

Lab 3: HTTP, DNS and FTP

Aim:

To provide a foundation in understanding high-level protocols such as HTTP, DNS and FTP

Time to complete: Up to 45 minutes.

Activities:

- Complete Lab 3: HTTP, DNS and FTP
- Complete Test 3.

Learning Activities:

At the end of these activities, you should understand:

- How to determine key details related to HTTP, DNS and FTP.
- Capture traffic for traces.

Reflective statements (end-of-exercise):


You should reflect on these questions:

- If an intruder managed to set themselves up as your gateway, how might they modify the DNS settings for your host?
- For a security point-of-view, which is one of the weaknesses of HTTP and FTP?
- How could an intruder determine the user name and password by listening to FTP network traffic?

Lab 3: 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

L1.1 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:

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?

L1.2 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:

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?

L1.3 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:

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?

L1.4 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?

L1.5 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:

L1.6 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: