Lab 4: ARP and ICMP

Aim:

To provide a foundation in understanding ARP and ICMP.

Time to complete: Up to 45 minutes.

Activities:

- **Complete Lab 4**: ARP and ICMP.
- **Complete Test 4**.

Leaning Activities:

At the end of these activities, you should understand:

- How to determine key details related to ARP and ICMP.
- Understand how ARP allows hosts to discover hosts on a network.
- Capture traffic for traces.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- Which network protocol is likely to be the first to be used when someone communicating over the Internet?

- In a highly secure environment, why might host have statically assigned addresses in their ARP cache?

- How might an intruder change the gateway MAC address that a host connects to?

- What device bounds the scope of an ARP request?

- With a trace route which network devices do we see along the way?

Lab 4: ARP and ICMP

1 Details

Aim: To provide a foundation in understanding ARP and ICMP.

The demo of this lab is at: http://youtu.be/T_jrAwZfE74

2 Activities

L1.1 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/webpage.zip

In this case a host connects to a Web server. Determine the following:

By examining the ARP request and reply. What is the IP and MAC address of the server for the host:

Why does the host not go through a gateway:

L1.2 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/googleWeb.zip

In this case a host connects to the Google Web server. Determine the following:

By examining the ARP request and reply. What is the IP and MAC address of the gateway for the host:

Can we determine the MAC address of the Google Web server?

L1.3 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/arp_scan.zip

Determine the following:

This was generated by an intruder.

What can you say about the aim of the scan?

What can say about whether this is an inside intruder or an external one?

Which nodes did the intruder find where connected to the network?

L1.4 **Start capturing network** packets on your main network adapter. Next go to **intel.com**, and access the page. Stop the network capture, and then from your network traffic, determine:

By examining the ARP request and reply. What is the IP and MAC address of the gateway for your host:

L1.5 **In Windows, using a command line console perform the following:**

Determine you ARP cache, by running arp –a**:**

Now ask your neighbour what their IP address is, and the ping it. Re-examine your ARP cache. What has changed:

Now add the address as a static route, using the command in the form: arp –s 1.2.3.4 00-11-22-33-44-55-66. Re-examine your ARP cache. How has it changed:

From your ARP cache, what is the MAC address of the gateway:

L1.6 **Start capturing network** packets on your main network adapter. Next go to **intel.com**, and access the page. Stop the network capture, and then from your network traffic, determine:

By examining the ARP request and reply. What is the IP and MAC address of the gateway for your host:

L1.7 **In Windows, using a command line console, and using the command tracert, determine the route to the following:**

Route to IBM.COM:

Route to INTEL.COM:

Which parts of these routes are the same, and why?

L1.8 Repeat the previous exercise, but this time capture the network traffic with Wireshark. Now determine the following:

Which ICMP type is used for the ping request?

Which ICMP type is used for the ping reply?

L1.9 From your Windows and also from Linux host, capture the traffic from a ping, and determine the payload:

Ping payload for Windows

Ping payload for Linux: