Laboratório - Usando Wireshark para examinar tráfego HTTP e HTTPS

Objetivos

Parte 1: Capturar e visualizar tráfego HTTP

Parte 2: Capture e visualize o tráfego HTTPS

Histórico/Cenário

HyperText Transfer Protocol (HTTP) é um protocolo de camada de aplicativo que apresenta dados através de um navegador da Web. Com HTTP, não há salvaguarda para os dados trocados entre dois dispositivos de comunicação.

Com HTTPS, a criptografia é usada por meio de um algoritmo matemático. Este algoritmo oculta o verdadeiro conteúdo dos dados que estão sendo trocados. Isso é feito através do uso de certificados que podem ser visualizados posteriormente neste laboratório.

Independentemente de HTTP ou HTTPS, só é recomendável trocar dados com sites em que você confia. Só porque um site usa HTTPS não significa que é um site confiável. Os atores de ameaças costumam usar HTTPS para ocultar suas atividades.

Neste laboratório, você explorará e capturará tráfego HTTP e HTTPS usando Wireshark.

Recursos necessários

- VM CyberOps Workstation
- Conexão com a Internet

Instruções

Parte 1: Capturar e visualizar tráfego HTTP

Nesta parte, você usará **tcpdump** para capturar o conteúdo do tráfego HTTP. Você usará as opções de comando para salvar o tráfego em um arquivo de captura de pacote (pcap). Esses registros podem ser analisados usando diferentes aplicativos que lêem arquivos pcap, incluindo Wireshark.

Etapa 1: Inicie a máquina virtual e faça login.

Inicie a VM CyberOps Workstation. Use as seguintes credenciais de usuário:

Username: **analyst**

Password: **cyberops**

Etapa 2: Abra um terminal e inicie o tcpdump.

a. Abra um aplicativo de terminal e digite o comando **ip address**.

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

b. Liste as interfaces e seus endereços IP exibidos na saída do **ip address**.

c. Enquanto estiver no aplicativo de terminal, digite o comando **sudo tcpdump —i enp0s3 —s 0 —w httpdump.pcap**. Insira as **cyberops** de senha para o analista de usuário quando solicitado.

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

Este comando inicia o tcpdump e registra o tráfego de rede na interface **enp0s3**.

A opção de comando **-i** permite especificar a interface. Se não for especificado, o tcpdump capturará todo o tráfego em todas as interfaces.

A opção de comando **-s** especifica o comprimento do instantâneo para cada pacote. Você deve limitar snaplen ao menor número que irá capturar as informações do protocolo em que você está interessado. Definir snaplen como 0 define-o para o padrão de 262144, para compatibilidade com versões anteriores recentes do tcpdump.

A opção de comando **-w** é usada para gravar o resultado do comando tcpdump em um arquivo. Adicionar a extensão .pcap garante que os sistemas operacionais e aplicativos serão capazes de ler em arquivo. Todo o tráfego gravado será impresso no arquivo httpdump.pcap no diretório home do analista do usuário.

Use as páginas de manual para tcpdump para determinar o uso das opções de comando -s e -w.

d. Abra um navegador da Web a partir da barra de inicialização dentro da VM CyberOps Workstation. Navegue até **http://www.altoromutual.com/login.jsp**

Como este site usa HTTP, o tráfego não é criptografado. Clique no campo Senha para ver o pop-up de aviso.

e. Digite um nome de usuário de **Admin** com uma senha de **Admin** e clique em **Login**.

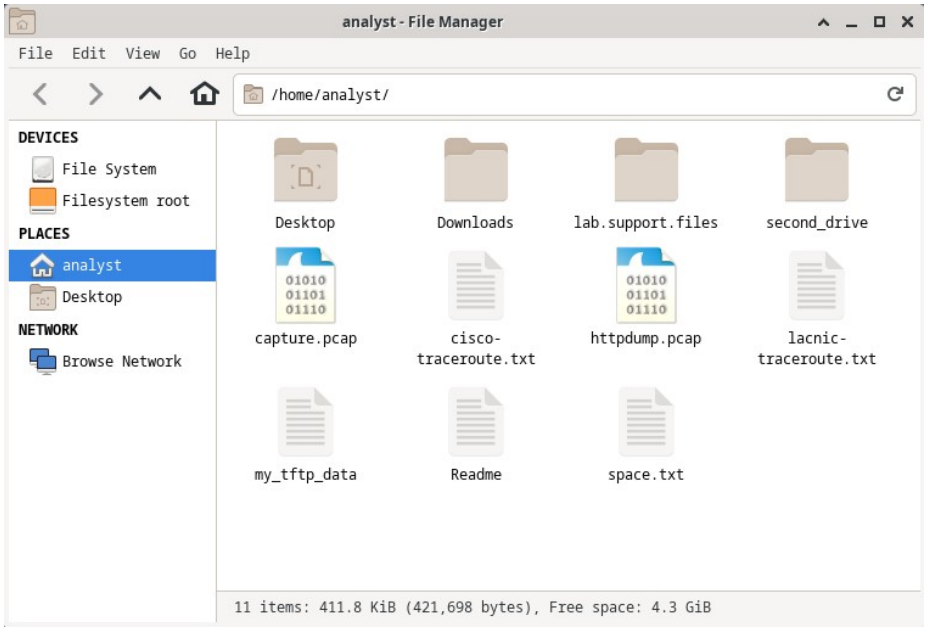
f. Feche o navegador da Web.

g. Retorne à janela do terminal onde o tcpdump está sendo executado. Digite **CTRL+C** para interromper a captura de pacotes.

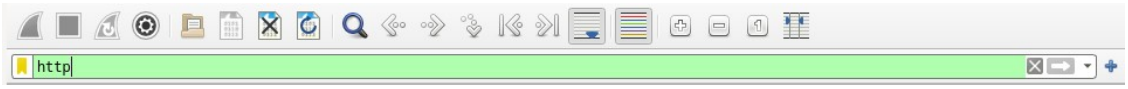
Etapa 3: Exiba a captura HTTP.

O tcpdump, executado na etapa anterior, imprimiu a saída para um arquivo chamado httpdump.pcap. Este arquivo está localizado no diretório home do usuário **analyst**

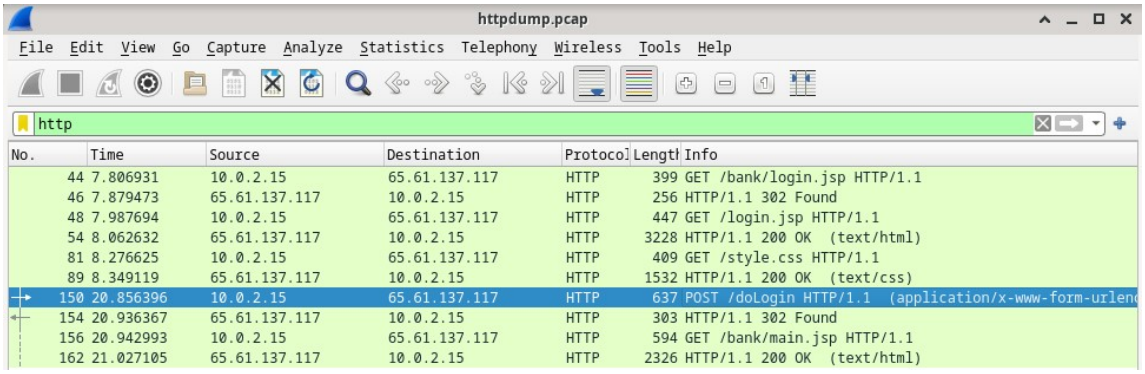
a. Clique no ícone Gerenciador de arquivos na área de trabalho e navegue até a pasta pessoal do usuário **analyst** Clique duas vezes no arquivo **httpdump.pcap**, na caixa de diálogo Abrir com role para baixo até Wireshark e clique em **Open**.



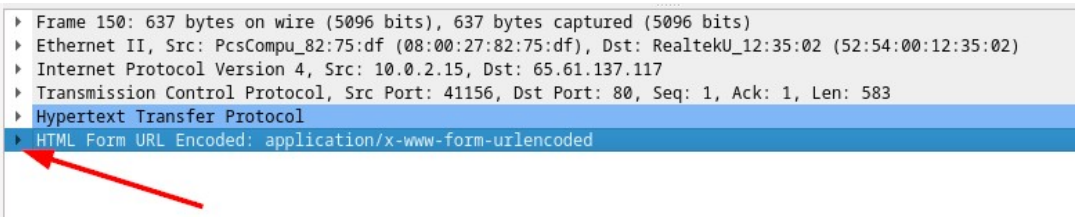
b. No aplicativo Wireshark, filtre para **http** e clique em **Apply**.



c. Navegue pelas diferentes mensagens HTTP e selecione a mensagem **POST**.



d. Na janela inferior, a mensagem é exibida. Expanda a seção **HTML Form URL Encoded: application/x-www-form-urlencoded**.



Quais são as duas informações exibidas?

e. Feche o aplicativo Wireshark.

Parte 2: Capture e veja o tráfego HTTPS

Agora você usará tcpdump a partir da linha de comando de uma estação de trabalho Linux para capturar tráfego HTTPS. Depois de iniciar o tcpdump, você gerará tráfego HTTPS enquanto o tcpdump registra o conteúdo do tráfego de rede. Esses registros serão novamente analisados usando Wireshark.

Etapa 1: Inicie o tcpdump dentro de um terminal.

a. Enquanto estiver no aplicativo de terminal, digite o comando **sudo tcpdump —i enp0s3 —s 0 —w dump.pcap**. Insira as **cyberops** de senha para o analista de usuário quando solicitado.

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

Este comando iniciará o tcpdump e registrará o tráfego de rede na interface **enp0s3** da estação de trabalho Linux. Se a sua interface for diferente do enp0s3, modifique-a ao usar o comando acima.

Todo o tráfego registrado será impresso no arquivo **dump.pcap** no diretório home do usuario analyst

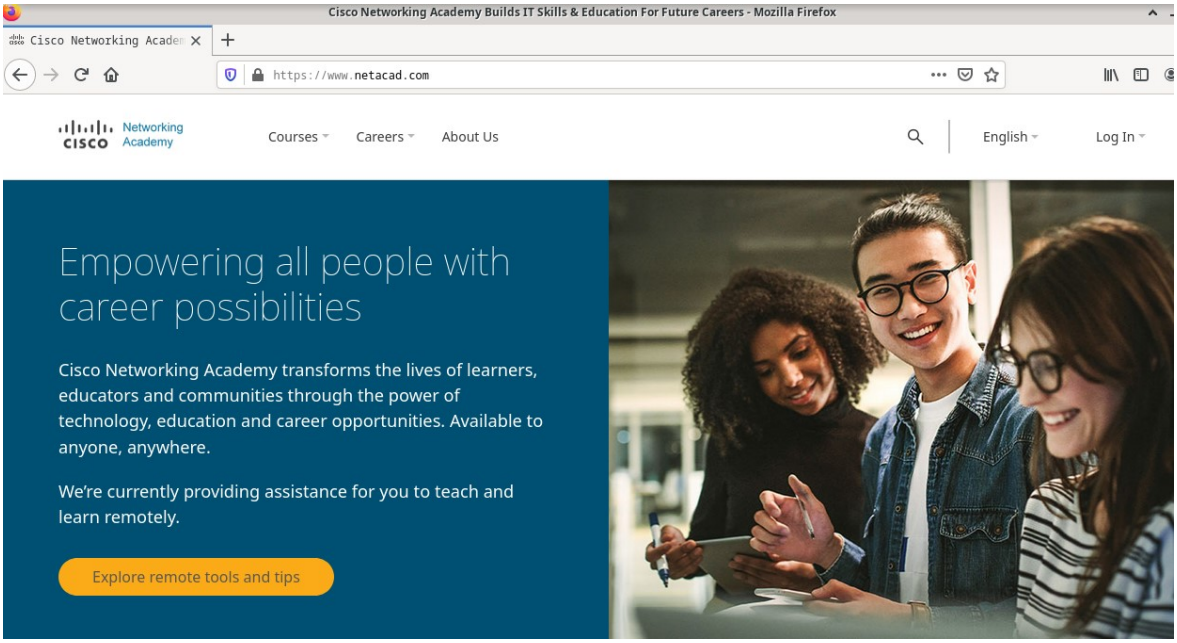
b. Abra um navegador da Web a partir da barra de inicialização dentro da VM CyberOps Workstation. Navigate to www.netacad.com.

