Droit et Sécurité de l'Information

Chapitre II : Les attaques informatiques et les systèmes de détection d'intrusions (IDS)

Département Informatique – Université Guelma

Plan du cours

I. Introduction
II. Anatomie d'une attaque
III. Les différents types d'attaques
    1. Les Malware
    2. Les attaques réseaux
    3. Les attaques applicatives
    4. Le Déni de service
IV. Détection d'attaques : les IDS
V. Les méthodes de défense

I. Introduction

- pare-feux
- systèmes d'authentification
- Etc…

La mise en place d'une PSSI autour de ces systèmes est donc primordiale

A priori bénéfique

Les systèmes d'information sont aujourd'hui de plus en plus ouverts sur Internet.

Pose un problème

Un nombre croissant d'attaques

I. Introduction

Il est nécessaire, pour compléter cette politique de sécurité, d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions.

Définition :

Intrusion signifie pénétration des systèmes d'information mais aussi :

- ⇨ tentatives des utilisateurs locaux d'accéder à de plus hauts privilèges que ceux qui leur sont attribués,
- ⇨ ou tentatives des administrateurs d'abuser de leurs privilèges.

Une attaque est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé.

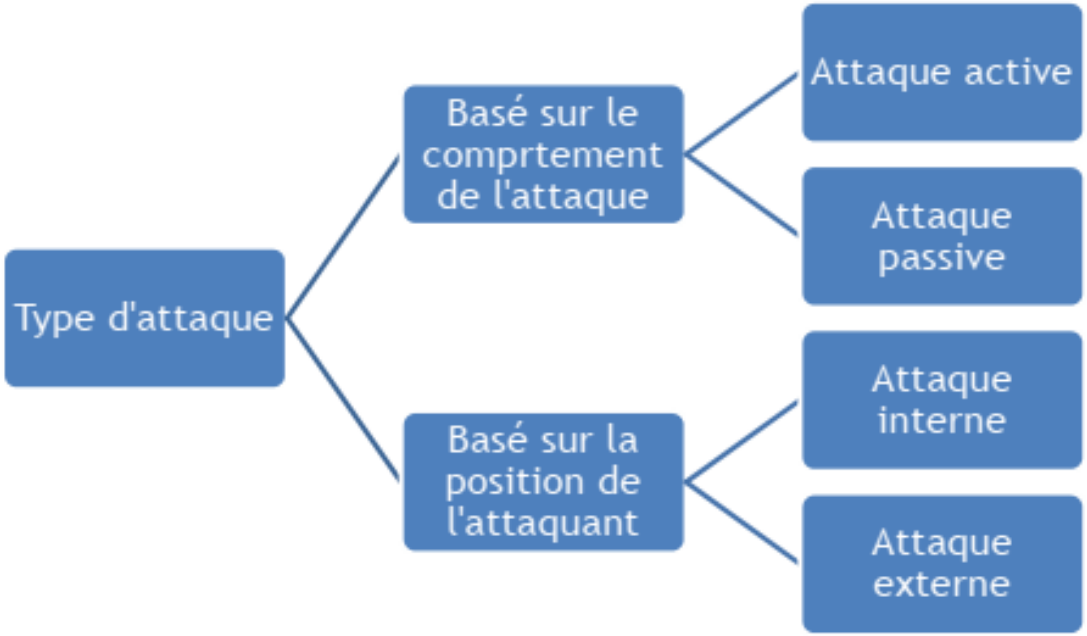
Le gouvernement des États-Unis, définit une attaque comme suit :

« Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même. »

I. Introduction

L'informatique étant un domaine très vaste, le nombre de vulnérabilités présentes sur un système peut donc être important .

Ainsi, les attaques **visant ces failles** peuvent être à la fois **très variées** et **très dangereuses**.



I. Introduction

Une attaque peut être active ou passive.

- une «**attaque active**» tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une «**attaque passive**» tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).

Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'o

- Une «**attaque interne**» est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
- Une «**attaque extérieure**» est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.

Plan du cours

I. Introduction

II. Anatomie d'une attaque

III. Les différents types d'attaques

1. Les Malware
2. Les attaques réseaux
3. Les attaques applicatives
4. Le Déni de service

IV. Détection d'attaques : les IDS

V. Les méthodes de détection

II. Anatomie d'une attaque

Fréquemment appelés « **les 5 P** » dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique.

- **Probe**, (Explorer)
- **Penetrate,** (Pénétrer)
- **Persist,** (S'obstiner)
- **Propagate,** (Propager)
- **Paralyze**. (Paralyser)

II. Anatomie d'une attaque

❶ **Probe** Consiste en la collecte d'informations sur le système cible par le biais d'un certains outils.

Outils : Whois, Arin, DNS lookup.

