TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

2IC80
Lab on offensive computer security

Manual for ARP/DNS spoofing tool
Group 3

Hristache, Ruxandra	1537180
Manka Huszar	1581368
Thanos Papamichail	1592378

Contents

1 How to run the tool

We have created a Linux-based tool which run on Python version 3.5. To start it, you need administrator rights. This can be done by either logging into the root environment (`sudo su`, followed on a new line by your command) or by running the command as a super user (`sudo command`).

`main.py` is the core of the program, which facilitates user interaction with the environment, thus one is only required to run this file. Either of the following commands would run the tool's help menu:

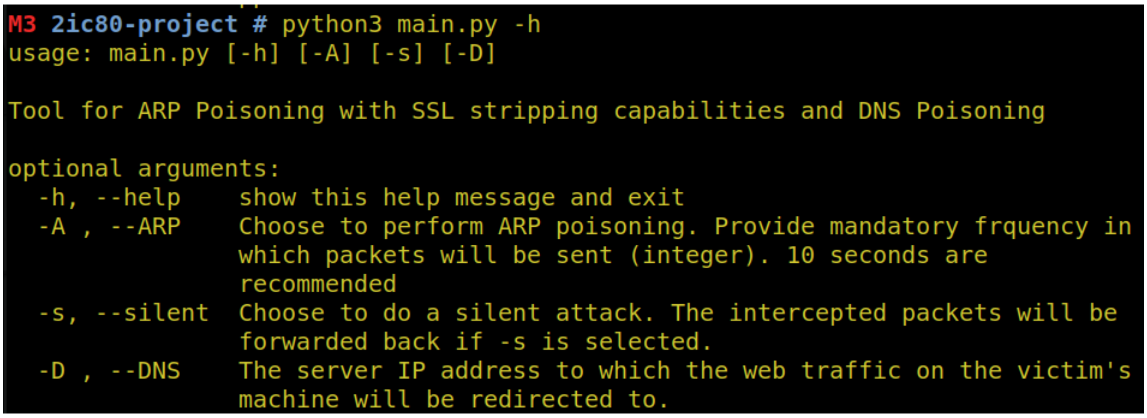
```
sudo su python3 main.py -h
sudo python3 main.py -h
```

2 Command line arguments

To perform an attack, the user would need to pick one of the various arguments which the software supports.

2.1 Help menu

The help menu describes all the possible arguments and their types.



```
M3 2ic80-project # python3 main.py -h
usage: main.py [-h] [-A] [-s] [-D]

Tool for ARP Poisoning with SSL stripping capabilities and DNS Poisoning

optional arguments:
  -h, --help    show this help message and exit
  -A , --ARP    Choose to perform ARP poisoning. Provide mandatory frquency in
                which packets will be sent (integer). 10 seconds are
                recommended
  -s, --silent  Choose to do a silent attack. The intercepted packets will be
                forwarded back if -s is selected.
  -D , --DNS    The server IP address to which the web traffic on the victim's
                machine will be redirected to.
```

Figure 1: Help menu - command line arguments

2.2 ARP poisoning arguments

ARP poisoning is called using the flag `--ARP/-A`, followed by an integer which indicates the frequency at which the attack will be performed. We recommend a frequency of 10 seconds for a consistent attack. ARP poisoning also supports the silent flag `--silent/-s` which enables packet forwarding so the attacker cannot be identified as a man-in-the-middle by the victim. `--silent/-s` does not require any data after it.

The following commands are possible for ARP poisoning:

- `pyton3 main.py -A 10` - perform ARP poisoning once every 10 seconds, but do not forward intercepted packets (all-out mode)
- `pyton3 main.py -A 10 -s` - perform ARP poisoning once every 10 seconds and forward intercepted packets (silent mode)

Any other combination which uses the flag `--ARP/-A` or `--silent/-s` is not supported and the tool will immediately stop.