Observação: se você receber uma página da Web “Falha na conexão segura”, provavelmente significa que a data e a hora estão incorretas. Atualize o dia e a hora com o seguinte comando, alterando para o dia e hora atuais:

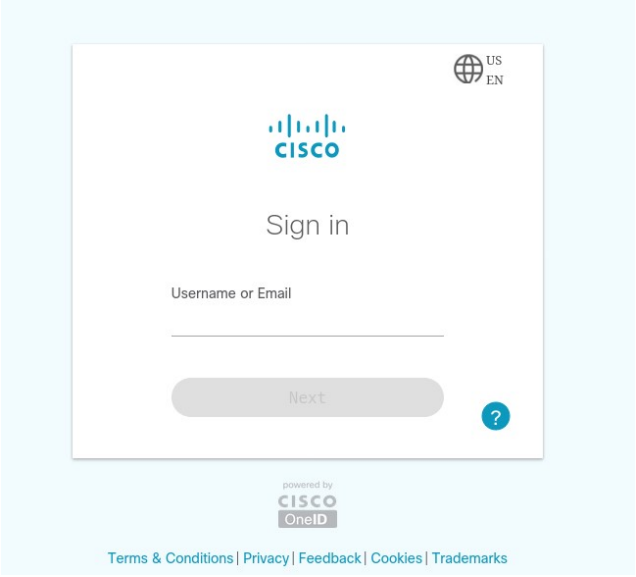
```
[analista @secOps ~] $ data sudo -s "12 MAIO 2020 21:38:20
```

O que você percebe sobre o URL do site?

c. Click **Log in**.



d. Enter in your NetAcad username and password. Clique em **Avançar**.



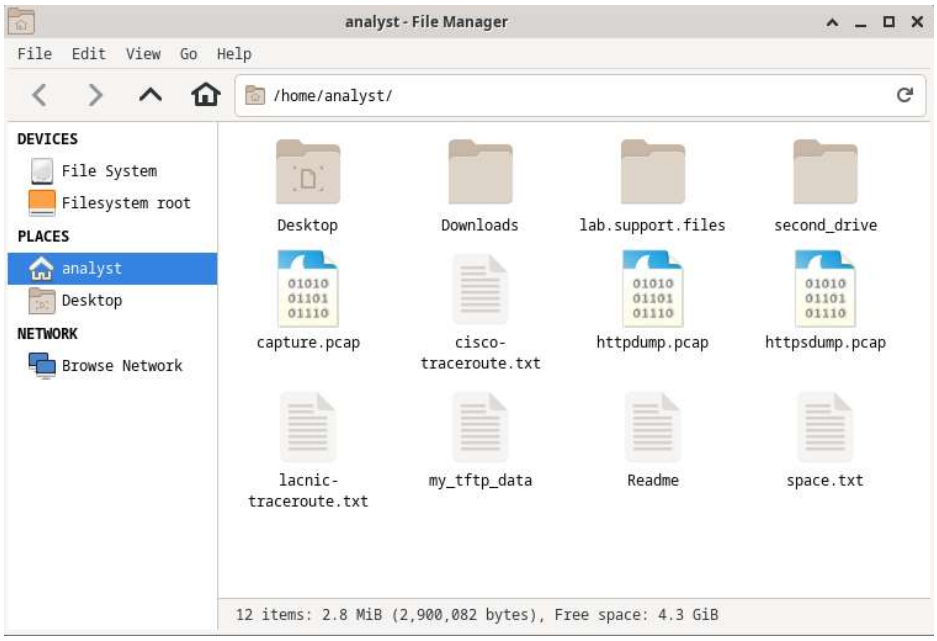
e. Close the web browser in the VM.

f. Retorne à janela do terminal onde o tcpdump está sendo executado. Digite **CTRL+C** para interromper a captura de pacotes.

Etapa 2: Exiba a captura HTTPS.

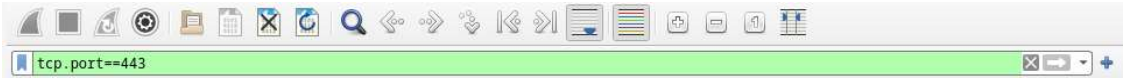
O tcpdump executado na Etapa 1 imprimiu a saída para um arquivo chamado dump.pcap. Este arquivo está localizado no diretório home do usuario **analyst**

a. Clique no ícone Sistema de arquivos na área de trabalho e navegue até a pasta pessoal do usuári analyst Abra o **arquivo dump.pcap**.

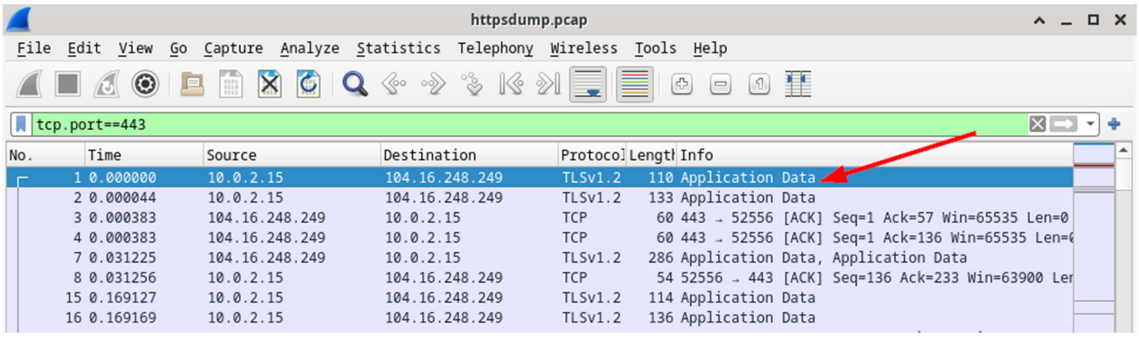


b. No aplicativo Wireshark, expanda a janela de captura verticalmente e filtre pelo tráfego HTTPS pela porta 443.

Digite **tcp.port==443** como um filtro e clique em **Apply**.



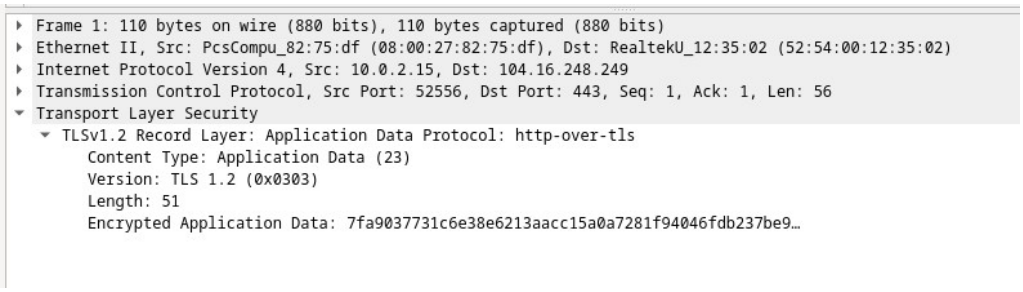
c. Navegue pelas diferentes mensagens HTTPS e selecione uma mensagem **Application Data**.



d. Na janela inferior, a mensagem é exibida.

O que substituiu a seção HTTP que estava no arquivo de captura anterior?

e. Expanda completamente a seção **Secure Sockets Layer**



f. Clique nos **Encrypted Application Data**.

Os dados do aplicativo estão em um formato de texto simples ou legível?

g. Feche todas as janelas e desligue a máquina virtual.

Perguntas para reflexão

1. Quais são as vantagens de usar HTTPS em vez de HTTP?

2. Todos os sites que usam HTTPS são considerados confiáveis?