Lab 8: Network Packet Inspection

Setup your network using AllocationC:

http://asecuritysite.com/csn11128/nets

And make sure that all your hosts can connect to Google.com.

Ethernet, IP and TCP

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

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

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 manufacturer of the network card:

What is the MAC address of the host contacting the server, 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:

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

Using the filter of tcp.flags.syn==1**, find all the packets that involve a SYN flag. What are there IDs?**

What does the filter of tcp.flags.syn==1 && tcp.flags.ack==**0 do?**

What does the filter of tcp.flags.syn==1 && tcp.flags.ack==1 **do?**

Which flags are set at the end of a connection?

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:

By tracing the TCP stream, can you view the contents of the CSS file? Give an example of some of the text in it?

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 (and its manufacturer):
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:

Apart from your network traffic, can you see other traffic from other hosts on the network? If so, which type of network traffic do you see?

HTTP, DNS and FTP

Aim: To provide a foundation in understanding HTTP, DNS and FTP.

The demo of this lab is at: http://youtu.be/l0A4Xrfq5Tc

L1.4 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:

Using the filter of http.request.method=="GET"**, identify the files that the host gets from the Web server:**

Using the filter of http.response**, determine the response codes. Which files have transferred and which have been unsuccessful?**

Which is the default file name on the server when the user accesses the top levels of the domain?

Which type of image files does the client want to accept?

Which language/character set is used by the client?

Which Web browser is the client using?

Which Web server technology is the server using?

On which date were the pages accessed?

L1.5 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:

Using the filter of http.request.method=="GET"**, identify the files that the host gets from the Web server:**

Using the filter of http.response**, determine the response codes. Which files have transferred and which have been unsuccessful?**

Which is the default file name on the server when the user accesses the top levels of the domain?

Which type of image files does the client want to accept?

Which language/character set is used by the client?

Which Web browser is the client using?

Which Web server technology is the server using?

On which date were the pages accessed?

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:

Using the filter of http.request.method=="GET"**, identify the files that the host gets from the Web server:**

Using the filter of http.response**, determine the response codes. Which files have transferred and which have been unsuccessful?**

Which is the default file name on the server when the user accesses the top levels of the domain?

Which type of image files does the client want to accept?

Which language/character set is used by the client?

Which Web browser is the client using?

Which Web server technology is the server using?

L1.7 Download the following file, and open it up in Wireshark:

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

For this trace, determine the following:

Which is the domain which is being searched for?

Which are the IP addresses of the domain being searched for?

The first request is of class of PTR. What is the PTR?

The second request is of class for A. What is the A class?

The last request is for class of AAAA. What is the AAAA class?

Does the domain have an IPv6 address?

L1.8 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/ftp2.zip

For this trace, determine the following:

Using the filter of ftp.command**, determine the FTP commands that the user has used:**

Using the filter of ftp.response**, determine the FTP codes that have been returned:**

What is the username and password for the access to the FTP server:

What is the name of the file which is uploaded:

What is the name of the file which is downloaded:

Using the filter of ftp.request.command=="LIST"**, determine the first packet number which performs a "LIST":**

In performing in the list of the files on the FTP server, which TCP is used on the server for the transfer:

From the final "LIST" command, which are the files on the server?

What does the filter ftp.response.code==227**, identify in terms of the ports that are used for the transfer:**

ARP and ICMP

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

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

L1.9 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:

L1.10 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?

L1.11 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?

SMTP, POP-3 and IMAP

Aim: To provide a foundation in understanding SNMP, POP-3 and IMAP.

The demo of this lab is at: http://youtu.be/3RHrq3EehsE

L1.12 Download the following file, and open it up in Wireshark:

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

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address and the TCP port used by the SMTP server:

Who is sending the email:

Who is receiving the email:

When was the email sent:

When was the email client used to send the email:

What was the message, and what was the subject of the email:

With SMTP, which character sequence is used to end the message:

L1.13 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/pop3.zip

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address and the TCP port used by the POP-3 server:

Whose mail box is being accessed:

How many email messages are in the Inbox:

The messages are listed as:

1 5565
2 8412
3 xxxx

Which is the ID for message 3:

For Message 1, who sent the message and what is the subject and outline the content of the message:

For Message 2, who sent the message and what is the subject and outline the content of the message:

For Message 3, who sent the message and what is the subject and outline the content of the message:

Which command does POP-3 use to get a specific message:

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

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

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address(es) and the TCP ports used by the SMTP and the IMAP server:

Whose mail box is being accessed:

How many email messages are in the Inbox:

Trace the email message that has been sent for its basic details:

Outline the details of email which are in the Inbox: