10.6.7 Lab - Using Wireshark to Examine HTTP and HTTPS Traffic

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

Part 1: View HTTP traffic

Part 2: View HTTPS traffic

Background / Scenario

HyperText Transfer Protocol (HTTP) is an application layer protocol that presents data via a web browser. With HTTP, there is no safeguard for the exchanged data between two communicating devices.

With HTTPS, encryption is used via a mathematical algorithm. This algorithm hides the true meaning of the data that is being exchanged. This is done through the use of certificates that can be viewed later in this lab.

Regardless of HTTP or HTTPS, it is only recommended to exchange data with websites that you trust. Just because a site uses HTTPS does not mean it is a trustworthy site. Threat actors commonly use HTTPS to hide their activities.

In this lab, you will explore and capture HTTP and HTTPS traffic using Wireshark.

Instructions

Part 1: View HTTP Traffic

In this part, you will use captured packet capture (*pcap*) files that can be analyzed using different applications that read pcap files, including Wireshark.

Step 1: Start the virtual machine and log in.

Start the **Workstation** VM. Use the following user credentials:

Username: `analyst`

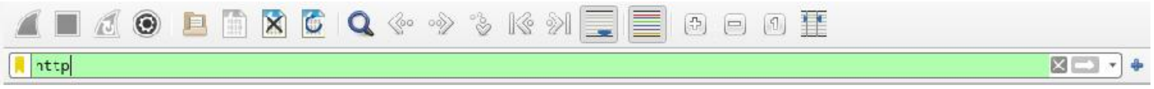
Password: `cyberops`

Step 2: View the HTTP capture.

The *httpdump.pcap* file is located in the home directory for the user *analyst*.

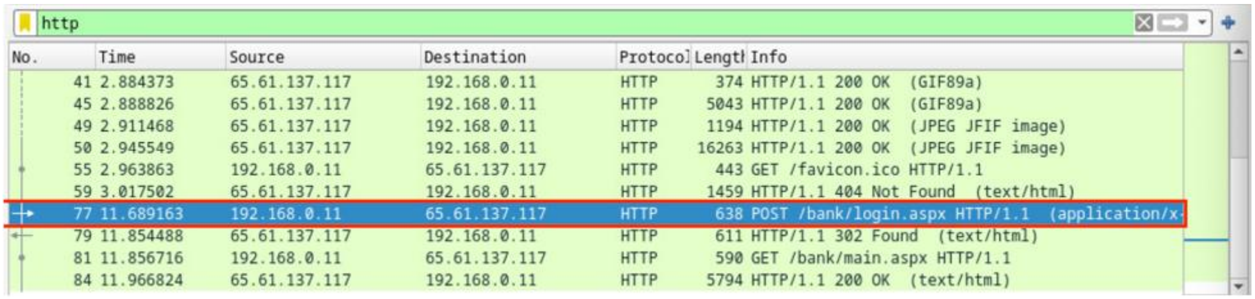
a. Click the **Home** icon on the desktop and browse to the **~/lab.support.files/pcaps/** folder for the user **analyst**. Double-click the **httpdump.pcap** file to open it in *Wireshark*.

b. In the Wireshark application, filter for **http** and press the **Enter** key to apply.



http

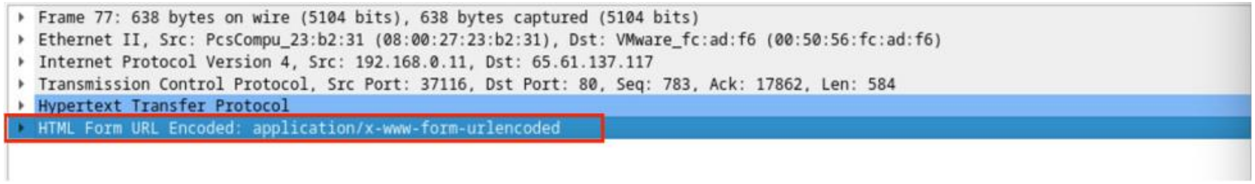
c. Browse through the different HTTP messages and select the **POST** message.



```
http

No.   Time        Source          Destination     Protocol Length Info
   41 2.884373    65.61.137.117   192.168.0.11    HTTP       374 HTTP/1.1 200 OK  (GIF89a)
   45 2.888826    65.61.137.117   192.168.0.11    HTTP      5043 HTTP/1.1 200 OK  (GIF89a)
   49 2.911468    65.61.137.117   192.168.0.11    HTTP      1194 HTTP/1.1 200 OK  (JPEG JFIF image)
   50 2.945549    65.61.137.117   192.168.0.11    HTTP     16263 HTTP/1.1 200 OK  (JPEG JFIF image)
   55 2.963863    192.168.0.11    65.61.137.117   HTTP       443 GET /favicon.ico HTTP/1.1
   59 3.017502    65.61.137.117   192.168.0.11    HTTP      1459 HTTP/1.1 404 Not Found  (text/html)
   77 11.689163   192.168.0.11    65.61.137.117   HTTP       638 POST /bank/login.aspx HTTP/1.1  (application/x-
   79 11.854488   65.61.137.117   192.168.0.11    HTTP       611 HTTP/1.1 302 Found  (text/html)
   81 11.856716   192.168.0.11    65.61.137.117   HTTP       590 GET /bank/main.aspx HTTP/1.1
   84 11.966824   65.61.137.117   192.168.0.11    HTTP      5794 HTTP/1.1 200 OK  (text/html)
```

d. In the lower window, the message is displayed. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** section.



```
▸ Frame 77: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits)
▸ Ethernet II, Src: PcsCompu_23:b2:31 (08:00:27:23:b2:31), Dst: VMware_fc:ad:f6 (00:50:56:fc:ad:f6)
▸ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 65.61.137.117
▸ Transmission Control Protocol, Src Port: 37116, Dst Port: 80, Seq: 783, Ack: 17862, Len: 584
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

What two pieces of information are displayed?

____

e. Close the Wireshark application.

Part 2: View HTTPS Traffic

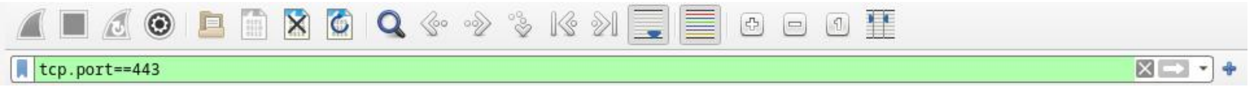
In comparison, *HTTPS* records will be analyzed using *Wireshark.*

Step 1: View HTTPS Traffic.

a. In the *~/lab.support.files/pcaps/* directory for the user **analyst**, Double-click the **httpsdump.pcap** file to open it in *Wireshark*.

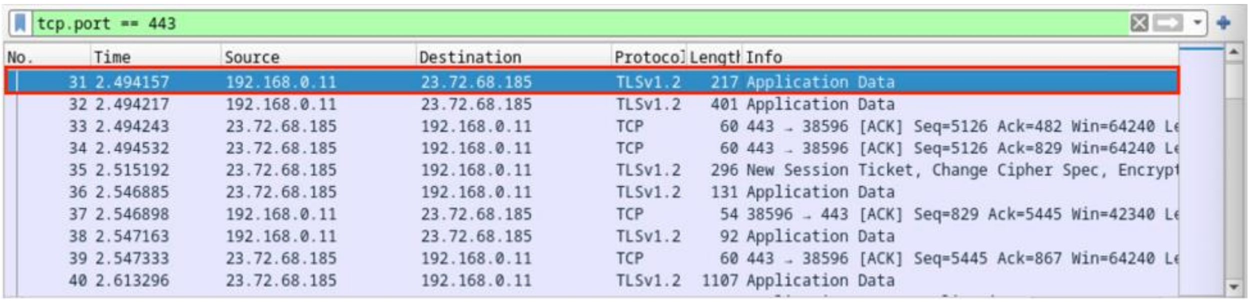
b. In the Wireshark application, expand the capture window vertically and then filter by HTTPS traffic via port 443.

Enter **tcp.port==443** as a filter, and press the **Enter** key to apply.



```
tcp.port==443
```

c. Browse through the different HTTPS messages and select an **Application Data** message.



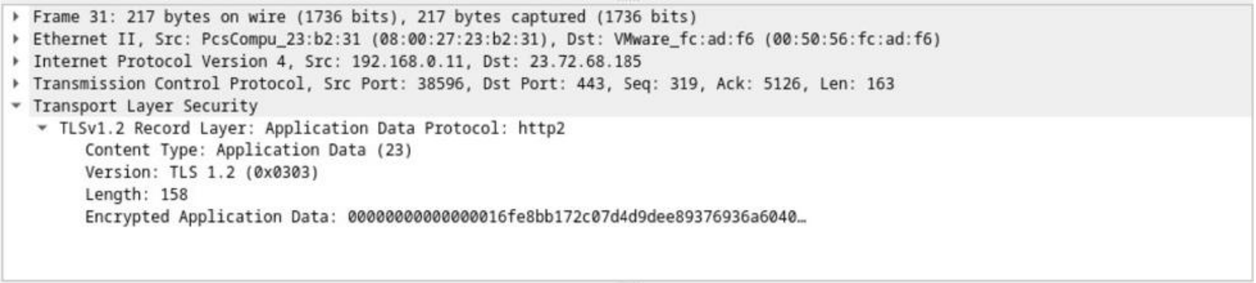
```
tcp.port == 443

No.   Time        Source          Destination     Protocol Length Info
   31 2.494157    192.168.0.11    23.72.68.185    TLSv1.2    217 Application Data
   32 2.494217    192.168.0.11    23.72.68.185    TLSv1.2    401 Application Data
   33 2.494243    23.72.68.185    192.168.0.11    TCP         60 443 → 38596 [ACK] Seq=5126 Ack=482 Win=64240 Le
   34 2.494532    23.72.68.185    192.168.0.11    TCP         60 443 → 38596 [ACK] Seq=5126 Ack=829 Win=64240 Le
   35 2.515192    23.72.68.185    192.168.0.11    TLSv1.2    296 New Session Ticket, Change Cipher Spec, Encrypt
   36 2.546885    23.72.68.185    192.168.0.11    TLSv1.2    131 Application Data
   37 2.546898    192.168.0.11    23.72.68.185    TCP         54 38596 → 443 [ACK] Seq=829 Ack=5445 Win=42340 Le
   38 2.547163    192.168.0.11    23.72.68.185    TLSv1.2     92 Application Data
   39 2.547333    23.72.68.185    192.168.0.11    TCP         60 443 → 38596 [ACK] Seq=5445 Ack=867 Win=64240 Le
   40 2.613296    23.72.68.185    192.168.0.11    TLSv1.2   1107 Application Data
```

d. In the lower pane, the message is displayed.

What has replaced the HTTP section that was in the previous capture file?

e. Completely expand the **Transport Layer Security** section.



```
▸ Frame 31: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits)
▸ Ethernet II, Src: PcsCompu_23:b2:31 (08:00:27:23:b2:31), Dst: VMware_fc:ad:f6 (00:50:56:fc:ad:f6)
▸ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 23.72.68.185
▸ Transmission Control Protocol, Src Port: 38596, Dst Port: 443, Seq: 319, Ack: 5126, Len: 163
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 158
      Encrypted Application Data: 0000000000000001 6fe8bb172c07d4d9dee89376936a6040…
```

f. Click the **Encrypted Application Data**.

Is the application data in a plaintext or readable format?

g. Close all windows and shut down the virtual machine.

Reflection Questions

1. What are the advantages of using HTTPS instead of HTTP?

2. Are all websites that use HTTPS considered trustworthy?