

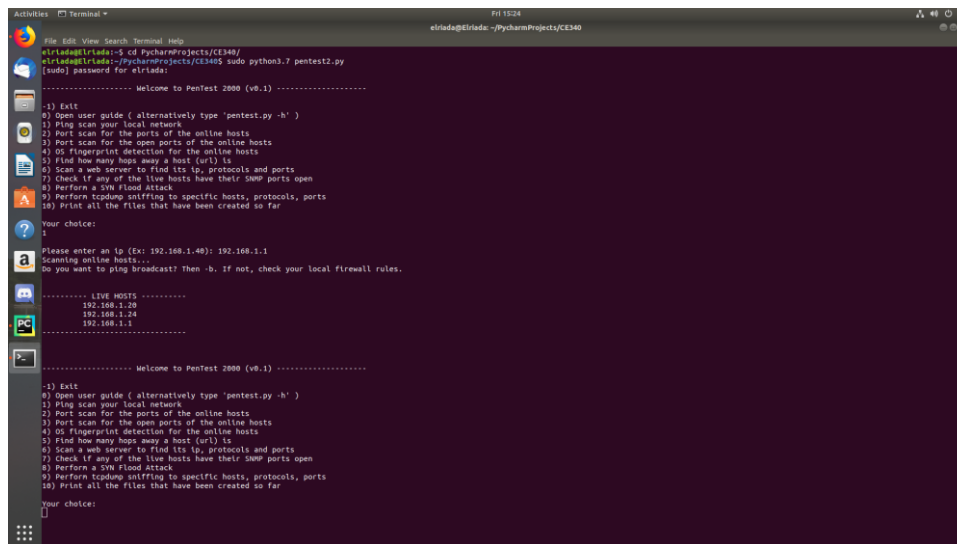
CE 340 Homework 2

I Penetration Test

As a second homework project of CE340 course we present you the Pentest2000. This program allows you to do various tasks within your local network. Let's have a look what Pentest2000 can do.

1. Deceting online hosts:

Our tool can detect online hosts via pinging each host. If it is live, it will return as live and will be recorded to the icmp.dat file.



```
elriada@elriada:~$ cd ~/PycharmProjects/CE340/
elriada@elriada:~/PycharmProjects/CE340$ sudo python3.7 pentest2.py
[sudo] password for elriada:

----- Welcome to Pentest 2000 (v0.1) -----

-> Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
1

Please enter an ip (Ex: 192.168.1.40): 192.168.1.1
Scanning online hosts...
Do you want to ping broadcast? Then -b, if not, check your local firewall rules.

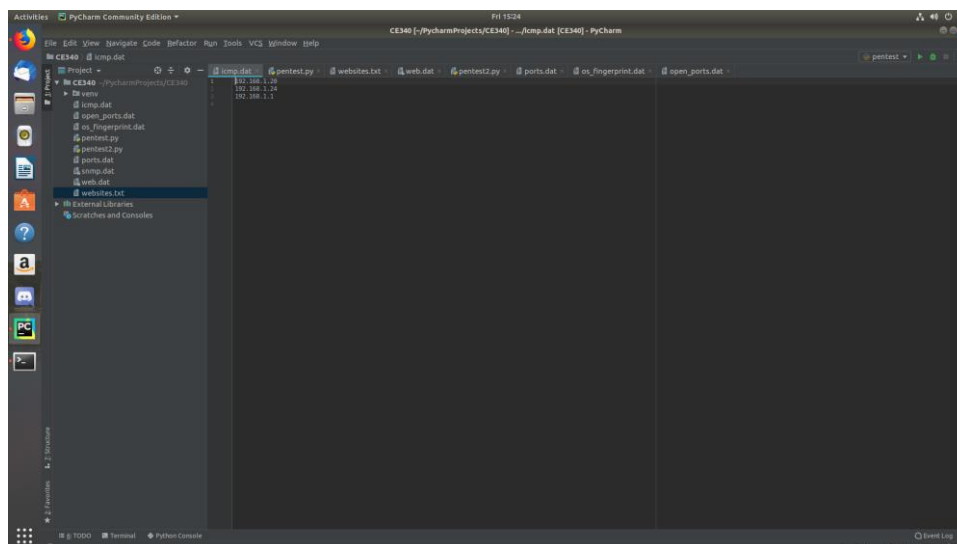
----- LIVE HOSTS -----
192.168.1.28
192.168.1.24
192.168.1.1
-----

----- Welcome to Pentest 2000 (v0.1) -----

-> Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:

