Introduction à la Sécurité des Systèmes et Réseaux

- Politique de sécurité
- Risques et menaces
- Contaminations diverses
- Les bons réflexes de l'utilisateur
- Bilan

La sécurité ..... pourquoi ?

- Les ordinateurs personnels sont de plus en plus puissants, complexes et connectés

  → vulnérabilité accrue

- Le nombre de failles des systèmes d'exploitation et des réseaux ne pourront qu'augmenter

  → nouveaux problèmes en permanence

- La sécurité devient par force l'affaire de tous :
  - Utilisateurs
  - Administrateurs de systèmes et de réseaux

Se protéger ?

- La protection absolue n'existe pas... si ce n'est…
- Définir une politique de sécurité : mettre en place des moyens en adéquation avec les risques encourus
- A éviter
  - **Sous-estimer** les risques et mettre en place des procédures insuffisantes
  - **Sur-estimer** les menaces, et rendre l'utilisation inutilement très contraignante

→ Quels risques et quelles menaces ?

Evaluer

- L ’existant
- Les risques et menaces
- Les vulnérabilités
- Les conséquences

- **Définir les besoins**
  - Protéger Quoi ?
  - Pourquoi ?
  - Contre quoi ?
  - Contre qui ?
  - A quel coût ?

Se protéger ……. De qui ?

- Voisins , utilisateurs du réseau local, soi-même
  - Maladresse ou malveillance
- Les concurrents de l'entreprise
  - espionnage industriel
- Les agences gouvernementales *NSA, CIA,*
  - Surveillance de cibles essentiellement économiques et technologiques
- Les « pirates »
  - amateurs avertis ou professionnels malintentionnés
  - Motivations
    - Gain financier, Malveillance, Vengeance, destruction, vol de données (*Cracker*)
    - Curiosité , partage de découvertes et jeu, par compétition entre pirates, ou pour disposer de ressources matérielles : zones de stockages (*Hacker*)

Que faut-il garantir ?

- **Identification** qui est-ce ?
- **Authentification** l'identité n'a-t-elle pas été usurpée ?
- **Confidentialité** un tiers a-t-il eu accès à l'information ?
- **Intégrité** l'information a-t-elle été altérée ?
- **Disponibilité** les ressources sont-elles toujours accessible
- **Non-répudiation** ne pas pouvoir nier être à l'origine d'une opération

Défendre quoi ?

- Utilisateurs
  - Perte des données, vols d'équipements
- Équipements réseaux
  - Plantage des équipements, détournement, intrusion
- Protocoles réseaux
  - Observation du réseau, déni de service
- Systèmes et services
  - Erreurs d'administration, de programmation, de configuration
- Communications
  - Intégrité et Confidentialité des échanges

Les difficultés

- Domaine complexe en pleine évolution, course entre ingénieurs et *pirates* (qui ont toujours une longueur d'avance)
- Solides compétences théoriques et pratiques
  - Bonnes connaissances en administration des systèmes d'exploitation
  - Expérience des réseaux TCP/IP
  - Connaissance Cryptographie, programmation, architectures de développement
- Investissement important sans valeur ajoutée en environnement industriel
- Formation insuffisante du public

Risques et Menaces

Gravité des risques

- Déni de service
  - plus de disponibilité des ressources
- Accès en lecture, vol d'informations
  - plus de confidentialité (données, communications)
- Accès en écriture
  - plus d'intégrité (données, communications)
- Exécution de code résident ou commande
  - plus d'authentification
- Exécution de code spécifique
  - plus rien ☹

Compromission

- faille de sécurité + une attaque
- Les phases d'une attaque
  - Recherche d'un cible vulnérable
    - Par des recherches (*scans)* à grande échelle
    - S'installer sur le système compromis
  - Puis, pour une cible donnée :
    - identification des composants du système cible
    - recherche de vulnérabilité sur ces composants
    - mise en œuvre d 'une attaque adaptée
    - recherche d'autres cibles

Origines des failles

- Mauvaise **conception**
  - d'un protocole
  - d'une architecture
- Mauvaise **implémentation**
  - Validation des paramètres d'entrée
  - Débordement de pile (buffer overflow)
  - Bugs logiciels
  - Mauvaise gestion des erreurs
- Mauvaise **configuration**
  - d'un ou plusieurs composants du SI

Mauvaise implémentation

- Provoquer le débordement d 'une zone mémoire (buffer overflow) en envoyant des données pour écraser les données du programme.
- Ces données contiennent un programme en langage machine appelé **shellcode**, qui prend la main.
- Cette technique est utilisable à tous les coups lorsque le programme ne contrôle pas la longueur des données en entrée.

