Assignment 4: DNF Spoof
COMP 8505

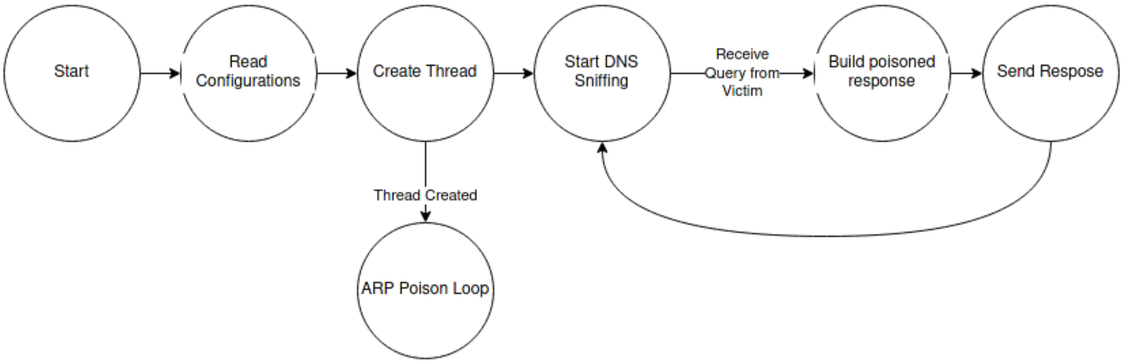
Nicole Jingco

A01001875

Table of Contents

Design

State Diagram



Pseudocode

Main

```
{
      Read configuration file
      Start arp poisoning on a thread
      Start DNF sniffing
}
```

Arp Poisoning

```
{
      Build Arp Packet
      While running:
            Send arp poison packet to Victim
            Send arp poison packet to Router
}
```

DNF Sniffing

```
{
      Start sniffing for DNS Query packets loop
      Build DNS Spoof Answer packet
      Send spoofed packet to victim
}
```

Tests

The application does not need to have firewall rules on. The application needs the have ip forwarding enabled:

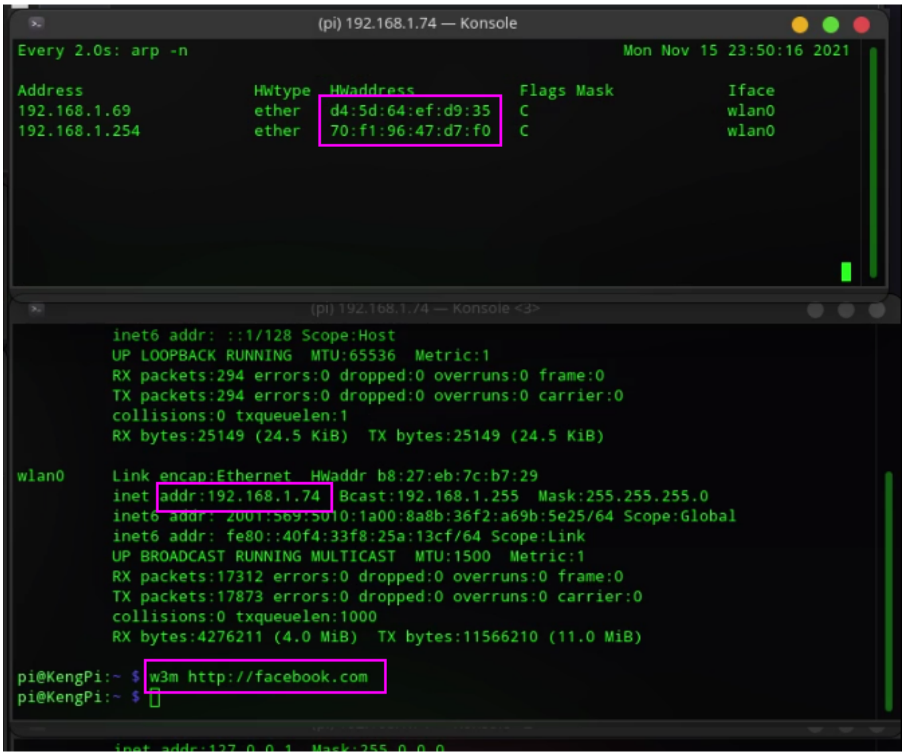
```
echo 1 >> /proc/sys/net/ipv4/ip_forward
```