Fournit des informations administratives et techniques sur les propriétaires des noms de domaine

Manière :

- **Un scan de ports** grâce au programme **Nmap** pour déterminer la version des logiciels utilisés,
- **Un scan de vulnérabilités** à l'aide du programme **Nessus**.

II. Anatomie d'une attaque

❷ **Penetrate** Utilisation des informations récoltées pour pénétrer un réseau.

Techniques : **La force brute** ou **les attaques par dictionnaires** peuvent être utilisées **pour outrepasser les protections par mot de passe**.

Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères.

Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire.

II. Anatomie d'une attaque

❸ **Persist** Création d'un compte avec des droits de super utilisateur pour pouvoir se ré-infiltrer ultérieurement

Techniques : Installer une **application de contrôle à distance** capable de résister à un reboot (ex : un cheval de Troie).

II. Anatomie d'une attaque

❹ **Propagate** Consiste à observer ce qui est accessible et disponible sur le réseau local.

❺ **Paralyze** Causer des dégâts

Actions :

- Mener une attaque sur une autre machine
- Détruire des données
- Endommager le système d'exploitation dans le but de planter le serveur

Plan du cours

I. Introduction

II. Anatomie d'une attaque

III. Les différents types d'attaques

1. Les Malware
2. Les attaques réseaux
3. Les attaques applicatives
4. Le Déni de service

IV. Détection d'attaques : les IDS

V. Les méthodes de détection

III. Les différents types d'attaques [1. Malware]

Le fait de s'introduire et de se maintenir dans un système informatique sans autorisation est un délit puni par la loi.

Malware est le terme général désignant les programmes destinés à causer des dégâts sur les systèmes d'information : vers, virus, chevaux de Troie...

III. Les différents types d'attaques [1. Malware]

A. Le virus : C'est un programme pirate, capable de se propager et de se reproduire à travers les systèmes informatiques dans l'intention d'y créer des dégâts.

Buts :

- Détruire une partie ou toutes les données de l'ordinateur.
- De rendre inutilisables certaines fonctions du PC.
- Ralentir certaines procédures.
- Etc….

Son principe de fonctionnement diffère suivant les virus.

III. Les différents types d'attaques [1. Malware]

Les différents types de virus :

1. Le virus de zone amorce

Un virus de zone d'amorce infecte la zone d'amorce des disques durs et des disquettes.

Une fois la zone d'amorce de l'ordinateur infectée, ce virus se transmettra sur toute disquette ou support amovible inséré dans l'ordinateur.

Remarque : La plupart des virus de zone d'amorce ne fonctionnent plus sous les nouveaux systèmes d'exploitation tels que Windows NT, Windows XP, 2000 car ils sont formatés en NTFS et non en FAT 32

III. Les différents types d'attaques [1. Malware]

2. Le virus Macro

Les virus Macros sont la plus grande menace à ce jour, ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté.

Une Macro est une série de commandes permettant d'effectuer des fonctions automatiquement au sein des applications Micro soft citées ci dessus.

Le but du langage de macro est de pouvoir créer des raccourcis pour effectuer des fonctions courantes, par exemple en une touche enregistrer un document et ensuite l'imprimer.

Conseil : pour les éviter, Mettez un haut niveau de sécurité (outils, puis macros, puis sécurité, mettez ensuite haut).

III. Les différents types d'attaques [1. Malware]

3. Le virus Polymorphe

Virus qui possède la capacité de modifier automatiquement ses principales caractéristiques (nom, taille...).

Les virus polymorphes incluent un code spécial permettant de rendre chaque infection différente de la précédente.

Remarque : Ces virus sont très difficiles à éliminer car ils trompent la vigilance de l'antivirus qui recherche une signature précise.

III. Les différents types d'attaques [1. Malware]

B. Le cheval de Troie :

Est un petit programme malveillant d'apparence anodine (jeu, petit utilitaire...) qui, une fois installé dans un ordinateur, peut causer des dégâts comme un virus classique, ou permettre de prendre le contrôle à distance de la machine.

III. Les différents types d'attaques [1. Malware]

C. Ver (worm)

Virus qui se propage aux autres correspondants listés dans la liste des contacts par l'intermédiaire des messageries, généralement sous la forme de pièce jointe. le ver ne peut pas se greffer à un autre programme et ne peut donc l'infecter.

