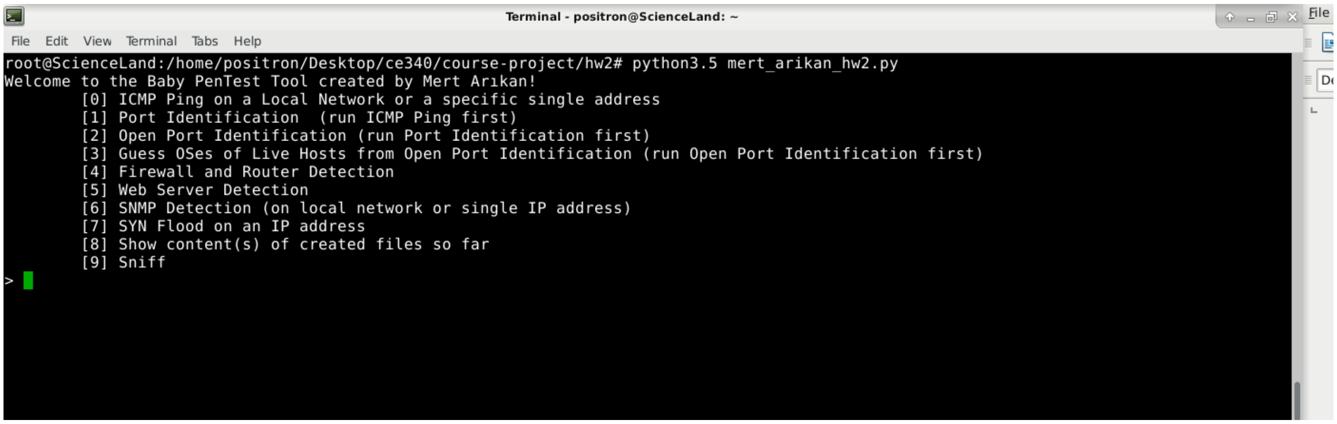
Homework 2
Mert ARIKAN 20140601004

Prerequisities:

- **Python 3.5 (it should work with all Python 3.x versions)**
- **python-nmap 0.6.1 (** *https://pypi.org/project/python-nmap/ or just type "pip install python-nmap" with root privileges***)**
- **Scapy**

This tool is for homework and a small tool for pentesting on local network(and remote addresses for some cases). Program must be run with root privileges and working directory should be where program is located at. Program can be started via command "python3.5 mert_arikan_hw2.py". Also, any Python3 version above 3.5 should work.

First, main menu looks like this:


Terminal - positron@ScienceLand: ~
File Edit View Terminal Tabs Help

```
root@ScienceLand:/home/positron/Desktop/ce340/course-project/hw2# python3.5 mert_arikan_hw2.py
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 
```

User should input one of the options on the menu. For features (1),(2) and (3), user *must* follow steps from (0) to (3),sequentially. Other features do not depend on another feature to run first.

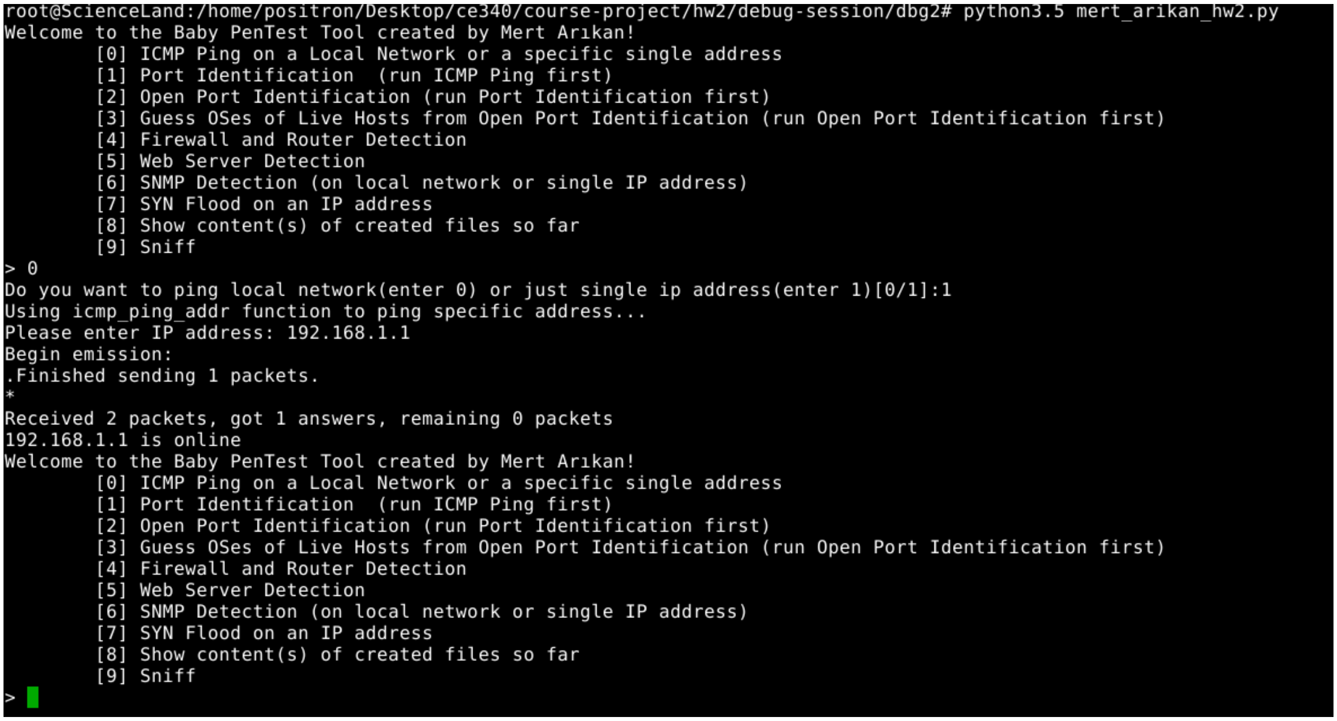
Features

1. ICMP Ping (selection '0')

User can ping multiple addresses on a local network within some range or choose to ping a single address on a local network or a remote address (It is not appropriate to ping any remote address if other end say otherwise).

After user choose ICMP ping, he/she is asked whether he/she wants to ping through some range (192.168.<user_input>.<user_input>) . With using Scapy module, the function craft an ICMP packet and send it to the destination. If a range is given, then the function craft packets,send them and wait for responses until loop ends.

