Lab 4.6.6.5 – Using Wireshark to Examine HTTP and HTTPS

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

Objectives

Part 1: View HTTP traffic

Part 2: Capture and 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 *HTTP* and *HTTPS* traffic using Wireshark.

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 CyberOps Workstation VM. Use the following user credentials:

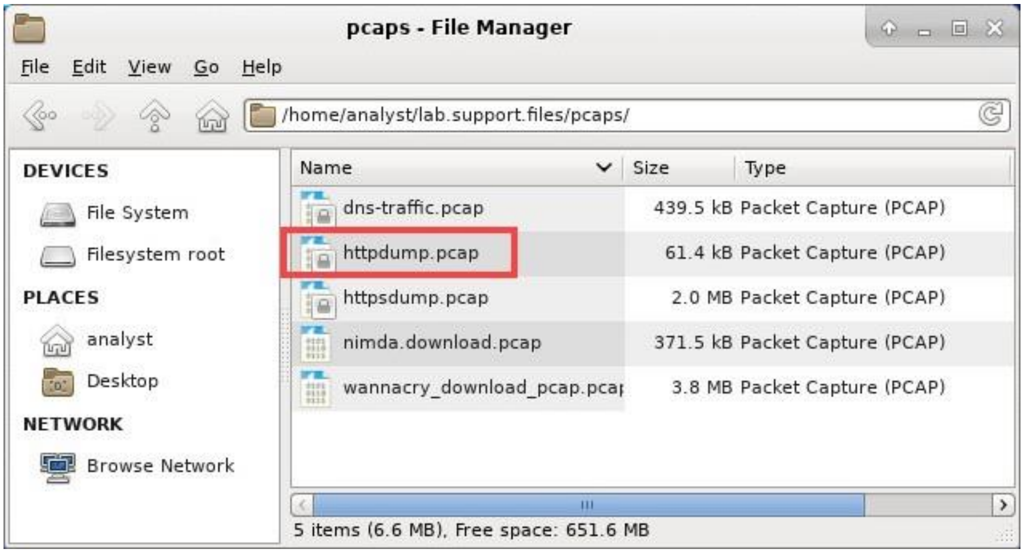
Username: `analyst`

Password: `cyberops`

Step 2: View the HTTP capture.

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

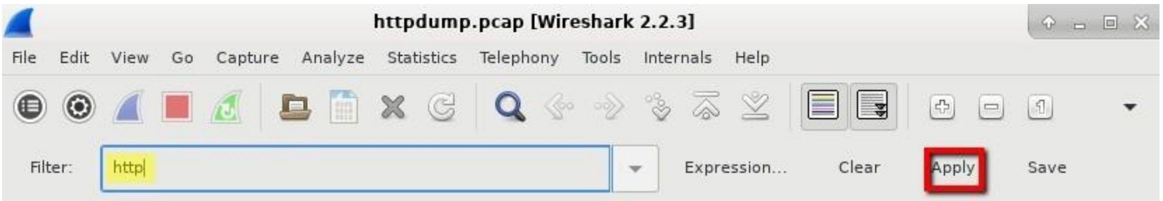
a. Click the **File Manger** icon on the desktop and browse to the **~/lab.support.files/pcaps/** folder for the user **analyst**. Double-click the **httpdump.pcap** file to open it in *Wireshark*.



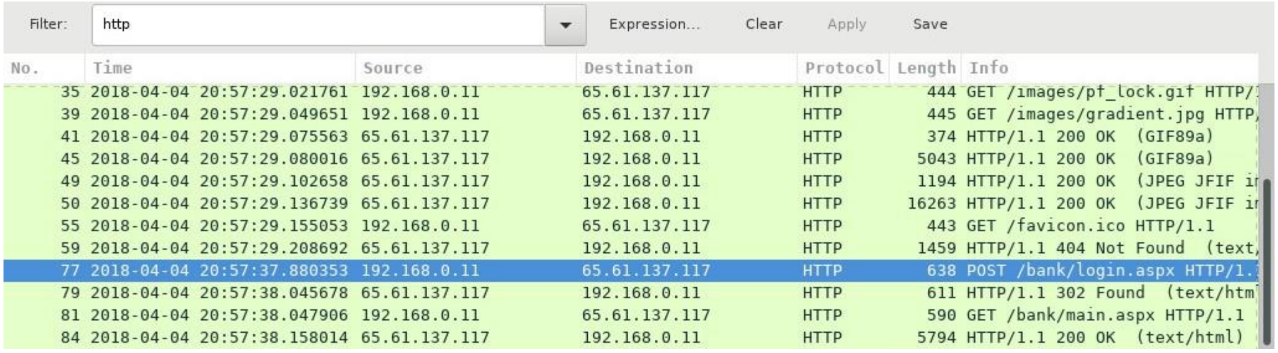
Name	Size	Type
dns-traffic.pcap	439.5 kB	Packet Capture (PCAP)
httpdump.pcap	61.4 kB	Packet Capture (PCAP)
httpsdump.pcap	2.0 MB	Packet Capture (PCAP)
nimda.download.pcap	371.5 kB	Packet Capture (PCAP)
wannacry_download_pcap.pcap	3.8 MB	Packet Capture (PCAP)

5 items (6.6 MB), Free space: 651.6 MB

b. In the *Wireshark* application, filter for `http` and click **Apply**.

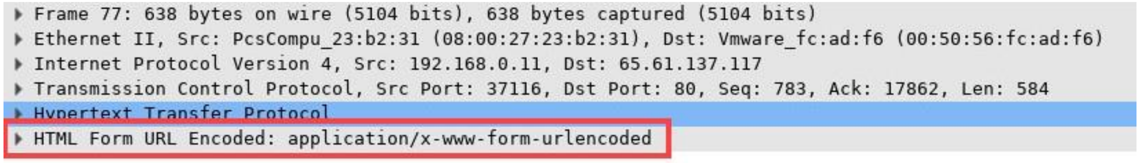

httpdump.pcap [Wireshark 2.2.3]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
http
Expression...
Clear
Apply
Save

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



```
No.    Time                          Source          Destination     Protocol Length Info
    35 2018-04-04 20:57:29.021761 192.168.0.11    65.61.137.117   HTTP        444 GET /images/pf_lock.gif HTTP/1
    39 2018-04-04 20:57:29.049651 192.168.0.11    65.61.137.117   HTTP        445 GET /images/gradient.jpg HTTP,
    41 2018-04-04 20:57:29.075563 65.61.137.117   192.168.0.11    HTTP        374 HTTP/1.1 200 OK  (GIF89a)
    45 2018-04-04 20:57:29.080016 65.61.137.117   192.168.0.11    HTTP       5043 HTTP/1.1 200 OK  (GIF89a)
    49 2018-04-04 20:57:29.102658 65.61.137.117   192.168.0.11    HTTP       1194 HTTP/1.1 200 OK  (JPEG JFIF ir
    50 2018-04-04 20:57:29.136739 65.61.137.117   192.168.0.11    HTTP      16263 HTTP/1.1 200 OK  (JPEG JFIF ir
    55 2018-04-04 20:57:29.155053 192.168.0.11    65.61.137.117   HTTP        443 GET /favicon.ico HTTP/1.1
    59 2018-04-04 20:57:29.208692 65.61.137.117   192.168.0.11    HTTP       1459 HTTP/1.1 404 Not Found  (text,
    77 2018-04-04 20:57:37.880353 192.168.0.11    65.61.137.117   HTTP        638 POST /bank/login.aspx HTTP/1.1
    79 2018-04-04 20:57:38.045678 65.61.137.117   192.168.0.11    HTTP        611 HTTP/1.1 302 Found  (text/htm
    81 2018-04-04 20:57:38.047906 192.168.0.11    65.61.137.117   HTTP        590 GET /bank/main.aspx HTTP/1.1
    84 2018-04-04 20:57:38.158014 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?

Yes , “uid” = “Admin”,”passw” = “Admin”,”btnsubmit”=”Login”.

e. Close the **Wireshark** application.

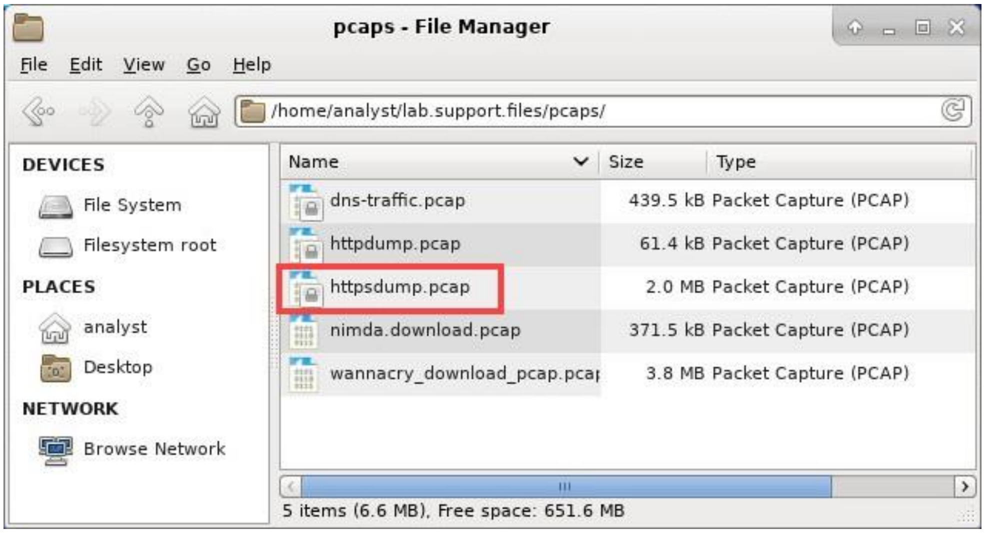
Part 2: View HTTPS Traffic

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

Step 1: View the HTTPS capture.

The tcpdump executed in Step 1 printed the output to a file named httpsdump.pcap. This file is located in the home directory for the user **analyst**.

a. In the *~/lab.support.files/pcaps/* directory for the user **analyst**, open the **httpsdump.pcap** file.



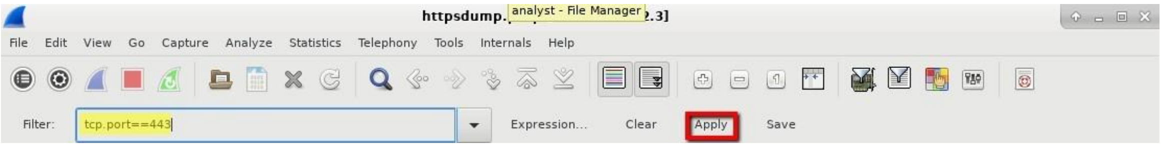
/home/analyst/lab.support.files/pcaps/

Name	Size	Type
dns-traffic.pcap	439.5 kB	Packet Capture (PCAP)
httpdump.pcap	61.4 kB	Packet Capture (PCAP)
httpsdump.pcap	2.0 MB	Packet Capture (PCAP)
nimda.download.pcap	371.5 kB	Packet Capture (PCAP)
wannacry_download_pcap.pcaj	3.8 MB	Packet Capture (PCAP)

5 items (6.6 MB), Free space: 651.6 MB

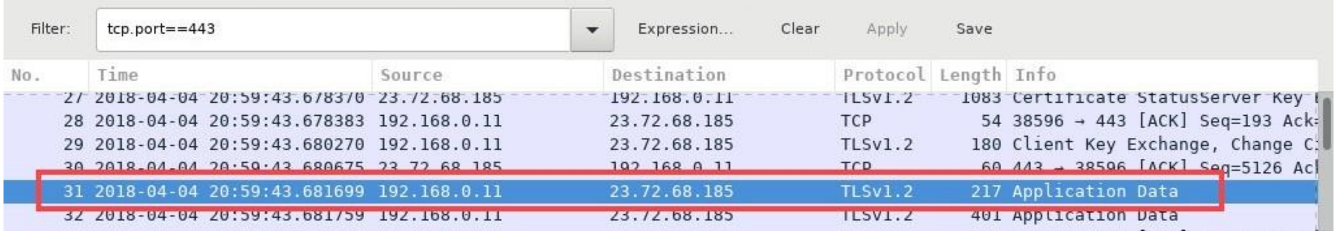
b. In the *Wireshark* application, expand the capture window vertically and then filter by *HTTPS* traffic via port 443.

Enter **tcp.port==443** as a filter, and click **Apply**.



Filter: tcp.port==443

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



Filter: tcp.port==443

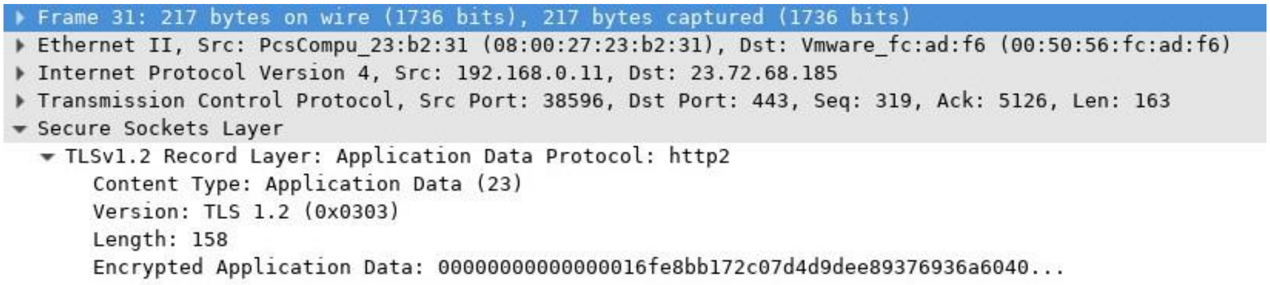
```
No.   Time                        Source          Destination     Protocol Length Info
   27 2018-04-04 20:59:43.678370  23.72.68.185    192.168.0.11    TLSv1.2    1083 Certificate StatusServer Key
   28 2018-04-04 20:59:43.678383  192.168.0.11    23.72.68.185    TCP          54 38596 → 443 [ACK] Seq=193 Ack=
   29 2018-04-04 20:59:43.680270  192.168.0.11    23.72.68.185    TLSv1.2     180 Client Key Exchange, Change C
   30 2018-04-04 20:59:43.680675  23.72.68.185    192.168.0.11    TCP          60 443 → 38596 [ACK] Seq=5126 Ac
   31 2018-04-04 20:59:43.681699  192.168.0.11    23.72.68.185    TLSv1.2     217 Application Data
   32 2018-04-04 20:59:43.681759  192.168.0.11    23.72.68.185    TLSv1.2     401 Application Data
```

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

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

In the place of HTTP it displayed Secure Sockets Layer.

e. Completely expand the **Secure Sockets Layer** 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
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 158
      Encrypted Application Data: 0000000000000016fe8bb172c07d4d9dee89376936a6040...
```

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

Is the application data in a plaintext or readable format?

It been encrypted using TLSv1.

g. Close all windows.

Reflection

1. What are the advantages of using HTTPS instead of HTTP?
HTTPS encrypts all records exchanged among the net server and the user's browser it also provides the authentication. Overall, using HTTPS is essential for protecting sensitive information, building trust with users, and approving with regulations.

2. Are all websites that use HTTPS considered trustworthy?

NO, Hackers and attackers can still use HTTPS to create fake websites with valid Secure Sockets layers. In additionally, HTTPS is a necessary step to make your website more secure and reliable, but it's important to stay alert and take additional steps to validate your website's authenticity.