


Lab 7a: 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 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?

Lab 7b: HTTP, DNS and FTP

1 Details

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

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

2 Activities

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 Start capturing network packets on your main network adapter. Next go to **imperial.ac.uk**, and access the page. Stop the network capture, and then from your network traffic, determine:

Using the filter of `udp.port==53`, and examining the A class request, determine the IPv4 address of imperial.ac.uk:

Using the filter of `udp.port==53`, and examining the AAAA class request, determine the IPv6 address of imperial.ac.uk:

L1.9 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:

Lab 7c: 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

3 Activities

L1.10 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:

L1.11 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?

L1.12 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?

L1.13 Start capturing network packets on your main network adapter (such as from your host in your DMZ). 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:

L1.14 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:

L1.15 Start capturing network packets on your main network adapter (such as your host in the DMZ). 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:

L1.16 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?

L1.17 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?

L1.18 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:

Lab 7d: SMTP, POP-3 and IMAP

1 Details

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

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

2 Activities

L1.19 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:

L1.20 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:

Lab 7e: SSL and TLS

1 Details

Aim: To provide a foundation in understanding SSL and TLS.

 The demo of this lab is at: <http://youtu.be/jejjoSCn6Yg>

2 Activities

L1.21 Download the following file, and open it up in Wireshark:

<http://asecuritysite.com/log/ssl.zip>

Determine the following:

The IP address and TCP port used by the host:

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

Which network protocol is thus being used:

Which Web site is being accessed:

Can you determine which organised signed the digital certificate passed from the server:

Can you read any of the encrypted data sent/received? Yes/No

L1.22 Start Wireshark and capture your network traffic Next go to <http://google.co.uk> and

Determine the following:

The IP address and TCP port used by the host:

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

Which network protocol is thus being used:

Which Web site is being accessed:

Can you determine which organised signed the digital certificate passed from the server:

Can you read any of the encrypted data sent/received? Yes/No

On the Web browser go to **google.co.uk**, find the digital certificate and determine the following:

The organisation who have issued the digital certificate:

The expiry date of the certificate:

The encryption method used for the public key:

The length of the encryption key:

On the Web browser go to **paypal.com**, find the digital certificate and determine the following:

The organisation who have issued the digital certificate:

The expiry date of the certificate:

The encryption method used for the public key:

The length of the encryption key:

For digital certificates, can you determine four digital certificate issuers who could be trusted to sign certificates:

Which of the following sites use an SSL/TLS connection by default:

http://cisco.com

http://microsoft.com

http://outlook.com

http://skydrive.com

Lab 7f: Tshark and Snort

Tshark can be used to run a command-line version of Wireshark. First locate Tshark on your system. Next, download this file:

https://asecuritysite.com/log/with_png.zip

and run the command of:

```
tshark.exe -Y "http contains "89:50:4E:47"" -r with_png.pcap
```

What packet number contains the packet with the PNG file?

We can also use Snort to analyse network traces by using an off-line filtering system. First, download this Pcap file:

<https://asecuritysite.com/log/newtrace.zip>

Next you can run Snort with a rules file and with a trace:

snort -c 1.rules -l log -r newtrace.pcap

You can then look in the log filter for the log file and alert.ids.

Some rules you can use are given in Appendix A.

Now test Snort to see if it can detect the same content that you found before:

Number of Bad FTP logins:

Number of Successful FTP logins:

Number of GIF files in the trace:

Number of PNG files in the trace:

Can you detect the port scan on a host:

Test

Now take this test:

http://asecuritysite.com/tests/tests?sortBy=d01_03

Appendix A

Bad logins:

```
alert tcp any 21 -> any any (msg:"FTP Bad login"; content:"530 User ";  
nocase; flow:from_server,established; sid:491; rev:5;)
```

Detecting email addresses:

```
alert tcp any any <> any 25 (pcr:"/[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]/"; \  
msg:"Email in message";sid:9000000;rev:1;)
```

Detect DNS:

```
alert udp any any -> any 53 (msg: "DNS"; sid:10000;)
```

File types:

```
alert tcp any any -> any any (content:"GIF89a"; msg:"GIF";sid:10000)  
alert tcp any any -> any any (content:@"%PDF"; msg:"PDF";sid:10001)  
alert tcp any any -> any any (content:"|89 50 4E 47|"; msg:"PNG";sid:10002)  
alert tcp any any -> any any (content:"|50 4B 03 04|"; msg:"ZIP";sid:10003)
```

Telnet login:

```
alert tcp any any <> any 23 (flags:S; msg:"Telnet Login";sid:9000005;rev:1;)
```

Port scan:

```
preprocessor sfportscan:\  
  proto { all } \  
  scan_type { all } \  
  sense_level { high } \  
  logfile { portscan.log }
```

DoS on Web server:

```
alert tcp any any -> any 80 (msg:"DOS flood denial of service attempt";flow:to_server;  
\  
detection_filter:track by_dst, count 60, seconds 60; \  
sid:25101; rev:1;)
```

Stealth scans:

```
alert tcp any any -> any any (msg:"SYN FIN Scan"; flags: SF;sid:9000000;)  
alert tcp any any -> any any (msg:"FIN Scan"; flags: F;sid:9000001;)  
alert tcp any any -> any any (msg:"NULL Scan"; flags: 0;sid:9000002;)  
alert tcp any any -> any any (msg:"XMAS Scan"; flags: FPU;sid:9000003;)  
alert tcp any any -> any any (msg:"Full XMAS Scan"; flags: SRAFPU;sid:9000004;)  
alert tcp any any -> any any (msg:"URG Scan"; flags: U;sid:9000005;)  
alert tcp any any -> any any (msg:"URG FIN Scan"; flags: FU;sid:9000006;)  
alert tcp any any -> any any (msg:"PUSH FIN Scan"; flags: FP;sid:9000007;)  
alert tcp any any -> any any (msg:"URG PUSH Scan"; flags: PU;sid:9000008;)
```



```
alert tcp any any -> any any (flags: A; ack: 0; msg:"NMAP TCP ping!";sid:9000009;)
```

ping sweep:

```
alert icmp any any -> any any (msg:"ICMP Packet found";sid:9000000;)
```

```
alert icmp any any -> any any (itype: 0; msg: "ICMP Echo Reply";sid:9000001;)
```

```
alert icmp any any -> any any (itype: 3; msg: "ICMP Destination  
Unreachable";sid:9000002;)
```

```
alert icmp any any -> any any (itype: 4; msg: "ICMP Source Quench Message  
received";sid:9000003;)
```

```
alert icmp any any -> any any (itype: 5; msg: "ICMP Redirect message";sid:9000004;)
```

```
alert icmp any any -> any any (itype: 8; msg: "ICMP Echo Request";sid:9000005;)
```

```
alert icmp any any -> any any (itype: 11; msg: "ICMP Time Exceeded";sid:9000006;)
```