```



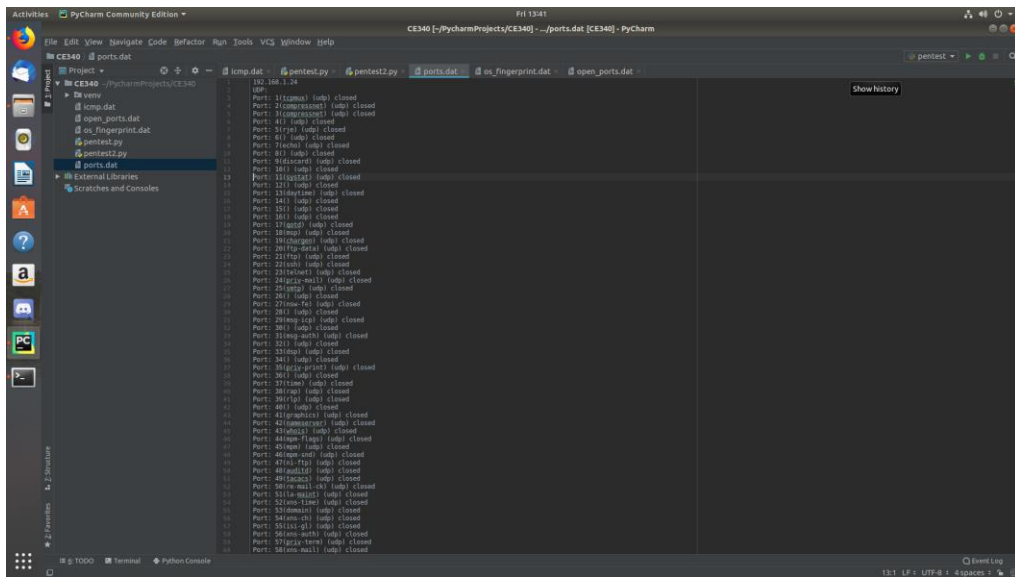
2.Scanning ports of the online hosts:

Our tools also can scan the ports of the each host desired range of ports but the amount of time will be longer as the range grows this task can take up to minutes. Even though we implemented multiprocessing for this task scanning all ports for an host will take sometime.

Results will be saved in a file called ports.dat.

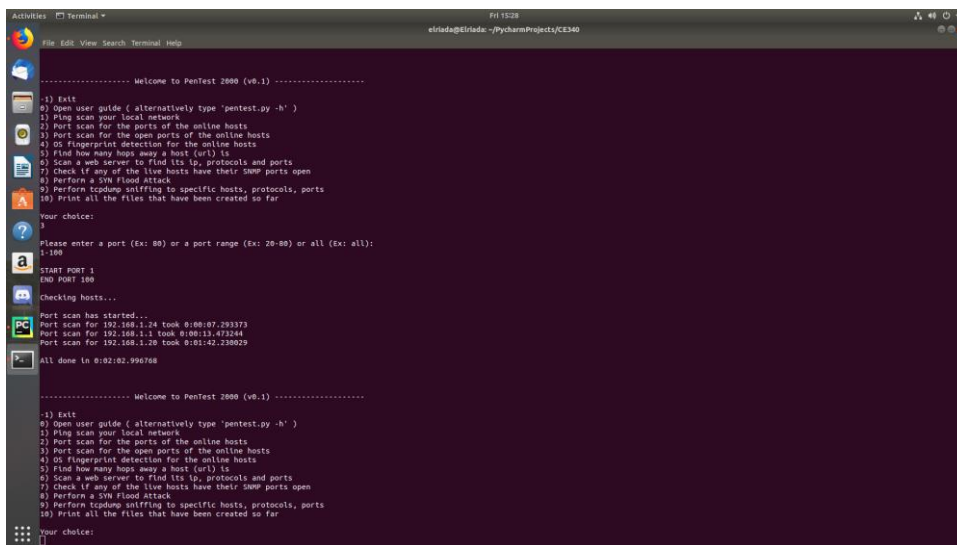
A screenshot of a Kali Linux desktop environment. The top bar shows the date 'Fri 15/01' and system icons. The desktop has several icons: a terminal, a file manager, a web browser, and a terminal. The terminal window is open, showing a Python script named 'pentest2.py' being executed. The script is located at 'e1rlada@e1rlada:~/PycharmProjects/CE3405'. The script prompts the user to enter a password, which is '1880'. It then displays a welcome message for 'PenTest 2000 (v0.1)' and a list of 10 menu options. The user selects option 1 (Exit), and the script prints 'All done in 0:00:20.608642'. The terminal window also shows the file explorer and terminal tabs at the top.