Le buffer overflow

- On parle de **local exploit** lorsque cette technique permet de gagner des privilèges sur une machine
- On parle de **remote exploit** lorsque cette technique permet de prendre le contrôle d ’un système à distance.
- Les serveurs classiques httpd, ftpd, bind, sendmail, nfs, etc… sont souvent la cible de ce type d ’attaque.

Erreur de configuration

- Exécution d ’activeX sur les navigateurs
- Mot de passe par défaut
- Relais ouvert sur un serveur SMTP
- Rebond sur un proxy HTTP
- Erreurs d’administration
  - Laisser des failles connues du SE ou d’une application
  - Ignorance de services actifs menaçant la sécurité

Composants concernés

- **Equipements** routeur, firewall, proxy, commutateurs, etc …
- **Clients** http, mail, news, ftp, telnet etc …
- **Serveurs** apache,IIS,oracle, ftpd, etc…
- **Systèmes** Ces composants sont implémentés sur un SE qui peut comporter des vulnérabilités

Les attaques liées aux réseaux

- Intrusion dans les systèmes
  - Vol d'informations
  - Compromission d'informations
  - Destruction d'informations
- Interception des communications
  - Passifs
    - sans modification de l'état des messages par prélèvement d'information
  - Actifs
    - par modification des messages émis légalement avec ajout de messages ou rejeu d'un message déjà transmis

Le déni de service

- Inonder un site ou service d'une multitude de requêtes ou de messages afin de consommer toutes ses ressources
  - Consommation de bande passante
  - Saturation de ressources
    - écrouler un site web par l'envoi de milliers de requêtes simultanées
    - Envoi massif de mels, pour inonder les boîtes aux lettres (spam)
  - Panne du système et des applications
    - Envoi de messages erronés : attaques TCP/IP

Usurpation et Falsification *(spoofing)*

- Identité d'un utilisateur
- Adresse IP source de paquets ➔ adresse usurpée
- L'émetteur des paquets, se faisant passer pour un autre, en profite pour :
  - Falsifier la source d'une attaque
  - Obtenir des privilèges sur une machine en profitant de la relation de confiance existant avec cette fausse adresse
  - Spoofing d 'adresse MAC, de nom DNS (cache poisoning), de mail, certificat , vol de session TCP

Le phishing

- Exploitation d'une faille humaine : à partir d'un mail avec usurpation de l'émetteur (partenaire de confiance)
- Un lien dans le message redirige vers une copie (page absolument conforme à l'original) du site du partenaire
- L'utilisateur risque ensuite de saisir des informations confidentielles (codes d'accès, numéros de comptes, de CB,…)

La Prévention contre les FAUX

- Les canulars ou fausses nouvelles ("myths, hoaxes, urban legends") se présentent faussement comme un avis de sécurité.
- Ils ont un double objectif de créer la confusion et de propager la désinformation en matière de sécurité
- Il est impératif de vérifier qu'une alerte virus est un canular en consultant les sites suivants :
  - http://www.hoaxbuster.com (site français souvent cité en référence)
  - http://www.symantec.com/avcenter/hoax.html (Liste symantec)

Informations : CERTA

- **C**entre d'**E**xpertise gouvernemental de **R**éponse et de **T**raitement des **A**ttaques informatiques
- Tiré de l 'acronyme CERT : Computer Emergency Response Team
- 2 principaux objectifs :
  - assurer la détection des vulnérabilités et la résolution d'incidents
  - prémunir contre de futurs incidents
- http://www.certa.ssi.gouv.fr