Victim: 192.168.1.74
Attacker: 192.168.1.69
Router: 192.168.1.254

Case #	Description	Result	Passed
1	Access facebook without spoofing	Return the facebook website	yes
2	Arp Poisoning	Router Mac Address shows Attacker Mac Address	yes
3	DNS Spoofing	Victim trying to go to http://facebook.com will be redirected to the victims apache server	yes

Case 1 - Access facebook without spoofing

Without arp poisoning and dns spoofing using w3n to browse http://facebook.com



(pi) 192.168.1.74 — Konsole

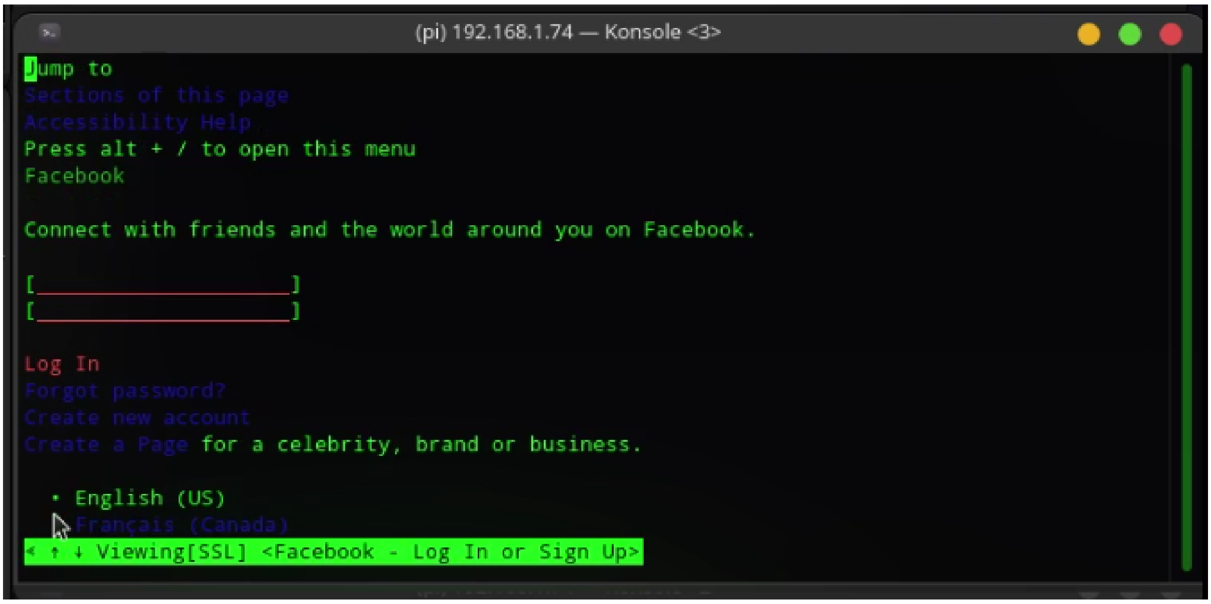
```
Every 2.0s: arp -n                                              Mon Nov 15 23:50:16 2021

Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.69             ether   d4:5d:64:ef:d9:35   C                     wlan0
192.168.1.254            ether   70:f1:96:47:d7:f0   C                     wlan0
```

(pi) 192.168.1.74 — Konsole <3>

```
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:294 errors:0 dropped:0 overruns:0 frame:0
          TX packets:294 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:25149 (24.5 KiB)  TX bytes:25149 (24.5 KiB)

wlan0     Link encap:Ethernet  HWaddr b8:27:eb:7c:b7:29
          inet addr:192.168.1.74  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:569:5010:1a00:8a8b:36f2:a69b:5e25/64 Scope:Global
          inet6 addr: fe80::40f4:33f8:25a:13cf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17312 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17873 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4276211 (4.0 MiB)  TX bytes:11566210 (11.0 MiB)

pi@KengPi:~ $ w3m http://facebook.com
pi@KengPi:~ $
```