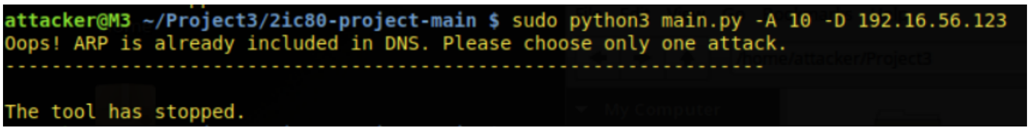
2.3 DNS poisoning arguments

DNS poisoning is called using the flag `--DNS/-D`, followed by a string which represents the IP address of the server to which the web traffic on the victim's machine will be redirected to. The program clearly mentions how `--DNS/-D` and `--silent/-s` cannot be used together since the DNS attack will not work if the packets keep being forwarded back to their destination.

There is only one command supported together with the DNS poisoning flag `--DNS/-D`, which is:

- `pyton3 main.py -D 192.168.56.102` - perform DNS poisoning and forward the web traffic on the victim's machine to the web page hosted on the server with the IP address 192.168.56.102

Any other combination with the flag `--DNS/-D` will make the tool stop immediately.



```
attacker@M3 ~/Project3/2ic80-project-main $ sudo python3 main.py -A 10 -D 192.16.56.123
Oops! ARP is already included in DNS. Please choose only one attack.
------------------------------------------------------------------

The tool has stopped.
```

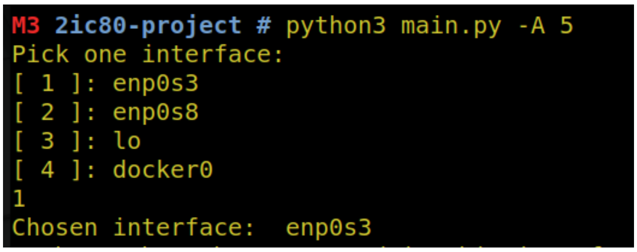
Figure 2: Invalid argument configuration

3 Interface and host discovery

Both attacks come with an integrated network discovery, which works by sniffing the traffic inside the local network. This section appears in different moments, depending on the attack you choose. For ARP it shows up right away, but with DNS, you first need to specify the domain names which should be spoofed. If, during either interface or host discovery, the scan is unsuccessful, the tool stops since it cannot continue without those parameters.

3.1 Interface discovery

The user is required to choose **one** interface on which the host scan will be performed. This is done by typing the corresponding number into the terminal.

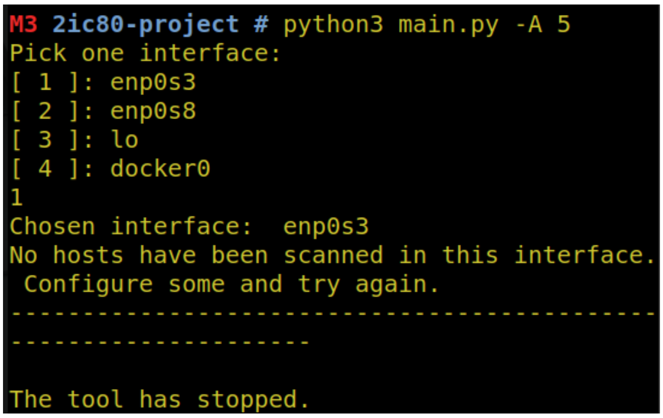


```
M3 2ic80-project # python3 main.py -A 5
Pick one interface:
[ 1 ]: enp0s3
[ 2 ]: enp0s8
[ 3 ]: lo
[ 4 ]: docker0
1
Chosen interface:  enp0s3
```

