Département Informatique

Nom :
Prénom :
Formation (rayer les inutiles) : 3A IT-S501/ISIC/TW3S

Année scolaire : 2004–2005
Date : 7 mars 2005

Module 3A IT-S501/ISIC/TW3S
Session de mars

—

Sécurité des systèmes informatique et des réseaux

—

Contrôle de connaissance[1] de 1h30

Merci de répondre (au moins) dans les blancs.
Lire tout le sujet en entier du début à la fin, en commençant à la première page et jusqu'à la dernière page, avant de commencer à répondre : cela peut vous donner de l'inspiration et vous permettre de mieux allouer votre temps en fonction de vos compétences.
Chaque question sera notée entre 0 et 10 et la note globale sera calculée par une fonction des notes élémentaires. La fonction définitive sera choisie après correction des copies.
Attention : tout ce que vous écrirez sur cette copie pourra être retenu contre vous, voire avoir une influence sur la note d'3A IT-S501/ISIC/TW3S.

1 Attaques

Question 1 : Donner des exemples d'attaques par détournement de connexions HTTP. Comment les éviter ?

→
→

[1] Avec document, avec calculatrice, sans triche, sans copie sur les voisins, sans micro-ordinateur portable ou non, sans macro-ordinateur, sans téléphone portable ou non, sans oreillette de téléphone ni de dictaphone, sans talkie-walkie, sans télépathie, sans métempsycose, sans pompe, avec anti-sèche, avec tatouage ou vêtement imprimé en rapport avec le sujet, avec mouchoir de poche pré-imprimé, avec piercing ou scarification en rapport avec l'3A IT-S501/ISIC/TW3S,...

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

Question 2 : Quelles sont les conséquences d'un système DNS piraté ? Comment éviter ?

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

Question 3 : On veut se connecter à une suite de machines avec `ssh` depuis la machine $\mathcal{A}$ en utilisant l'agent d'authentification `ssh-agent` pour éviter d'avoir à retaper sa phrase secrète protégeant sa clé secrète à chaque nouvelle connexion. Il suffit de rajouter une seule fois sa clé secrète avec la bonne phrase secrète dans le `ssh-agent` via la commande `ssh-add`.

On se connecte en `ssh` de la machine $\mathcal{A}$ à la machine $\mathcal{B}$, puis de la machine $\mathcal{B}$ à la machine $\mathcal{C}$. On utilise aussi le mode proxy de `ssh` de $\mathcal{A}$ vers $\mathcal{B}$ pour autoriser le `ssh-add` de $\mathcal{A}$ à répondre à $\mathcal{C}$ l'autorisation de connexion lors du `ssh` de $\mathcal{B}$ vers $\mathcal{C}$. On constate que c'est très pratique ! Un

seul `ssh-agent` et `ssh-add` plus le mode de proxy-authentification et on peut se connecter partout !

Mais si sa clé permet des connexions vers la machine $\mathcal{D}$ et que l'administrateur de la machine $\mathcal{B}$ est un méchant, pourra-t-il se connecter assez simplement à la machine $\mathcal{D}$? Si oui, comment ?

→
→
→
→
→
→
→
→
→

2 Architecture & système

Question 4 : Quel sont les avantages et inconvénient de la segmentation du réseau par type service (un réseau pour le courrier, un pour le serveur WWW,...) avec un parefeu par rapport à tout mettre sur une unique DMZ ?

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

Question 5 : Un programmeur système veut transformer un système d'exploitation monolithique en micronoyau avec une séparation claire entre le cœur du système d'exploitation (faire une action) et un serveur de sécurité qui gérera tout ce qui est lié à la sécurité (autoriser une action) afin de pouvoir vendre des systèmes adaptés aux politiques sécuritaires de ses clients. Donnez une idée des informations et messages qui devront transiter entre les 2 entités.

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

3 Questions ouvertes

Question 6 : Comparer les modèles de certification à la PGP/GPG et le modèle centralisé à la X.509 avec autorité de certification. Lequel est plus adapté au grand public et pourquoi ? Peut-on imaginer de mélanger sérieusement les 2 approches (accepter systématiquement quelque chose de signé par n'importe qui, qui a lui-même sa clé publique signée par une autorité de certification) ?

→
→
→

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

Question 7 : Si on replace la sécurité dans le modèle OSI du réseau en couche[2], quels sont les avantages et inconvénients de placer la sécurité plutôt à un endroit qu'à un autre ? Donner des exemples (réels ou futuristes, mais qui se tiennent) pour argumenter.

→
→
→
→
→
→
→
→
→
→
→
→

[2]Merci à un certain élève dans la salle qui se reconnaîtra pour avoir inspiré cette question ! ☺

→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→
→

ONE OF SEVERAL POSTERS FOR THE THIRD MATRIX MOVIE THAT DIDN'T QUITE MAKE THE CUT