Aller au contenu

AP#2 SISR – Atelier 10
Analyse de logs
Analyse de trames
TCP – HTTP - HTTPS

Un exemple de formulaire de connexion est disponible sur la machine 10.187.20.5. Il est composé de deux pages :
• index.html
• style.css
Copiez ces 2 fichiers avec la commande scp sur votre serveur dans le répertoire racine du VirtualHost www.m2l.org [http://www.m2l.org].

machine qui possede les fichiers dans **/home/std/** sur la machine **10.187.20.5**
Vous pouvez utiliser le compte **std et mdp : password**

Téléchargement des fichier index.html et style.css depuis la machine 187.20.5 dans le repertoire racine de www
scp std@10.187.20.5:/home/std/index.html /home/htdocs/m2l.org/www/
scp std@10.187.20.5:/home/std/style.css /home/htdocs/m2l.org/www/

Deplacer les fichier dans le dossier intranet car www.m2l.org [http://www.m2l.org] ne marche pas
site : http://intranet.m2l.org [http://intranet.m2l.org]

Du coup deplacer les fichier dans **/home/htdocs/m2l.org/intranet/**

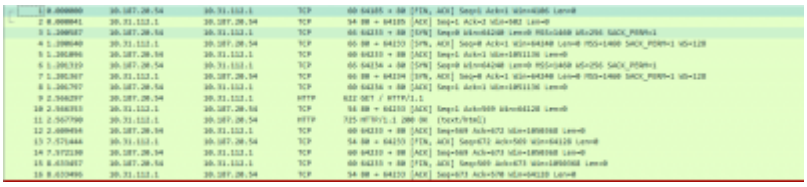
Dans /etc/apache2/apache2.conf, se trouvent les directives qui déterminent le format des fichiers de logs d'apache.
✓ Dans la configuration de votre Virtualhost, quel format décrit dans le fichier apache2.conf est utilisé comme CustomLog ?
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
%h Serveur distant. Contiendra l'adresse IP
%l Le nom de connexion distant
%u L'utilisateur distant
%t Date à laquelle la requête a été reçue
%r La première ligne de la requête
%s Statut. Pour les requêtes redirigées en interne
%O Nombre d'octets envoyés

✓ Grâce à la documentation, expliquez en détail le format des logs par défaut. Écrasez le fichier fichier access.log dont le chemin est défini dans votre VirtualHost. Dans un navigateur web, allez sur www.m2l.org [http://www.m2l.org].

Le fichier access.log pour www.m2l.org [http://www.m2l.org] est dans : **nano /var/log/apache2/www-access.log**

```
1 10.187.20.54 - sio [19/Mar/2021:08:17:55 +0100] "POST / HTTP/1.1" 200 671 "http://intranet
2 10.187.20.54 - sio [19/Mar/2021:08:17:58 +0100] "POST / HTTP/1.1" 200 670 "http://intranet
```

✓ Analyse du protocole HTTP



• Expliquez dans l'ordre les trames HTTP (colonne protocol)
Le client envoie une requete syn sur le serveur
Le serveur repond avec une reponse syn et ack
Et le client repond avec une reponse ack

SYN : Le client qui désire établir une connexion avec un serveur va envoyer un premier paquet SYN (synchronized) au serveur.
SYN-ACK : Le serveur va répondre au client à l'aide d'un paquet SYN-ACK (synchronize, acknowledge).
ACK : Pour terminer, le client va envoyer un paquet ACK au serveur qui va servir d'accusé de réception. Le numéro d'acquittement de ce paquet est défini selon le numéro de séquence reçu précédemment.

NOTE :
Utilise filezilla pour transferer les fichier .pcap depuis le serveur vers sa machine pour pouvoir l'analyser avec wireshark

- Capture de la trame avec tcpdump **apt install tcpdump** On capture les trame pour http soit sur le port 80 donc :

• Notez bien qui émet la trame (le client ou le serveur) Le client émet la premiere trame

• Pour les trames émises par le client, notez le nom de la requête et la cible dans le cas d'une requête GET

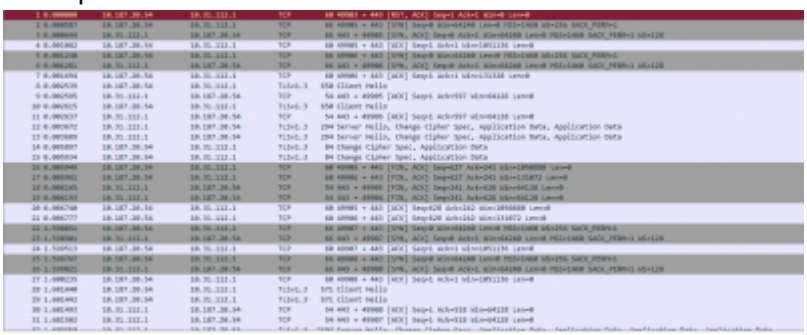
```
1   11  2.607176    10.31.112.1 10.187.20.54    HTTP    725 HTTP/1.1 200 OK  (text/html)
```

• Pour les trames émises par le serveur et les requêtes POST du client, cherchez les données échangées

Les données echange sont le htpasswd et l'identifiant et le mot de passe ecrit dans la page html

Vous avez créé un certificat auto-signé lors de la mission 7.
✓ Allez sur un site web sécurisé (https) et affichez le certificat du site. Notez les informations principales que vous pourrez trouver dans ce certificat Les informations sont :
Delivré a www.google.com [http://www.google.com]
Delivré par : GTS CA 101
Valide du 23/02/2021 au 18/05/2021

✓ Réalisez la même capture de trames que précédemment à la différence que vous utiliserez votre site en https cette fois-ci.



✓ Analysez à nouveau les trames HTTPS. Quelles sont les éléments auxquels vous avez accès ? Que pouvez-vous en conclure sur SSL/TLS.
Avec le protocole https il se passe exactement la meme chose au debut, mais cette fois le serveur et le client se mette d'accord sur le protocole de chiffrement qui sera utilisé se qui rend impossible la lecture
des données brutes car elle sont chiffres.

Essayez de faire un suivi de la/les connexion(s) TCP établies lors de la communication entre client et le serveur web et des requêtes/réponses HTTP en distinguant :
• Le/Les handshake(s) TCP

- Le/Les fermeture(s) de session TCP
- Les ACK en cours de session
- Les informations couche 4 sur les différentes trames HTTP