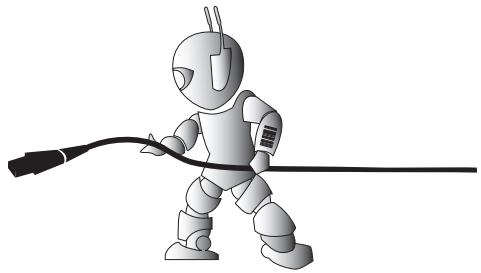
Introduction à la sécurité réseau

Cours de Réseaux

Tuyêt Trâm DANG NGOC
<dntt@u-cergy.fr>

Université de Cergy-Pontoise

2012-2013



DÉPARTEMENT
Sciences Informatiques

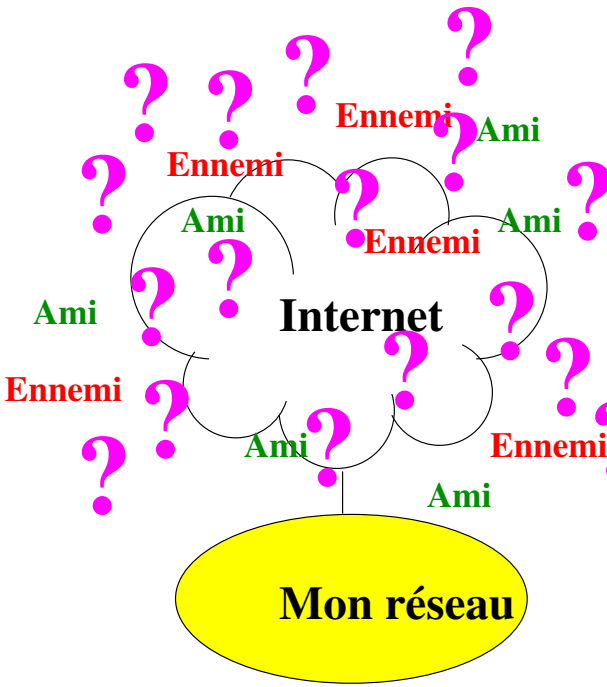
Pourquoi la sécurité

- Une connexion à l'Internet permet à un réseau de se connecter à plusieurs centaines de milliers d'autres réseaux.

⇒ avantages considérables

- chacun de ces centaines de milliers d'autres réseaux peuvent se connecter à ce réseau.

⇒ parmi eux, combien de personnes animées de mauvaises intentions, et potentiellement dangereuses ?



DÉPARTEMENT
Sciences Informatiques

Problèmes de sécurité possibles

Différentes catégories de problèmes de sécurité

- Chacun ayant son contexte propre et ses solutions.
- Sécuriser un environnement informatique revient à considérer chacun de ces cas.

Catégories de problèmes de sécurité

- Erreur humaine : Une destruction de fichiers importants par mégarde
- Problème logiciel : Un système d'exploitation, un logiciel qui plante et corrompt des données importantes
- Problème matériel : un crash de disque, un incendie, une inondation
- Piratage : Le vol, détournement ou destruction de données par des personnes malveillantes

DÉPARTEMENT Sciences Informatiques

Problèmes de sécurité possibles

Catégories de problèmes de sécurité

- Erreur humaine : Une destruction de fichiers importants par mégarde
  $\Rightarrow$ Education des utilisateurs
- Problème logiciel : Un système d'exploitation, un logiciel qui plante et corrompt des données importantes
- Problème matériel : un crash de disque, un incendie, une inondation
- Piratage : Le vol, détournement ou destruction de données par des personnes malveillantes

+

- Duplicata du système et des logiciels utilisés, ainsi que un report précis de l'état du système (lorsqu'il est stable).
- Sauvegardes régulières des données.

DÉPARTEMENT Sciences Informatiques

Problèmes de sécurité possibles

Catégories de problèmes de sécurité

- Erreur humaine : Une destruction de fichiers importants par mégarde
- Problème logiciel : Un système d'exploitation, un logiciel qui plante et corrompt des données importantes $\Rightarrow$ Mise à jours des logiciels
- Problème matériel : un crash de disque, un incendie, une inondation
- Piratage : Le vol, détournement ou destruction de données par des personnes malveillantes

+

- Duplicata du système et des logiciels utilisés, ainsi que un report précis de l'état du système (lorsqu'il est stable).
- Sauvegardes régulières des données.

DÉPARTEMENT Sciences Informatiques

Problèmes de sécurité possibles

Catégories de problèmes de sécurité

- Erreur humaine : Une destruction de fichiers importants par mégarde
- Problème logiciel : Un système d'exploitation, un logiciel qui plante et corrompt des données importantes
- Problème matériel : un crash de disque, un incendie, une inondation
  $\Rightarrow$
  - Maintenance du matériel
  - Redondance du matériel
  - dispersion sur plusieurs sites
- Piratage : Le vol, détournement ou destruction de données par des personnes malveillantes

+

- Duplicata du système et des logiciels utilisés, ainsi que un report précis de l'état du système (lorsqu'il est stable).
- Sauvegardes régulières des données.

DÉPARTEMENT Sciences Informatiques

Problèmes de sécurité possibles

Catégories de problèmes de sécurité

- Erreur humaine : Une destruction de fichiers importants par mégarde
- Problème logiciel : Un système d'exploitation, un logiciel qui plante et corrompt des données importantes
- Problème matériel : un crash de disque, un incendie, une inondation
- Piratage : Le vol, détournement ou destruction de données par des personnes malveillantes ⇒ Sécurisation des systèmes et du réseau

+

- Duplicata du système et des logiciels utilisés, ainsi que un report précis de l'état du système (lorsqu'il est stable).
- Sauvegardes régulières des données.

DÉPARTEMENT Sciences Informatiques

Agression - Motivation et conséquences

- Accès abusifs ou non autorisés aux ressources
  - Temps de calculs : "crack" de mots de passe, de clefs
  - Place disque : stockage de logiciels piratés ou de documents inavouables
  - Site clandestin : échange FTP pour des logiciels warez ou des images illégales
  - Site relais : utilisation du site comme point de départ vers un site à attaquer afin de pouvoir "brouiller" les traces
- Espionnage industriel, conflit militaire
  - Récupération : de documents sensibles
  - Détournement : des clients/utilisateurs du concurrents
  - Paralysie : des serveurs du concurrent
- Désoeuvrement, Erreurs de jeunesse
  - Attirance de l'interdit :
  - Désir de renommée, impressioner ses amis :
  - Envie de nuire, vandalisme :

Ces points ne sont pas exclusifs.

DÉPARTEMENT Sciences Informatiques

Conséquence d'une agression

Les conséquences peuvent être plus ou moins graves suivant les précautions prises en matière de sécurité, du type de l'attaque, et de la cible visée.

- Pertes : documents perdus, outils de travails détruits, mois de travail perdu
- Manque à gagner :, perte financière dans le cas d'espionnage industriel
- perte de crédibilité : Une entreprise passoire quand à la confidentialité des dossiers de ses clients, une page web d'accueil détournée ...
- illégalité : en étant utilisée pour des trafics clandestins
- divulgation : d'informations confidentielles
- déclenchement d'actions : pouvant provoquer des accidents physiques : drames humains, destruction matérielles, etc.

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

L'humain & sa machine

Environ 80% des problèmes de sécurités ont pour origine les utilisateurs internes qui mettent le réseau en danger (souvent) par ignorance ou inconscience par leur comportement :

- installation intempestives de logiciels de sources douteuses (chevaux de troie :vers, virus, porte dérobée)
- mauvaise utilisation du lecteur de courrier (en ouvrant automatiquement les fichiers attachés) mêmes risques que ceux cités précédemment
- mots de passe "basique"
- "prêt" de mot de passe
- Trou dans le réseau par ignorance (modem, wifi) ou volontairement (IRC, utilisation à distance)

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Logiciel malveillant (*malware*)

But : nuire à un système informatique.

- virus : programme se dupliquant sur d'autres ordinateurs ;
- ver (worm) : exploite les ressources d'un ordinateur afin d'assurer sa reproduction ;
- wabbit : programme qui se réplique par lui-même (mais qui n'est ni un virus, ni un ver) ;
- cheval de Troie (trojan) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;
- porte dérobée (backdoor) : ouvreur d'un accès frauduleux sur un système informatique, à distance ;
- logiciel espion (spyware) : collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers ;
- enregistreur de frappe (keylogger) : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ;
- exploit : programme permettant d'exploiter une faille de sécurité d'un

DÉPARTEMENT Sciences Informatiques

Cheval de Troie (trojan)

Cheval de Troie (trojan)

programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;

En général, piège l'utilisateur naïf qui croit exécuter un logiciel attirant car décrit et nommé avec un nom qui semble inoffensif (setup, tetris.exe, office.bin, super_mario.exe, mise-a-jour-v1.2.4, update_tool)

Incorporation plus ou moins subtile. Lorsque l'utilisateur exécute le programme qui semble inoffensif :

- la routine nuisible est exécutée et l'utilisateur peut s'apercevoir de son erreur, mais... trop tard.
- la routine nuisible est exécutée en arrière plan et rien ne semble se lancer. L'utilisateur est déçu, mais oublie l'incident.
- la routine nuisible est exécutée et affiche un message d'erreur laissant penser à un problème dans l'exécution du logiciel.
- le logiciel se lance au grand bonheur de l'utilisateur, et la routine nuisible est exécutée en arrière plan.

DÉPARTEMENT Sciences Informatiques

Cheval de Troie (trojan)

Cheval de Troie (trojan)

programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;

La routine nuisible peut être :

- Un programme effectuant directement son action (destruction de fichiers, plantage du système, envoi de certaines informations du disque, s'autoréplique pour utiliser toutes les ressources du système (wabbit))
- L'installation de virus, de vers
- L'installation d'espion (spyware, keylogger)
- Une installation d'une porte dérobée (backdoor)

DÉPARTEMENT Sciences Informatiques

Vers

1. Exploitation d'un bug d'un service
2. Modification du code du service pour :
   - effectuer des opérations malveillantes
   - contacter ce service sur une autre machine
3. Goto 1

Les grands vers :

Vers

1. Exploitation d'un bug d'un service
2. Modification du code du service pour :
   - effectuer des opérations malveillantes
   - contacter ce service sur une autre machine
3. Goto 1

Les grands vers :

ver Morris (1988 - Morris) /sendmail+fingerd+mot de passe faible :

- *possibilité, en mode 'DEBUG', d'envoyer des fichiers sur une machine distante en utilisant un shell utilisé ensuite pour compiler le code source envoyé*
- *dépassement de tampon de l'utilitaire finger*
- *devine les mots de passe faible des utilisateurs à l'aide de dictionnaires, et se copie sur des machines distantes avec les commandes rsh et rexec*

DÉPARTEMENT Sciences Informatiques

Vers

1. Exploitation d'un bug d'un service
2. Modification du code du service pour :
   - effectuer des opérations malveillantes
   - contacter ce service sur une autre machine
3. Goto 1

Les grands vers :
I love you (2000) /mail : avec en pièce jointe le programme lui-même. L'utilisateur croit que la pièce jointe est un fichier de texte. En ouvrant ce fichier, l'utilisateur exécute le programme, qui va explorer la liste des contacts de l'utilisateur pour leur envoyer un mail semblable.

DÉPARTEMENT Sciences Informatiques

Vers

1. Exploitation d'un bug d'un service
2. Modification du code du service pour :
   - effectuer des opérations malveillantes
   - contacter ce service sur une autre machine
3. Goto 1

Les grands vers :
Code Red (2001) /IIS : prendre le contrôle de ces serveurs pour lancer à partir d'eux une attaque par déni de service (DoS), visant à saturer les ressources d'un site Web précis (serveur de la Maison Blanche)

DÉPARTEMENT Sciences Informatiques

Autres Vers

- Se propageant en utilisant les adresses contenues dans le carnet d'adresse de l'utilisateur ou d'autres fichiers. Exécuté lors de l'exécution de la pièce jointe attachée : Bagle (2004), Melissa (1999 - David Smith) virus de macro word 97/2000et outlook 95/98, NetSky (2004 - Jaschan), Sobig (2003 - ?)
- Sasser (2004 - Jaschan), faille LSASS de Windows
- Blaster (2003 - Parson), Faille DCOM RPC de toute la gamme Windows
- Nimda () faille Unicode Web Traversal exploit. S'installer sur simple visite d'un site infecté. Peut se transmettre par courriel en utilise une faille de l'implémentation de MIME par Microsoft Internet Explorer, lui permettant de s'exécuter sur simple prévisualisation du courriel.
- SQL Slammer (2003 - ?) sur faille de Microsoft SQL Server. Sert ensuite à stocker des warez.
- Santy (2004 - ?) sur faille du logiciel de forum phpBB : utilise Google pour trouver des serveurs web l'utilisant. Puis DoS de phpBB
- Conficker-A, B, B++, C (nov 2008) : faille de Windows Server Service (2000, XP, XP, 2003, 2007, 2008, Vista, 7) 9 millions d'infectés. infection classique et cassage de mot de passe. MAIS le vers se protège lui-même et se met à jour. Connexion vers serveurs pseudo-aléatoire pour récupérer des ordres (mise à jour, patch, p2p, etc.).

DÉPARTEMENT Sciences Informatiques

Espions

Espions - Spyware

logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance.

Un Spyware peut (liste non exhaustive) capturer des mots de passe, espionner les programmes exécutés à telle ou telle heure, espionner les sites Internet visités, capture d'écrans puis transmettre ces informations à un tier.

Enregistreur de frappe (keylogger)

Matériel ou logiciel qui enregistre les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux ou via des ondes électromagnétiques.

es

Espions

Mais encore :
Rayonnement electromagnetique produits par écran, clavier, cordons (serie, parallele, clavier, Modem etc...), imprimantes, etc. exploitables. Protection TEMPEST (cage de Faraday).
interceptions de tres bonne qualite entre 30 et 40 metre de distance et a travers un etage de hauteur dans le quartier des affaires de Tokyo.
Vibrations sur vitres détectables par rayon laser (mais là on sombre dans la pranoia !)

Portes dérobées : backdoor

- Introduit par le développeur du logiciel ou par un pirate informatique.
- La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par contournement de l'authentification).
- Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel contenant la porte dérobée, le contrôle peut s'étendre à l'ensemble des opérations de l'ordinateur. item Peut ouvrir un port d'écoute que le pirate pourra contacter à tout moment (socket de troie)

Exemple célèbre :
Back Orifice (Cult of the Dead Cow) est un logiciel de prise de contrôle à distance (port 31337) de machines utilisant le système d'exploitation Windows.

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Courrier électronique

Courrier électronique

- énormément utilisé
- transporte tout type de données
- utilisés par des utilisateurs n'ayant pas ou peu de connaissance en informatique et sécurité
- moyen de diffusion efficace, peu contrôlable et peu contrôlé.

Canular Informatique (hoax)

Canular Informatique (hoax)

Courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes (messages alarmiste, fausses alertes de virus, vente pyramidale, promesse de gains, légendes urbaines, faux complots, prises par les bons sentiments, etc).
Ils encombrent le réseau, et font perdre du temps à leurs destinataires. es canulars sont, eux, relayés manuellement par des personnes de bonne foi à qui on demande de renvoyer le message à toutes ses connaissances Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

http ://www.hoaxbuster.com/

DÉPARTEMENT
Sciences Informatiques

Spam

Spam

Un courrier électronique non sollicité, la plupart du temps de la publicité. Ils encombrent le réseau, et font perdre du temps à leurs destinataires La plupart du temps envoyés de manière automatisée à une liste de destinataires. Certains essayent d'exploiter la crédulité du destinataire.

```
81 ND  Jan 29 Eugenio Oneill  (   2) buy now 100mg x 60 pills $129.95
66 ND  Jan 29 ftragten_1990@S (  11) Discount for you. Right time to buy items
32 ND  Jan 29 Jennifer Yang   (   2) Price for Viagra (Sildenafil) 50mg x 10 p
24 ND  Jan 29 Rodney Crum     (  30) Best gift for you
46 ND  Jan 29 ikaihc_1995@LAF (  11) Discount. Save 70% on on your meds now.
28 ND  Jan 29 Shauna Tidwell  (  32) Easiest way to burn pounds
77 ND  Jan 29 Ellwood Mooney  (   4) You are nominated for an Associates
62 ND  Jan 29 Service PayPal  (  74) Attention! Votre compte PayPal a ete limi
47 ND  Jan 29 Clayton. Pre 20 (   9) Vegas Casino Club, le meilleur choix en l
 6 ND  Jan 29 Alfred Collins  ( 180) Confirm your order
 8 ND  Jan 29 Alfonzo Bush    ( 761) Over 10 million men made their women happ
 4 ND  Jan 29 Albrecht Aguila ( 180) Your wife need your attention? Solve all
44 ND  Jan 29 European Casino (  99) Offre de bonus incroyable!
12 ND  Jan 29 Agustin Curtis  ( 175) Make money Fast
19 ND  Jan 29 Abner Cross     ( 180) Enlarge your penis fast
87 ND  Jan 29 Aguistin Davids (  76) You want to impress your girlfriend
 2 ND  Jan 29 Addison Copelan ( 876) Breaking News
```

DÉPARTEMENT Sciences Informatiques

L'hameçonnage (phishing)

hameçonnage (phishing)

Un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles

1. l'utilisateur reçoit un mail semblant provenir de sa banque
2. ce mail lui indique qu'il y a un problème sur son compte et qu'il faut y remédier rapidement.
3. l'utilisateur est invité à cliquer sur un lien sensé le diriger vers la page d'accueil de sa banque
4. en réalité, ce lien le redirige vers le site de l'arnaqueur. La page d'accueil imitant celle de la banque.
5. l'utilisateur est invité à rentrer son login/mot de passe ou code de carte bleue
6. l'arnaqueur est content...

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Le réseau

- Ecoute des connexions (*sniffing*) : interception des messages et/ou mot de passe par des renifleurs, identification des services du réseaux, des machines qui communiquent, des comportaments, etc.
- Mystification (spoofing) : prendre l'identité d'une autre personne/machine, DNS, routeur, machine sécurisée, etc.
- Déni de service (denial of service - DoS) : empêcher le bon fonctionnement d'un système en empêchant un service/machine de fonctionner.
- Intrusion exploitant :
  - Les bugs des services (serveur de mail, routeurs ...)
  - Des portes dérobées déjà mises en place par une intrusion précédente
  - Faille dans l'architecture du réseau, sur les systèmes employés, dans les éléments d'interconnexion.

DÉPARTEMENT Sciences Informatiques

Ecoute des connexion (Sniffing)

- Sur réseau en bus, utilisant du cable coaxial
- Sur réseau Wi-Fi !

Interception de mots de passes, de correspondances privées.

Mystification (spoofing) - Usurpation d'identité

- ARP Cache Poisoning : envoi ARP reply au routeur en prétendant être la machine dont on a usurpé l'identité. Envoi ARP reply à la machine victime en prétendant être le routeur. Tout le traffic entre la victime et le routeur passe par l'attaquant
- IP Spoofing : abuse la machine cible en se faisant passer une autre machine (par ex. un hôte de confiance) en usurpant son adresse IP.
  - ICMP, UDP :
  - Vol de session TCP : plux complexe, car numéro de séquence à deviner.
- DNS Cache Poisoning :

DÉPARTEMENT Sciences Informatiques

DNS Cache Poisoning - Attaque par l'ajout de plusieurs résolutions (Kashpureff - 1997)

Rappel : Dans une transaction DNS, l'identifiant de 16 bits pseudo-aléatoire doit être le même.

- Le pirate demande au serveur DNS cible, l'IP d'une zone dont il gère le serveur DNS.
- le serveur DNS cible interroge le serveur DNS du pirate
- le serveur DNS du pirate renvoi l'information + des infos concernant d'autres sites.
- le serveur DNS cible insère toutes ces informations dans son cache.

Utilisation d'un serveur DNS ne prenant que les réponses à la question posée.

DÉPARTEMENT Sciences Informatiques

DNS Cache Poisoning - Attaque basée sur le paradoxe des anniversaires (1995 ?)

Paradoxe des anniversaires : Il suffit de 23 personnes pour avoir une chance sur deux que deux personnes de ce groupe aient leur anniversaire le même jour de l'année. À partir d'un groupe de 57 personnes, la probabilité est supérieure à 99

- Le pirate envoie un grand nombre de requête de résolution au serveur DNS A (résoudre www.gogole.com)
- En même temps, le pirate se fait passer pour le serveur de nom B interrogé par le serveur DNS A pour résoudre la requête en envoyant dans la réponse : un identifiant aléatoire et la résolution IP h.a.c.k (l'adresse IP d'un serveur pirate).
- si par hasard, l'identifiant tombe sur celui utilisé dans la transaction entre A et le vrai B, et que la réponse du pirate arrive avant la réponse du B légitime, alors le serveur DNS A insère h.a.c.k dans son cache
- les autres clients DNS interrogeant A pour obtenir l'adresse de www.gogole.com auront pour réponse h.a.c.k.

DÉPARTEMENT Sciences Informatiques

Amélioration de DNS-poisonning par (Kaminsky - 2008)

"Attaque basée sur le paradoxe des anniversaires" laborieuse et peu de chance de succès : si l'attaque ne réussit pas, la "vraie" IP sera insérée dans le cache pendant un bon moment (TTL).
Attaque de Kaminsky : utiliser des résolutions en série sur des hotes du même domaine pour augmenter les tentatives, et ajouter dans la réponse (Additional)

```
xxx.gogole.com      IN A x.y.z.t
gogole.com          IN NS    www.gogole.com
www.gogole.com      IN A h.a.c.k
```

Pour chaque tentative xxx, on applique l'attaque par paradoxe des anniversaires. Si la tentative échoue, on fait varier le xxx.
Méthode qui marche à presque tous les coups en une dizaine de minutes.

DÉPARTEMENT Sciences Informatiques

Déni de services

Déni de service (*Denial of Service - DoS*)

Empêcher une machine de fournir les services qu'elle devrait fournir.

- sabotage d'un concurrent, chantage
- malveillance pure, défi
- bloquer la surveillance pendant une intrusion
- se faire passer pour la machine attaquée

- saturation des ressources
- attaque de la machine (piratage, virus, vers)

Distributed Denial of Service (DDoS) repose sur une parallélisation d'attaques DoS, simultanément menées par plusieurs systèmes (machines rebond) contre un seul.

DÉPARTEMENT Sciences Informatiques

DoS par saturation des ressources I

- Saturation d'un serveur : Attaque faisant planter un système (en général celui d'un serveur), en surchargeant ses ressources.
- Saturation d'un réseau : Attaque submergeant un réseau d'un flot de trafic plus grand qu'il n'est capable de le traiter - la bande passante est alors saturée et le réseau devient indisponible.

- Attaque ARP : demandes incessantes ARP envoyées vers un routeur ou serveur d'un même réseau.
- ping de la mort : ICMP echo request de taille supérieure (65535 octets) au maximum spécifié.
- Attaque ping : innondation de ICMP echo request vers un routeur ou serveur
- Attaque Smurf : innondation de ICMP echo request avec pour adresse IP source l'adresse de la victime et pour destination l'adresse de diffusion du réseau

DÉPARTEMENT Sciences Informatiques

DoS par saturation des ressources II

- Host Unreachable : envoi de message ICMP "Host unreachable" à la victime ($\Rightarrow$ déconnexion des session)
- Lan Attack : envoi de paquet TCP d'IP et port source identiques à ceux de la victime.
- Teardrop Attack : messages fragmentés contruits pour que les fragments se chevauchent et soient impossibles à reconstituer ($\Rightarrow$ crash)
- SYN Flood : innondation de demandes d'ouverture de session TCP.
- Evasive UDP Attack : innondation de paquets UDP de longueur variable et d'adresse source IP aléatoire vers la victime.
- mail bombing : avalanche d'e-mail sur le compte d'un utilisateur ou sur un serveur pour l'engorger.

DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Technique d'intrusion

1. Connexion à une ressource partagée
2. Attaque
   - Attaque par force brute
   - Attaque par débordement de tampon
   - Exploitation d'une faille logicielle
3. Accès à un interpréteur de commandes interactif
4. Élévation des privilèges
5. Installation d'un rootkit
6. Effacement des traces

+

- cassage de logiciel (Cracking)
- cryptanalyse
- rétro-ingénierie

DÉPARTEMENT Sciences Informatiques

Attaque par usurpation d'identité

Exemple : Attaque de Mitnick sur le réseau de Tsutomu Shimomura

- identification d'une machine de confiance du serveur victime
- choix d'une date propice pour l'attaque (Noël 1994)
- recherche de l'algorithme de génération d'identifiant de session TCP par envoi de SYN et RESET
- DoS de la machine de confiance par envoi de TCP SYN
- Envoi de segments TCP en usurpant l'identité de la machine de confiance et en prévoyant l'identifiant de session TCP utilisé.
- Utilisation de la connexion TCP pour modifier le .[sr]hosts de la machine
- Libération de la machine de confiance par envoi de TCP RESET

DÉPARTEMENT Sciences Informatiques

Piratage par rebond

- Interception d'un mot de passe en clair
- Utilisation du mot de passe pour se connecter à la machine
  - mots de passes enregistrés,
  - crack passwd
  - autorisation distantes depuis cette machine (.[sr]hosts, etc.)
  - reniflement du réseau de la machine pour intercepter d'autres mots de passes.

Sites clandestins et sites relais

1. Répertoire de stockage de document ouvert pour téléchargement (upload) ou piratage de compte
2. Fichiers inavouables mis à disposition d'autres pirates

$\Rightarrow$ Responsabilité de l'entreprise

3. Ce site sert de relai pour attaquer d'autres sites

$\Rightarrow$ Traçage difficile

Intrusion physique, Social Engineering

- mot de passe sous le clavier, écrit sur le tableau...
- social engineering

DÉPARTEMENT
Sciences Informatiques

- se tenir au courant
- connaître les systèmes d'exploitation
- connaître son infrastructure
- restreindre l'accès au réseau (pare-feu)
- réduire le nombre de points d'entrée (ports ouverts, machines accessibles)
- Supprimer les services, machines, utilisateurs inutiles
- définir une politique de sécurité interne (mots de passe, lancement d'exécutables)
- eduquer les utilisateurs
- déployer des utilitaires de sécurité (journalisation, statistiques, traces, tests d'intrusion)

Parades (1)

- Sensibilisation de l'utilisateur à la sécurité. La solidité d'une chaîne est égale à celle de son maillon le plus faible
- La sécurité est une affaire de compromis entre confort et sécurité un utilisateur frustré par les contraintes de sécurité aura tendance à les contourner (modem, wifi ...)
- Sauvegarde régulière des données, et identifiants uniques des outils systèmes (md5)
- Les logiciels, services, machines ... inutiles doivent être arrêtés ou supprimés.

Parades (2)

- Utilisation d'équipements adaptés (ex. switch plutôt que hub contre les renifleurs)
- Se mettre à jour sur les nouvelles failles de sécurité découvertes, et appliquer les correctifs aussitôt qu'ils sont disponibles (Ref : avis du CERT, bugstraq)
- Vérification de l'intégrité des logiciels (MD5, SHA256) et de leur provenance
- Vérification des sites accédés
  - certificats
- utilisation du chiffrement (ssh, VPN)
- Mettre en place une architecture de réseau bien pensé, et éventuellement un (ou des) firewall.

Une bonne sécurité = Bon sens + organisation + pédagogie

DÉPARTEMENT
Sciences Informatiques

Mise en place d'une architecture sécurisée

- un firewall restrictif
- une passerelle
- un traçage des connexions
- une gestion d'une DMZ
- différents services réseaux (FTP, HTTP, DNS ...) dont certains doivent pouvoir être accédés depuis l'extérieur.

DÉPARTEMENT
Sciences Informatiques

Filtrage IP

Les deux types de politiques pour un filtre sont :

- politique restrictive : ce qui n'est pas explicitement autorisé est interdit (souvent ce qui est mis en place dans les entreprises)
- politique permissive : ce qui n'est pas explicitement interdit est autorisé (ex : les réseaux "à la maison", certains réseaux d'université)

DÉPARTEMENT Sciences Informatiques

Types de parefeux

- Pare-feu sans état (stateless firewall) : regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.
- Pare-feu à états (stateful firewall) : vérifie que chaque paquet est bien la suite d'un précédent paquet et la réponse à un paquet dans l'autre sens.
- Pare-feu applicatif : Vérifie la complète conformité du paquet à un protocole attendu.
  - pour ouverture de ports dynamique (FTP)
  - contre ceux qui utilisent un tunnel TCP pour contourner le filtrage par ports.
  - mais couteux en ressource

Filtrage IP - parefeux sans état

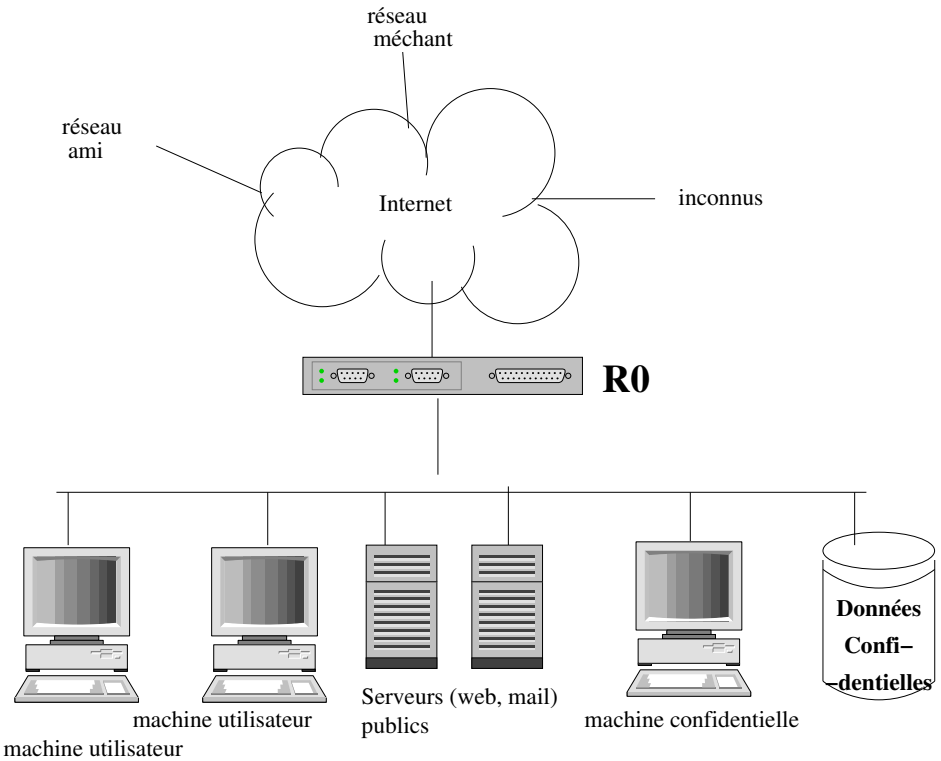
(Note : les règles sont parfois appelées ACL - Access Control List (CISCO), politique/policy (Juniper), filter/filtres, règles/rules)

- Le numéro en début de ligne correspond au numéro de la règle de filtrage.
- On juge du passage d'un paquet (s'il doit être autorisé, interdit, tracé), en évaluant les règles de filtrage par ordre CROISSANT
  - lorsqu'une condition est vérifiée, on exécute l'action correspondante (interdiction/autorisation) et on SORT du script.
  - L'ordre d'évaluation des règles a donc son importance.

DÉPARTEMENT Sciences Informatiques

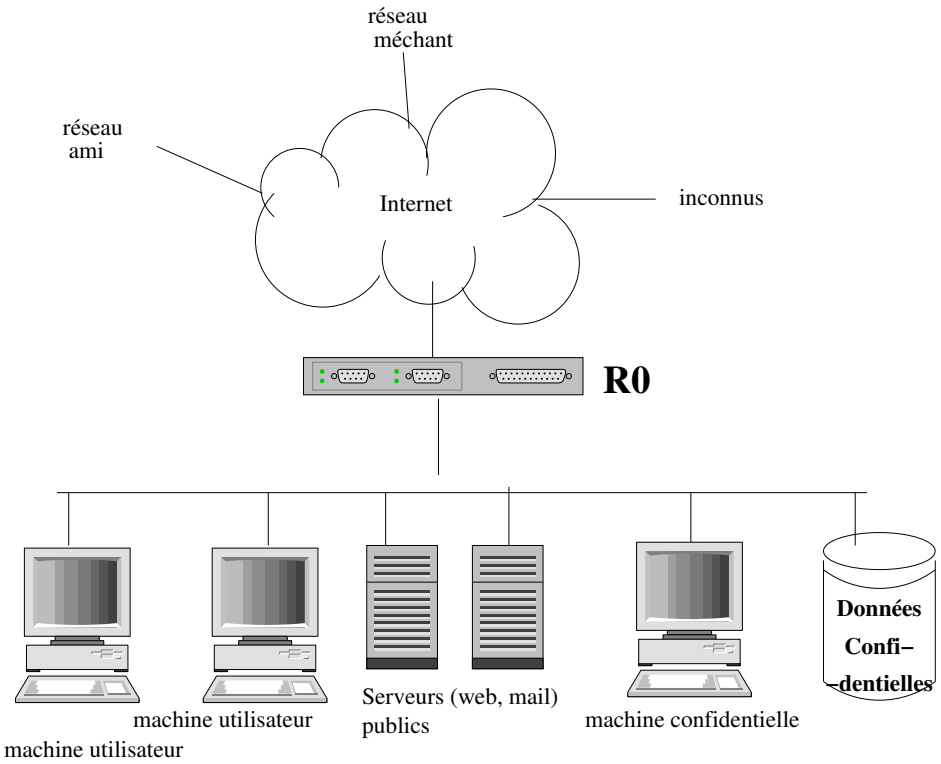
Filtrage IP

- filtrage sur les interfaces
- filtrage sur les sources
- filtrages sur les destinations
- filtrage sur les ports (donc les services)
- filtrage sur les paquets (protocole TCP / UDP / ICMP ...)
- traçage de la connexion (ce qui permet de repèrer un agresseur potentiel afin de pouvoir permettre à l'administrateur de prendre les mesures appropriées).



DÉPARTEMENT Sciences Informatiques

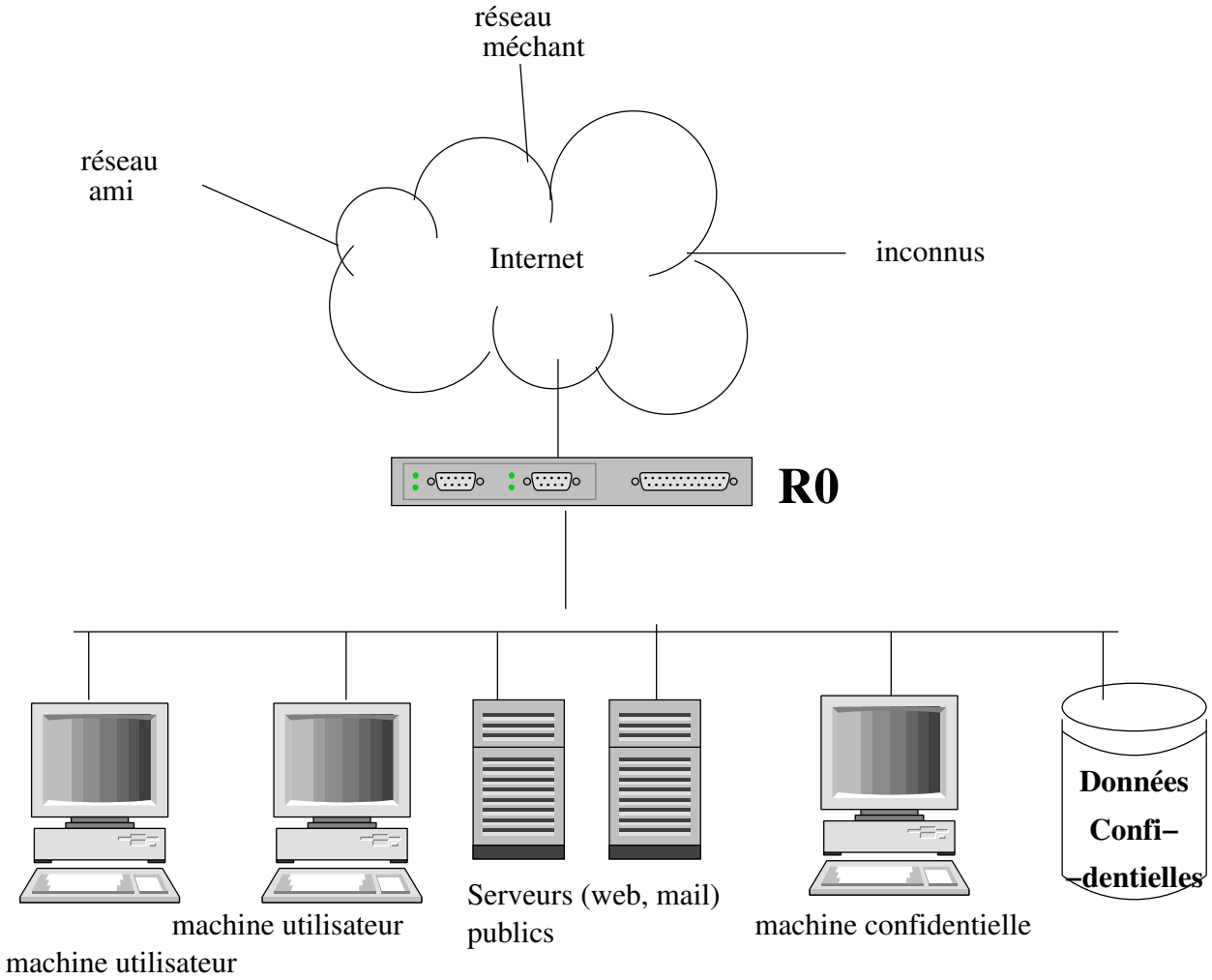
Règle de filtrage pour routeur 0




```
# Une connexion TCP établie est definitivement acceptée.
pass tcp from  any to  any established

# Toute connexion TCP établie depuis l'intérieur
# est autorisée
pass tcp from REZO to  any setup

# Connexion de l'extérieur à notre serveur de mail autori
pass tcp from  any to IP_S_MAIL 25 setup

# Acces de l'extérieur vers nos serveurs confidentiels in
pass tcp from  any to IP_CONFIDENTIEL1
pass tcp from  any to IP_CONFIDENTIEL2

# Connexion de l'extérieur à notre serveur web autorisé
pass tcp from  any to IP_S_MAIL 25 setup

# Requêtes DNS autorisées pour notre serveur DNS cache
pass tcp from IP_S_DNS to  any 53 setup
pass udp from  any 53 to IP_S_DNS 53
pass udp from IP_S_DNS to  any 53

# Autorisation des pings
pass icmp from  any to  any

# Tout paquet non reconnu est rejeté
# (politique restrictive)
deny all from  any to  any
```

DÉPARTEMENT
Sciences Informatiques

Règle de filtrage pour routeur 1



DÉPARTEMENT
Sciences Informatiques

Règle de filtrage pour routeur 1

```
# tout ce qui passe par l'interface de loopback
# (lo0) est acceptée
pass all from  any to  any via lo0

# un paquet à destination du réseau réservé
# au loopback (127.0.0.0/)  mais ne provenant pas
# de l'interface lo0 est invalide. On le rejette donc.
deny all from  any to 127.0.0.0/8

# Arreter le "spoofing"
deny all from REZO to  any in via INTERFACE_0-E

# Arreter les paquets de la RFC 1918
deny all from 192.168.0.0:255.255.0.0 to  any
deny all from  any to 192.168.0.0:255.255.0.0
deny all from 172.16.0.0:255.240.0.0 to  any
deny all from  any to 172.16.0.0:255.240.0.0
deny all from 10.0.0.0:255.0.0.0 to  any
deny all from  any to 10.0.0.0:255.0.0.0
```

```
# tout ce qui passe par l'interface de loopback (lo0) es
pass all from  any to  any via lo0

# Une connexion TCP établie est definitivement acceptée.
pass tcp from  any to  any established

# Toute connexion TCP établie depuis l'intérieur est auto
pass tcp from INET to  any setup
pass tcp from ONET to  any setup

# Connexion de l'extérieur à notre serveur de mail autori
pass tcp from  any to IP_S_MAIL 25 setup

# Connexion de l'extérieur à notre serveur web autorisé
pass tcp from  any to IP_S_MAIL 25 setup

# Requêtes DNS autorisées pour notre serveur DNS cache
pass tcp from IP_S_DNS to  any 53 setup
pass udp from  any 53 to IP_S_DNS 53
pass udp from IP_S_DNS to  any 53

# Autorisation des pings
pass icmp from  any to  any

# Tout paquet non reconnu est rejeté
# (politique restrictive)
deny all from  any to  any
```

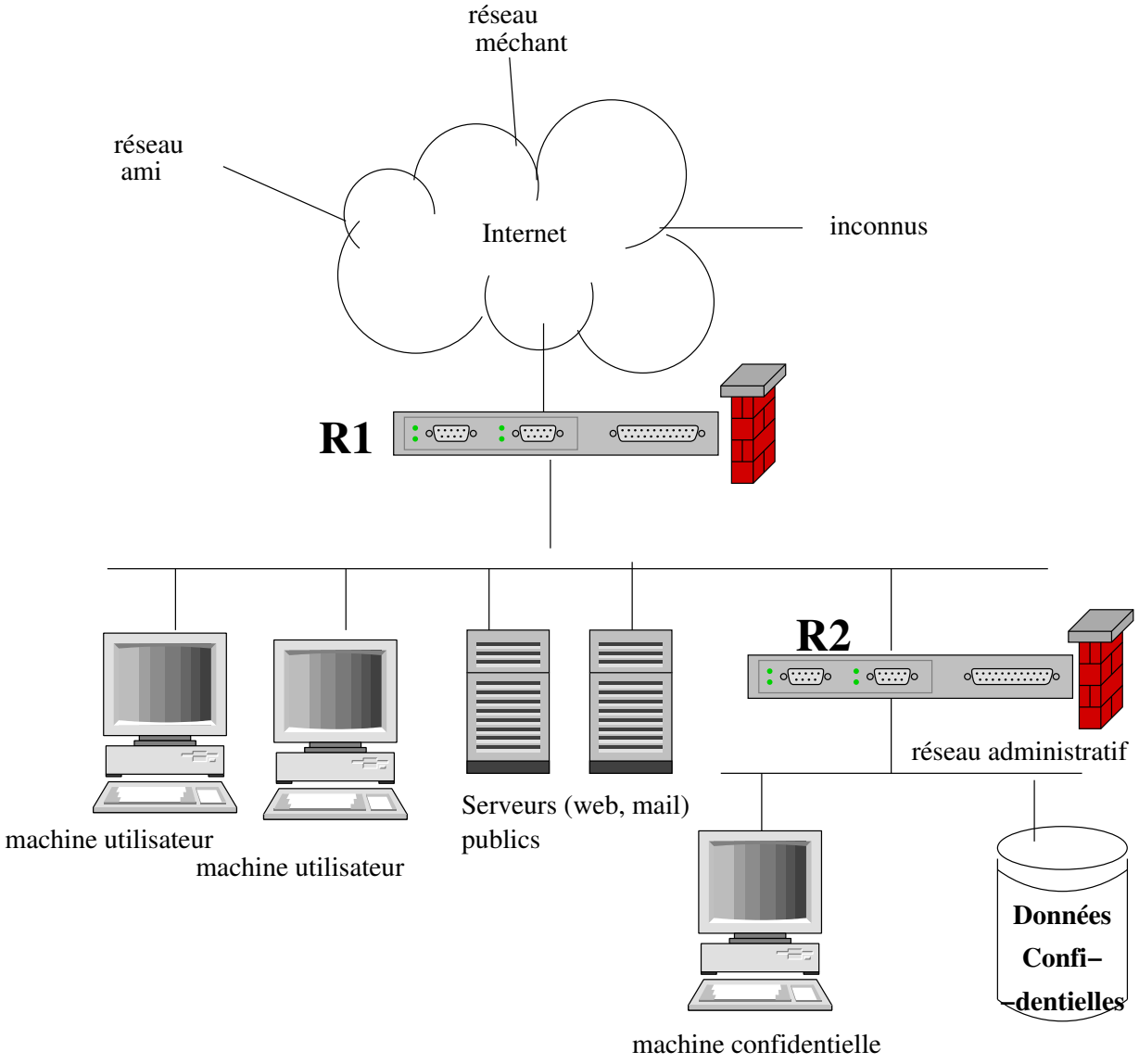
DÉPARTEMENT Sciences Informatiques

Règle de filtrage pour routeur 2

```
# tout ce qui passe par l'interface de loopback
# (lo0) est acceptée
pass all from  any to  any via lo0

# un paquet à destination du réseau réservé
# au loopback (127.0.0.0/)  mais ne provenant pas
# de l'interface lo0 est invalide. On le rejette donc.
deny all from  any to 127.0.0.0/8

# Arreter le "spoofing"
deny all from INET to  any in via INTERFACE_2-0
# Une connexion TCP établie est acceptée.
pass tcp from  any to  any established

# On interdit tout ce qui concerne l'acces à ce site
pass all from INET to IP_SERVEUR_JEUX
pass all from IP_SERVEUR_JEUX to INET

# On fait une confiance totale à cette machine
pass all from INET to IP_AMI
pass all from IP_AMI to INET

# On interdit les connexions vers ces ports (IRC)
pass all from INET to  any 6660-6669

# Toute connexion vers l'extérieur accepté
pass tcp from INET to  any setup

# Accès à notre DNS autorisé
pass tcp from INET to IP_SERVEUR_DNS 53 setup
pass udp from INET to IP_SERVEUR_DNS 53
pass udp from IP_SERVEUR_DNS 53 to INET

# Autorisation des pings
pass icmp from INET to
any icmptypes 8 # echo request
pass icmp from  any to INET icmptypes 0 # echo reply

# Autorisation des traceroutes depuis l'interieur
add pass udp from INET to  any 33434-33534
add pass icmp from  any to INET icmptypes 3, 11

pass udp from ONET to  any

# Tout paquet non reconnu est rejeté
deny all from  any to  any
```

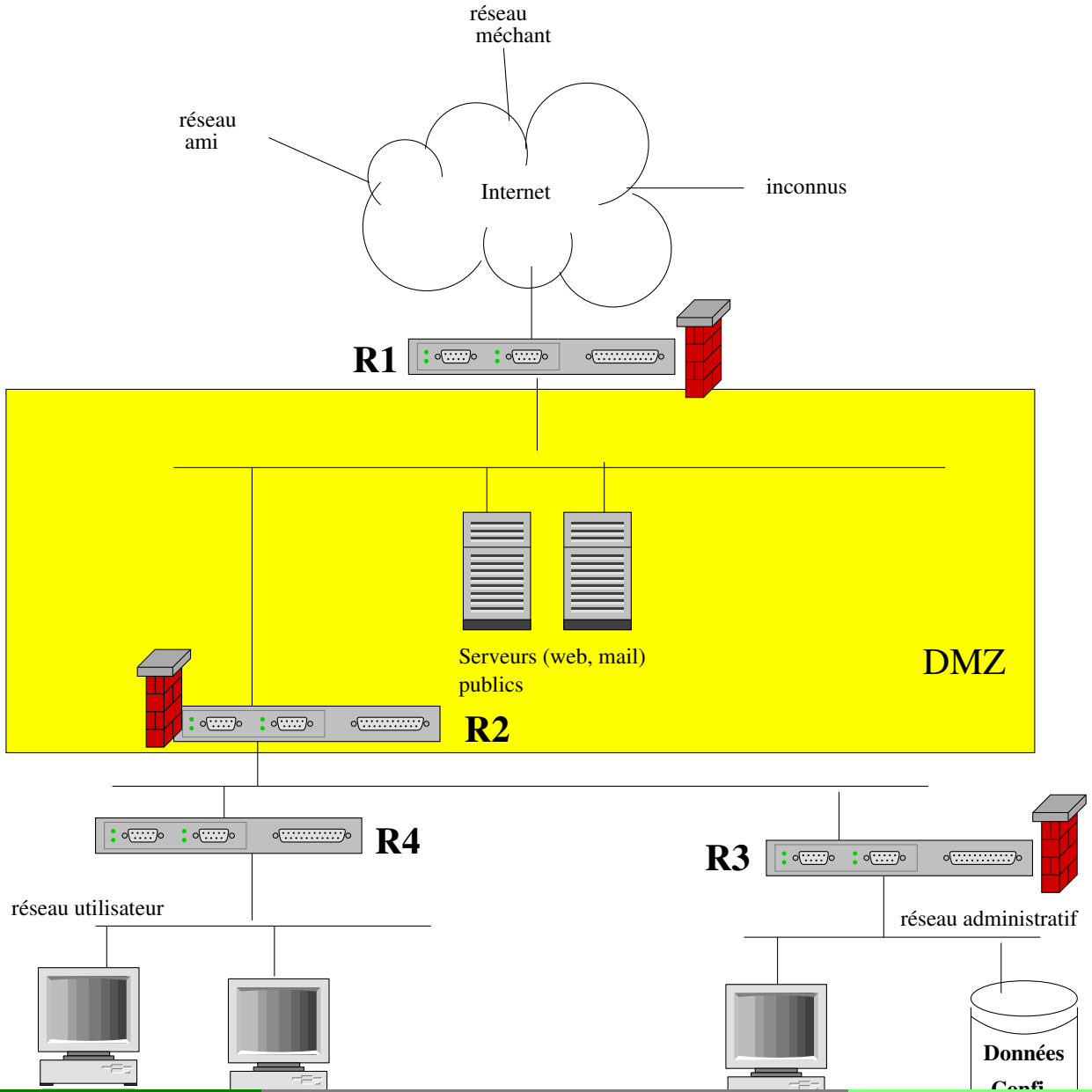
DÉPARTEMENT Sciences Informatiques

DMZ



DÉPARTEMENT
Sciences Informatiques

DMZ


réseau
méchant
réseau
ami
Internet
inconnus
R1
Serveurs (web, mail)
publics
DMZ
R2
R4
R3
réseau utilisateur
réseau administratif
Données

Zone démilitarisée (DMZ)

- Les services courants comme le serveur web, serveur FTP, gestionnaire de domaines (DNS) ... doivent être accessibles de l'extérieur suivant certains critères bien précis.
- Ces ouverture même contrôlées en font des trous de sécurité potentiels, ils doivent donc être placés dans un endroit "moins sécurisé" que l'on appelle DMZ.
- Une de ces machines mise dans la DMZ, si elle était attaquée, ne pourrait en aucune manière accèder au réseau interne (à cause du pare-feux miroetoile).
- Suivant la politique de sécurité décidé, le réseau interne doit pouvoir accéder librement aux services extérieurs ou non.
- Dans le cas négatif, la mise en place de relais applicatifs pourrait alors être mis en oeuvre via une autre machine sous placée dans la DMZ (SQUID, delegate, FWTK)

DÉPARTEMENT Sciences Informatiques

Gestion des services I

- Serveur de noms de domaines (DNS) : ainsi on peut affecter des noms à chaque machine et chaque sous-réseaux. Ceci en interne. Par sécurité, on peut aussi faire du relayage, afin que les postes clients internes ne puissent interroger que celui-ci pour résoudre les adresses DNS.
- le serveur WEB (http) : doit pouvoir être accessible de l'extérieur et de l'intérieur.
- Mandataire (*proxy*) : S'il faut une sécurité maximale et / ou de bonnes performances, on peut mettre en place un proxy (squid).
- Serveur de fichiers (FTP) : un FTP anonyme pour permettre aux clients et partenaires de déposer leurs logiciels, documents, mais aussi d'en charger.
- Serveur et gestionnaires de courrier (SMTP, POP, IMAP) : :
- Synchronisation du temps sur une horloge universelle (NTPD) :

DÉPARTEMENT Sciences Informatiques

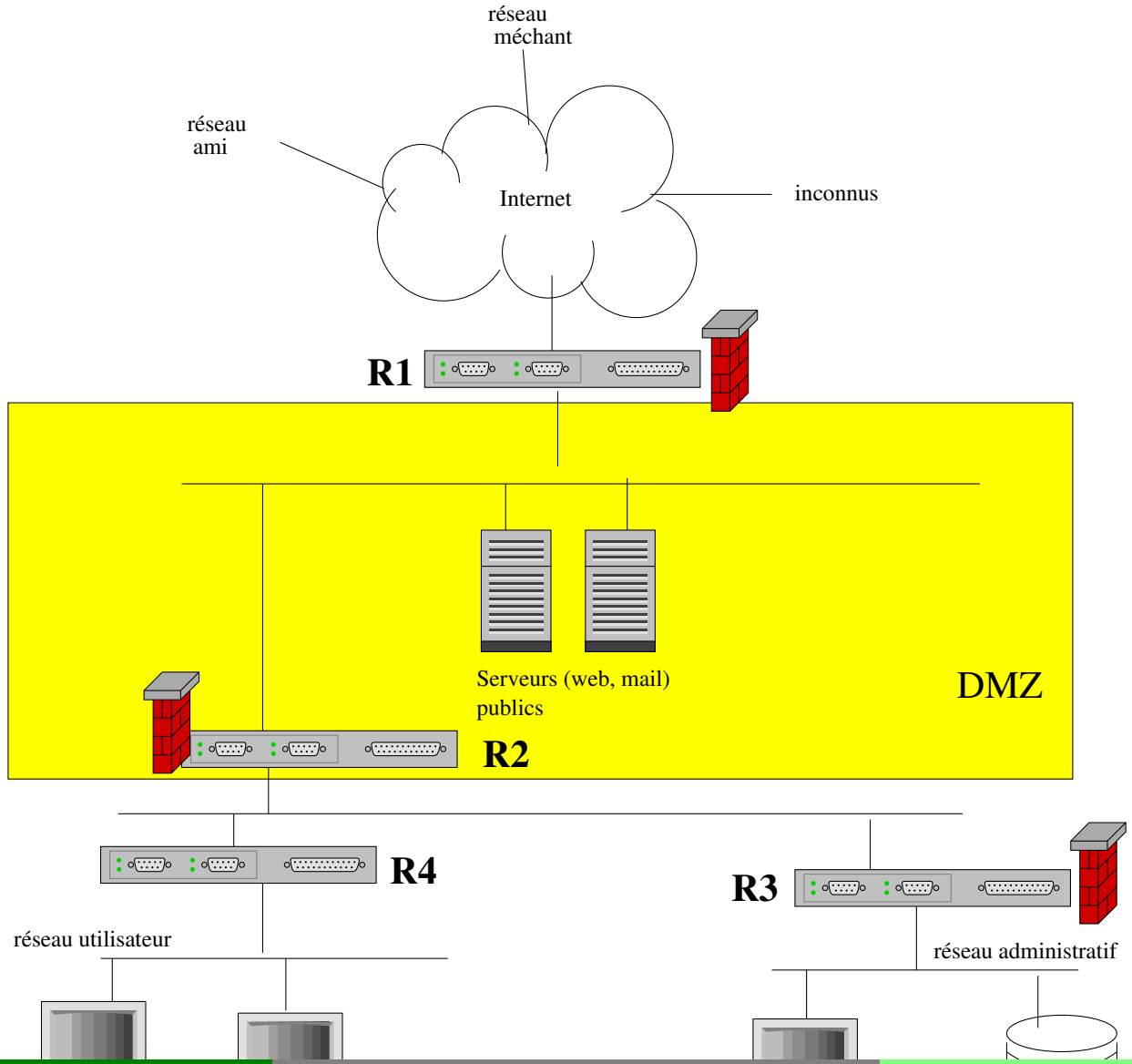
Gestion des services II

- partage des disques (NFS) :, Bases de données : à mettre sur un réseau INTERNE
- partage des disques et des imprimantes sur un réseau Microsoft (SMB) : à mettre sur un réseau INTERNE

DÉPARTEMENT Sciences Informatiques

Proxy

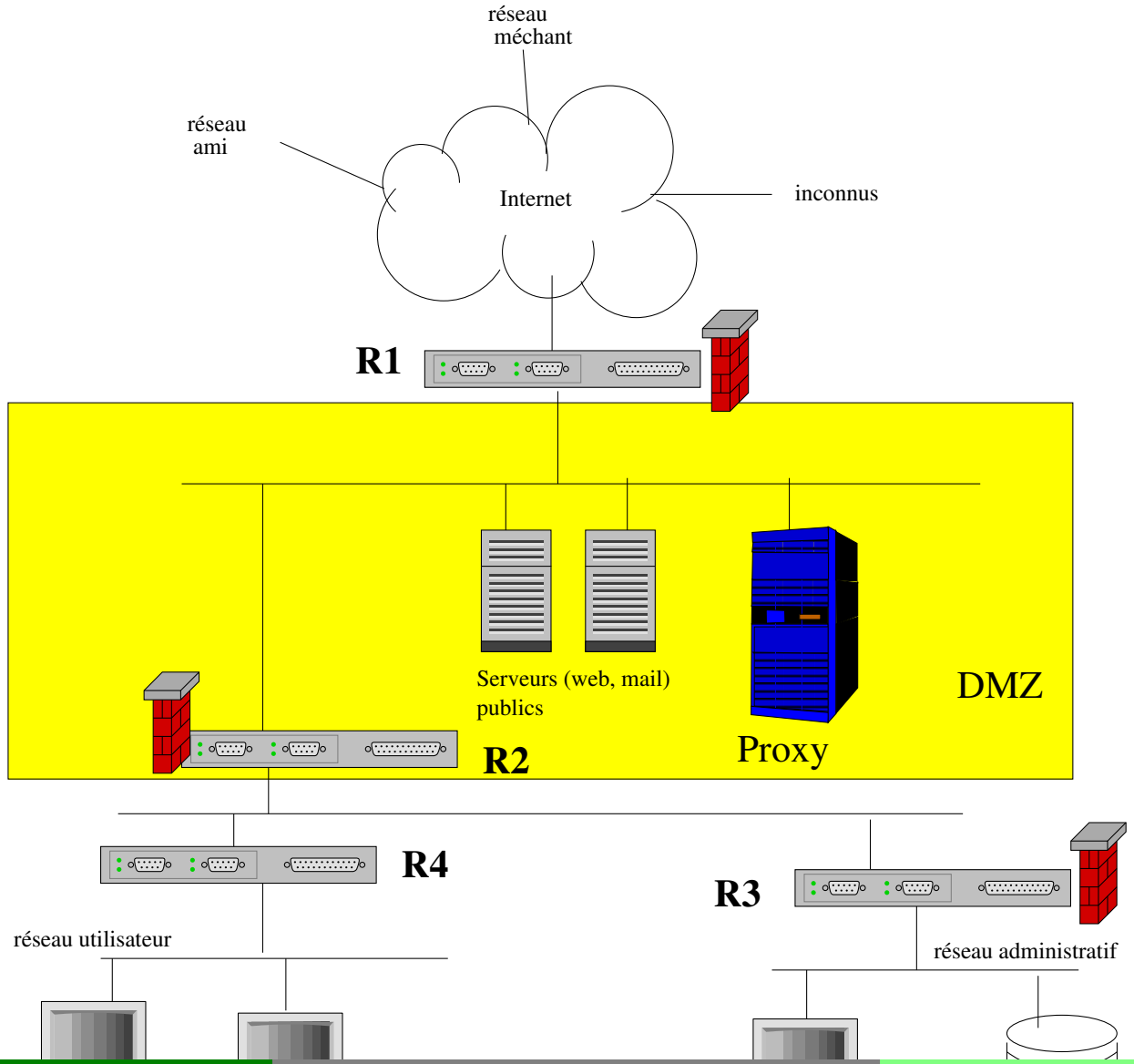
Pas de connexion directe entre l'intérieur et l'extérieur



DÉPARTEMENT
Sciences Informatiques

Proxy

Pas de connexion directe entre l'intérieur et l'extérieur



DÉPARTEMENT
Sciences Informatiques

Cryptographie

- contre les écoutes : Il faut chiffrer les données
  - de machine-à-machine de manière applicative : ssh, ssl, etc.
  - de machine-à-réseau ou de réseau-à-réseau : tunnel, VPN
- contre les usurpations d'identité : Il faut authentifier
  - Gestion de certificats
  - Challenge dans les protocoles

DÉPARTEMENT Sciences Informatiques

Traçage, journalisation

- tracer un maximum d'information (connexion, lancement de services, anomalies, etc.)
- ... mais de façon analysable (organiser l'info, la stocker de manière fiable et datée, rotation des logs pertinents, synthèse des résultats)
- remonter les alertes pertinentes (trop d'info tue l'info)

DÉPARTEMENT Sciences Informatiques

Que faire après une attaque ?

- garder son calme
- archiver, tracer, isoler tout ce qui peut l'être
- avertir les autorités compétentes
- colmater la faille, vérifier TOUS les systèmes (voire les réinstaller)
  - corriger immédiatement les effets de la contamination et supprimant la contamination elle-même.
  - Rechercher la causes en amont.
  - Prévoir les conséquences en aval, les conséquences éventuelles de son action à l'encontre de notre machine, nos données, notre réseau, notre entreprise et nous même

DÉPARTEMENT
Sciences Informatiques

Arsenal législatif

Chasser les idées reçues

- Internet n'est pas « une zone de non-droit »
- Il n'y a pas de « vide juridique »
- Il y a plutôt un « trop plein non adapté »

DÉPARTEMENT
Sciences Informatiques

Arsenal législatif

Lois spécifiques à l'informatique :

- Loi 78-17 du 6 janvier 1978 : (dite « Loi Informatique et Libertés ») : protection des libertés individuelles
- Loi 85-660 du 3 juillet 1985 : droit d'auteur
- Loi 88-19 du 5 janvier 1988 : (dite « Loi Godfrain ») : fraude informatique sur le fondement d'une atteinte à un système de traitement automatisé de données (STAD)
- Loi 90-1170 du 30 décembre 1990 : réglementation de la cryptologie
- Loi du 29/07/1881 (modifiée en 1986) : lois régissant la presse qui ne dépassent pas le cadre de la liberté d'expression (Cass., Crim., 16/12/1986)
- Loi du 10/07/1991 : : secret des correspondances
- articles 9 et 226-1 à 226-8 du Code civil, tout individu jouit d'un droit au respect de sa vie privée ainsi que d'un droit à l'image,.

DÉPARTEMENT Sciences Informatiques

Arsenal législatif

Toutes les lois générales s'appliquent également, en particulier :

- diffusion de propos à caractère raciste
- diffusion d'images pédophiles

Comment les appliquer ?

- images pédophiles dans les news, site à caractère raciste, Qui est responsable ? gérants d'ISP mis en examen (article 227/23 du code pénal)

DÉPARTEMENT
Sciences Informatiques

Arsenal législatif

La protection des biens informatiques :

- Les logiciels
- Les machines (matériel)
- Les inventions

DÉPARTEMENT
Sciences Informatiques

Acteurs institutionnels en France

- Police nationale, Gendarmerie, DST, etc
- Haut fonctionnaire de défense : un par ministère
- DISSI (Délégation Interministérielle pour la Sécurité des Systèmes d'Information)
  - dépend du premier ministre
  - organe de décision et d'organisation
- SCSSI (Service Central de la Sécurité des Systèmes d'Information)
  - dépend de la DISSI
  - pour les services de l'Etat
- CNIL (Commission Nationale de l'Informatique et des Libertés)
  - organe indépendant

DÉPARTEMENT Sciences Informatiques

Au niveau international

- aucune législation véritablement internationale concernant la criminalité informatique.
- la loi du pays dans lequel le crime est constaté s'applique.

$\Rightarrow$ un pirate américain attaquant un serveur en France via une machine située en Allemagne ?
$\Rightarrow$ un pirate Ukrainien attaquant un serveur en France via une machine située au Vénézuela via une machine situé au Gabon via une machine situé en Birmanie ?

DÉPARTEMENT Sciences Informatiques

1. Motivation
2. Facteurs d'insécurité
   - L'humain & sa machine
3. Programmes malveillant
   - Cheval de Troie
   - Vers
   - Virus
   - Espions
   - Portes dérobées : backdoor
4. attaque par courrier électronique
5. Attaque sur le réseau
   - Ecoute des connexion (Sniffing)
   - Mystification (spoofing)
   - Déni de services (DoS)
6. Technique d'intrusions
7. Parade
8. Architecture sécurisée
   - Filtrage IP - Pare-feux
   - Liste d'accès

DÉPARTEMENT
Sciences Informatiques

Ingénieur sécurité : c'est un métier !

- maîtriser les systèmes
- maîtriser les réseaux
- mettre à jour (avis du CERT, MAJ)
- pédagogue
- être organisé
- et surtout du bon sens

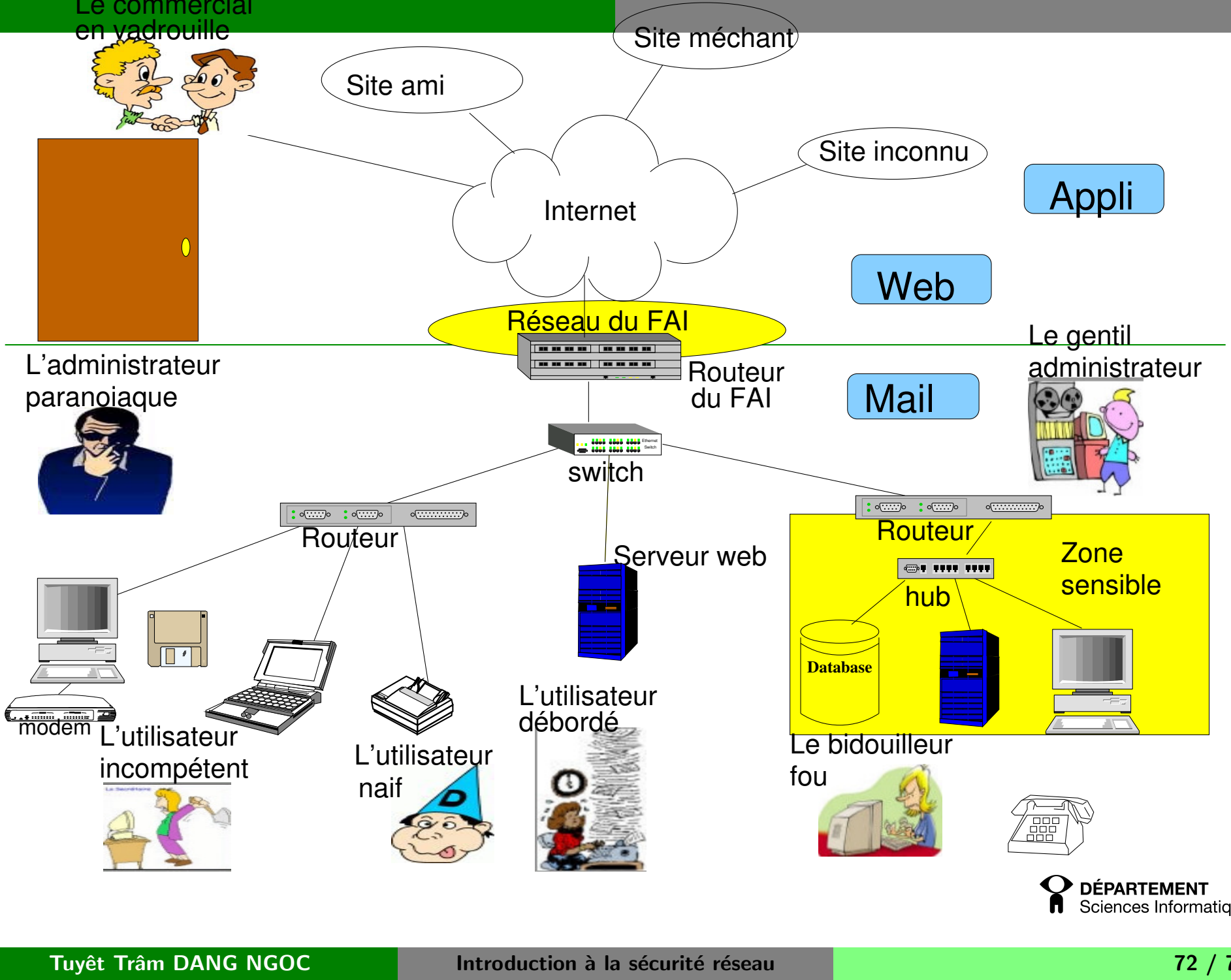
$\Rightarrow$ On a toujours besoin d'un ingénieur sécurité.
$\Rightarrow$ Rentable à long terme.

DÉPARTEMENT
Sciences Informatiques

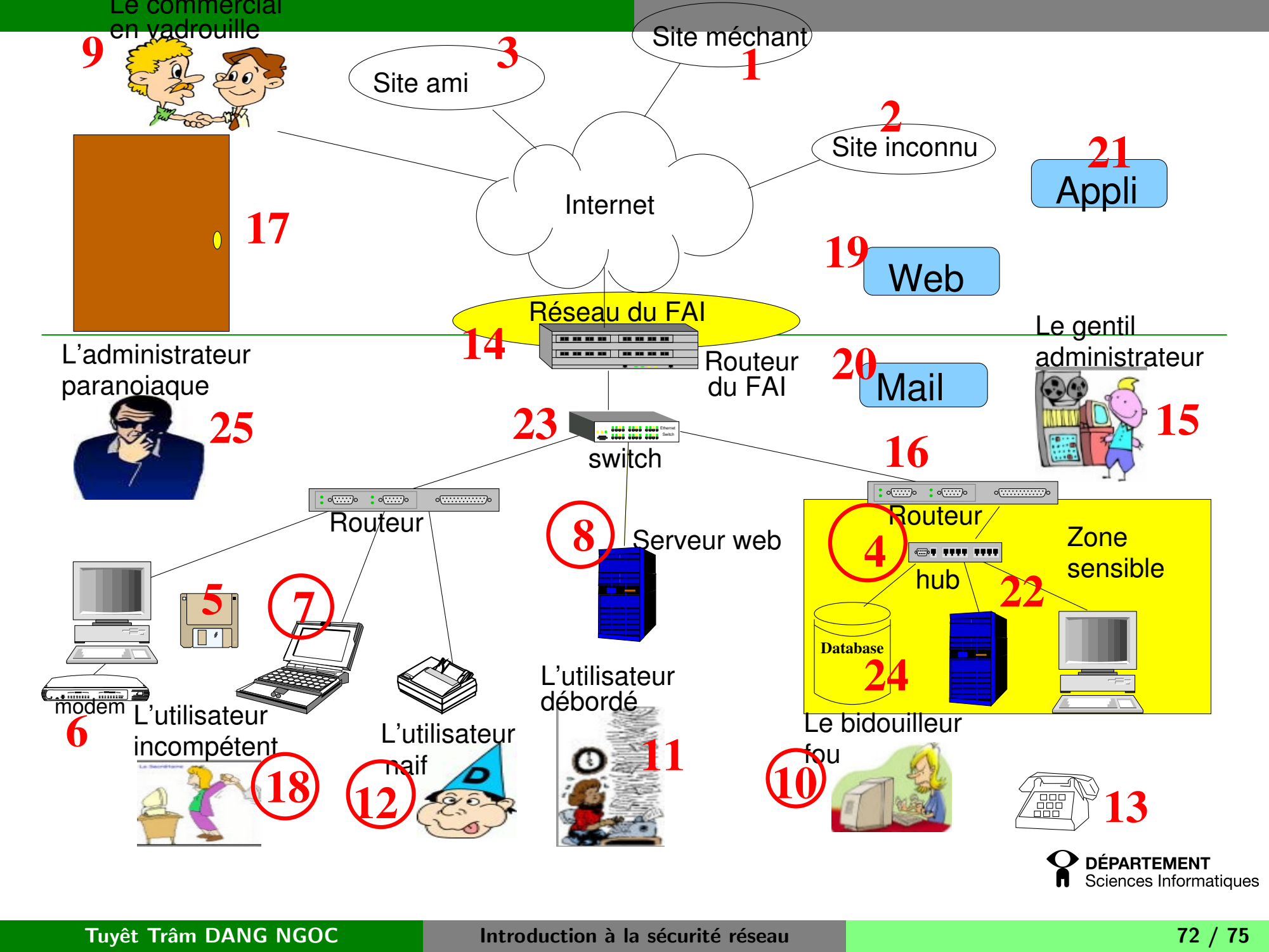
Jeu ! ! !

Dans les dessins suivants : cherchez les failles de sécurité potentielles ! ! !

DÉPARTEMENT
Sciences Informatiques

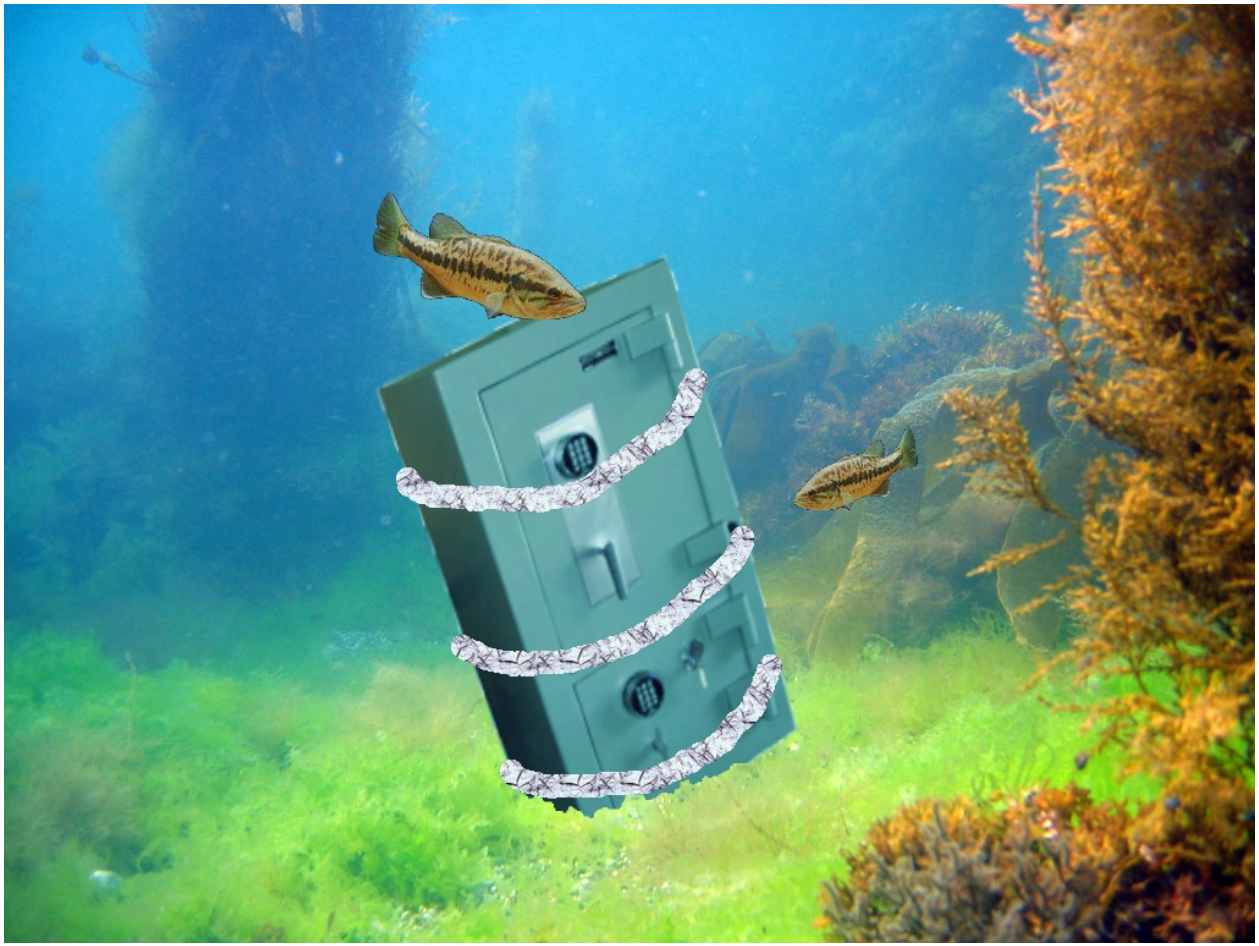


DÉPARTEMENT Sciences Informatiques



DÉPARTEMENT Sciences Informatiques

Une sécurité (presque) absolue



DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

Crédits

Ce cours a largement été inspiré du support de cours de Pierre David, Maître de conférences à l'université de Strasbourg.
Les définitions proviennent de l'encyclopédie collaborative wikipédia.