Menace passive :

L'intrus ne s'interfère pas dans le trafic ou autre et se contente d'observer pour une éventuelle attaque active

Menace active :

L'intrus tente de modifier ou supprimer des informations relatives au réseau ou au système ou ajouter des logiciels malveillants

Confidentialité :

Seuls les utilisateurs autorisés ont accès aux données

Intégrité :

Une information est intègre si on est capable de prouver avec certitude qu'elle n'a pas été modifiée

Disponibilité :

Quand un système d'information fonctionne correctement lors d'un haussement de trafic ou lors des pannes

Authenticité :

Lorsqu'on peut déduire l'origine de l'information d'une manière sûre

Autorisation :

Spécifier et vérifier les droits d'accès

Principes fondamentaux :

- **Moindres privilèges**
- **Ne pas faire reposer la sécurité sur un seul mécanisme de protection**
- **Goulet d'étranglement : l'entrée et sortie des informations concentrées en un point**
- **On interdit toutes activité first, puis nous autorisons petit à petit**

Sniffing :

Capture une image du trafic dans le réseau

Sniffing :

L'écoute du réseau en capturant des images du trafic

Hijacking (vol d'une session) :

Quand l'utilisateur se connecte, le pirate prend le control de sa session

Spoofing :

Cas 1 : attaquant et victime ne sont pas sous le même réseau

1. **Utilisant l'@IP de la machine 3 de confiance, l'attaquant envoie une requête à la cible**
2. **La cible renvoi un paquet avec un ACK (exp = 100) à la machine 3**
3. **Puisque l'attaquant et la machine 3 sont sous le même réseau, il utilise le sniffer pour connaitre l'ACK reçu et envoyer un nouveau paquet avec ACK=101 pour devenir digne de confiance**

Cas 2 : sous le même réseau

Même scénario sauf que tout cela se trouvera dans le même sous réseau

Cas 3 : Spoofing aveugle

L'attaquant n'est ni dans le sous réseau de la machine 3 ni dans celui de la cible => Ouverture de quelques connexions légitimes avec la cible

Dénis de service :

Empêche le service de fonctionner correctement

Flooding :

Bombardement de données sur un serveur ou une machine

Attaque par réflexion :

Envoie de la requête à grand nombre de machines, chacune allant répondre à la victime

Distribué (DDOS) :

Attaque d'une cible avec plusieurs machines simultanément

Virus :

Se lie à un fichier hôte

Vers :

S'auto-reproduit et se déplace à travers un réseau

Cheval de Troie :

Joue le rôle d'un logiciel normal pour enfin voler les données ou nuire

Backdoors :

Logiciel qui permet à l'attaquant de prendre le contrôle de la machine cible à distance

Spywares :

Logiciel espion qui récole des données

Adwares :

Présente des pubs sans espionner

RoolKits:

Ensemble de d'outils qui cachent le logiciel malveillant

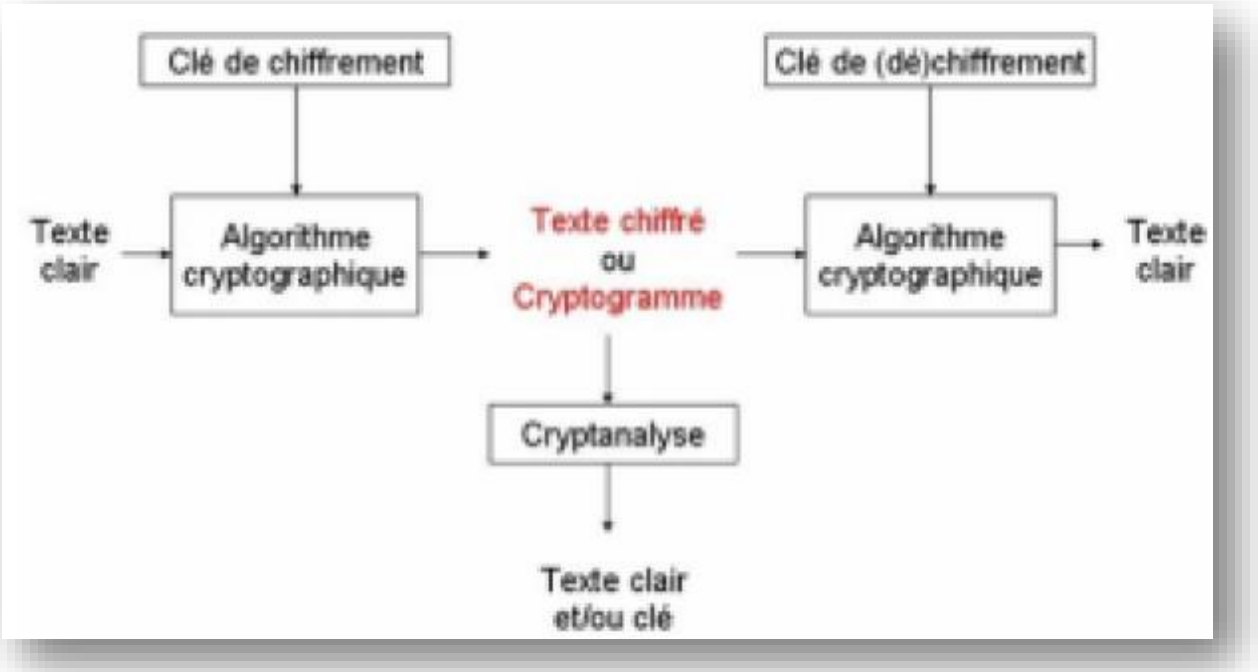
CryptoVirus :

Le code malveillant est chiffré sur une clé aléatoire et différente pour chaque copie de ce code

Fonctionnement de l'anti-virus :

1. **Scanning de la signature du virus**
2. **Analyse du comportement de possible virus**

Cryptographie :



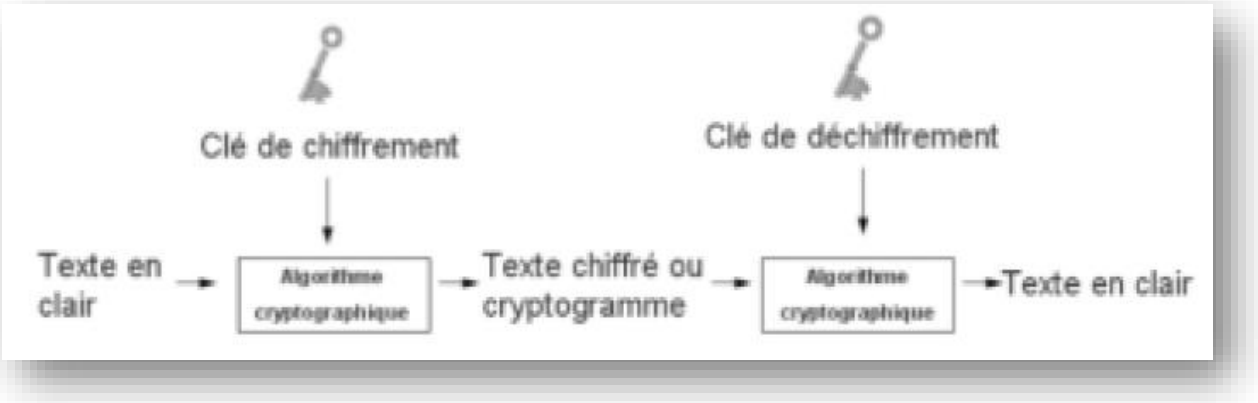
L'étude permettant de protéger l'information en termes de *confidentialité, authenticité* et *intégrité*

Décryptage :

Retrouver le texte chiffré sans avoir recours à la clé de déchiffrement

Algorithmes les plus répondus :

- **DES**
- **AES**
- **3DES**



Clé secrète asymétrique :

- **Une paire de clé**
- **Clé publique (distribuée pour tout le monde)**
- **Clé privée (une seule entité la possède)**
- **Exp : RSA**

La fonction de hashage :

Ne prend pas une clé cryptographique en paramètre

Comment assurer les objectifs principaux de la sécurité :

1. **Confidentialité : Chiffrement du message**
2. **Intégrité : Voir si le message n'a pas subi de modification durant la communication**
3. **Authenticité :**
    a. **Au niveau des communicant : Par des défis (envoi d'un message attendant la bonne réponse)**
    b. **Au niveau du code MAC : Le bloc authentificateur se base sur le message et la clé secrète**

Le pare-feu :

Filtrage :

- **Allow : Autoriser le paquet**
- **Deny : Bloquer le paquet**
- **Drop : Le rejeter sans avertissement et informations**

Critère de filtrage :

@IP_s, @IP_d, Protocole, Port, Drapeau (SYN, ACK, …)

Génération du journal :

Journalisation

NAT :

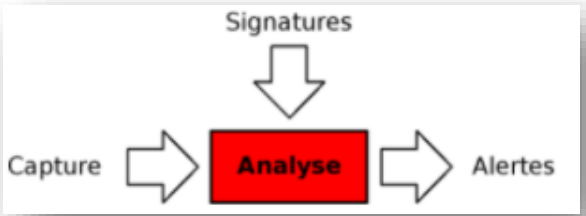
Source	Port	Dest	Port	Source	Port	Dest	Port
~~10.0.0.1~~	3001	128.8.6.3	80	172.1.3.2	3001	128.8.6.3	80
~~10.0.0.1~~	~~3001~~	128.8.6.3	80	172.1.3.2	1102	128.8.6.3	80

Transformation de l'@IP_s en une seule avec changement du port, faisant croire qu'il s'agit de la même machine qui envoie

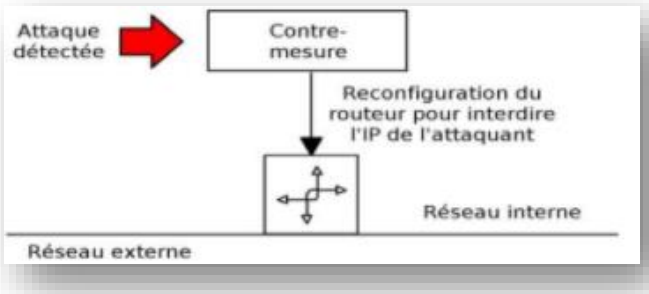
Détection d'intrusion :

Principe de fonctionnement :

1. **Informer l'utilisateur**



2. **Reconfigurer le pare-feu**



Méthodes de détection :

Se base sur une base de données de signatures d'attaques connues ou le comportement du trafic et compare

Proxy :

- **Traite la sécurité au niveau de la couche application**
- **Un utilisateur ne se connecte plus à un serveur directement mais à travers un proxy**

Fonctionnement :

1. **Connexion de l'ordi au proxy**
2. **Le proxy se connecte au serveur (Internet)**
3. **Vous demandez des pages au serveur**
4. **Analyse de la requête (filtrage) du proxy pour voir si elle est autorisée ou non**
5. **Recherche de la page sur le serveur**
6. **Analyse de la page et renvoi vers l'utilisateur**

Avantages :

- **Utilisation de l'@ du proxy pour naviguer**
- **Filtrage**

Inconvénients :

- **L'administrateur du proxy a à sa disposition toutes vos informations et peut tout enregistrer**
- **Peut-être plus lent**

DMZ :

Il est utilisé quand un niveau de sécurité intermédiaire est requis

Celui-ci n'est ni connecté à un réseau interne, ni directement à Internet (Mise en place de pare-feu requise)

Mise en place des proxys pour une meilleure sécurité

Pour éviter que l'un des proxys n'espionne l'autre, le réseau local qui relie les proxys doit être un Switch