Both TCP and UDP ports are scanned and recored to the corresponding file.



3. Scanning open ports for online hosts:

This task is pretty similar to the previous task but this time our tool will only look for open ports and record the open ports to the `open_ports.dat` file.



5. Finding the distance between you and a host(URL):

This task allows you to find how far an a host(URL) is away from you.

```
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
5

If packets get stuck please quit with 'Ctrl + C' combination!!
Please enter a host name (Ex: www.google.com):
www.facebook.com
1 hop(s): 192.168.1.1
2 hop(s): 212.57.0.25
3 hop(s): 10.36.251.165
4 hop(s): 10.36.216.73
5 hop(s): 10.40.119.38
6 hop(s): 10.38.218.81
7 hop(s): 10.36.219.34
8 hop(s): 10.36.6.2
9 hop(s): 157.240.67.70
10 hop(s): 31.13.27.219
11 hop(s): 157.240.38.97
Host is 12 hop(s) away 157.240.9.35
```

```
File Edit View Search Terminal Help
elriada@elriada: ~/PycharmProjects/CE340

7) Scan a web server to find its ip, protocols and ports
8) Check if any of the live hosts have their SNMP ports open
9) Perform a SYN Flood Attack
10) Perform tcpdump sniffing to specific hosts, protocols, ports
11) Print all the files that have been created so far

Your choice:
0

If packets get stuck please quit with 'Ctrl + C' combination!!
Please enter a host name (Ex: www.google.com):
www.google.com

NOTE: Where the SA and repetition of an ip address starts
The corresponding number on the left is the hop count

Begin emission:
Finished sending 20 packets.
Received 9 packets, got 9 answers, remaining 11 packets
1 192.168.1.1 II
2 212.57.0.25 II
3 10.36.251.165 II
4 10.36.216.73 II
5 10.40.119.38 II
6 10.38.218.81 II
7 172.217.16.100 SA
8 172.217.16.100 SA
9 172.217.16.100 SA
10 172.217.16.100 SA
11 Traceroute: TCP:3 UDP:0 ICMP:6 Other:0

NOTE: Where the SA and repetition of an ip address starts
The corresponding number on the left is the hop count

----- Welcome to Pentest 2000 (v0.1) -----

You can end any process with the 'Ctrl + C' combination!!

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Alternative hop count of a host (url)
7) Scan a web server to find its ip, protocols and ports
8) Check if any of the live hosts have their SNMP ports open
9) Perform a SYN Flood Attack
10) Perform tcpdump sniffing to specific hosts, protocols, ports
11) Print all the files that have been created so far

Your choice:
0
```

```
File Edit View Search Terminal Help
elriada@elriada: ~/PycharmProjects/CE340

11 hop(s): 72.14.212.42
^C
----- Welcome to Pentest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
5

If packets get stuck please quit with 'Ctrl + C' combination!!
Please enter a host name (Ex: www.google.com):
www.instagram.com
1 hop(s): 192.168.1.1
2 hop(s): 212.57.0.25
3 hop(s): 10.36.251.165
4 hop(s): 10.36.216.73
5 hop(s): 10.40.119.38
6 hop(s): 10.38.218.81
7 hop(s): 10.36.219.34
8 hop(s): 10.36.6.2
9 hop(s): 157.240.67.70
10 hop(s): 157.240.40.51
11 hop(s): 173.252.67.128
Host is 12 hop(s) away 157.240.9.174

----- Welcome to Pentest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
0
```