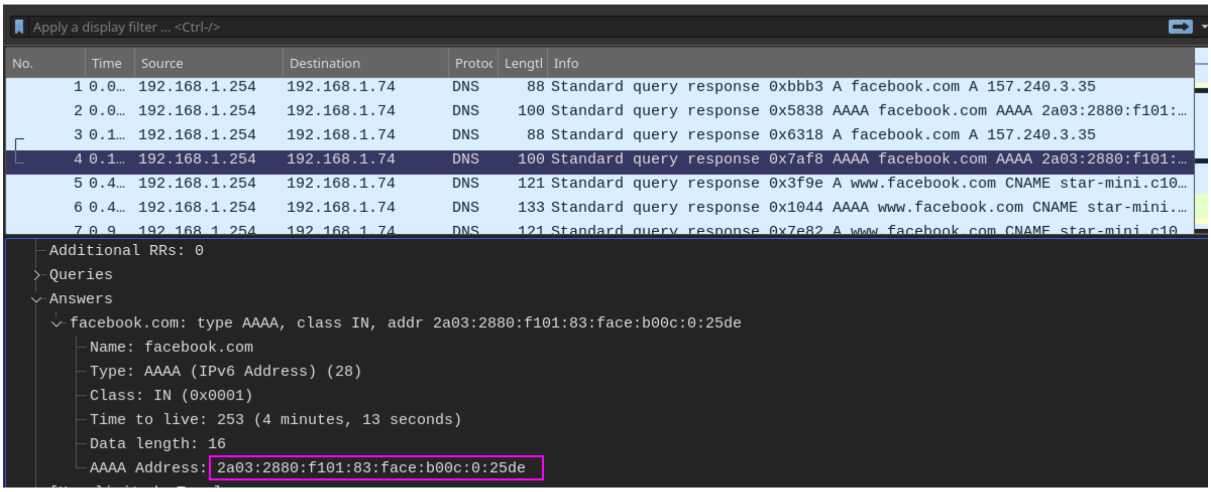
```
          inet addr:127.0.0.1  Mask:255.0.0.0
```

This will return the facebook’s webpage contents on the console



```
Jump to
Sections of this page
Accessibility Help
Press alt + / to open this menu
Facebook

Connect with friends and the world around you on Facebook.

[____________________]
[____________________]

Log In
Forgot password?
Create new account
Create a Page for a celebrity, brand or business.

  • English (US)
    Français (Canada)
← ↑ ↓ Viewing[SSL] <Facebook - Log In or Sign Up>
```

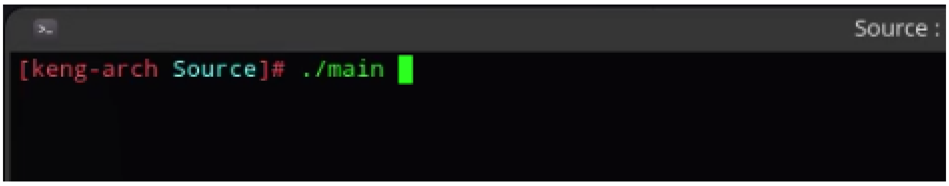
On the victims packet captures it will send the response with the real facebook address



```
No.    Time  Source         Destination    Protoc Lengtl Info
     1 0.0…  192.168.1.254  192.168.1.74   DNS       88 Standard query response 0xbbb3 A facebook.com A 157.240.3.35
     2 0.0…  192.168.1.254  192.168.1.74   DNS      100 Standard query response 0x5838 AAAA facebook.com AAAA 2a03:2880:f101:…
     3 0.1…  192.168.1.254  192.168.1.74   DNS       88 Standard query response 0x6318 A facebook.com A 157.240.3.35
     4 0.1…  192.168.1.254  192.168.1.74   DNS      100 Standard query response 0x7af8 AAAA facebook.com AAAA 2a03:2880:f101:…
     5 0.4…  192.168.1.254  192.168.1.74   DNS      121 Standard query response 0x3f9e A www.facebook.com CNAME star-mini.c10…
     6 0.4…  192.168.1.254  192.168.1.74   DNS      133 Standard query response 0x1044 AAAA www.facebook.com CNAME star-mini.…
     7 0.9   192.168.1.254  192.168.1.74   DNS      121 Standard query response 0x7e82 A www.facebook.com CNAME star-mini.c10

  Additional RRs: 0
 > Queries
 v Answers
   v facebook.com: type AAAA, class IN, addr 2a03:2880:f101:83:face:b00c:0:25de
       Name: facebook.com
       Type: AAAA (IPv6 Address) (28)
       Class: IN (0x0001)
       Time to live: 253 (4 minutes, 13 seconds)
       Data length: 16
       AAAA Address: 2a03:2880:f101:83:face:b00c:0:25de
```

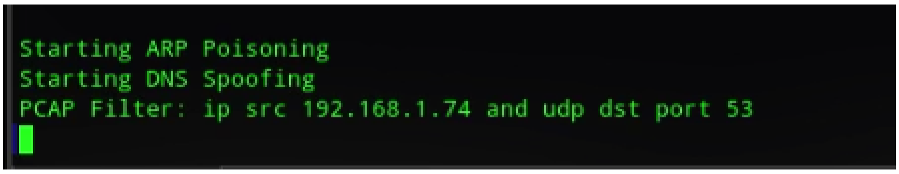
Case 2 - Arp Poisoning

When I start the dns spoofing program



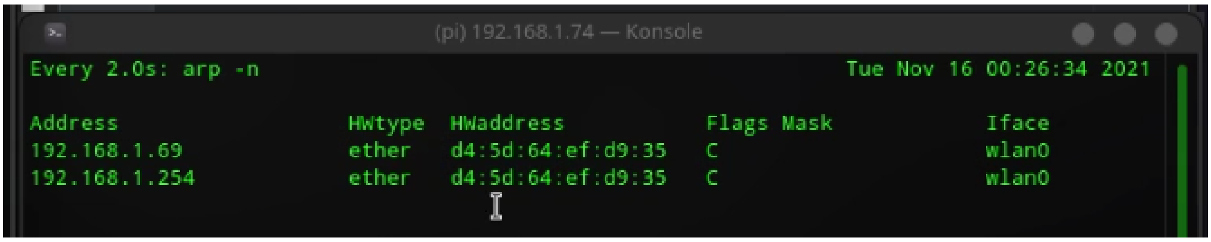
```
[keng-arch Source]# ./main
```

It will start spoofing



```
Starting ARP Poisoning
Starting DNS Spoofing
PCAP Filter: ip src 192.168.1.74 and udp dst port 53
```

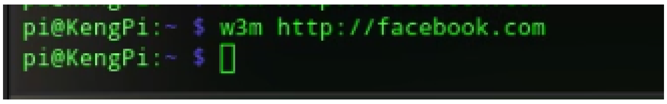
The Victims arp table will show the routers mac address change to the attacker's mac address



```
Every 2.0s: arp -n                                          Tue Nov 16 00:26:34 2021

Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.69             ether   d4:5d:64:ef:d9:35   C                     wlan0
192.168.1.254            ether   d4:5d:64:ef:d9:35   C                     wlan0
```

