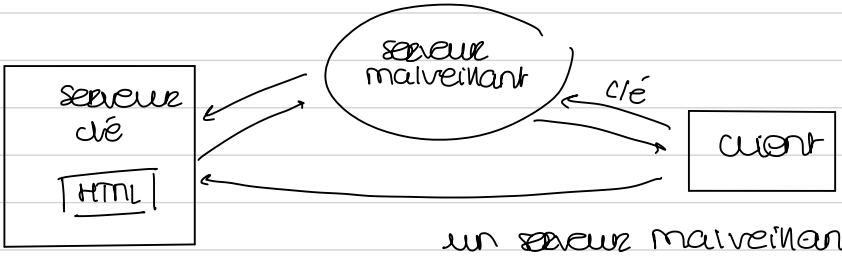
Fiche TD 1

EXERCICE 1 HTTPS

Certificat = fiche d'identité du site (infos du site)

1) Protocole HTTPS = Hypertext Transfert Protocole Secure
Combinaison du HTTP avec du chiffrement comme SSL ou TLS
Il permet de vérifier l'identité du site web auquel un client accède grâce à un certificat d'authentification.
Il garantie la confidentialité et l'intégrité des données envoyées par l'utilisateur



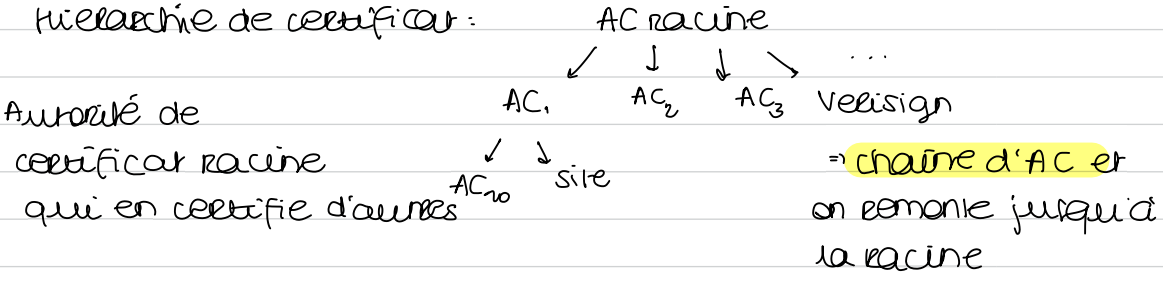
un serveur malveillant peut s'interposer entre les 2 et récup les données

- certificat pour éviter ça

2) Regarder le nom de domaine
notion de vérification de l'identité du domaine dans l'HTTPS
Connexion non certifiée : ne fait pas confiance à l'autorité qui a délivré le certificat

↳ autorité de certification inconnue

Hiérarchie de certificat :



Autorité de certificat racine qui en certifie d'autres

⇒ chaîne d'AC et on remonte jusqu'à la racine

Le navigateur collecte les AC au fur et à mesure, si on accepte une AC, tous les certificat signés par cette AC seront acceptés
→ on peut aussi révoquer des certificats

⇒ site pas forcément malveillant mais juste pas dans la chaîne de confiance

3) 1) master.support.mozilla.com
SSL - début de la sécurisation sur Internet
transformé en TLS
- protocole d'échange de clé

2) master.support.mozilla.com
délivrant

3) master.support.mozilla.com
chaîne

4) master.support.mozilla.com auto-signé

└ certificat auto-signé révoqué dès qu'il est détecté

EXERCICE ② Attaque Blacknurse

1) denial of service with limited resources
sending Type 3 code 3 ICMP packets to overwhelm
Destinat unreachable ↑ Port unreachable processors on servers

ICMP – Internet Control Message Protocole
└ use by router and other networking devices to send and receive error messages
└ un des protocoles compagnon d'IP

déni de service – trop grand nb de requêtes
└ sur une seule machine
déni de service distribué – ensemble d'acteurs qui envoient toutes les requêtes en même temps

"Ping de la mort" = messages trop nombreux et malformés (mauvais format donc prend + de ressources)

smurf attack ⇒ envoi de messages ICMP à plusieurs serveurs et donnent l'adresse IP de la victime pour envoyer les réponses qui reçoit des milliers de réponses

Paquets de grandeur supérieure – une seule machine avec peu de bande passante peu créer un gros déni de

service avec juste des messages malformés

2) - désactiver communicat ICMP de type 3 (sans interdire toutes les communicat ICMP)
   └ mais peut bloquer la découverte du MTU
   (= taille max des packets sur un chemin)
- blacklister ou mettre en quarantaine l'IP en question