Université Grenoble Alpes

M33-2. Cyber-attaques

M33-2. 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).

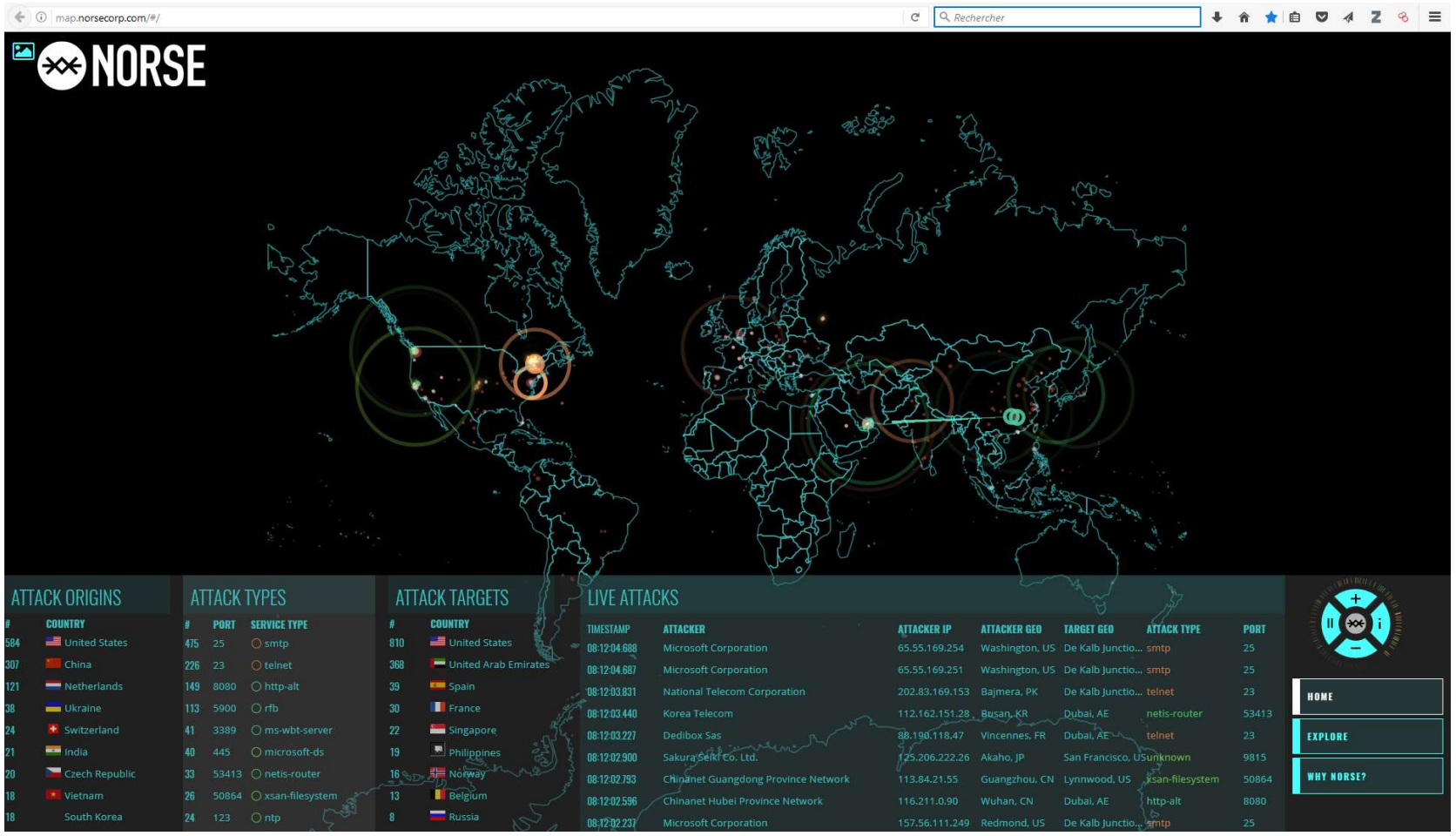
Considérations juridiques

- **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

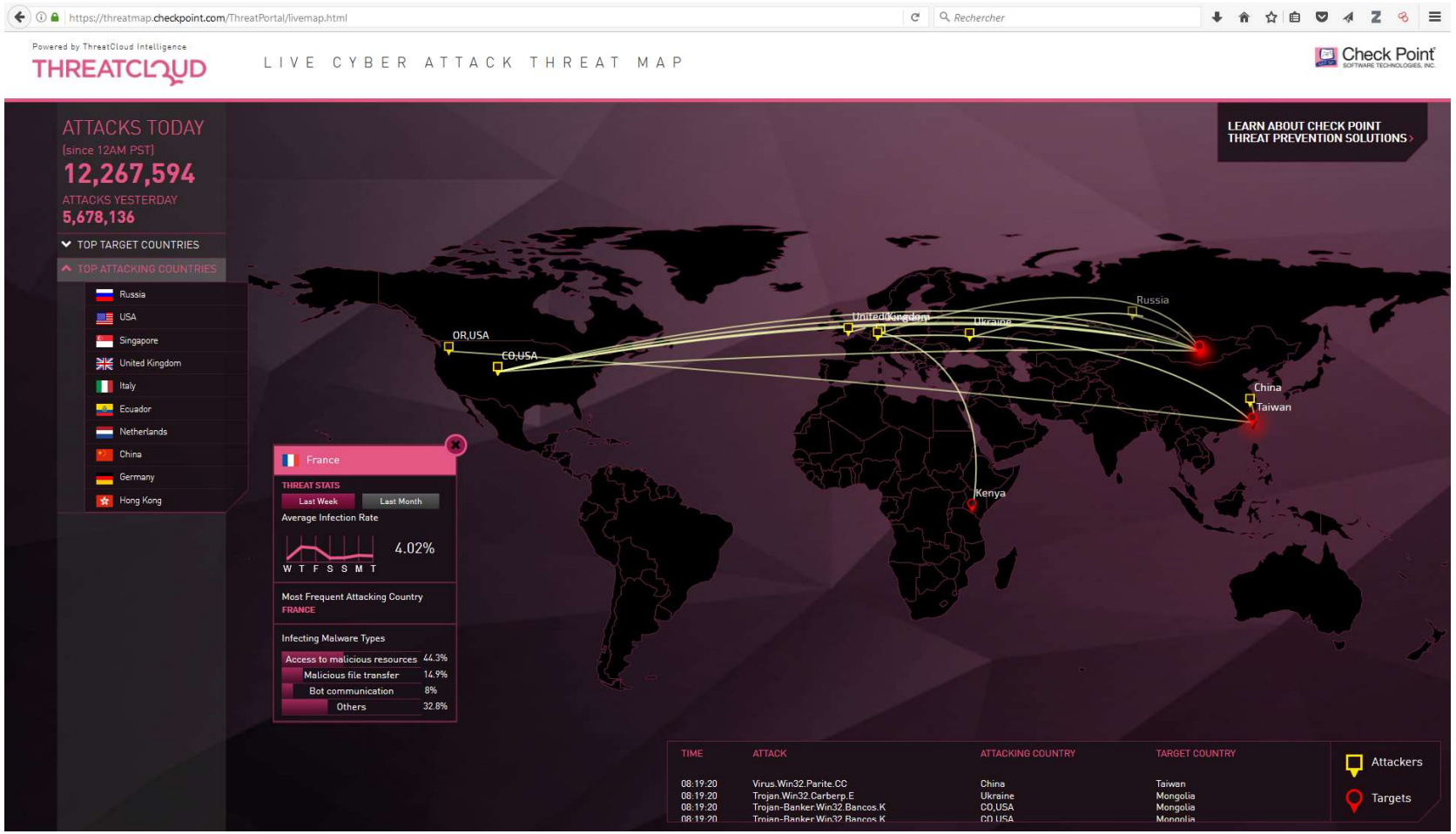
L'utilisation des méthodes décrites dans ce cours engage la responsabilité des utilisateurs en cas d'usage !

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



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

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



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 ?

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

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

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

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking:** ↗ Going up, --- Same, ↙ Going down

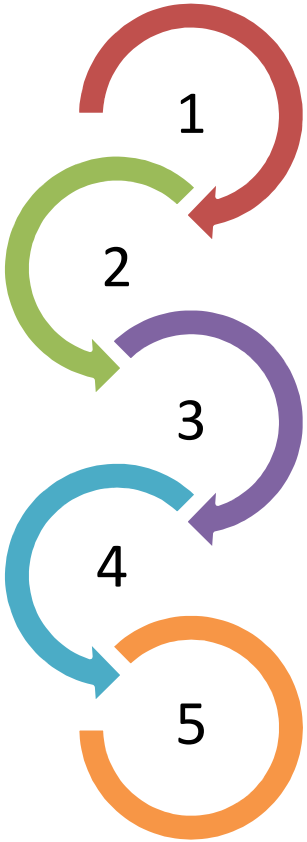
Source : ENISA Threat Landscape 2020

Université Grenoble Alpes

F t-ils aux S.I. ndividus ?

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

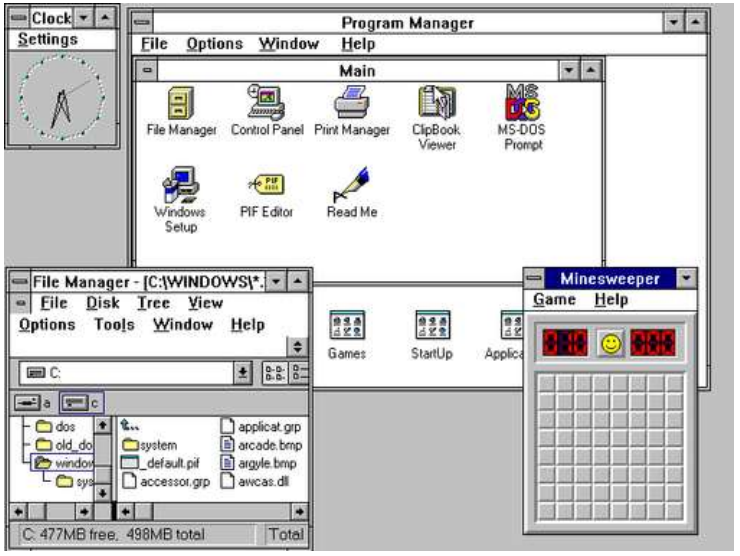
2.399 $ le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $)

Les 3 couches cyber

- La couche physique
  - Equipements réseaux, câbles
  - Ordinateurs
  - …

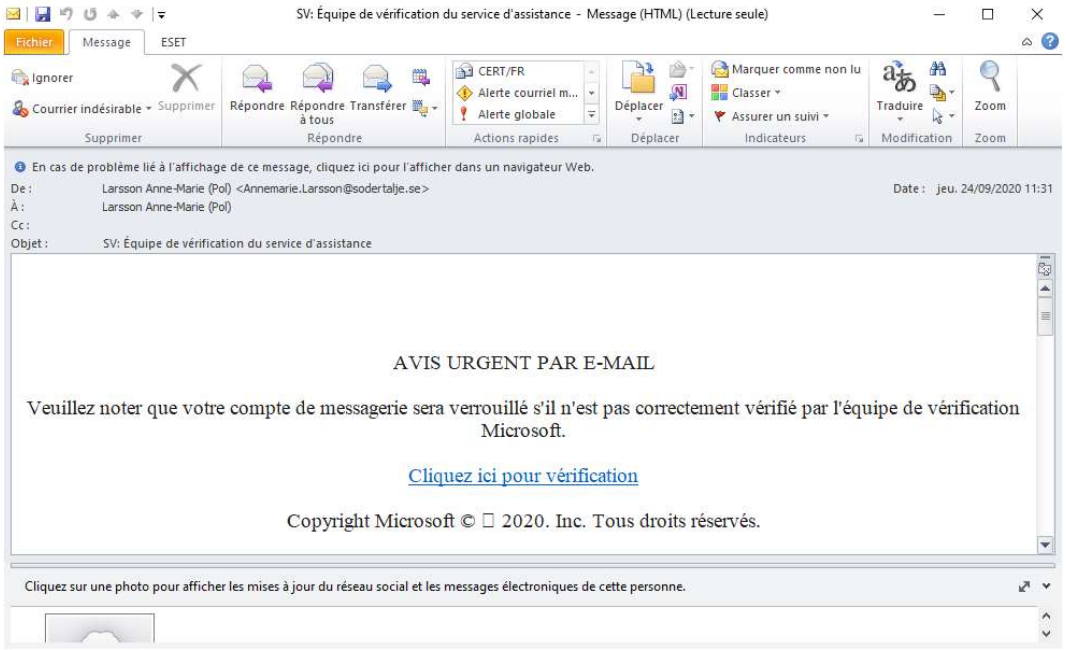
Les 3 couches cyber

- La couche logique ou logicielle :
  - Système d'exploitation
  - Suite bureautique
  - Navigateur web
  - …



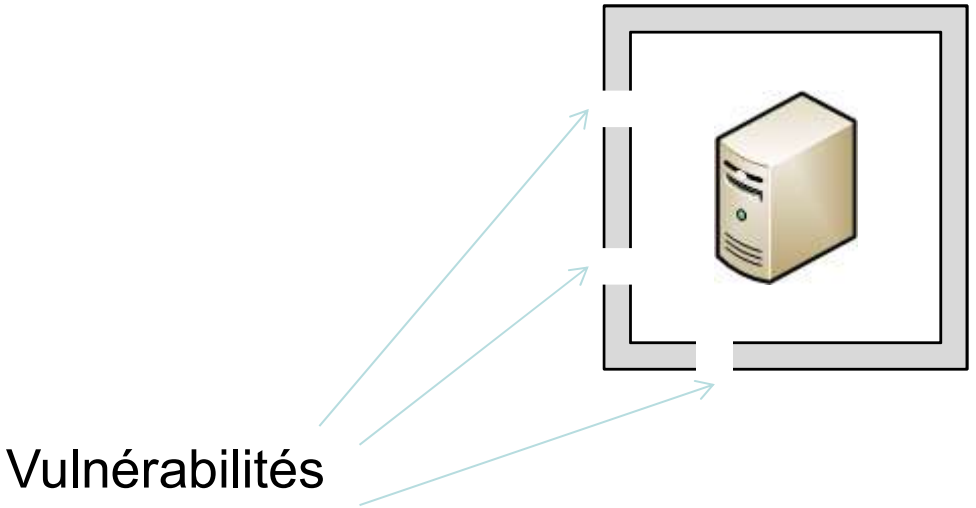
Les 3 couches cyber

- La couche sémantique, ce que nous comprenons :
  - D'un courriel
  - D'une page web
  - D'un document
  - …



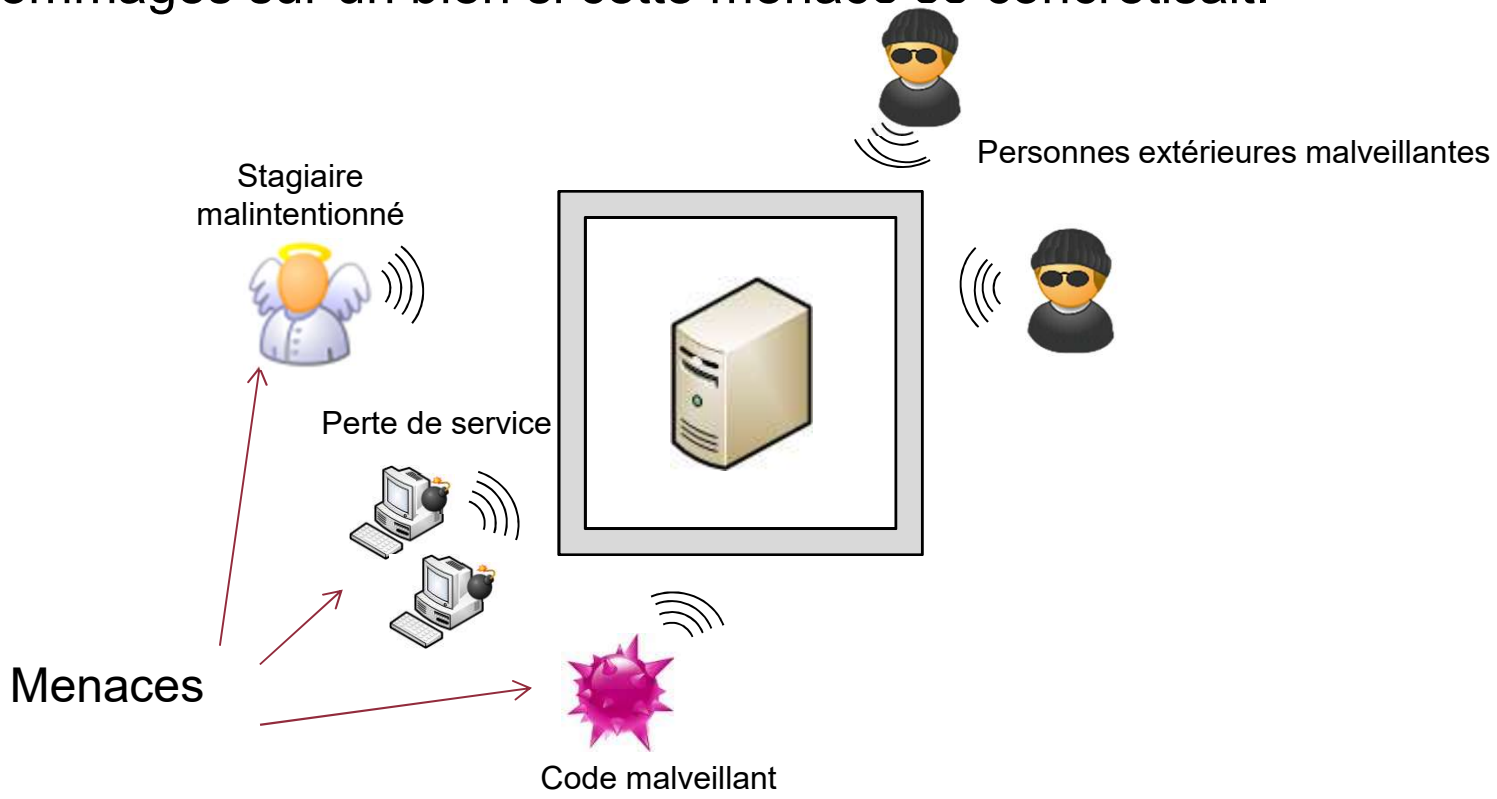
Notions de vulnérabilité, menace, attaque

- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



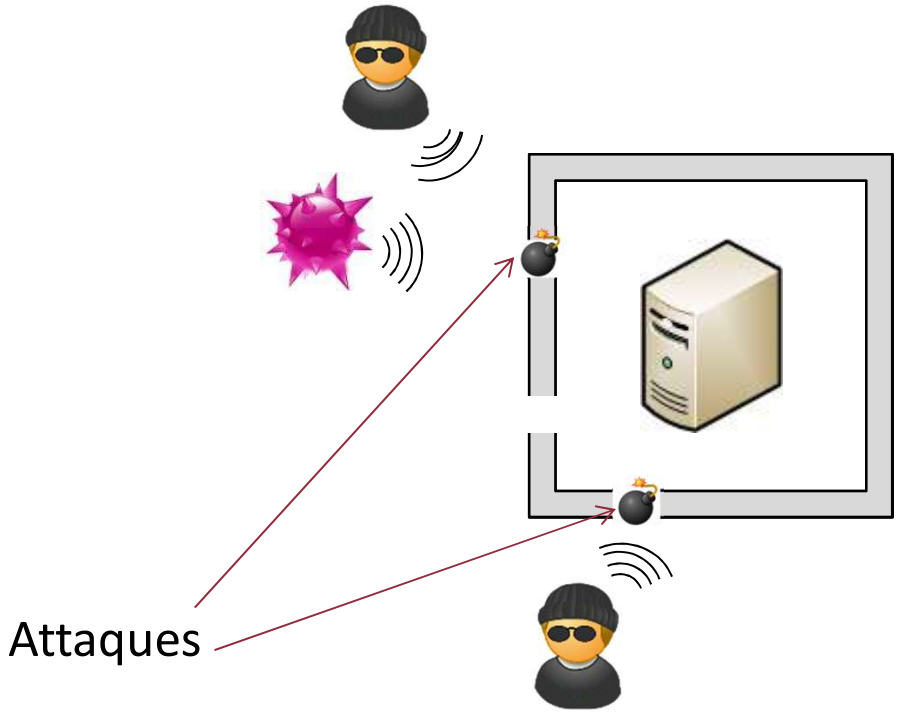
Notions de vulnérabilité, menace, attaque

- **Menace**
- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



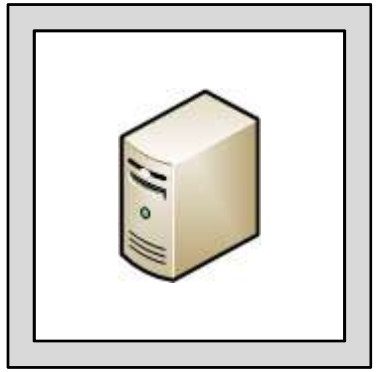
Notions de vulnérabilité, menace, attaque

- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



Notions de vulnérabilité, menace, attaque

- **Attaque**
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.



Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

M33-2. Cyber-attaques

- Les ingrédients
  - Ressources informatiques vulnérables aux attaques
  - Types de cibles
  - Sources potentielles de menaces
  - Types d'attaquants

Ressources informatiques vulnérables aux attaques

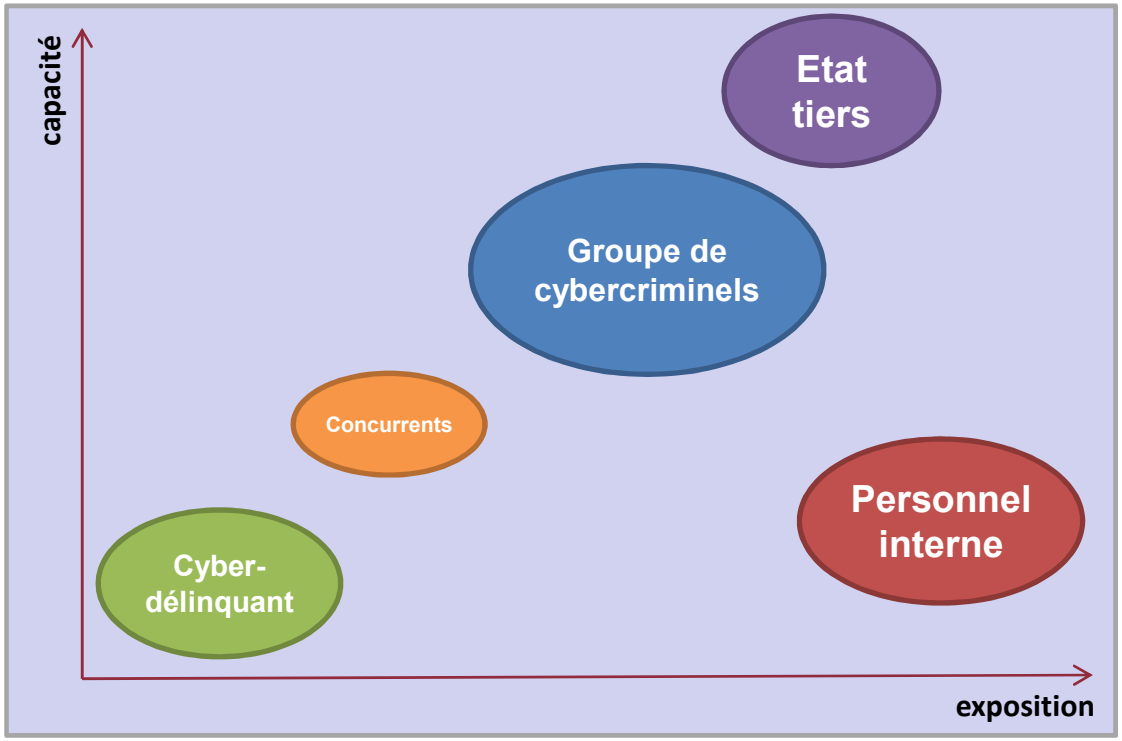
- Serveurs
  - Obtention d'une machine esclave pour attaquer d'autres cibles
- Clients
  - Machine potentiellement moins protégée
  - Vulnérable via une connexion sans fil
- Autres terminaux (sans fil)
  - Téléphones portables
- Espace disque
  - Sauvegarde de fichiers illégaux
- Bande passante
  - Utilisation d'un réseau piraté pour se connecter à d'autres réseaux
- Informations personnelles et confidentielles

matériel

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…

Sources potentielles de menaces



Exemple d'une cartographie des principales sources de menaces qui pèsent sur un S.I.

Capacité
degré d'expertise et ressources de la source de menaces

Exposition
opportunités et intérêts de la source de menaces

Attention : cette cartographie doit être individualisée à chaque organisation car toutes les organisations ne font pas face aux mêmes menaces.

Exemple : le S.I. d'une administration d'état ne fait pas face aux mêmes menaces que le S.I. d'un e-commerce ou d'une université

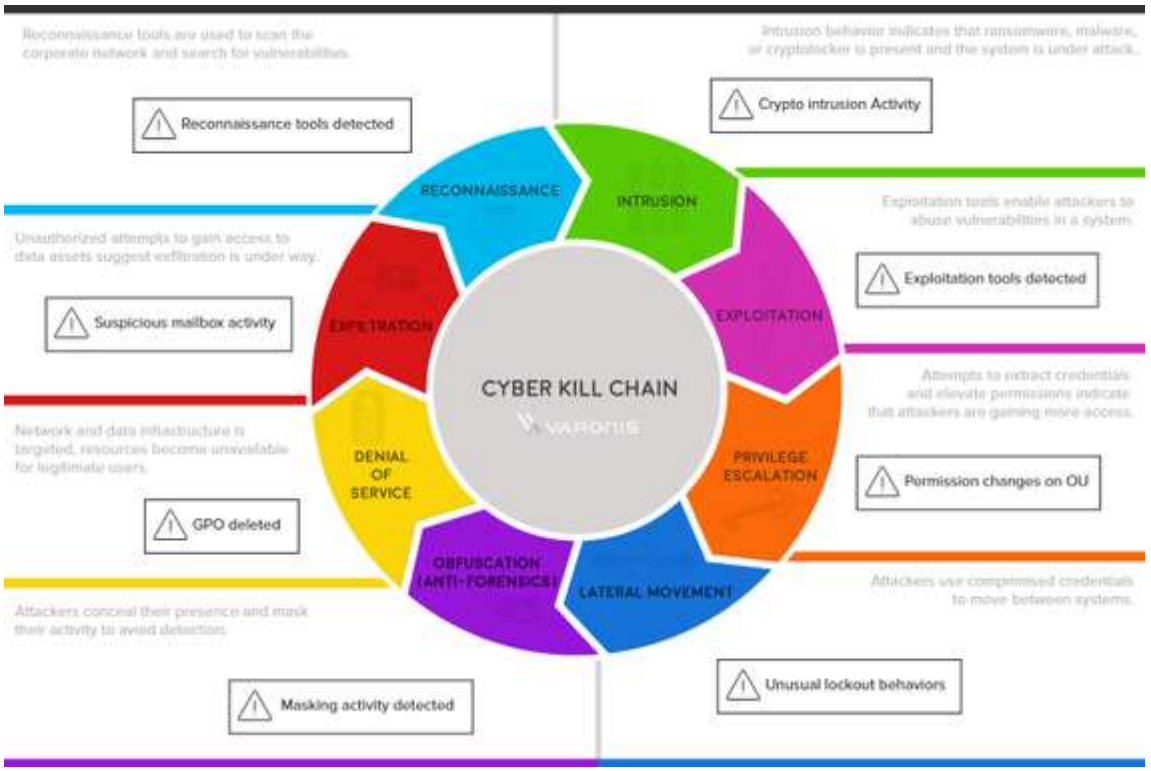
Types d'attaquants

- **Hackers** (informaticien qui utilise ses connaissances de la sécurité informatique pour en rechercher et en exploiter les faiblesses)
  - Les **chapeaux blancs** ou *white hat* : professionnels de la sécurité informatique (consultants en sécurité, administrateurs réseaux…) effectuant des tests d'intrusions en accord avec leurs clients et la législation en vigueur
  - Les **chapeaux bleus** ou *blue hat* : consultants en sécurité informatique chargés de vérifier l'absence de bogues et de corriger d'éventuels exploits avant le lancement d'un site web en ligne ou système d'exploitation sur le marché.
  - Les **chapeaux noirs** ou *black hat* : créateurs de virus, cyber-espions, cyber-terroristes ou cyber-escrocs, agissant la plupart du temps hors-la-loi dans le but soit de nuire, de faire du profit ou d'obtenir des informations.
  - Les **chapeaux gris** ou *grey hat* : s'ils n'hésitent pas à pénétrer dans les systèmes sans y être autorisés, ils n'ont pas de mauvaises intentions. C'est souvent l'« exploit informatique » qui les motive, une façon de faire la preuve de leur agilité.
  - Les ***script kiddies*** ou *lamer*, littéralement « gamins qui utilisent des scripts » : sans grande compétence, ceux-ci piratent en utilisant des programmes codés par d'autres. Ces personnes ne sont pas à proprement parler des *hackers*, mais elles peuvent se considérer comme tels.
  - Les **hacktivistes** : agissant afin de défendre une cause, ils peuvent transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations, ainsi qu'attaquer des plateformes gouvernementales dans le cadre de conflits en cours ou passés.

Types d'attaquants

- Organisation des pirates
  - Mise en commun des trouvailles
  - Motivations par des défis (*challenges*)
  - Mercenaires
  - Etatiques

M33-2. Cyber-attaques



Catégorisation des attaques

On classe les types d'attaques en deux catégories :

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

Stratégie d'une attaque

- Reconnaissance et collecte de renseignements
- Sondage et scan, énumération
- Obtention d'un accès
- Augmentation des privilèges
- Progression et intensification de la présence
- Couverture des traces

Reconnaissance et collecte de renseignements (1/4)

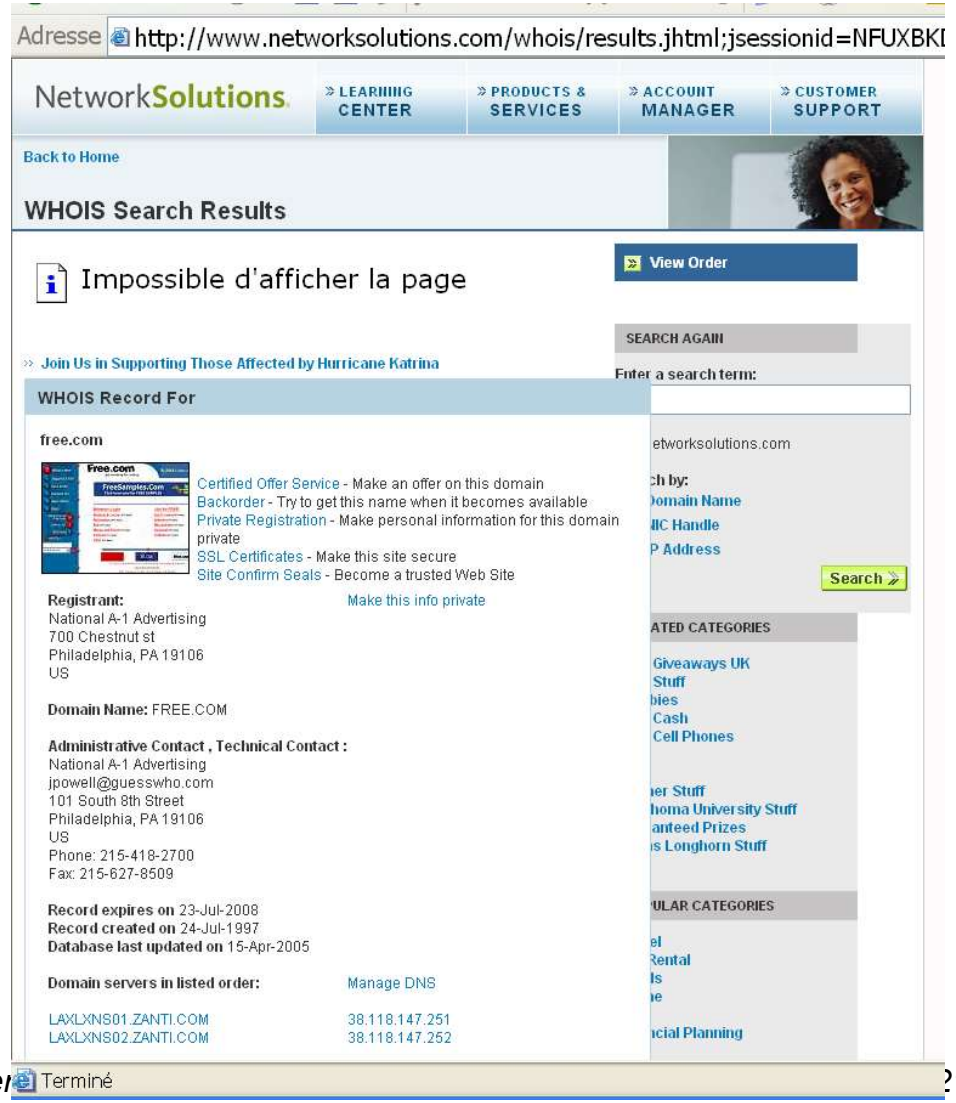
- Noms de domaine, serveurs DNS, blocs d'adresses IP a
- A
- S
- T tent
- des
- N
- Type de pare-feu et d'IDS (Intrusion Detection System)

```
root@bt:/pentest/enumeration/dns/dnswalk# ./dnswalk czarby.com.
Checking czarby.com.
Getting zone transfer of czarby.com. from ferriere.czarby.com...failed
FAIL: Zone transfer of czarby.com. from ferriere.czarby.com failed: Response code from server: REFUSED
Getting zone transfer of czarby.com. from balaruc.czarby.com...done.
SOA=ferriere.czarby.com contact=cyril\.bras.czarby.com
WARN: 192.168.254.254.czarby.com PTR routeur.czarby.com: unknown host
WARN: balaruc-vpn.czarby.com A 10.7.0.1: no PTR record
WARN: balaruc-vpn.czarby.com A 10.8.0.1: no PTR record
WARN: balaruc1.czarby.com A 192.168.1.1: no PTR record
WARN: balaruc2.czarby.com A 192.168.1.2: no PTR record
WARN: balaruc3.czarby.com A 192.168.1.3: no PTR record
WARN: balaruc4.czarby.com A 192.168.1.5: no PTR record
WARN: bb.czarby.com A 192.168.0.6: no PTR record
WARN: ferriere-mob.czarby.com A 192.168.0.3: no PTR record
WARN: ferriere-vpn.czarby.com A 10.8.0.6: no PTR record
WARN: ferriere1.czarby.com A 192.168.0.10: no PTR record
WARN: ferriere1-vpn.czarby.com A 10.7.0.6: no PTR record
WARN: ferriere2.czarby.com A 192.168.0.2: no PTR record
WARN: ferriere4.czarby.com A 192.168.0.4: no PTR record
WARN: freebox-serveur.czarby.com A 192.168.1.254: no PTR record
WARN: p-tel.czarby.com A 192.168.0.11: no PTR record
WARN: p-voip.czarby.com A 192.168.0.9: no PTR record
WARN: p-voip2.czarby.com A 192.168.1.4: no PTR record
WARN: p-wifi.czarby.com A 192.168.0.8: no PTR record
```

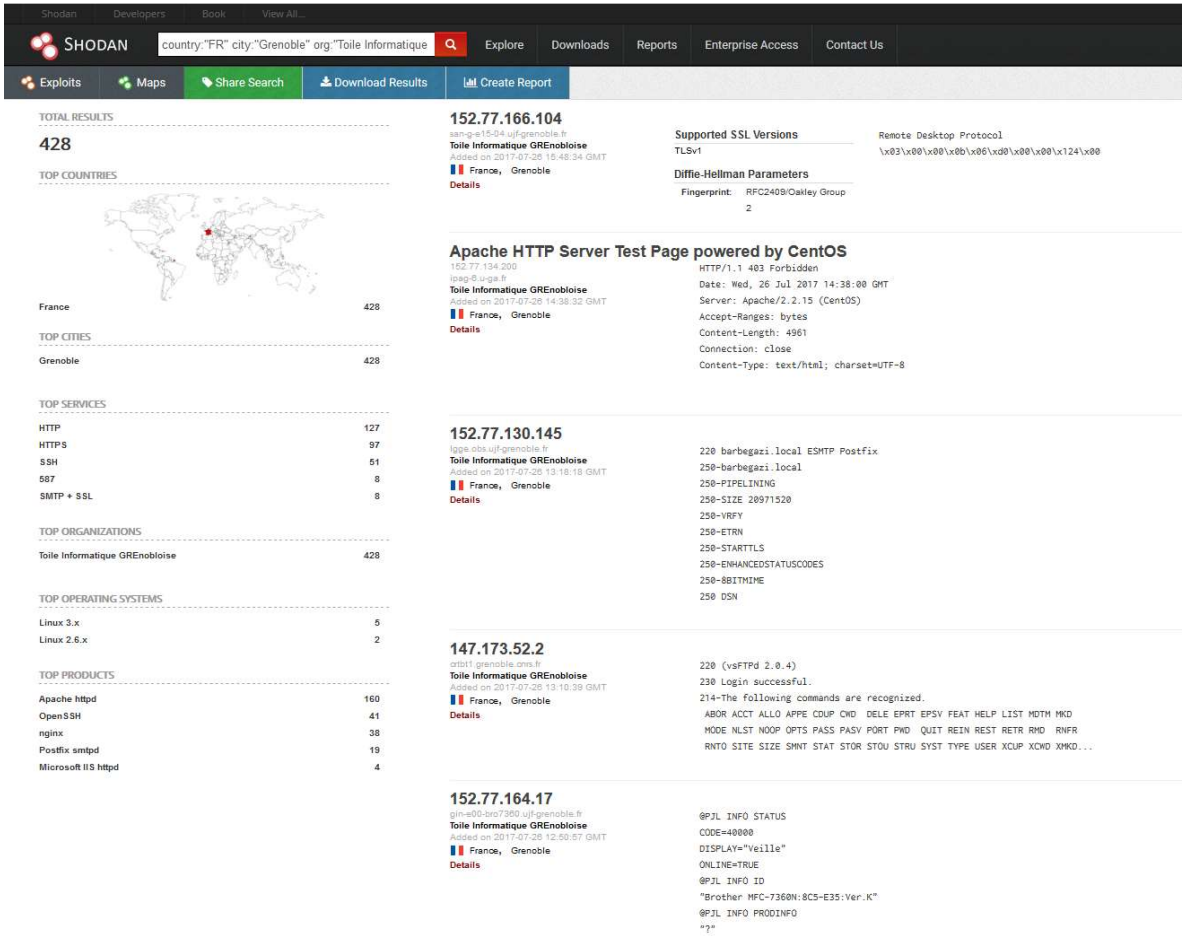
Reconnaissance et collecte de renseignements (2/4)

- 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…

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



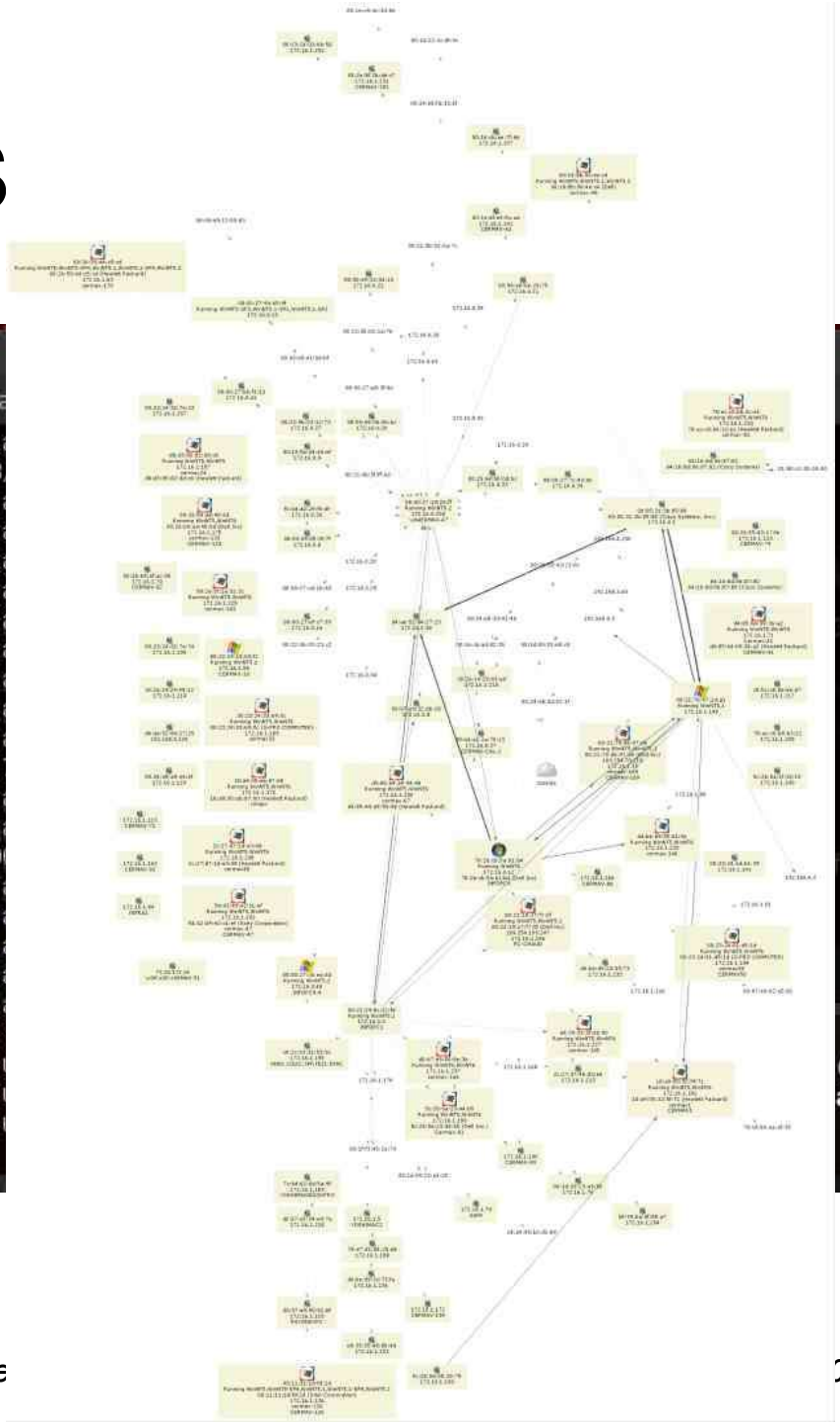
Reconnaissance et collecte de renseignements: Shodan (4/4)

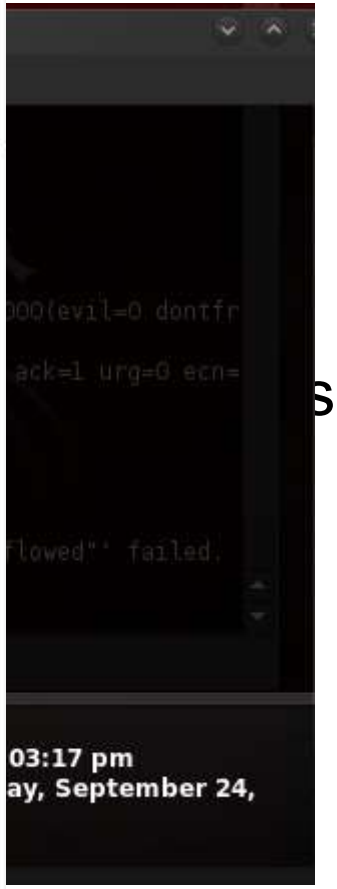


S des ports

-
- s


File Edit View Bookma
Completed SYN Stealth Sc
Discovered open port 513
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Discovered open port 491
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Discovered open port 490
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Completed SYN Stealth Sc
Initiating Service scan
Scanning 220 services on
Service scan Timing: Abo
Service scan Timing: Abo
Service scan Timing: Abo




03:17 pm
ay, September 24,

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)

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

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 !

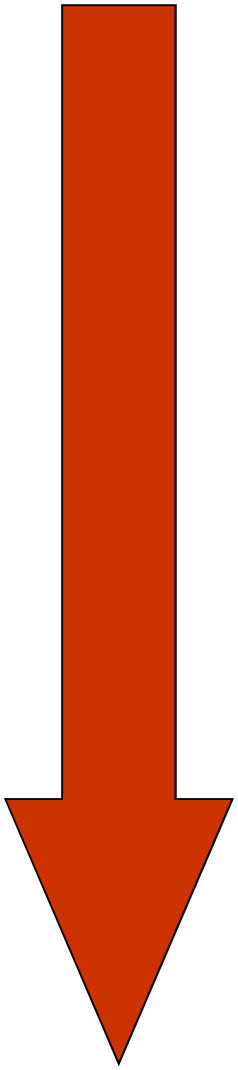
Analyse de risques: Nature des méfaits

Tolérable

Dangereux

Inadmissible

Très grave



- Simple observation
- Enregistrement des données observées
- Pénétration par fausse identité
- Substitution d'identité
- Modifications de données (limitées)
- Destruction de données (limitées)
- Perturbations de services (ralentissements)
- Dénis de service
- Destruction de service
- Arrêt de la machine (boot obligatoire)
- Arrêt d'un serveur (perte de toutes les données, nécessite une réinstallation…)

M33-2. 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

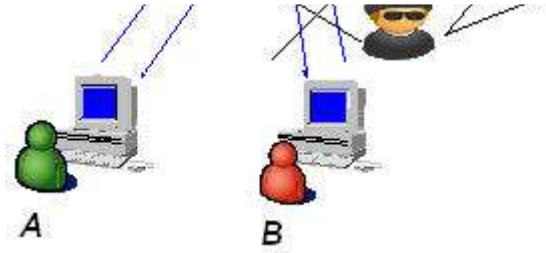
Les types d'attaques

- Deny of Service (Déni de service DOS)

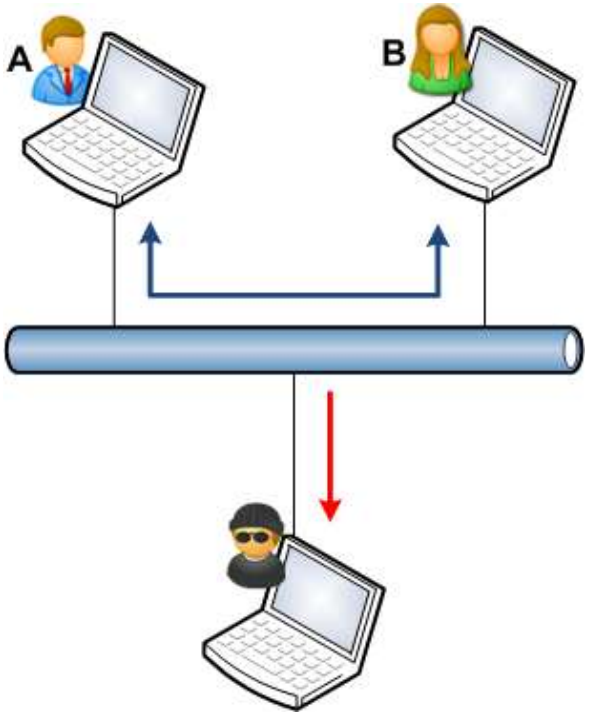
Comment s'en protéger ?

- 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

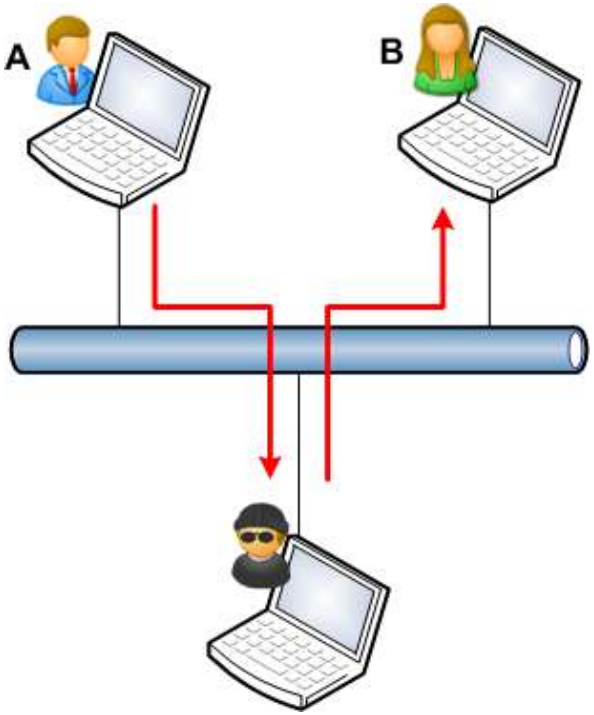


Les types d'attaques



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

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

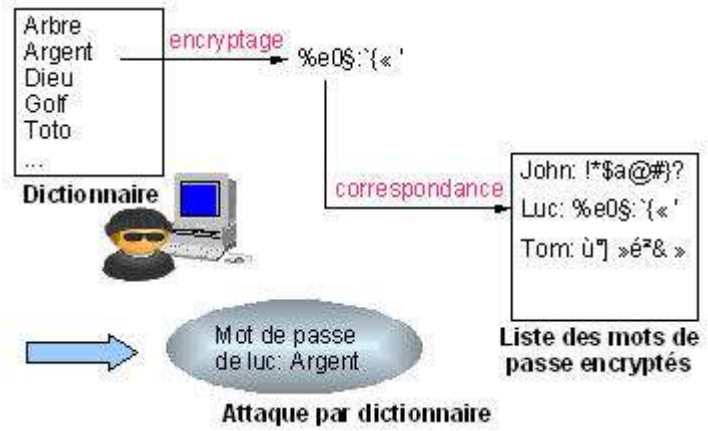
-Faire attention aux informations que l'on laisse sur Internet et particulièrement dans les réseaux sociaux

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

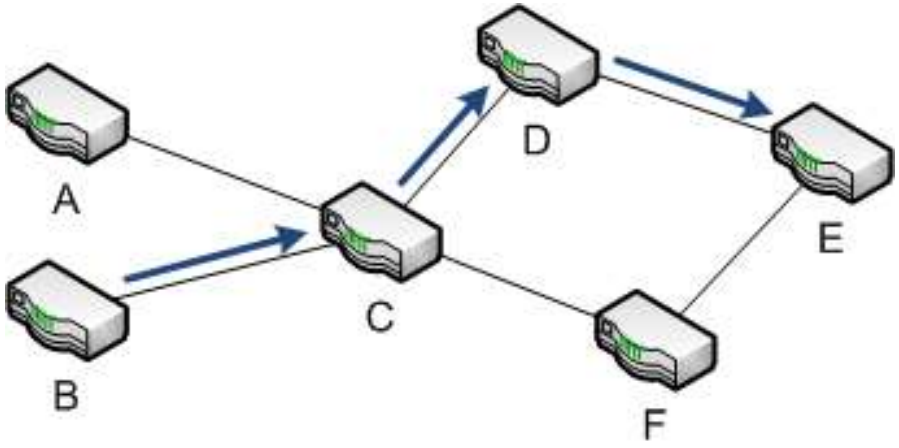
- Spoofing ou usurpation

Comment s'en protéger ?

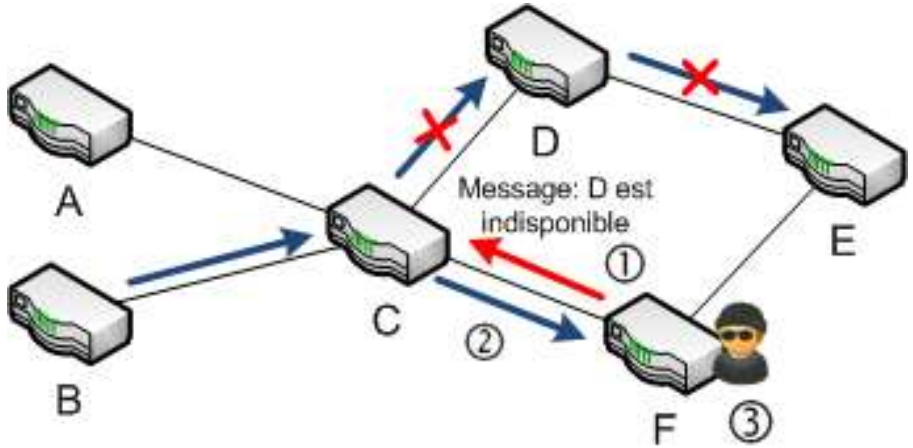
-Pas de solution pour l'empêcher

-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

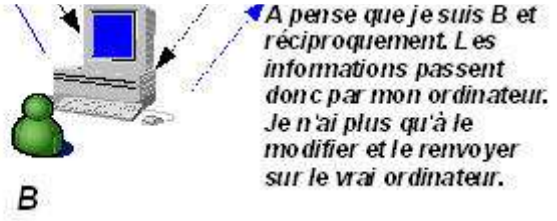
- Man in the middle ou
  « homme du milieu »

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

Université Grenoble Alpes

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.

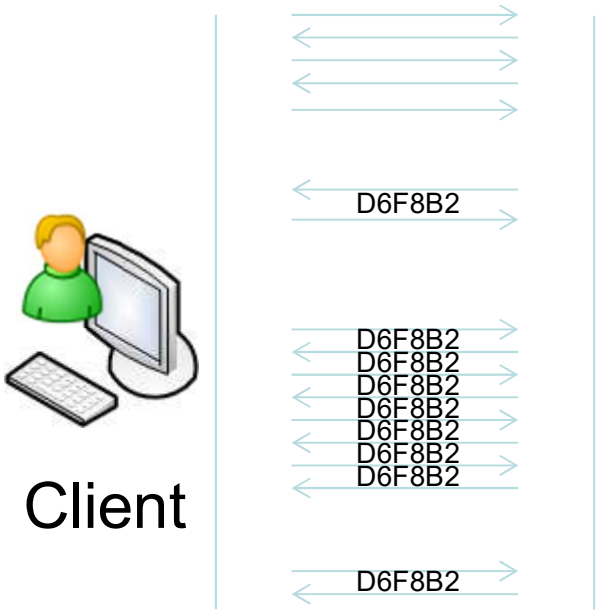
Les cookies sont nécessaires pour toutes les pages web dynamiques qui nécessitent d'identifier ou d'authentifier l'utilisateur, en permettant notamment la mise en œuvre de sessions :

- 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

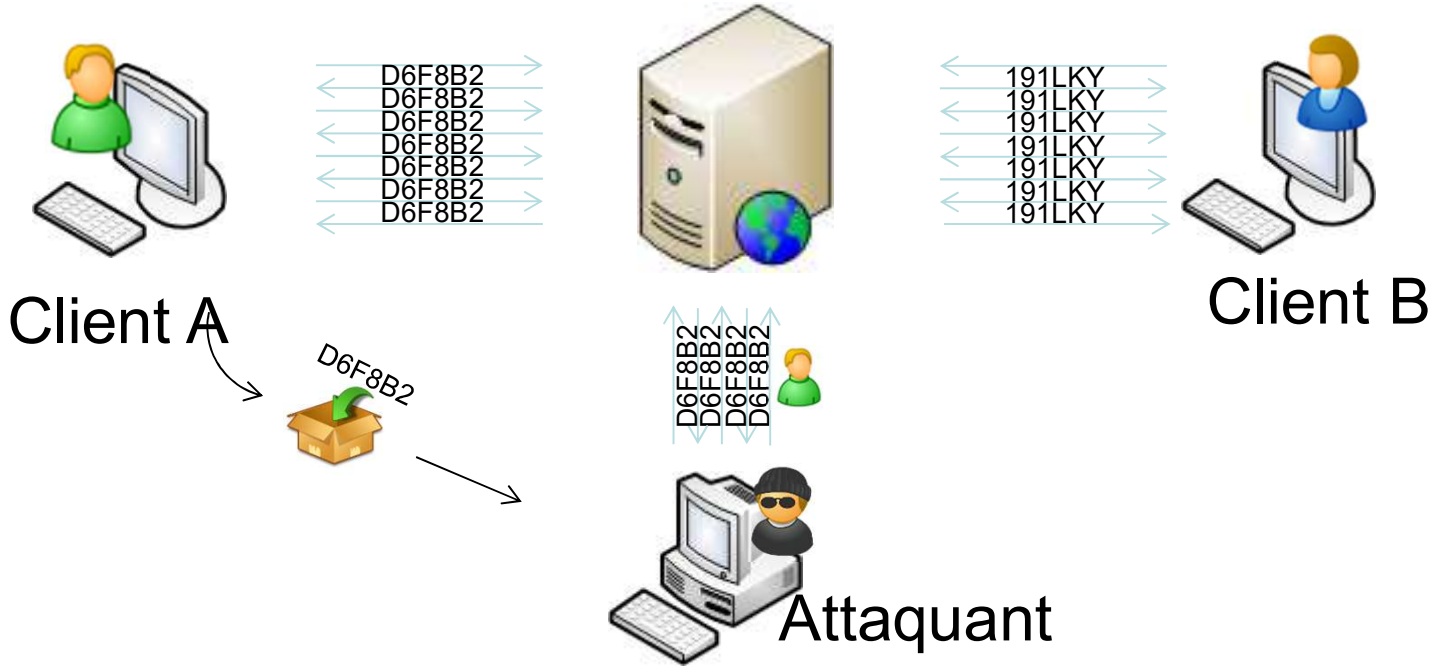
Les attaques Web

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.

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

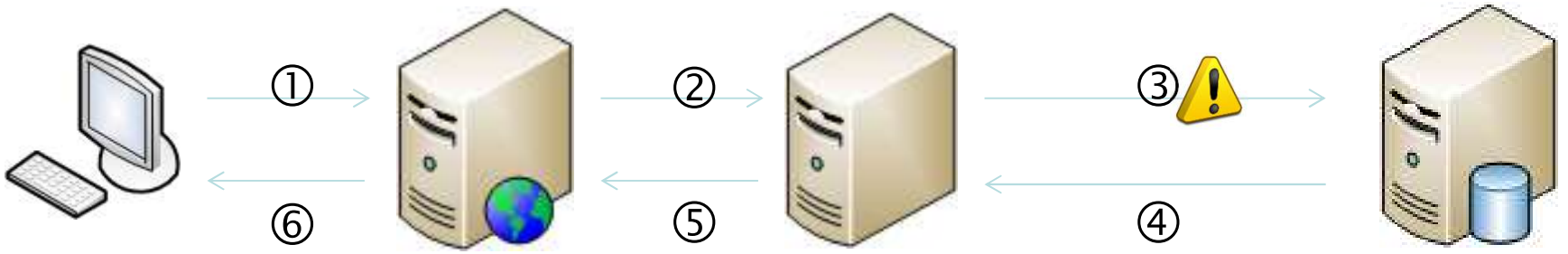
- Une attaque par injection SQL permet à un **attaquant d'interagir directement avec la base de données** d'un site web (alors que l'accès à cette base est bien entendu interdite) ;

- 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

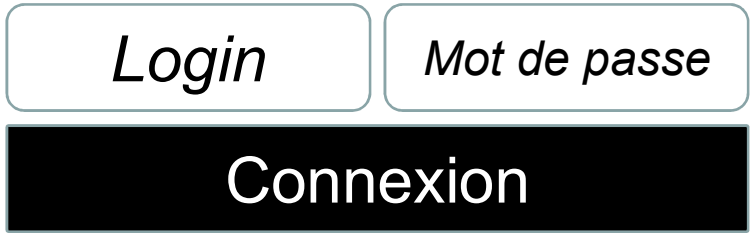
- L'objectif d'une attaque de type injection SQL consiste à détourner la requête SQL de l'étape 3 (diapositive précédente), et – en fonction du contexte – créer sa propre requête SQL malveillante ;

- 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'
```

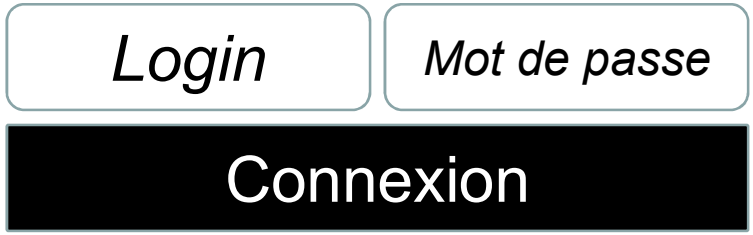
Ainsi, une requête légitime serait la suivante :

```
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.

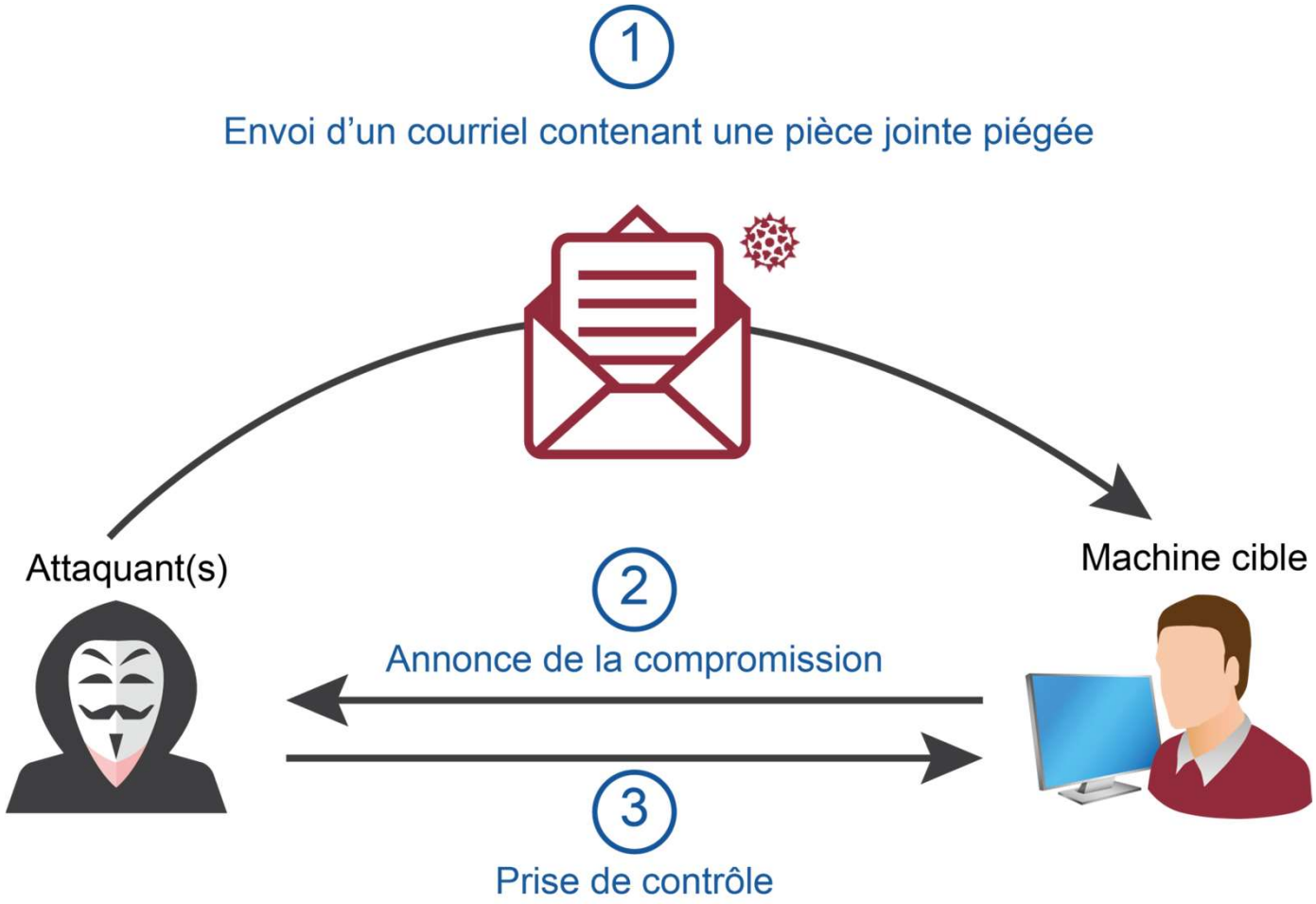
Les attaques APT

- 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

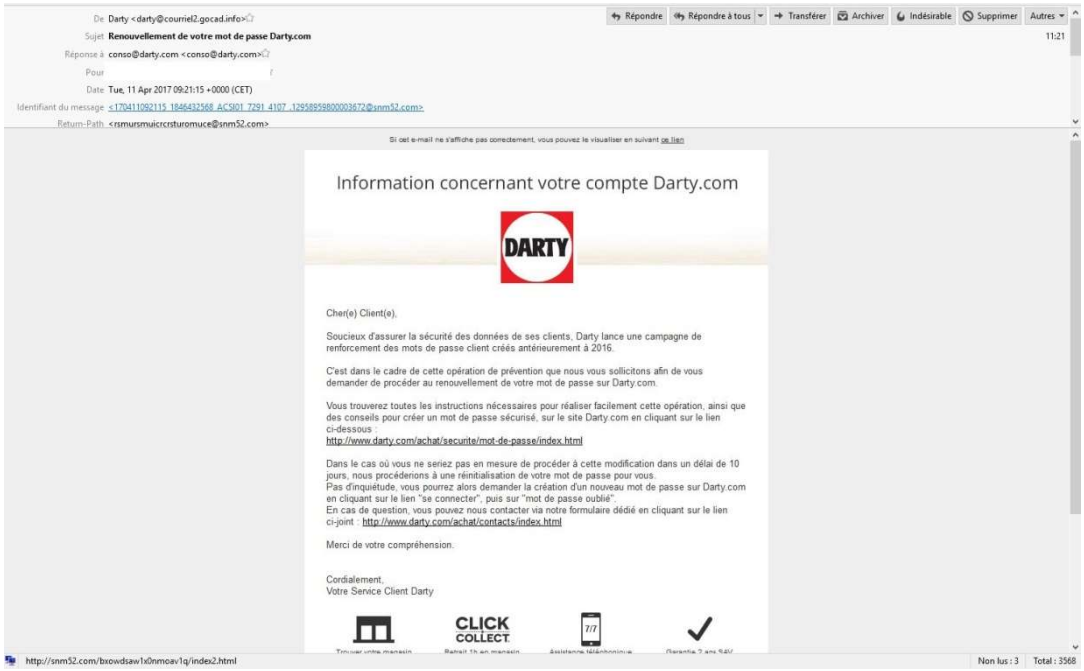
- Le terme *Advanced Persistent Threat* est aussi utilisé pour désigner un groupe, comme un gouvernement, avec à la fois la capacité et l'intention de cibler, de façon persistante et efficace, une entité spécifique.
- Un individu, comme un pirate informatique, n'est généralement pas désigné comme un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

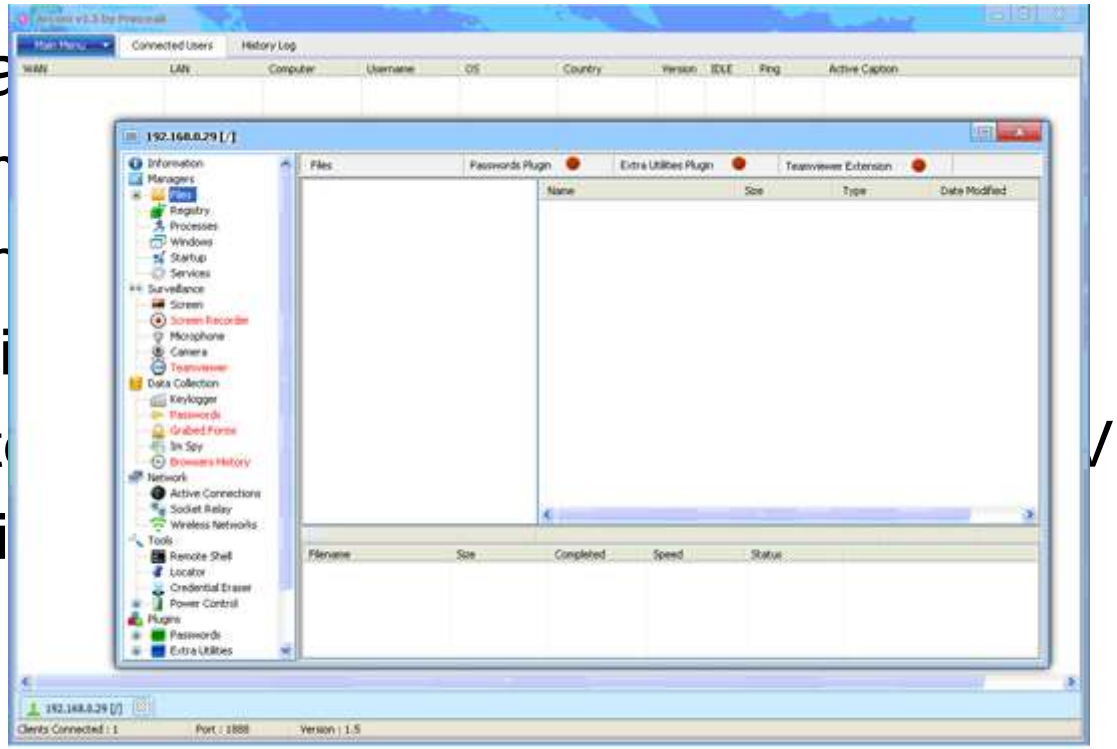
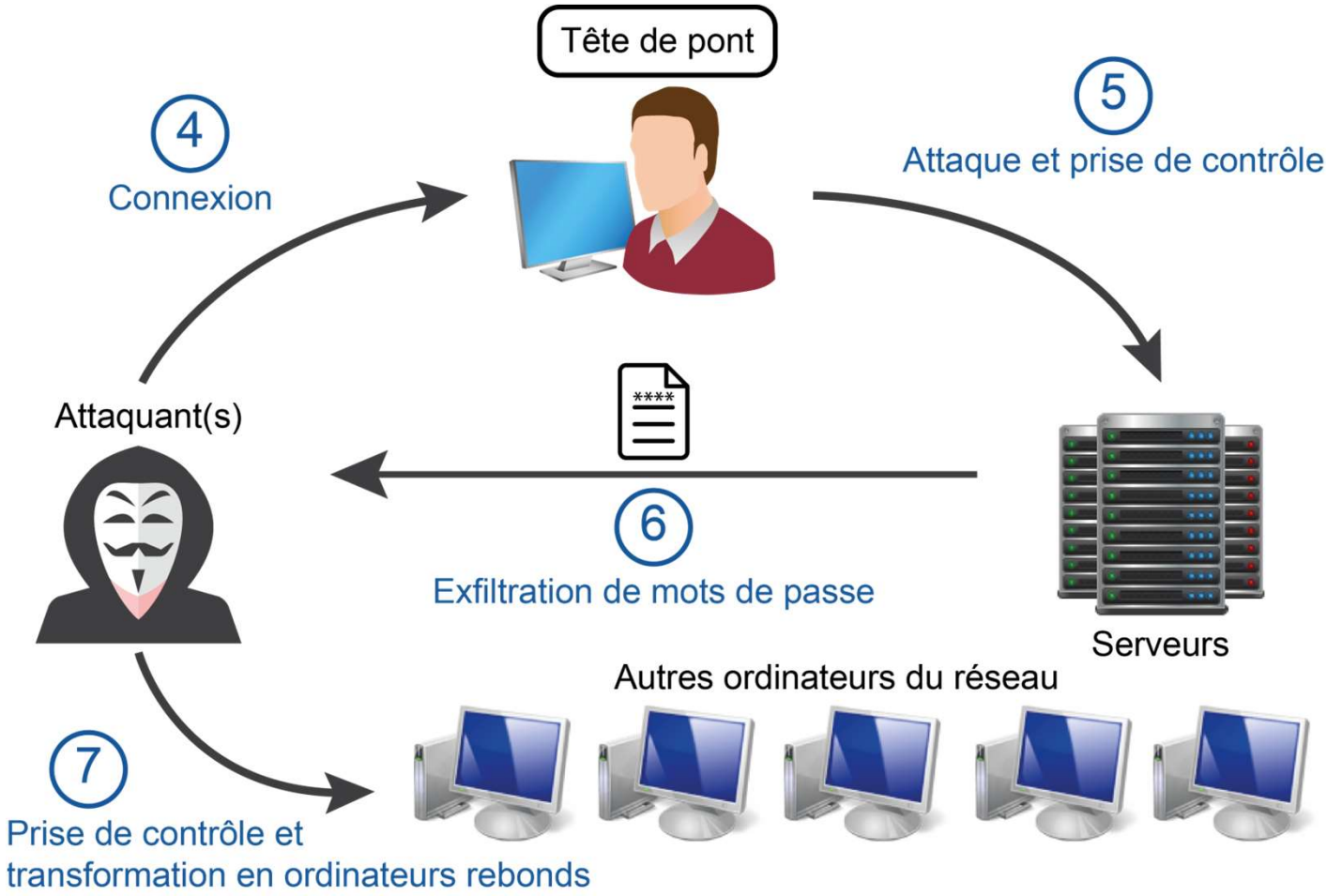
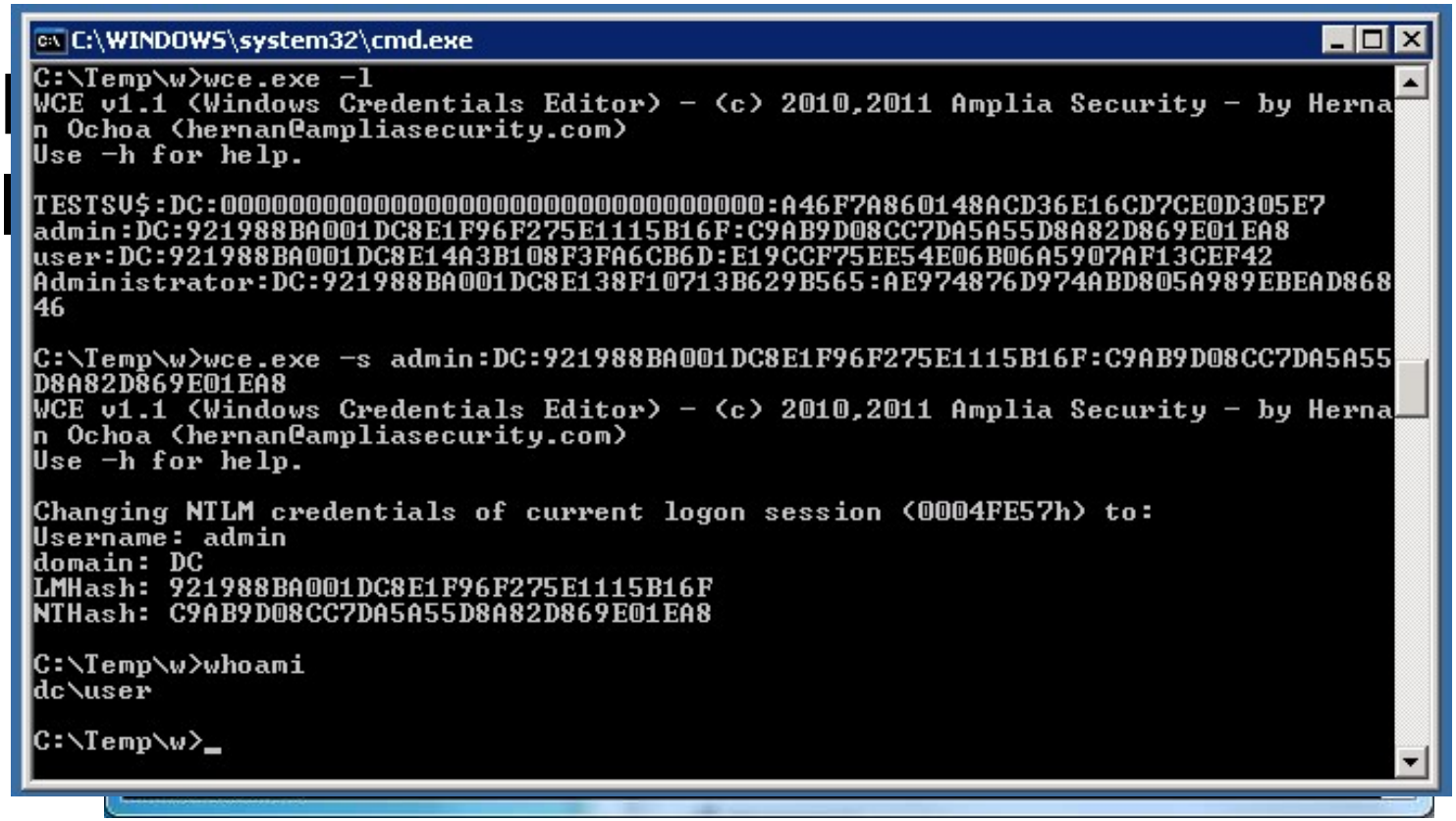


Figure 2. Cybercriminals use this to control compromised systems

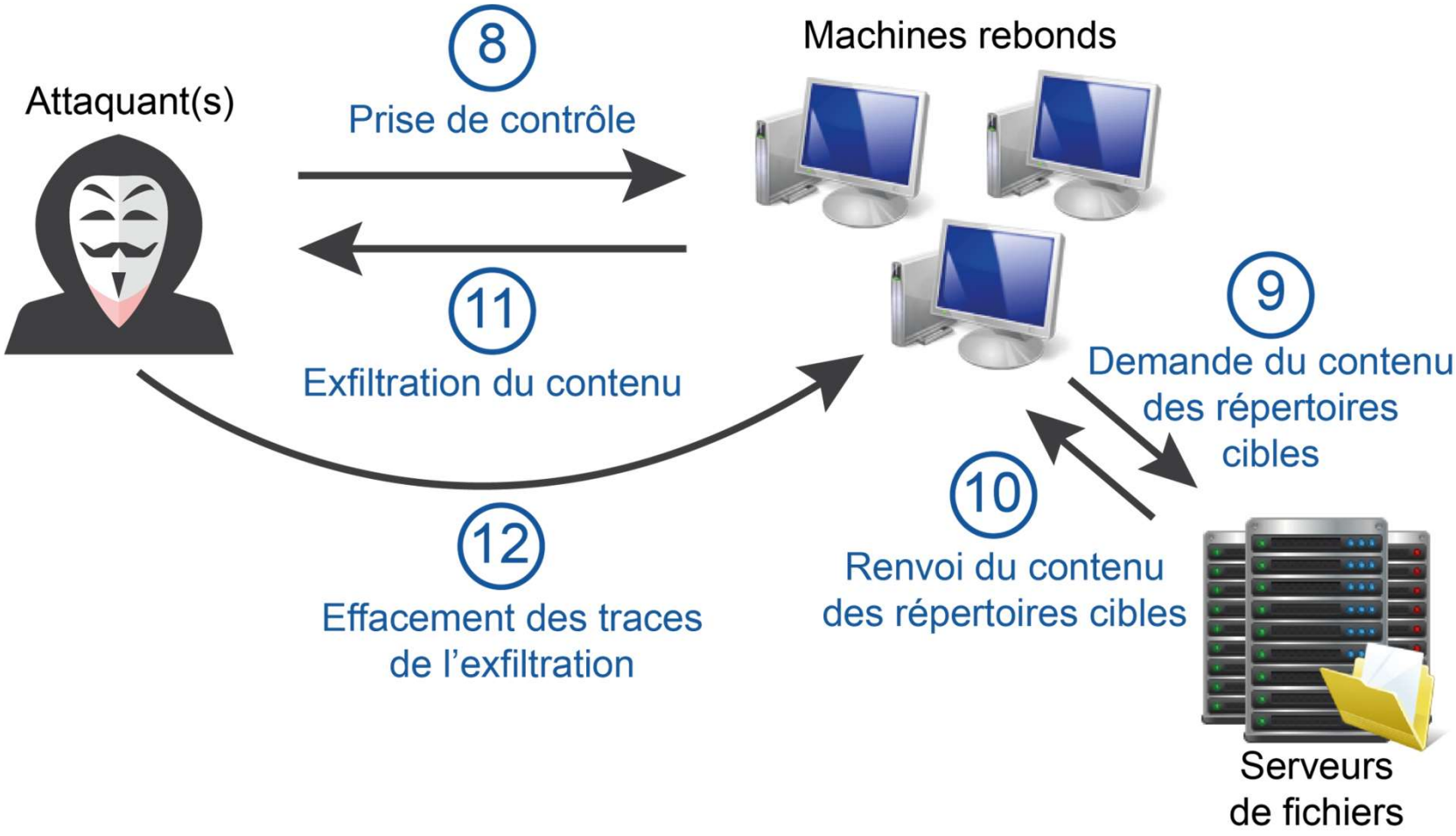
Déroulement d'une attaque avancée



Déroulement d'une attaque avancée

- 

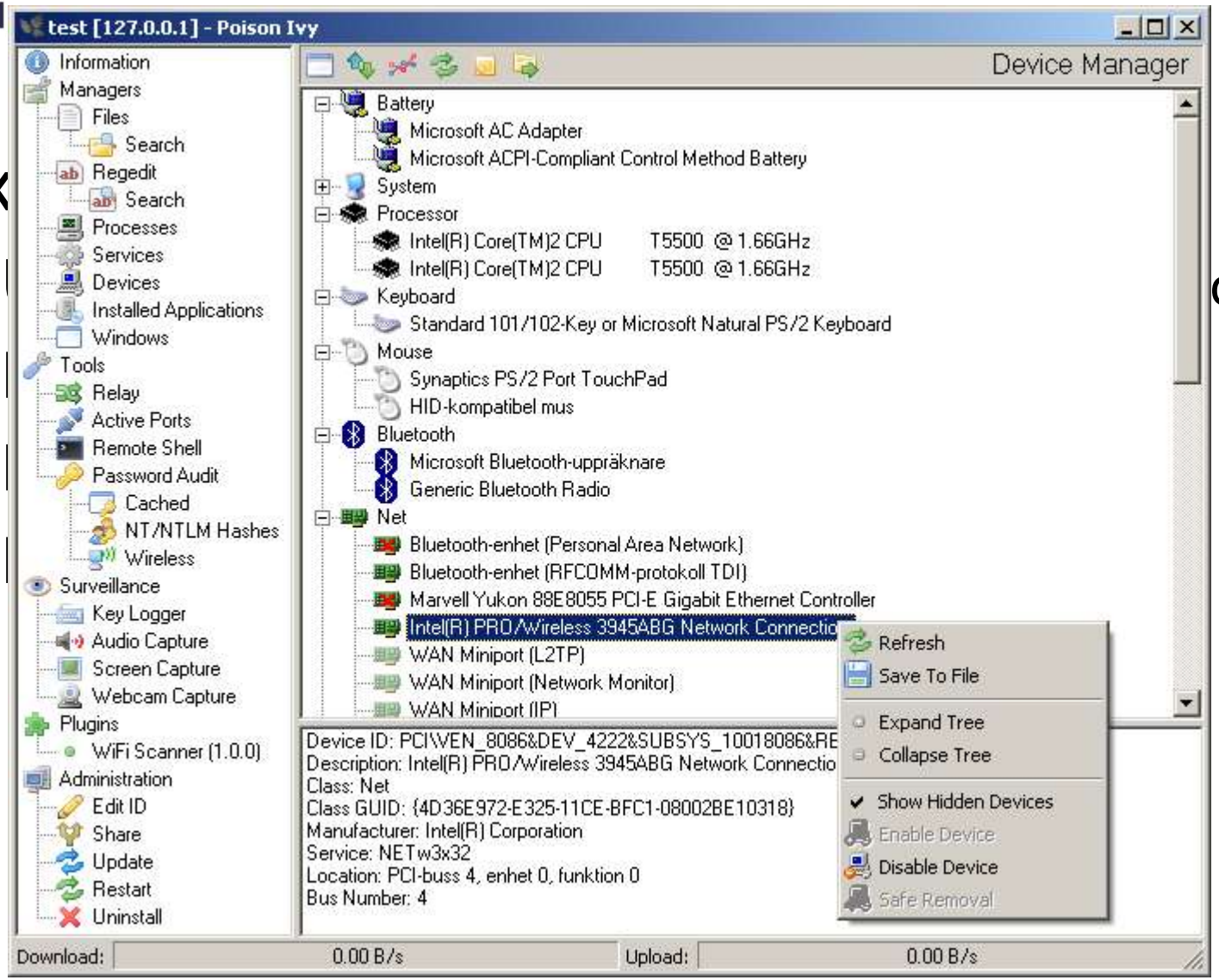
Déroulement d'une attaque avancée



Déroulement d'une attaque

- Ex
  -
  -
  -
  -

ool)

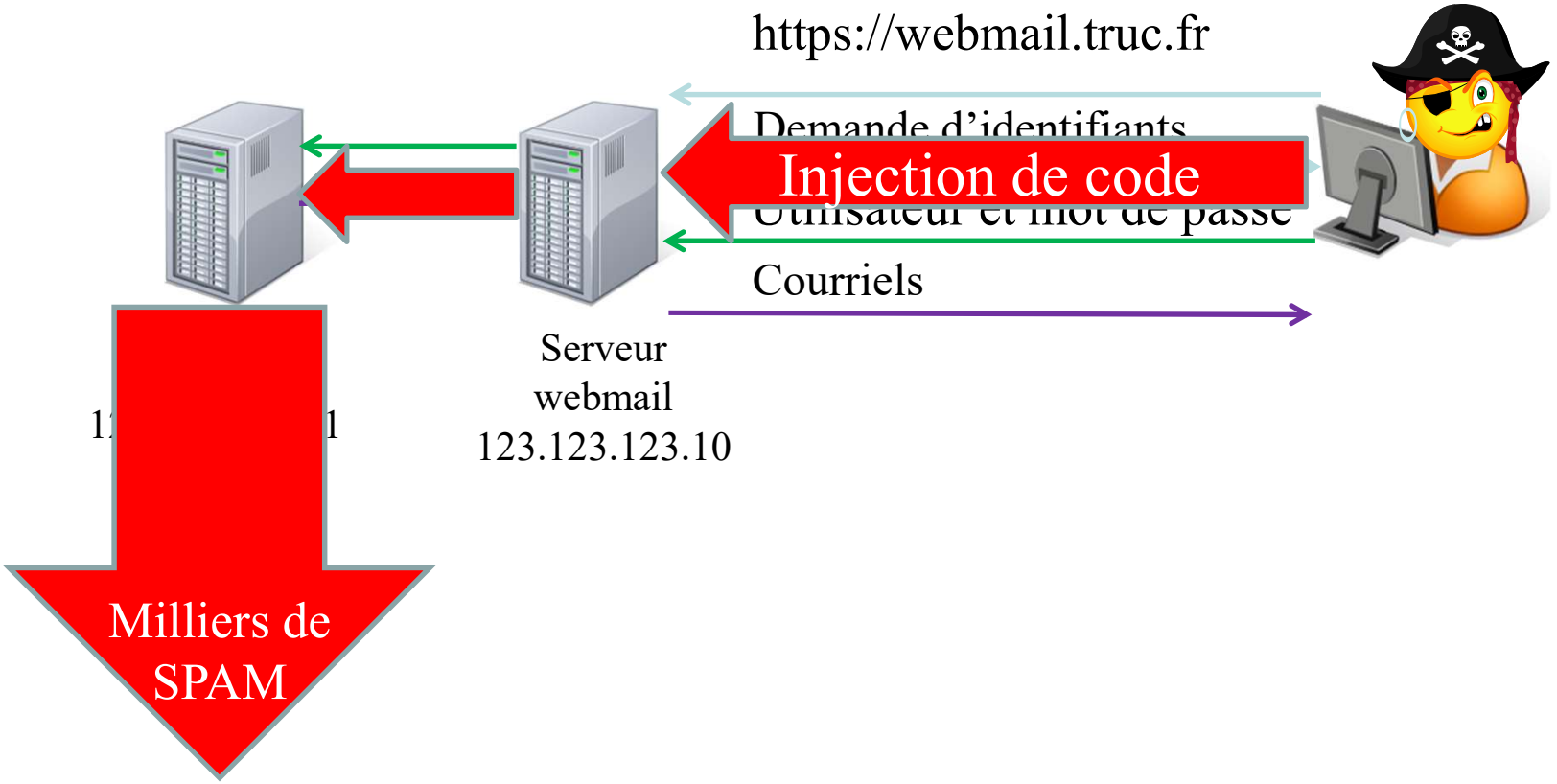


Détection des attaques

- 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 » !

Etude de cas :


https://webmail.truc.fr
Demande d'identifiants
Injection de code
Courriels
Serveur
webmail
123.123.123.10
Milliers de
SPAM

Etude de cas

- Analyse des logs sur le serveur webmail

41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET / HTTP/1.1" 200 4383
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /skins/classic/common.css?s=13
66058542 HTTP/1.1" 200 14668
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /skins/classic/images/favicon.
ico HTTP/1.1" 200 1150
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /plugins/jqueryui/js/i18n/jque
ry.ui.datepicker-fr.js?s=1366058541 HTTP/1.1" 200 1008
41.203.69.1 - - [30/Aug/2013:17:43:08 +0200] "GET /program/js/jstz.min.js?s=1366
058541 HTTP/1.1" 200 4984
41.203.69.1 - - [30/Aug/2013:17:43:08 +0200] "GET /program/js/common.js?s=136605
8565 HTTP/1.1" 200 14799

Etude de cas

- Analyse des logs sur le serveur courriel

Aug 30 17:43:36 serveur36 dovecot: imap-login: Login: user=<hxxxXXXxx>, method=PLAIN, rip=123.123.123.10, lip=123.123.123.11, mpid=1250, TLS
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Debug: Effective uid=30207, gid=100, home=/home/hxxxXXXxx
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Debug: fs: root=/home/hxxxXXXxx/mail, index=, control=, inbox=/var/mail/hxxxXXXxx
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Disconnected: Logged out bytes=29/399
Aug 30 17:43:37 serveur36 dovecot: imap-login: Login: user=<hxxxXXXxx>, method=PLAIN, rip=123.123.123.10, lip=123.123.123.11, mpid=1251, TLS
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Debug: Effective uid=30207, gid=100, home=/home/hxxxXXXxx
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Debug: fs: root=/home/hxxxXXXxx/mail, index=, control=, inbox=/var/mail/hxxxXXXxx
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Disconnected: Logged out bytes=44/533

From hxxxxXXXxx@serveur36.truc.fr Sat Aug 31 14:33:50 2013
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Sat, 31 Aug 2013 13:33:49 +0100
From: Norman Chan <norman@mail.com>
To: undisclosed-recipients:;
Bcc: hr832000@yahoo.com, hrabino11@yahoo.com, hracca666@yahoo.com,
 hradsky5@yahoo.com, hraeh76@yahoo.com, hrafael99@yahoo.com,
 hraffin@yahoo.com, hraiskin@yahoo.com, hrajappa@yahoo.com,
 hralizadeh_2007@yahoo.com, hrandell1@yahoo.com,
 hranislav_niciforovic@yahoo.com, ... **(plusieurs centaines d'adresses….)**
Subject: Hi
Organization: Norman Chan
Reply-To: mrcchannorman@qq.com
Mail-Reply-To: mrcchannorman@qq.com
Message-ID: <ef05796bed486b07e7d63f8fc8c4a02d@cermav.cnrs.fr>
X-Sender: norman@mail.com
User-Agent: Roundcube Webmail/0.9.0
X-UID: 582
Status: R
X-Keywords:
Content-Length: 247

--
Hello, I'm Norman Chan, Tak-Lam, S.B.S., J.P, Chief Executive, Hong Kong Monetary Authority (HKMA). I have a Business worth $47.1M USD for you to handle with me. Contact me on my email (mrcchannorman@qq.com) for more details of the business

URLs

- Organizations
  - https://www.ssi.gouv.fr
  - https://www.ncsc.gov.uk
  - https://www.enisa.europa.eu
  - https://www.cisa.gov
  - https://attack.mitre.org/
  - https://www.cvedetails.com/
- Threat intelligence
  - https://fraudguard.io
  - https://observatory.mozilla.org
  - https://www.shodan.io
  - https://www.virustotal.com
  - https://app.any.run
  - https://haveibeenpwned.com
  - https://osintframework.com/
  - https://www.nomoreransom.org/
  - https://www.exploit-db.com/
  - https://www.threatcrowd.org/
  - https://www.ipneighbour.com/

References

- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Hackers heroes of the computer revolution**, S. Levy, 2010, *O'Reilly*
- **Learn Social Engineering**, *Dr E. Orzkaya,* 2018, *Packt*
- **Cybersecurity – Attack and defense strategies**, Y Diogenes E. Ozkaya, 2019, *Packt*
- **Digital Forensics and incident response**, G. Johansen, 2017, *Packt*
- **Network scanning cookbook,** S. Jetty, 2018, *Packt*

TD

- 1. Quelles sont les différences entre une attaque active et une attaque passive?
- 2. Quelles sont les conditions de succès d'une attaque ?
- 3. Analyse d'un site web (liste précédente, à compléter), contenu, intérêt, parties intéressantes ou inintéressantes
- 4. 2nde étape du mémoire de sécurité : proposez une classification des attaques, en mettant en face la stratégie de sécurité permettant de les éviter
- 5. Identifiez des outils (logiciels) qui peuvent être utilisés pour mettre en oeuvre des attaques