Epreuve de sécurité réseaux Troisième Année F2 - F5 2023

1. **Sur un réseau local mal protégé physiquement, il est assez facile de réaliser une attaque pour voir les trames échangées.**

   a. Pour vous, que signifie « réseau local mal protégé physiquement » ?

   Un réseau local mal protégé physiquement signifie que les équipements réseau (routeurs, switchs ou câbles réseau) sont accessibles physiquement à des personnes non autorisées, permettant des manipulations ou des écoutes non légitimes.

   b. Quel serait l'attaque possible et comment le pirate pourrait s'y prendre?

   Attaque: sniffing ou écoute passive

   - Un attaquant peut brancher un dispositif (comme un ordinateur ou un sniffer matériel) sur le réseau pour capturer les trames échangées.
   - Outils: Wireshark, tcpdump
   - Méthode: L'attaquant configure sa carte réseau en mode promiscuous pour capturer tout le trafic.

c. Comment l'administrateur peut-il essayer de s'en protéger?

   Restreindre l'accès physique au matériel (utilisation de salles verrouillées)

   Activer des fonctionnalités comme Port Security sur les switchs pour limiter les péripériques autorisés par adresse MAC.

   Utiliser le chiffrement au niveau applicatif (TLS) ou au niveau réseau (IPsec)

2. **Quels sont les différents équipements actifs qui permettent de faire du filtrage dans un réseau ? Explicitez leurs rôles et leurs différences.**

   - Pare-feu
     - Rôle: Bloquer ou autoriser le trafic basé sur des règles IP, ports ou protocoles.
     - Différence: Focalisé sur les couches réseau(3) et transport(4)
   - Proxy
     - Rôle: Intermédiaire entre le client et le serveur, contrôle et filtre les requêtes HTTP/HTTPS
     - Différence: Fonctionne au niveau applicatif
   - Routeur avec ACL
     - Rôle: Applique des règles de filtrage simples au niveau des adresses IP ou des ports
     - Différence: Moins granulaire qu'un pare-feu
   - IDS/IPS
     - Rôle: IDS détecte les intrusions; IPS bloque les comportements malveillants en temps réel
     - Différence: IDS est passif, IPS est actif

3. **En réseau, lorsqu'on parle de sécurité, très rapidement, le concept d'une "défense en profondeur" est abordé. Quelle est l'idée derrière ce concept?**

   Utiliser plusieurs couches de sécurité indépendantes pour ralentir ou empêcher un attaquant d'accéder à une ressource critique, même si une couche est compromise

Exemple: Utilisation combinée de pare-feu, VPN, IDS/IPS, VLAN, chiffrage des données et authentification forte.

4. **En quoi consiste l'attaque "DDOS" ? Comment faire pour s'en protéger?**
   - Description:

     Une attaque par déni de service distribué (DDoS) consiste à submerger une cible avec un volume de trafic massif en provenance de multiples sources, rendant ses services indisponibles.

   - Protection:

     Utiliser un load balancer

     Configurer des filtres au niveau du pare-feu pour limiter les connexions simultanées

     Adopter des solutions anti-DDoS basées sur le cloud

5. **Quelle est l'objectif dans un réseau ?**
   a. D'un SIEM ?

      Rôle: Collecte, corrèle et analyse les logs de tous les équipements pour identifier des incidents de sécurité

   b. D'un IDS ?

      Rôle: Détecte les comportements anormaux dans le trafic réseau mais ne les bloque pas

   c. Quelles différences existe-t-il entre ces deux équipements ?

      SIEM agrège et analyse les données sur une vue globale; IDS se focalise sur les attaques réseau en temps réel

6. **Quel est le rôle d'une autorisé de certification ?**

   Une CA certifie l'identité des entités en émettant des certificats numériques, assurant que les clés publiques appartiennent bien à leurs propriétaires légitimes

7. **Comment chroot**
   a. Quelle est l'objectif de la commande chroot sous linux ?

      Créer un environnement isolé où programme s'exécute comme s'il était dans répertoire racine différent, limitant son accès au reste du système

b. Que faut-il faire pour qu'un programme puisse fonctionner dans un environnement chrooter ?

- Copier les binaires nécessaires et leurs dépendances dans l'environnement chrooté.
- Configurer les fichiers essentiels, comme

```
/etc/passwd
/etc/resolv.conf
```

8. **Quelle est l'utilisé d'un VPN sécurisé ? Deux protocoles différents sont utilisés pour des situations différentes ? Lesquels et quand ?**
   - Utilité:
     - Protéger les communications en chiffrant le trafic entre deux points.
     - Scénarios: Accès à distance, interconnexion de sites.
   - Protocoles:
     - IPsec: Sécurisation au niveau du réseau (VPN site è site)
     - SSL/TLS: Sécurisation au niveau applicatif (VPN utilisateur)
9. **Souvent, sous quelques distributions linux, on trouve l'applicatif: selinux. Qu'est-ce que c'est et à quoi cela sert-il ?**
   - Description:

     Un module de sécurité sous Linux qui applique une politique de contrôle d'accès obligatoire (MAC)
   - Utilité:

     Renforce la sécurité en limitant les actions des processus, même s'ils sont compromis
10. **Lorsque l'on utilise un pare-feu, sur quelles informations peut-on filtrer ?**

    Un pare-feu peut filtrer sur:

    Adresse IP source ou destination

    Numéro de port

    Type de protocole (TCP, UDP, ICMP)

    Etat de connexion (nouveau, établi)

11. **Qu'est-ce-que l'authentification forte? Pouvez-vous citer un exemple ?**
    - Description: Utilisation d'au moins deux facteurs d'authentification différents (MFA)
    - Exemple: Combinaison d'un mot de passe (connaissance) et d'un code envoyé sur téléphone(possession)
12. **En utilisant l'algorithme de Diffie-Hellman?**
    a. Que verrait-on passer comme information sur le réseau si les nombres choisis sont: P=37 comme nombre premier et g=11 comme nombre générateur et si Bob prend le nombre 4 et Alice le nombre 3 ?

$$A = g^a \mod P => A = 11^3 \mod 37 = 31$$

$$B = g^b \mod P => B = 11^4 \mod 37 = 4$$

    b. Quelle serait d'ailleurs la clé issue de l'algorithme ?

$$K = A^b \mod P = 31 \mod 37 = 16$$

$$K = B^a \mod P = 4^3 \mod 37 = 16$$

    c. Pourquoi la clé est-elle considérée comme sûre ?

    Le problème mathématique inverse (logarithme discret) est difficile à résoudre, même avec P, g, A et B connus.

13. **La communication par mail est très importante de nos jours? Est-ce que les informations qui circulent sont protégées ? Oui, non ? Est-il possible d'avoir un mail sécurisé totalement, comment ?**

    Les mails standards (SMTP) ne sont pas sécurisés.

    Sécurisation:

    Chiffrement TLS entre serveurs

    Utilisation de PGP ou S/MIME pour chiffrer le contenu das mails

14. **WhatsApp fait de la publicité sur le fait que les communications sont chiffrées de bout en bout. Qu'est-ce que cela signifie ?**
    - Description:

Les messages sont chiffrés sur l’appareil de l’expéditeur et ne peuvent être déchiffrés que sur l’appareil du destinataire.

- Avantage:

  Même si les serveurs sont compromis, le contenu reste inaccessible aux attaquants