Fondements de la sécurité : TD1 - Cryptographie

Exercice 1 : HTTPS

Sujet

1. Décrivez brièvement en quoi consiste le protocole HTTPS (trois phrases maximum).

Lors d'une connexion à un site web, une fenêtre apparaît :

2. S'agit-il d'un site contrefait et/ou malveillant ?
3. En cliquant sur "Détails techniques", j'observe également les avertissements suivants, que vous devez compléter :

   3.1. Le certificat n'est valide que pour (https ://master.support.mozilla.com)

   - Ce site utilise un certificat de sécurité invalide. Le certificat n'est valide que pour _____ (Code d'erreur : ssl_error_bad_cert_domain)

   3.2. Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue

   - _____ utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue. (Code d'erreur: sec_error_unknown_issuer)

   3.3. Le certificat n'est pas sûr car aucune chaîne d'émetteurs de confiance n'est fournie

   - _____ utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car aucune _____ d'émetteurs de confiance n'est fournie. (Code d'erreur : sec_error_unknown_issuer)

   3.4. Le certificat n'est pas sûr car il est auto-signé

    - _____ utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car il est signé. (Code d'erreur : sec_error_untrusted_issuer)
4. Expliquez chaque message et donnez pour chacun une hypothèse optimiste (i.e. erreur justifiable sans qu'il y ait un risque de sécurité pour l'utilisateur) et une hypothèse alarmiste (i.e. erreur résultant d'une tentative d'attaque).

Résolution

Question 1

HTTPS : (*HyperText Transfer Protocol Secure*) est un protocole de sécurité pour les communications sur le web. Il crypte les données transmises entre un navigateur et un site web pour protéger les informations sensibles, telles que les mots de passe et les informations de carte de crédit. L'utilisation d'un certificat SSL (*Secure Sockets Layer*) est nécessaire pour établir une connexion HTTPS sécurisée.

Question 2

Ce message signifie que le navigateur n'a pas confiance en l'autorité de certification du site. Cela n'implique donc pas forcément que celui-ci est contrefait et/ou malveillant.

Question 3

1. Le certificat n'est valide que pour (https ://master.support.mozilla.com)
    - Ce site utilise un certificat de sécurité invalide. Le certificat n'est valide que pour **https ://master.support.mozilla.com** (Code d'erreur : ssl_error_bad_cert_domain)
2. Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue
    - **https ://master.support.mozilla.com** utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue. (Code d'erreur: sec_error_unknown_issuer)
3. Le certificat n'est pas sûr car aucune chaîne d'émetteurs de confiance n'est fournie
    - **https ://master.support.mozilla.com** utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car aucune **chaîne** d'émetteurs de confiance n'est fournie. (Code d'erreur : sec_error_unknown_issuer)
4. Le certificat n'est pas sûr car il est auto-signé
    - **https ://master.support.mozilla.com** utilise un certificat de sécurité invalide. Le certificat n'est pas sûr car il est signé. (Code d'erreur : sec_error_untrusted_issuer)

Question 4

- Le certificat n'est valide que pour (https ://master.support.mozilla.com) :

    - **Hypothèse optimiste :** Le site web a été migré vers un nouveau domaine et un nouveau certificat n'a pas encore été obtenu pour le nouveau domaine.
    - **Hypothèse alarmiste :** Un tiers malveillant a créé un site web phishing ressemblant au site web légitime et a utilisé un certificat délivré pour un autre domaine.
- Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue :
    - **Hypothèse optimiste :** Le site web utilise un certificat émis par une autorité de certification peu connue mais fiable.
    - **Hypothèse alarmiste :** Le site web utilise un certificat auto-signé ou émis par une autorité de certification compromise, ce qui rend le site potentiellement dangereux.
- Le certificat n'est pas sûr car aucune chaîne d'émetteurs de confiance n'est fournie :
    - **Hypothèse optimiste :** Le site web utilise un certificat émis par une autorité de certification qui n'a pas encore été incluse dans la liste des autorités de confiance du navigateur web.
    - **Hypothèse alarmiste :** Le site web utilise un certificat falsifié ou émis par une autorité de certification compromise, ce qui rend le site potentiellement dangereux.
- Le certificat n'est pas sûr car il est auto-signé :
    - **Hypothèse optimiste :** Le site web utilise un certificat auto-signé pour des raisons de coûts ou de commodité, mais il est toujours considéré comme sécurisé.
    - **Hypothèse alarmiste :** Le site web utilise un certificat auto-signé pour masquer son identité et tromper les utilisateurs en les incitant à transmettre des informations sensibles.

Exercice 2 : Analyse de texte (*Blacknurse*)

Sujet

L'article fourni traite de l'attaque ***Blacknurse***.

1. En quoi consiste cette attaque et pourquoi est-elle surprenante ?
2. Discutez des actions qu'un administrateur pourrait mettre en oeuvre pour se protéger de cette attaque.

Résolution

Question 1

Cette attaque consiste à envoyer des paquets **ICMP** (*Internet Control Message Protocol*, utilisé pour échanger des informations sur l'état ou des messages d'erreur) de type 3 (type 3 : permet de dire que la destination n'est pas atteignable) avec un code de 3 pour causer un **DoS** (*Denial of Service*) en surchargeant le processeur. En effet, les messages ICMP doivent être traités par le serveur.

Ce qui est surprenant c'est que nous pouvons faire cette attaque depuis un ordinateur portable avec peu de bande passante $(15Mb/s)$.

Question 2

Pour éviter ce genre d'attaque, l'administrateur réseau peut :

- Filtrer le trafic pour refuser les messages ICMP de type 3 et de code 3 mais cette solution n'est pas optimale car ces messages peuvent être importants.
- Blacklister les attaquants lorsque nous les identifions.
- Améliorer le matériel physique.