# 4. Stratégies d’attaques et organismes de sécurité

# 4. Stratégies d’attaques et organismes de sécurité

4.1 Ressources informatiques vulnérables aux attaques et types de cibles

4.2 Stratégie d’une attaque

4.3 Types d'attaque

4.4 Les organismes de sécurité

4.5 Etude de cas

# 4. Cyber-attaques

- Introduction
  - Considérations juridiques
  - Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?
  - La nouvelle économie de la cybercriminalité
  - Notions de vulnérabilité, menace, attaque

# Considérations juridiques

- Rappel réglementaire :
  - **le seul fait** de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal)
  - **le seul fait** de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code).

# Considérations juridiques

- **Article 323-3-1 du code pénal**
  - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

# Considérations juridiques

The use of methods described in this course involves the responsibility of users in case of use!

# Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- Les motivations évoluent
  - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
  - De nos jours : majoritairement des actions organisées et réfléchies

# Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

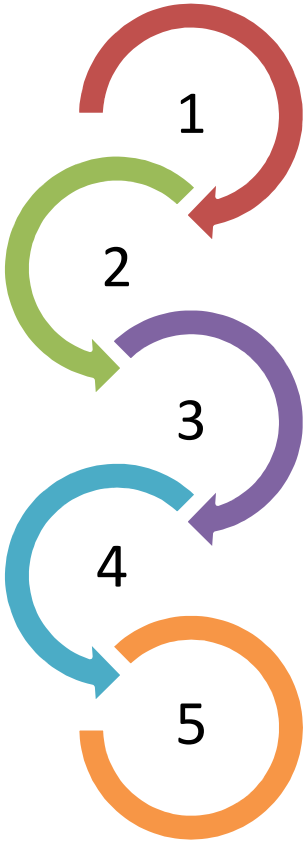
- Cyber délinquance :
  - Les individus attirés par l'appât du gain
  - Les « hacktivistes »
  - Motivation politique, religieuse, etc.
  - Les concurrents directs de l'organisation visée
  - Les fonctionnaires au service d'un état
  - Les mercenaires agissant pour le compte de commanditaires
  - …

# Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires
- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)
- **Chantage**
  - Déni de service
  - Modifications des données
- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

# La nouvelle économie de la cybercriminalité

- Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs




des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques

des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques

un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates

des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire

des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

# La nouvelle économie de la cybercriminalité

- Quelques chiffres pour illustrer le marché de la cybercriminalité…

**de 2 à 10 $** le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

**5 $** le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet

**2.399 $** le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $ )

# 4.1 Types de cibles

- Cible opportune
  - Au hasard : détecté par les pirates à la recherche de machines ou serveurs peu protégés
  - Que faire : mettre à jour l'infrastructure avec les correctifs des systèmes
  - Tester son système (essayer de trouver des failles)
- Cible de choix
  - Cible précise : intérêt stratégique de l'entreprise pour des tiers…

# 4.2. Cyber-attaques

- Recette :
  - Catégorisation des attaques
  - Stratégie d'une attaque
  - Reconnaissance et collecte de renseignements
  - Scan des services et des ports
  - Obtention d'un accès
  - Extension des privilèges acquis
  - Couverture des traces
  - Analyse de risques: Nature des méfaits

# Catégorisation des attaques

On classe les types d'attaques en deux catégories :

- Attaques passives
  - Interception, écoute, analyse
- Attaques actives
  - Modification, destruction
  - Interruption, perturbation

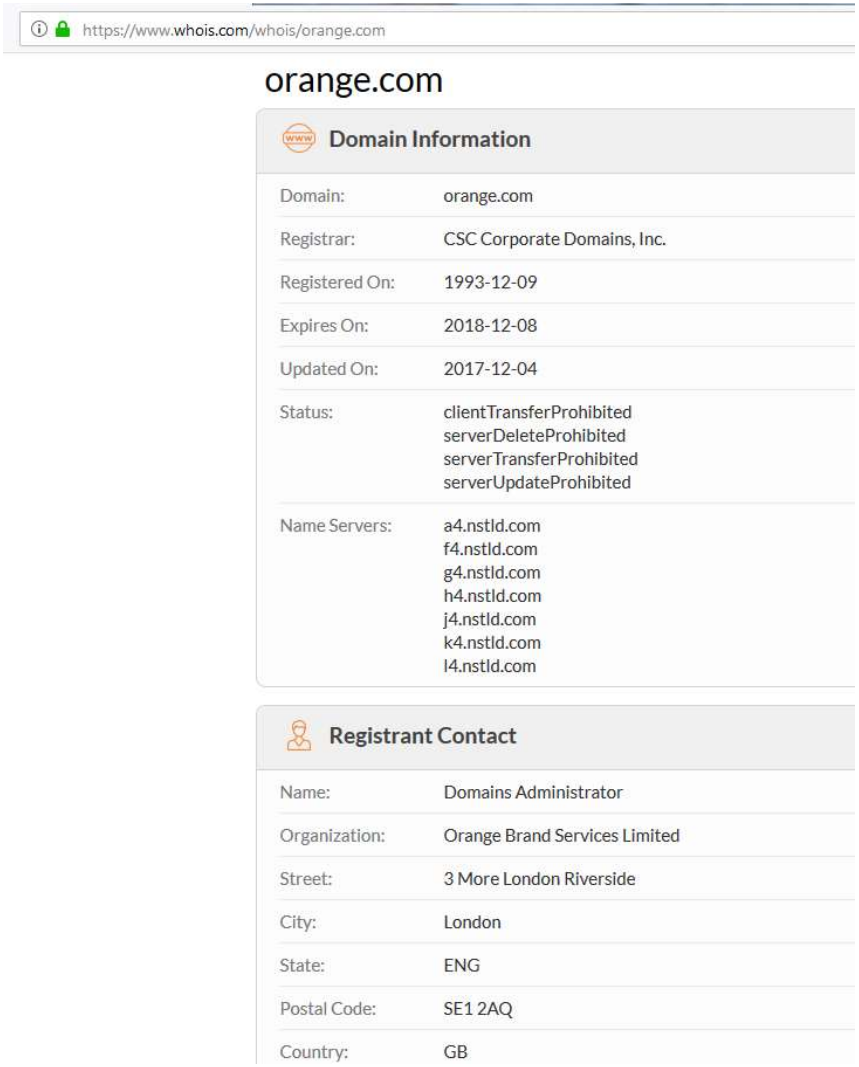
# 4.2.1 Reconnaissance et collecte de renseignements (1/4)

- Noms de domaine, serveurs DNS, blocs d'adresses IP assignés
- Adresses IP accessibles de l'extérieur
- Services présentant une cible valable
  - www, ftp, e-mail…
- Types de machines sur lesquels les services s'exécutent
  - Systèmes d'exploitation et numéro de version => utilisation des failles connues exploitables
- Mécanismes en place contrôlant l'accès au réseau
- Type de pare-feu et d'IDS (Intrusion Detection System)

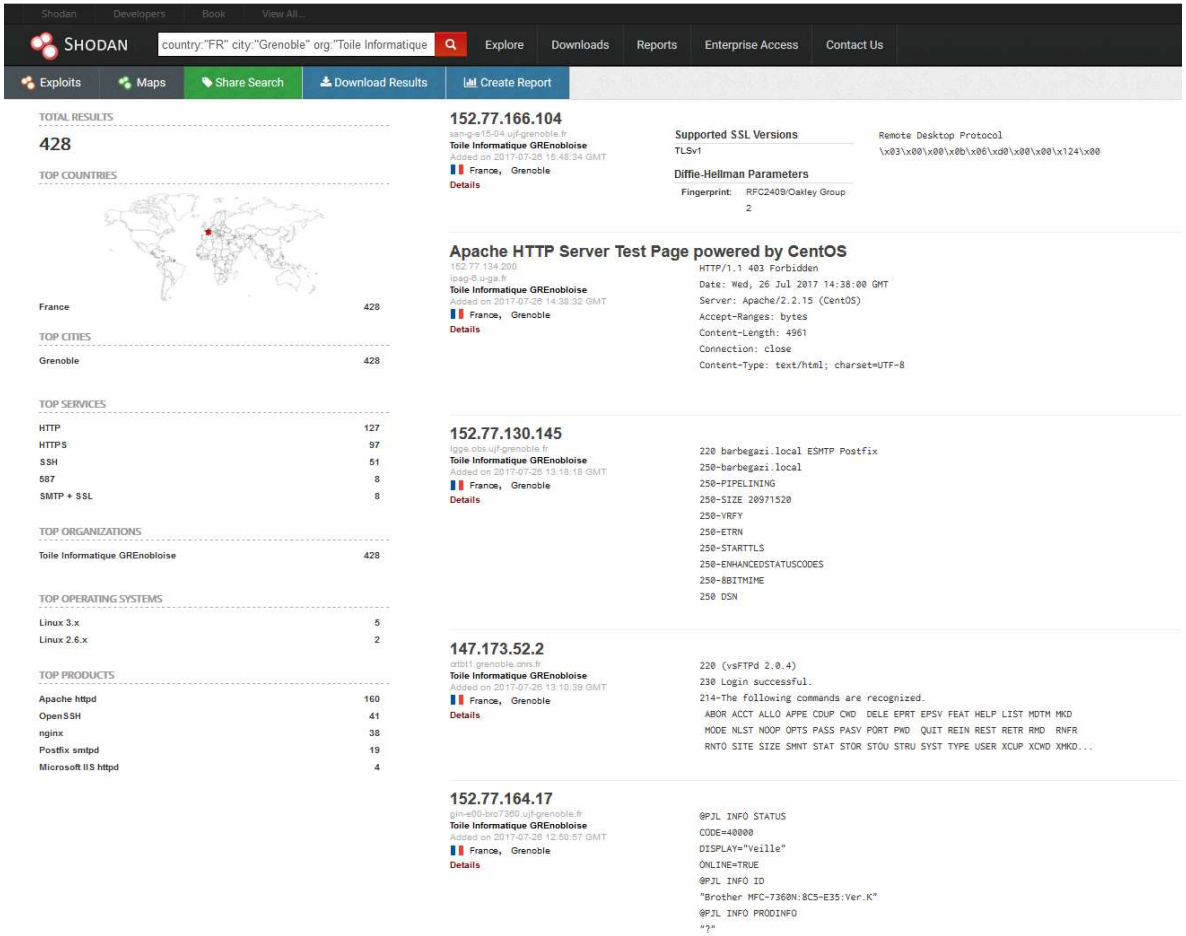
# 4.2.1 Reconnaissance et collecte de renseignements (2/4)

- Noms d'utilisateurs, groupes, tables de routage, informations SNMP (techniques d'énumération des sources du système)
- Emplacement physique des équipements et systèmes
- Protocoles de réseau utilisés (IP, IPv6, IPSec, SSL, OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*))
- Cartographie du réseau
- Type de liaisons d'accès
  - Accès traditionnel (frame relay, large bande)
  - Accès par numérotation téléphonique (modem)
  - Accès par Wi-Fi
- Approche par « ingénierie sociale » (consiste à interroger des gens et à récupérer des informations en les piégeant)
  - Informations sur les personnes, leurs noms, numéros de téléphone, situation dans l'entreprise, adresse…

# 4.2.1 Reconnaissance et collecte de renseignements: Whois (3/4)



# Reconnaissance et collecte de renseignements: Shodan (4/4)



# 4.2.2 Scan des services et des ports

- Scan détaillé d'une cible (NMAP = Network Mapper)

# 4.2.3 Enumération

- Extraction d'information sur les comptes valides et les ressources
  - ressources réseau et partages
  - utilisateurs et groupes (organisation fct du type de Système d'Exploitation)
  - applications
  - bandeaux envoyés en réponse par les équipements

# 4.2.4 Obtention d'un accès

- Attaque de niveau système d'exploitation
  - Utilisation des fonctionnalités du S.E.
- Attaque de niveau application
  - Utilisation des fonctionnalités de l'application
- Attaque profitant d'une mauvaise configuration
  - Système "ouvert", configuration par défaut (nom et mot de passe administrateur !), nombreuses fonctionnalités activées
- Attaque utilisant des scripts hébergés
  - Scripts disponibles sur le système et quelques fois activés par défaut (Unix/Linux)
  - Détournement de requêtes SQL lors de l'interrogation d'une base de données via interface web

- Attaque automatisée (ex : scan du port 80 d'un bloc entier d'adresses de classe C afin de chercher une faille)
- Attaque ciblée : beaucoup plus rare mais difficile à détecter (pirates expérimentés)

# 4.2.5 Extension des privilèges acquis

- Si le pirate a réussi à entrer sur le système avec un mot de passe "faible" => extension des droits
  - Exécuter du code pour obtenir du privilège
  - Chercher à déchiffrer d'autres mots de passe
  - Rechercher des mots de passe enregistrés en clair
  - Rechercher d'éventuelles relations inter-réseaux
  - Identifier des permissions de fichiers ou de partages mal configurées

# 4.2.6 Couverture des traces

- Dissimuler à l'administrateur le fait que l'on ait pénétré le système
  - Windows : Eliminer les entrées dans le journal d'événements et le registre
  - Unix : vider le fichier d'historique (exécution du programme *log wiper*)
  - ! L'attaquant nettoie les journaux mais ne les supprime pas !

- Suite transparent 68

# 4.2.7. Cyber-attaques

- Définitions :
  - Les types d'attaques
  - Attaques TOIP
  - Les attaques APT
  - Détection des attaques
  - Étude de cas

# Les types d'attaques

- Deny Of Service DOS
- Sniffing
- Scanning
- Social engineering
- Cracking
- Spoofing
- Man in the middle
- Hijacking
- Buffer overflow

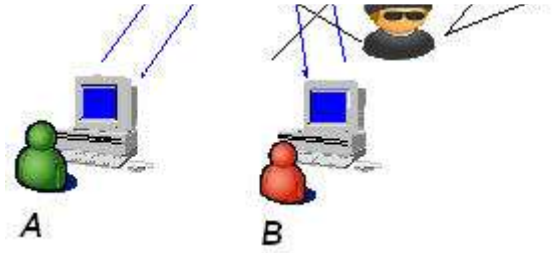
# Les types d'attaques

- Deny of Service (Déni de service DOS)

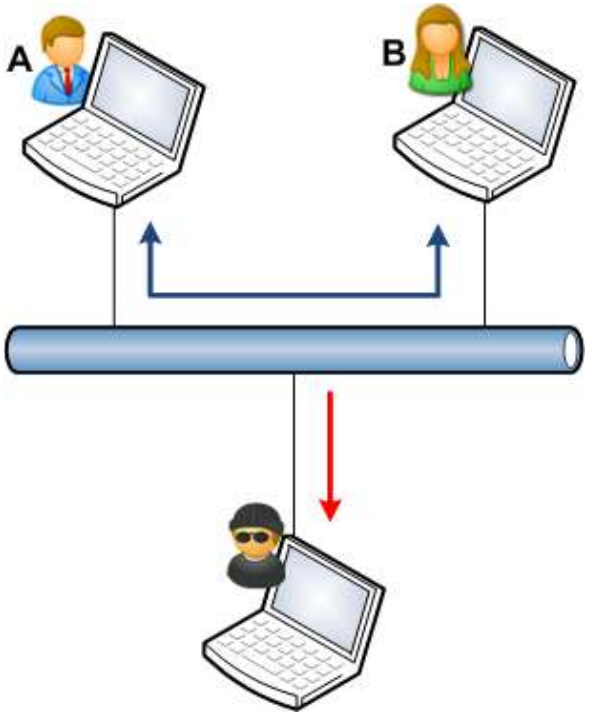
Comment s'en protéger ?

- Pas vraiment de solution
- Utiliser une sonde pour la détection de l'attaque

  – Utilisé autant contre un serveur qu'un poste client
  – Tous les S/E sont vulnérables

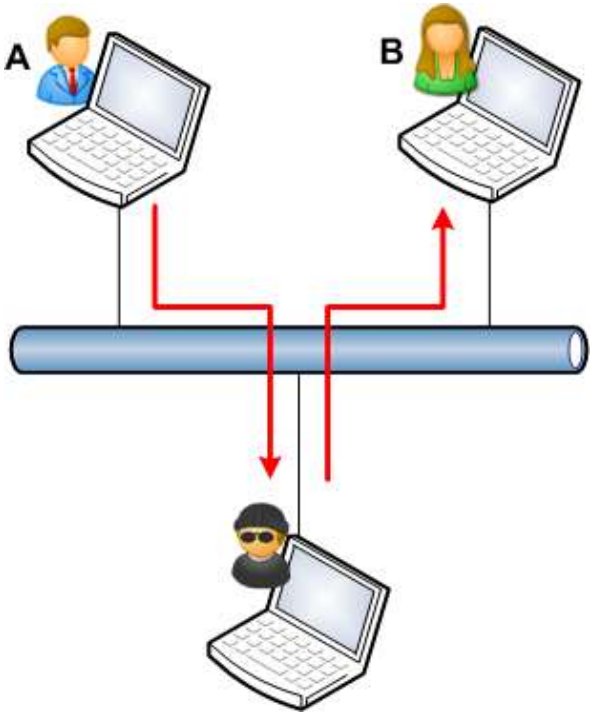


# Les types d'attaques




## Ecoute passive

L'attaquant est en mesure d'écouter les conversations entre A et B (atteinte à la ***confidentialité*** des échanges).




## Ecoute active

L'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent (atteinte à la ***confidentialité*** et à l'***intégrité*** des échanges).

# Les types d'attaques

- Sniffing ou reniflage
  - Analyser le trafic

Comment s'en protéger ?

-Utiliser de préférence un switch (commutateur) plutôt qu'un hub.

-Utiliser des protocoles chiffrés pour les informations sensibles comme les mots de passe.

-Utiliser un détecteur de sniffer.

-Ne pas laisser des prises connectés sans équipement d'avoir accès au réseau

# Les types d'attaques

- Scanning
  - Balayer tous les ports

Comment s'en protéger ?

-Scanner sa machine pour connaitre les ports ouverts

-Fermer les ports inutiles à l'aide d'un pare-feu

-Utiliser un détecteur d'intrusion IDS

scanner va en déduire si les ports sont ouverts.

  - Permet de connaitre les points faibles d'une machine et ainsi de savoir par où attaquer.

# Les types d'attaques

- Social Engeneering
  - Il s'agit d'une technique

Comment s'en protéger ?

-Faire preuve de bon sens

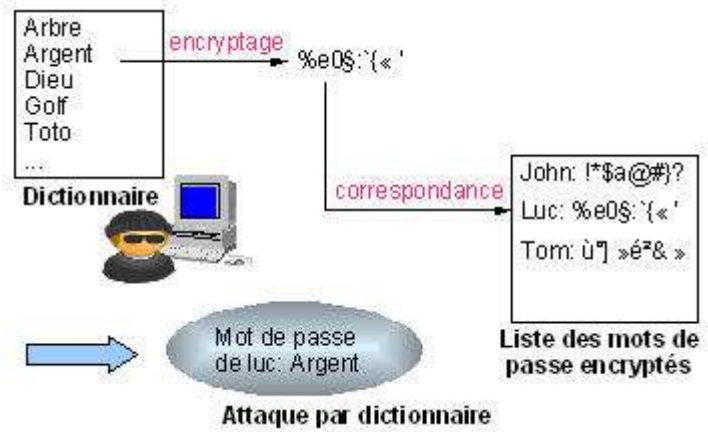
-Faire attention aux informations que l'on laisse sur Internet et particulièrement dans les réseaux sociaux

faire par téléphone, par courrier électronique, par lettre écrite,

  - Si elle est bien menée elle peut être très efficace

# Les types d'attaques

- Cracking : casser des mots de passe
  - Deviner le mot de passe de la victime.
  - Trop souvent des mots passe triviaux sont utilisés (prénom des enfants, date de naissance…)
  - Utilisations de logiciels dédiés se basant souvent sur des comparaisons de signature
  - Les fonctions de hachages utilisées pour l'encodage des mots de passe ne fonctionne que dans un sens



# Les types d'attaques

- Cracking : types d'attaques
  - attaque par dictionnaire : le logiciel teste tous les mots de
  - attaque hybride : le logiciel teste tous les mots de passe stockés dans un fichier texte et y ajoute

Comment s'en protéger ?

-Choisir un mot de passe robuste et ne pas l'écrire sur un support autre que sa propre mémoire

-Changer régulièrement de mot de passe

possibles. Ainsi ce genre d'attaque aboutit à chaque fois. Cette solution peut toutefois ne jamais aboutir dans un temps humain

# Les types d'attaques

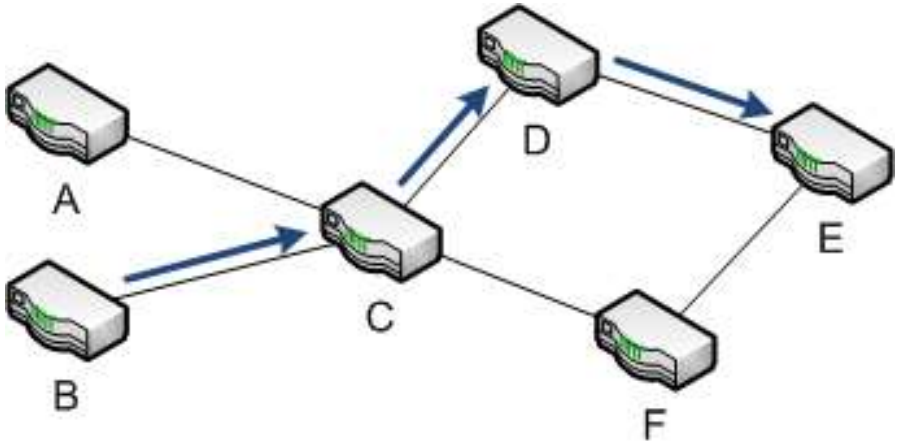
- Spoofing ou usurpation

Comment s'en protéger ?

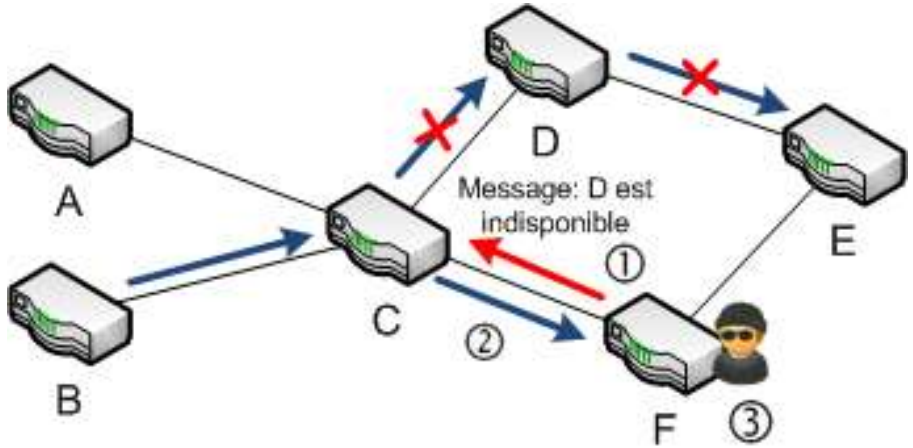
-Pas de solution pour l'empêcher

-Utiliser des mécanismes pour déterminer la confiance (signature électronique de mail, protocoles sécurisés…)

# Les types d'attaques




Chaque routeur possède une table de routage qui indique vers quel routeur voisin transmettre les datagrammes. Cette table peut être mise à jour dynamiquement en fonction des évènements réseaux (protocoles BGP, RIP, OSPF, etc.).




But de l'attaque : **dérouter les paquets** à destination du réseau E, vers le réseau F maitrisé par l'attaquant.

Méthode :

① L'attaquant utilise une faiblesse du protocole de routage pour indiquer au routeur C que le routeur D est indisponible, et que le routeur F peut router les paquets vers E ;

② le routeur C transfère donc à F les paquets pour E, afin qu'ils puissent être routés à destination ;

③ Selon le but visé par l'attaquant, celui-ci peut décider de router ou non les paquets vers E.

# Les types d'attaques

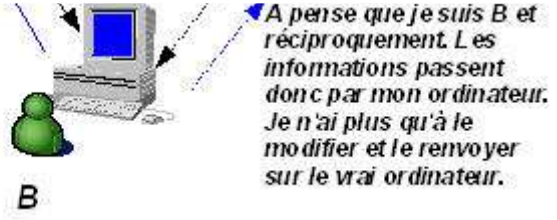
- Man in the middle ou
  « homme du milieu »

Comment s'en protéger ?

-Utiliser des protocoles sécurisés lors des interactions entre machines

-Ne se connecter qu'à des machines de confiance.

décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.



# Les types d'attaques

- Hijacking

Comment s'en protéger ?

-Utiliser des protocoles sécurisés

utilisateur légitime

– Pas besoin de connaître le mot de passe de l'utilisateur

# Les types d'attaques

- Buffer over flow ou débordement de tampon
  - Consiste à utiliser un programme résidant sur

Comment s'en protéger ?

-Pas de solution directe puisqu'elle s'appuie sur des erreurs ou des faiblesses de programmation

-Veillez à appliquer les correctifs et mises à jour des programmes que vous utilisez.

paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.

# Attaques TOIP

- 3 Types d'attaques
  - Over IP
  - Voicemail (répondeur)
  - Administrateur

# Attaques TOIP


**3** Ils détournent des appels frauduleusement vers l'international (Cuba, Balkans, Afrique) et les numéros surtaxés (0899) et les revendent à des opérateurs internationaux.

**Faille** : Toutes les destinations sont autorisées sur le standard téléphonique.



**2** Ils se connectent sur le standard téléphonique en trouvant les identifiants / mot de passe d'un compte utilisateur par brute force.

**Faille** : Mot de passe trop simple (0000, 1234, etc.)

**1** Les pirates utilisent le réseau Internet pour chercher des installations téléphoniques non-sécurisées.

**Faille** : Firewall non activé ou mal paramétré

# Attaques TOIP

- Voicemail (répondeur)

Bien souvent, les utilisateurs ne personnalisent pas l'accès (mot de passe) au répondeur de leur société. Certains PABX donnent alors la possibilité de passer des appels par ce biais.

Ce defaut est utilisé par les hackers pour transformer une ligne téléphonique en passerelle vers des appels longues distances, serveurs de jeux, rechargement (par ex. Paypal).

# Attaques TOIP

**Exemple de méthodologie des pirates :**

La faille par les messageries vocales

- Permettant d'être renvoyé avant ou après dépôt de message.
- Permettant une configuration à distance

Procédure des pirates

- Appeler des n° d'une entreprise.
- Si on tombe sur celui de la messagerie vocale, navigation dans les menus (consultation, configuration), saisie du mot de passe, configuration du n° de renvoi
- Appel vers l'utilisateur, renvoyé vers messagerie, qui, elle–même, renvoie vers un destinataire… lointain!
- Pour ne pas être repéré tout de suite, désactiver le renvoi après usage.

# Attaques TOIP

**Le piratage de l'interface Administrateur**

Le standard téléphonique possède une interface d'administration qui peut être piratée si les identifiants ne sont pas personnalisée de manière complexe. Les risques sont les suivants:

- Autorisation des renvois vers l'extérieur
- Programmation des renvois
  - Utilisateur,
  - Messagerie,
  - SVI
- Gestion des mots de passe (reset)
- Gestion des journaux de trace

# Attaques TOIP

**Exemple de méthodologie des pirates :**

1- Accès à l'administration d'un PABX
- Trouver l'adresse IP
- Suivre la documentation d'administration
- Tenter les mots de passe constructeur par défaut

2- Modification de la configuration
- Configurer les renvois

3- Après utilisation
- Restaurer la configuration
- Supprimer les journaux de traces

4- Prévoir la suite
- Explorer la configuration
- Eventuellement ouvrir d'autres accès à l'administration

# Attaques TOIP

**Les conséquences du piratage**

Les entreprises subissent des conséquences financières énormes. Plusieurs piratages sont recensés chaque jour en France et plusieurs dizaines de millions d'euros piratés chaque année.

Le piratage Télécom représente des fraudes de plusieurs dizaines de milliers d'euros à plusieurs centaines de milliers d'euros chacune. Le cas recensé le plus important en France est de 600,000 euros.

La plupart du temps, le piratage a lieu durant des périodes ou l'entreprise est fermée, notamment durant les weekend, les fêtes, les jours fériés. L'entreprise piratée ne pourra pas être prévenue puisqu'elle est fermée. il suffit de quelques heures de piratage pour subir des préjudices de plusieurs dizaines de milliers d'euros.

# Attaques TOIP

## Les conséquences du piratage

Prenons par exemple le cas d'une PME francilienne: Entre Noël et le jour de l'an, elle était fermée. Des pirates ont très facilement pénétré le système d'information, en utilisant la messagerie. Bilan : 70,000 euros perdus.

Les principales destinations piratées à ce jour sont les suivantes: Taiwan, Somalie, Cuba, Iles Caimans, Estonie, Corée du Nord, Azerbaibjan, Slovénie, Afganistan, Global Satellite, Globastar, Egypte, Nigeria, Togo, Sri Lanka, Benin, Ethiopie.

# Les attaques Web

## a. Usurpation d'identité via les cookies

Comme toutes les applications, les applications web sont sujettes à des vulnérabilités. Nous allons en voir deux d'entre elles :

- une faiblesse basée sur les cookies ;
  - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification.

- une faiblesse basée sur un code source mal développé.
  - Ce qui permet – par exemple – à un attaquant de contourner un mécanisme d'authentification, d'accéder à des données pour les divulguer ou les corrompre.

# Les attaques Web

## a. Usurpation d'identité via les cookies

Les cookies sont des fichiers gérés par les navigateurs web afin de stocker (et réutiliser) des informations concernant l'utilisateur, par exemple :

- son identifiant ;
- ses préférences d'affichage et de disposition de la page web.

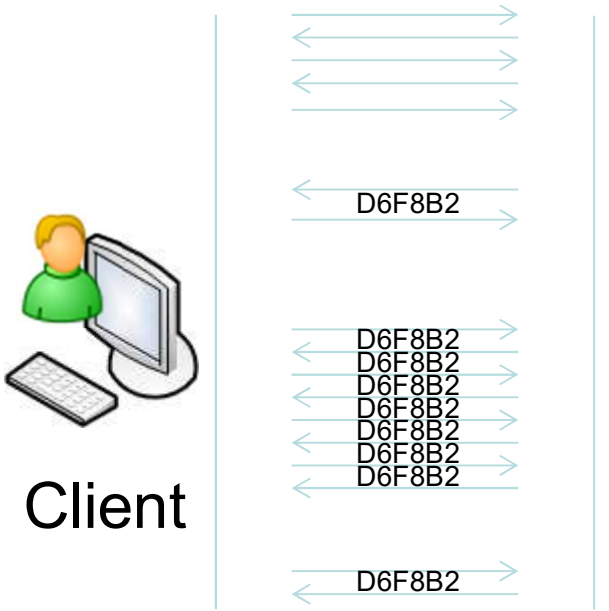
Les cookies sont nécessaires pour toutes les pages web dynamiques qui nécessitent d'identifier ou d'authentifier l'utilisateur, en permettant notamment la mise en œuvre de sessions :

- les sites marchand (afin d'afficher le panier de l'utilisateur connecté) ;
- les sites bancaires (afin d'afficher le solde du compte de l'utilisateur connecté et non pas celui d'un autre client) ;
- les sites « en général » (afin d'afficher des publicités ciblées sur notre navigation).

Il est possible – sous certaines conditions – d'usurper l'identité d'un utilisateur sur un site web si on arrive à récupérer son cookie d'identification.

# Les attaques Web

Fonctionnement habituel d'une connexion sur un site web nécessitant une authentification (site marchand, site bancaire, etc.) :




① Phase d'authentification (via un mot de passe en général) ;

② Phase de génération du cookie d'identification*. L'utilisateur est maintenant connecté « à son compte »

③ Phase de « navigation » : le cookie est inclus dans tous les échanges afin que le serveur puisse identifier la connexion de l'utilisateur ;

④ Phase de déconnexion : la session de l'utilisateur est maintenant clôturée. Le cookie est invalidé.

- Un cookie d'identification est en fait une chaine de caractères aléatoire et **unique**, suffisamment longue pour qu'elle ne puisse pas être générée deux fois par erreur. Exemple d'un cookie d'identification : D6F8B2BE3ED3040D9A3C10-D6F8B2A305D048B9

# Les attaques Web

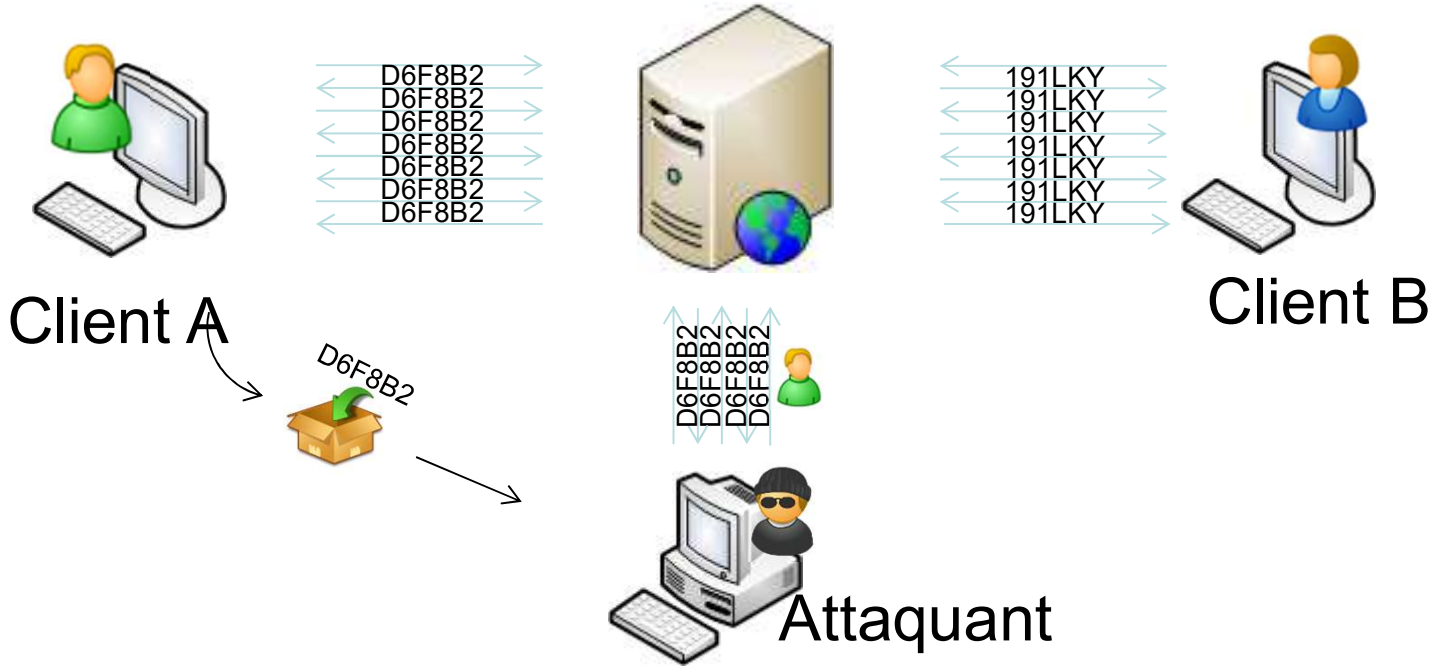
A tout moment d'une connexion, chaque utilisateur du site web possède donc son propre cookie, unique à lui. Le serveur est donc en mesure d'identifier à qui appartient chaque connexion, et donc d'afficher les pages web qui lui sont propre.


Client A Serveur Client B

# Les attaques Web

Mais que se passe-t-il si un attaquant arrive à dérober le cookie d'un utilisateur et se connecte au même serveur ?

•Il se fait passer pour l'utilisateur dont il a dérobé le cookie au près du serveur applicatif ! Il usurpe donc l'identité de la victime et accède à son compte.



# Les attaques Web

L'attaquant peut dérober un cookie d'identification par différents moyens :

– soit en écoutant le trafic réseau HTTP et en interceptant les données applicatives, dont le cookie ;
  - Moyen de protection : l'utilisateur doit **s'assurer que le site auquel il est connecté utilise du HTTPS** (le cookie est donc chiffré pendant le transport).

– soit en dérobant le cookie sur le poste de travail en utilisant une vulnérabilité du système ;
  - Moyen de protection : l'utilisateur doit **sécuriser son système d'exploitation et ses logiciels** correctement (services inutiles désactivés, installation des mises à jours de sécurité, anti-virus, etc. voir le module 2 pour plus d'informations).

– soit en dérobant le cookie sur le poste de travail via des méthodes d'ingénierie sociale ciblées sur l'utilisateur ;
  - Moyen de protection : l'utilisateur doit **être sensibilisé aux méthodes d'ingénierie sociale** (phishing, spam, etc.) afin de « ne pas tomber dans le panneau »

– soit en dérobant le cookie via une faille sur le serveur ;
  - Moyen de protection : l'exploitant du serveur doit **suivre les bonnes pratiques de sécurisation et du maintien en condition de sécurité** du serveur, ainsi que les **bonnes pratiques de développement applicatif**.

# Les attaques Web

## *b. Injection SQL*

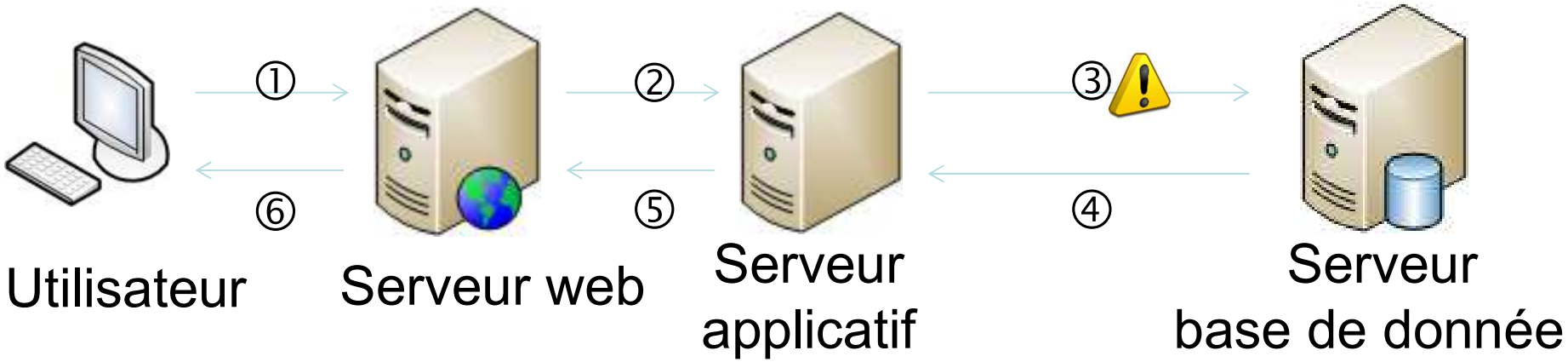
- Une attaque par injection SQL permet à un **attaquant d'interagir directement avec la base de données** d'un site web (alors que l'accès à cette base est bien entendu interdite) ;

- L'objectif de ce type d'attaque est en général de **contourner le mécanisme d'authentification, d'accéder ou de modifier frauduleusement les données** confidentielles de la base (mots de passe, téléphones, numéro de carte bancaire, etc.) ;

- Il existe de multiples variantes possibles, la diapositive suivante présente un exemple de contournement d'authentification d'une page web.

# Les attaques Web

Architecture standard logicielle d'un site web faisant appel à une base de données




① Le navigateur client demande l'affichage d'une page ;
②Le serveur web transfère la demande au serveur applicatif ;
③Le serveur applicatif génère une requête SQL afin de récupérer les informations nécessaires ;
④Le serveur base de données retourne le résultat de la requête au serveur applicatif ;
⑤Le serveur applicatif transmet au serveur web les informations nécessaires à la création de la page à afficher ;
⑥ Le serveur web envoie les pages HTML au navigateur client.

# Les attaques Web

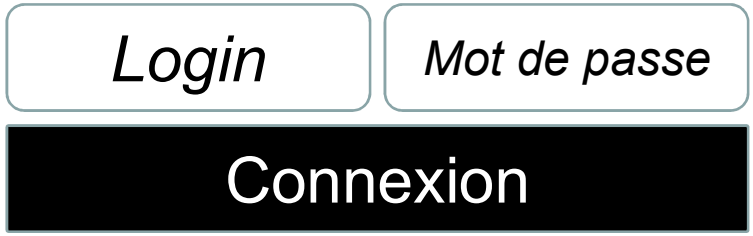
- L'objectif d'une attaque de type injection SQL consiste à détourner la requête SQL de l'étape 3 (diapositive précédente), et – en fonction du contexte – créer sa propre requête SQL malveillante ;

- La diapositive suivante illustre comment une telle attaque peut être menée à partir d'un navigateur client.

# Les attaques Web

Formulaire WEB :

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion :




$user contient le login renseigné dans le formulaire par l'utilisateur.
$mdp contient le mot de passe.

La requête SQL permettant de vérifier le login et le mot est la suivante :

```
select count(*) from user where user='$user' and mdp='$mdp'
```

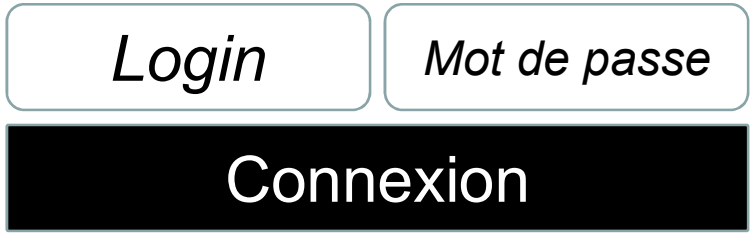
Ainsi, une requête légitime serait la suivante :

```
select count(*) from user where user='thomas' and mdp='cykUfl9an'
```

# Les attaques Web

## Formulaire WEB :

Entrez votre identifiant et votre mot de passe puis cliquez sur Connexion.




Mais que se passe-t-il si un attaquant rentre précisément les chaines de caractères suivantes ?

Login : azerty

Mot de passe : **abcd' or 1=1/***

La requête SQL `select count(*) from user where user='$user' and mdp='$mdp'`

devient donc : `select count(*) from user where user='azerty' and mdp='abcd' or 1=1/*'`

Cette condition est toujours vraie !

# Les attaques Web

- La condition étant toujours vraie, la requête est donc toujours valide, quel que soit le mot de passe renseigné par l'attaquant !
  - Les caractères /* sont utilisés pour ignorer la fin de la requête légitime.
- La faiblesse réside ici dans le code applicatif : les **données** renseignées par l'utilisateur (i.e. un attaquant dans notre scénario) **ne sont pas vérifiées/validées ;** elles sont au contraire utilisées telles quelles sans aucune vérification préalable qu'elles sont « inoffensives »
- Comment s'en protéger ?
  - **Valider systématiquement chaque donnée** extérieure avant de l'utiliser ;
  - Recourir à des requêtes préparées (connues sous le nom de « **prepared statements** »), qui ont l'avantage d'être plus résistantes aux injections ;
  - D'une façon générale, **respecter les bonnes pratiques de développement** recommandées par l'industrie concernant le code PHP, Java, etc.

# Les attaques APT

- Une **Advanced Persistent Threat** (traduction littérale, **menace persistante avancée** ; en anglais, souvent abrégé ***APT***) est un type de piratage informatique furtif et continu, souvent orchestré par des humains ciblant une entité spécifique.

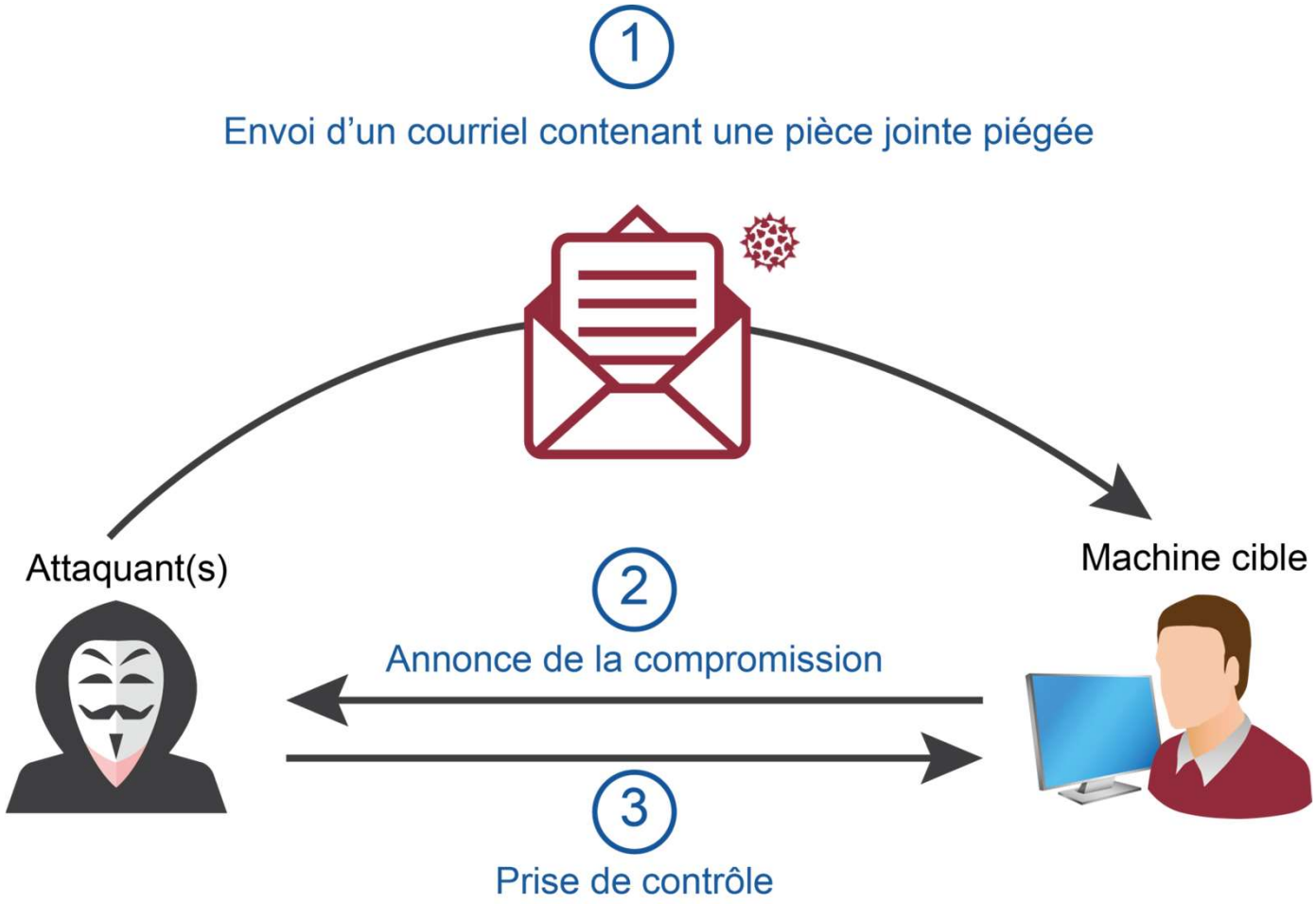
# Les attaques APT

- Une APT **cible généralement une organisation** pour des **motifs d'affaires** ou un **État** pour des **motifs politiques**.
- Une APT exige un degré élevé de dissimulation sur une longue période de temps. Le but d'une telle attaque est de placer du code malveillant personnalisé sur un ou plusieurs ordinateurs pour effectuer des tâches spécifiques et rester inaperçu pendant la plus longue période possible.

# Les attaques APT

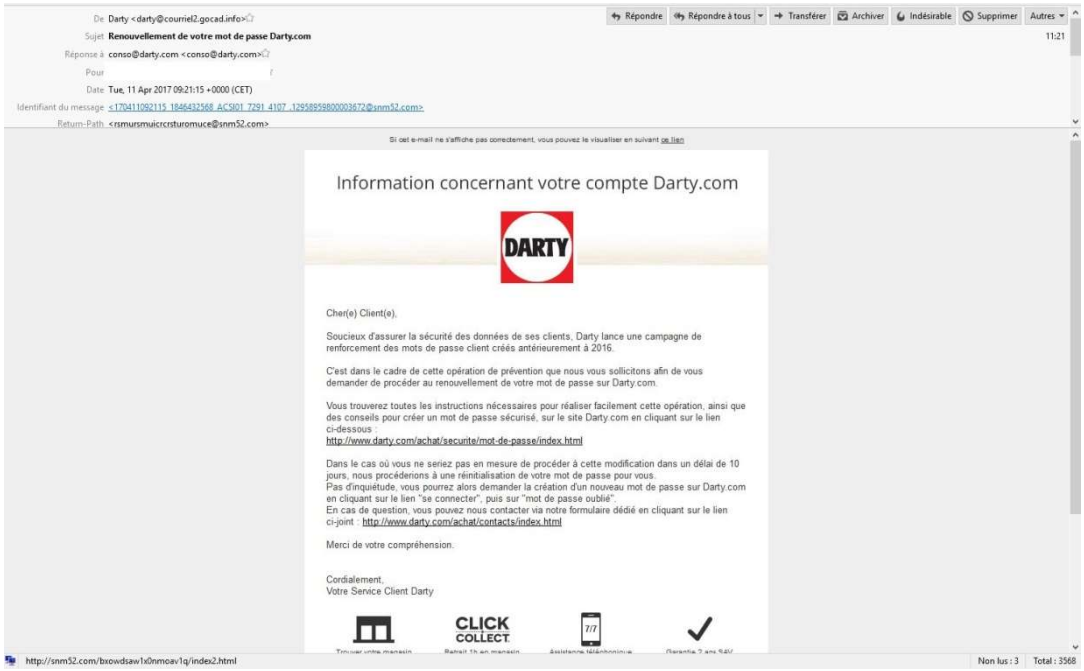
- Le terme *Advanced Persistent Threat* est aussi utilisé pour désigner un groupe, comme un gouvernement, avec à la fois la capacité et l'intention de cibler, de façon persistante et efficace, une entité spécifique.
- Un individu, comme un pirate informatique, n'est généralement pas désigné comme un *Advanced Persistent Threat*, car il n'a pas les ressources pour être à la fois avancé et persistant.

# Déroulement d'une attaque avancée



# Déroulement d'une attaque avancée

- Compromission initiale
  - *Phishing* et *spear phishing*



# Déroulement d'une attaque avancée

- Compromission initiale
  - Utilisa
    - Cor
    - Cor
    - Écri
    - Dét
    - Utili

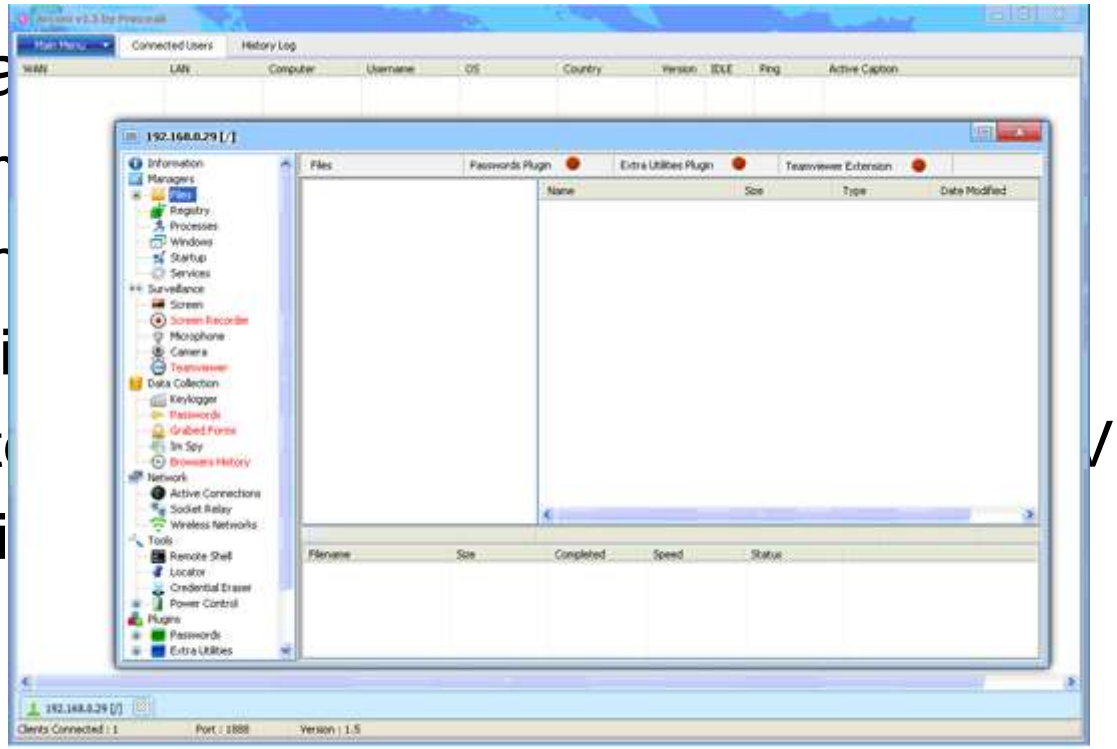
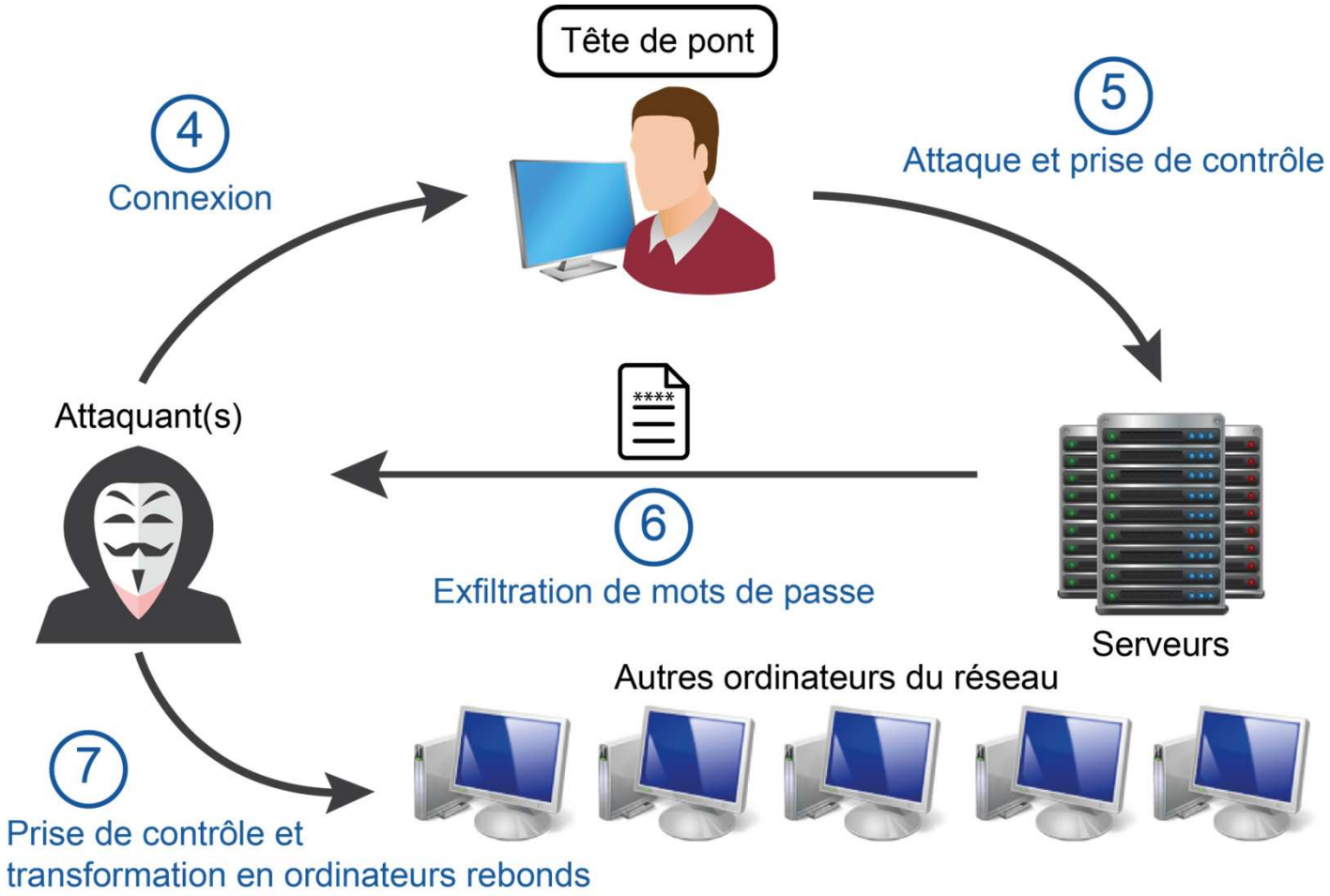


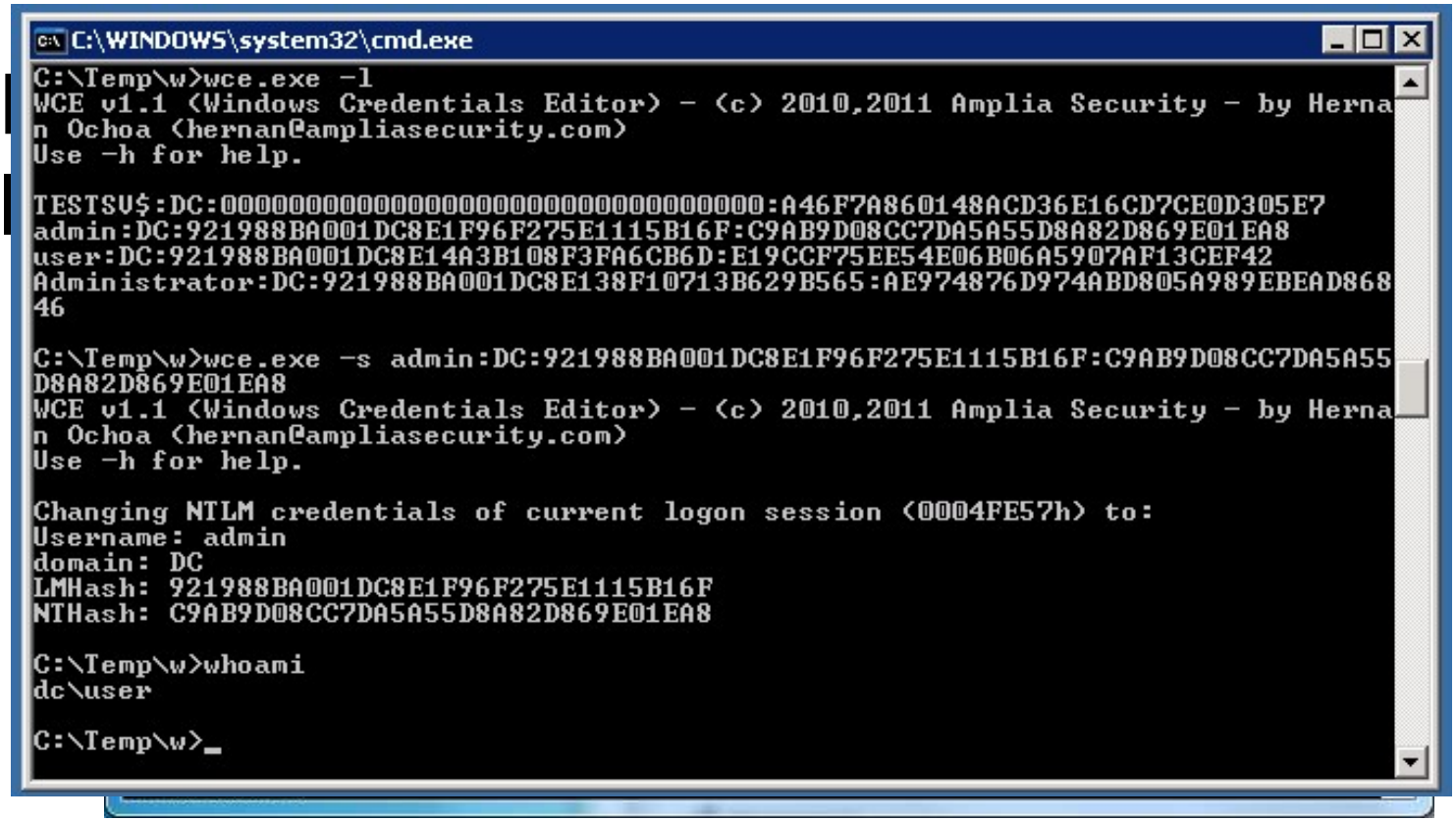

Figure 2. Cybercriminals use this to control compromised systems

# Déroulement d'une attaque avancée

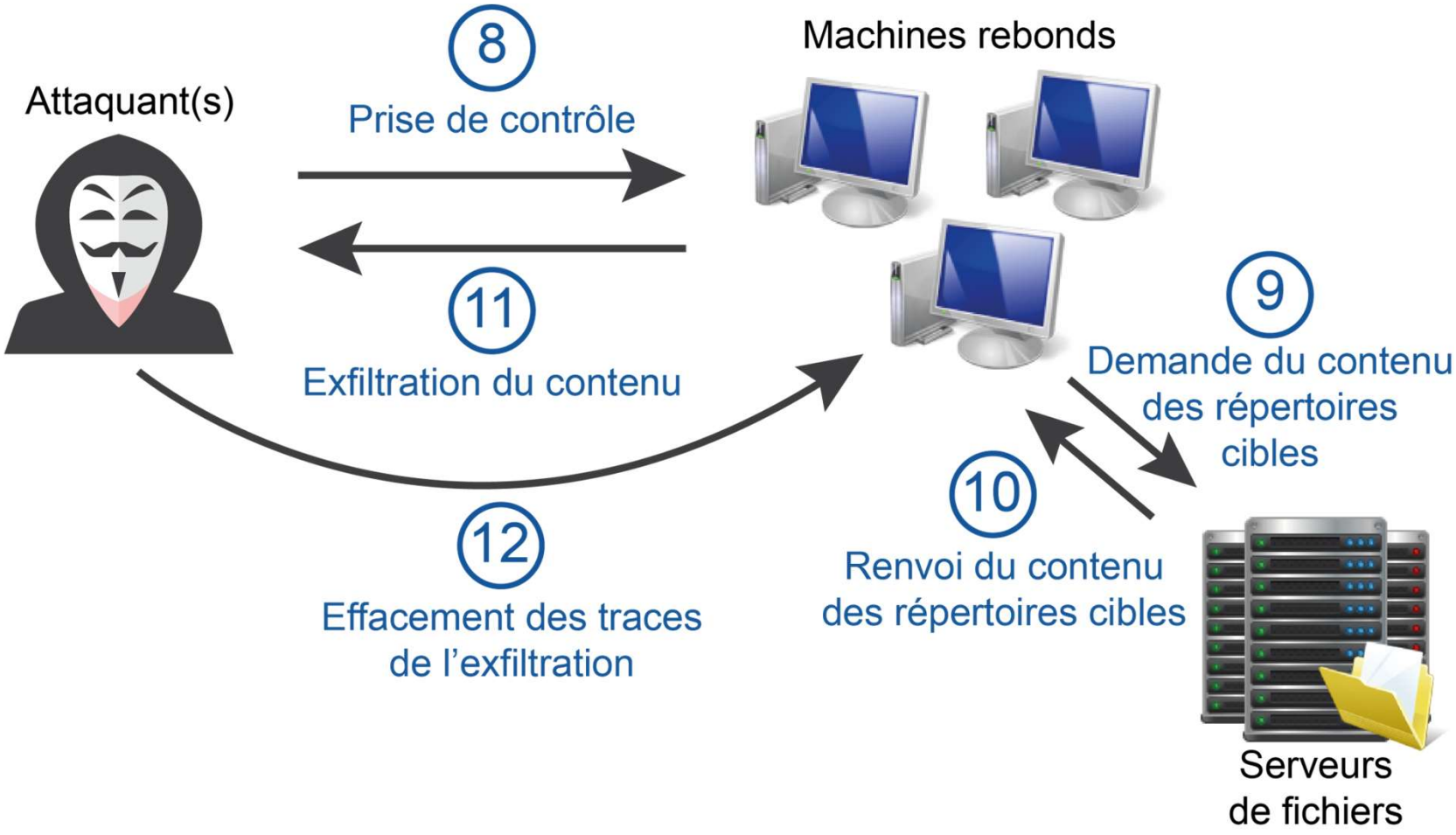


# Déroulement d'une attaque avancée

- I ts



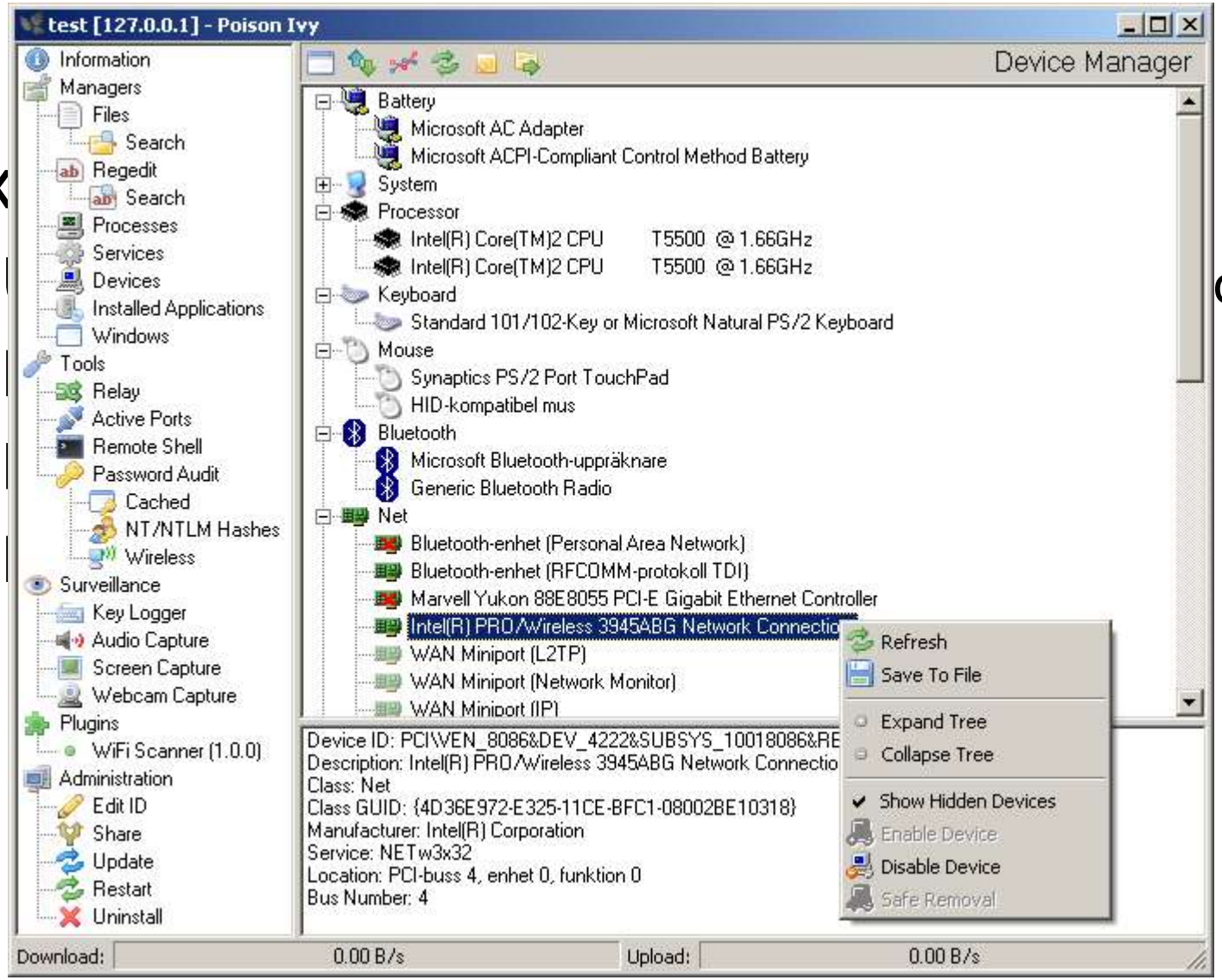
# Déroulement d'une attaque avancée



# Déroulement d'une attaque

- Ex
  - 
  - 
  - 
  - 

ool)

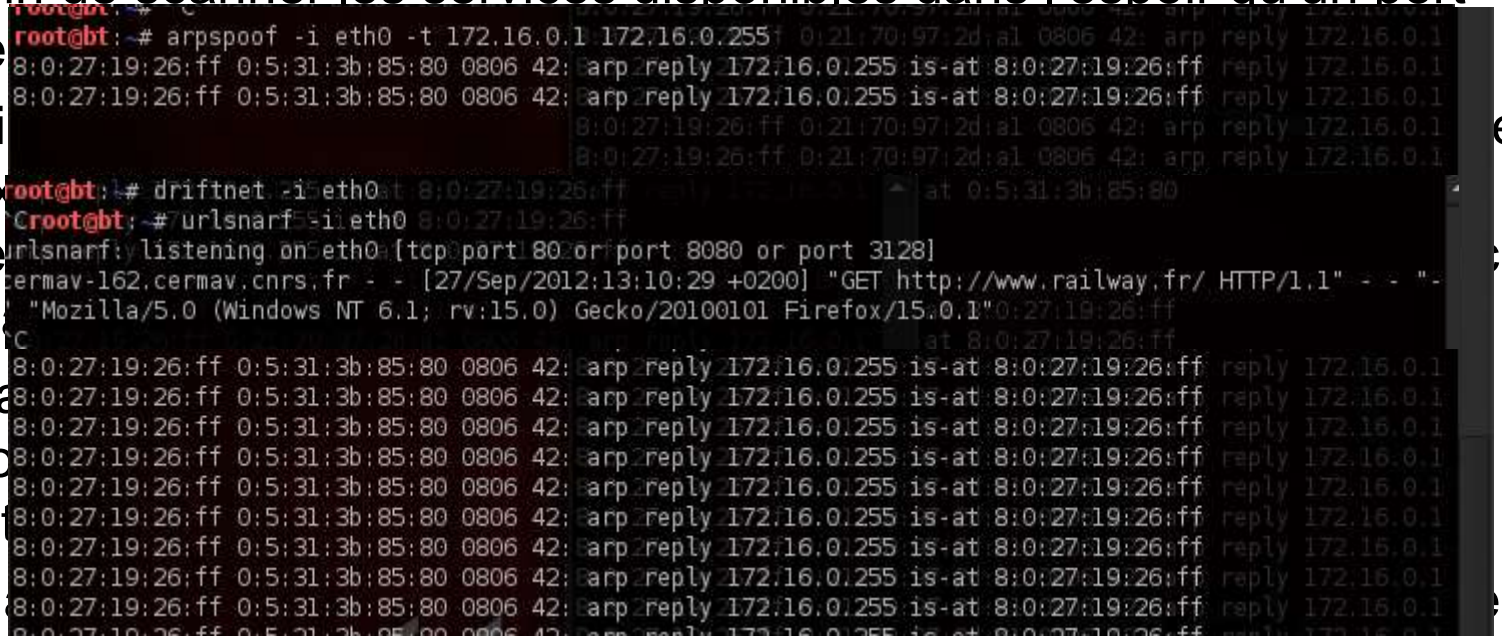


# 4.3 Types d'attaques (1/3)

- DoS (Denial of service, déni de service) : Faire décroître la capacité du système
- DDoS (Distributed DoS) : idem mais avec une attaque provenant de plusieurs emplacements (http://grc.com/dos/grcdos.htm)
- SYN Flood: l'attaquant inonde un système de paquets de synchronisation SYN afin d'initier des requêtes de connexion jamais terminées => forte exploitation des ressources processeur, mémoire, carte réseau => déni de service
- UDP Flood: attaque qui submerge un système de paquets UDP et le ralentit pour l'empêcher de traiter les demandes de connexion valides (souvent sur le port 53 DNS) (ICMP Flood : idem pour submerger un système de messages ICMP (Internet Control Message Protocol) en utilisant l'utilitaire Ping)

# 4.3 Types d'attaques (2/3)

- Scan de ports : Paquets envoyés en utilisant des numéros de port afin de scanner les services disponibles dans l'espoir qu'un port ré
- Pi e ex ce, ré pl
- Ea co int
- M la communication comme s'il était l'interlocuteur attendu : conséquences néfastes sur la confidentialité et éventuellement l'intégrité



# 4.3 Types d'attaques (3/3)

- Java/ActiveX/ZIP/EXE: composants Java ou Active X malveillants cachés dans des pages Web, chevaux de Troie dissimulé dans un fichier ZIP/TAR ou EXE
- Breaking into a system: en violant l'authentification ou le contrôle d'accès, l'attaquant obtient la possibilité de contrôler la communication : conséquences sur la confidentialité et l'intégrité
- Virus : court-circuite l'authentification et le contrôle d'accès dans le but d'exécuter du code destructeur : conséquences sur la disponibilité de la machine et/ou du réseau
- Chevaux de Troie (trojan) : virus caché dans une fonction habituellement utilisée, programme s'exécutant sur la machine piratée pour envoyer de l'information au pirate
- Vers (Worm) : explore et exploite automatiquement les failles d'un système, sans action d'utilisateur : entraîne des problèmes de disponibilité

# Détection des attaques

- Par les opérateurs humains (culture, formation)
- Par des logiciels ou matériels spécialisés (anti-virus, pare-feux, IDS)
- Par des ports normalement non ouverts (scan d'alertes)
- Par des réactions anormales
  - Lors des connexions, en votre absence
  - Des applications (lente, double validation)
- Par des surcharges anormales
  - Ressources réseaux
  - Ressources processeur, disque, mémoire…
- Par des données invalides
- Par des pertes de données

Tout événement anormal doit rendre très « vigilant » !

# 4.4 Les organismes de sécurité

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques)
  - www.certa.ssi.gouv.fr
- SANS (SysAdmin, Audit, Network, Security)
  - www.sans.org
  - Recherche en sécurité des informations
- SCORE (Security Consensus Operational Readiness Evaluation)
  - www.sans.org/score
  - Communauté de professionnels en sécurité
- ISC (Internet storm center)
  - http://isc.sans.org
  - Journal concernant les détections d'intrusion
- ANSSI
  - www.ssi.gouv.fr
  - Agence Nationale de Sécurité des Systèmes d'Information

# Les organismes de sécurité

https://www.cert.ssi.gouv.fr/

## ALERTES DE SÉCURITÉ

*Les alertes sont des documents destinés à prévenir d'un danger immédiat*

| | | | |
|---|---|---|---|
| 4 janvier 2018 | CERTFR-2018-ALE-001 | Multiples vulnérabilités de fuite d'informations dans des processeurs | Alerte en cours |
| 1 février 2018 | CERTFR-2018-ALE-002 | Vulnérabilité dans Cisco Adaptive Security Appliance | Alerte en cours |
| 13 décembre 2017 | CERTFR-2017-ALE-020 | Vulnérabilité dans des implémentations de TLS | Alerte en cours |
| 5 décembre 2017 | CERTFR-2017-ALE-019 | Vulnérabilité d'usurpation d'identité dans plusieurs clients de messagerie | Alerte en cours |
| 2 février 2018 | CERTFR-2018-ALE-003 | Vulnérabilité dans Adobe Flash Player | Cloturée le 07/02/2018 |

VOIR TOUTES LES ALERTES »

## AVIS DE SÉCURITÉ

*Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir*

| | | |
|---|---|---|
| 6 mars 2018 | CERTFR-2018-AVI-112 | Multiples vulnérabilités dans Google Android |
| 5 mars 2018 | CERTFR-2018-AVI-111 | Vulnérabilité dans les produits Pivotal |
| 2 mars 2018 | CERTFR-2018-AVI-110 | Vulnérabilité dans le noyau Linux de SUSE |
| 2 mars 2018 | CERTFR-2018-AVI-109 | Multiples vulnérabilités dans PHP |

# Egalement les systèmes industriels

des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.

### MULTIPLES VULNÉRABILITÉS DANS LES PRODUITS INTEL

CERTFR-2018-AVI-432 • *Publié le 12 septembre 2018*

De multiples vulnérabilités ont été découvertes dans les produits Intel. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données.

### MULTIPLES VULNÉRABILITÉS DANS GOOGLE CHROME

CERTFR-2018-AVI-431 • *Publié le 12 septembre 2018*

De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.

### MULTIPLES VULNÉRABILITÉS DANS ADOBE FLASH PLAYER ET COLD FUSION

CERTFR-2018-AVI-430 • *Publié le 12 septembre 2018*

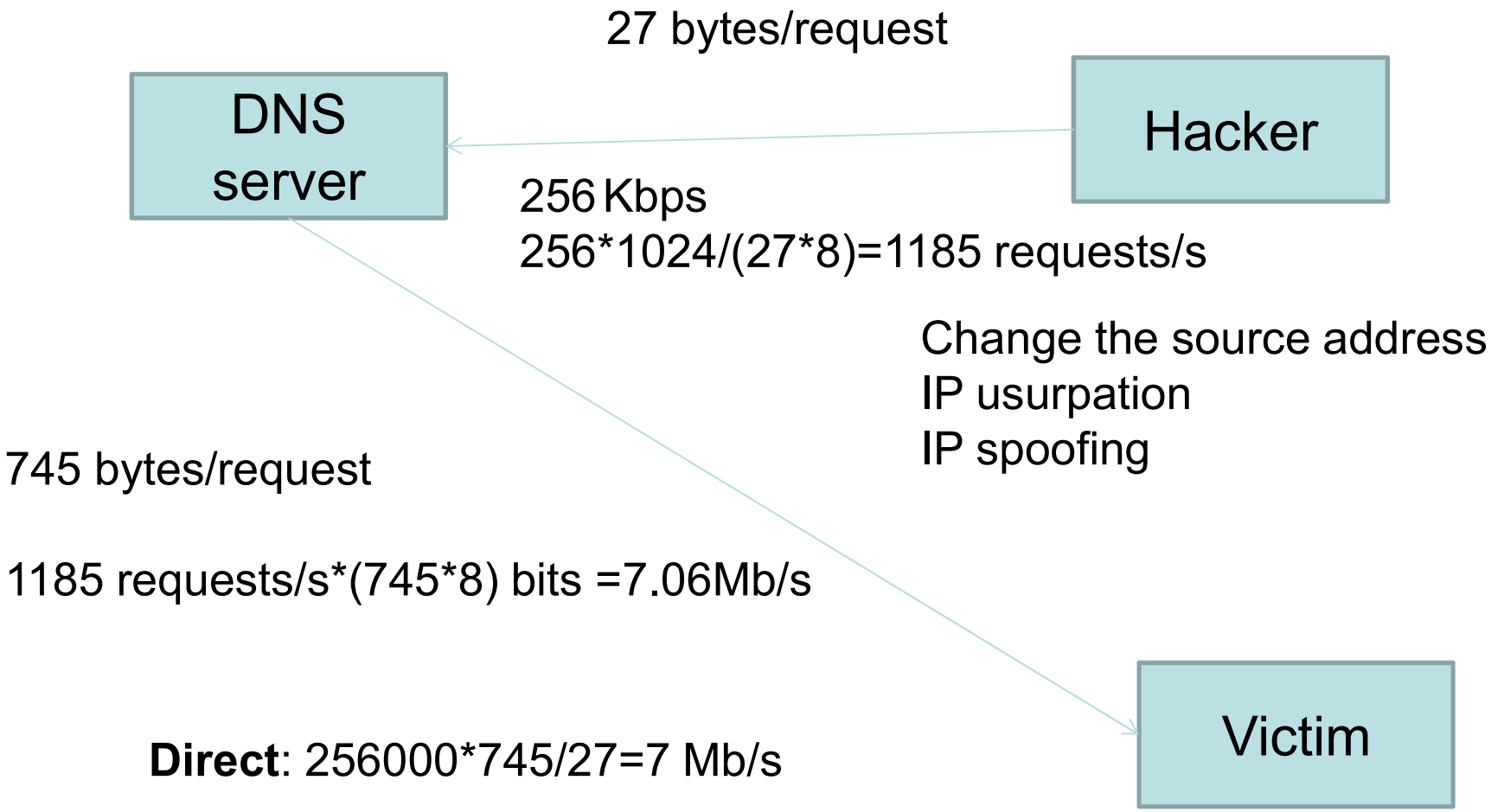
De multiples vulnérabilités ont été découvertes dans Adobe Flash Player et Cold Fusion. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.

### MULTIPLES VULNÉRABILITÉS DANS SCADA LES PRODUITS SIEMENS

CERTFR-2018-AVI-429 • *Publié le 11 septembre 2018*

De multiples vulnérabilités ont été découvertes dans SCADA les produits Siemens. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une élévation de privilèges.

# Attack by third party




**Direct**: 256000*745/27=7 Mb/s

# URL de références

- www.ssi.gouv.fr
- www.insecure.org
- www.tigertools.net
- www.deter.com/unix/index.html
- www.nessus.org
- www.cerias.purdue.edu/coast/satan.html
- www.uk.research.att.com/archive/vnc
- www.iss.net
- www.wallix.com
- www.checkpoint.com
- www.laser.epfl.ch/securitereseaux
- www.urec.fr
- www.afnic.fr
- www.icann.org
- www.internic.ne
- www.isc.org
- www.loria.fr/services/moyens-info/securite/
- …

# Sentences for security

- I should prove that I have done the best as possible compare to the actual/present state of the art
- Everything your system need should be explicitely authorized. Everything which is not authorized is FORBIDDEN.

# Références Bibliographiques


- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Cours de Jean-Luc Noizette, ESSTIN, Nancy.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006
- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – Sûreté de fonctionnement des systèmes industriels – Editions Eyrolles, Paris, 1988.
- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Guide d'autodéfense numérique,** *éditions Tahin Party*
- **Cybertactique : Conduire la guerre numérique,** Bertrand Boyer, *Nuvis*
- **Learn Social Engineering***, Dr E. Orzkaya,* 2018, Packt

- L’utilisation des méthodes décrites dans ce cours engage la responsabilité des utilisateurs !