Homework 2
Mert ARIKAN 20140601004



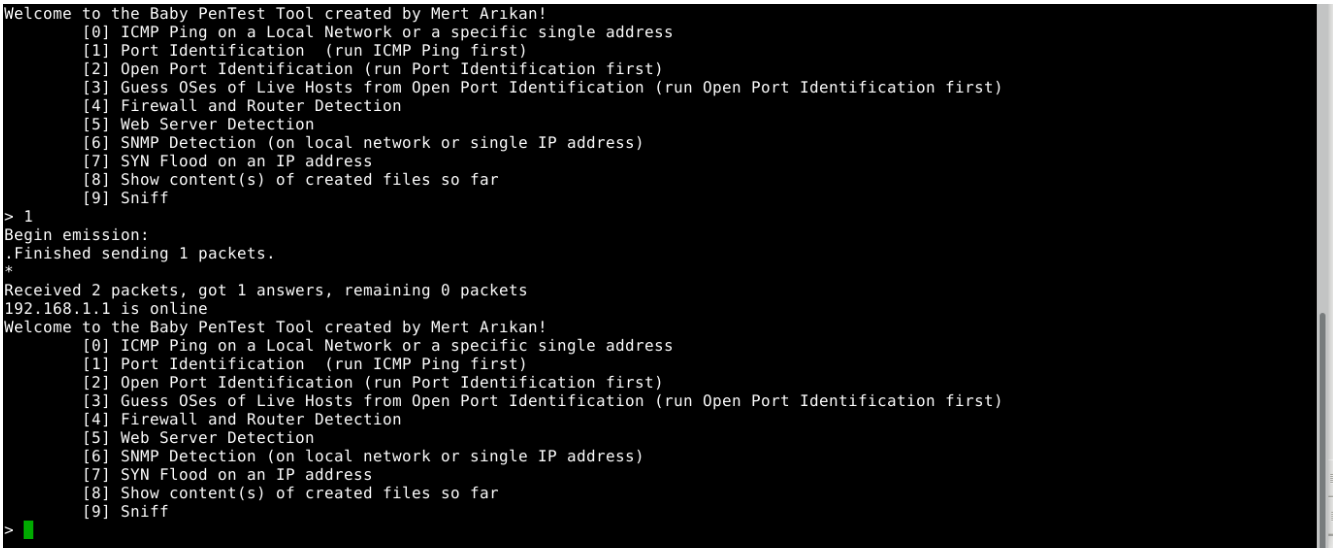
```
root@ScienceLand:/home/positron/Desktop/ce340/course-project/hw2/debug-session/dbg2# python3.5 mert_arikan_hw2.py
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 0
Do you want to ping local network(enter 0) or just single ip address(enter 1)[0/1]:1
Using icmp_ping_addr function to ping specific address...
Please enter IP address: 192.168.1.1
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
192.168.1.1 is online
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
>
```

Figure 1: ICMP ping was sent to router of the author's network.

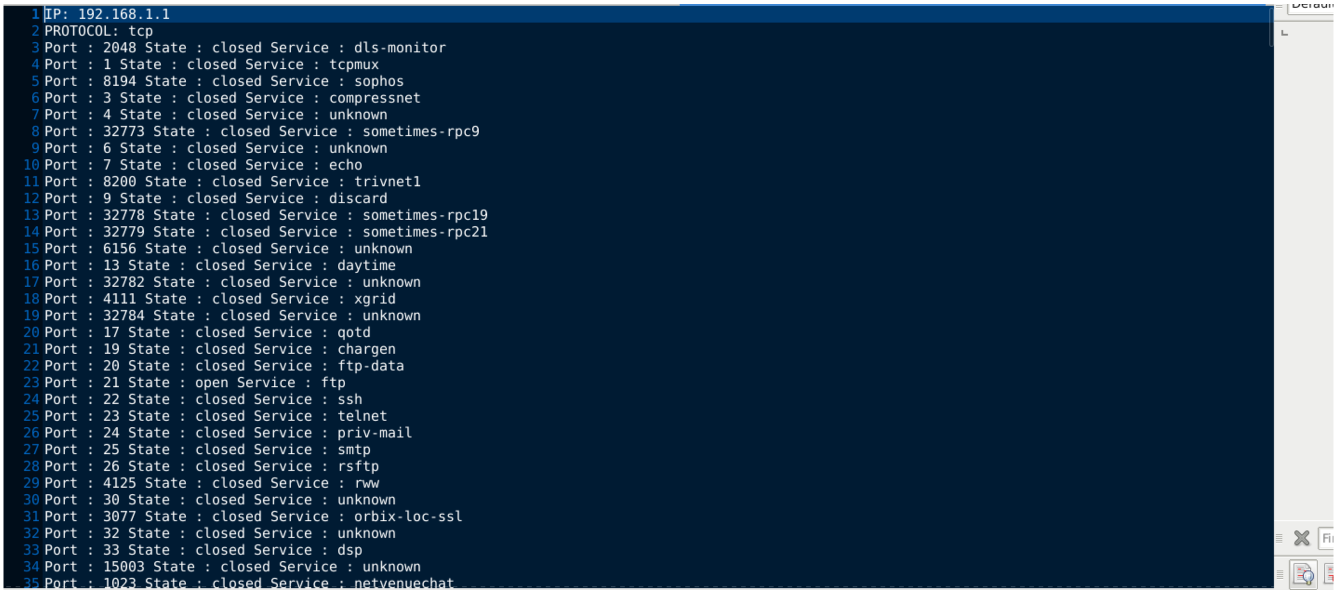
After packet is sent to its destination, program gives an output whether says " *<ip_addr> is not online"* , "*<ip_addr> is not online or there is an error"* or *"<ip_addr> is online"*,writes the result to a file called "icmp.dat" and returns to the main menu.

2. Port Identification (selection '1')

User has the ability to scan ports of previously-pinged hosts. This scan identify any port that is open or close -and their services - and write the result to a file called "ports.dat".



```
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 1
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
192.168.1.1 is online
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
>
```

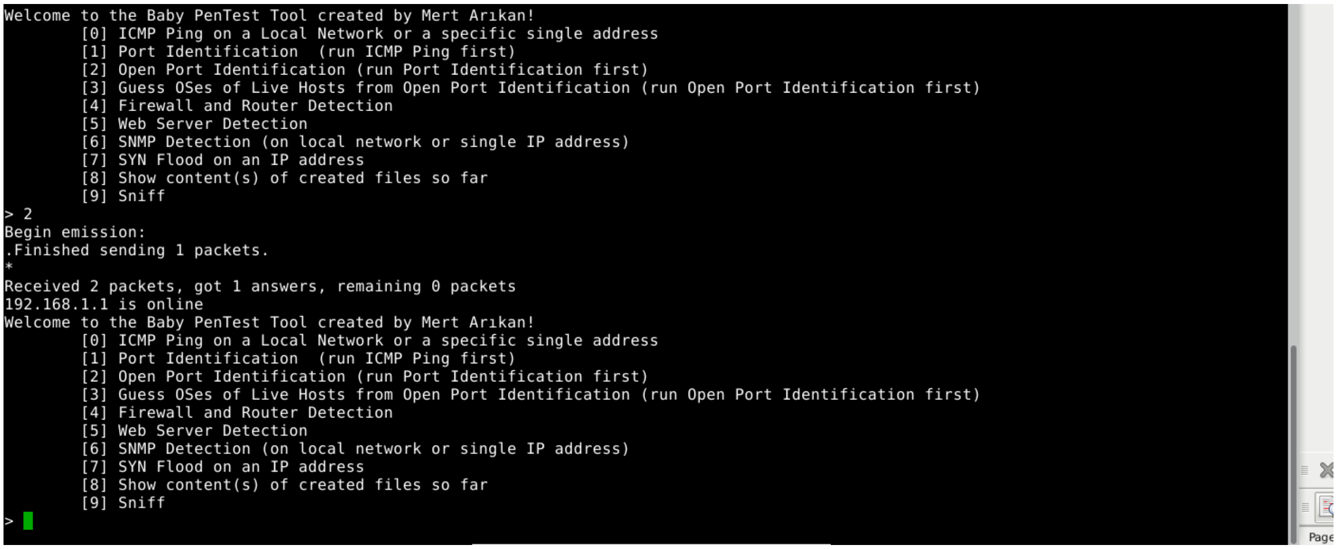


```
IP: 192.168.1.1
PROTOCOL: tcp
Port : 2048 State : closed Service : dls-monitor
Port : 1 State : closed Service : tcpmux
Port : 8194 State : closed Service : sophos
Port : 3 State : closed Service : compressnet
Port : 4 State : closed Service : unknown
Port : 32773 State : closed Service : sometimes-rpc9
Port : 6 State : closed Service : unknown
Port : 7 State : closed Service : echo
Port : 8200 State : closed Service : trivnet1
Port : 9 State : closed Service : discard
Port : 32778 State : closed Service : sometimes-rpc19
Port : 32779 State : closed Service : sometimes-rpc21
Port : 6156 State : closed Service : unknown
Port : 13 State : closed Service : daytime
Port : 32782 State : closed Service : unknown
Port : 4111 State : closed Service : xgrid
Port : 32784 State : closed Service : unknown
Port : 17 State : closed Service : qotd
Port : 19 State : closed Service : chargen
Port : 20 State : closed Service : ftp-data
Port : 21 State : open Service : ftp
Port : 22 State : closed Service : ssh
Port : 23 State : closed Service : telnet
Port : 24 State : closed Service : priv-mail
Port : 25 State : closed Service : smtp
Port : 26 State : closed Service : rsftp
Port : 4125 State : closed Service : rww
Port : 30 State : closed Service : unknown
Port : 3077 State : closed Service : orbix-loc-ssl
Port : 32 State : closed Service : unknown
Port : 33 State : closed Service : dsp
Port : 15003 State : closed Service : unknown
Port : 1023 State : closed Service : netvenuechat
```

