DS

Sécurité et cryptographie

Classes: 2ing GLSI

Documents autorisés

Exercice 1 [8pts]:

1) Expliquer pourquoi il est plus facile d'écouter (sniffer) un réseau local sans fil qu'un réseau local câblé ?
2) Expliquer comment la segmentation réseau (mise en place de sous réseau) assure une certaine sécurité pour le réseau de l'entreprise?
3) Vue le nombre limité des adresses publiques, on utilise souvent un adressage privée (adresse non routable) pour le réseau local d'une entreprise. Expliquer comment cet adressage permet de cacher le réseau local par rapport aux attaquants externes?
4) Est-ce que n'importe quelle attaque peut être lancée à partir de l'extérieur du LAN de l'entreprise? Expliquer ?
5) Expliquer pourquoi les attaques internes sont plus faciles à mener que les attaques externes ?
6) Expliquer pourquoi les attaques passives sont plus utiles (pour l'attaquant) dans un réseau partagé que dans réseau commuté ?
7) Expliquer comment un attaquant peut transformer un réseau Ethernet commuté en un réseau partagé ? Donner une solution permettant de contrer cette attaque ?
8) En se basant sur DHCP, expliquer comment un attaquant peut faire passer le trafic destiné à Internet par lui ? Donner une solution permettant de contrer cette attaque ?
9) Donner une solution permettant de détecter et identifier les serveurs DHCP pirates
10) Soit trois nœuds A, B et C relié à un commutateur. Donner une solution permettant à A d'intercepter les messages échangés entre B et C.?

Exercice 2 [5pts]:

1) Est-il nécessaire d'utiliser un canal authentifié pour échanger la clé de chiffrement dans un système à chiffrement symétrique? Expliquer ?
2) Citer les deux problèmes principaux que le chiffrement hybride permet de résoudre. Expliquer ?
3) Expliquer pourquoi il est utile, dans un système à chiffrement hybride, de changer la clé d'encryptage des données à chaque session?
4) Comparer les systèmes de chiffrement symétriques et asymétrique de point de vue problématique de gestions de clés (nombre et sécurité des clés, problématique de mise en place des clés…etc) ?
5) Comparer l'authentification par adresse IP à celle par signature de point de vue robustesse. Expliquer ?
6) Quel problème peut surgir si la clé privée du PKI est compromise?

7) Un certificat numérique, signé par une autorité de certification de confiance (AC), permet de garantir l'appartenance d'une clé publique à une entité. Dans certains cas, les certificats sont fournis d'une manière personnelle dans le sens qu'un nœud peut certifier les nœuds qu'il connait. L'authentification se fait en trouvant une chaine de certificat entre la source et la destination (A connait B, B connait C ➔ donc A fera confiance à C). Donner deux inconvénients de ce système ?

Exercice 3 [3pts]:

1) Soit le bout de code BC1 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Donner deux conséquences possibles.

BC1 :

```
Void mycopy (char * input) {
char buffer[20];
strcpy(buffer,input);
}
int main(int argc, char * argv[]) {
    mycopy(argv[1]) ;
}
```

2) Soit le bout de code BC2 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Comment peut-on améliorer ce code pour le rendre sécurisé?

BC2 :

```
$login = Request.Form("login")
$password = Request.Form("password")
SELECT * FROM users WHERE Login=$login AND Password=$password
```

Exercice 3 [4pts]:

Nous nous intéressons à l'évaluation du risque d'un site web d'une entreprise. Pour simplifier le travail, nous considérons une seule attaque qui ne peut être lancé que par des entités (utilisateurs Internet) ayant des compétences réseaux et logiciels. Ces entités cherchent à nuire aux propriétaires du site web plutôt que d'avoir des récompenses. L'exécution de l'attaque ne nécessite aucun droit d'accès et aucune ressource. Bien qu'aucune information sur le point faible à exploiter par l'attaque ne soit disponible et que les propriétaires du site avaient mis en place des détecteurs d'intrusions incorporés dans l'application, il est facile de déterminer et d'exploiter ce point faible.

Comme conséquences de l'attaque en question, de nombreuses données critiques peuvent être divulguées ou corrompues. Cependant peu de services, jugés secondaires, seront interrompus et les propriétaires du site auront probablement une certaine traçabilité sur ce qui s'est passé. Sur le plan d'affaires, l'attaque peut causer des effets significatifs sur les bénéfices annuels et peut endommager la réputation de l'entreprise. De plus, une violation haute de la conformité des services du site ainsi qu'une atteinte aux vies privées de milliers de personnes seront observés.

Questions :

En se basant sur la méthode OWASP, déterminer la gravité du risque de l'attaque en question. Expliquer ?