Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

Objectifs

Partie 1 : capturer et afficher le trafic HTTP

Partie 2 : capturer et afficher le trafic HTTPS

1. Contexte/scénario

Le protocole HTTP (HyperText Transfer Protocol) est un protocole de couche application qui présente des données via un navigateur web. Avec HTTP, aucune mesure de protection n'est appliquée pour les données échangées entre deux appareils qui communiquent.

Avec HTTPS, le chiffrement est assuré par un algorithme mathématique. Cet algorithme cache la véritable signification des données échangées. Pour cela des certificats, présentés ultérieurement dans ces travaux pratiques, sont utilisés.

Qu'il s'agisse de HTTP ou de HTTPS, il est recommandé d'échanger des données uniquement avec des sites web de confiance. Car même si un site utilise HTTPS cela ne signifie pas qu'il est sécurisé. Les hackers utilisent couramment HTTPS pour cacher leurs activités.

Au cours de ces travaux pratiques, vous allez explorer et capturer le trafic HTTP et HTTPS à l'aide de Wireshark.

1. Ressources requises

* Poste de travail virtuel CyberOps
* Connexion Internet

1. Capture et affichage du trafic HTTP

Dans cette partie, vous allez utiliser **tcpdump** pour capturer le contenu du trafic HTTP. Vous allez utiliser des options de commande pour enregistrer le trafic dans un fichier de capture (pcap) de paquets. Les enregistrements peuvent ensuite être analysés à l'aide de différentes applications qui lisent les fichiers pcap comme Wireshark.

* 1. Démarrez la machine virtuelle et connectez-vous.

Démarrez le poste de travail virtuel CyberOps. Utilisez les informations d'identification d'utilisateur suivantes :

Nom d'utilisateur : **analyst**

Mot de passe : **cyberops**

* 1. Ouvrez un terminal et lancez tcpdump.
     1. Ouvrez une application de terminal et saisissez la commande **ifconfig**.

[analyst@secOps ~]$ **ifconfig**

* + 1. Répertoriez les interfaces et leurs adresses IP affichées dans la sortie d'ifconfig.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Dans l'application de terminal, saisissez la commande **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**. Saisissez le mot de passe **cyberops** pour l'utilisateur analyst lorsque vous y êtes invité.

[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

Cette commande démarre tcpdump et enregistre le trafic réseau sur l'interface **enp0s3**.

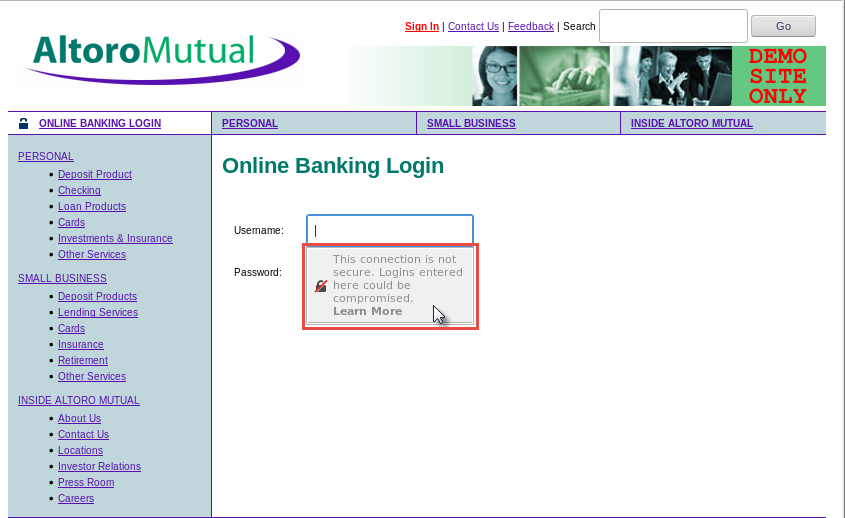
L'option de commande **-i** permet de spécifier l'interface. Si cette option n'est pas spécifiée, la commande tcpdump capturera tout le trafic sur toutes les interfaces.

L'option de commande **-s** spécifie la longueur de la capture pour chaque paquet. Vous devez limiter la longueur de la capture (snaplen) avec la plus petite valeur possible de manière à capturer les informations de protocole qui vous intéressent. Lorsque la longueur est définie sur 0, elle est en fait définie avec la valeur par défaut 262144, pour des raisons de rétrocompatibilité avec les versions plus anciennes de tcpdump.

L'option de commande **-w** sert à écrire le résultat de la commande tcpdump dans un fichier. En ajoutant l'extension .pcap, les systèmes d'exploitation et les applications pourront lire ce fichier. Tout le trafic enregistré sera enregistré dans le fichier httpdump.pcap dans le répertoire de base de l'utilisateur analyst.

Utilisez les pages man de la commande tcpdump pour connaître l'utilisation des options de commande -s et -w.

* + 1. Ouvrez un navigateur web à partir de la barre de lancement dans le poste de travail Linux. Accédez à [**www.altoromutual.com/bank/login.aspx**](http://www.altoromutual.com/bank/login.aspx)

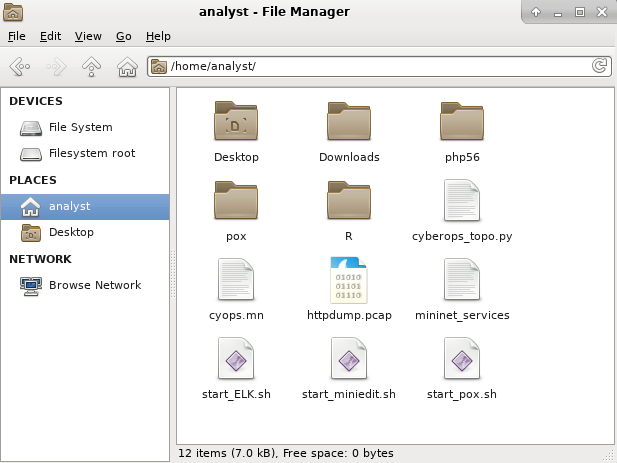


Étant donné que ce site web utilise le protocole HTTP, le trafic n'est pas chiffré. Cliquez sur le champ de nom d'utilisateur pour afficher le message d'avertissement.

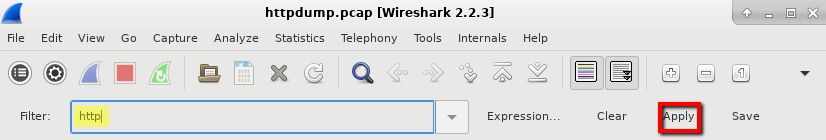
* + 1. Saisissez le nom d'utilisateur **Admin** avec le mot de passe **Admin** et cliquez sur **Login**.
    2. Fermez le navigateur web virtuel.
    3. Revenez à la fenêtre de terminal où tcpdump est en cours d'exécution. Appuyez sur **Ctrl+C** pour arrêter la capture des paquets.
  1. Affichez la capture HTTP.

La commande tcpdump, exécutée à l'étape précédente, a enregistré la sortie dans un fichier nommé httpdump.pcap. Ce fichier se trouve dans le répertoire de base de l'utilisateur **analyst**.

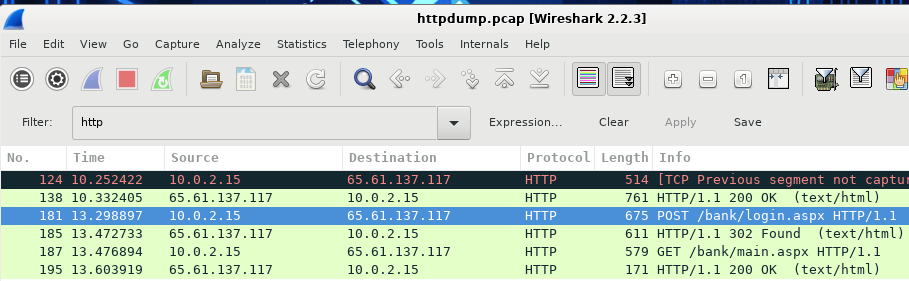
* + 1. Cliquez sur l'icône du gestionnaire de fichiers sur le bureau et accédez au dossier de base pour l'utilisateur **analyst**. Double-cliquez sur le fichier **httpdump.pcap** pour l'ouvrir dans Wireshark.



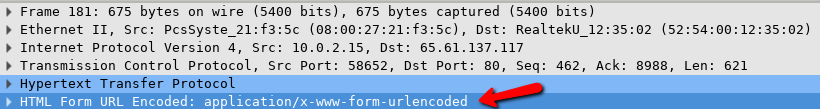
* + 1. Dans l'application Wireshark, recherchez **http** et cliquez sur **Apply**.