Sometimes packet can stuck! So we made an alternative for hop task!

```
Activities Terminal Fri 15:43 elirida@Elirida: ~/PycharmProjects/CE340
File Edit View Search Terminal Help

Your choice:
5
If packets get stuck please quit with 'Ctrl + C' combination!!
Please enter a host name (Ex: www.google.com):
www.facebook.com
1 Hop(s): 192.168.1.1
2 Hop(s): 212.57.8.25
3 Hop(s): 19.36.251.165
4 Hop(s): 19.38.219.73
5 Hop(s): 19.40.119.38
6 Hop(s): 19.38.219.81
7 Hop(s): 19.38.219.34
8 Hop(s): 19.36.6.2
9 Hop(s): 62.115.149.8
^C
----- Welcome to PenTest 2000 (v0.1) -----

-) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
5
If packets get stuck please quit with 'Ctrl + C' combination!!
Please enter a host name (Ex: www.google.com):
www.tcloud.com
1 Hop(s): 192.168.1.1
2 Hop(s): 212.57.8.25
3 Hop(s): 19.36.251.165
4 Hop(s): 19.38.219.73
5 Hop(s): 19.40.119.38
6 Hop(s): 19.38.219.81
7 Hop(s): 19.38.219.34
8 Hop(s): 19.36.6.2
9 Hop(s): 19.117.15.65
10 Hop(s): 154.54.36.54
11 Hop(s): 154.54.38.4
12 Hop(s): 130.117.0.70
13 Hop(s): 130.117.0.93
14 Hop(s): 154.54.37.73
15 Hop(s): 154.23.11.274
16 Hop(s): 149.14.44.38
^C
```

6.Scanning the web server:

Scanning the web server will show you its ip and protocols and open ports.

You can either enter your own URL or you can leave the decision to our tool to scan web servers randomly.

```
Activities Terminal Fri 15:47 elirida@Elirida: ~/PycharmProjects/CE340
File Edit View Search Terminal Help

----- Welcome to PenTest 2000 (v0.1) -----

-) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
6
1) Enter your own URL
2) Let the program pick 10 random websites out of 60 preset websites

Your choice:
1
Please enter a URL (Ex: www.google.com): www.youtube.com
Process has started...
Port scan for www.youtube.com (216.58.207.78) took 0:00:07.592584
All done in 0:00:12.724219

----- Welcome to PenTest 2000 (v0.1) -----

-) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
1
```

```
Activities Terminal * Fri 15:47
elirida@Elirida: ~/PycharmProjects/CE340

----- Welcome to PenTest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
0

1) Enter your own URL
2) Let the program pick 10 random websites out of 60 preset websites

Your choice:
1

Please enter a URL (Ex: www.google.com): www.tau.edu.tr
Process has started....

Port scan for www.tau.edu.tr (213.14.255.87) took 0:00:07.630516

All done in 0:00:11.693728

----- Welcome to PenTest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
0
```

```
Activities Terminal * Fri 15:47
elirida@Elirida: ~/PycharmProjects/CE340

----- Welcome to PenTest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
0

1) Enter your own URL
2) Let the program pick 10 random websites out of 60 preset websites

Your choice:
1

Please enter a URL (Ex: www.google.com): www.google.com
Process has started....

Port scan for www.google.com (172.217.16.100) took 0:00:09.214239

All done in 0:00:12.580015

----- Welcome to PenTest 2000 (v0.1) -----

-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far

Your choice:
0
```

7.SNMP port check:

