# Práctica de laboratorio: Utilizar Wireshark para examinar tráfico HTTP y HTTPS

# Objetivos

**Parte 1: Capturar y ver tráfico HTTP**

**Parte 2: Capturar y ver tráfico HTTPS**

## Antecedentes / Escenario

El Protocolo de transferencia de hipertexto (HyperText Transfer Protocol, HTTP) es un protocolo de la capa de aplicación que presenta datos a través de un navegador web. Con HTTP, no se protegen los datos intercambiados entre dos dispositivos que se están comunicando.

Con HTTPS, se emplea cifrado por medio de un algoritmo matemático. Este algoritmo oculta el verdadero significado de los datos que se está intercambiando. Esto se hace mediante el uso de certificados que podremos ver más adelante en esta práctica de laboratorio.

Independientemente de que se utilice HTTP o HTTPS, solo se recomienda intercambiar datos con sitios web de confianza. El solo hecho de que un sitio utilice HTTPS no significa que sea confiable. Los atacantes suelen utilizar HTTPS para ocultar sus actividades.

En esta práctica de laboratorio explorarán y capturarán tráfico HTTP y HTTPS con Wireshark.

## Recursos necesarios

- VM CyberOps Workstation
- Conexión a Internet

## Instrucciones

## Parte 1: Capturar y ver el tráfico de HTTP

En esta parte utilizará **tcpdump** para capturar el contenido del tráfico HTTP. Utilizará opciones de comandos para guardar el tráfico en un archivo de captura de paquetes (pcap). Estos registros se pueden analizar posteriormente con diferentes aplicaciones que leen archivos pcap, incluida Wireshark.

### Paso 1: Iniciar la máquina virtual e iniciar sesión.

Inicien la VM CyberOps Workstation. Utilicen las siguientes credenciales de usuario:

Nombre de usuario: **analyst**

Contraseña: **cyberops**

### Paso 2: Abra un terminal e inicie tcpdump

a. Abrir una aplicación de terminal e ingresar el comando **ip address**

```
[analyst@secOps ~]$ ip address
```

b. Enumere las interfaces y sus direcciones IP desplegadas con la entrada **ip address**

