Sécurité informatique

Concepts fondamentaux de la sécurité

- Menace: En anglais « threat» représente le type d'action susceptible de nuire dans l'absolu.
- Vulnérabilitéen anglais « vulnerability», appelée parfois faille ou brèche, représente le niveau d'exposition face à la menace dans un contexte particulier
- Contre-mesureest l'ensemble des actions mises en œuvre en prévention de la menace

RisqueRisque= (Menace x Vulnérabilité)/Contre-Mesure

Objectifs de la Sécurité

- Intégrité: Garantir queles données sont bien cellesque l'oncroit être

  Confidentialité: Garantir que seules les personnes autorisées aient accès aux ressources
- échangées
- Disponibilité: Maintenir le bon fonctionnement du système d'information et de l'information

  Non répudiation : Garantir qu'une transaction ne peut être niée
- Authentification: assurer que seules les personnes autorisées aient accès aux ressources

Principaux facteurs de motivation des pirates

- legoût du défi : certains pirates aiment prouver leur habileté et l'étenduede leurs connaissances ;
- l'appât du gain : certains sont appâtés par les rémunérations qu'offrent des entreprises peu scrupuleuses qui souhaitent saboter l'outil de travail informatique de leur concurrent et/ou lui dérober des informations confidentielles (devis, plans, secrets industriels…) ;
- la volonté de détourner à son profit des ressources informatiques dont on ne dispose pas (puissance de calcul, espace disque, connexion rapide au réseau…) ;
- la méconnaissance des conséquences et des risques encourus par des pirates aveuglément hostiles.

Bases de sécurité

- Les objectifs principauxde la sécurité informatique concernent :

  La sécurité de la connexion : il s'agit de contrôler que les utilisateurs qui se connectent sont bien autorisés à
- le faire et de leur interdire l'accès au système dans le cas contraire.
- L'intégrité des données : il s'agit de faire en sorte que les fichiers et les bases de données ne soient pas

  corrompus et de maintenir la cohérence entre les données.
- La confidentialité des données : l'accès aux données en consultation et en modification doit être limité aux

  seuls utilisateurs autorisés.

Moyens de sécurité

- L’authentification des utilisateurs par un mot de passe. Le cryptage des données. La sécurité physique en contrôlant
- l’accès des personnes aux salles informatiques, en utilisant des circuits inviolables
- matériellement. L’information sur les risques pénaux
- encourus en cas d’infraction. Un « braquage » informatique est un délit, pas un jeu. Le contrôle fréquent des droits d’accès aux fichiers et
- aux bases de données.

  Le contrôle des « checksum » des fichiers pour s’assurer de leur intégrité.
- La sauvegarde régulière des données.

Moyens de sécurité -suite

- L’auditdesprincipaux événementsdu système.
- L’installationdemurs de feu « firewall » qui contrôlent les accès au système informatique depuis l’extérieur et limitent l’accès à des services externes par des utilisateurs non avertis ou qui n’en ont pas besoin pour, par exemple, limiter le risque de rapatriement de virus.
- L’installation d’un antivirus, même sous Linux, si le serveur traite des données depuis et vers des systèmes d’exploitation concernés par les virus.
- L’installation d’outils antispams et antispywares, selon le même principe, afin d’éviter une intrusion et la saturation des serveurs de courrier électronique.
- Le démarrage uniquement des services réellement utiles sur le serveur et sur le client.

Secteurs de sécurité

- Sécurité globale: s'occupe de la sécurité des locaux, des documents papiers et du personnel dirigeant.
- La sécurité réseau: architecture, pare-feu, techniques anti-intrusions réseau
- Sécurité des serveurs
- Sécurité des applications
- Sécurité des postes de travail

attaques

- Exploit: est un programme quiexploite unefaille d'un logiciel ==> déni de ser vice

  Usurpation d'adresse IP (IP Spoofing): prendre l'identité d'un poste victime

- Session Hijacking: le pirate se substitue à un poste après sa phase d'authentification

  Replay: enregistrer les information d'authentification et les utiliser ultérieurement lors d'une autre session