This tasks allow you to see if the online hosts at your local network got their SNMP ports open or not.It is basically scanning a single port for online hosts at your local network.


```
Activities Terminal
Fri 13:55
elriada@Elriada: ~/PycharmProjects/CE340

File Edit View Search Terminal Help
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their SNMP ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far
Your choice:
?
Checking hosts...
SNMP scan has started...
192.168.1.24
Port: 161(snmp) (tcp) closed
Port: 161(snmptrap) (tcp) closed
Port: 161(snmp) (udp) closed
Port: 162(snmptrap) (udp) closed
192.168.1.1
Port: 161(snmp) (tcp) filtered
Port: 162(snmptrap) (tcp) filtered
Port: 161(snmp) (udp) open|filtered
Port: 162(snmptrap) (udp) open|filtered
192.168.1.20
Port: 161(snmp) (tcp) closed
Port: 162(snmptrap) (tcp) closed
Port: 161(snmp) (udp) closed
Port: 162(snmptrap) (udp) closed
All done in 0:00:03.701853
----- Welcome to PenTest 2000 (v0.1) -----
-1) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Scan a web server to find its ip, protocols and ports
7) Check if any of the live hosts have their Smp ports open
8) Perform a SYN Flood Attack
9) Perform tcpdump sniffing to specific hosts, protocols, ports
10) Print all the files that have been created so far
Your choice:
[]
```

8.Performing a SYN flood attack to a target:

In this task you can easily attack a target with SYN flood method.Your attack will also shown in the screen.

```
Activities Terminal
Fri 13:56
elriada@Elriada: ~/PycharmProjects/CE340

File Edit View Search Terminal Help
Please enter how many thousand syn packets you want to send (Ex: 1 -> 1000):
10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s8, link-type EN10MB (Ethernet), capture size 262144 bytes
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s8, link-type EN10MB (Ethernet), capture size 262144 bytes
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s8, link-type EN10MB (Ethernet), capture size 262144 bytes
13:56:24.659249 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [S.], seq 1044153494, ack 2777748694, win 28160, options [mss 1412,sackOK,TS val 1171437826 ecr 2795670294,nop,wscale 7], length 0
13:56:24.659257 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [S.], seq 1044153494, ack 2777748694, win 28160, options [mss 1412,sackOK,TS val 1171437826 ecr 2795670294,nop,wscale 7], length 0
13:56:24.659263 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [S.], seq 1044153494, ack 2777748694, win 28160, options [mss 1412,sackOK,TS val 1171437826 ecr 2795670294,nop,wscale 7], length 0
13:56:24.659310 IP .gateway.domain > Elriada.57908: 58613 ServFail- 0/0/0 (43)
13:56:24.236562 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 88, win 204, options [nop,nop,TS val 1171438057 ecr 2795670458], length 0
13:56:24.271653 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [P.], seq 1149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 148: HTTP: HTTP/1.1 204
No Content
13:56:24.274440 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 0
13:56:24.470484 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 89, win 204, options [nop,nop,TS val 1171438295 ecr 2795670673], length 0
13:56:24.473403 IP .gateway.domain > Elriada.60977: 17812 1/0/0 PTR 177.143.198.104.bc.googleusercontent.com. (100)
13:56:24.474076 IP .gateway.domain > Elriada.44049: 54703 ServFail- 0/0/0 (42)
13:56:24.475309 IP .gateway.domain > Elriada.57908: 58613 ServFail- 0/0/0 (43)
13:56:24.236561 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 88, win 204, options [nop,nop,TS val 1171438057 ecr 2795670458], length 0
13:56:24.271651 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [P.], seq 1149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 148: HTTP: HTTP/1.1 204
No Content
13:56:24.274438 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 0
13:56:24.470481 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 89, win 204, options [nop,nop,TS val 1171438295 ecr 2795670673], length 0
13:56:24.473401 IP .gateway.domain > Elriada.60977: 17812 1/0/0 PTR 177.143.198.104.bc.googleusercontent.com. (100)
13:56:24.474077 IP .gateway.domain > Elriada.44049: 54703 ServFail- 0/0/0 (42)
13:56:24.475307 IP .gateway.domain > Elriada.57908: 58613 ServFail- 0/0/0 (43)
13:56:24.236559 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 88, win 204, options [nop,nop,TS val 1171438057 ecr 2795670458], length 0
13:56:24.236566 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [P.], seq 1149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 148: HTTP: HTTP/1.1 204
No Content
13:56:24.271849 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [P.], seq 1149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 148: HTTP: HTTP/1.1 204
No Content
13:56:24.274435 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 149, ack 88, win 204, options [nop,nop,TS val 1171438096 ecr 2795670458], length 0
13:56:24.470477 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 89, win 204, options [nop,nop,TS val 1171438295 ecr 2795670673], length 0
13:56:24.470477 IP 177.143.198.104.bc.googleusercontent.com.http > Elriada.55618: Flags [F.], seq 89, win 204, options [nop,nop,TS val 1171438295 ecr 2795670673], length 0
13:56:24.473399 IP .gateway.domain > Elriada.60977: 17812 1/0/0 PTR 177.143.198.104.bc.googleusercontent.com. (100)
13:56:24.474072 IP .gateway.domain > Elriada.44049: 54703 ServFail- 0/0/0 (42)
13:56:24.474071 IP .gateway.domain > Elriada.44049: 54703 ServFail- 0/0/0 (42)
13:56:29.851609 ARP, Request who-has Elriada tell .gateway, length 46
13:56:29.851675 ARP, Request who-has Elriada tell .gateway, length 46
13:56:29.851671 ARP, Request who-has Elriada tell .gateway, length 46
```