* + 1. Naviguez dans les différents messages HTTP, puis sélectionnez le message **POST**.



* + 1. Le message s'affiche dans la fenêtre inférieure. Développez la section **HTML Form URL Encoded: application/x-www-form-urlencoded**.



Quelles sont les deux informations affichées ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Fermez l'application Wireshark.

1. Capturer et afficher le trafic HTTPS

Vous allez maintenant utiliser tcpdump depuis la ligne de commande d'un poste de travail Linux pour capturer le trafic HTTPS. Après avoir démarré tcpdump, vous allez générer le trafic HTTPS et tcpdump enregistrera le contenu du trafic réseau. Ce contenu sera également analysé à l'aide de Wireshark.

* 1. Lancez tcpdump dans un terminal.
     1. Dans l'application de terminal, saisissez la commande **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**. Saisissez le mot de passe **cyberops** pour l'utilisateur analyst lorsque vous y êtes invité.

[analyst@secOps ~]$ **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**

[sudo] password for analyst:

tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

Cette commande démarre tcpdump et enregistre le trafic réseau sur l'interface **enp0s3** du poste de travail Linux. Si votre interface est différente de celle d'enp0s3, modifiez-la lorsque vous utilisez la commande ci-dessus.

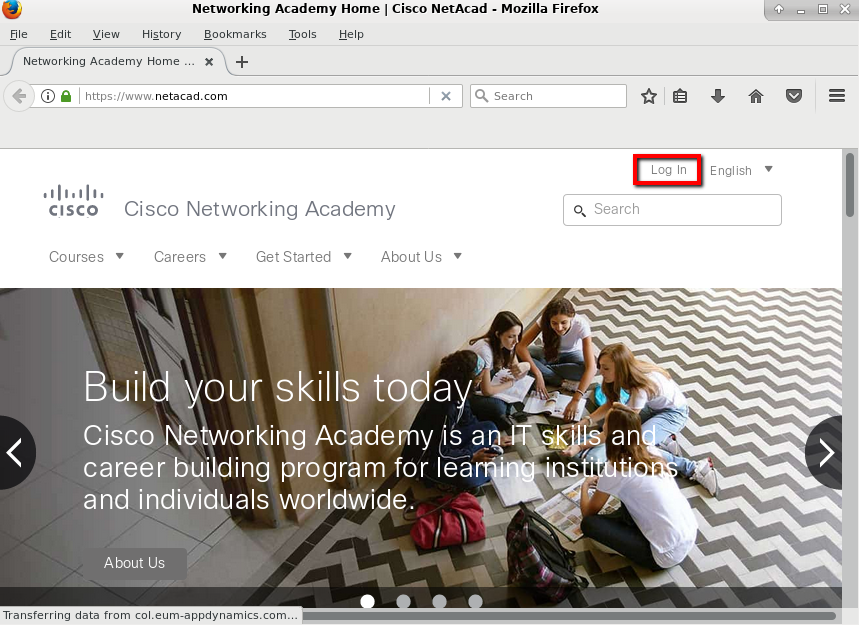
Tout le trafic enregistré sera enregistré dans le fichier **httpsdump.pcap** dans le répertoire de base de l'utilisateur analyst.

* + 1. Ouvrez un navigateur web à partir de la barre de lancement dans le poste de travail Linux. Accédez à [www.netacad.com](http://www.netacad.com).

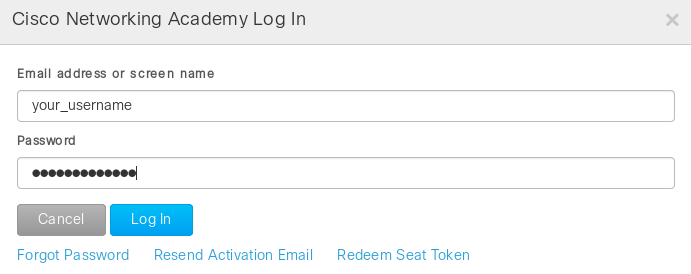
Que remarquez-vous à propos de l'URL du site web ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Cliquez sur **Log in**.



