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

%I 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

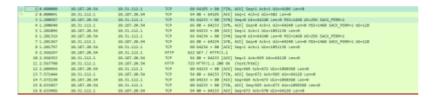
%s Statut. Pour les requêtes redirigées en interne

%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

✓ 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.

1.0.000000	18, 187, 39, 14	18.75.311.1	109	88 40985 + 440 [107, ACK] Sep-1 ACK-5 100-0 Set-0
2 0.000187	18.187.39.16	18.70.331.1	107	88 4090 + 440 [170] 34q-0 834-04340 Lav-0 703-1488 30-236 3402_7000-1
3 0.000044	18.35.311.1	18,187,38,16	107	HE SEE - 49900 [178, ACC] Depth Acts. His-state Level PRI-1488 DAIL/FRE-1 M-128
4 0.000803	18,187,39,16	16.15.331.1	107	Bernal of the Child (See Local March March 1997) 1846 - 1986 Ba
1 0.001238	18.187.39.16	18.30.331.1	109	AN ADDRES - ARC [UNG] Despit microlable Leroit PRE-Links and ARC PRE-Links Links (PRE-Links)
6.9.965265	18.35.311.1	16.187.36.48	107	NE SEC + \$1000 [UN, ACK] Depth Acked Microbiate Level PRE-LINE SACK PRESS MILITED
7 0.001474	10.107.30.56	10.10.111.1	107	48 ADDRE - AAD [DOT] Sept into 1 March 10200 DOTS
8 9-990539	10.107.30.58	10.70-111-1	Tidel-3	658 Client Hella
9 0.002505	10.70-311-1	10.107.30.54	101	54 AND = 49965 [MOI] Sept. Adm957 MEMBASS Lamp8
30 0.000535	10.107.30.56	10-50-331-1	Tt5vt-3	658 (Lient Pello
11.0-000507	19-20-211-1	19-197-29-54	702	54 440 × 49966 [AOT] Seprit, Admits Francisco Lamille
11 0.000072	19-20-211-1	19-187-29-14	71395-3	ISM Server Mello, Change Cipher Spec, Application Sate, Application Sate
15 0.000600	18-20-331-1	19,187,09,04	71395.0	INM Server Hello, thange tipher Spec, Application Sats, Application Data
14 9,985897	18.187.39.16	18.05.331.1	71395.3	BM Change Cipher Spec, Application Data
13-0.0000004	18,187,39,34	18.75.331.1	71395.3	BM Change Cipher Spec, Application Data
30 0.000049	18.187.39.34	18.70.333.1	107	88 4000 + 440 [FOR, ACK] ImpelIT ALK-ON MIN-180000 Lan-8
TT 0.0000HG	18.187.39.36	18.70.333.1	107	88 40000 + 440 [FOR, ACK] ImpelIT Ask-OHI Mar-DERIY Lear-B
18 0.006185	18.35.311.1	18.187.39.36	107	16 661 - 6666 [Fib., ACC] Impidd Astrolii Mareklii Larek
29 0.004183	18.35.311.1	18.187.39.38	107	DE SEE - 40000 [Fib., ACK] Republi Autorial Marchilla Larvell
20 0.006748	10.107.30.56	10.10.331.1	108	69 48981 + 663 [SOX] SequiDE Sch-262 Mon-2006689 Lennill
21.0.006277	10,107,20,16	10.10.331.1	707	AN ARREST + AAS [ACK] SequEDE Activided Microsoft Lennis
22 1.104851	18.167.30.58	10.70.311.1	109	A CONTROL OF THE CONTROL WAS A STATE OF THE CASE OF TH
25 1.504090	18.35.112.1	10.107.30.54	101	EX AND A \$5000 [CVM, ACK] Septé Acket simulates canné PSS-LANS SACK_PERMIT ME-128
84 1-100503	19.107.30.56	10-30-311-1	102	58 40987 - 445 [MOI] Sept. Admit Mintellist Namel
25-1/500000	19.107.00.54	19-70-331-1	102	SS ADDRE 4 AND [STR] SHOPE REPORTED LINES TREATMEN ASKEDS SHOW, FRIEND
35-1/599923	18-20-001-1	19.187-09.54	107	56 MO - 4990 [S78, ACK] Supel ACKS, Kinnelse Lune 1951-148 SACK, PERFO ISS-129
17 1/699005	18-187-19-19	18-20-331-1	707	SE 400ES + 440 [ACX] 340E-C ACK-1 MIN-ESCRIP LAN-E
39 1/005448	18.187.09.16	19.75.331.1	71395.3	pri cliest sello
39 1.000.443	18,187,39,14	18.75.331.1	T13V5.3	PT. Cliest Helia
30 1,460,403	18.75.311.1	18,187,38,14	707	14 440 + 4898 (401) 344-1 A0-118 M3-04128 Lan-8
31.1.460363	18.70.311.1	18,187,38,16	707	54 440 + 46007 (ACC) 344-5 ACC-512 MA-04122 Lan-8
25.1.480EB	15.05.711.1	15.107.75.44	715-1-4	AND Francis States Phones States Sant Surface States State States State States States States States States States

✓ Analysez à nouveau les trames HTTPS. Quelles sont les éléments auxquels vous avez accès ? Que pouvez-vous en conclure sur SSL/TLS.

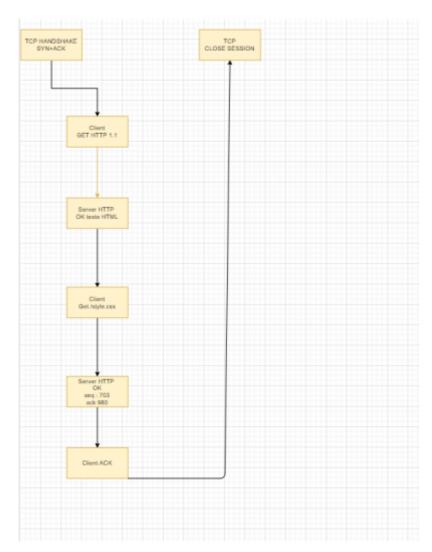
Avec le protocole https il se passe exactement la meme chose au debut, mais cette fois le serveur et le client se mette d'accord sur le protocole de chiffrement qui sera utilisé se qui rend impossible la lecture

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



sisr1-g7/mission_10.txt · Dernière modification: 2021/03/23 11:46 de h-benzahaf