLISHED
  TCP    192.168.246.136:1226   52.156.99.28:https     TIME_WAIT
  TCP    192.168.246.136:1233   40.65.111.94:https     TIME_WAIT
  TCP    192.168.246.136:1239   52.156.147.113:https   TIME_WAIT
  TCP    192.168.246.136:1241   52.156.147.113:https   TIME_WAIT
  TCP    192.168.246.136:1333   maa05s26-in-f2:https   FIN_WAIT_1
  TCP    192.168.246.136:1360   server-13-32-145-81:https  TIME_WAIT
  TCP    192.168.246.136:1362   maa05s26-in-f14:https  ESTABLISHED
  TCP    [::1]:1404             LAPTOP-TUS84B9V:1405   ESTABLISHED
  TCP    [::1]:1405             LAPTOP-TUS84B9V:1404   ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1039  [64:ff9b::14c6:7754]:https  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1040  [2001:1900:2381:1f01::1fc]:http  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1188  [64:ff9b::cc4f:c5de]:https  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1189  [2620:1ec:c11::200]:https  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1195  [64:ff9b::98c3:264c]:http  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1196  [64:ff9b::1736:52d0]:https  CLOSE_WAIT
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1198  [64:ff9b::1736:52d0]:https  CLOSE_WAIT
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1203  [2603:1046:c06:d::2]:https  ESTABLISHED
  TCP    [2402:8100:2828:d644:dde1:3d91:625d:1746]:1204  [2603:1046:c06:d::2]:https  ESTABLISHED
```

9. vulnerability cgi scanning