c. Sin salir de la aplicación del terminal, introduzcan el comando **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**. Introduzcan la contraseña **cyberops** para el usuario analyst cuando el sistema se los solicite.

```
[analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap
[sudo] contraseña para analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Este comando inicia tcpdump y registra el tráfico de red en la interfaz **enp0s3**.

La opción de comando **-i** les permite especificar la interfaz. Si no se la especifica, tcpdump capturará todo el tráfico en todas las interfaces.

La opción de comando **-s** especifica la longitud de la captura correspondiente a cada paquete. Deberían limitar snaplen a la cifra más pequeña que capturará la información del protocolo en la que están interesados. Si se define snaplen en 0 se lo establece en el valor predeterminado de 262144, para ofrecer retrocompatibilidad con versiones anteriores recientes de tcpdump.

La opción de comando **-w** se utiliza para escribir el resultado del comando tcpdump en un archivo. Si se agrega la extensión .pcap, se garantiza que los sistemas operativos y las aplicaciones podrán leer el archivo. Todo el tráfico registrado se imprimirá al archivo httpdump.pcap, en el directorio de inicio del usuario analyst.

Consulten las páginas man correspondientes a tcpdump para conocer el uso de las opciones de comando -s y -w.

d. Abra un buscador web desde la barra de inicio de CyberOps Workstayion VM. Vaya a **http://www.altoromutual.com/login.jsp**

Como este sitio web utiliza HTTP, el tráfico no está cifrado. Seleccione el espacio de la contraseña para ver la advertencia emergente.

e. Introduzcan **Admin** como nombre de usuario y **Admin** como contraseña; luego, hagan clic en **Login** (Iniciar sesión).

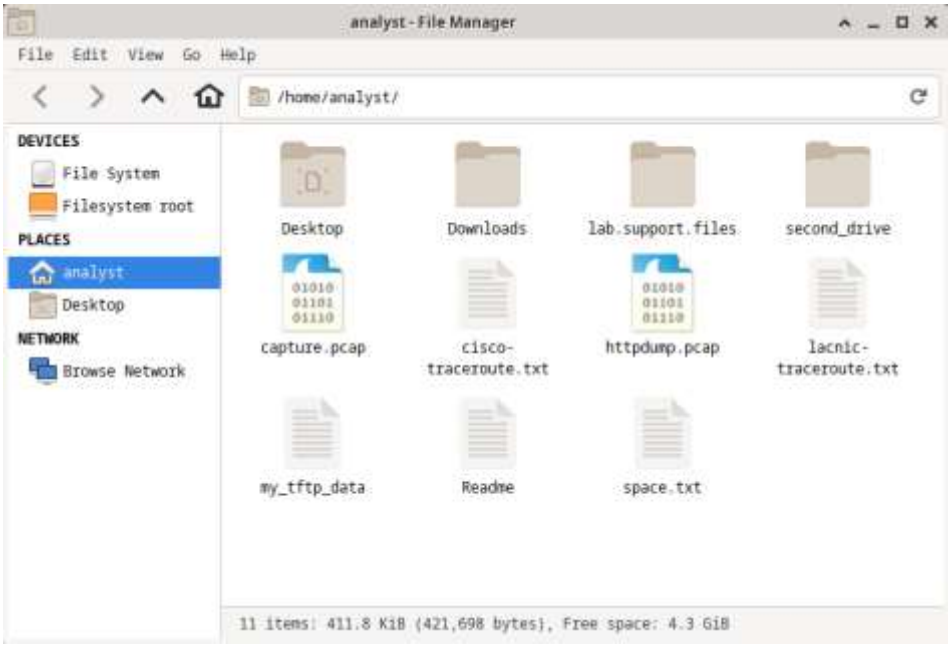
f. Cierre el navegador web.

g. Regresen a la ventana del terminal donde se está ejecutando tcpdump. Presionen **CTRL+C** para detener la captura de paquetes.

## Paso 3: Ver la captura HTTP

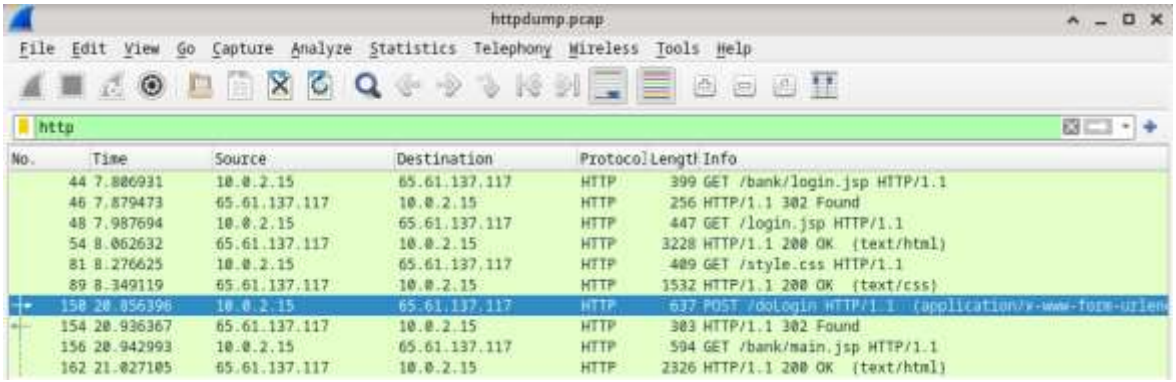
El comando tcpdump, que se ejecutó en el paso anterior, imprimió la salida a un archivo de nombre httpdump.pcap. Este archivo está ubicado en el directorio de inicio correspondiente al usuario **analyst.**

a. Haga clic en el icono del Administrador de archivos del escritorio y diríjase a la carpeta de inicio correspondiente al usuario **analyst**. Haga doble clic en el archivo **httpdump.pcap**, en el cuadro de diálogo Abrir con, desplácese hacia abajo hasta Wireshark y, a continuación, haga clic en **Abrir**.

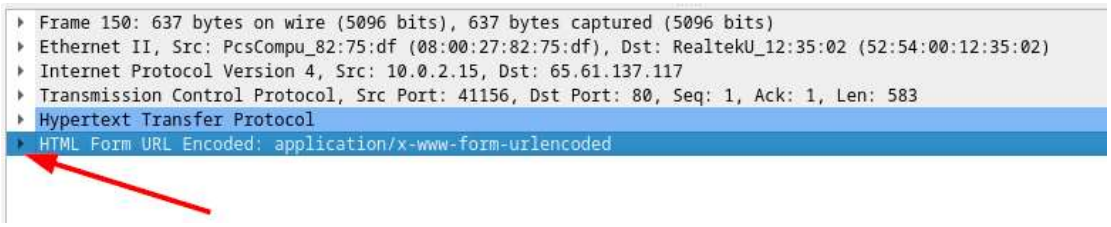



b. En la aplicación Wireshark, filtren por **http** y hagan clic en **Apply** (Aplicar).


c. Busque entre los diferentes mensajes HTTP y seleccionen el mensaje **POST**.



d. El mensaje aparece en la ventana inferior. Expanda la sección **URL de forma HTML decodificada: application/x-www-form-urlencoded**.




¿Cuáles son los dos datos que aparecen en pantalla?

e. Cierren la aplicación Wireshark

## Parte 2: Capturar y ver tráfico HTTPS

Ahora utilizarán tcpdump desde la línea de comandos de una estación de trabajo Linux para capturar tráfico HTTPS. Después de iniciar tcpdump, generarán tráfico HTTPS mientras tcpdump registra el contenido del tráfico de red. Estos registros nuevamente se analizará con Wireshark.

### Paso 1: Abrir tcpdump en un terminal

a. Sin salir de la aplicación del terminal, introduzca el comando **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**. Introduzcan la contraseña **cyberops** para el usuario analyst cuando el sistema se los solicite.