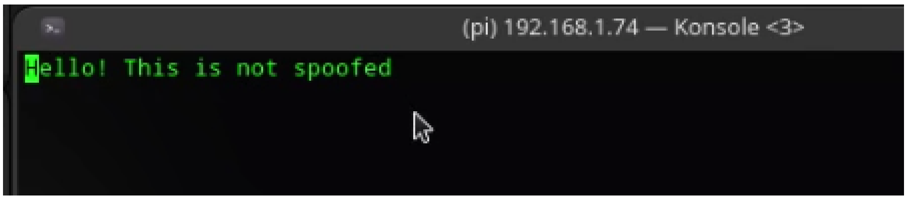
Case 3 - DNS Spoofing

While the router is poisoned we can we try to open http://facebook.com



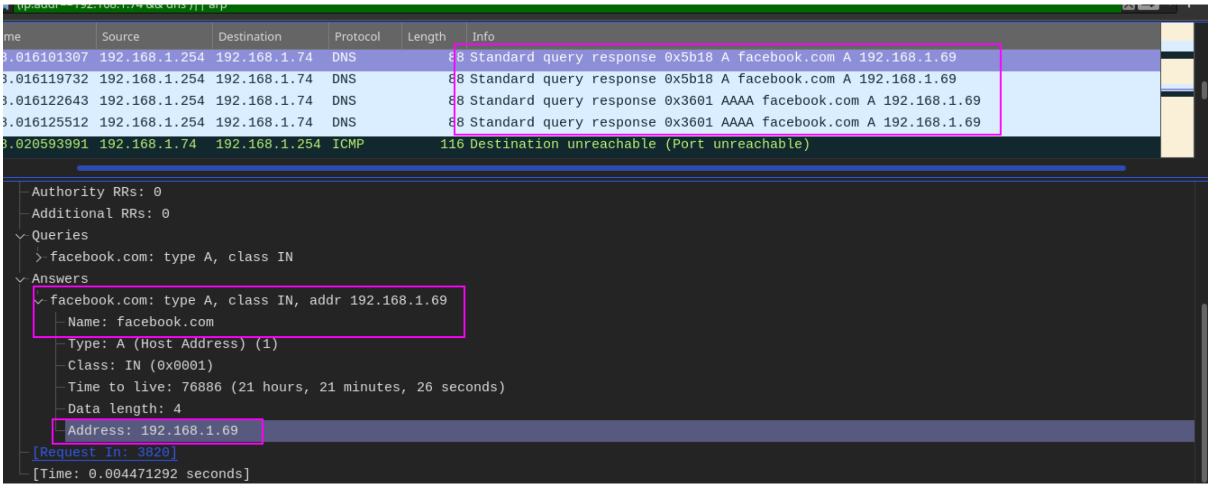
```
pi@KengPi:~ $ w3m http://facebook.com
pi@KengPi:~ $
```

And it will return the spoofed page



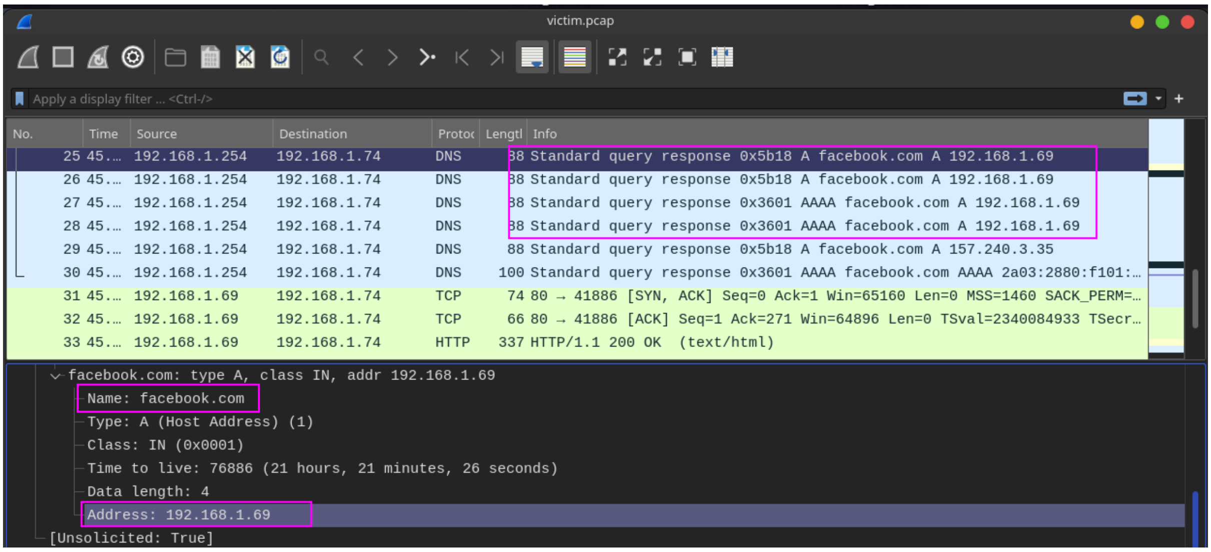
```
Hello! This is not spoofed
```

On the attackers packet capture it will show the dns response of facebook with the spoofed address



```
me          Source         Destination    Protocol   Length   Info
.016101307  192.168.1.254  192.168.1.74   DNS            88 Standard query response 0x5b18 A facebook.com A 192.168.1.69
.016119732  192.168.1.254  192.168.1.74   DNS            88 Standard query response 0x5b18 A facebook.com A 192.168.1.69
.016122643  192.168.1.254  192.168.1.74   DNS            88 Standard query response 0x3601 AAAA facebook.com A 192.168.1.69
.016125512  192.168.1.254  192.168.1.74   DNS            88 Standard query response 0x3601 AAAA facebook.com A 192.168.1.69
.020593991  192.168.1.74   192.168.1.254  ICMP          116 Destination unreachable (Port unreachable)

 Authority RRs: 0
 Additional RRs: 0
 Queries
   facebook.com: type A, class IN
 Answers
   facebook.com: type A, class IN, addr 192.168.1.69
     Name: facebook.com
     Type: A (Host Address) (1)
     Class: IN (0x0001)
     Time to live: 76886 (21 hours, 21 minutes, 26 seconds)
     Data length: 4
     Address: 192.168.1.69
 [Request In: 3820]
 [Time: 0.004471292 seconds]
```

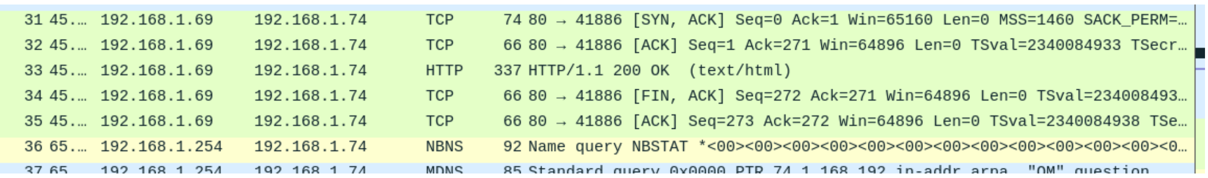
We can also see the spoofed dns response on the victims packet captures



victim.pcap

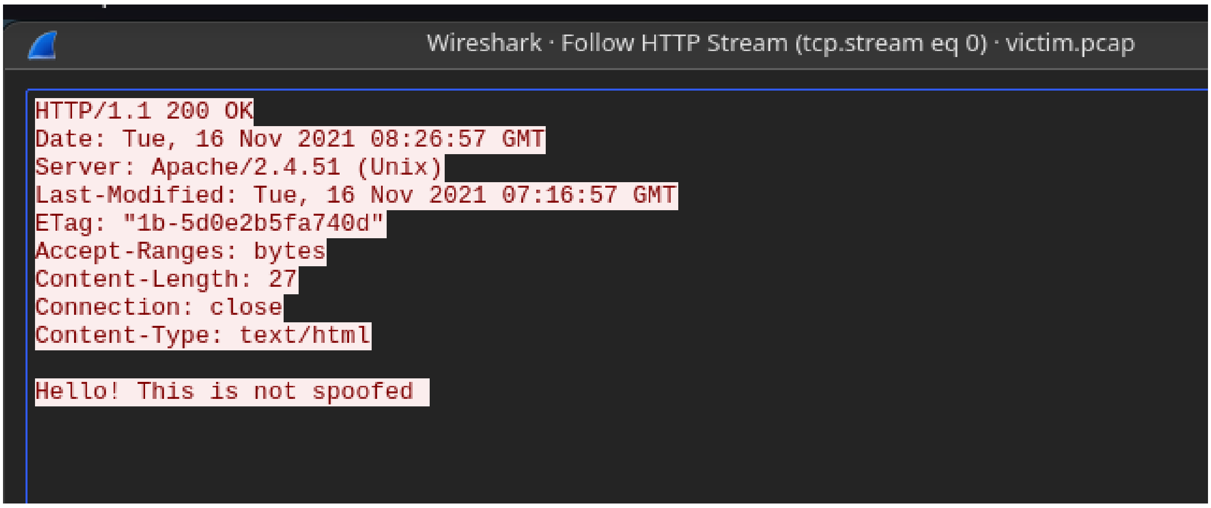
```
No.  Time  Source         Destination    Protoc Lengtl Info
 25  45.…  192.168.1.254  192.168.1.74   DNS      88 Standard query response 0x5b18 A facebook.com A 192.168.1.69
 26  45.…  192.168.1.254  192.168.1.74   DNS      88 Standard query response 0x5b18 A facebook.com A 192.168.1.69
 27  45.…  192.168.1.254  192.168.1.74   DNS      88 Standard query response 0x3601 AAAA facebook.com A 192.168.1.69
 28  45.…  192.168.1.254  192.168.1.74   DNS      88 Standard query response 0x3601 AAAA facebook.com A 192.168.1.69
 29  45.…  192.168.1.254  192.168.1.74   DNS      88 Standard query response 0x5b18 A facebook.com A 157.240.3.35
 30  45.…  192.168.1.254  192.168.1.74   DNS     100 Standard query response 0x3601 AAAA facebook.com AAAA 2a03:2880:f101:…
 31  45.…  192.168.1.69   192.168.1.74   TCP      74 80 → 41886 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=…
 32  45.…  192.168.1.69   192.168.1.74   TCP      66 80 → 41886 [ACK] Seq=1 Ack=271 Win=64896 Len=0 TSval=2340084933 TSecr…
 33  45.…  192.168.1.69   192.168.1.74   HTTP    337 HTTP/1.1 200 OK  (text/html)

   facebook.com: type A, class IN, addr 192.168.1.69
     Name: facebook.com
     Type: A (Host Address) (1)
     Class: IN (0x0001)
     Time to live: 76886 (21 hours, 21 minutes, 26 seconds)
     Data length: 4
     Address: 192.168.1.69
 [Unsolicited: True]
```

We can also see the http traffic



```
 31 45.…  192.168.1.69    192.168.1.74   TCP     74 80 → 41886 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=…
 32 45.…  192.168.1.69    192.168.1.74   TCP     66 80 → 41886 [ACK] Seq=1 Ack=271 Win=64896 Len=0 TSval=2340084933 TSecr…
 33 45.…  192.168.1.69    192.168.1.74   HTTP   337 HTTP/1.1 200 OK  (text/html)
 34 45.…  192.168.1.69    192.168.1.74   TCP     66 80 → 41886 [FIN, ACK] Seq=272 Ack=271 Win=64896 Len=0 TSval=234008493…
 35 45.…  192.168.1.69    192.168.1.74   TCP     66 80 → 41886 [ACK] Seq=273 Ack=272 Win=64896 Len=0 TSval=2340084938 TSe…
 36 65.…  192.168.1.254   192.168.1.74   NBNS    92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><0…
 37 65    192 168 1 254   192 168 1 74   MDNS    85 Standard query 0x0000 PTR 74 1 168 192 in-addr arpa  "QM" question
```