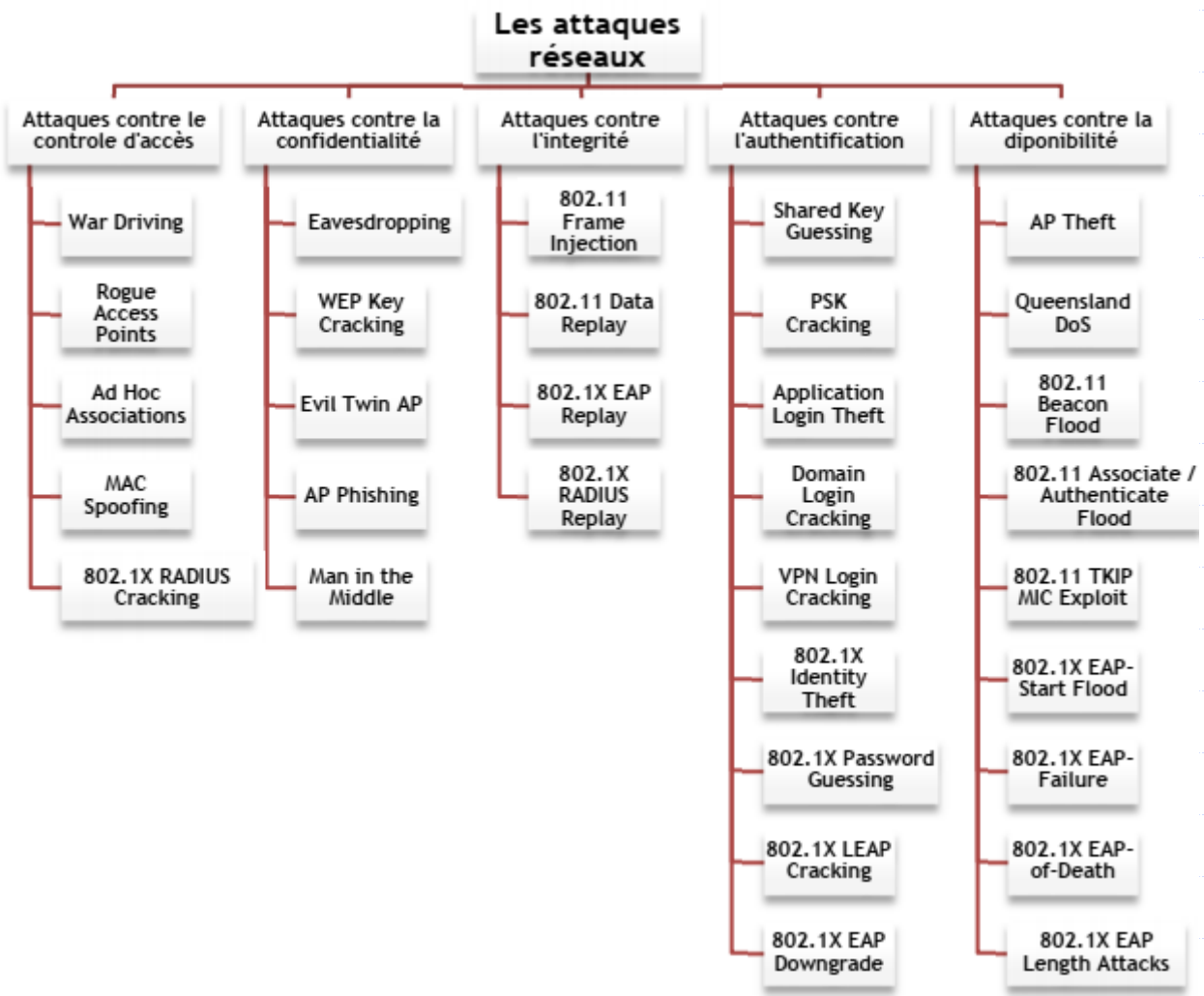
D. Hoax (blague)

Ce n'est pas un virus, mais un simple message qui incite celui qui le reçoit à le renvoyer à toutes ses connaissances, voire à supprimer certains fichiers systèmes de son ordinateur. Contrairement aux virus, les hoax ne contiennent aucun code destructif.

III. Les différents types d'attaques

2. Les attaques réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation.



III. Les différents types d'attaques

2. Les attaques réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation.

Observons quelques attaques bien connues :

i. Les techniques de scan

Le but des scans est de déterminer quels sont les ports ouverts, et donc en déduire les services qui sont exécutés sur la machine cible.

(ex : port 80/TCP pour un service HTTP).

Remarque : La plupart des attaques sont précédées par un scan de ports lors de la phase Probe.

III. Les différents types d'attaques

2. Les attaques réseaux

Il existe un nombre important de techniques de scan. Idéalement, la meilleure technique de scan est celle qui est la plus furtive afin de ne pas alerter les soupçons de la future victime.

IP Spoofing : Usurper l'adresse IP d'une autre machine

C'est une technique d'intrusion consistant à envoyer à un serveur d'une entreprise, des messages (paquets) semblant provenir d'une adresse IP connue par le firewall (adresse interne existante autorisée).

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets).

Pour que la communication ne s'établisse pas avec la machine possédant réellement cette adresse, le hacker doit dans le même temps rendre cette machine injoignable pour avoir le temps d'intercepter les codes de communication et établir la liaison pirate.

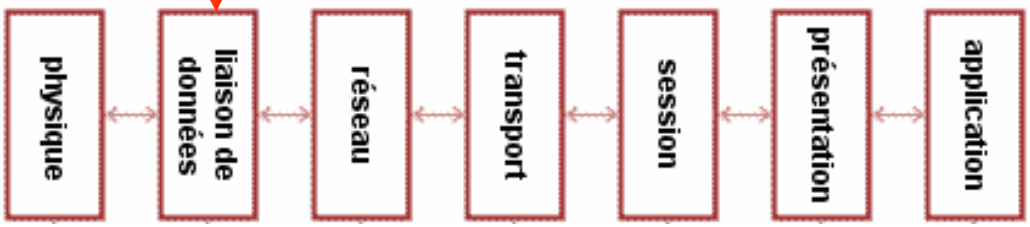
III. Les différents types d'attaques

2. Les attaques réseaux

ARP Spoofing : Rediriger le trafic d'une machine vers une autre

Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien.

Remarque : La finalité est la même que l'IP spoofing mais on travaille ici au niveau de la couche liaison de données.



III. Les différents types d'attaques

2. Les attaques réseaux

DNS Spoofing :

Fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine.

Rediriger, à leur insu, des Internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer ses identifiants en toute confiance par exemple.

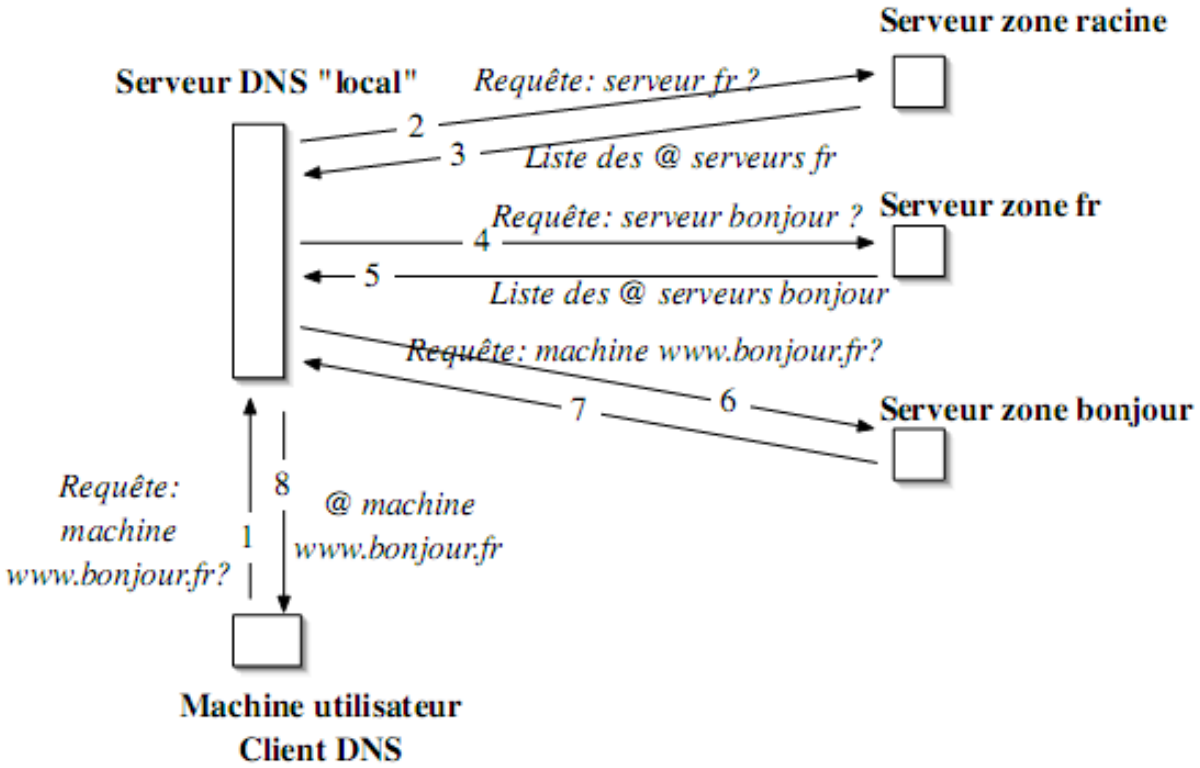
Exemple : L'adresse DNS (Domain Name Server).

Adresse DNS	Adresse IP
www.ibm.com	204.146.80.99
users.skynet.be	194.237.109.73

III. Les différents types d'attaques

2. Les attaques réseaux

Exemple d'une interrogation DNS



III. Les différents types d'attaques

2. Les attaques réseaux

Fragments attacks (attaque par fragmentation) :

Le but de cette attaque est de passer outre les protections des équipements de filtrage IP.