This task allows you to sniff the packets for a specific host(s), protocol(s) or port(s).

[illegible][illegible]

This task allows you to tell which type of firewall is being used on the specific host.

This task allows you to tell which type of firewall is being used on the specific host.

11.Show:

Basically shows all results that we obtain during the execution of Pentest2000.

You can either show files one by one or you can show all those at once it is up to you.

Icmp.dat file:

```
File Edit View Search Terminal Help
elirada@Elirada: ~/PycharmProjects/CE340

2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Alternative hop count of a host (url)
7) Scan a web server to find its ip, protocols and ports
8) Check if any of the live hosts have their SNMP ports open
9) Perform a SYN flood attack
10) Perform tcpdump sniffing to specific hosts, protocols, ports
11) Print all the files that have been created so far
Your choice:
11
Please select files to print
Your options are:
1) icmp.dat
2) ports.dat
3) open_ports.dat
4) web.dat
5) snmp.dat
6) All the files
Your choice:
1
----- ICMP.DAT FILE: -----
192.168.1.1
192.168.1.24
192.168.1.28
192.168.1.23
----- Welcome to Pentest 2000 (v0.1) -----
You can end any process with the 'Ctrl + C' combination!!
-3) Exit
0) Open user guide ( alternatively type 'pentest.py -h' )
1) Ping scan your local network
2) Port scan for the ports of the online hosts
3) Port scan for the open ports of the online hosts
4) OS fingerprint detection for the online hosts
5) Find how many hops away a host (url) is
6) Alternative hop count of a host (url)
7) Scan a web server to find its ip, protocols and ports
8) Check if any of the live hosts have their SNMP ports open
9) Perform a SYN flood attack
10) Perform tcpdump sniffing to specific hosts, protocols, ports
11) Print all the files that have been created so far
Your choice:
11
```

