Administration et Sécurité des Réseaux

Module M4212C
ASR8 : Infrastructures de sécurité et sécurité de fonctionnement

Sommaire

Bases de la sécurité

Introduction

La sécurité, tout le monde s'en fout mais c'est super important

Quelques recommandations élémentaires :

- mots de passe forts et différents,
- SE et logiciels politiques,
- sauvegardes régulières des données,
- désactivation des logiciels les plus faillibles,
- vigilance concernant les liens (phishing, …),
- vérifier l'authenticité de l'émetteur d'un mail.

Les pré-requis pour une bonne sécurité informatique sont :

- être infaillible,
- être sur tous les fronts (ubiquitaire), à jour, actualiser ses logiciels, SE, surveiller, … (= veille),
- avoir une connaissance complète,
- ne jamais plier, avoir une énergie infinie.

Bien sûr, ces quatre points sont impossibles à atteindre. Ils constituent donc la difficulté de la sécurité.

Concepts de base

Il faut garder en tête que l'attaquant gagnera toujours alors autant s'y préparer.

Il faut rester humble.

La sécurité commence en dehors de l'informatique (contrôle des accès par ex), et on forme les personnes aux bonnes pratiques.

Il faut prévoir des plans de recouvrement, si l'attaquant arrive à ses fins : revenir en arrière, prévenir les bonnes personnes, estimer l'étendu des dégâts, comment couvrir les pertes, etc.

Domaines de la sécurité

La stratégie consiste à évaluer les risques et à identifier les solutions. On identifie dans un premier temps les biens, les sources de menaces, la vulnérabilité, les risques (leur dangerosité), les solutions (leur priorité). C'est donc un audit. Ensuite, on établit une politique de sécurité, on s'organise, on forme et on anticipe la gestion des incidents.

La tactique concerne les moyens mis en œuvre dans le cadre de la défense. Il faut veiller à la certification des logiciels et matériels ainsi qu'aux utilisateurs. Le contrôle d'accès de ces derniers passe par : identification, authentification, autorisation. On emploie également des protections dites

techniques au sein d'un réseau, d'un SE ou d'un logiciel telle que la cryptographie.

Quelques définitions

Principes de base concernant toute information :

- confidentialité : pas d'accès aux personnes non autorisées,
- intégrité : pas de modification,
- disponibilité : toujours accessible.

Mécanismes associés : AAA(A) ou Authentication, Authorisation and Accounting (and Auditing) :

- authentification : vérification d'identité,
- autorisation : politique d'accès,
- traçabilité : qui a fait quoi et quand (logs),
- auditabilité : étude après coup.

Les attaquants sont principalement internes mais peuvent aussi être externes.
Les attaques ont pour but :

- écoute sur le réseau,
- contournement des mécanismes d'authentification et d'autorisations,
- déni de service (DoS/DdoS).

Composants fondamentaux d'une architecture sécurisée

Principe

Il est préférable d'utiliser des switches même en terme de sécurité. Ces derniers, contrairement aux hubs, ne diffusent pas les messages dans tous les ports (sauf MAC non connue). On utilisera également la fonction *port security* et on veillera à ce que les locaux où se trouvent les équipements réseau sont verrouillés et sécurisés.

Les VLANs sont une première sécurité : niveau 1 (ports), niveau 2 (adresse MAC) ou niveau 3 (adresse IP). Cela revient à créer différents LANs physiquement séparés.

Le firewall (pare-feu) permet d'affiner la politique de sécurité. On peut filtrer en fonction du protocole couche 4 (UDP/TCP/ICMP), des ports et adresses IP et du sens entrant ou sortant. Les différents types de firewall étant :

- stateless : examen de chaque paquet indépendamment, à un instant t,
- statefull : prend en compte les paquets précédents (ex connexion établie),
- applicatif : vérifie le protocole, en particulier avec un port imprévisible,
- personnel : statefull + ACL.

Cependant, ils sont basés sur l'adresse IP, ce qui requiert un lien machine-utilisateur qui n'est pourtant pas systématique. Lors de l'utilisation d'un tunnel SSH par exemple, le filtrage sur le protocole n'aura certainement pas l'effet escompté.

On peut utiliser des relais applicatifs (proxy) pour garantir l'authentification des utilisateurs et permettre la mise en place de logs (= Authentification, Autorisation, Traçabilité).

Cependant, il est facile de l'attaquer de par sa complexité élevée. Il faut réduire les services au strict minimum.

Architectures

Screening router : routeur avec firewall applicatif ou ACL

Bastion relais : n'effectue pas de routage, proxys entrants et sortants pour chaque service

Screening router + bastion : protection du bastion par le routeur firewall

DMZ : devient screening router si le bastion tombe (sauf fusion bastion et routeur interne!), les serveurs se trouvent dans le réseau du bastion

Voir poly de cours pour les illustrations

Sécurisation des protocoles

Quelques protocoles non sécurisés

Les protocoles en r : rlogin, rsh, rcp, …

La relation de confiance est basée sur l'authentification d'un utilisateur sur l'hôte, indiquée dans les fichiers */etc/rhosts* et *~/.rhosts*

D'autres protocoles où les flux sont en clair comme TFTP, FTP, NFS, X, telnet, …

Le protocole NFS utilisait (avant NFSv4) l'adresse IP pour authentifier l'utilisateur !! Il faut maintenant un serveur d'authentification Kerberos. Il en est de même pour le protocole X (qui utilise maintenant des cookies d'authentification).

Sécurisation

Sécurisation des protocoles (SSH)

Bases

Redirections SSH