Figure 3: Interface scanning

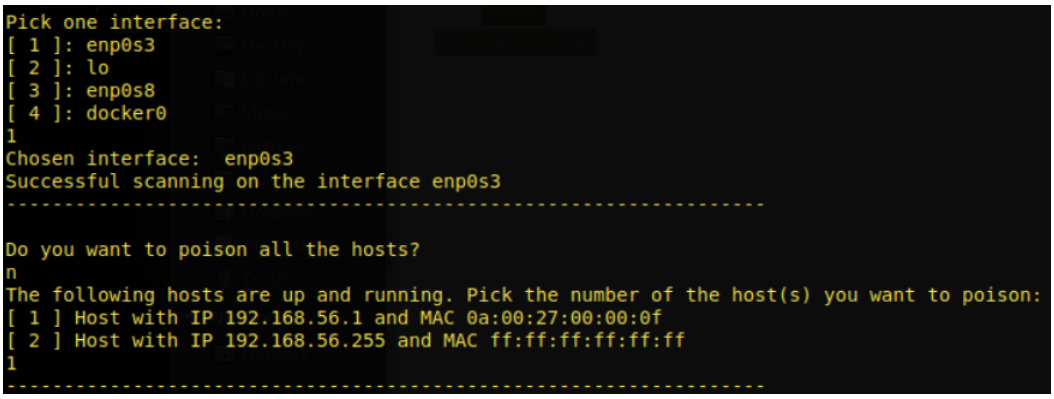
3.2 Host discovery

Once the interface has been chosen, it will be scanned for any incoming and outgoing traffic in order to store the IP and MAC addresses of all the available hosts. This is why, it is important to ping your targets while you use this tool. The generated traffic will make them immediately show up under the host discovery algorithm.



```
M3 2ic80-project # python3 main.py -A 5
Pick one interface:
[ 1 ]: enp0s3
[ 2 ]: enp0s8
[ 3 ]: lo
[ 4 ]: docker0
1
Chosen interface:  enp0s3
No hosts have been scanned in this interface.
 Configure some and try again.
---------------------------------------------
---------------------

The tool has stopped.
```

Figure 4: Unsuccessful host scanning

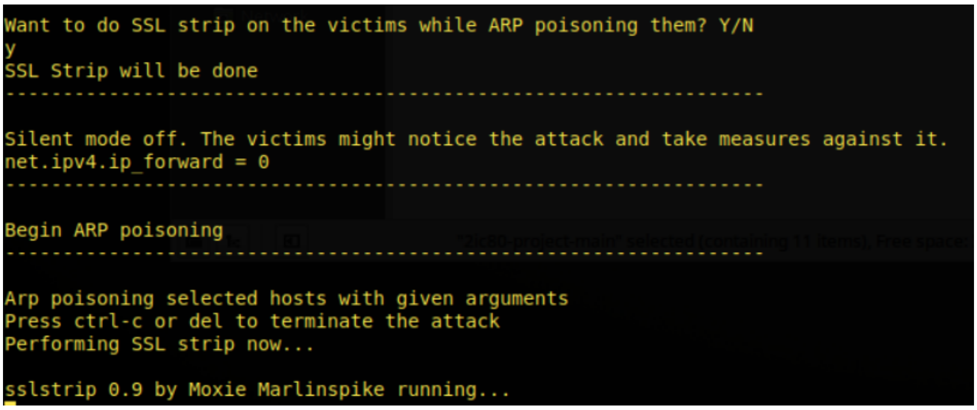


```
Pick one interface:
[ 1 ]: enp0s3
[ 2 ]: lo
[ 3 ]: enp0s8
[ 4 ]: docker0
1
Chosen interface:  enp0s3
Successful scanning on the interface enp0s3
-----------------------------------------------------------------

Do you want to poison all the hosts?
n
The following hosts are up and running. Pick the number of the host(s) you want to poison:
[ 1 ] Host with IP 192.168.56.1 and MAC 0a:00:27:00:00:0f
[ 2 ] Host with IP 192.168.56.255 and MAC ff:ff:ff:ff:ff:ff
1
-----------------------------------------------------------------
```