```
[analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap
[sudo] contraseña para analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Este comando iniciará tcpdump y registrará el tráfico de red en la interfaz **enp0s3** de la estación de trabajo Linux. Si la interfaz no es enp0s3, modifíquenla con el comando anterior.

Todo el tráfico registrado se imprimirá al archivo **httpsdump.pcap**, en el directorio de inicio del usuario analyst.

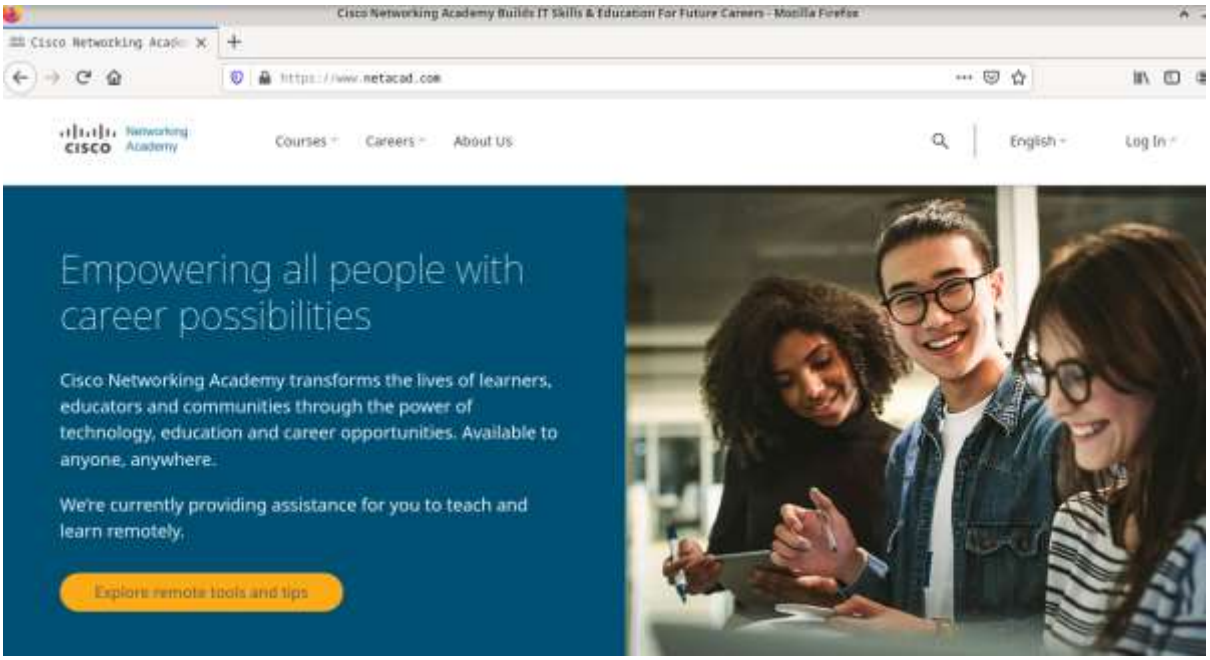
**b.** Abra un buscador web desde la barra de inicio de CyberOps Workstayion VM. Diríjanse a www.netacad.com.

**Nota**: Si recibe una página web de “Conexión segura fallida”, probablemente signifique que la fecha y la hora son incorrectas. Actualice el día y la hora con el siguiente comando, cambiando al día y la hora actuales:

```
[analista @secOps ~] $ sudo date -s «12 MAYO 2020 21:38:20
```

¿Qué notan con respecto a la URL del sitio web?

c. Haga clic en **Log in** (Iniciar sesión).




d. Introduzca su nombre de usuario y contraseña de NetAcad. Haga clic en **Siguiente**.

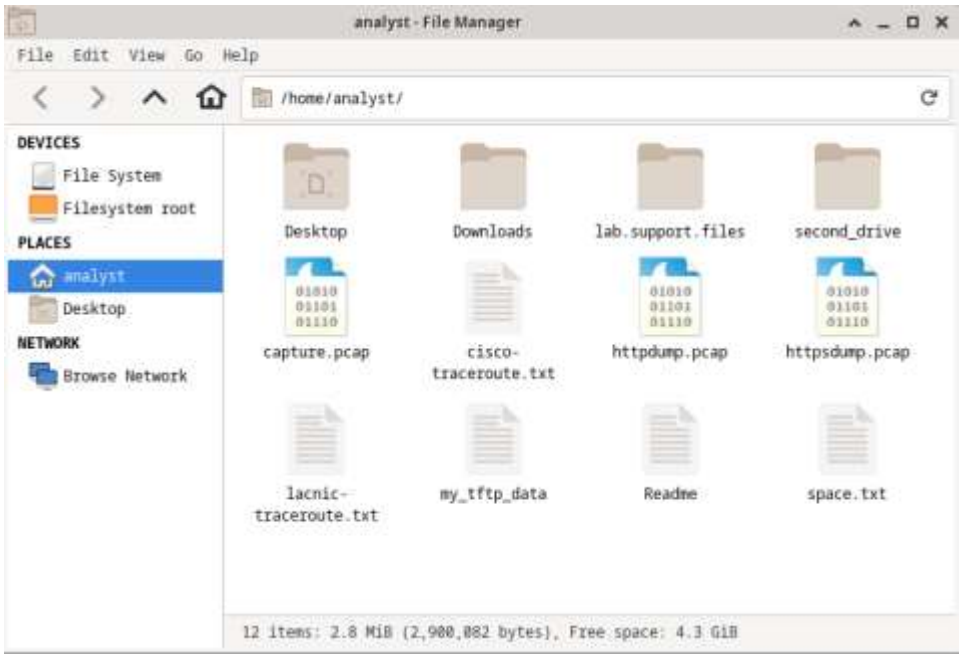

e. Cierre el navegador web en el VM

f. Regrese a la ventana del terminal donde se está ejecutando tcpdump. Presione **CTRL+C** para detener la captura de paquetes.