- Homme au milieu (Man in the middle): se mettre entre le client et le serveur

  Dénie de service DoS: rendre inutilisable le système cible
  Phishing: consiste à acquérir de manière frauduleuse des informations

- sensibles (ex mot de passe)

  Pharming: consiste à rediriger le trafic d'un serveur vers un autre dont on a control

- Attaque des mots de passe: par dictionnaire ou exhaustive

Logiciels malveillants

- Virus: un morceau de codeinjecté dans unlogiciel

  Ver(worm) : c'est un logiciel qui s'auto réplique Cheval
- de Troie (trojan horse):c'est morceau de code introduit dans un autre logiciel qui effectue une
- action maligne Espion(spyware) c'est un logiciel qui
- s'installe dans
  le but est de récolter des informations
- Rootkit: un ensemble de commandes qui se substitue au commandes système.

Politiques de sécurité

- Identifierce qu'ilfautprotéger:quelsréseaux, ordinateurs et données.
  - Réseaux:privé, publique,démilitarisée …
  - ordinateurs: bastions (serveurs hyper protégés), poste sensibles, ordinateurs a accès libre
  - données: documents "très secret", secret, confidentiel, publique
- Analyse des risques: analyser l'existant et mettre en évidence les risques potentiels, on peut faire des tests d'intrusion

Politiques de sécurité

- Pondérer lesrisques: les risquesse ressemblent

  mais ils se diffèrent par leur taille, les conditions d'exploitation, leur métier.
- Evaluer les contraintes: l'existant (matériels,

  logiciels, personnels, locaux …), le budget et le

  temps.
- Choisir les moyens:

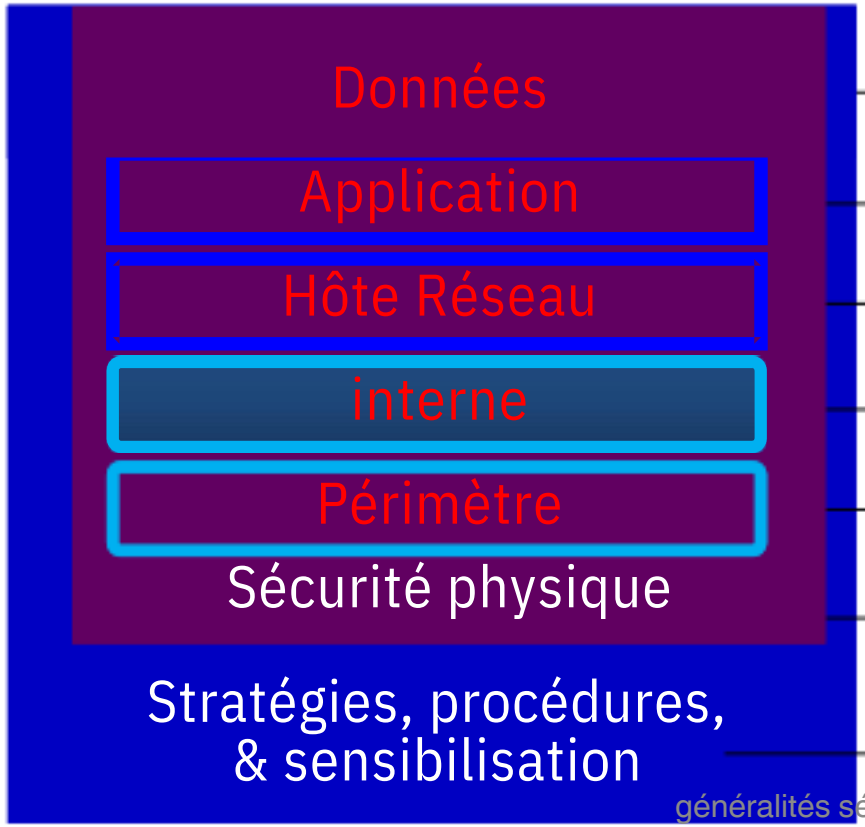
  les moyens de sécurisation. les
  moyens de détection d'intrusion.

Politiques de sécurité

- Adopterla politique de sécurité:la meilleure méthode, nommer le responsable de sécurité
- Tester: s'assurer que ces procédés répondent au cahier des charges. En réalisant des intrusions et démontrer la résistance.

Structure d'organisation pour la sécurité

- L'utilisation d'une approche en couches :
  - Augmente leschances dedétecter unintrus
  - Réduit les chances de succès d'un intrus



ACL, cryptage Renforcement de la sécurité des applications,logicielantivirus

Renforcement de lasécurité du système d'exploitation, gestion des mises à jour, authentification,HIDS

Segments réseau, IPSec, NIDS

Pare-feu, mise en quarantaine desVPN

Protections, verrous, dispositifsdesuivi

Éducationdes utilisateurs

Liste de contrôle de réponse à un incident

Identifier qu'une attaque se produit
Identifier l'attaque

Communiquer l'attaque
Contenir l'attaque

Implémenter des mesures préventives
Documenter l'attaque

Maîtrise des effets d'une attaque

- Arrêter les serveurs touchés
- Supprimer les ordinateurs touchés du réseau
- Bloquer le trafic réseau entrant et sortant
- Prendre des mesures préventives pour protéger
  - les ordinateurs qui ne sont pas encore infectés
- Conserver les preuves

En cas d'incident

- Evaluer l'importance del'incident etsa nature
- Construire un dossier d'analyse et diagnostiquer le problème
- Avertir le CERT(Computer Emergency Response Teamoucentresd'alerteetderéactionauxattaques informatiques), les autorités, la direction, les utilisateurs
- Réparer le système, reprendre l'activité
  Évaluer les dommages et les couts de l'incident
- Vérifier s'il n'est pas nécessaire de revoir la stratégie et les moyens de sécurité

Exemple CERT-FR

- Centre gouvernemental de veille,d'alerte et de réponse aux attaques informatiques

  Gestion du document
  http://www.cert.ssi.gouv.fr

-

Référence	CERTFR-2015-AVI-012
Titre	Vulnérabilité dans le service Telnet de Microsoft Windows
Date de la première version	14 janvier 2015
Date de la dernière version	-
Source(s)	Bulletin de sécurité Microsoft MS15-002 du 13 janvier 2015
Pièce(s) jointe(s)	Aucune

Méthodes conseillées de sécurité

Défense en profondeur (couches) Sécurité prévue à la conception Privilèges minimaux
Apprendre des erreurs passées
Conserver les niveaux de sécurité à jour Faire prendre conscience aux utilisateurs de la nécessité de la sécurité

Développer et tester des plans et procédures de réponse aux incidents

Méthodes pour limiter les risques

- Vous pouvez définir une valeurde umask restrictive (ex : 077) quitte à étendreensuiteles droits d'accès de certains fichiers.
- Il ne faut pas quitter son terminal sans se déconnecter ou le verrouiller.

  Il faut prêter attention aux dates de dernière connexion réussies et infructueuses qui sont
- affichées à chaque connexion.
- Ne jamais autoriser l'accès, même en lecture, au fichier .profile.

  Ne jamais mettre le . en première position du PATH, et contrôler ses chemins.

Politique de mot de passe

Les motsde passe sont à la base de l'authentification d'un utilisateur. Ils doivent être sûrs. C'est pourtant généralement une grosse lacune, tant au travail qu'à la maison, et même sur Internet :

- mot de passe présent sur un postit;
- emploi d'un gestionnaire de mot de passe automatique lui même sans mot de passe ;
- même mot de passe pour tous les sites Web et logiciels ;
- mot de passe jamais changé ;
- mot de passe et/ou compte communs à toute la famille/service ;
- mot de passe pas assez complexe ;
- etc.

Interdire les connexions

- Certains comptes nedoiventpas êtreinteractifs : les connexions depuis une console devraient leur être interdites.

  Shell: /bin/false ou /bin/nologin

- Ces comptes peuvent être dédiés à une application, à un service, à une connexion FTP, etc., mais la connexion devrait être refusée : pas de shell!
- le fichier /etc/securettycontient la liste des terminaux considérés comme sûrs.

  Pour le service donné, la connexion sera interdite si le terminal de la personne tentant de s'y connecter
- n'apparaît pas.

Rechercher des rootkits

- Une fois qu'un pirate quelconque aura réussi,

  via une faille ou un mot de passe trop simple, à pénétrer votre machine, il cherchera probablement à s'aménager une porte d'entrée plus importante (backdoor)
- L'idéal pour le pirate est de pouvoir s'accaparer

  les droits de root

  ==> devenir intégralement le maître de votre machine.

Exemple de pirate

```
$cat su #!/bin/bash echo -e "Mot
de passe :\c" read-s password
echo"$@ $password" > /tmp/fic
echo echo"su: Mot de passe
incorrect." /bin/su $@
```

$ chmod +x su $ export PATH=$HOME:$PATH $ su -

root

Mot de passe : ===> FAUX SU su: Mot de passe incorrect. ===> FAUX SU Mot de passe : ===> VRAI SU

$ cat /tmp/fic <== contient le vrai mot de passe

rootkit

- Le fait de placer des scripts, de modifier l'environnement, de remplacer un fichier par un autre de manière à obtenir un accès privilégié à une machine s'appelle installer un rootkit.

Se protéger : chkrootkit

- L’outil chkrootkit est un outil simple permettant de rechercher la présence des rootkitsles plus connus et les plus courants.
- Il est efficace seulement s’il est mis à jour régulièrement et lancé régulièrement.

Méthodes conseillées pour les mots de passe

Instruire les utilisateurs sur la bonne utilisation des mots de passe

Utiliser des expressions de mot de passe contenant des espaces, des chiffres et des caractères spéciaux et non de simples mots

Utiliserdes mots de passe différents pour des ressources différentes et protéger la liste de mots de passe

Configurerdes écransde veille protégés par mot de passe et Verrouiller les stations de travail avant de les laisser sans

sur veillance

Utiliser une authentification à plusieurs facteurs pour ajouter des niveaux de sécurité

Logiciel antivirus

- Conseils
  - Appliquez régulièrement les mises à jour de l'antivirus
  - Utilisez une stratégie de déploiement centralisée
  - Déployez sur les ordinateurs clients des logiciels qui leur sont adaptés

Pare-feu

- Pour Personnel ou individuel
- esclientsduréseaulocal,unpare-feulocal protège les ordinateurs du réseau contre les attaquesautomatisées internes. Les ordinateurs de
- bureau avec connexions (modem, ADSL …)Internet.
- Lesordinateursportablesavec connexionInternet à domicile, à l'hôtel ou sur un site de connexion WiFi

Collecte d’informations

fonctionnement des outils permettant de récupérer des informations à distance

Scanner

- L'objectif du pirate est de repérer les serveurs offrant des services particuliers et de les identifier.
- Lorsqu'un service est en écoute sur un port, on dit que le numéro de port associé à ce service est ouvert.
- L'intérêt du scanner est très simple : il permet de trouver dans un délai très court, tous les ports ouverts sur une machine distante.

Scanner : Nmap

- Exemples :
  - nmap <@ ip | nom_de_la_machine>
  - nmap -sT <@ip>
    pour scanner les services TC- sU pour UDP
  - nmap –o <@ip>

    pour déterminer le systèmed'exploitation

Vérifier les ports ouverts

- # netstat -a -A inet –p

Ou # netstat .atup

- nmap localhost

Désactivation des services inutiles

- Désactivation au redémarragedu système d'exploitation :

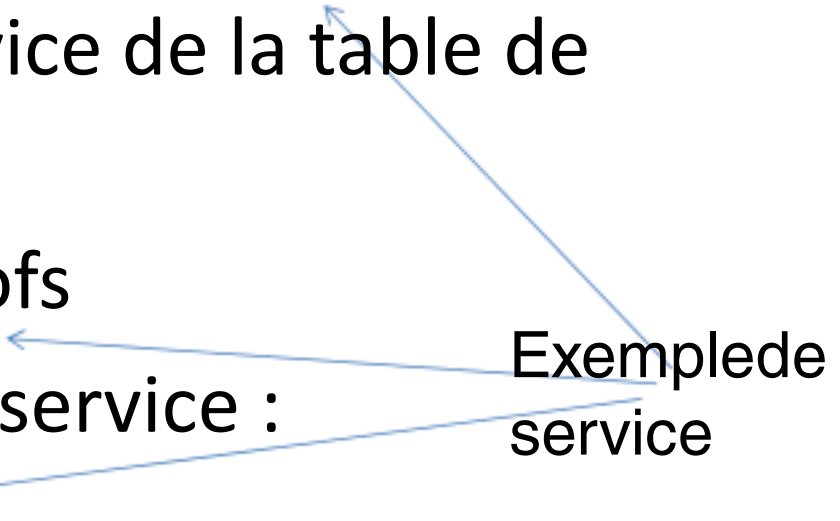
chkconfig --level 0123456 autofs off

- Suppression du service de la table de configuration :

chkconfig --del autofs

- Arrêt immédiat du service :

service autofs stop



Sécurisation du système de fichiers

Détection des fichiers dotésdedroitstrop permissifs

- Fichiers en écriture pour tous:

find / .type f .perm .o+w.ls

- Fichiers en écriture pour le groupe:

find / .type f .perm .g+w.ls

- Répertoires en écriture pour tous:

find/ .type d .perm .o+w .ls

- Répertoires en écriture pour le groupe:

find / .type d .perm .g+w.ls

Droits suid et sgid

- De nombreuses attaques détournent

  l'utilisation des droits particuliers suid et sgid positionnés sur des fichiers de programmes pour obtenir des accès privilégiés aux ressources du système

- Recherche des fichiers dotés du droit « suid » :

find / -perm -4000 -type f -ls

- Recherche des fichiers dotés du droit « sgid » :

find / -perm -2000 -type f -ls

Blocage des comptes inutiles

- Le shell de tous les autres comptes doit être positionné à /sbin/nologin (sous Red Hat) ou /bin/false (sous Debian).

Filtrage réseau avec TCP Wrapper

- TCPWrapperest une bibliothèquepermettantde filtrer les connexions réseau au niveau applicatif

/etc/hosts.denyet /etc/hosts.allow

Exemple:

Fichier /etc/hosts.denysur l'ensemble des machines:

```
# Interdit toutes les connexions par défaut et envoie un
# courrier électronique d'alerte lors d'une tentative de
# connexion refusée.
ALL:ALL spawn (echo "%s refuses connection from %c" | /bin/mail -s "tcpdalert" hostmaster@ss.com) &
```

Fichier /etc/hosts.allowsur l’ensembles des serveurs

- # Autorise les connexions SSHenprovenance des réseaux internes de l'entreprise et de l'adresse de bouclage interne.
- sshd: 192.168.154.0/255.255.255.0, 192.168.155.0/255.255.255.0, 127.0.0.1

Supprimer les services inutiles

- Les services contrôlés par xinetdpeuventêtre activés et désactivés par la ligne « disable»de leur fichier de configuration.
- $ grepdisable/etc/xinetd.d/*

  chargen: disable= yes

  chargen-udp: disable= yes

  cups-lpd: disable= yes

  ...

  vmware-authd: disable= no

Configuration sécurisée de la pile TCP/IP

- Lefichier de configuration/etc/sysctl.conf.

  Permet d'apporter un ensemble de sécurité:
- ICMP Redirect:

Le but des messages ICMP Redirectest

d’indiquer à une machine ou à un routeur qu’il y a un chemin plus court pour joindre une destination donnée.

- # Ignore ICMP Redirectmessage

net.ipv4.conf.all.accept_redirects= 0

- ICMP Echo request: # Ignore ICMP Echo request message

net.ipv4.icmp_echo_ignore_broadcasts = 1

net.ipv4.icmp_echo_ignore_all = 1

- Interdiction du source routing: # Disabling source routing

net.ipv4.conf.all.accept_source_route = 0

Les pare-feux (Firewalls)

- Un pare-feuxempêchelapropagationd'un incendie
- Les Firewalls doivent empêcher la propagation d'une attaque, tout en laissant passer le trafic utile
- Un Firewall peut être constitué d'un ou de plusieurs équipements