Figure 5: Successful host scanning

4 ARP poisoning

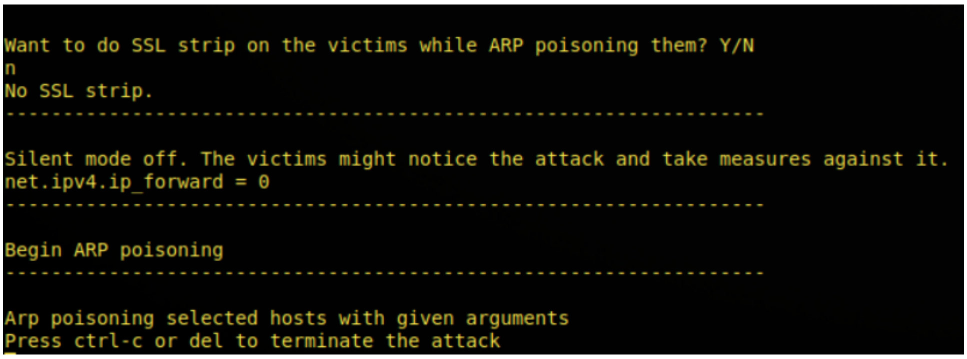
Once the network is successfully scanned, the ARP poisoning attack begins by asking the user if they would like to concomitantly perform an SSL strip on the victim. If the response is yes, a corresponding message is displayed. The SSL strip can be stopped by pressing `ctrl+c` or `del`.



```
Want to do SSL strip on the victims while ARP poisoning them? Y/N
y
SSL Strip will be done
------------------------------------------------------------------

Silent mode off. The victims might notice the attack and take measures against it.
net.ipv4.ip_forward = 0
------------------------------------------------------------------

Begin ARP poisoning
------------------------------------------------------------------

Arp poisoning selected hosts with given arguments
Press ctrl-c or del to terminate the attack
Performing SSL strip now...

sslstrip 0.9 by Moxie Marlinspike running...
```

Figure 6: ARP poisoning with SSL stripping

If the user requests no SSL strip, the simple ARP attack will begin right away.



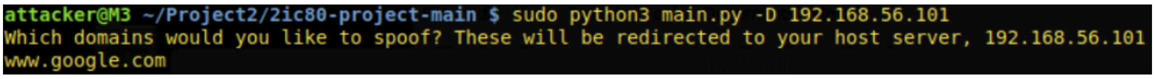
```
Want to do SSL strip on the victims while ARP poisoning them? Y/N
n
No SSL strip.
------------------------------------------------------------------

Silent mode off. The victims might notice the attack and take measures against it.
net.ipv4.ip_forward = 0
------------------------------------------------------------------

Begin ARP poisoning
------------------------------------------------------------------

Arp poisoning selected hosts with given arguments
Press ctrl-c or del to terminate the attack
```

Figure 7: ARP poisoning without SSL stripping

To check if ARP poisoning was successful, one needs to look at the ARP tables of the victims and confirm that the MAC address has been changed to attacker's MAC address.

5 DNS poisoning

The DNS attack begins by inquiring the domain names which the tool will spoof. They must be given as URL links. The tool then verifies if there is a corresponding IP address to said domain. If there is, it means the URL is valid and the attack begins. If there is not, the tool stops.



```
attacker@M3 ~/Project2/2ic80-project-main $ sudo python3 main.py -D 192.168.56.101
Which domains would you like to spoof? These will be redirected to your host server, 192.168.56.101
www.google.com
```

Figure 8: Inputting domain names which will be spoofed

Since DNS poisoning requires the attacker to be man-in-the-middle, this implies that ARP poisoning must be done at the same time. However, the user does not have the option to choose the frequency of the ARP attack, so it will be performed with the recommended setting of 10 seconds.

6 Stopping the ongoing attack

Any ongoing attack can be simply stopped by pressing `ctrl+c` or `del`. Since the attacks run on multiple process, a forced stopping of the program will make the processes misbehave and that will show an error, unrelated to the functionality of the code.

7 Issues

Unfortunately, due to set-up issues, the DNS poisoning attack could not be verified. It is possible that on other systems it could be safely deployed. Similar problem with SSL strip.