Sécurité

L’objectif de GNS3 est de simuler un réseau, et spécialement un routeur Cisco que l’on connecte à des machines.

Les dockers sont équivalent à un Raspberry dans la vie réelle.

# Système d’information

C’est un ensemble de ressources (matérielles et humaines) qui permet de regrouper, de collecter, de traiter, de classifier et de diffuser de l’information dans un environnement donné.

# Sécurité

C’est un ensemble de moyens techniques, organisationnels, juridiques et humains qui s’assurent que les ressources d’un système d’information sont bien utilisées suivant le cadre pour lequel ils ont été conçus.

# Contrôle d’accès

Contrôle d’accès sur l’environnement contenant les ressources.

# Filtrage

Contrôle des personnes qui ont accès aux ressources. Application d’un ensemble de règles qui va filtrer l’accès aux ressources.

# Anti-virus

**Virus :** Programme malveillant qui veut accéder aux ressources du système d’information en passant outre la sécurité (filtrage et contrôle d’accès).

**Antivirus :** Programme qui détecte les virus.

# Respect de la vie privée

Est-ce que mon système ne met pas en danger les informations privées de l’utilisateur. Est-ce que oui ou non j’ai le droit d’analyser, de surveiller les activités que l’utilisateur est en train de réaliser.

* Attaquant

Une personne qui dispose d’une expertise.

Différents types :

* **Whitehat** : Gentil
* **Blackhat** : Méchant
* **Greyhat** : Dépend des jours
* **Redteam** : Recrute un Blackhat pour faire les attaques

Un groupe d’attaquant est plus puissant, cela démultiplie l’attaque.

# Les motivations

Ces motivations peuvent être l’argent, la notoriété, la vengeance, le défi technique.

**Crime organisés, terrorisme** : l’objectif est de nuire.

**Concurrence** : On a tout intérêt à montrer que la sécurité du concurrent est facilement prenable.

# Les menaces

C’est une violation potentielle de la sécurité, du système d’information. Cette violation peut être accidentelle, intentionnelle. Elle peut être active ou passive.

Passive : Je ne fais que d’écouter

**Quels sont les menaces ?**

## Déguisement

**IP Spoofing** : Recruter l’@IP d’une autre station afin de se comporter comme elle

**DNS Spoofing** : Faire croire que [www.google.fr](http://www.google.fr) pointe sur le site de google alors qu’il pointe vers moi.

**Social engineering :**  Plus on a d’informations personnelles sur une personne, plus on est en mesure de la hacker.

## Répétition (ou replay)

On écoute quelqu’un qui est en train de se connecter à un serveur distant.

**Ex**: quelqu’un se connecte à un serveur, en écoutant, on a réussi à récupérer le login et le mot de passe. Si le serveur est crypté, on renvoie la capture que l’on a faite.

## Analyse de trafic

**Sniffing :** Analyser le trafic (ex : Wireshark). Pour limiter, il faut mettre du contrôle d’accès et du filtrage.

## Inférences

Obtenir des données confidentielles à partir d’un raisonnement sur les données accessibles. Deviner des données confidentielles à partir des données qui sont publiquement accessibles.

## Répudiation

Nier le fait d’avoir commis une action.

Modification des messages et/ou interception de trafic

Wireshark

John the ripper : Cracker les mots de passe

Déni de service (Denial of Service) : DOS/DDOS

L’objectif est de surcharger la machine cible. On cherche à faire un arrêt du service distant.

Modification de programmes

* **Virus** : C’est un exécutable qui va exécuter des opérations plus ou moins destructibles sur la machine.
* **Cheval de troie (trojan)** : Lance un serveur qui ouvre une socket et prend le contrôle de la machine distante. Le pirate a accès à la totalité du disque.
* **Keylogger** : Logiciel espion ou périphérique qui espionne électroniquement l'utilisateur d'un ordinateur (enregistreur de frappe).

Porte dérobée ou backdoor

Dans un [logiciel](https://fr.wikipedia.org/wiki/Logiciel), une **porte dérobée** est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en [cheval de Troie](https://fr.wikipedia.org/wiki/Cheval_de_Troie_(informatique)).

Une porte dérobée peut être introduite soit par le [développeur](https://fr.wikipedia.org/wiki/D%C3%A9veloppeur) du logiciel, soit par un tiers. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par contournement de l'[authentification](https://fr.wikipedia.org/wiki/Authentification)).

Spyware (collecte de données personnelles)

Un **logiciel espion** est un [logiciel malveillant](https://fr.wikipedia.org/wiki/Logiciel_malveillant) qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des [informations](https://fr.wikipedia.org/wiki/Information) sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'[Internet](https://fr.wikipedia.org/wiki/Internet) qui lui sert de moyen de [transmission de données](https://fr.wikipedia.org/wiki/Transmission_de_donn%C3%A9es).