Un pirate peut par exemple s'infiltrer dans un réseau pour effectuer des attaques ou récupérer des informations confidentielles.

III. Les différents types d'attaques

2. Les attaques réseaux

TCP Session Hijacking :

Le but de cette attaque est de rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe.

Cette attaque rend donc possible le « vol » de session. Le vol d'une session **ftp** par exemple, se fera après la phase d'authentification

III. Les différents types d'attaques

3. Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, comme précédemment, il est possible de classifier ces attaques selon leur provenance.

i. Les problèmes de configuration

Il est très rare que les administrateurs réseaux configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel.

Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants, ou mettant en jeu l'intégrité du système d'exploitation.

C'est pourquoi il est important de bien lire les documentations fournies par les développeurs afin de ne pas créer de failles.

III. Les différents types d'attaques

3. Les attaques applicatives

ii. Les bugs

Liés à un problème dans le code source, ils peuvent amener à l'exploitation de failles. On ne peut toutefois rien faire contre ce type de problèmes, si ce n'est attendre un correctif de la part du développeur.

iii. Les buffer overflows

Ou dépassement de la pile, sont une catégorie de bug particulière. Issus d'une erreur de programmation, ils permettent l'exploitation d'un shellcode à distance .

Ce shellcode permettra à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction.

III. Les différents types d'attaques

3. Les attaques applicatives

iv. Les scripts

Principalement web (ex : Perl, PHP, ASP), ils s'exécutent sur un serveur et renvoie un résultat au client. Cependant, lorsqu'ils sont dynamiques (i.e. qu'ils utilisent des entrées saisies par un utilisateur), des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées.

v. Les injections SQL

les injections SQL profitent de paramètres d'entrée non vérifiés. Comme leur nom l'indique, le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données.