Contaminations diverses

Les virus

- Un virus est une partie de programme qui, à l'insu de l'utilisateur, exerce une action nuisible à son environnement
- Son action peut être permanente, sporadique, périodique, être déclenchée par l'utilisateur à son insu, ou n'avoir lieu qu'à une date précise ou selon la conjonction d'événements extérieurs.
- Pour être plus difficile à neutraliser, le virus peut être *polymorphe* et subir des mutations, ou *furtif* pour devenir indétectable

Virus et infection

- Un virus infecte des fichiers : portion de code qui s'attache aux programmes
- Il s'exécute dans un programme infecté à l'insu de l'utilisateur → action néfaste + reproduction
  - Il peut s'attaquer aux données des utilisateurs, créer des dysfonctionnements inoffensifs, manifestations visuelles
  - Il peut s'attaquer aux fonctions vitales du système: neutralisation des ressources du système
  - Il peut s'attaquer au réseau par inondation
- Reproduction : par la messagerie, macros, scripts

Ver et propagation

Un ver est un programme qui possède la faculté de s'auto-reproduire et de se déplacer au travers d'un réseau. Il se déplace de manière autonome en exploitant des mécanismes système ou réseau. Il s'exécute de manière transparente.

- Lors d'une première exécution, il s'installe dans le système d'exploitation, ce qui lui garantit une présente permanente
- Ensuite, en local il infecte tour à tour les programmes sains exécutés en sa présence

Ver et propagation

- Par le réseau, un ver migre de système en système en utilisant :
  - les failles des services réseau
  - des accès ouvert dans ce but
  - tout simplement le courrier électronique (à l'insu de l'utilisateur, un courrier peut être envoyé à chaque personne figurant dans le carnet d'adresses)
- Un grand nombre de vers contiennent des virus qui peuvent altérer les données ou rendre les systèmes inutilisables en consommant toutes les ressources

Bombe logique

- Programme ou altération de programme capable de réaliser une action néfaste avec un déclenchement différé ou téléguidé
- Attaque la plus répandue dans les entreprises
  - un programmeur, suite à un licenciement, insère dans un programme une fonction insidieuse dont l'exécution sera déclenchée lorsque son nom disparaîtra du fichier du personnel
  - un administrateur système peut modifier des utilitaires (tels que *login*) de manière à garder la possibilité de se connecter sur le système suite à un départ.

Cheval de Troie

- Un cheval de Troie se présente généralement sous la forme d'un programme inoffensif à caractère utilitaire ou d'un jeu.
- Ce programme comporte, en plus des fonctions déclarées, une partie insidieuse (mécanisme caché qui s'exécute de façon illicite)
- L'utilisateur peu méfiant n'hésite pas à l'installer, et les mécanismes sont déclenchés par l'utilisateur lui-même à son insu : le plus souvent pour ouvrir une porte dérobée (back-door) sur le système concerné

Les virus trans-applicatifs

- Macros
  - Les divers langages de macros ont ouvert la porte à des virus trans-applicatifs appelés macro-virus
  - Un macro-virus sous Microsoft Office peut se propager aisément lorsqu'il utilise les procédures d'exécution automatiques et peut intégrer l'environnement global en mettant à jour les fichiers modèles (normal.dot par ex.)
- Cookies
  - Information stockée par un navigateur pour un serveur, qui peut ainsi « se souvenir » de l'utilisateur, de son mot de passe,…
  - Une entreprise ou annonceur peut suivre les mouvements de l'utilisateur entre différents sites …

Les virus trans-applicatifs

- Contenu dynamique des pages web
  - La plupart des navigateurs interprètent les langages de script contenus dans des pages html envoyés par des serveurs WWW
    - Java / ActiveX ; JavaScript / JScript (*Dynamic HTML*)
    - Scripts CGI (Common Gateway Interface)
    - ASP (Active Server Pages)
    - PHP (Personal Home Pages)
- Une machine virtuelle exécute sur la machine locale, les codes java émis par un serveur

  → problème de sécurité si l'origine ne peut être garantie

Les virus la solution

Il existe une catégorie d'anti-virus qui opèrent sur une collection de signatures.

- Les virus les plus simples comportent tous, en effet, une suite d'instructions caractéristique, propre à chacun, mais parfaitement identifiable et qu'on appelle leur signature.
- On peut en établir un catalogue incrémental au fur et à mesure qu'apparaîtront de nouveaux virus (définitions virales ou fichier de signatures).
- Ils ne donnent que très peu de fausses alarmes, mais ils sont naturellement inefficaces pour les virus polymorphes puisque ceux-ci ont la faculté de modifier leur apparence.

Les virus la solution

- L'inconvénient de la méthode précédente est la nécessité de remise à jour périodique du catalogue, chaque nouveau virus nécessitant une mise à jour : c'est la course incessante entre fauteurs de virus et éditeurs de logiciels
- Une autre méthode existe, qui a l'avantage de ne pas nécessiter de mise à jour. Elle se base sur des algorithmes heuristiques pour soupçonner dans certaines successions d'instructions la possibilité d'un virus. La probabilité de fausses alarmes est plus forte mais l'efficacité est permanente. Tout au moins jusqu'à l'apparition d'une nouvelle forme générale d'attaques.

Les virus la solution

1. Installer un anti-virus avec mise à jour automatique des signatures
2. Activer la protection « temps-réel » qui vérifie tous les documents externes
3. Programmer une analyse complète hebdomadaire
4. Lancer une analyse complète en cas de doute
5. Sauvegarder vos données après analyse
6. Protection du BIOS et boot
7. Faire une image du système et applications après analyse complète

http://www.symantec.fr

http://www.f-secure.com/

Les bons réflexes

Charte des Utilisateurs

- Sensibilisation des utilisateurs.
- Code de bonne conduite associé au règlement intérieur.
- A faire signer à chaque utilisateur
- Points forts :
  - Responsabiliser l'utilisateur dans l'usage des ressources informatiques mises à sa disposition
  - Contribuer à la sécurité générale (mot de passe, signaler les tentatives de violation, fermer sa session)
  - Respecter les données des autres utilisateurs (confidentialité et ne pas introduire de perturbations physiques ou logicielles, comme les virus)
  - Respecter la législation concernant les logiciels

Authentification

- Plusieurs niveaux d'authentification
  - *Ce que je connais* → mot de passe
    - faible
  - *Ce que je possède* → token, carte à puce, challenge
    - fort
  - *Ce que je suis* → biométrie
    - cher

Les mots de passe

La saisie de mot de passe est le moyen le plus répandu pour prouver qu'on est bien celui que l'on prétend (authentification faible)

- **Mais ce moyen n'est pas sûr**
- Le mot de passe peut être volé, deviné, recalculé par programme
- De nombreux utilisateurs sont trop laxistes dans la gestion de leur mot de passe : choix trivial, mot de passe inchangé durant des années, circule en clair

Le mot de passe
le risque

- L'usurpation d'identité
- Une personne ayant connaissance de votre mot de passe peut se faire passer pour vous :
  - Accéder à toutes vos données et ressources
  - Bénéficier de votre droits
  - Agir en votre nom
- Chaque personne est responsable de son mot de passe et doit assumer tous les faits réalisés sous son identité

Le mot de passe

la solution

- Le choix du mot de passe est primordial, il doit respecter les règles suivantes :
  - Pas de mot du langage courant
  - Pas de nom propre proche (prénom, nom d'animal, …)
  - Doit être supérieur à 6 caractères et contenir des caractères spéciaux (chiffres, ponctuation, …)
- Il ne doit pas trop simple, pour ne pas être *deviné* par quelqu'un ou *trouvé* par un programme utilisant un dictionnaire ou recherchant toutes les combinaisons

→ **recherche par force brute**

Le mot de passe

la solution

- Le changement
  - Il doit être changé régulièrement
  - Les mots de passe que vous utilisez doivent être différents pour chaque application ou service
- La confidentialité
  - Il ne doit être noté nulle part ni être tapé à la vue d'une autre personne
  - Il ne doit être divulgué à personne, car il permet de vous identifier et vous avez la responsabilité de son usage
  - Si il est émis dans le réseau, il ne doit pas circuler « en clair »
- **Ne plus utiliser de mot de passe !**

Authentification forte

- L'authentification par « mot de passe » avec toutes les précautions reste faible
  - Les claviers ont des oreilles…
- Mécanismes plus forts
  - **Challenge** : contrôle de la connaissance du secret sans l'échanger (il reste stocké sur une machine)
  - **Token** , **carte à puce** : augmente la sécurité du stockage du secret (toujours en possession de l'utilisateur)
  - **Biométrie** : reconnaissance d'une caractéristique physique

Challenge

- A veut s'authentifier auprès de B
- A et B partagent un secret K
- A contacte B : « Je suis A »
- B tire aléatoirement R, calcule C avec R et K C=f(R,K)
- B transmet R à A « si tu es A, alors calcule C »
- A calcule C', C'=f(R,K) et renvoie C' en réponse
- B vérifie si C==C', A est authentifié

Token

- A veut s'authentifier auprès de B
- A possède un token, à code secret T, connu de B
- A entre son code PIN sur le token qui génère un mot de passe P=f(T, heure courante)
- A contacte B : « Je suis A », mon code est P
- B vérifie P == P'=f(T,heure courante)
- Le code P change à chaque connexion
- Sa durée de validité est limitée à quelques dizaines de secondes
- Si le token est perdu, il faut connaître le code PIN, et il peut être bloqué en B

Les données

le risque

- L'accès illicite à vos données personnelles est parfois aggravé par un action malveillante
  - Modification des informations
  - Destruction totale ou partielle de données
  - Action qui est souvent irréversible, sauf cas exceptionnel
- Destruction accidentelle (incendie, catasptrophe)

Les données

la solution

Pour protéger des **données très sensibles**, il faut empêcher physiquement l'accès aux données

- Fermer les locaux à clé
- Verrou pour attacher physiquement la machine à un meuble ou bureau (vital pour un ordinateur portable)
- Fermer les sessions avant de s'absenter
- Économiseur d'écran avec mot de passe
- Mettre des protections physiques :
  - une porte avec un code d 'entrée
  - des cartes d'identification
  - des caméras de surveillance
  - Des capteurs de vibration …

Les données

la solution

- La **sauvegarde des données** est le SEUL moyen sûr de lutter contre la perte des données
  - Utiliser l'outil de sauvegarde du système d'exploitation qui archive les données sur un support amovible (disquette, disque, bande, cartouche, Streamer, CD, …..
    - sauvegarde complète périodique de répertoires ou partitions
    - sauvegarde incrémentale (uniquement les fichiers modifiés)
  - Copier les données sur un autre disque
  - Graver un CD
- Le support de sauvegarde des données ne doit en aucun cas se trouver « proche » des données (éviter vol des données + sauvegarde ou incendie)

Trous de sécurité
le risque

- De nombreuses intrusions profitent d'erreurs de programmation (trous de sécurité) des systèmes d'exploitation et logiciels largement utilisés par le grand public
  - Un trou de sécurité dans un système d'exploitation est gravissime car il concerne un très grand nombre d'utilisateurs (plusieurs millions pour les SE Microsoft)
  - La multitude de cibles potentielles est un appât pour les *pirates*

Trous de sécurité

la solution

- Arrêt des services inutilisés
- Les mises à jour et Service Pack
  - Dès la connaissance des trous de sécurité, les éditeurs de logiciels corrigent les logiciels et diffusent les mises à jour
  - A charge à l'utilisateur de vérifier le niveau de mise à jour de ses versions logicielles, consulter impérativement pour les systèmes *Windows Update et Office Update*

    → Microsoft Update

    http://update.microsoft.com

En résumé…

- **La sécurité par l'Utilisateur**
  - Sensibilisation et formation des utilisateurs
  - Politique des mots de passe
  - Mises à jour, correctifs et patchs
  - Anti-virus
  - Sauvegarde
- **La sécurité de l'administrateur** (A venir)
  - Authentification forte, PKI
  - Pare-feu, Filtrage applicatif, proxy
  - Contrôle de contenu, services sécurisés
  - Détection d'intrusion IDS, Outils d 'analyse
  - Contrôle d 'intégrité : utilisateurs, fichiers
  - Chiffrement : VPN, IPSec