ARP Spoofing with Ettercap

By: Devery Channell
What is ARP

- ARP stands for Address Resolution Protocol
- It allows the network to translate IP addresses into MAC addresses.
- ARP works like this:
  - If a host using IP on a LAN ties to contact another it needs the **MAC Address** of the host it is trying to contact.
  - It first looks in its **ARP cache** to see if it already knows the **MAC Address**
  - If not, it broadcasts out an **ARP Request** asking "Yo, who has this IP address I'm looking for?"
Even with a switched network it’s not hard for an attacker to ARPSPOOF and redirect traffic through them for the purposes of sniffing.

Useful arpspoofing tools:

- Dsniff
- Ettercap
- Cain (Windows)

These tools can even parse out usernames and passwords automatically, making the attacker's job easy.
Uses of Arpspoofing

- Sniff SSL encrypted information
  - Passwords
  - Emails
  - Usernames
  - FTP Accounts
  - Etc.
- Any online authentication requiring credentials can be sniffed when arpspoofing.
Ettercap is a suite for man in the middle attacks on LAN.

It features sniffing of live connections, content filtering on the fly and many other interesting tricks.

This suite also includes a very useful GUI. (seen to the left)
Helpful Commands

- `arp -a`
  - Lists all entries in machines arp cache
- `arp -d`
  - Clear out machines arp cache
- `Ettercap -T -q -M ARP // //`
  - `-T`: Use Text based interaction
  - `-q`: Be relatively quiet while spoofing
  - `-M`: type of MITM attack to use
- `Ettercap -G`
  - `-G`: Use Gui version
How does it work?
Sample ARP Traffic

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.679064</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>75.589440</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>75.589536</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>76.699838</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>76.699920</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>77.710230</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.1 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>77.710315</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>Who has 192.168.1.23? Tell 192.168.1.1</td>
</tr>
<tr>
<td>77.865976</td>
<td>WestellT_3b:e9:ac</td>
<td>Broadcast</td>
<td>ARP</td>
<td>Who has 192.168.1.37 Tell 192.168.1.4</td>
</tr>
<tr>
<td>82.040040</td>
<td>Giga-Byt_34:64:9c</td>
<td>Broadcast</td>
<td>ARP</td>
<td>Who has 192.168.1.13 Tell 192.168.1.4</td>
</tr>
<tr>
<td>82.043777</td>
<td>Alfa_1a:ec:33</td>
<td>Giga-Byt_34:64:9c</td>
<td>ARP</td>
<td>192.168.1.13 is at 00:c0:ca:1a:ec:33</td>
</tr>
<tr>
<td>87.039392</td>
<td>WestellT_3b:e9:ac</td>
<td>Giga-Byt_34:64:9c</td>
<td>ARP</td>
<td>Who has 192.168.1.47 Tell 192.168.1.1</td>
</tr>
<tr>
<td>87.039414</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.14 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>87.720611</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.13 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>87.720674</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.11 is at 00:1a:4d:34:64:9c</td>
</tr>
<tr>
<td>90.536335</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.13 is at 00:ca:1a:ec:33</td>
</tr>
<tr>
<td>90.536435</td>
<td>Giga-Byt_34:64:9c</td>
<td>Alfa_1a:ec:33</td>
<td>ARP</td>
<td>192.168.1.11 is at 00:23:97:3b:e9:ac</td>
</tr>
<tr>
<td>90.536556</td>
<td>Giga-Byt_34:64:9c</td>
<td>WestellT_3b:e9:ac</td>
<td>ARP</td>
<td>192.168.1.13 is at 00:ca:1a:ec:33</td>
</tr>
</tbody>
</table>

Frame 24 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Giga-Byt_34:64:9c (00:1a:4d:34:64:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

0000 ff ff ff ff ff ff 00 1a 4d 34 64 9c 08 06 00 01 .......... M4d.....
0010 08 00 06 04 00 01 00 1a 4d 34 64 9c c0 a8 01 04 .......... M4d.....
0020 00 00 00 00 00 00 00 c0 a8 01 01 ...........
Examples

- ARP Spoofing
  - IG – *Intro to sniffers*
- DNS Spoofing
  - IG - *DNS Spoofing with Ettercap*
  - SecurityTube – *Etter Filters Tut*