III. Les différents types d'attaques

3. Les attaques applicatives

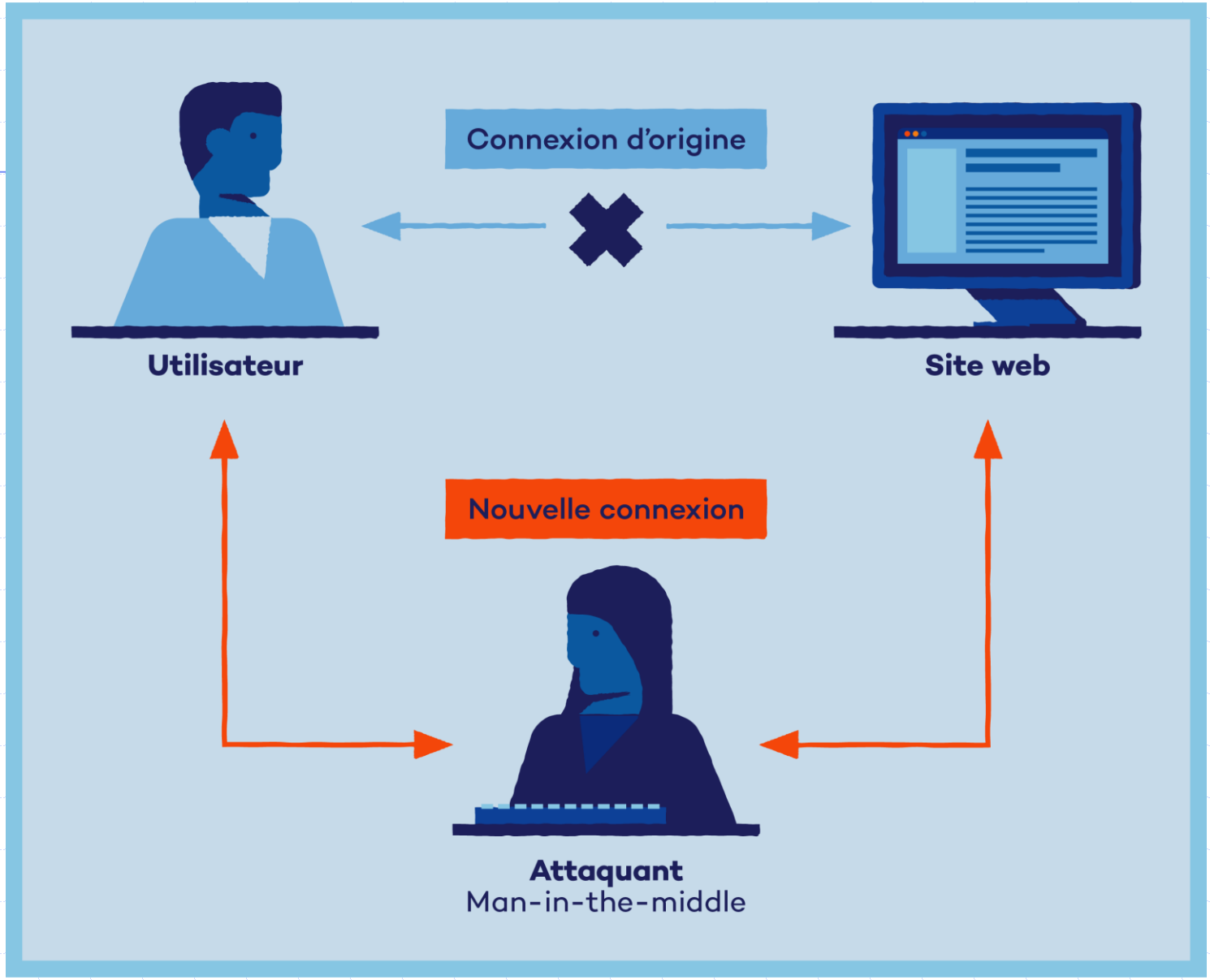
vi. Man in the middle

Moins connue, mais tout aussi efficace, cette attaque permet de détourner le trafic entre deux stations.

Exemple :

Imaginons un client **C** communiquant avec un serveur **S**. Un pirate peut détourner le trafic du client en faisant passer les requêtes de **C** vers **S** par sa machine **P**, puis transmettre les requêtes de **P** vers **S**. Et inversement pour les réponses de **S** vers **C**.

Totalement transparente pour le client. Il accédera ainsi à toutes les communications et pourra en obtenir les informations sans que l'utilisateur s'en rende compte.


Connexion d'origine
Utilisateur
Site web
Nouvelle connexion
Attaquant
Man-in-the-middle

III. Les différents types d'attaques

4. Le Déni de service

Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières :

- Une surcharge réseau : rendant ainsi la machine totalement injoignable ;
- De manière applicative : crashant l'application à distance.
- L'utilisation d'un buffer overflow : peut permettre de planter l'application à distance.
- Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service voire un système complet.

III. Les différents types d'attaques

4. Le Déni de service

Voici quelques attaques réseaux connues permettant de rendre indisponible un service :

- SYN Flooding
- UDP Flooding
- Packet Fragment
- Smurfling
- Déni de service distribué

III. Les différents types d'attaques

4. Le Déni de service

Remarque :

Actuellement, la sécurité contre les attaques distantes se renforce, notamment par le biais d'équipements réseaux plus puissants (comme des firewalls plus intelligents), mais les attaques locales restent toutefois encore fort efficaces : l'ARP Spoofing, le vol de session, … restent souvent possibles.

L'informatique évolue, les applications sont de plus en plus complexes et les délais laissés aux programmeurs et administrateurs sont souvent très (trop) courts. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues. Les attaques distribuées seront toujours redoutables si la plupart des machines personnelles ne sont pas protégées. Ce qui nous amène à notre seconde partie : comment détecter et empêcher ces attaques ?

Plan du cours

I. Introduction
II. Anatomie d'une attaque
III. Les différents types d'attaques
    1. Les Malware
    2. Les attaques réseaux
    3. Les attaques applicatives
    4. Le Déni de service
IV. Détection d'attaques : les IDS
V. Les méthodes de détection

IV. Détection d'attaques : les IDS

Un **système de détection d'intrusion** (ou **IDS** : Intrusion detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions.

Il existe deux grandes catégories d'IDS, les plus connues sont les détections par signatures (reconnaissance de programme malveillant) et les détections par anomalies (détecter les écarts par rapport à un modèle représentant les bons comportements).

Il est aussi possible de classifier les IDS selon la cible qu'ils vont surveiller, les plus communs sont les systèmes de détection d'intrusion réseau et les systèmes de détection d'intrusion hôte.

IV. Détection d'attaques : les IDS

A l'origine, les premiers systèmes de détection d'intrusions ont été initiés par l'armée américaine, puis par des entreprises. Plus tard, des projets open-source ont été lancés et certains furent couronnés de succès, comme par exemple **Snort** et **Prelude**

Certains IDS ont la possibilité de répondre aux menaces qu'ils ont détectées, ces IDS avec capacité de réponse sont des **systèmes de prévention d'intrusion**.

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

Comme nous l'avons vu, les attaques utilisées par les pirates sont très variées. Certaines utilisent des failles réseaux et d'autres des failles de programmation. Nous pouvons donc facilement comprendre que la détection d'intrusions doit se faire à plusieurs niveaux.

