Attaques et Vulnérabilités

Cours 06

Ahmed Amou El Arby

Attaques/ Vulnérabilités

- Attaque != Vulnérabilité
- Attaque
  - Action de malveillance consistant à tenter de contourner les fonctions de sécurité d'un SI (ISO)
- Vulnérabilité
  - Faiblesse ou faille dans les procédures de sécurité, les contrôles administratifs, les contrôles internes d'un système, qui pourrait être exploitée pour obtenir un accès non autorisé au SI, à un de ses services, à des informations ou à la connaissance de leur existence et de permettre de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité du SI et de ses informations

Vulnérabilités

- Dans la conception
  - Matériel
  - Protocole
  - Architecture (Système, Réseau, …)
  - Logiciel (OS, application, …)
- Dans l'implémentation
  - Matériel
  - Protocole
  - Architecture (Système, réseau …)
  - Logiciel (OS, application, …)
- Configuration, exploitation
  - Équipement (Routeurs, Firewalls, Serveur, …)
  - Logiciel (OS, application, …)

Attaques

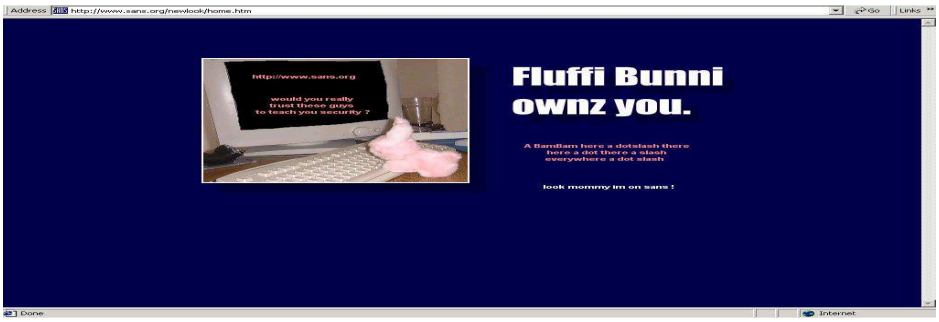
- Intrusions
- Vandalisme
- Denis de service (DOS)
- Vol d'informations
- Escroqueries
- Logiciels/Virus

Attaques (1)

- Intrusions
  - Recherche de mots de passe
    - Écoute du réseau
  - Le « Spoofing » : Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.
  - Les sniffers et scanners : Écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée. Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe. Vise surtout à intercepter les données non chiffrées.

Attaques (2)

- Vandalisme
  - Destruction de fichiers
  - Destruction de systèmes
  - Défiguration de site Web



Attaques (3)

- Denis de service (DOS) : Une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à de fausses requêtes de connexion.

- Denis de service distribué (DDOS)
  - Amplification des DOS

Attaques (4)

- Vol d'information
  - Suite à une intrusion
  - Interception
  - Écoute
  - Cryptanalyse

Les principales escroqueries

- L'ingénierie sociale.
  - Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct
    - Exemple : Le message vocal du Président de Hewlett-Packard à son Directeur administratif et financier, où il évoquait la fusion avec Compaq a été intercepté et diffusé à travers l'Internet. » - Avril 2002 -

Les principales escroqueries

- Le scam.
  - Pratique frauduleuse consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage.

Les principales escroqueries (3)

- Le phising.
  - Contraction des mots anglais «fishing», en français pêche, et «phreaking»
    - Technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.
    - Technique d'«ingénierie sociale» c'est-à-dire consistant à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance.

Les virus

- Programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé
- Différents types.
  - Les vers
  - Les trojans
  - Les bombes logiques
  - Les spywares

Les virus (2)

- Les vers.
  - Programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique pour se propager
  - Les vers actuels se propagent principalement grâce à la messagerie grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-même à tous ces destinataires.

Les virus (3)

- Les chevaux de Troie.
  - Programme (en anglais trojan horse) caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (en anglais backdoor)
    - Vol de mots de passe
    - Copie de données
    - Exécution d'action nuisible

Les virus (4)

- Les bombes.
  - Dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système
  - Généralement utilisées dans le but de créer un déni de service
    - Exemple la bombe logique

Les virus (5)