Ver ou worm

Un ver, contrairement à un [virus informatique](https://fr.wikipedia.org/wiki/Virus_informatique), n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

L'objectif d'un ver n'est pas seulement de se reproduire. Le ver a aussi habituellement un objectif malfaisant, par exemple :

* [espionner](https://fr.wikipedia.org/wiki/Logiciel_espion) l'ordinateur où il se trouve ;
* offrir une [porte dérobée](https://fr.wikipedia.org/wiki/Porte_d%C3%A9rob%C3%A9e) à des [pirates informatiques](https://fr.wikipedia.org/wiki/Pirates_informatiques) ;
* détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts ;
* envoyer de multiples requêtes vers un [site Internet](https://fr.wikipedia.org/wiki/Site_Internet) dans le but de le saturer ([déni de service](https://fr.wikipedia.org/wiki/D%C3%A9ni_de_service)).

Exploits

Sur les consoles.

Un **exploit** est, dans le domaine de la [sécurité informatique](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_informatique), un élément de [programme](https://fr.wikipedia.org/wiki/Programme_informatique) permettant à un individu ou à un [logiciel](https://fr.wikipedia.org/wiki/Logiciel) malveillant d'exploiter une [faille de sécurité informatique](https://fr.wikipedia.org/wiki/Faille_de_s%C3%A9curit%C3%A9_informatique) dans un système informatique.

Que ce soit à distance (*remote exploit*) ou sur la machine sur laquelle cet exploit est exécuté (*local exploit*), le but de cette manœuvre est de s'emparer des ressources d'un ordinateur ou d'un [réseau](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique), d'accroître le [privilège](https://fr.wikipedia.org/wiki/Privil%C3%A8ge_(informatique)) d'un logiciel ou d'un utilisateur sur la machine-cible, ou encore d'effectuer une attaque par [déni de service](https://fr.wikipedia.org/wiki/D%C3%A9ni_de_service).

Rootkit

Ensemble de logiciels qui permettent d’avoir le droit d’administration sur une machine.

Web

Injection de code dans chaine de caractère

Fingerprinting

Détecter quel OS et quelle version possède l’utilisateur

**Cryptographie : Les bases**

**Cryptographie** : permet de protéger l’information : l’art de garder un secret

**Cryptanalyse** : Déchiffrer des messages chiffrés (avec le plus d’informations possibles).

**Cryptologie** : Cryptographie + Cryptanalyse → Branche de mathématiques

Le message d’origine : texte clair

Chiffrement : Processus qui consiste à transformer le texte clair. (le processus inverse est le déchiffrement)

Le chiffrement seul ne suffit pas à tout garantir:

* la confidentialité
* l’intégrité
* authentification
* non répudiation

Un cryptage adéquat est un cryptage qui utilise :

* Un algorithme de chiffrement
* Un algorithme de déchiffrement
* Une clé ou une paire de clé
* Bon sens

Algorithme de chiffrement = Fonction mathématique

Attention : Ce n’est pas parce que l’algorithme est secret que l’on peut garantir la sécurité.

Les algorithmes à clés secrètes

La clé de chiffrement peut être déduit de la clé de déchiffrement (en générale c’est la même).

L'émetteur et le destinataire doivent se mettre d’accord sur une clé.

→ Cette clé doit rester secrète

Les algorithmes à clés publiques

La clé de chiffrement ne peut pas être déduite de la clé de déchiffrement.

→ Evaluation du coût en fonction de la complexité de l’information.

On a donc une complexité en temps et complexité en mémoire.

Les clés doivent être échangées de façon secrète

Cryptographie asymétrique

* 1976 Diffie et Hellmar révolutionne la cryptographie en introduisant le cryptage à clé publique
* Chaque participant possède 1 paire de clé différente reliée par un fonction mathématique
* La clé dite publique peut-être diffusée à tout le monde

Attention : La clé privée doit rester secrète. On ne peut pas déduire une clé d’une autre.

Bob veut envoyer un message à Alice. Il faut qu’il ait la clé publique d’Alice.

Si n participants :

→ n paires de clés

→ chaque participant possède la paire de clé

→ Un mécanisme permet de distribuer les clés publiques

Authentification

Signatures : Signature numérique qui permet d’authentifier l’auteur d’un document et d’en garantir l’intégrité.

Fonction de hachage

Fonction non réversible.

Il faut faire attention aux collisions.

On utilise l’algorithme md5.