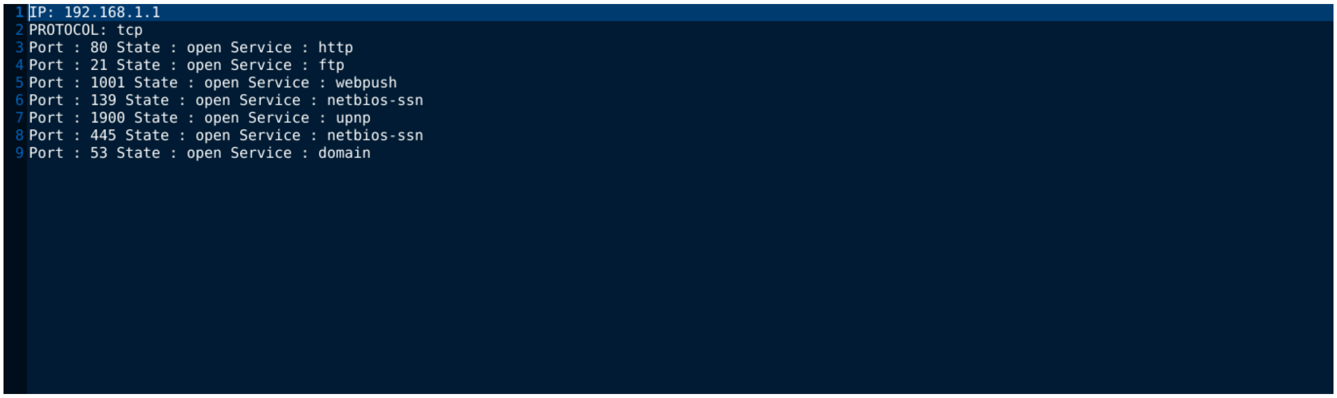
Figure 2: User entered 1 and results were written on a file *ports.dat*

3. Open Ports Identification (selection ‘2’)

Port identification function finishes and now,user can choose to identify open ports based on IP addresses written in *ports.dat* file. This function parses IP addresses from aforementioned file and see if they are still up. It scans live hosts for open ports(and respective services) and writes the result to a file *open_ports.dat*



```
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 2
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
192.168.1.1 is online
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
>
```

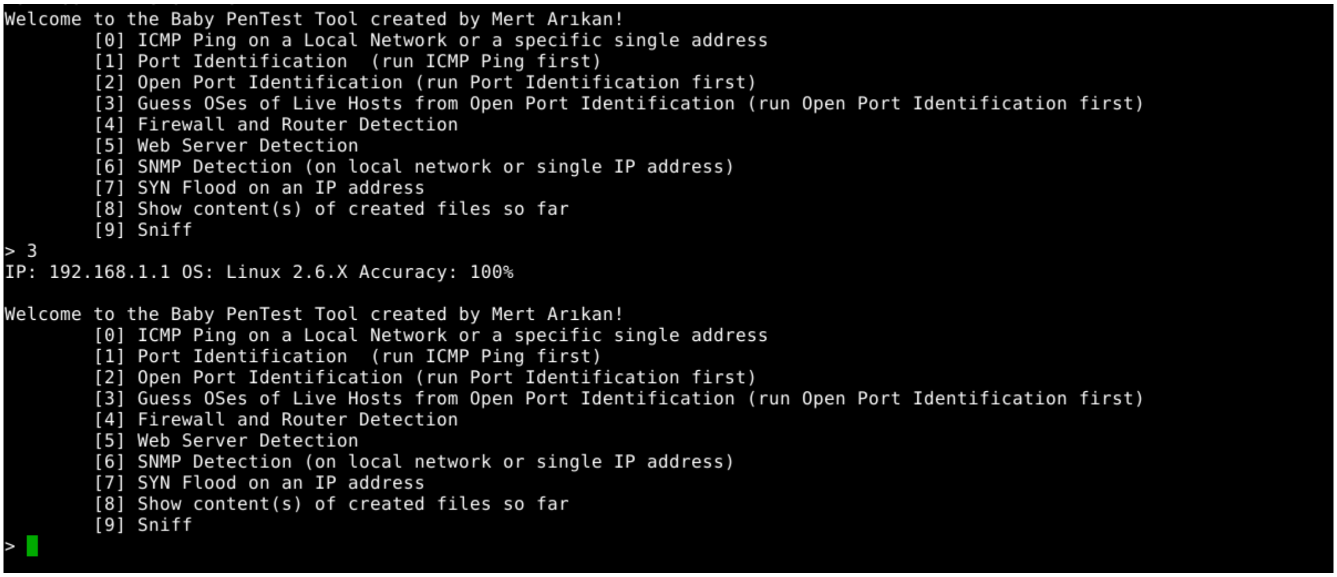


```
IP: 192.168.1.1
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 21 State : open Service : ftp
Port : 1001 State : open Service : webpush
Port : 139 State : open Service : netbios-ssn
Port : 1900 State : open Service : upnp
Port : 445 State : open Service : netbios-ssn
Port : 53 State : open Service : domain
```

Figure 3: Open Port Identification was selected and the result was written to open_ports.dat

4. Identify Operating System (selection '3')

This feature depends on previous features;so they must be runned previously.
This function uses nmap to guess operating system of the targets from *open_ports.dat* file.
However,the feature does not include save capability!



```
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 3
IP: 192.168.1.1 OS: Linux 2.6.X Accuracy: 100%

Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 
```

