Avertissement

Le contenu de cet enseignement est à visée strictement pédagogique. Toute personne (étudiante ou non) exploitant son contenu hors du cadre qu'il définit s'expose à rendre des comptes devant des instances universitaires voire juridiques !!!

Sécurité

Matériels, Données, Systèmes, Réseaux, Logiciels

Nicolas Hernandez

Cours de DUT informatique – 2ème année
IUT de Nantes – Département Informatique
2006 – 2007

Nantes, le February 5, 2007

Organisation du module

- **Volume horaire** : 26H
  - soit 1H CM et 2 * 1H30 TD/TP sur 5 semaines + 2H de DS
- **Modalité d'examen** : à préciser type, date et durée
  - 1 TD/TP test mi-parcours coeff. 1
  - 1 DS en fin de module coeff. 2
  - En fin de CM : Quizz de synthèse
- **Equipe pédagogique**
  - CM : Nicolas Hernandez
  - TD/TP : Nicolas Hernandez, Sébastien Faucou, Jean François Hue, Pierre Levasseur

Objectifs du module

- **Sensibilisation aux problèmes de sécurité**
- **Comment ca marche ?**
  Présentation et utilisation des outils, des technologies, et des techniques visant à **attaquer/sécuriser/et contrôler** des données, des matériels, des systèmes, des réseaux et des logiciels
- **Mettre en place une architecture sécurisée pour une petite entreprise**

En fin de module, on pourra faire un bilan des pistes à suivre pour compléter ce cours

Contexte du module

- M. Liscouet : Sensibilisation à une politique de sécurité
- T. Brugere (1ère année) : Mathématique pour la cryptographie
- P. Levasseur (2ème année) : Administration de réseaux (notamment un TP sur le *backup*)
- S. Faucou et N. Hernandez (2ème année) : Réseaux (couches basses et hautes ; physique et protocolaire)
- Licence Pro. (pour 2 ans encore) : Sécurité (cryptographie, réseaux)

Planning prévisionnel du module

Date	CM	TD/TP
29/1/7	Politiques de sécurité, Pirate et administrateur, Attaques	Attaque du système par Buffer Stack overflow
5/1/7	Sûreté des fonctionnement et cryptographie appliquée	Chiffrement, authentification, intégrité, et échange de clé
12-23/2/7	*Vacances de Février*	
26/2/7	Echanges sécurisés : IPv6 et IPSec, VPN, DMZ, VLAN...	Sniffing, ARP Spoofing, Authentification basic HTTP
5/3/7	Infrastructures, Firewall, IDS...	Fitrage IPTables, NAT, ssh
12/3/7	Appli. sécurisées : messagerie (S/MIME, PGP), Internet (SSL, HTTPS), Développ.	GPG, Cassage de mots de passe John The Ripper, SQL Injection
19-26/3/7	*Eventuellement un dernier CM/TD/TP, puis DS*	
2/4/7	*Vacances de Printemps*	

Un saut vers la bibliographie

Ici [2]

Introduction – Sommaire

A méditer...

"Ce ne sont pas les murs qui protègent la citadelle,
mais l'esprit de ses habitants"

Thudycite

Définition

Définition

(en) **Sécurité** : état qui résulte de l'absence de *risque*

Le Petit Robert

Ce qui nous intéresse c'est : **veiller à la sécurité**

Objectif

Protéger les *éléments sensibles* d'un (d'une architecture) réseau afin d'assurer sa pérennité en cas d'*incidents* de sécurité