Remarque : IDS est un système capable de détecter tout type d'attaque. Certains termes sont souvent employés quand on parle d'IDS:

- **Faux positif** : une alerte provenant d'un IDS mais qui ne correspond pas à une attaque réelle.
- **Faux négatif** : une intrusion réelle qui n'a pas été détectée par l'IDS

Ainsi, il existe différents types d'IDS :

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

i. Les systèmes de détection d'intrusions (IDS)

Définition : ensemble de composants logiciels et matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction (volontaire ou non).

Fonctions : détection des techniques de sondage (balayages de ports, fingerprinting), des tentatives de compromission de systèmes, d'activités suspectes internes, des activités virales ou encore audit des fichiers de journaux (logs).

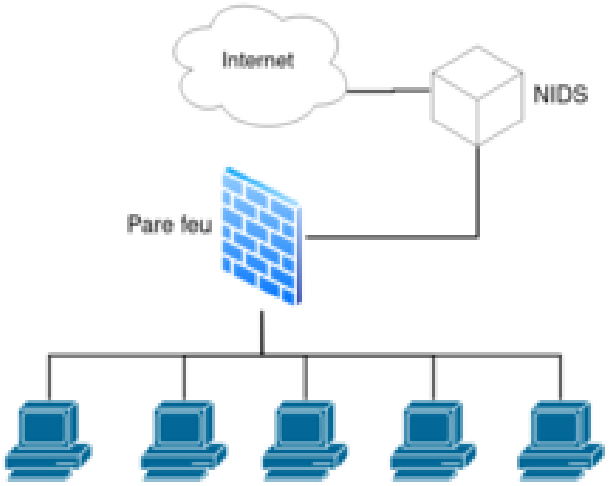
IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

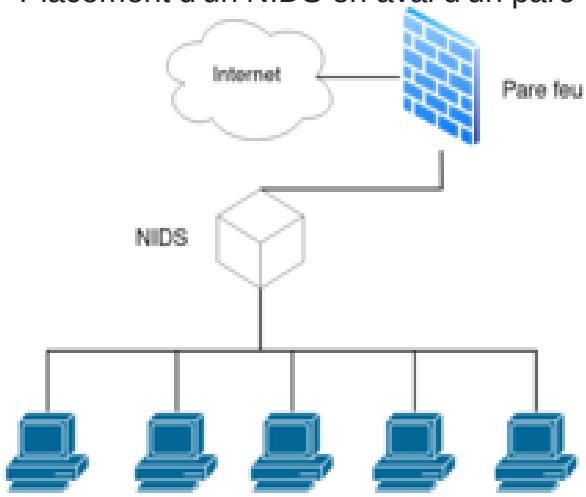
ii. Les systèmes de détection d'intrusions « réseaux » (NIDS)

Objectif : analyser de manière passive les flux en transit sur le réseau et détecter les intrusions en temps réel. Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Les NIDS étant les IDS plus intéressants et les plus utiles du fait de l'omniprésence des réseaux dans notre vie quotidienne.

Placement d'un NIDS en amont d'un pare-feu.



Placement d'un NIDS en aval d'un pare-feu



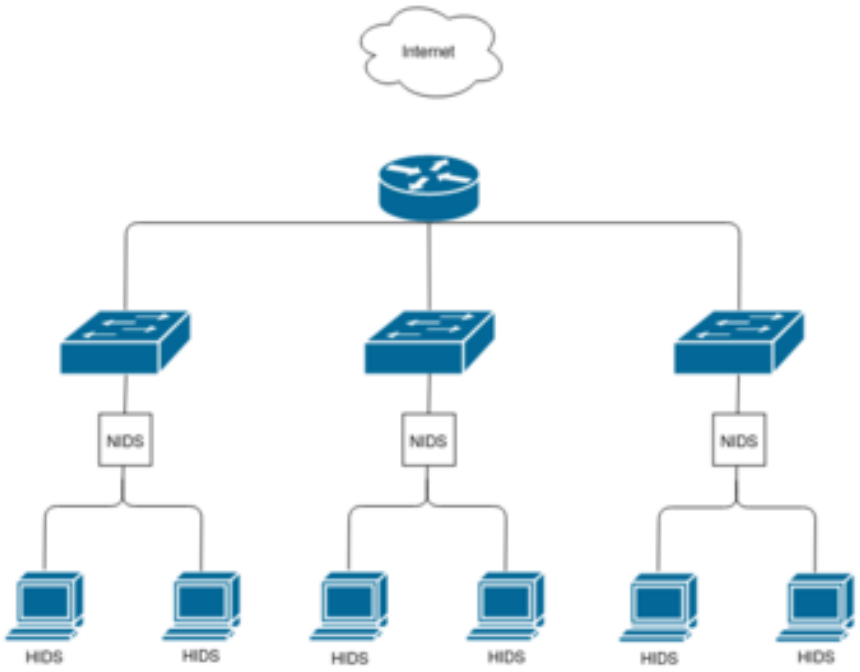
IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

iii. Les systèmes de détection d'intrusions de type hôte (HIDS)

Un HIDS se base sur une unique machine, n'analysant cette fois plus le trafic réseau mais l'activité se passant sur cette machine. Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.

Un HIDS a besoin d'un système sain pour vérifier l'intégrité des donnés. Si le système a été compromis par un pirate, le HIDS ne sera plus efficace.



IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

iv. Les systèmes de détection d'intrusions « hybrides »

Généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS.

v. Les systèmes de prévention d'intrusions (IPS)

Ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.

Contrairement aux IDS simples, les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

vi. Les systèmes de prévention d'intrusions « kernel » (KIDS/KIPS)

L'utilisation d'un détecteur d'intrusions au niveau noyau peut s'avérer parfois nécessaire pour sécuriser une station

Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le système.

Exemples de systèmes de détection d'intrusion

Systèmes de détection d'intrusion

- Snort
- Bro
- Suricata
- Enterasys

Systèmes de détection d'intrusion hôtes

- AIDE
- Chkrootkit
- DarkSpy
- Fail2ban

Hybrides

- Prelude
- OSSIM

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

vii. Les firewalls

Les firewalls ne sont pas des IDS à proprement parler mais ils permettent également de stopper des attaques.

Les firewalls sont basés sur des règles statiques afin de contrôler l'accès des flux. Ils travaillent en général au niveau des couches basses du modèle OSI (jusqu'au niveau 4), ce qui est insuffisant pour stopper une intrusion.

Il existe trois types de firewalls :

❶ Les systèmes à filtrage de paquets sans état : analyse les paquets les uns après les autres, de manière totalement indépendante.

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

❷ Les firewalls de type proxy : Le firewall s'intercale dans la session et analyse l'information afin de vérifier que les échanges protocolaires sont conformes aux normes.

❸ Les systèmes à maintien d'état (stateful) : vérifient que les paquets appartiennent à une session régulière. Ce type de firewall possède une table d'états où est stocké un suivi de chaque connexion établie, ce qui permet au firewall de prendre des décisions adaptées à la situation. Ces firewalls peuvent cependant être outrepassés en faisant croire que les paquets appartiennent à une session déjà établie.

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

viii. Les technologies complémentaires

- **Les scanners de vulnérabilités** : systèmes dont la fonction est d'énumérer les vulnérabilités présentes sur un système. Ces programmes utilisent une base de vulnérabilités connues (exemple : Nessus).

- **Les systèmes de leurre** : le but est de ralentir la progression d'un attaquant, en générant des fausses réponses.

- **Les systèmes de leurre et d'étude (Honeypots)** : le pirate est également leurré, mais en plus, toutes ses actions sont enregistrées. Elles seront ensuite étudiées afin de connaître les mécanismes d'intrusion utilisés par le hacker. Il sera ainsi plus facile d'offrir des protections par la suite.

IV. Détection d'attaques : les IDS

1.Les différents types d'IDS

viii. Les technologies complémentaires

- **Les systèmes de corrélation et de gestion des intrusions (SIM – Security Information Manager)** : centralisent et corrèlent les informations de sécurité provenant de plusieurs sources (IDS, firewalls, routeurs, applications, …). Les alertes sont ainsi plus faciles à analyser.

- **Les systèmes distribués à tolérance d'intrusion** : l'information sensible est répartie à plusieurs endroits géographiques mais des copies de fragments sont archivées sur différents sites pour assurer la disponibilité de l'information. Cependant, si un pirate arrive à s'introduire sur le système, il n'aura qu'une petite partie de l'information et celle-ci lui sera inutile .

Plan du cours

I. Introduction

II. Anatomie d'une attaque

III. Les différents types d'attaques

1. Les Malware
2. Les attaques réseaux
3. Les attaques applicatives
4. Le Déni de service

IV. Détection d'attaques : les IDS

V. Les méthodes de détection

V. Les méthodes de détection

Pour bien gérer un système de détection d'intrusions, il est important de comprendre comment celui-ci fonctionne.

- Comment une intrusion est elle détectée par un tel système ?
- Quel critère différencie un flux contenant une attaque d'un flux normal ?

Deux techniques sont mises en place dans la détection d'attaques :

⇨ La première consiste à détecter des signatures d'attaques connues dans les paquets circulant sur le réseau.

⇨ La seconde, consiste quant à elle, à détecter une activité suspecte dans le comportement de l'utilisateur

V. Les méthodes de détection

i. L'approche par scénario

Cette technique s'appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques. Elle ne tient pas compte des actions passées de l'utilisateur et utilise des signatures d'attaques (= ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte, …).

V. Les méthodes de détection

ii. L'approche comportementale (Anomaly Detection)

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Pour cela, il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent.

Cette technique peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion, …