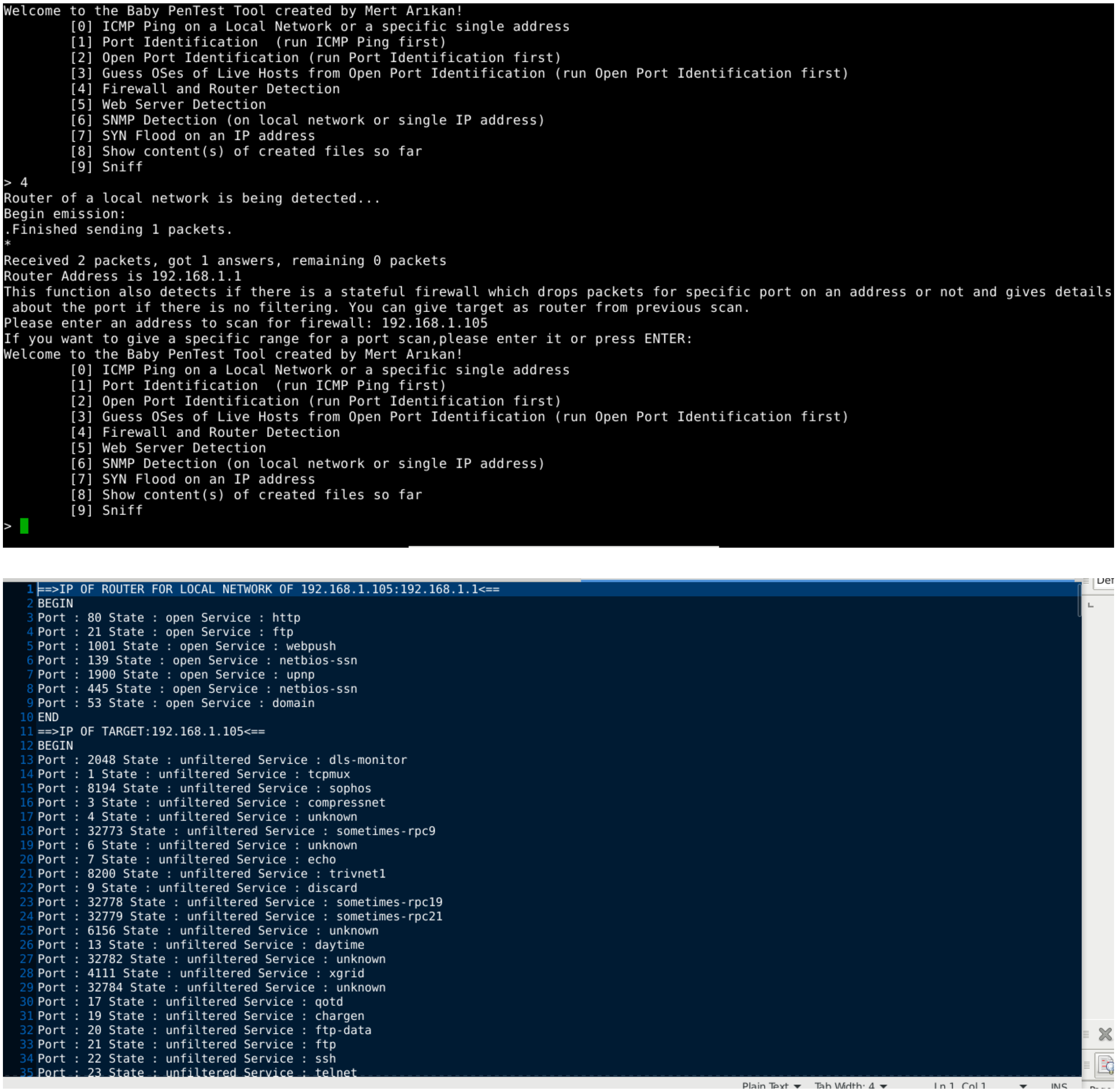
Figure 4: OS of IP address from open_ports.dat is guessed with accuracy of 100 percent

5. Firewall and Router Detection (selection '4')

firewallAndRouterDetection function,which is associated function with this feature, takes advantages of the behaviours of router and firewall. For router detection, when one computer wants to sent a packet to another computer, it sends the packet with time-to-live (ttl) which defines packet's total lifetime. If a node sends a packet with ttl equals to 0, router sends an ICMP response to it. After router is detected, function scan ports of it and write results to a file *wall.dat*.

Homework 2
Mert ARIKAN 20140601004

Firewall detection is another feature of author’s program. It ,first, wants user to give an IP address to it. Then,it checks every port with an TCP ACK packet. If target gives any response(ACK or RST), then program can say that that port does not have any firewall rule to filter it. Program writes port number,state of a port and its service to a file *wall.dat* if it is not filtered.



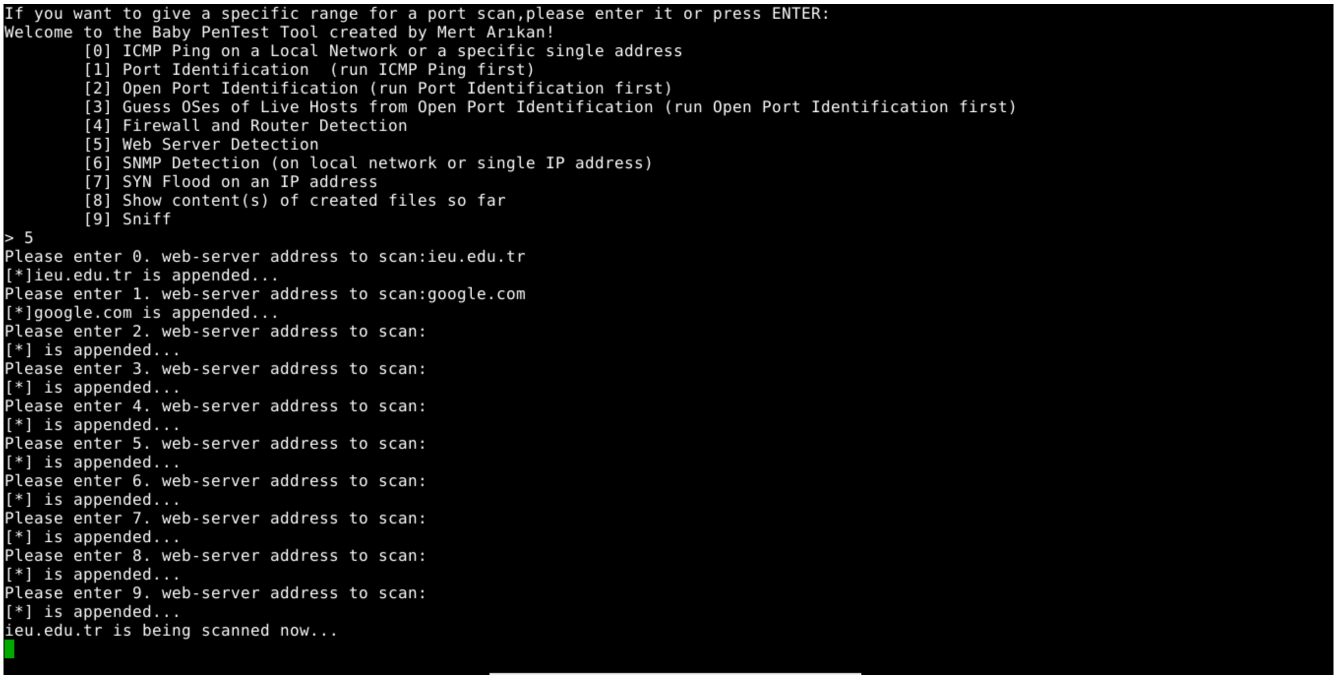
```
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 4
Router of a local network is being detected...
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
Router Address is 192.168.1.1
This function also detects if there is a stateful firewall which drops packets for specific port on an address or not and gives details
 about the port if there is no filtering. You can give target as router from previous scan.
Please enter an address to scan for firewall: 192.168.1.105
If you want to give a specific range for a port scan,please enter it or press ENTER:
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 
```

```
==>IP OF ROUTER FOR LOCAL NETWORK OF 192.168.1.105:192.168.1.1<==
BEGIN
Port : 80 State : open Service : http
Port : 21 State : open Service : ftp
Port : 1001 State : open Service : webpush
Port : 139 State : open Service : netbios-ssn
Port : 1900 State : open Service : upnp
Port : 445 State : open Service : netbios-ssn
Port : 53 State : open Service : domain
END
==>IP OF TARGET:192.168.1.105<==
BEGIN
Port : 2048 State : unfiltered Service : dls-monitor
Port : 1 State : unfiltered Service : tcpmux
Port : 8194 State : unfiltered Service : sophos
Port : 3 State : unfiltered Service : compressnet
Port : 4 State : unfiltered Service : unknown
Port : 32773 State : unfiltered Service : sometimes-rpc9
Port : 6 State : unfiltered Service : unknown
Port : 7 State : unfiltered Service : echo
Port : 8200 State : unfiltered Service : trivnet1
Port : 9 State : unfiltered Service : discard
Port : 32778 State : unfiltered Service : sometimes-rpc19
Port : 32779 State : unfiltered Service : sometimes-rpc21
Port : 6156 State : unfiltered Service : unknown
Port : 13 State : unfiltered Service : daytime
Port : 32782 State : unfiltered Service : unknown
Port : 4111 State : unfiltered Service : xgrid
Port : 32784 State : unfiltered Service : unknown
Port : 17 State : unfiltered Service : qotd
Port : 19 State : unfiltered Service : chargen
Port : 20 State : unfiltered Service : ftp-data
Port : 21 State : unfiltered Service : ftp
Port : 22 State : unfiltered Service : ssh
Port : 23 State : unfiltered Service : telnet
```