## Paso 2: Vea la captura HTTPS.

El comando tcpdump que se ejecutó en el Paso 1 imprimió la salida a un archivo de nombre httpsdump.pcap. Este archivo está ubicado en el directorio de inicio correspondiente al usuario **analyst.**

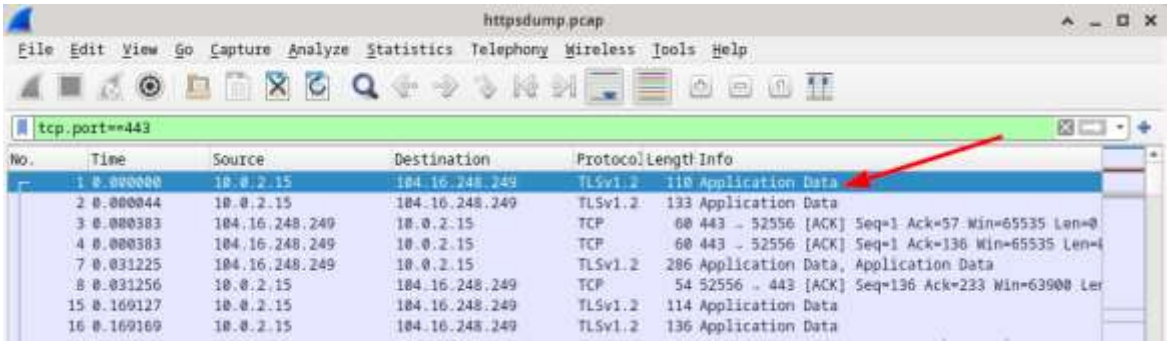
a. Haga clic en el icono del Sistema de archivos del escritorio y diríjanse a la carpeta de inicio correspondiente al usuario analyst. Abra el archivo **httpsdump.pcap**.




b. En la aplicación Wireshark, expanda verticalmente la ventana de la captura y, luego, filtren por tráfico HTTPS a través del puerto 443.

Introduzca **tcp.port==443** como filtro y hagan clic en **Apply**.

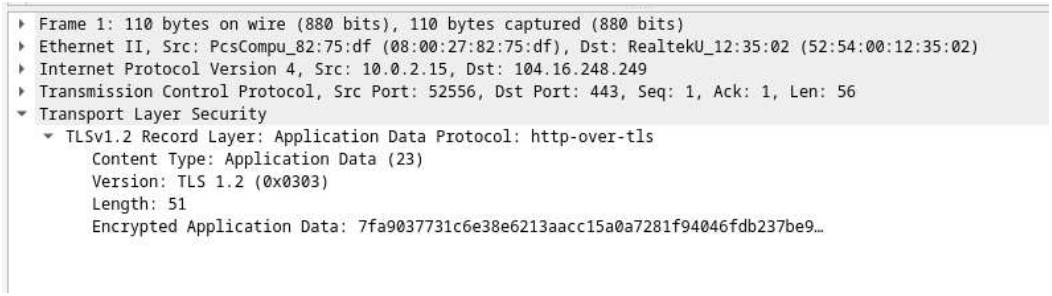

c. Desplácese por los diferentes mensajes HTTPS y seleccione el mensaje **Application Data** (Datos de aplicación).




d. El mensaje aparece en la ventana inferior.

¿Qué ha sustituido a la sección HTTP que estaba en el archivo de captura anterior?

e. Expanda completamente la sección **Secure Sockets Layer**.




f. Haga clic en **Encrypted Application Data** (Datos de aplicación cifrados).

¿Los datos de aplicación están en texto plano o formato legible?

g. Cierre todas las ventanas y apague la máquina virtual (virtual machine).

## Preguntas de reflexión

1. ¿Cuáles son las ventajas de utilizar HTTPS y no HTTP?

2. ¿Se consideran confiables todos los sitios web que utilizan HTTPS?