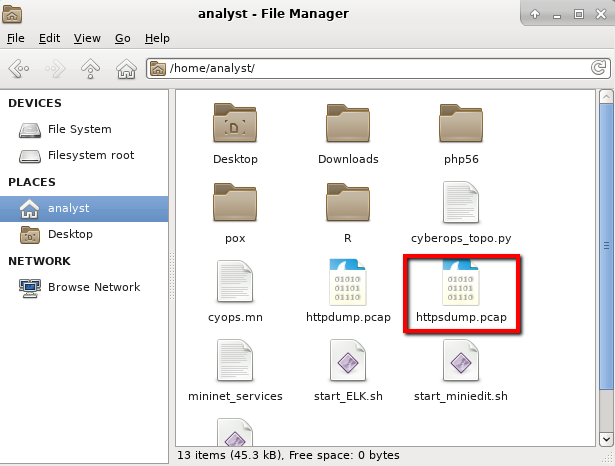
* + 1. Saisissez votre nom d'utilisateur et votre mot de passe pour NetAcad. Cliquez sur **Log In**.



* + 1. Fermez le navigateur web virtuel.
    2. Revenez à la fenêtre de terminal où tcpdump est en cours d'exécution. Appuyez sur **Ctrl+C** pour arrêter la capture des paquets.
  1. Affichez la capture HTTPS.

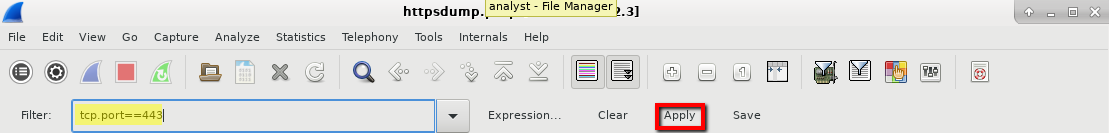
La commande tcpdump exécutée à l'étape 1 a enregistré la sortie dans un fichier nommé httpsdump.pcap. Ce fichier se trouve dans le répertoire de base de l'utilisateur **analyst**.

* + 1. Cliquez sur l'icône du système de fichiers sur le bureau et recherchez le dossier de base de l'utilisateur analyst. Ouvrez le fichier **httpsdump.pcap**.

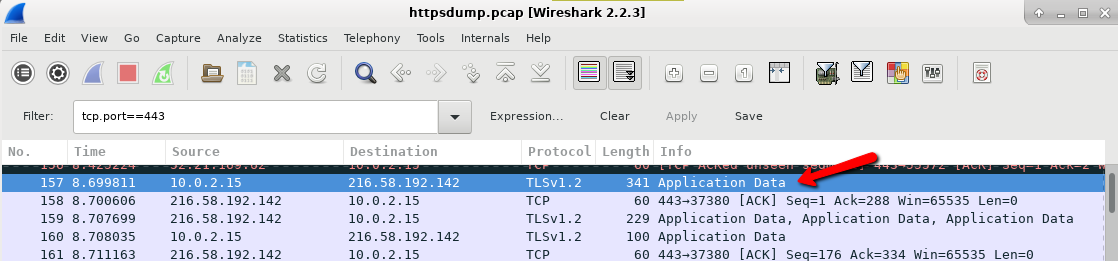


* + 1. Dans l'application Wireshark, agrandissez la fenêtre de capture verticalement, puis filtrez par trafic HTTPS via le port 443.

Saisissez **tcp.port==443** comme filtre, puis cliquez sur **Apply**.



* + 1. Naviguez parmi les différents messages HTTPS, puis sélectionnez un message **Application Data**.

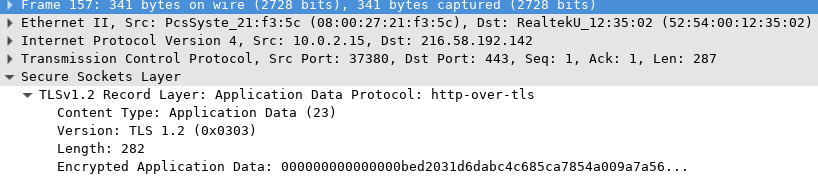


* + 1. Le message s'affiche dans la fenêtre inférieure.

Par quoi la section HTTP qui était dans le fichier de capture précédent a-t-elle été remplacée ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Développez complètement la section **Secure Sockets Layer**.



* + 1. Cliquez sur **Encrypted Application Data**.

Les données d'application sont-elles en texte clair ou dans un format lisible ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Fermez toutes les fenêtres et arrêtez la machine virtuelle.

1. Remarques générales
   1. Quels sont les avantages d'utiliser HTTPS plutôt que HTTP ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Tous les sites web qui utilisent le protocole HTTPS sont-ils considérés comme sécurisés ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_