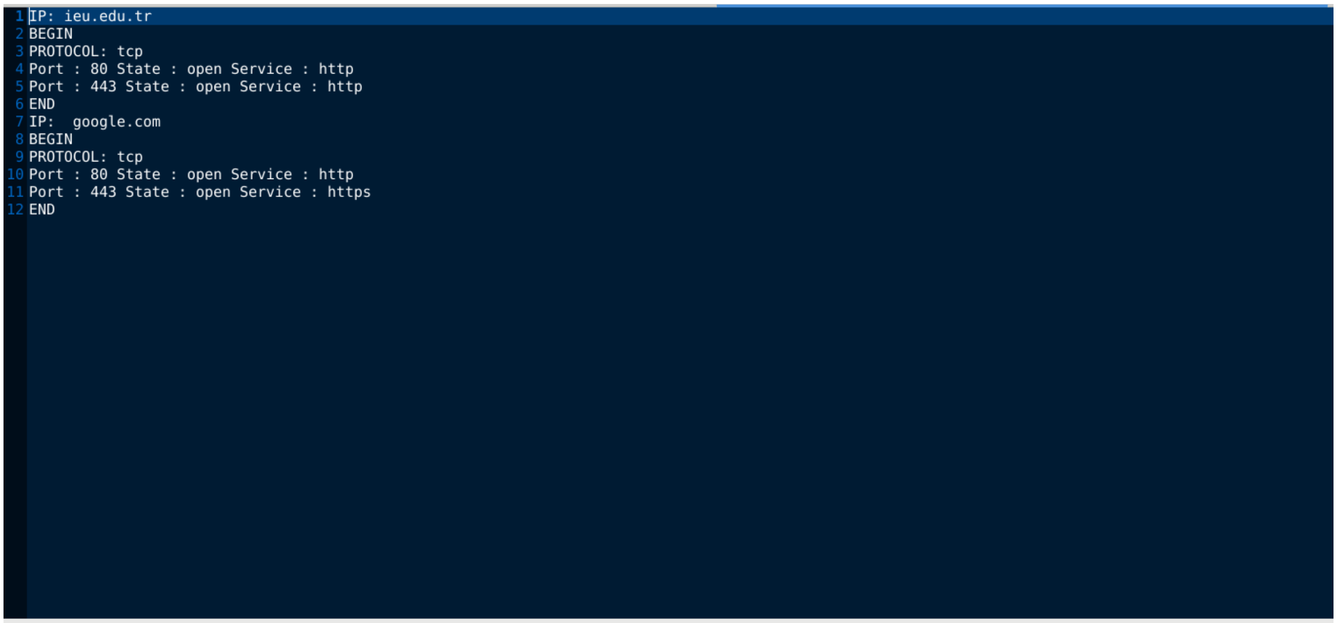
Figure 5: Router and firewall detections complete and results were written to a file wall.dat

6. Web Server Detection (selection ‘5’)

The function *webServerDetection* asks user 10 web addresses for it to scan. The results from these scans are written to a file named *web.dat.*
This function also relies on nmap and get results from that module.



```
If you want to give a specific range for a port scan,please enter it or press ENTER:
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 5
Please enter 0. web-server address to scan:ieu.edu.tr
[*]ieu.edu.tr is appended...
Please enter 1. web-server address to scan:google.com
[*]google.com is appended...
Please enter 2. web-server address to scan:
[*] is appended...
Please enter 3. web-server address to scan:
[*] is appended...
Please enter 4. web-server address to scan:
[*] is appended...
Please enter 5. web-server address to scan:
[*] is appended...
Please enter 6. web-server address to scan:
[*] is appended...
Please enter 7. web-server address to scan:
[*] is appended...
Please enter 8. web-server address to scan:
[*] is appended...
Please enter 9. web-server address to scan:
[*] is appended...
ieu.edu.tr is being scanned now...
```



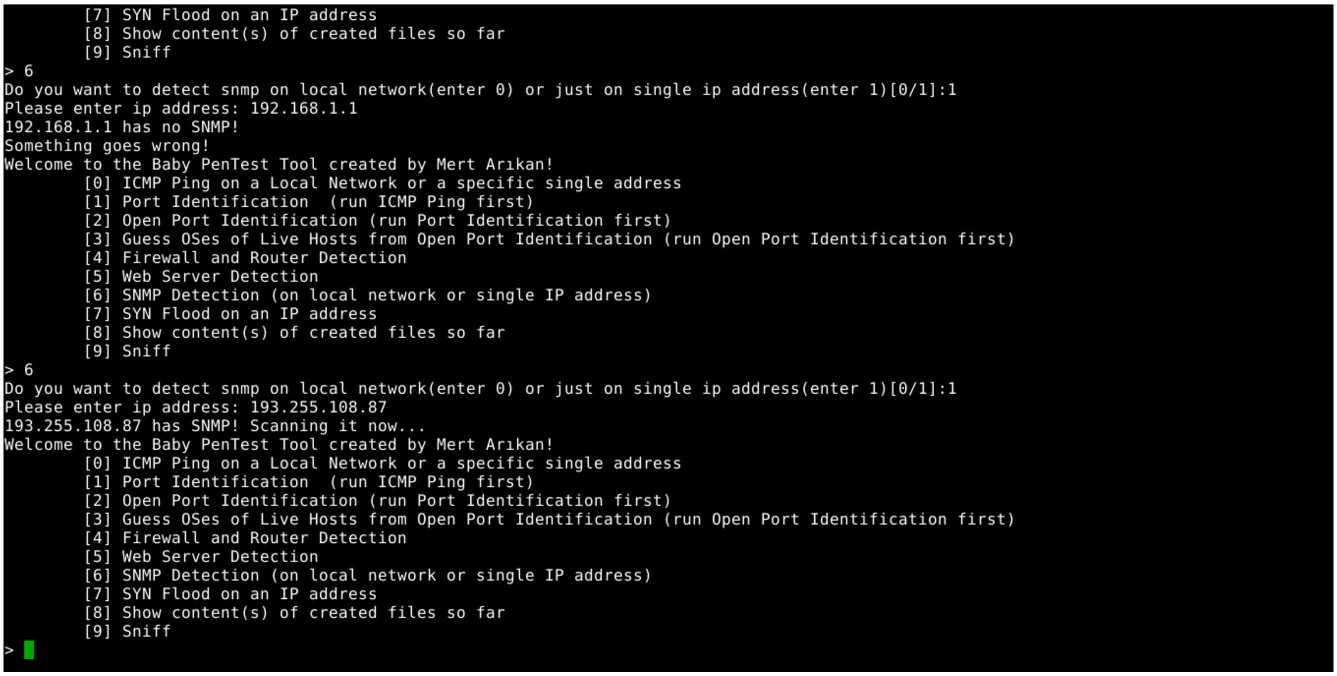
```
IP: ieu.edu.tr
BEGIN
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 443 State : open Service : http
END
IP:  google.com
BEGIN
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 443 State : open Service : https
END
```

Figure 6: User gave two addresses and program scans them via nmap. Results are written to web.dat

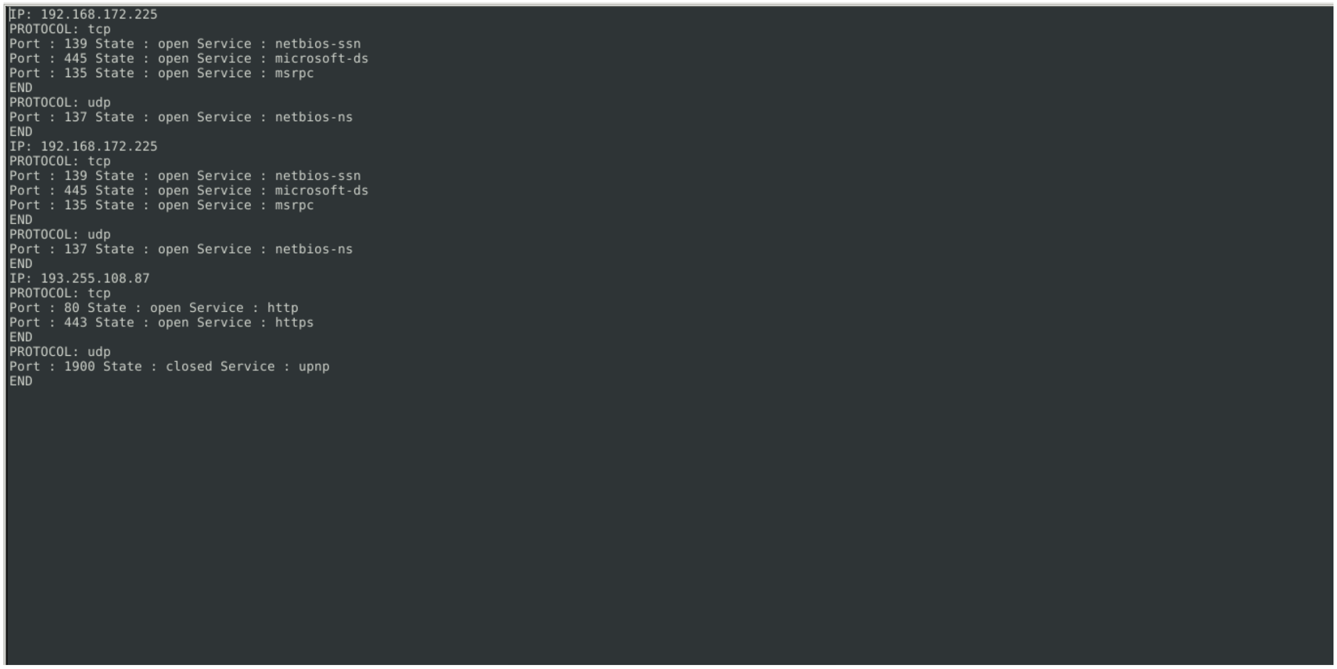
Homework 2
Mert ARIKAN 20140601004

7. SNMP Detection(selection ‘6’)

Simple Network Management Protocol is a protocol that is used to manage networks. It has a lot of privileges on a network and listens on 161 and 162 ports. So that, this function checks if it is listening on port 161. If it listens on that port, program scans for open ports and write results to a file named *snmp.dat*. Also, user can choose to give a range for scanning on local network and results are written in *snmp.dat* file.



```
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 6
Do you want to detect snmp on local network(enter 0) or just on single ip address(enter 1)[0/1]:1
Please enter ip address: 192.168.1.1
192.168.1.1 has no SNMP!
Something goes wrong!
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 6
Do you want to detect snmp on local network(enter 0) or just on single ip address(enter 1)[0/1]:1
Please enter ip address: 193.255.108.87
193.255.108.87 has SNMP! Scanning it now...
Welcome to the Baby PenTest Tool created by Mert Arıkan!
        [0] ICMP Ping on a Local Network or a specific single address
        [1] Port Identification  (run ICMP Ping first)
        [2] Open Port Identification (run Port Identification first)
        [3] Guess OSes of Live Hosts from Open Port Identification (run Open Port Identification first)
        [4] Firewall and Router Detection
        [5] Web Server Detection
        [6] SNMP Detection (on local network or single IP address)
        [7] SYN Flood on an IP address
        [8] Show content(s) of created files so far
        [9] Sniff
> 
```