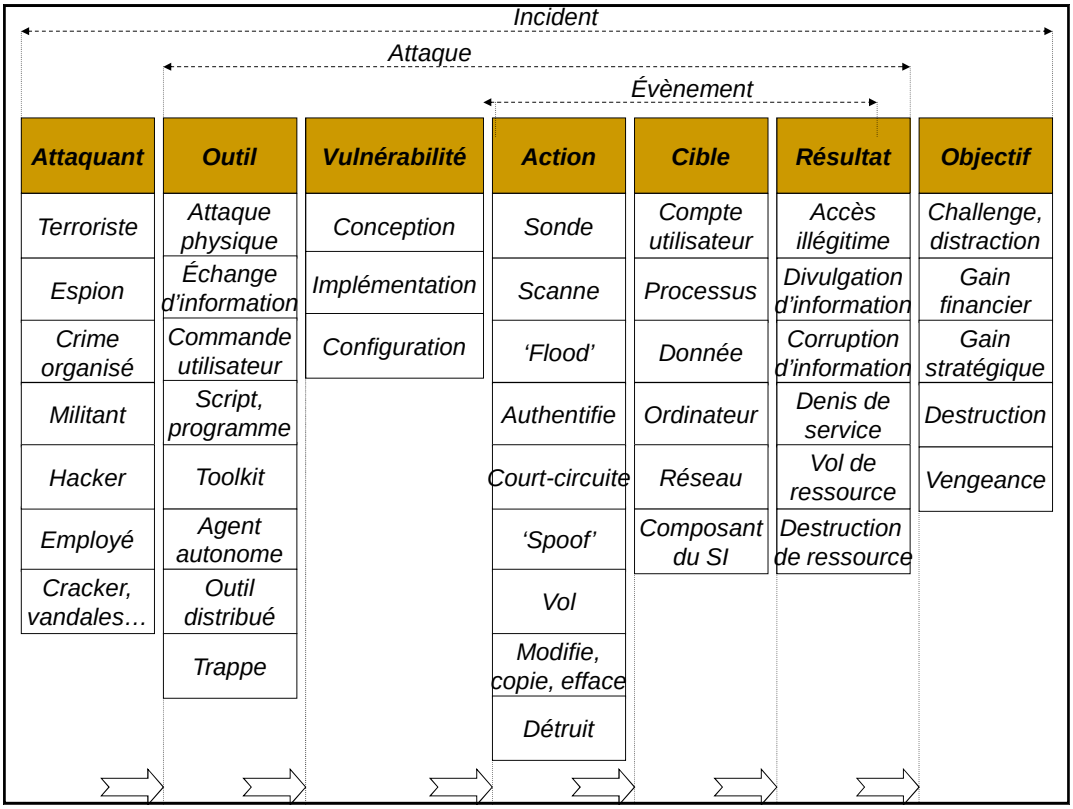
- Les spyware ou espiogiciels.
  - Programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois mouchard) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (profiling).
  - Keyloggers : Dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.

Autres Attaques

- Attaque par rebond («bounce attack») : Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.
- Attaque de l'homme du milieu : Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaquer.
- Trébuchage sans fil («war-driving») : Dans le cas des réseaux sans fil. Consiste à circuler dans la ville avec un portable ou un assistant numérique personnel («PDA») pour repérer et pénétrer les réseaux locaux non protégés.

Taxinomie d'un incident

- Taxinomie (ou Taxonomie)
  - Classification d'éléments selon des taxons
- Taxon (biologie)
  - Unité formelle représentée par un groupe d'organismes, à chaque niveau de la classification.


Incident
Attaque
Évènement
Attaquant
Outil
Vulnérabilité
Action
Cible
Résultat
Objectif
Terroriste
Espion
Crime organisé
Militant
Hacker
Employé
Cracker, vandales…
Attaque physique
Échange d'information
Commande utilisateur
Script, programme
Toolkit
Agent autonome
Outil distribué
Trappe
Conception
Implémentation
Configuration
Sonde
Scanne
'Flood'
Authentifie
Court-circuite
'Spoof'
Vol
Modifie, copie, efface
Détruit
Compte utilisateur
Processus
Donnée
Ordinateur
Réseau
Composant du SI
Accès illégitime
Divulgation d'information
Corruption d'information
Denis de service
Vol de ressource
Destruction de ressource
Challenge, distraction
Gain financier
Gain stratégique
Destruction
Vengeance

Prévention

Disposer d'une sauvegarde de ses données.

Faire un audit des accès inutilement ouverts.

Applications des methodes de securitees

Anti-Virus à jour

Les comptes d'administration ont des mots de passe sécurisés.

Suppression des comptes utilisateurs non utilisés.

Désactiver les services (p. ex. internet) non utilisés sur les machines et supprimer les partages de fichiers qui ne sont pas nécessaires.

Prévention

Mettre à jour les logiciels à l'aide des dernières rustines («patches») de sécurité officielles pour fermer les brèches.

Installer un coupe-feu.

Structurer les réseaux en zones étanches par activité et sensibilité (VLAN). Instituer un système de mots de passe. Isoler les serveurs Internet. VLAN : Virtual Local Area Network, regroupe les machines de façon logique et non physique.

S'abonner aux lettres d'information («newsletters») de sécurité des différents fournisseurs.

Coupe-feu

Un coupe-feu permet de couper l'accès à un réseau local. C'est le seul point d'accès à un réseau local à partir de l'extérieur.

Les techniques que nous avons vues jusqu'à maintenant ne permettent pas d'éviter de communiquer avec des adversaires.

> Même si nous insistons pour faire un échange de clé authentifié avec quelqu'un, une certaine quantité d'information échangée avec des adversaires potentiels ne peut être évitée.
>
> Ceci pourrait permettre à l'adversaire de pirater un ordinateur en utilisant une attaque par débordement de tampon.

Le concept du coupe-feu : L'adversaire ne peut attaquer un ordinateur avec lequel il ne communique pas!