Lab 2: Ethernet, IP and TCP

Aim:

To provide a foundation in understanding Ethernet, IP and TCP

Time to complete: Up to 45 minutes.

Activities:

- **Complete Lab 2**: Ethernet, IP and TCP
- **Complete Test 2**.

Leaning Activities:

At the end of these activities, you should understand:

- How to determine key details related to Ethernet, IP and TCP
- Capture traffic for traces.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- In Wireshark, how might you view all the MAC addresses which are involved in the communication? For this, investigate some of the options that Wireshark provides.

- In Wireshark, how might you view all the IP addresses which are involved in the communication? For this, investigate some of the options that Wireshark provides.

- In Wireshark, how might you view all the TCP ports which are involved in the communication? For this, investigate some of the options that Wireshark provides.

Lab 2: Ethernet, IP and TCP

1 Details

Aim: To provide a foundation in understanding Ethernet, IP and TCP.

🖱 The demo of this lab is at: http://youtu.be/FhVN-gZnQq0

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:

Host src IP address (Hint: Examine the Source IP on Packet 3):

Server src IP address (Hint: Examine the Dest IP on Packet 3):

Host src TCP port (Hint: Examine the Source Port on Packet 3):

Server src TCP port (Hint: Examine the Destination Port on Packet 3):

What is the MAC address of the server (Hint: Examine the reply for Packet 2), and which is the manufacture of the network card:

What is the MAC address of the host contacting the server, and which is the manufacture of the network card:

Identify the packets used for the SYN, SYN/ACK and ACK sequence. Which packets are these:

In Packet 1, which is the destination MAC address used in the ARP request?

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:

Host src IP address:

Server src IP address of the Web server:

Host src TCP port:

Server src TCP port:

Can you determine the MAC address of the server:

What is the MAC address of the host contacting the server, and which is the manufacturer of the network card:

What is the IP address of the local gateway?

What is the MAC address of the local gateway, and which is the manufacturer of the network card:

Identify the packets used for the SYN, SYN/ACK and ACK sequence. Which packets are these:

L1.3 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:

Your MAC address:

Your IP address:

The MAC address of the gateway:

The IP address of intel.com

The source TCP port of your connection:

The destination TCP port used by the server: