Sécurité avancée des réseaux

Concepts fondamentaux de la sécurité

IUT d'Auxerre
Département RT
2ème année 2013-2014
ZHANG Tuo
tuo.zhang@u-bourgogne.fr
http://www-l2ti.univ-paris13.fr/~zhang/

Organisation UE SECUR

•Quoi?—Cours

1.Concepts fondamentaux

2.Cryptographie

3.Filtrage de paquets

•Pourquoi?—TDs

1. Algorithme de Crypto (RSA etc..)

2. ACL, SSL/TLS, SSH, IPsec etc.

•Comment?—TPs

1. ACL Cisco & Pare-feu Linux

2. Cryptographie

3. SSL/TLS

4. VPN & IPsec

Examen:

40% TPs(2*4=8 points)

60% Contrôle écrit(12 points)

Outline

- Introduction générale
- Pourquoi la sécurité est importante?
- Les définitions
- Menaces de sécurité courante
- Type d’ attaque d’ un réseau
- Techniques générales d’ atténuation des risques
- Stratégie de sécurité de l’ entreprise

Introduction générale

Qu'est que la sécurité ?

Recouvre tout ce qui concerne la protection du système d'information

- Consiste à assurer qu'une personne qui modifier ou consulte des données du système en a l'autorisation et qui peut le faire correctement car le service est disponible

- Fonction incontournable des réseaux

Pourquoi les systèmes sont vulnérables?

- La sécurité est chère et difficile
- Un système ne peut être sûr à 100%
- La stratégie de sécurité est complexe et basée sur des jugements humains
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes (*errare humanum est !*)

Les enjeux de la sécurité

- Maîtriser le Transport, le Traitement et le Stockage du Patrimoine Numérique Industriel, Intellectuel et Culturel
  - ➔ Politique (souveraineté)
  - ➔ Technologie maîtresse : cryptologie
- Valoriser les Contenus
  - Multimédia, Logiciel, «Intellectual Properties», Base de Données
  - Assurer la libre circulation des contenus en toute confiance
  - Disséminer les oeuvres, Rétribuer les auteurs, Essaimer le savoir-faire
  - ➔ Économique
  - ➔ Technologie maîtresse : tatouage et cryptologie
- Instaurer (ou Restaurer) la confiance dans l'univers numérique
  - e-commerce, e-business, e-content, e-government, e-vote, e-democracy
  - ➔ Social (usage, lutter contre la fracture numérique)
  - ➔ Technologie maîtresse : infrastructure de confiance (distribuer des secrets et des certificats)
- Sécuriser **les infosphères**
  - L'individu (liberté, intimité) : protéger
  - L'entreprise (banques, transport, santé) : prévenir
  - Les infrastructures critiques et leurs interdépendances (effet de cascades des catastrophes en chaîne) : poursuivre la cyber-criminalité
  - ➔ Liberté, droits élémentaires, civilisation
  - ➔ Technologies maîtresses : ingénieries matérielle, biométrique, informatique, des réseaux,

Pourquoi un système ne peut être sûr à 100% ?

- Il est impossible de garantir la sécurité totale d'un système pour les raisons suivantes:

  - Les bugs dans les programmes courants et les systèmes d'exploitation sont nombreux
  - La cryptographie a ses faiblesses : les mots de passe peuvent être cassés
  - Même un système fiable peut être attaqué par des personnes abusant de leurs droits
  - On peut s'attaquer aux systèmes de sécurité eux-mêmes…

Pourquoi la sécurité des réseaux est-elle importante ?

PRISM

- **PRISM**, également appelé **US-984XN**
- Ce programme classé, relevant de la National Security Agency (NSA), prévoit le ciblage de personnes vivant hors des États-Unis
- Création par président Bush après 911.

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.
  (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

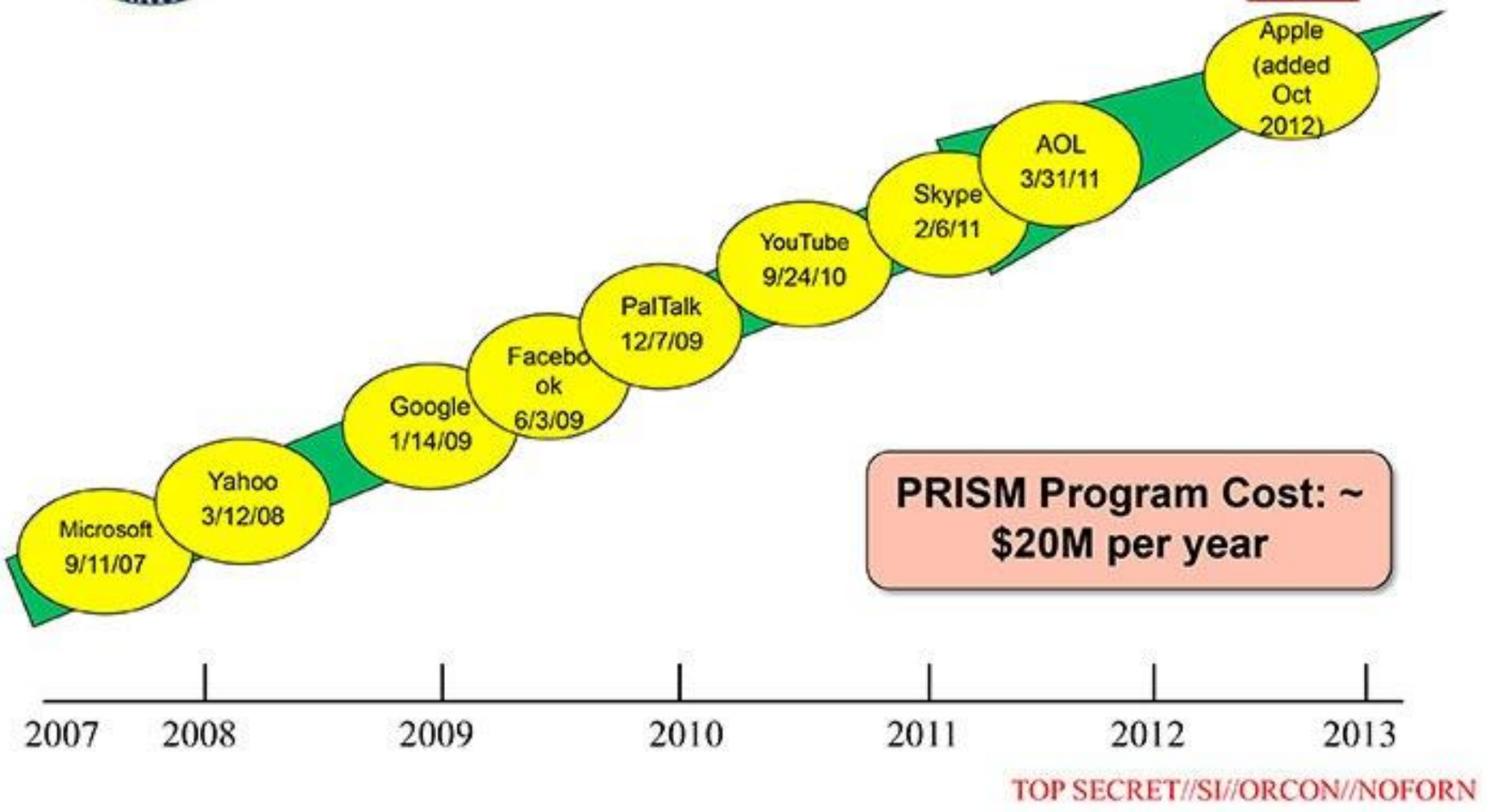
You Should Use Both

PRISM

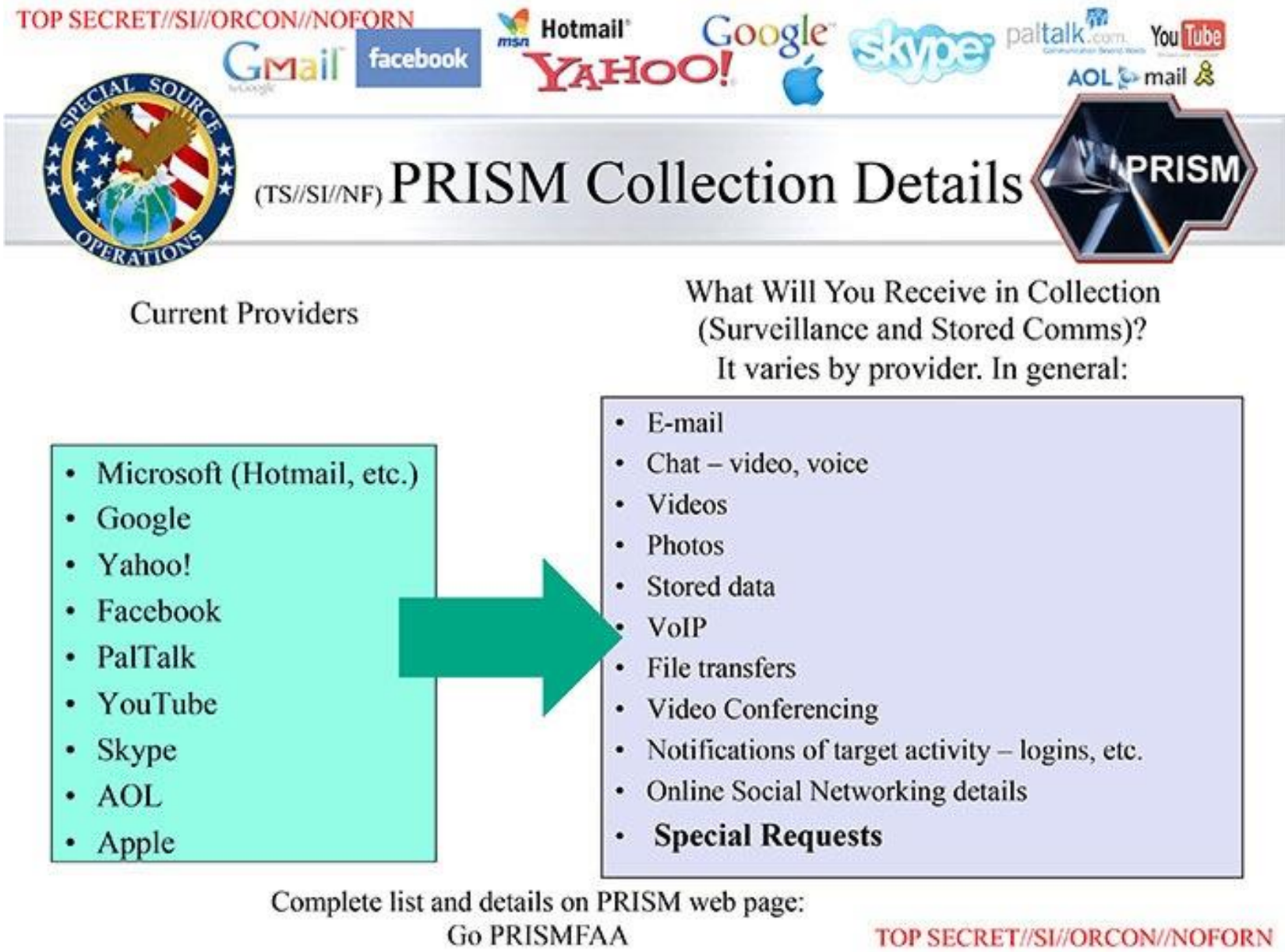
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