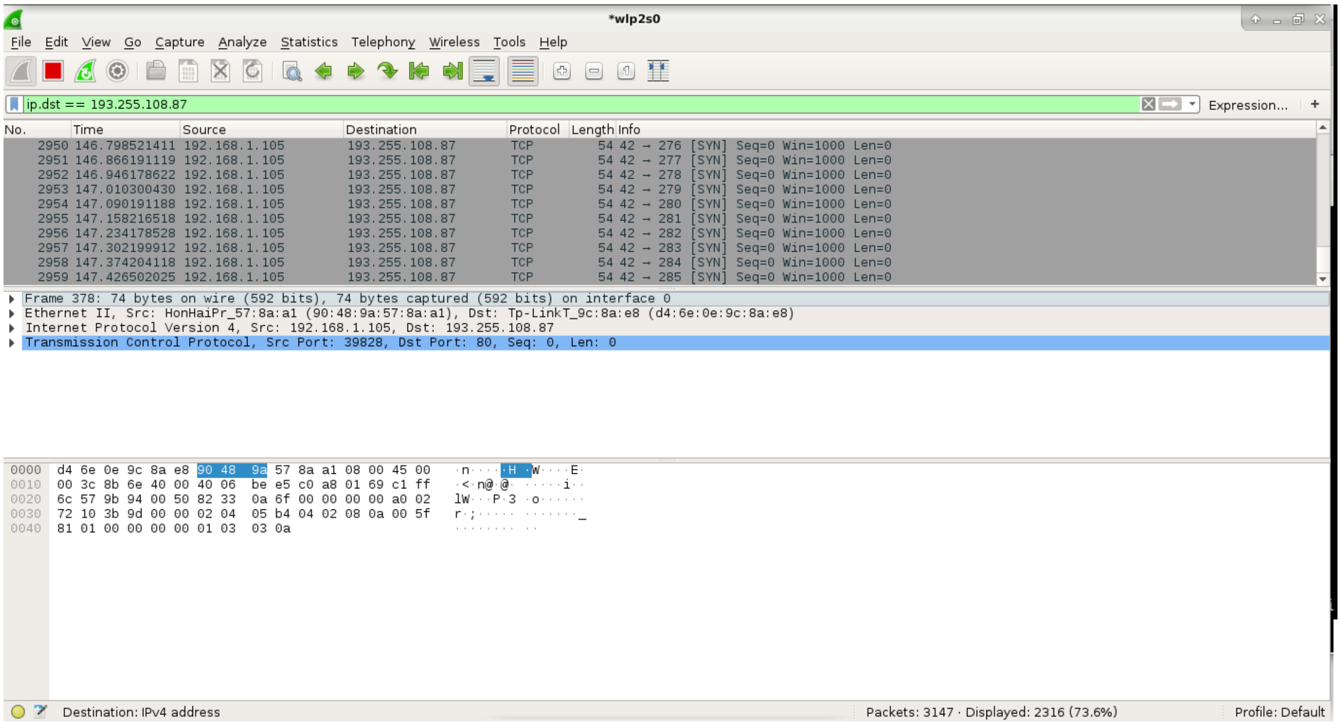
```
IP: 192.168.172.225
PROTOCOL: tcp
Port : 139 State : open Service : netbios-ssn
Port : 445 State : open Service : microsoft-ds
Port : 135 State : open Service : msrpc
END
PROTOCOL: udp
Port : 137 State : open Service : netbios-ns
END
IP: 192.168.172.225
PROTOCOL: tcp
Port : 139 State : open Service : netbios-ssn
Port : 445 State : open Service : microsoft-ds
Port : 135 State : open Service : msrpc
END
PROTOCOL: udp
Port : 137 State : open Service : netbios-ns
END
IP: 193.255.108.87
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 443 State : open Service : https
END
PROTOCOL: udp
Port : 1900 State : closed Service : upnp
END
```

Figure 7: User type an IP address and find out that this address has no SNMP listening on. Author did some scanning on university's network. Results were written on snmp.dat

8. SYN Flood (selection '7')

One of the features of this program is to SYN flood one address. First, function asks user some input such as port range. Then, it creates a bunch of TCP packets with SYN flag set. It sends crafted packets multiple times.

(Actually,there was a spoofing capability. When the function was crafting a packet, it produced a random IP to put in IP Header of Scapy Packet. However,due to unobservability via Wireshark, author decided to remove it. User can find it in the comment of that function.)



```
ip.dst == 193.255.108.87
```

```
No.     Time          Source          Destination      Protocol  Length Info
   2950 146.798521411 192.168.1.105   193.255.108.87   TCP          54 42 → 276 [SYN] Seq=0 Win=1000 Len=0
   2951 146.866191119 192.168.1.105   193.255.108.87   TCP          54 42 → 277 [SYN] Seq=0 Win=1000 Len=0
   2952 146.946178622 192.168.1.105   193.255.108.87   TCP          54 42 → 278 [SYN] Seq=0 Win=1000 Len=0
   2953 147.010300430 192.168.1.105   193.255.108.87   TCP          54 42 → 279 [SYN] Seq=0 Win=1000 Len=0
   2954 147.090191188 192.168.1.105   193.255.108.87   TCP          54 42 → 280 [SYN] Seq=0 Win=1000 Len=0
   2955 147.158216518 192.168.1.105   193.255.108.87   TCP          54 42 → 281 [SYN] Seq=0 Win=1000 Len=0
   2956 147.234178528 192.168.1.105   193.255.108.87   TCP          54 42 → 282 [SYN] Seq=0 Win=1000 Len=0
   2957 147.302199912 192.168.1.105   193.255.108.87   TCP          54 42 → 283 [SYN] Seq=0 Win=1000 Len=0
   2958 147.374204118 192.168.1.105   193.255.108.87   TCP          54 42 → 284 [SYN] Seq=0 Win=1000 Len=0
   2959 147.426502025 192.168.1.105   193.255.108.87   TCP          54 42 → 285 [SYN] Seq=0 Win=1000 Len=0
```

```
▸ Frame 378: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_57:8a:a1 (90:48:9a:57:8a:a1), Dst: Tp-LinkT_9c:8a:e8 (d4:6e:0e:9c:8a:e8)
▸ Internet Protocol Version 4, Src: 192.168.1.105, Dst: 193.255.108.87
▸ Transmission Control Protocol, Src Port: 39828, Dst Port: 80, Seq: 0, Len: 0
```

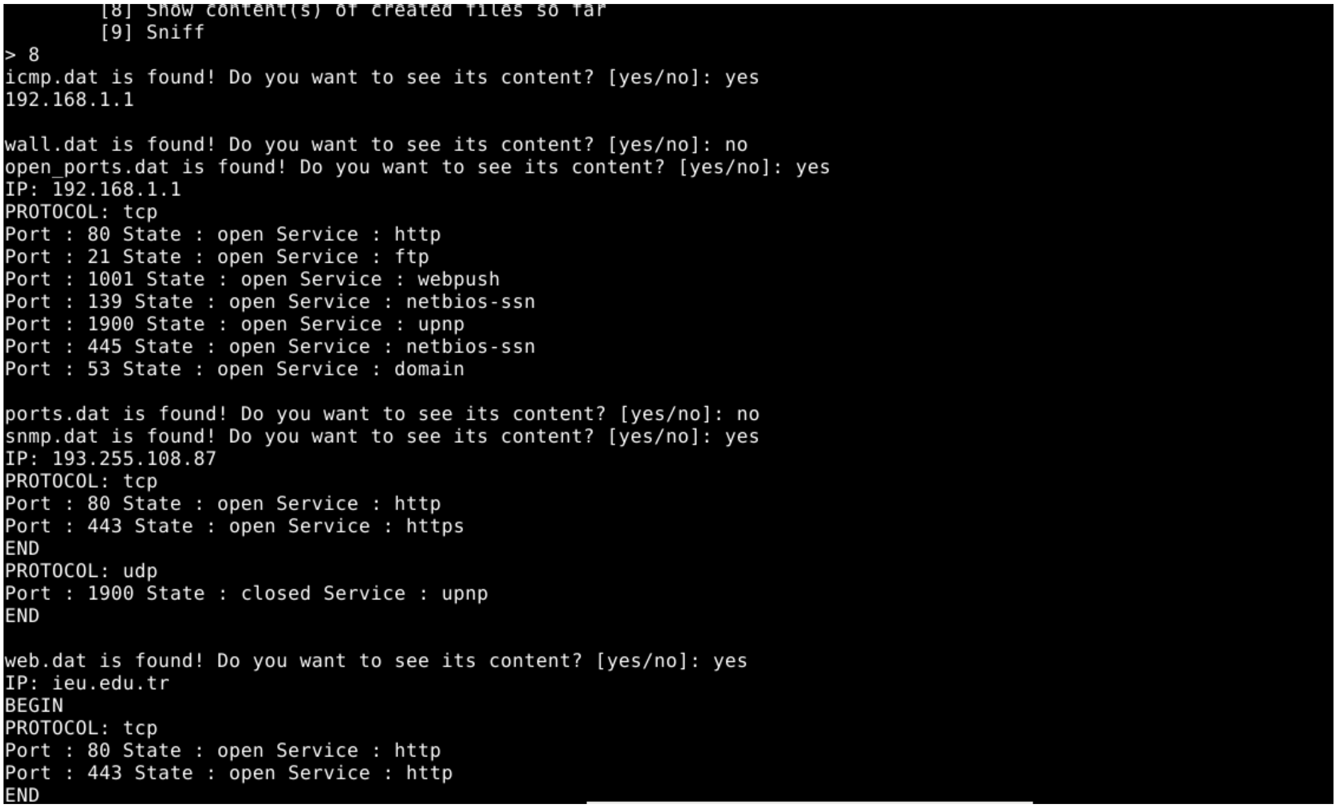
```
0000  d4 6e 0e 9c 8a e8 90 48  9a 57 8a a1 08 00 45 00   ·n·····H ·W····E·
0010  00 3c 8b 6e 40 00 40 06  be e5 c0 a8 01 69 c1 ff   ·<·n@·@· ·····i··
0020  6c 57 9b 94 00 50 82 33  0a 6f 00 00 00 00 a0 02   lW···P·3 ·o······
0030  72 10 3b 9d 00 00 02 04  05 b4 04 02 08 0a 00 5f   r·;····· ·······_
0040  81 01 00 00 00 00 01 03  03 0a                     ········ ··
```