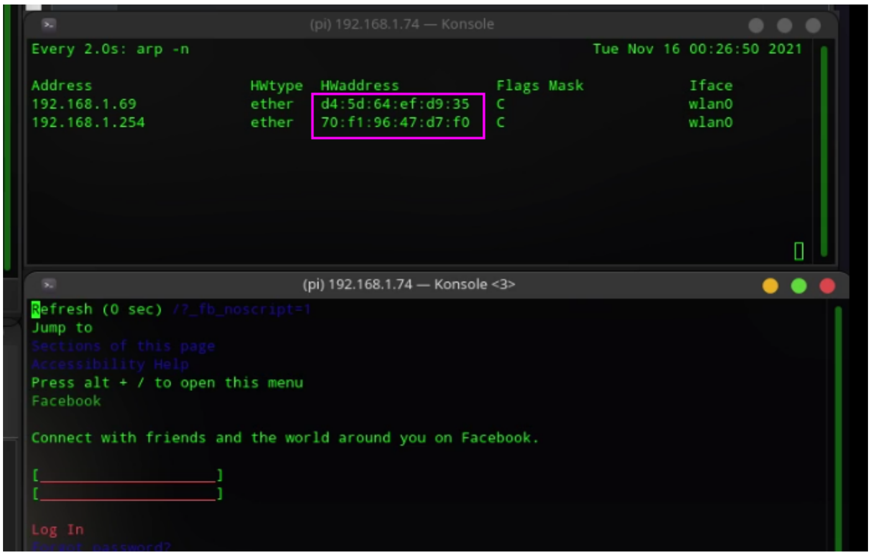
When followed will displace the message



Wireshark · Follow HTTP Stream (tcp.stream eq 0) · victim.pcap

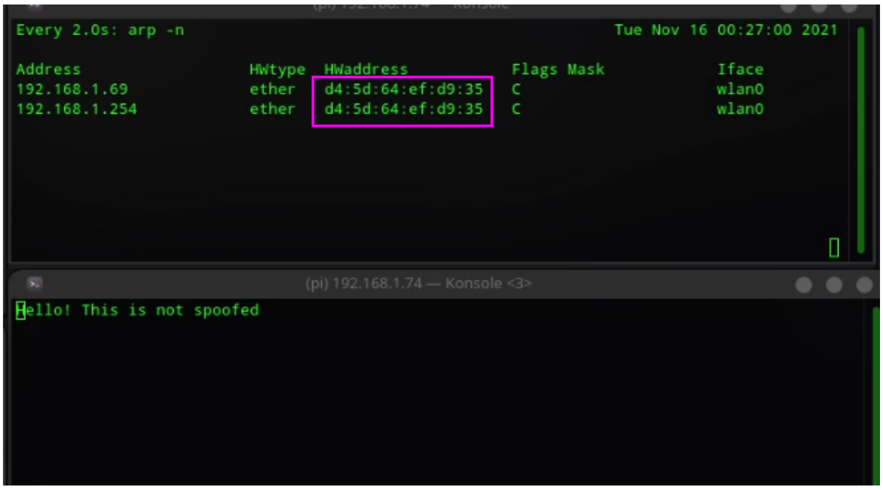
```
HTTP/1.1 200 OK
Date: Tue, 16 Nov 2021 08:26:57 GMT
Server: Apache/2.4.51 (Unix)
Last-Modified: Tue, 16 Nov 2021 07:16:57 GMT
ETag: "1b-5d0e2b5fa740d"
Accept-Ranges: bytes
Content-Length: 27
Connection: close
Content-Type: text/html

Hello! This is not spoofed
```

Side Note:
In the demo video, the router's mac address changed back to normal and the real dns response was able to get through. Once the router got poisoned again it was able to receive the spoofed dns packet.



```
Every 2.0s: arp -n                                        Tue Nov 16 00:26:50 2021

Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.69             ether   d4:5d:64:ef:d9:35   C                     wlan0
192.168.1.254            ether   70:f1:96:47:d7:f0   C                     wlan0
```

```
Refresh (0 sec) /?_fb_noscript=1
Jump to
Sections of this page
Accessibility Help
Press alt + / to open this menu
Facebook

Connect with friends and the world around you on Facebook.

[________________________]
[________________________]

Log In
Forgot password?
```



```
Every 2.0s: arp -n                                         Tue Nov 16 00:27:00 2021

Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.69             ether   d4:5d:64:ef:d9:35   C                     wlan0
192.168.1.254            ether   d4:5d:64:ef:d9:35   C                     wlan0
```

```
Hello! This is not spoofed
```