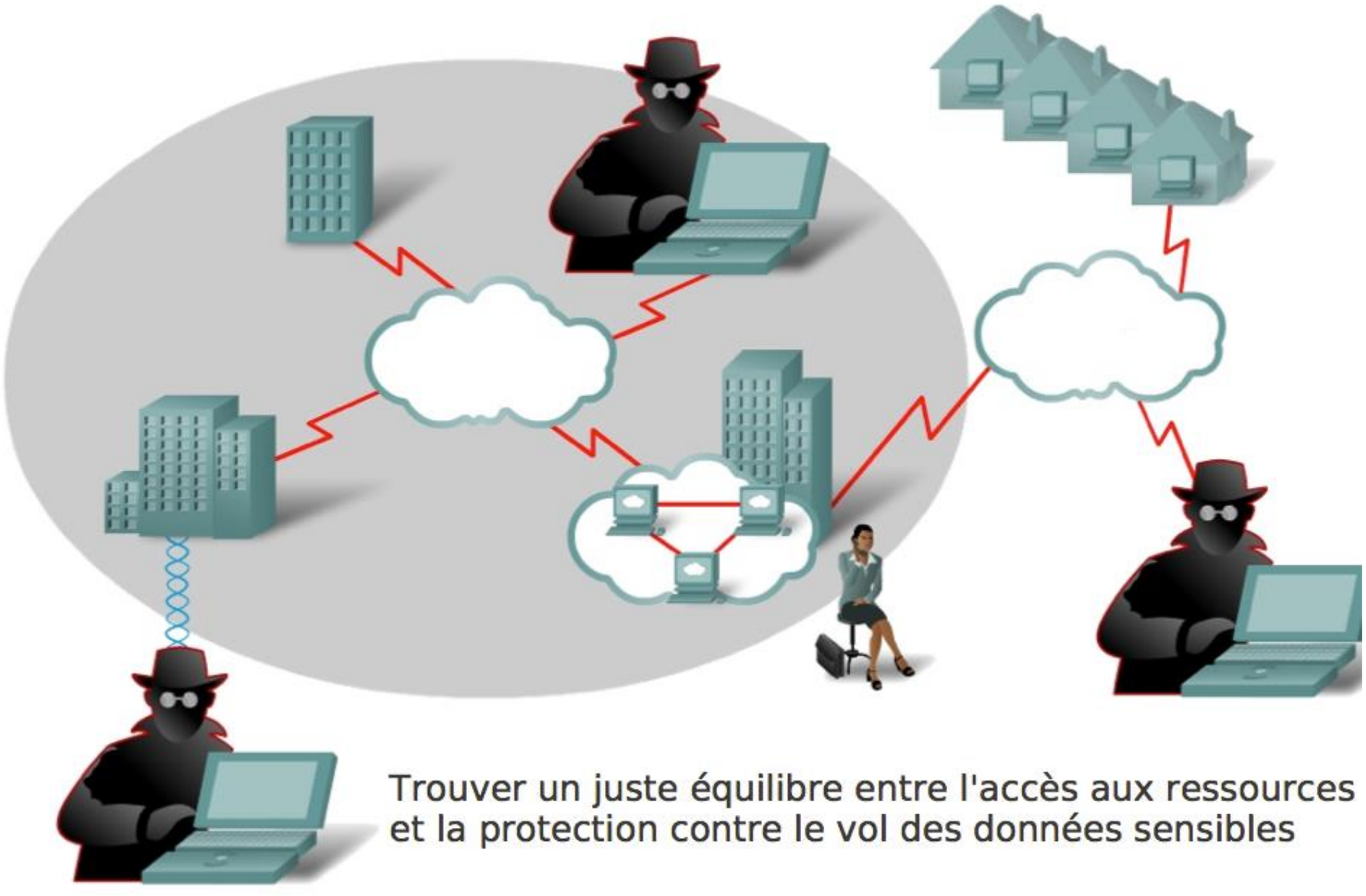


TOP SECRET//SI//ORCON//NOFORN



En juin 2013, le quotidien britannique *The Guardian* affirme, à la suite des révélations d'Edward Snowden, que la NSA dispose d'un accès direct aux données hébergées par les géants américains des nouvelles technologies, parmi lesquels Google, Facebook, YouTube, Microsoft, Yahoo!, Skype, AOL et Apple. Barack Obama le présente comme un outil de lutte antiterroriste.

Pourquoi la sécurité des réseaux est-elle importante ?



Trouver un juste équilibre entre l'accès aux ressources et la protection contre le vol des données sensibles

Pourquoi la sécurité des réseaux est-elle importante ?

- Types d'assaillant
  - Fouineur (*white hat*)
  - Bidouilleur (*hacker*)
  - Pirate informatique (*black hat / cracker*)
  - Pirate téléphonique (*phreaker*)
  - Spammeur
  - Hameçonneur (*phisher*)

Pourquoi la sécurité des réseaux est-elle importante ?

- Pensez comme l'assaillant
  - Le but de l'assaillant est de compromettre un réseau ou une application s'exécutant dans un réseau
  - *Étape 1 :* Analyse d'empreinte (page Web, adresse IP...)
  - *Étape 2 :* Énumération des informations (WireShark...)
  - *Étape 3 :* Manipulation des utilisateurs pour obtenir un accès (mot de passe...)
  - *Étape 4 :* Escalade des privilèges
  - *Étape 5 :* Collecte d'autres mots de passe et secrets
  - *Étape 6 :* Installation de portes dérobées (port TCP...)
  - *Étape 7 :* Exploitation du système compromis

Pourquoi la sécurité des réseaux est-elle importante ?

- Types de délits informatiques :
  - Accès abusif au réseau par des personnes autorisées
  - Virus
  - Vol d'équipement mobile
  - Hameçonnage où une organisation est usurpée par l'expéditeur
  - Abus de messagerie instantanée
  - Déni de service
  - Accès non autorisé à des informations
  - Robots au sein de l'organisation
  - Vol de données des clients ou des employés
  - Accès abusif à un réseau sans fil
  - Intrusion dans un système
  - Fraude financière
  - Interception de mots de passe
  - Enregistrement des frappes
  - Dégradation d'un site Web
  - Abus d'une application Web publique
  - Vol d'informations propriétaires
  - Exploitation du serveur DNS d'une organisation
  - Fraude aux télécommunications
  - Sabotage

Les définitions

Sécurité, Protection, Dissuasion

- Sécurité (Security)
  - Quête d'indépendance vis à vis d'un péril, d'une peur, d'un piège, d'une menace, d'un risque, d'un doute, d'une crainte
  - Confidentialité, Intégrité, Disponibilité
- Protection (Protection)
  - Ensemble de mécanismes et de politiques nécessaires (pas suffisantes) pour atteindre la sécurité
- Dissuasion (Deterrence)
  - Ensemble de mécanismes et de politiques nécessaires (pas suffisantes) pour décourager un adversaire potentiel
  - Défense fondée sur la crainte de ripostes que le propriétaire peut faire subir à des agresseurs éventuels
  - Inciter un attaquant potentiel à abandonner son projet

Politique de sécurité(Informatique)

- Une politique de sécurité
  - Ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein de l'organisation
  - un ensemble de règles qui spécifient les autorisations, interdictions et obligations des sujets (agents)
    - (notion qui inclut à la fois les utilisateurs et les applications)
  - qui peuvent accéder au système informatique
- Une politique de sécurité
  - doit permettre d'exprimer des exigences
    - de confidentialité (pas de consultation illégale d'information)
    - d'intégrité (pas de création, de modification ou de destruction illégale d'information) et
    - de disponibilité (ne pas pouvoir empêcher que les autres agents puissent avoir un accès légitime à certains services ou ressources du système).

Fonctionnalité de sécurité

- exigences de sécurité pour maintenir la confidentialité, l'intégrité, la disponibilité d'un système ou d'un produit

- mise en place de mesures techniques(fonctions dédiées à la sécurité)

— identification et authentification, contrôle d'accès ,protection des données

— Audit, protection des mécanisme de sécurité

Identification et Authentification

- fonctions destinées à établir et vérifier une identité annoncée
- exigences pour la détermination et le contrôle des utilisateurs qui sont autorisés à avoir accès aux ressources contrôlées par la cible
  - implique d'établir l'identité annoncée par un utilisateur
  - vérifier que cet utilisateur est bien la personne qu'il prétend être (le sujet fournira à la cible une information que la cible sait être associée au sujet en question)
    - fonctions: ajouter de nouvelles identités, éliminer, invalider d'anciennes identités
    - permettre à des utilisateurs autorisés de contrôler les informations nécessaires pour vérifier l'identité d'utilisateurs
    - fonctions pour assurer l'intégrité des informations d'authentification
    - limiter la possibilité d'essais répétés d'établissement d'une fausse identité

Contrôle d'accès

- exigences pour garantir que les utilisateurs (et les processus qui agissent pour le compte de ceux-ci) sont empêchés d'accéder aux informations et aux ressources auxquelles ils ne sont pas autorisés à accéder ou auxquelles ils n'ont pas besoin d'accéder
  - exigences concernant la création ou la modification (y compris la suppression) non autorisées d'informations
  - fonctions destinées à contrôler les flux d'informations entre utilisateurs, processus
  - cela inclut l'administration (l'octroi ou le retrait) des droits d'accès et leur vérification
  - fonctions servant à établir et entretenir les listes et règles qui régissent les droits d'effectuer différents types d'accès

Politique de Contrôle d'accès

- Accès aux services & contenus
  - Identification & Authentification
  - Fédérations des solutions pour transcender l'hétérogénéité
  - Pare-feu : goulets d'étranglement
    - Signature électronique, graffiti sur paquets
- Autorisation, Délégation
- Outils de Gestion des Droits

Stratégie de sécurité

Ensemble de principes qui guident les prises de décision et permettent aux dirigeants d'une organisation de déléguer l'autorité en toute confiance

Développement d'une stratégie de sécurité

- Informer les utilisateurs, le personnel et les responsables de leur obligation de protéger les données vitales et les ressources technologiques de l'entreprise
- Spécifier les mécanismes permettant de respecter ces exigences
- Fournir une base de référence à partir de laquelle acquérir, configurer et auditer les systèmes informatiques pour qu'ils soient conformes à la stratégie

Mécanisme de de sécurité

- ***Mécanisme de sécurité***
  - Logique, algorithme ou protocole qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité.
  - Assure que le système ne rentre pas dans un état non autorisé
  - Exemple : mécanismes d'authentification
    - Mots de passe à usage unique
    - Biométrie
    - Protocole de type défi-réponse

➡ Les mécanismes de sécurité doivent eux-mêmes être sécurisés

Développement d'une stratégie de sécurité

- Norme ISO / CEI 27002
- Évaluation des risques
- Stratégie de sécurité
- Organisation de la sécurité des informations
- Gestion des biens
- Sécurité liée aux ressources humaines
- Sécurité physique et environnementale
- Gestion opérationnelle et gestion des communications
- Contrôle d'accès
- Acquisition, développement et maintenance des SI
- Gestion des incidents liés à la sécurité des informations
- Gestion de lac continuité de l'activité
- Conformité

Menaces de sécurité courante

Menaces(1/2)

- ***Source de Menaces***
  - Origine d'une menace
  - Type
    - Humain (utilisateur ou hacker), élément naturel (fleuve, …)
    - Cause accidentelle ou délibérée (***attaquant***)
    - Interne vs externe
  - Potentiel d'attaquant (dans le cas d'une cause délibérée)
    - Motivation
    - Expertise (compétences techniques, …)
    - Ressources disponibles (moyens financiers, temps, …)
  - Modèle (formel) d'attaquant
    - Modèle de Dolev-Yao (pour les protocoles cryptographiques)

Menaces(2/2)

- ***Menace (threat)***
  - Moyen type utilisée par une source de menace
    - Menaces délibérées (attaques) ou involontaires (erreurs ou incidents)
  - Exemples :
    - Crue d'un fleuve,
    - Vol de supports ou de documents,
    - Ecoute passive,
    - Piégeage du logiciel
    - Attaque par débordement de tampon, …

Objectifs de sécurité,menaces

- Quelles sont les objectifs et les menaces ?
  - Politique de sécurité d'un individu
    - Intimité numérique : confidentialité
  - Politique de sécurité pour une entreprise
    - Intégrité du système d'information
  - Politique de sécurité pour une grande entreprise multi site
    - Disponibilité du réseau
  - Politique de sécurité d'une grande organisation (administration, état, etc)
    - Disponibilité du système
  - Politique de sécurité vis à vis d'Internet
    - Contenus illicites
    - Politique de contrôle d'accès des flux entrants
  - Politique d'accès à des contenus
    - Filtrage

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Sources des problèmes de sécurité les plus courants:***
  - Introduction de nouvelles fonctionnalités
  - Possibilité de contournement du contrôle d'accès
  - Vérification incorrecte de la syntaxe ou de la taille d'arguments
  - Erreur dans la gestion d'appels/interruptions systèmes
  - Situation de concurrence (race condition)
  - Faille dans la conception/implémentation d'un protocole

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Introduction de nouvelles fonctionnalités***
  - Le besoin de fonctionnalités facilitant l'installation, l'utilisation d'un système peut se révéler néfaste du point de vue de la sécurité
  - Exemple : programme *sendmail* sous Unix
    - Une des sources de l'attaque du Ver Internet (Morris Worm, 1988)
    - Besoin : faciliter le travail de l'administrateur du système de messagerie en lui permettant de configurer à distance la messagerie d'un poste
    - Fonctionnalité : un mode « debug » activé au niveau d'un poste destination, permettait d 'inclure dans un mail une séquence de commandes que sendmail exécutait sur le poste destination
    - Le ver utilisait ce mode pour se copier sur une nouvelle machine
    - Correction : configurer correctement les postes en supprimant le mode debug

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Introduction de nouvelles fonctionnalités***
  - Le besoin de fonctionnalités facilitant l'installation, l'utilisation d'un système peut se révéler néfaste du point de vue de la sécurité
  - Exemple : programme *sendmail* sous Unix
    - Une des sources de l'attaque du Ver Internet (Morris Worm, 1988)
    - Besoin : faciliter le travail de l'administrateur du système de messagerie en lui permettant de configurer à distance la messagerie d'un poste
    - Fonctionnalité : un mode « debug » activé au niveau d'un poste destination, permettait d 'inclure dans un mail une séquence de commandes que sendmail exécutait sur le poste destination
    - Le ver utilisait ce mode pour se copier sur une nouvelle machine
    - Correction : configurer correctement les postes en supprimant le mode debug

Solution: déclarer */usr/spool/atjobs* comme non lisble

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Vérification incorrecte de la syntaxe ou de la taille d'arguments***
  - Non vérification de la taille d'arguments
    - Attaque par débordement de tampon : permet de réécrire des zones mémoires contenant des informations liées à la sécurité
    - Exemple : Commande *finger* sous Unix 4BSD (Internet Worm of 1988)

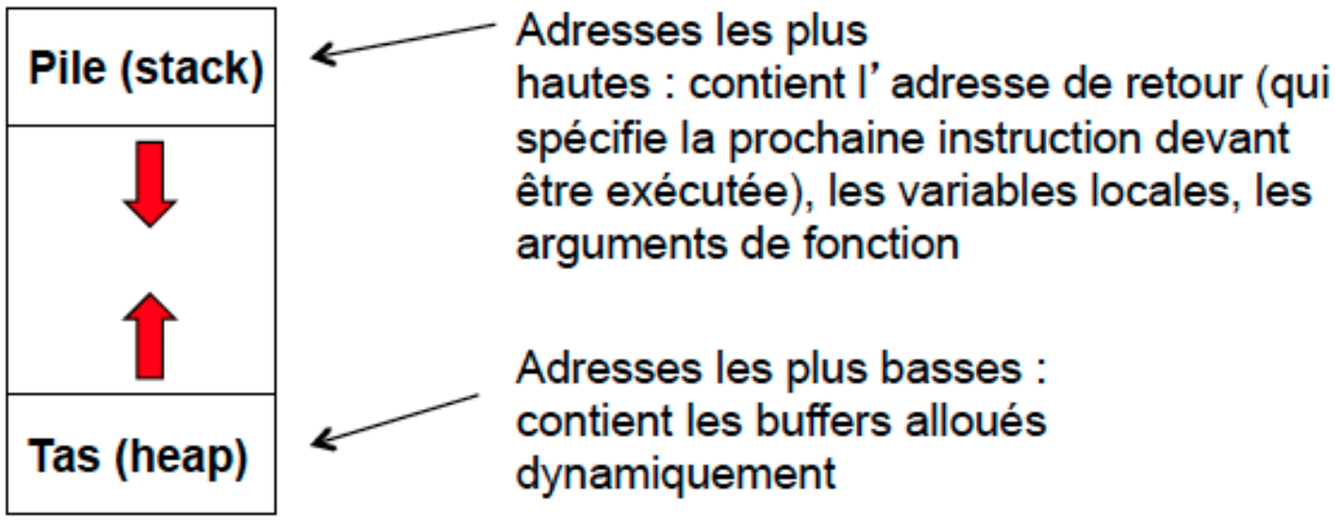
– Démon fingerd : sert des requêtes finger distantes,

– fingerd utilise la fonction gets, qui prend ses arguments dans un tampon sans en vérifier la taille

– Avec un message de 356 bits il est possible de faire exécuter un bout de code qui lance un shell via TCP avec les droits de fingerd

Menaces de sécurité courantes
1.Vulnérabilité usuelles

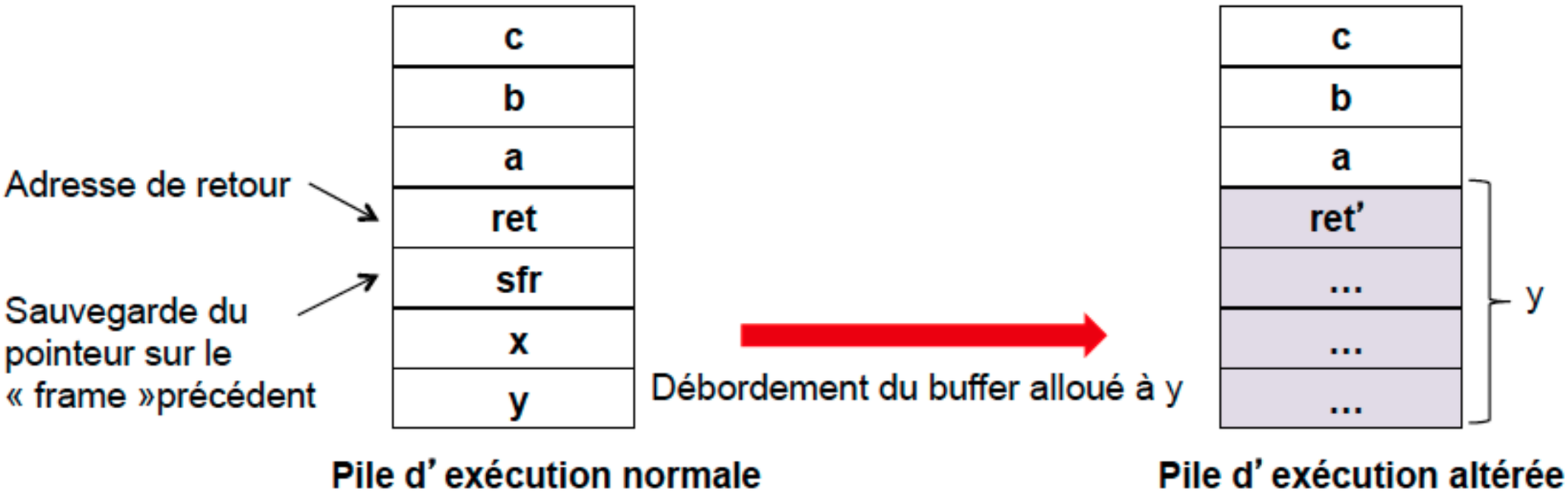
- ***Débordement de tampon (Buffer overrun)***
  - Configuration de la mémoire



- Si la valeur affectée à une variable dépasse la taille du buffer allouée :
  - peut causer une erreur d'exécution
  - peut permettre à de faire exécuter son code en écrasant la mémoire de la pile jusqu'à l'adresse de retour du processus en cours d'exécution

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Dépassement de pile = débordement de tampon sur la pile***
  - Exemple fonction avec trois arguments a, b, c et deux variables locales x et y



- ret' = adresse du code de l' attaquant
- Le code peut être passé en argument de la fonction pour qu' il soit stocké sur la pile
- Le code de l' attaquant s' exécute alors avec les privilèges du processus courant

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Vérification incorrecte de la syntaxe d'arguments***
  - Exemple : attaque par injection de code SQL
    - Contexte : une application traite des requêtes SQL à une base de données via une page Web

```
String sql = "select * from client where name = '"+ name +"' »
```

- L'intention est de traiter des requêtes de la forme

```
select * from client where name = 'Bob'
```

- Si l'attaquant peut entrer, `name = Bob' OR 1=1 --`, la requête devient :

```
select * from client where name = 'Bob' OR 1=1
```

(`--` est interprété comme le début d'un commentaire)

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Faille dans la conception/implémentation d'un protocole***
  - Certains choix ou erreurs de conception ou d'implémentation dans les protocoles peuvent introduire des problèmes de sécurité
  - Exemple : Inondation de requêtes SYN « SYN Flooding » :
    - L'attaquant envoi un grand nombre de requêtes TCP SYN sur une cible (un serveur) et n(acquitte jamais les réponses
    - La cible accumule les requêtes SYN, jusqu'à atteindre la limite de connexions ouvertes (à demi)
    - Toute nouvelle requête légitime sera refusée par la cible

➡ Crée un Deni de service

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Faille dans la conception/implémentation d'un protocole (suite)***
  - Exemple : « TCP session hijacking »
    - Ouverture de session TCP entre un client A et un serveur B

      A → B : SYN, ISSa *(ISSa, ISSb : numéro de séquence de 32 bits)*

      B → A : SYN/ACK, ISSb, ACK(ISSa) *(ACK(ISSa)=ISSa+1)*

      A → B : ACK,ACK(ISSb)
    - On suppose que les messages parviennent toujours aux serveurs et ne peuvent être observés : l'attaquant ne peut que forger des messages avec de fausses adresses
    - Les numéros de séquences initiaux sont aléatoires
    - RFC793 : le compteur doit être incrémenté toutes les 4 microsecondes
    - Cependant dans certaines implémentations : incrémenté toutes les 128s seulement
  - Attaque : X ouvre une première session avec B, reçoit ISSb, puis spoofe l'adresse IP de A

    X/A → B : SYN, ISSc

    B → A : SYN/ACK, ISSb', ACK(ISSc) *X ne voit pas ce message*

    X/A → B : ACK(ISSb') *mais X devine la valeur d'ISSb' grâce à ISSb*
    + TCP SYN Flooding sur A
    - *X peut exécuter des commandes sur le serveur B avec les privilèges de A, mais ne peut obtenir les résultats*

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Autres exemples d'attaques réeaux***
  - Attaque par réflexion (« Smurf »)
    - Envoyer une requête ICMP « echo » à un ou plusieurs serveurs de diffusion (« broadcast) avec une adresse IP source correspondant à la cible de l'attaque ;
    - Le serveur de diffusion répercute la requête sur l'ensemble du réseau ;
    - Toutes les machines du réseau renvoient une réponse au serveur de diffusion ;
    - Le serveur de diffusion redirige les réponses vers la cible.
    - → crée un Deni de Service (DoS) sur la cible

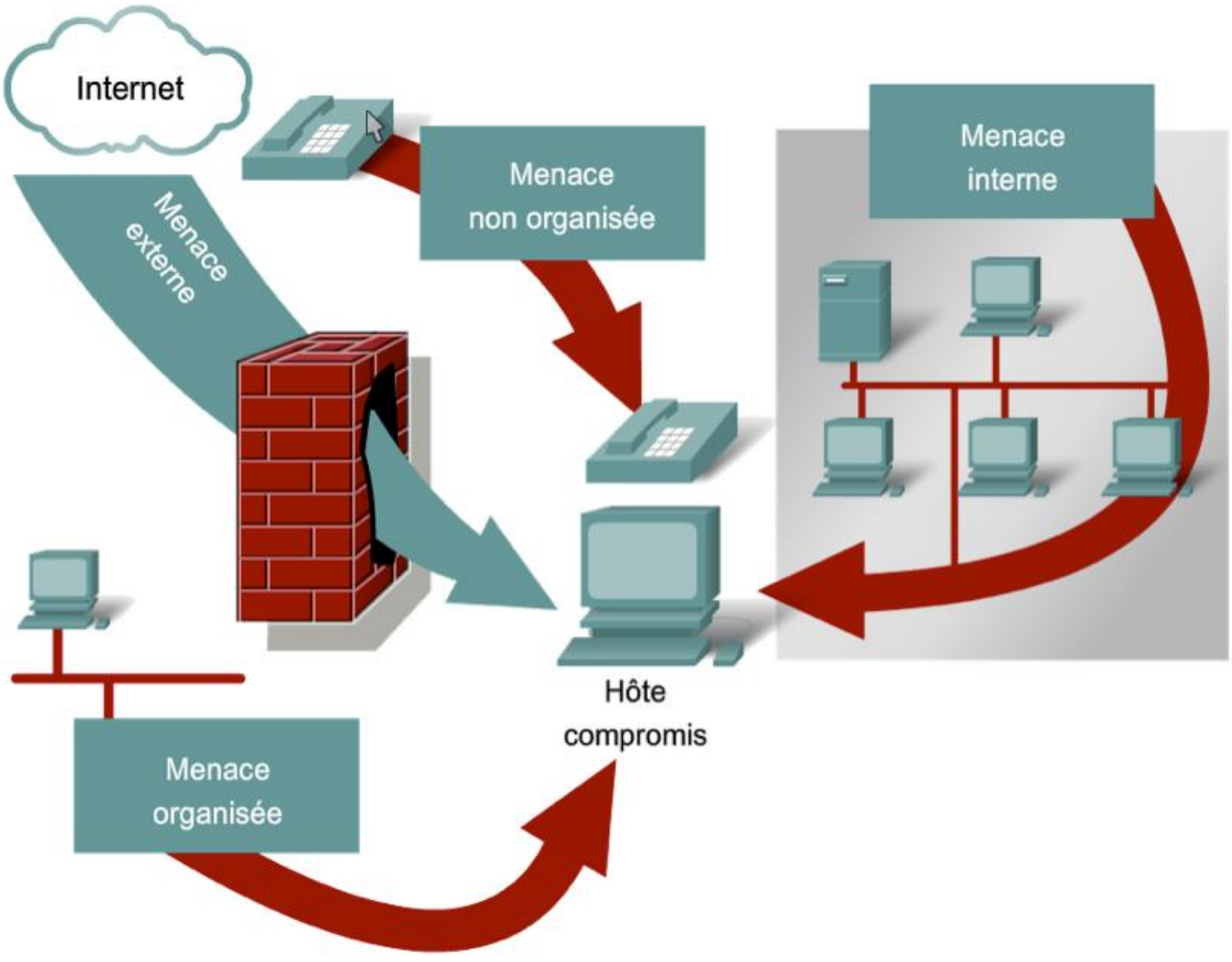
  - Attaques sur le serveur DNS (Domain Name System)
    - Fait le lien entre nom de domaine et l'adresse IP
    - DNS « cache poisoning » : inclure des fausses informations dans le cache du DNS
    - Permet de rediriger des pages web vers un autre site

Menaces de sécurité courantes
1.Vulnérabilité usuelles

- ***Attaque sur les mécanismes de décurité : exemple SSL/TLS***
  - Faille (historique) dans le générateur de nombre aléatoire
    - Goldberg and Wagner, Dr. Dobb's Journal, Jan. 1996.
    - http://www.ddj.com/documents/s=965/ddj9601h/
  - Timing attacks
    - L'analyse de temps de réponses d'un serveur OpenSSL permet à un attaquant dans un même segment de LAN de dériver la clef privée du serveur
    - Boneh and Brumley, 12th Usenix Security Symposium. http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html
  - Problème dans le rapport d'erreur
    - Exploite une mauvaise implémentation du "padding" dans le mode CBC
    - Des différences de temps de réponses du serveur dans le cas d'erreurs permet de retrouver un texte en clair
    - Vaudenay & alii, Crypto2003. http://lasecwww.epfl.ch/php_code/publications/search.php?ref=CHVV03

Menaces de sécurité courantes

Menaces envers les réseaux



Menaces de sécurité courantes

Piratage psychologique

- Ne demande aucune compétence en informatique
- Exploite des faiblesses personnelles (ego, faux documents...)
- Attaques par « Hameçonnage »(Phishing= Phreaking+fishing)
  - Messages non sollicités pour tenter d'obtenir par la ruse des informations confidentielles (numéros de carte de crédit, mots de passe…)
  - Le hameçonneur se fait passer pour une institution de confiance qui aurait un besoin légitime de ces données sensibles
  - Il est possible de lutter contre le hameçonnage en informant les utilisateurs et en leur prodiguant des conseils à suivre lorsqu'ils reçoivent des messages suspects
  - Les administrateurs peuvent également empêcher l'accès à certains sites Web et configurer des filtres de blocage du courriel suspect

Attention:

Le phishing en action

Cooling, Tammy (ASD-N)
À : Undisclosed recipients:;
WEBMASTER EMAIL HELP

tammy.cooling@nbed.nb.ca
Copier l'adresse
Ajouter aux VIP
Nouvel e-mail
Ajouter à Contacts
Rechercher « Cooling, Tammy (ASD-N) »

4 mars 2014 10:43
Masquer les détails

Information Technolog … new
website accounts. Thi … reatly
Increased amount of e-mail correspondence in your e-mail account and
also reduce spam emails that is received in your email on the daily
basis. Your account has been selected, as one of the accounts that are
to be upgraded. Please click the link below and follow the instruction
to upgrade your email account.

| | | | | | CLICK HERE<http://www.tuinenjeroencogen.be/helpdesk/upgrade.php>

The new minimum quota level for e-mail accounts will be set to 10 G.
Cooling, Tammy (ASD-N) ITS
© Copyright 2014 | WEBMASTER EMAIL HELP DESK • • ALL RIGHTS RESERVED.
CONFIDENTIALITY NOTICe

HelpDesk
À : undisclosed-recipients:;
Répondre à : noreply@webmaster.edu
Email Notice!

3 mars 2014 00:10
Masquer les détails

WEBMASTER EMAIL ACCOUNT UPGRADE.

Information Technology Services (ITS) are currently updating our new website accounts. This will provide you the ability to store a greatly Increased amount of e-mail correspondence in your e-mail account and also reduce spam emails that is received in your email on the daily basis. Your account has been selected, as one of the accounts that are to be upgraded. Please click the link below and follow the instruction to upgrade your email account.

CLICK HERE

The new minimum quota level for e-mail accounts will be set to 10 G.

Sara Malott ITS
Copyright 2014 | WEBMASTER EMAIL HELP DESK ALL RIGHTS RESERVED.
CONFIDENTIALITY NOTICE

[personnels] PHISHING 25 Février 2014 9:00

Expéditeur : Franck DEHER
À: Liste de l'ensemble des personnels DIJON AUXERRE

Bonjour,

et encore un nouveau mail de phishing qui circule :

Expéditeur : administrateur système
Envoyé à l'aide de : Zimbra 8.0.4_GA_5737 (zclient/8.0.4_GA_5737)

Votre boîte aux lettres a dépassé la limite de stockage de 2.GB
Créé par l'administrateur est actuellement 2,30 Go, ne peut pas
envoyer ou recevoir de nouveaux messages jusqu'à ce que vous re-valider votre e-mail

Cliquez sur le lien ci-dessous pour valider votre adresse e-mail

http://servicedemessagerie6.yolasite.com/ <----NE PAS CLIQUER !

merci
administrateur système

SURTOUT, NE PAS CLIQUER SUR L'URL PROPOSEE !!

Bien cordialement,

Sujet : {Spam?} Votre compte de Credit Mutuel
De : dient-access@cmmd.creditmutuel.fr <client-access@cmmd.creditmutuel.fr>
Réponse à : dient-access@cmmd.creditmutuel.fr
Date : 18/11/2006 09:54
Pour : undisclosed-recipients:;

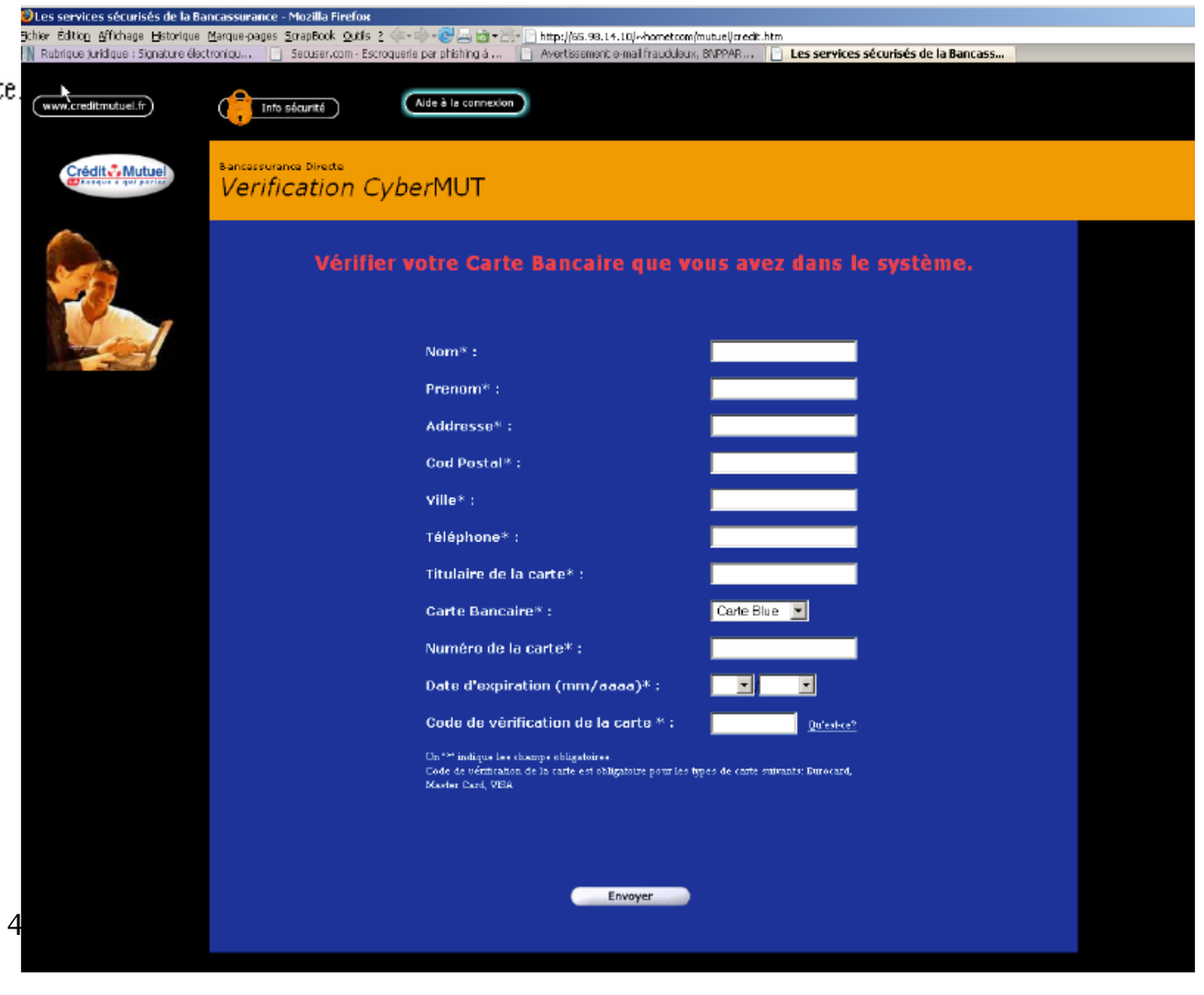
Cher Client de CreditMutuel

En raison des erros multiple de login, votre accиs a CreditMutuel a йtй temporairement fermй.Protйger la sйcuritй de votre compte et du rйseau de CreditMutuel est notre inquiйtude primaire.

Donc, comme une mesure prйventive, nous avons limitй temporairement l'accиs aux caractйristiques sensibles de votre compte avec CreditMutuel.
Si vous кtes le titulaire lйgitime du compte, s'il vous plaot login a **MailScanner soupçonne le lien suivant d'être une tentative de fraude de la part de "www.webhost119.com"** http://www.creditmutuel.com/client-access/, comme nous essayons de vйrifier votre identitй.

Merci pour votre patience comme nous travaillons ensemble a protйger votre compte.

En cliquant…



Types d’attaque d’un réseau

Types d'attaque d'un réseau

Catégories principales d'attaques :

Reconnaissance

- Découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou encore la découverte de leurs vulnérabilités
- Collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque
- Similaire au repérage effectué par un cambrioleur à la recherche d'habitations vulnérables, comme des maisons inoccupées, des portes faciles à ouvrir ou des fenêtres ouvertes

Accès

- Possibilité pour un intrus d'accéder à un périphérique pour lequel il ne dispose pas de compte ou de mot de passe
- Implique généralement l'utilisation d'un moyen de piratage, d'un script ou d'un outil exploitant une vulnérabilité connue de ce système ou de l'application attaquée

Types d’attaque d’un réseau

Catégories principales d’attaques :

Déni de service (*DoS*)

- Désactivation ou altération d'un réseau, des systèmes ou des services dans le but de refuser le service prévu aux utilisateurs normaux
- Les attaques par déni de service mettent le système en panne ou le ralentissent au point de le rendre inutilisable.
- Le déni de service peut consister simplement à supprimer ou altérer des informations.
- Dans la plupart des cas, l’attaque se résume à exécuter un programme pirate ou un script. C’est pour cette raison que les attaques par déni de service sont les plus redoutées.

Types d'attaque d'un réseau

Catégories principales d'attaques :

- ***Code malveillant* (« malware » *ou* « rogue program »)**
  - Ensemble d'instruction permettant intentionnellement de mettre en défaut une politique de sécurité
  - Programme simple ou auto-reproducteur s'installant dans un système d'information à l'insu des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité, la disponibilité ou d'impersonnifier un utilisateur (afin de réaliser un délit et de l'incriminer à tort)
- ***Les codes malveillants existent depuis longtemps***
  - Découverte des virus : Cohen, 1984
  - Références à menaces et vulnérabilités découlant de failles de programmes remontant bien avant : Ware, 1970 et Anderson, 1972

Types d'attaque d'un réseau

Attaques de reconnaissance

- Demandes d'informations Internet (http://www.whois.net) Balayages ping (Nmap)
- Balayages de ports (Nmap)
- Analyseurs de paquets (WireShark)
- Écoute électronique
- Collecte d'informations (noms d'utilisateur, mots de passe...)
- Vol de données

Attaques d'accès

- Exploitent des vulnérabilités connues dans les services d'authentification, les services FTP et les services Web pour accéder à des comptes Web, à des bases de données confidentielles ou à toute autre information sensible

Types d'attaque d'un réseau

Attaques de mot de passe

- Analyseur de paquets pour glaner les comptes et les mots de passe utilisateur transmis en clair
- Tentatives de connexion répétées à une ressource partagée, comme un serveur ou un routeur, afin d'identifier un compte utilisateur, un mot de passe ou les deux
- Attaque par force brute
- Attaque par dictionnaire
  - Tente de se connecter de manière répétitive en utilisant les mots d'un dictionnaire comme nom d'utilisateur
  - Réussit souvent du fait que les utilisateurs ont tendance à choisir des mots de passe simples constitués d'un seul mot ou de variations faciles à prévoir, comme l'ajout du chiffre 1 à un mot

Types d'attaque d'un réseau

- Attaques de mot de passe
  - Attaque en force (*brute force*)
    - Effectue une recherche exhaustive à l'aide de combinaisons de jeux de caractères pour déterminer tous les mots de passe possibles constitués de ces caractères
    - Demande plus de temps
    - Peut résoudre des mots de passe simples en moins d'une minute
    - Résolution de mots de passe plus complexes peut demander des jours ou des semaines

Types d'attaque d'un réseau

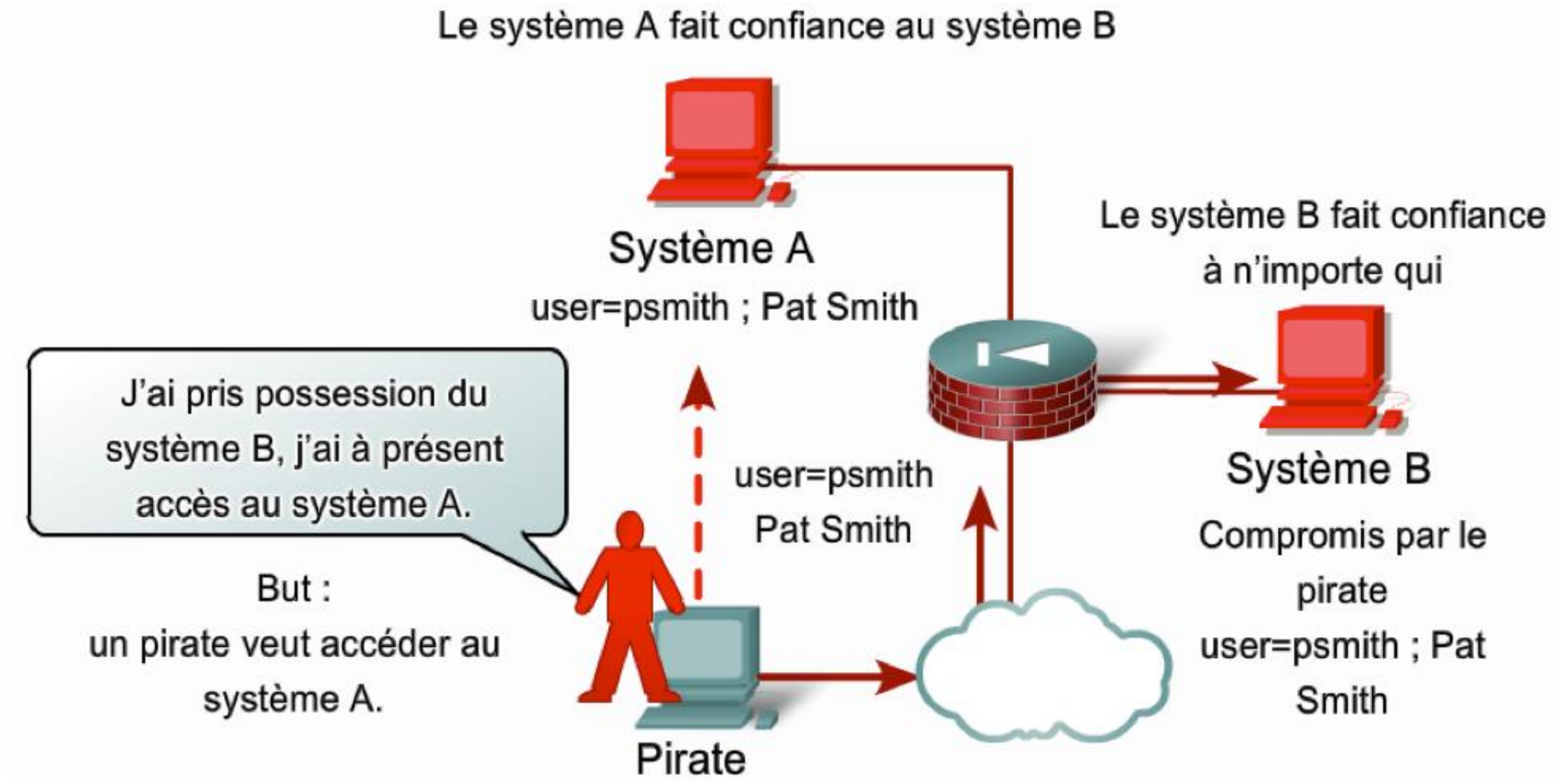
- Limitation des attaques de mot de passe
  - Apprendre aux utilisateurs à définir des mots de passe complexes et en spécifiant une longueur de mot de passe minimale
  - Limiter le nombre d'échecs de connexion
    - Une attaque en force peut cependant aussi s'effectuer hors ligne.
    - Par exemple, si un pirate intercepte un mot de passe crypté lors d'une écoute électronique ou en accédant à un fichier de configuration, il pourrait tenter de casser ce mot de passe sans se connecter à l'hôte.

Types d'attaque d'un réseau

- Exploitation de la confiance
  - Compromet un hôte de confiance, et l'utilise ensuite pour lancer des attaques sur d'autres hôtes du réseau
  - Dans le réseau d'une entreprise, si un hôte est protégé par un pare-feu (hôte interne), mais qu'il est accessible depuis un hôte de confiance situé de l'autre côté du pare-feu (hôte externe), l'hôte interne peut être attaqué par le biais de l'hôte externe.

Types d'attaque d'un réseau

- Exploitation de la confiance



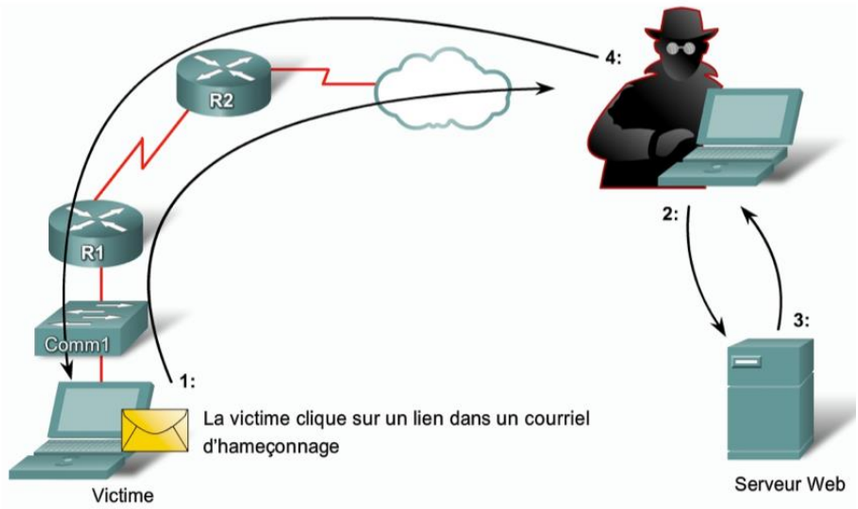
Types d'attaque d'un réseau

- Redirection de port
  - Utilise un hôte compromis pour faire passer, au travers d'un pare-feu, un trafic qui serait normalement bloqué
  - Peut être limitée principalement par des modèles de confiance appropriés, qui sont spécifiques au réseau
  - En cas d'attaque, un système de détection des intrusions (*IDS*) installé sur l'hôte permet de détecter le pirate et de l'empêcher d'installer de tels utilitaires de redirection sur un hôte

Types d'attaque d'un réseau

- Attaque de l'homme du milieu (*man-in-the-middle*)
  - Attaque menée par un pirate qui s'arrange pour se placer entre deux hôtes légitimes
  - Permet le déroulement normal des transactions entre les deux hôtes et ne manipule leur conversation que de temps à autre
  - Si l'assaillant arrive à se placer à un endroit stratégique, il peut voler des données, pirater la session en cours pour accéder aux ressources du réseau privé, mener des attaques par déni de service, altérer les données transmises ou introduire de nouvelles informations dans les sessions en cours.

- Exemple : proxy transparent par hameçonnage



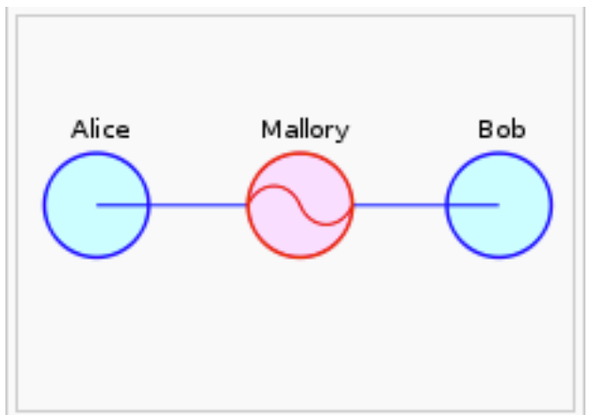
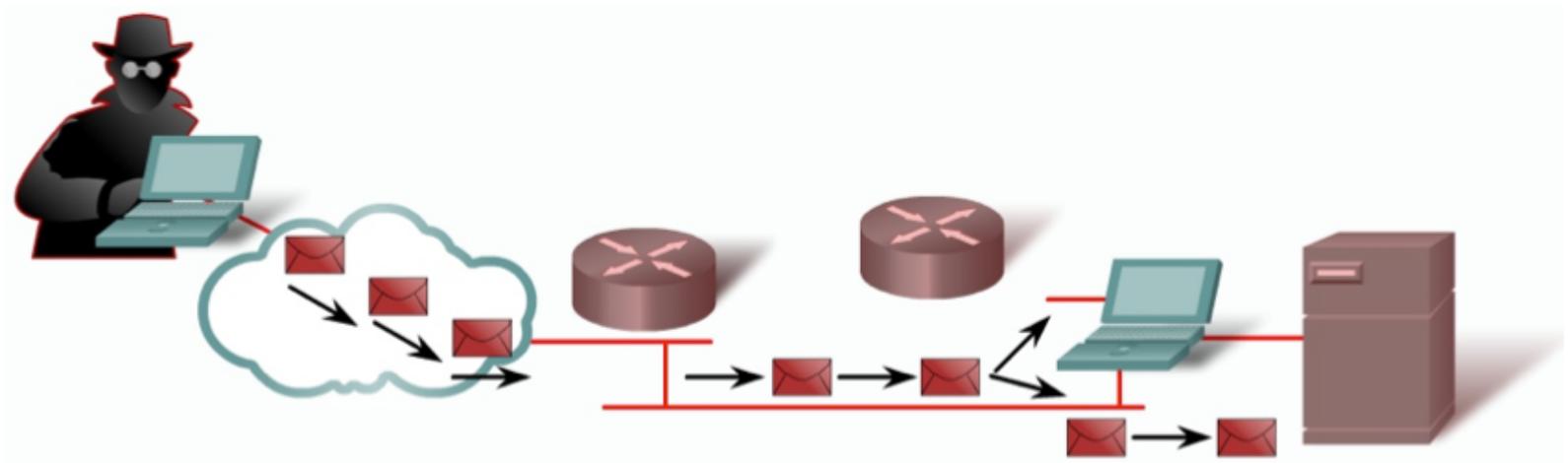


Schéma de l'attaque de l'homme du milieu: Mallory intercepte les communications entre Alice et Bob

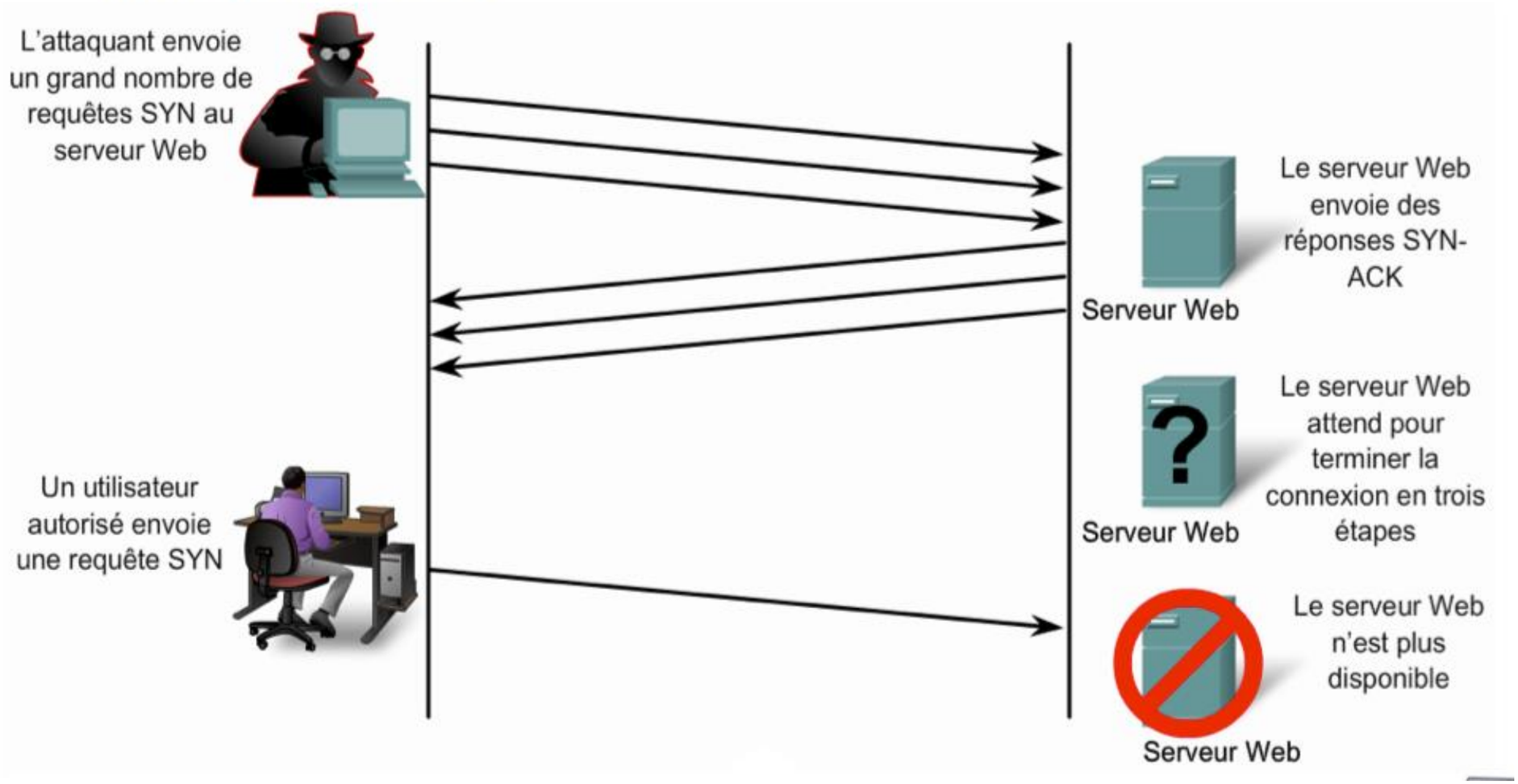
Types d'attaque d'un réseau

- Attaques par déni de service (DoS)
  - Empêche l'utilisation d'un service par des personnes autorisées en épuisant les ressources du système
    - Surcharge de ressources (espace disque, inondation de paquets...)
    - Données mal formées (paquets surdimensionnés, chevauchement de paquets...)
  - Attaque la plus répandue et aussi la plus difficile à éliminer
  - Exemples des menaces DoS les plus courantes :
    - *Ping of Death,* Inondation SYN, email bombing...



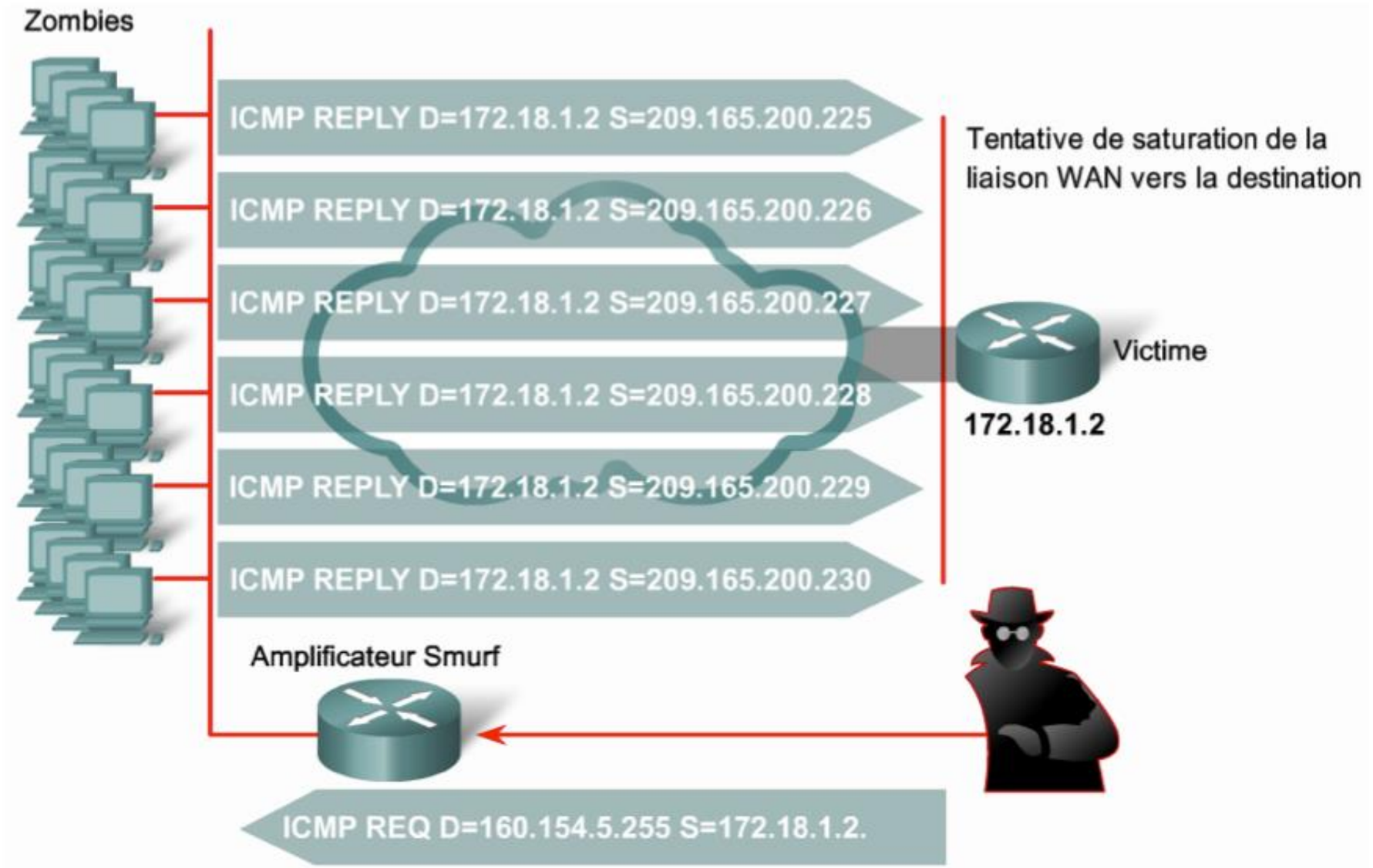
Types d'attaque d'un réseau

- Attaques par déni de service (DoS)
  - Inondation SYN



Types d'attaque d'un réseau

- Attaques par déni de service distribué (DDoS)
  - SMURF



Types d'attaque d'un réseau

Attaques de programmes malveillants

- Les stations de travail des utilisateurs finaux sont principalement vulnérables aux attaques de vers, de virus et de chevaux de Troie.
- Un ver exécute un code et installe des copies de lui- même dans la mémoire de l'ordinateur infecté, ce qui infecte par la suite d'autres ordinateurs hôtes.
- Un virus est un logiciel malveillant intégré à un autre programme afin d'exécuter des fonctions particulières indésirables sur l'ordinateur de l'utilisateur.
- Un cheval de Troie se distingue uniquement des vers et des virus par le fait qu'il a été entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un instrument d'attaque.

Types d’ attaque d’ un réseau
Codes malveillants

Vers:

Voici les étapes recommandées pour limiter les attaques de vers :

•Confinement : limitez la diffusion du ver au sein du réseau, en cloisonnant les parties non infectées.

•Inoculation : commencez par appliquer les correctifs à tous les systèmes, si possible, en recherchant les systèmes vulnérables.

•Quarantaine : dépistez toutes les machines infectées au sein du réseau. Déconnectez, retirez ou bloquez les machines infectées du réseau.

•Traitement : nettoyez tous les systèmes infectés. Certains vers peuvent nécessiter une réinstallation complète du système pour le nettoyer.

Types d'attaque d'un réseau

Codes malveillants

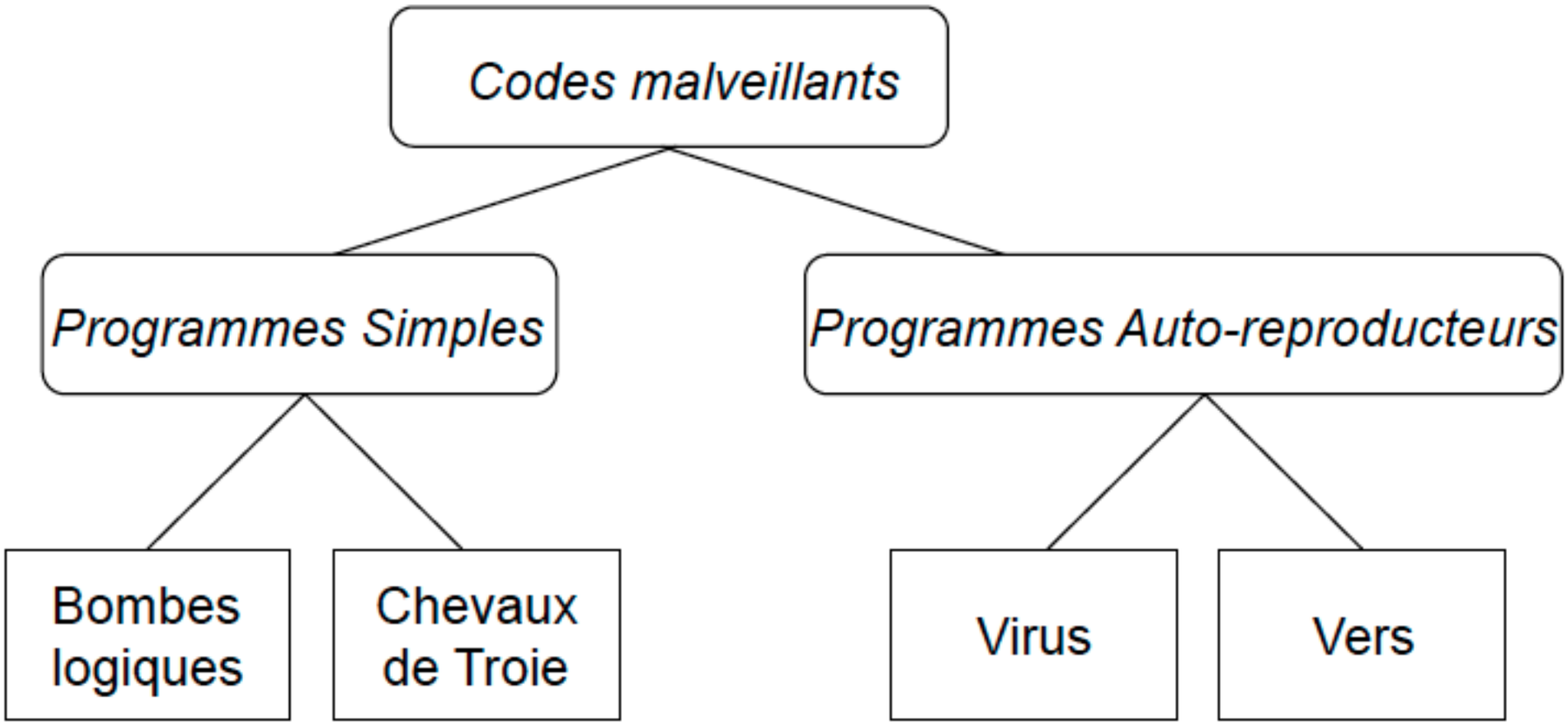
- ***Virus***
  - Code attaché à un programme non malveillant, pouvant s'auto-reproduire en infectant d'autres programmes non malveillants, et contenant une *charge* (« *payload* »)
- ***Vers (worm)***
  - Programme s'auto-reproduisant à travers un réseau mais n'infectant pas forcément d'autres programmes
- ***Rabbit***
  - Virus ou vers qui s'auto reproduit localement sans limite pour épuiser des ressources

Types d'attaque d'un réseau
Codes malveillants

- ***Cheval de troie (« Trojan Horse »)***
  - Programme ayant des effets de bords cachés (non documentés et non prévus par l'utilisateur exécutant le programme)
  - *Porte dérobée (« Trapdoor » ou « Backdoor »)* : fonctionnalité non documentée d'un programme permettant d'obtenir un accès au système autrement que par la procédure documentée
    - Module serveur/module client
    - Exple : Back Orifice (protocole UDP, port 31337), Netbus (TCP, port 12345)
    - Peuvent être répandus par des vers
    - *« ratware »* : porte dérobée qui transforme des ordinateurs en « zombie » pour envoyer du spam
- *Logiciel espion (« Spyware »)* : petits modules insérés dans des logiciels commerciaux pour renseigner l'éditeur du logiciel
- *Leurre* : programme imitant le fonctionnement normal d'un programme légitime du système
  - Fausse bannière de connexion Unix
  - Espion de clavier (« Keylogger ») : logiciel copiant et envoyant les frappes de clavier

Types d’ attaque d’ un réseau
Codes malveillants

- ***Classification des infections informatiques***



Types d'attaque d'un réseau
Codes malveillants

- ***Fonctionnement général d'un virus***
  - Le programme infectant est porté par un programme hôte (« dropper »)
  - Lorsque le dropper est exécuté
    - Le programme infectant prend la main et le programme hôte est temporairement mis en sommeil,
    - Puis il rend la main au programme hôte qui s'exécute normalement sans trahir la présence du programme infectant.
  - L'infection d'un utilisateur n'est possible que s'il a exécuté le dropper ou importé des données corrompues (virus de document)
    - basé sur l'ingénierie sociale
    - dropper= jeu, animation anodine, mail racoleur …, afin d'inciter la victime a l'exécuter.

Types d'attaque d'un réseau
Codes malveillants

- ***Installation du virus***
  - Mode transient : s'exécute qd le programme auquel il est attaché est exécuté, et termine qd le programme termine
  - Mode résident : se copie en mémoire, peut rester actif ou être activé même si l'exécution du programme auquel il est attaché est terminée
  - Mode furtif : le processus n'est pas visible lors de l'affichage des processus en cours
  - Mode persistant : en cas d'effacement ou de désinstallation, le programme infectant est capable de se réinstaller indépendamment d'un dropper

Types d'attaque d'un réseau
Codes malveillants

- ***Virus d'exécutable***
  - Une copie du virus est ajoutée dans le fichier de l'exécutable cible
  - Il en résulte une hétérogénéité du code source
- ***Virus de code source***
  - Une copie du source du virus est ajoutée dans le fichier du source du programme cible
  - Permet d'infecter des machines dont l'environnement n'est pas connu
- ***Virus de document***
  - Code viral contenu dans un fichier de données non exécutable.
  - L'activation du code viral est réalisée soit par une fonctionnalité prévue dans l'application associée à ce format de fichier, soit en vertu d'une faille de l'application considérée

Techniques générales d'atténuation des risques

Techniques générales d'atténuation des risques

Sécurité basée sur les hôtes et les serveurs

Durcissement des périphériques

- À l'installation d'un nouveau système d'exploitation sur un ordinateur, les paramètres de sécurité sont définis à leur valeur par défaut.

- Dans la plupart des cas, le niveau de sécurité correspondant n'est pas suffisant.

- Voici quelques étapes simples qu'il convient d'effectuer sur la plupart des systèmes d'exploitation :
  - Changement immédiat des noms d'utilisateur et des mots de passe par défaut.
  - Accès aux ressources du système limité strictement aux personnes autorisées à utiliser ces ressources.
  - Désactivation des services et applications qui ne sont pas nécessaires et désinstallation dans la mesure du possible.

Techniques générales d'atténuation des risques

Sécurité basée sur les hôtes et les serveurs

- Il est vital de protéger les hôtes du réseau, tels que les ordinateurs des utilisateurs et les serveurs.
- Ces hôtes doivent être sécurisés à mesure qu'ils sont ajoutés au réseau et doivent être mis à jour à l'aide des correctifs de sécurité dès que ceux-ci sont disponibles.
- Les antivirus, les pare-feu et les systèmes de détection des intrusions sont des outils précieux pour la sécurisation des hôtes d'un réseau.
- Étant donné qu'une grande quantité de données de l'entreprise peuvent résider sur un même serveur de fichiers, il est en général important que ce serveur soit accessible et disponible.

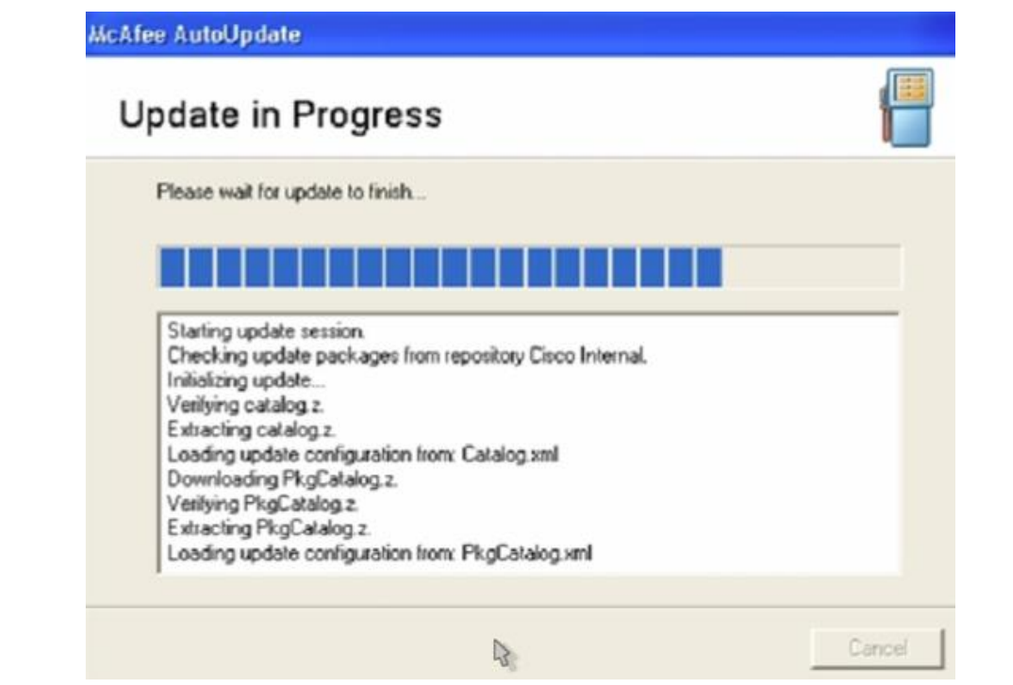
Techniques générales d'atténuation des risques

Logiciel antivirus

- Installez un logiciel antivirus sur les hôtes pour les protéger contre les virus connus.
- Les logiciels antivirus peuvent détecter la plupart des virus et des chevaux de Troie et les empêcher de se propager dans le réseau.
- Le logiciel antivirus peut procéder de deux manières différentes :

A. Il analyse les fichiers, en comparant leur contenu aux virus d'un dictionnaire de virus connus. Les virus détectés sont signalés selon la méthode définie par l'utilisateur.

B. Il surveille les processus suspects sur un hôte susceptible d'être infecté. Cette surveillance comprend la saisie de données, la surveillance des ports et d'autres méthodes.



Techniques générales d'atténuation des risques

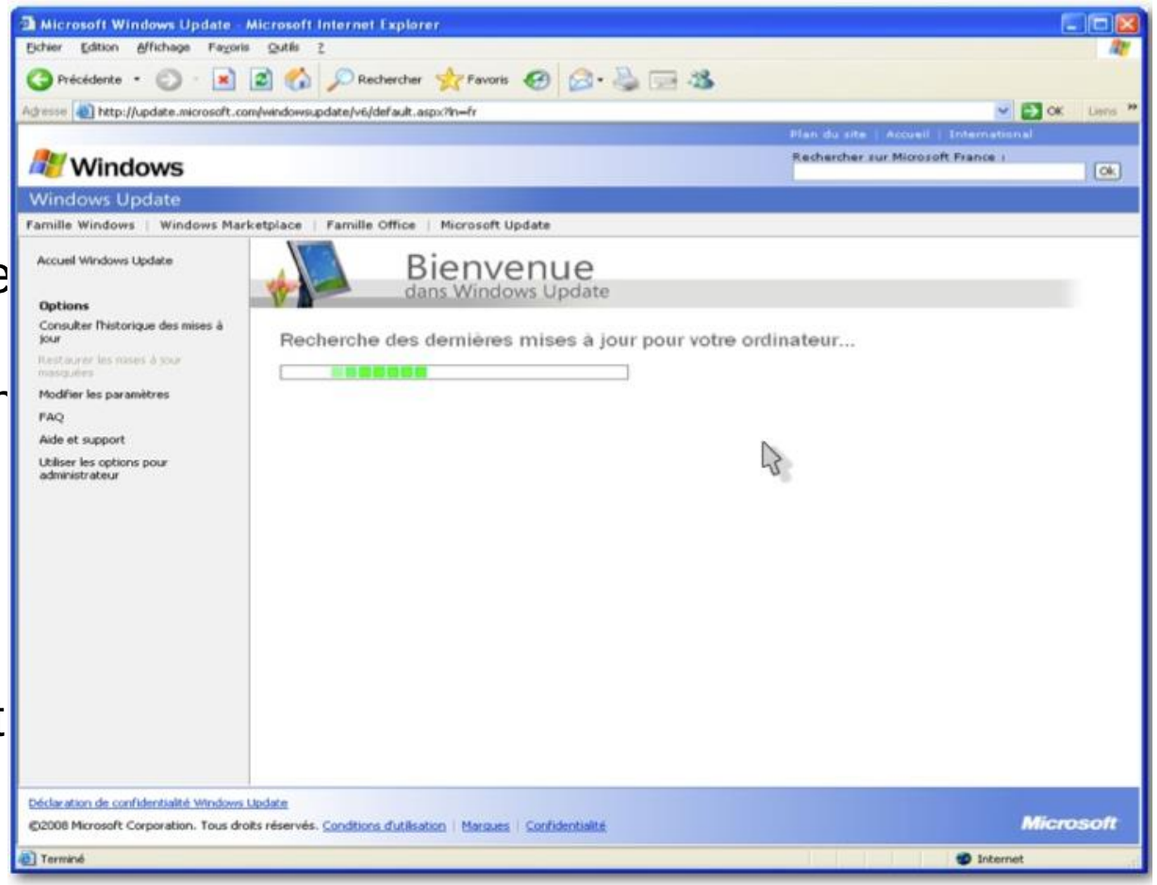
Pare-feu personnel

- Les ordinateurs personnels connectés au réseau Internet par une ligne téléphonique, un câble DSL ou un modem câble sont aussi vulnérables que les ordinateurs d'entreprise.
- Le pare-feu personnel réside sur l'ordinateur de l'utilisateur et tente d'empêcher les attaques.
- Les pare-feu personnels ne sont pas conçus pour une mise en œuvre dans un réseau local, comme les pare-feu hébergés par un périphérique ou un serveur.
- De plus, ils peuvent empêcher l'accès au réseau s'ils sont installés en même temps que d'autres clients, services, protocoles ou adaptateurs réseau.
- McAfee, Norton, Symantec et Zone Labs sont quelques exemples de fournisseurs de logiciels pare-feu personnels.

Techniques générales d'atténuation des risques

Correctifs du système d'exploitation

- La meilleure façon de limiter les risques liés aux vers et à leurs variantes consiste à télécharger les mises à jour de sécurité du fournisseur du système d'exploitation et d'appliquer les correctifs aux systèmes vulnérables.
- L'administration d'un grand nombre de systèmes implique la création d'une image logicielle standard (système d'exploitation et applications accréditées dont l'utilisation est autorisée sur les systèmes clients déployés) utilisée pour de nouvelles installations ou pour des mises à niveau.
- L'installation des correctifs sur tous les systèmes impose que ces systèmes soient connectés au réseau, ce qui peut s'avérer impossible.



Techniques générales d'atténuation des risques

Détection des intrusions et méthodes de prévention

- Les systèmes de détection des intrusions (IDS) détectent les attaques contre un réseau et envoient des données de journalisation à une console de gestion.
- Les systèmes de protection contre les intrusions (IPS) empêchent les attaques contre le réseau et doivent être dotés des mécanismes de défense suivants en plus de la détection :
  - Un mécanisme de prévention pour empêcher l'exécution de l'attaque détectée.
  - Un mécanisme de réaction pour immuniser les système contre les attaques ultérieures provenant d'une source malveillante.
- Chacune de ces techniques peut s'appliquer au niveau du réseau ou des hôtes, ou encore aux deux niveaux pour une protection maximale.

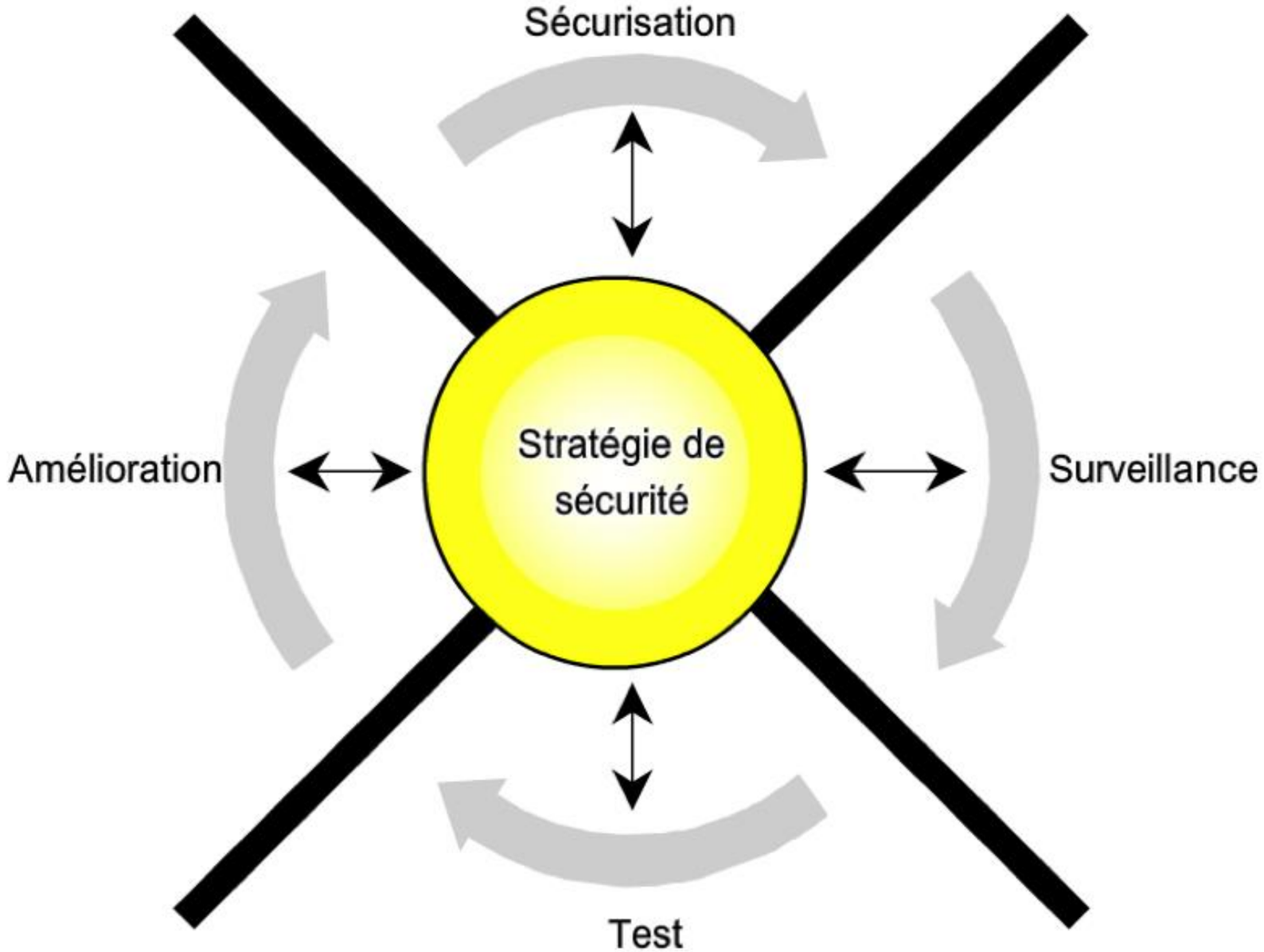
Stratégie de sécurité de l'entreprise

Stratégie de sécurité de l'entreprise

- ***Comment évaluer la sécurité ?***
  - Approche quantitative
    - Utiliser le nombre de failles déjà détectées et le temps de détection pour prévoir le temps de découverte de la prochaine faille
    - Mesurer la ***surface d'attaque*** (nombre d'interfaces, nombre d'instructions dangereuses dans un code, …)
    - → Démarche quantitative peu utilisée en sécurité
  - Approche qualitative
    - Apprécier les ***risques*** auxquels les ***biens*** sont exposés
    - → Approche la plus répandue : ***l'analyse de risques***

Stratégie de sécurité de l'entreprise

- Roue de la sécurité des réseaux



Stratégie de sécurité de l'entreprise

- Roue de la sécurité des réseaux
  - Étape 1 : Sécurisation
    - Sécurisez le réseau en appliquant la stratégie de sécurité et en mettant en œuvre les solutions de sécurisation suivantes :
      - Protection contre les menaces
      - Inspection dynamique et filtrage des paquets
      - Systèmes de prévention contre les intrusions
      - Correction des vulnérabilités
      - Désactivation des services
      - Sécurisation de la connectivité
        - Réseaux virtuels privés
        - Authentification

Stratégie de sécurité de l'entreprise

- Roue de la sécurité des réseaux
  - Étape 2 : Surveillance
    - Audit des fichiers journaux
    - Périphériques IDS
    - La surveillance du réseau offre en outre l'avantage de pouvoir vérifier que les mesures prises à l'étape 1 de la roue de la sécurité ont bien été configurées et fonctionnent convenablement.

Stratégie de sécurité de l'entreprise

- Roue de la sécurité des réseaux
  - Étape 3 : Test
    - Outils d'évaluation de la vulnérabilité (SATAN, Nessus, Nmap...)
  - Étape 4 : Amélioration
    - Analyse des données collectées pendant les phases de surveillance et de test
    - Développement et mise en œuvre de mécanismes d'amélioration qui renforcent la stratégie de sécurité et ses résultats en ajoutant des éléments à l'étape 1
  - Répéter continuellement le cycle de la roue de la sécurité, car de nouvelles vulnérabilités et de nouveaux risques apparaissent tous les jours

Stratégie de sécurité de l'entreprise

Éléments d'une stratégie de sécurité

- Déclaration d'autorité et de portée (personnes, domaines) Règles de bon usage
- Stratégie d'identification et d'authentification
- Stratégie d'accès Internet
- Stratégie d'accès interne
- Stratégie d'accès à distance
- Procédure de gestion des incidents
- Stratégie de demande d'accès et de compte Stratégie sur les informations confidentielles Stratégie relative aux mots de passe
- Stratégie de messagerie électronique
- Stratégie sur le courrier indésirable
- Stratégie de sécurité des réseaux privés virtuels