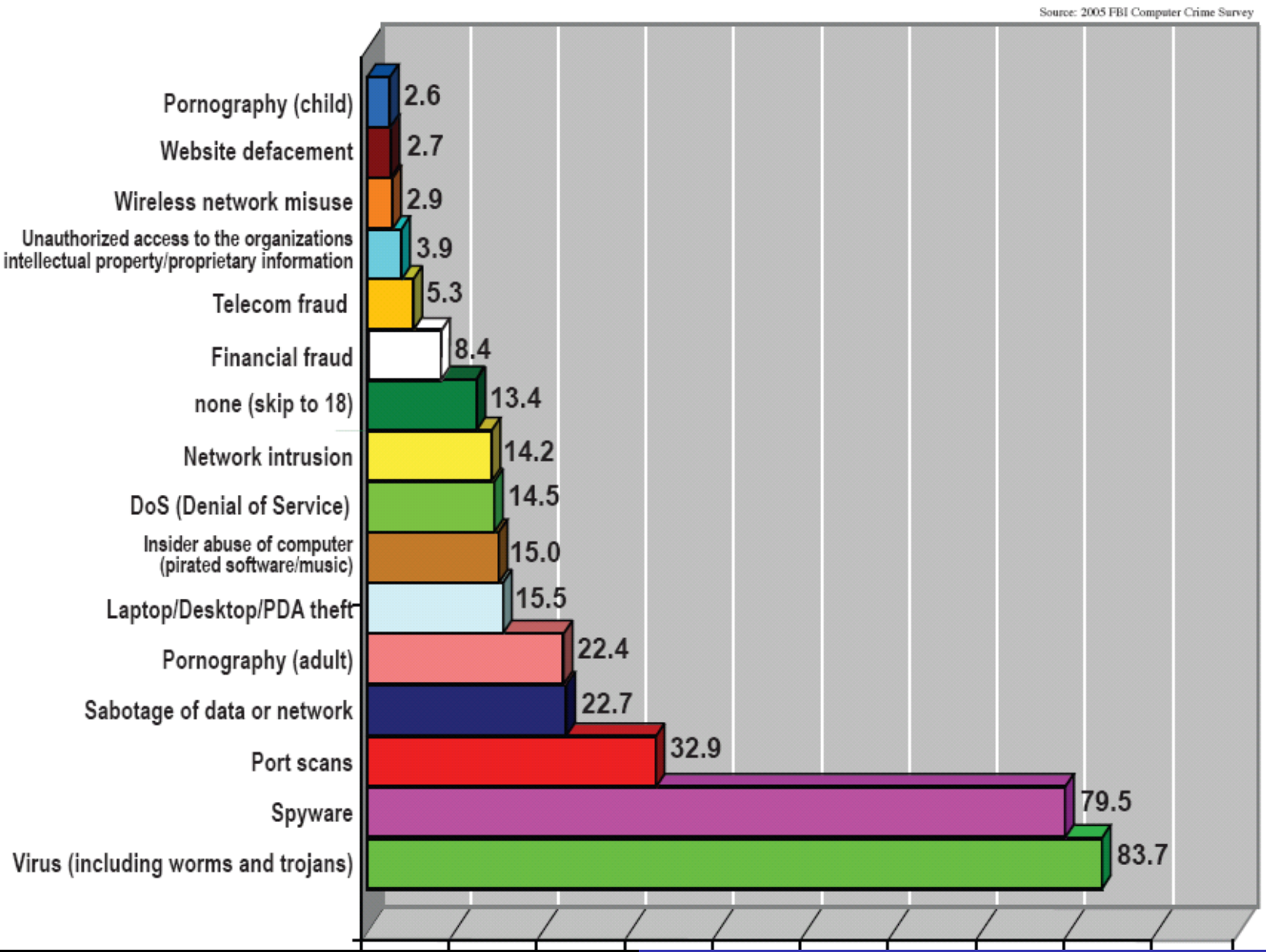
Plan général

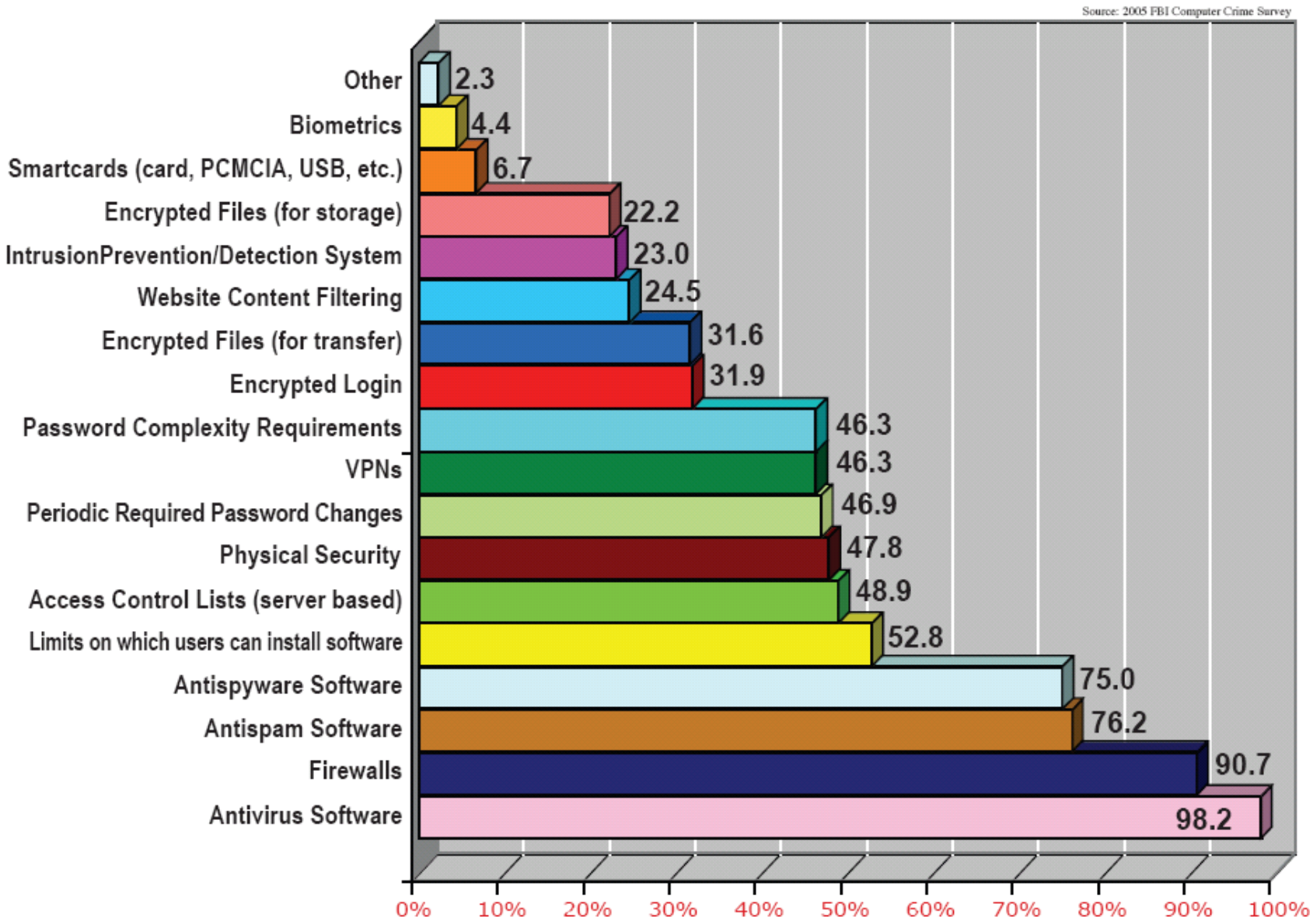
- Sécurité des Systèmes d'Informations (SI)
- Deux acteurs majeurs : le pirate et l'administrateur
- Quelques attaques

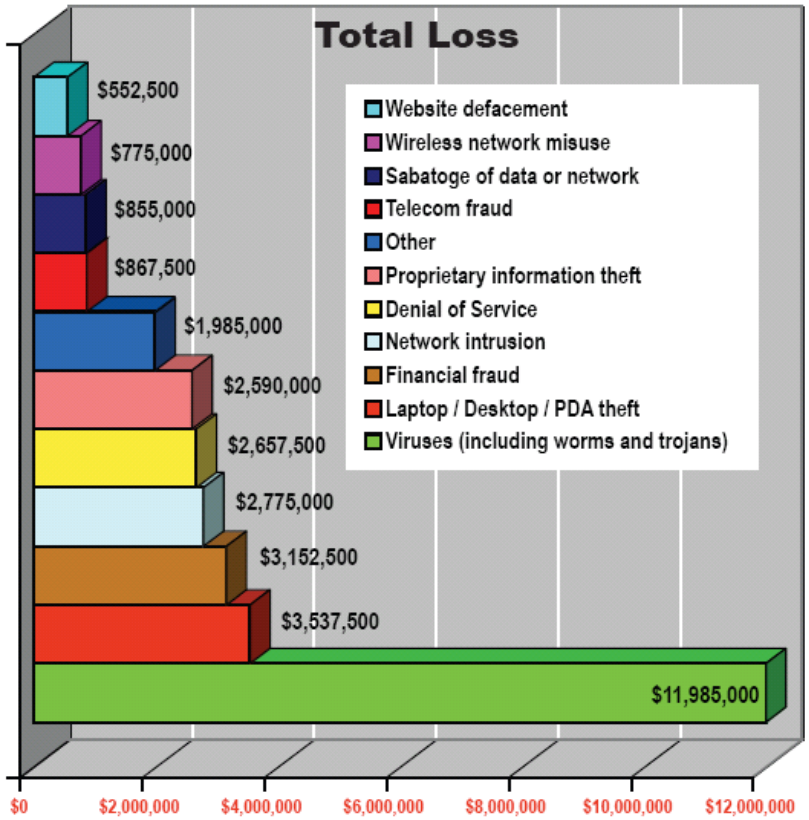
Etat des lieux des incidents en informatique

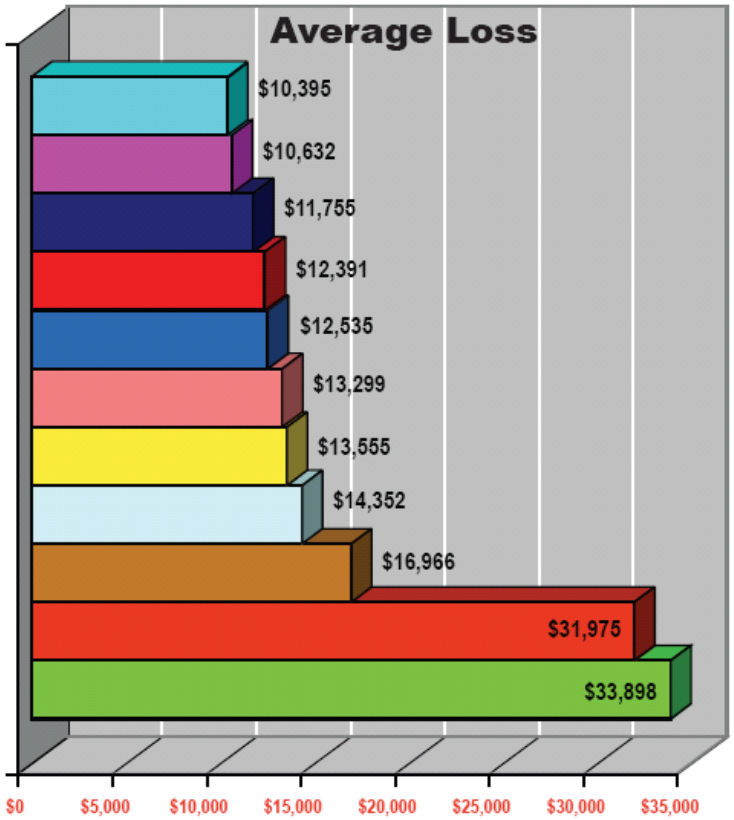
Le **Computer Crime**[1] **Survey**, sondage réalisé par le FBI en 2005 (observation des 12 mois précédents) auprès de 2000 organisations publiques et privées situées aux états unis.
www.fbi.gov/publications/ccs2005.pdf
Présenté à titre d'information pour observation pas nécessairement pour commentaires (les chiffres ne parlent pas, on en parle...)
Les diapo. suivantes se lisent "**Pourcentage d'organisations ayant rencontré...**"

[1] Cyber-criminalité : Suivant la définition légale, une distinction doit être faite entre le délit, puni d'une peine correctionnelle, et le crime, puni d'une peine afflictive (corporel) et infamante.
Or jusqu'à ce jour la plupart des attaques pouvent être classifiées comme des délits, et non des crimes...


Source: 2005 FBI Computer Crime Survey
Pornography (child) 2.6
Website defacement 2.7
Wireless network misuse 2.9
Unauthorized access to the organizations intellectual property/proprietary information 3.9
Telecom fraud 5.3
Financial fraud 8.4
none (skip to 18) 13.4
Network intrusion 14.2
DoS (Denial of Service) 14.5
Insider abuse of computer (pirated software/music) 15.0
Laptop/Desktop/PDA theft 15.5
Pornography (adult) 22.4
Sabotage of data or network 22.7
Port scans 32.9
Spyware 79.5
Virus (including worms and trojans) 83.7


Source: 2005 FBI Computer Crime Survey
Other
2.3
Biometrics
4.4
Smartcards (card, PCMCIA, USB, etc.)
6.7
Encrypted Files (for storage)
22.2
IntrusionPrevention/Detection System
23.0
Website Content Filtering
24.5
Encrypted Files (for transfer)
31.6
Encrypted Login
31.9
Password Complexity Requirements
46.3
VPNs
46.3
Periodic Required Password Changes
46.9
Physical Security
47.8
Access Control Lists (server based)
48.9
Limits on which users can install software
52.8
Antispyware Software
75.0
Antispam Software
76.2
Firewalls
90.7
Antivirus Software
98.2
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%





Total approximate cost of security incidents for the organizations responding: $31,732,500
Note: Dollar figures were approximated by assuming that the average loss in each dollar cost range was the median value. For example, if a respondent indicated that the loss was between $5,000 and $15,000, a $10,000 loss was assumed. For the $100,000+ category, a $200,000 loss was used for the calculation.

Source: 2005 FBI Computer Crime Survey

Sécurité des Systèmes d'Informations (SI) – Sommaire

Gestion des risques et évaluation de la sécurité

1. Identification des **éléments sensibles**
2. Déterminer les **objectifs de sécurité** pour ces ressources
3. Analyse des risques qui leur sont attachés
4. Définition des exigences de sécurité
5. Sélection et implémentation de contrôles de sécurité

Les éléments sensibles (ou ressources critiques) d'une entreprise

- **Matériels** (ordinateurs, équipements réseaux, etc.)
- **Données** (bases de données, sauvegardes, etc.)
- **Systèmes** (l'exploitation des matériels)
- **Réseaux** (l'échange des données)
- **Logiciels** (sources des programmes, services démons (DNS, FTP,...), applications web, etc.)
- **Personnes** (salariés, personnel en régie, etc.)

Objectifs de sécurité

- **Disponibilité** garantie l'accès et l'utilisation à des ressources (services, bande passante, données) de manière continue et non altérée (test de montée en charge, sauvegarde)
- **Intégrité** garantie qu'une ressource (données, applications, materiels...) n'a pas été modifié, altérée ou détruite (transfert sécurisé)
- **Confidentialité** permet de garder privée des (échanges de) données (contrôle d'accès, chiffrement)

Objectifs de sécurité

- **Identification** indique qui vous prétendez être (username)
- **Authentification** valide l'identité prétendue (password)
- **Autorisation** détermine les actions et ressources auxquelles un utilisateur identifié et autorisé a accès
- **Non-répudiation** garantie qu'un message a bien été envoyé par un émetteur authentifié
- **Traçabilité** permet de retrouver les opérations réalisées sur les ressources (logs)

Méthodes d'analyse des risques

Diverses méthodes qualitatives et quantitatives permettent d'analyser des risques de sécurité
Consulter [Llorrens et al., 06] Chapitre 4.

Politique de sécurité

Principe

Son objectif est de protéger les éléments sensibles de l'entreprise afin d'assurer sa pérennité en cas d'incidents de sécurité

Une politique consiste à rédiger des documents qui décrivent :

- **à un niveau formel** les règles de sécurité dans l'entreprise (guide, standard, recommandation)
- **la mise en oeuvre opérationnel et technique** de la politique (procédure).

La politique est l'expression d'un besoin tandis que la procédure est l'implémentation du besoin.

Domaines concernés par la politique de sécurité

- audit des éléments physiques, techniques et logiques constituants du SI
- sensibilisation des responsables et du personnel
- formation du personnel
- structuration et protection des locaux et matériels
- ingénierie et maîtrise d'oeuvre des projets
- gestion du SI
- définition d'un cadre juridique et réglementaire
- classification des informations selon différents niveaux de confidentialité et de criticité

Organisme et standard

Pour aider à élaborer une politique de sécurité :

- **DCSSI** (Direction Centrale de la Sécurité des Systèmes d'Information) **Organisme interministériel officiel définissant les normes** de la sécurité des SI (évaluation, certification)
  www.ssi.gouv.fr
- La **norme ISO 17799** : code de bonnes pratiques pour la gestion de la sécurité de l'information
- La **NSA** (*National Security Agency*)

Principalement à propos de la sécurité des SI, très peu au sujet de la sécurité des réseaux informatiques...

Deux acteurs majeurs : le pirate et l'administateur – sommaire

Définitions

"Menaces" humaines intentionnelles

- **Pirate** : personne commettant des **actes illégaux** liés à l'informatique (Kevin Mitnick, Cap'tain Crunch)
- **Hacker** : personne apte à modifier astucieusement un objet pour le destiner à un autre usage que celui prévu initialement (**non péjoratif**)
- **White hat Hacker** : consultants, administrateurs ou cyber-policier se servent de leurs compétences pour résoudre des problèmes en avertissant la personne ou l'organisme concerné d'un problème de sécurité.
  Black hat Hacker : créateurs de virus, cyber espions, cyber-terroristes et cyber-escrocs, ont une nette préférence pour les actions illégales
  Mais réducteur de dire : *white hats* sont les gentils et les *black hats* sont les méchants. De nombreux *White hats* ne servent que leurs interêts alors que d'autres *Black hats* protègent ceux des autres...
- **Script kiddies** : Gamin (pirate néophyte) utilisateur de scripts écrits par d'autres (péjoratif)

Wikipedia

Motivations du hacker

Vis-à-vis des ressources sensibles (Matériels, Données, Systèmes, Réseaux, Applications)

- prendre connaissance (données)
- modifier (données)
- altérer ou détruire (données)
- paralyser (service, réseau)
- se faire identifier ou pas (espionnage)
- exploiter pour ses propres intérêts
- cacher ses traces

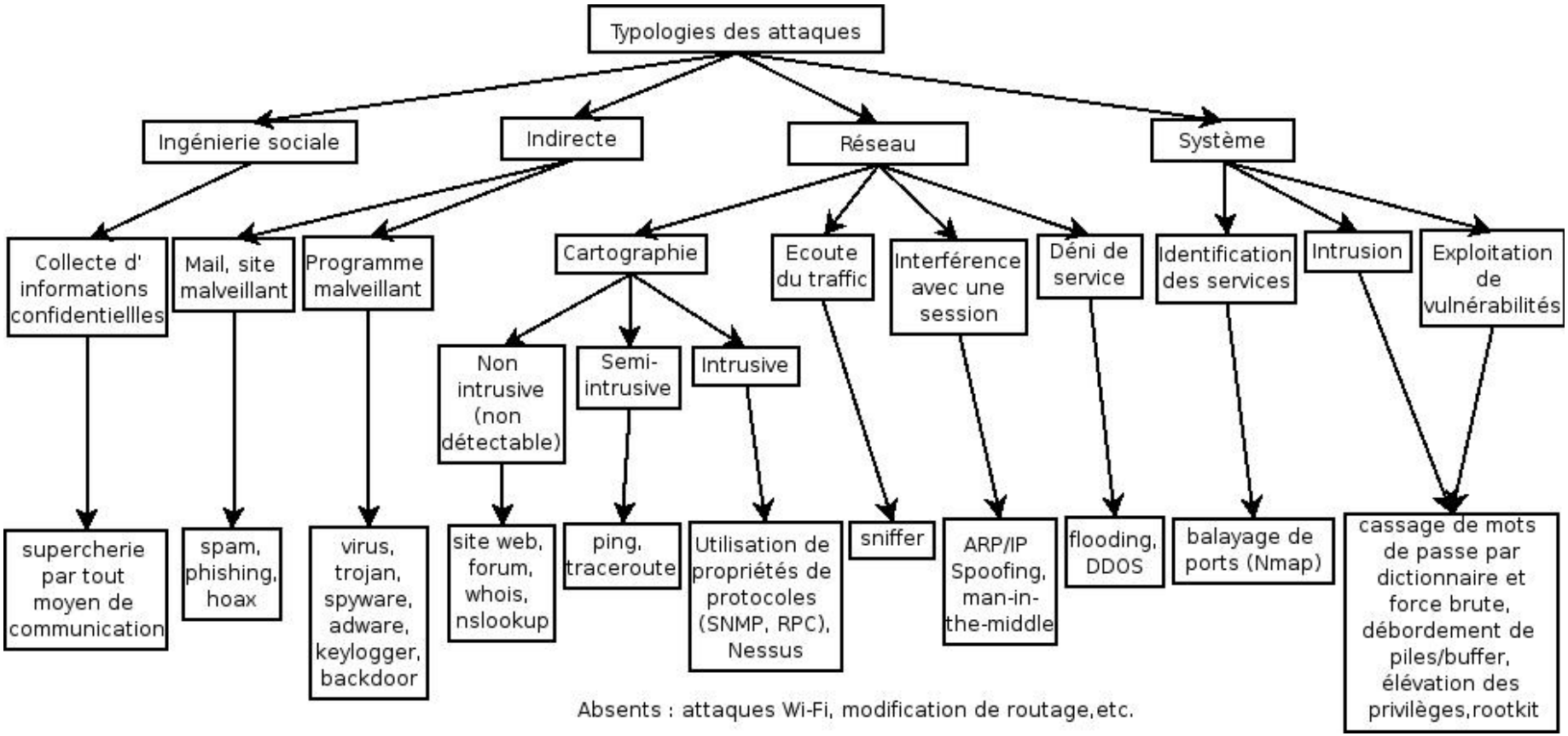
Méthodologie du hacker

1. **Collecte d'information et recherche de vulnérabilités**
   1. **Calcul d'empreinte** : activités économiques, à travers site web de l'entreprise, son forum d'aide, les services Whols, interrogation de DNS...
   2. **Balayage des systèmes** : connaître services, ports ouverts, systèmes d'exploitation (OS), version...
   3. **Enumération intrusive** : exploiter les caractéristiques propre à chaque OS, service, port... pour connaître des noms d'utilisateurs, l'existence de données en partage...
2. **Attaques à proprement parler**
   - **réseau**
   - **système**
   - **logiciel**

L'approche est cyclique : une attaque amenant à une autre pour une quête accrue de privilèges et de connaissances

Typologie des attaques[a]

[a]Voir le glossaire



Méthodologie générique de stratégie de sécurité

1. Identifier les menaces (virus, erreur, etc.)
2. Choisir une stratégie de défense

Pro-active (prévenir une attaque)

- prédire les dommages possibles (courte indisponibilité, réinstallation)
- calculer le degré de vulnérabilité

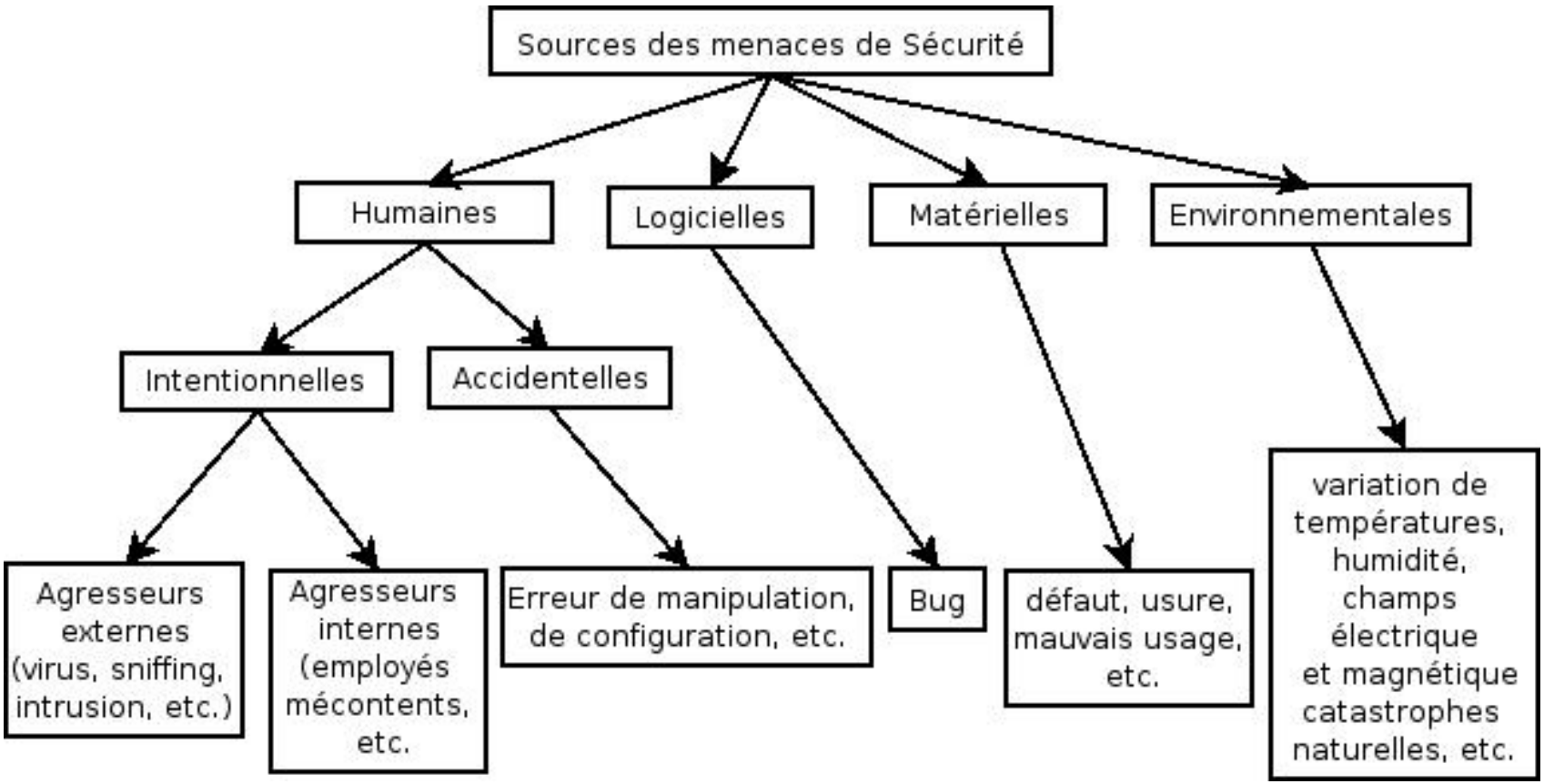
Réactive (minimiser les conséquences)

- déterminer les origines (logs, IDS)
- réparer les dommages

- mettre en oeuvre de solutions techniques pour minimiser ces degrés
- plan de contingence : actions à réaliser en situation critique

3. Analyser des résultats (de simulation ou d'attaques réelles) et améliorer la stratégie

Typologie des sources des menaces



Quelques règles de stratégie de sécurité

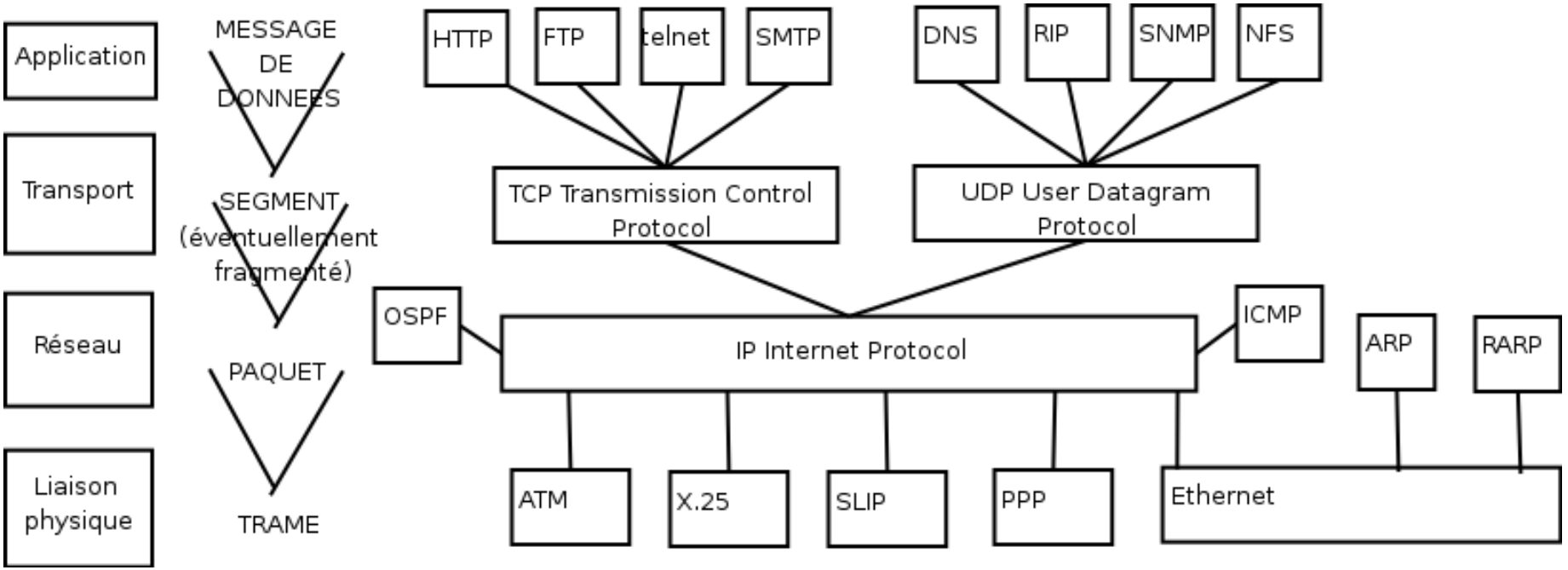
- **Découper en périmètres logiques** (e.g. réseau étudiant, enseignant, personnel)
- **Limiter et différencier les contrôles d'accès** à chaque périmètre (e.g. filtrage de paquets, relais applicatifs (proxy))
- Mettre en place des **contrôles d'authentification** aux accès
- Un utilisateur **ne dispose que des privilèges dont il a besoin**
- Toute communication intersite transitant sur des réseaux publics **est chiffrée** si elle contient des données confidentielles

Quelques règles de stratégie de sécurité

- **Des responsables distincts** de chaque périmètre
- **Des contrôles d'accès au sein d'un périmètre** sont définis afin de contrôler les portes dérobées
- **La zone d'administration est une zone dédiée et séparée pour chacun des périmètres**
- **Tout vecteur de propagation de virus** (e.g. document, média amovible) fait l'objet de contrôle avant de pénétrer un périmètre
- **Des campages d'information et de sensibilisation sont lancés**
- L'application de la politique de sécurité **est validée par un contrôle régulier**

Quelques attaques – sommaire

Couches, Protocoles et Services



Couches : découpage fonctionnel d'une architecture réseau (encodage physique, correction d'erreurs, transport internet, contrôle de la transmission...)
Protocole : Convention de communication entre 2 couches de même niveau
Service : Traitement particulier selon une architecture de programmation Client/Serveur

Couches, Protocoles et Services

- Sur *Internet*, une machine est joignable par son **IP (adresse logique)** et une fois *en (réseau) local* grâce à sa **MAC (adresse physique)**
  Sur 1 *machine*, 1 service est accessible par 1 **numéro de port** spécifique
- **Ethernet** se charge de la liaison physique entre des matériels
- **ARP** En local, prot. de demande d'1 MAC (par diffusion) à partir d'1 IP
- **ICMP** Prot. de signal d'erreur dans la transmission (ping, traceroute)
- **IP** Prot. assurant l'échanges de paquets entre des réseaux ; sans connexion ni acquittement
- **TCP** Prot. assurant une transmission fiable (tous les paquets arrivent et sont réordonnées) ; avec connexion et acquittement
- **UDP** Prot. non fiable mais rapide
- **telnet** Commande pour se connecter à distance sur une autre machine
- **DNS** Prot. faisant la correspondance entre un nom intelligible et une IP
- **SMTP, POP3/IMAP** Prot. d'envoi et de réception/consultation de mails
- **SNMP** Simple prot. de gestion (d'équipements) de réseau
- **RIP/OSPF** Prot. de routage entre des réseaux

L'ingénierie sociale (*social engineering*)

Définition

Obtention d'information par de la supercherie

Variante par mail :

```
From: resp-sec@organisation.com
To:  empl@organisation.com
Eric,
nous sommes un peu en situation de crise actuellement (un pirate cherche
à pénétrer notre réseau). Pouvez-vous remplacer immédiatement votre mot
de passe par la séquence sécurisée suivante : H0P/G3Tu11
merci
```

Variante par installation de logiciels :

X-Tetris (qui est en fait un *trojan* et qui installe un *spyware*)

Contre-mesures : informer les utilisateurs

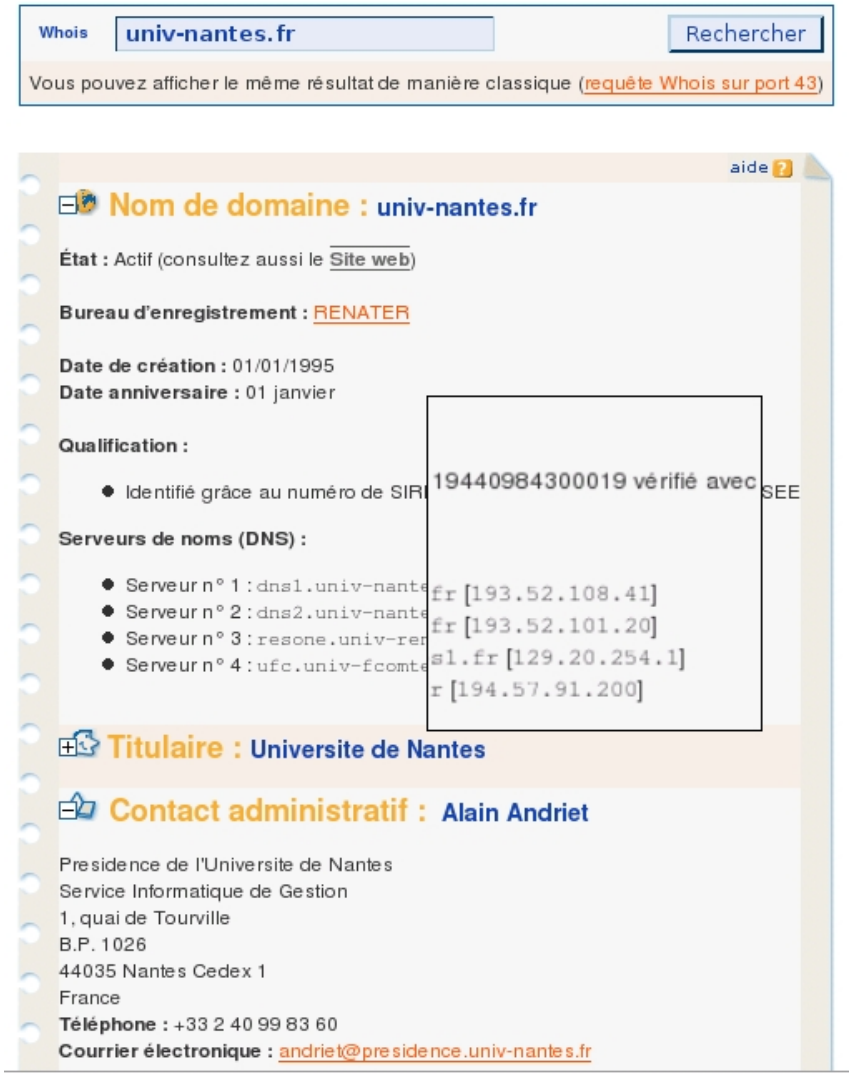
choisir un mot de passe long appartenant à aucun dictionnaire, ne jamais donner son mot de passe ni même à un autre employé, etc.

Cartographie du réseau

- **Who is ?** Centre d'information sur internet (*Network Information Centre*), **informant sur adresse IP et nom de domaine**
- En France, **AFNIC** (Association Française pour le Nommage Internet en Coopération) organisme chargé de la gestion administrative et technique des noms de domaine en .fr (France) et .re (Île de la Réunion)
- www.afnic.fr/outils/whois

Variantes :

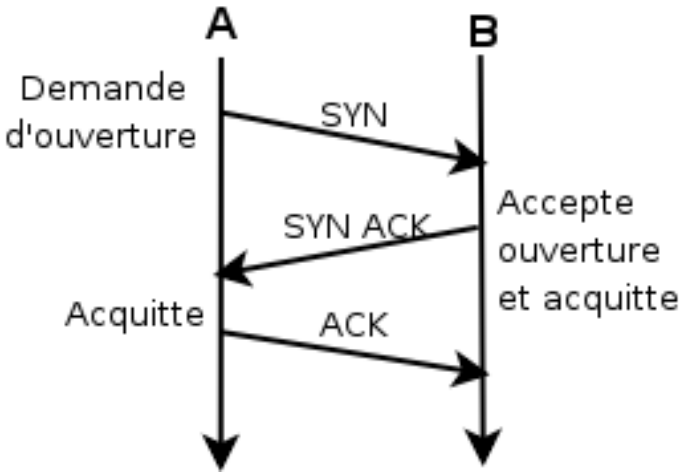
site web de l'entreprise, nslookup, ping, traceroute...



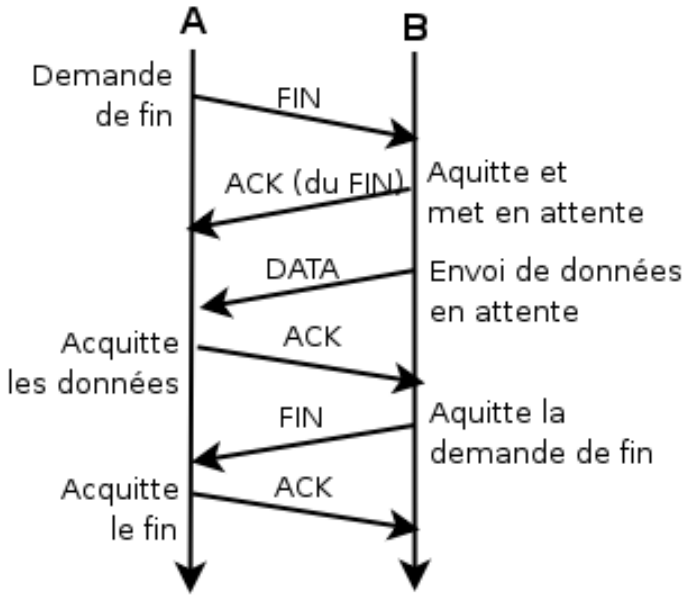
Rappels sur le fonctionnement de TCP

- **Connexion/déconnexion/problème/échange de données** gérés par un jeu de flags (dont les bits SYN, ACK, RST, FIN)
- **Ordre des paquets** géré par un **Numéro de Séquence** : Initialisé "aléatoirement" à la connexion (ISN). Un **Numéro d'Acquittement** égal au (NS + nombre d'octets) reçus +1 est envoyé

Ouverture de connexion (*3ways handshake*)



Fermeture de connexion



- L'envoi du flag RST, signale une **déconnexion immédiate** suite à la détection d'une anomalie

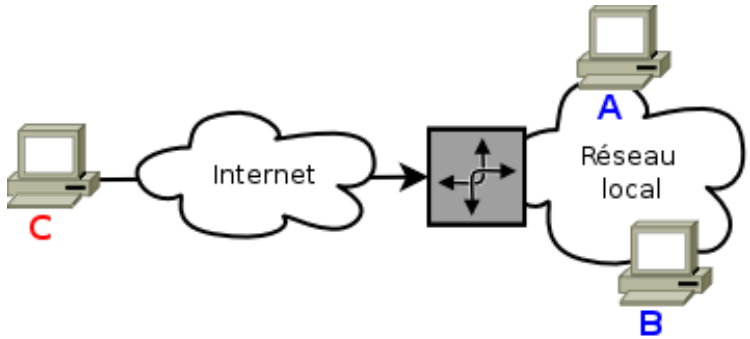
IP Spoofing

Définition

Usurpation d'identité en falsifiant son IP. L'objectif est d'acquérir des privilèges d'une machine (accès à certains services)

L'attaque : **C** souhaite usurper l'identité de **A** auprès de **B**

1. **C** apprend l'algorithme d'incrémentation des SN de **B** en lui envoyant des paquets et en analysant ses réponses
2. **C** rend inopérant **A**
3. **C** **forge** un paquet en falsifiant son IP avec celle de **A**, et demande une connexion à **B** (SYN)
4. **B** envoie à **A** un paquet SYN/ACK, que ce dernier ne peut valider car rendu inopérant...



5. **C** aquitte cette connexion (ACK) avec le NS prévu. La connexion est établie en toute impunité...

IP Spoofing

Commentaires :

- Difficile à mettre en oeuvre car en aveugle

Variantes :

- Qui contournent les limites : *attaque de routage* et *man-in-the-middle*
- Sur un réseau local : ARP Spoofing (plus aisé)

Contre-mesures :

- Interdire l'accès par confiance aux machines externes
- Refuser toutes requêtes externes d'une machine interne
- Améliorer la génération des NS (chiffrement)

Déni de service (*Denial Of Service (DOS)*)

Définitions

DOS : attaque qui **vise à rendre indisponible** un service, un système, un réseau

Attaque par inondation : une ou plusieurs (*DDOS, Distributed DOS*) machines inondent le réseau de paquets

Variantes :

- **Ping of Death** : **envoie de ICMP request**. Sans précision de délai d'attente, la machine victime répond aussi vite qu'elle peut (*ICMP reply*).
  `ping -l 65510 victim@organisation.com`
- **Smurf and Fraggle** : envoie de *ICMP request* **avec fausse adresse source : une IP broadcast**
- **Inondation SYN** : **demande d'établissement de connexion sans jamais la terminer**. Le serveur réserve alors de plus en plus de ressources (ports, mémoires...)

Cassage de mots de passe

Principe

Faire des essais jusqu'à trouver le bon mot de passe

Attaque par **dictionnaire**

Mot testé à partir d'une liste prédéfinie

Contient les mots de passe les plus courants (dont mots existants et diminutifs *powa*, *power*, *G0d*, *god*)
et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin, etc.).

Attaque par **force brute**

Toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution

Exemple : de *aaaaaa* à *ZZZZZZ* pour un mot de passe composé strictement de six caractères alphabétiques

Buffer overflow

Principe

Profiter de "faiblesses" de fonctions de langages de programmation qui ne contrôlent pas la taille de chaîne de caractères à enregistrer dans un tampon, pour écraser la mémoire du processeur et faire exécuter du code pernicieux

Example

En langage C, les fonctions telles que `scanf()` (analyse de chaîne de caractères) ou `strcpy()` (copie de chaîne de caractères) ne contrôlent pas la taille de la chaîne à enregistrer dans un tampon

Conclusion et éléments de synthèse – Sommaire

Quizz de synthèse

- En vous appuyant sur les attaques présentées, donner un exemple de vulnérabilité de protocole.
- Donner les principales étapes de la démarche du pirate lorsqu'il cherche à accomplir un méfait.
- Enumérer différents axes/facettes par lesquels on peut aborder les questions de sécurité ?

En sécurité : voir les autres ouvrages de ces auteurs !

C. Llorrens et al.,
Tableaux de bord de la sécurité réseau,
2ème édition, Eyrolles, 2006
bonne couverture ; attaques, contrôles et protections ; outils ; pratique

S. Ghernaouti-Hélie,
Sécurité informatique et réseaux, Cours et exercices corrigés, Licence 3e année, master, écoles d'ingénieurs,
Dunod, 2006
général ; 50% aspect managériale et 50% technologique ; théorique

Bruce Schneier
Cryptographie appliquée, Algorithme, Protocole et Code source en C,
Vuibert, 2ème édition, 2001

McClure et al.,
Hacking Exposed 5th Edition, Network Security Secrets & Solutions,
Mc Graw Hill/Osborne, 2005
comment hacker ; listes de vulnérabilités et de leurs contre-mesures des systèmes (unix, windows), des réseaux et des logiciels ; orienté pratique

En sécurité, sur le web...

- **DCSSI** (Direction Centrale de la Sécurité des Systèmes d'Information) définition de normes (évaluation, certification) www.ssi.gouv.fr
- **CERT** (Computer Emergency Response Team) centres d'alerte et de réaction aux attaques informatiques www.certa.ssi.gouv.fr
- **OSSIR** (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux) www.ossir.org
- **hakin9** (revue) www.hakin9.org
- **Outils** (pass crackers, sniffers, vuln. scanners, vuln. exploitation, web scanners, wireless, packet crafting, etc.) sectools.org
- **Mailing lists** seclists.org
- **bugtraq** (mailing list de failles, d'exploits) www.securityfocus.com/archive, insecure.org/sploits.html
- **Challenges de hacking** www.securiteinfo.com/attaques/hacking/challengeshacking.shtml
- **Etc.** fr.thehackademy.net, www.securite.org, newbiecontest.n0ne.org, www.securityfocus.com

En réseau : voir les autres ouvrages de ces auteurs ! [2]


C. Servin,
Réseaux et Télécoms,
Dunod, 2003
exercices avec corrigés


G. Pujolle
Initiation aux réseaux,
Eyrolles, 2002


A. Tannenbaum,
Réseaux - Architectures, protocoles, applications,
InterEditions, 3eme édition, 1996


R. Dapoigny,
Les protocoles dans les réseaux informatiques,
Gaëtan Morin éditeur, 1999
exercices avec corrigés


P. Rolin et al.,
Les réseaux - principes fondamentaux,
Hermès, 1996

Glossaire

- **canular informatique** (*hoax*) : courriel incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Encombrent le réseau et preneur du temps.
- **cheval de Troie** (*trojan*) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur
- **exploit** outil ou technique permettant d'exploiter une faille
- **hameçonnage** (*phishing*) : courriel (site web falsifié) dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles (ingénierie sociale)
- **log** : journaux enregistrant l'activité d'un système ou d'un réseau. Sous linux, voir le démon syslogd pour personnaliser la gestion des logs (/etc/syslog.conf). Voir aussi : /var/log/wtmp, connexions et déconnexions au système et consultable grâce à /usr/bin/last ; /var/log/lastlog, historique des dernières connexions et consultable grâce à /usr/bin/lastlog et /var/run/utmp, qui est connecté sur le système, lu par /usr/bin/w.

Glossaire

- **porte dérobée** (*backdoor*) : ouvreur d'un accès frauduleux sur un système informatique, à distance
- **pourriel** (*spam*) : courrier électronique non sollicité (publicité). Encombrent le réseau et preneur du temps
- **rootkit** : outils permettant d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer ses traces dans les logs