Destination: IPv4 address   Packets: 3147 · Displayed: 2316 (73.6%)   Profile: Default

Figure 8: User chose to SYN flood a target and enter target IP. It is possible to observe floooding with wireshark

9. Show Content(s) of Created Files So Far (selection ‘8’)

User may want to see the contents of each file that are created via this program without actually going to the working directory of the program or user may not have any program to see contents of a text file. This feature helps user to see contents of created files by the program. User can choose which ones he/she wants to see.



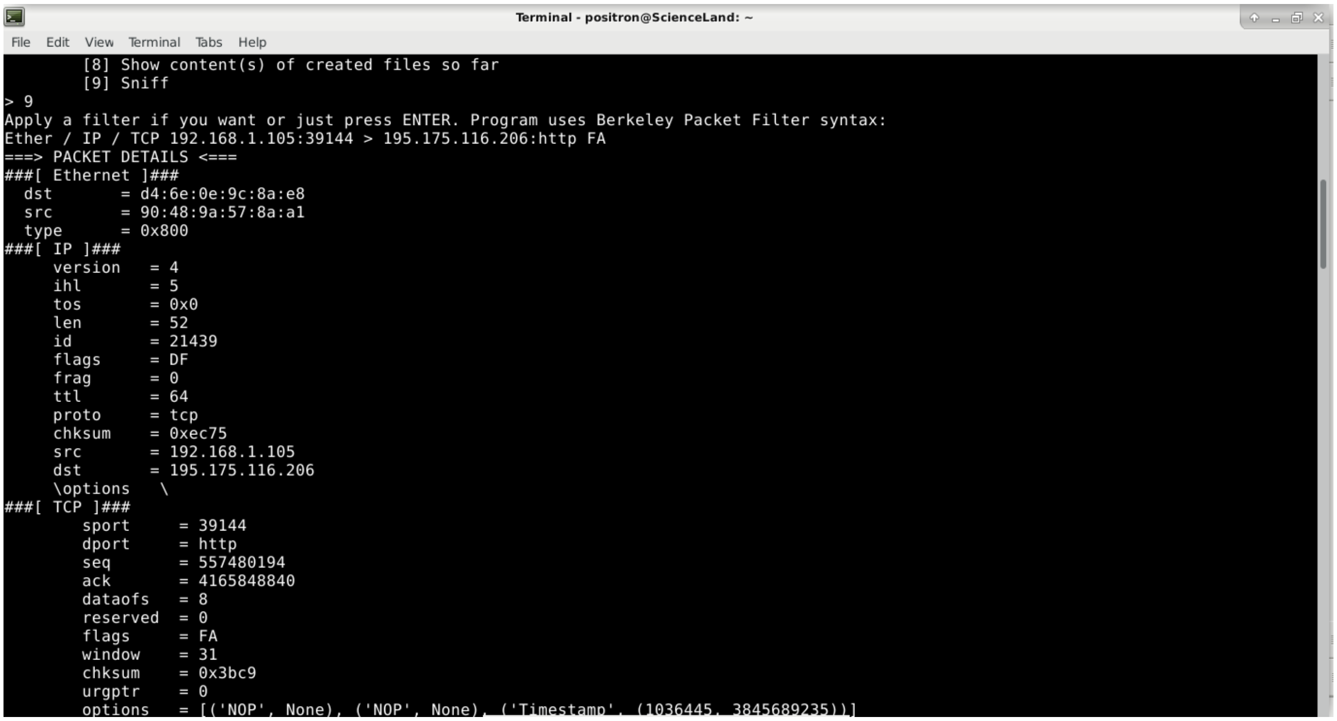
```
        [8] Show content(s) of created files so far
        [9] Sniff
> 8
icmp.dat is found! Do you want to see its content? [yes/no]: yes
192.168.1.1

wall.dat is found! Do you want to see its content? [yes/no]: no
open_ports.dat is found! Do you want to see its content? [yes/no]: yes
IP: 192.168.1.1
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 21 State : open Service : ftp
Port : 1001 State : open Service : webpush
Port : 139 State : open Service : netbios-ssn
Port : 1900 State : open Service : upnp
Port : 445 State : open Service : netbios-ssn
Port : 53 State : open Service : domain

ports.dat is found! Do you want to see its content? [yes/no]: no
snmp.dat is found! Do you want to see its content? [yes/no]: yes
IP: 193.255.108.87
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 443 State : open Service : https
END
PROTOCOL: udp
Port : 1900 State : closed Service : upnp
END

web.dat is found! Do you want to see its content? [yes/no]: yes
IP: ieu.edu.tr
BEGIN
PROTOCOL: tcp
Port : 80 State : open Service : http
Port : 443 State : open Service : http
END
```

Figure 9: m_show() function find and show created files.

Homework 2
Mert ARIKAN 20140601004

10. Sniffing (selection ‘9’)

The program also provide sniffing functionality via Scapy module. User can sniff the network and see contents of packets via this feature. It does not include save capability.


Terminal - positron@ScienceLand: ~
File Edit View Terminal Tabs Help

```
        [8] Show content(s) of created files so far
        [9] Sniff
> 9
Apply a filter if you want or just press ENTER. Program uses Berkeley Packet Filter syntax:
Ether / IP / TCP 192.168.1.105:39144 > 195.175.116.206:http FA
===> PACKET DETAILS <===
###[ Ethernet ]###
  dst       = d4:6e:0e:9c:8a:e8
  src       = 90:48:9a:57:8a:a1
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 52
     id        = 21439
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xec75
     src       = 192.168.1.105
     dst       = 195.175.116.206
     \options   \
###[ TCP ]###
        sport     = 39144
        dport     = http
        seq       = 557480194
        ack       = 4165848840
        dataofs   = 8
        reserved  = 0
        flags     = FA
        window    = 31
        chksum    = 0x3bc9
        urgptr    = 0
        options   = [('NOP', None), ('NOP', None), ('Timestamp', (1036445, 3845689235))]
```

Figure 10: Sniffing in progress.