Ports.dat file:

```
File Edit View Search Terminal Help
elirada@Elirada: ~/PycharmProjects/CE340

----- PORTS.DAT FILE: -----
192.168.1.24
UDP:
Port: 1(tcpmux) (udp) closed
Port: 2(compressnet) (udp) closed
Port: 3(compressnet) (udp) closed
Port: 4() (udp) closed
Port: 5(rpc) (udp) closed
Port: 6() (udp) closed
Port: 7(icmp) (udp) closed
Port: 8() (udp) closed
Port: 9(discard) (udp) closed
Port: 10() (udp) closed
Port: 11(sysstat) (udp) closed
Port: 12() (udp) closed
Port: 13(daytime) (udp) closed
Port: 14() (udp) closed
Port: 15() (udp) closed
Port: 16() (udp) closed
Port: 17(qotd) (udp) closed
Port: 18(msg) (udp) closed
Port: 19(chargen) (udp) closed
Port: 20(ftp-data) (udp) closed
Port: 21(ftp) (udp) closed
Port: 22(ssh) (udp) closed
Port: 23(telnet) (udp) closed
Port: 24(priv-mail) (udp) closed
Port: 25(ftp) (udp) closed
Port: 26() (udp) closed
Port: 27(nsw-fe) (udp) closed
Port: 28() (udp) closed
Port: 29(msg-icp) (udp) closed
Port: 30() (udp) closed
Port: 31(msg-auth) (udp) closed
Port: 32() (udp) closed
Port: 33(dsp) (udp) closed
Port: 34() (udp) closed
Port: 35(priv-print) (udp) closed
Port: 36() (udp) closed
Port: 37(time) (udp) closed
Port: 38(rap) (udp) closed
Port: 39() (udp) closed
Port: 40() (udp) closed
Port: 41(graphics) (udp) closed
Port: 42(ameserver) (udp) closed
Port: 43(whats) (udp) closed
Port: 44(ngn-flag) (udp) closed
Port: 45(ngn) (udp) closed
Port: 46(ngn-mb) (udp) closed
Port: 47(ni-ftp) (udp) closed
Port: 48(authts) (udp) closed
Port: 49(tacacs) (udp) closed
Port: 50(re-mail-ck) (udp) closed
```

```
Activities Terminal Fri 15:54 eirlada@eirlada: ~/PycharmProjects/CE340
File Edit View Search Terminal Help
Port: 50(re-mail-ch) (udp) open|filtered
Port: 51(la-maint) (udp) open|filtered
Port: 52(xns-tlm) (udp) open|filtered
Port: 53(domain) (udp) open|filtered
Port: 54(xns-ch) (udp) open|filtered
Port: 55(sit-gll) (udp) open|filtered
Port: 56(xns-auth) (udp) open|filtered
Port: 57(priv-tern) (udp) open|filtered
Port: 58(xns-mail) (udp) open|filtered
Port: 59(priv-file) (udp) open|filtered
Port: 60() (udp) open|filtered
Port: 61(nl-mail) (udp) open|filtered
Port: 62(ccs) (udp) open|filtered
Port: 63(via-ftp) (udp) open|filtered
Port: 64(ccs) (udp) open|filtered
Port: 65(tacacs-ds) (udp) open|filtered
Port: 66(sqlnet) (udp) open|filtered
Port: 67(dhcp) (udp) open|filtered
Port: 68(dhpc) (udp) open|filtered
Port: 69(ftp) (udp) open|filtered
Port: 70(gopher) (udp) open|filtered
Port: 71(netrjs-2) (udp) open|filtered
Port: 72(netrjs-2) (udp) open|filtered
Port: 73(netrjs-3) (udp) open|filtered
Port: 74(netrjs-4) (udp) open|filtered
Port: 75(priv-dial) (udp) open|filtered
Port: 76(dns) (udp) open|filtered
Port: 77(priv-rje) (udp) open|filtered
Port: 78(vetcp) (udp) open|filtered
Port: 79(ftp) (udp) open|filtered
Port: 80(http) (udp) open|filtered
Port: 81(host2ns) (udp) open|filtered
Port: 82(xfer) (udp) open|filtered
Port: 83(nl-nl-dns) (udp) open|filtered
Port: 84(ctf) (udp) open|filtered
Port: 85(nl-nl-dns) (udp) open|filtered
Port: 86(nf-subol) (udp) open|filtered
Port: 87() (udp) open|filtered
Port: 88(kerbersec) (udp) open|filtered
Port: 89(su-mit-tg) (udp) open|filtered
Port: 90(dns) (udp) open|filtered
Port: 91(mit-dns) (udp) open|filtered
Port: 92(ftp) (udp) open|filtered
Port: 93(dcp) (udp) open|filtered
Port: 94(abcall) (udp) open|filtered
Port: 95(su-dns) (udp) open|filtered
Port: 96(dixie) (udp) open|filtered
Port: 97(cu-ft-rf) (udp) open|filtered
Port: 98(tachons) (udp) open|filtered
Port: 99(metagram) (udp) open|filtered
Port: 100() (udp) open|filtered
Port: 101(hostname) (udp) open|filtered
Port: 102(iso-tsap) (udp) open|filtered
Port: 103(ggptnp) (udp) open|filtered
Port: 104(ocr-mms) (udp) open|filtered
```