Cyber Sécurité

**Formateur** sylvain THIROINE

# Introduction

La cybersécurité c’est la protection des données numérique pour l’humain. En France, c’est l’ANSSI qui est responsable de toutes la certification, prévention autour de la cybersécurité. Dans l’éco system cyber il y a deux entités : les acteur public *(ANSSI, CNIL, gendarmerie)* & les entreprise privé *(TALES, airbus security)*. C’est ANSSI qui gère cela en définissant les accréditations de chacun.

En France le COM Cyber a le droit de faire des attaques informatiques, à part eux les gendarmes doivent demander à COM Cyber l’autorisation de faire des attaques informatiques.

Acteur public

**ANSSI**

Premier organisme responsable du cyber en France, elle s’occupe de la sécurité informatique des OAV *(entreprise vitale pour la survie de la France si elle est attaqué)* & délivre des certificat et des référentielle pour normalisé les connaissances attendu d’un expert cyber & guide de transmission.

**Les services de renseignement**

* DGSE
* DGSI
* DRSD : Direction du Renseignement et de la sécurité de la Défense
* DRM : Direction du Renseignement Militaire
* DNRED : Direction Nationale du Renseignement et des Enquêtes Douanières
* TRACFIN : Service

**Armée française**

* COMCYBER : COMandemant de la CYBERdéfanse
* DGA : Direction Général de L’armement

Seuls les services de renseignements et l’armée française (via COMCYBER) ont le droit de mener des cyberattaques.

Acteur privée

**Les entreprises du service numérique**

Ces entrepris proposent :

* Des audits
* Mise en place d’un SOC
* Mise à disposition d’expert en cybersécurité CERT

# Les principes de bases de la cybersécurité

## Les objectifs de la cybersécurité

**L’intégrité :** Le DCP définie comment protéger le réseau contre toutes suppression ou modification abusive, afin de garantie que les données sont bonnes celle que l’on croit être.

**La disponibilité :** Le réseau doit toujours être disponibles *(déni de service)*.

**Confidentialité :** empêcher l’accès aux données *(chiffrement authentification, mot de passe)*

**La non-répudiation :** consiste en l’assurance qu’une action est bien identifié à une personne.

**L’authentification :** assurer que seules les personnes autorisées ont accès aux ressources.

## Les aspects élémentaires de la sécurité informatique

**La prévention :**

* Analyser les risques
* Définir une politique de sécurité
* Mettre en œuvre cette solution
* Évaluer cette solution
* Mettre à jours la solution et la politique au regard de l’évolution des risques

**Détection :** *(*Effectuer l’inventaire des actifs*)*

* Des systèmes d’exploitation
* Antivirus à jour
* Examiner les programmes et services inactif

**La réaction :** *(qui peut accéder à quoi)*

* Niveau d’accès de chaque utilisateur
* Rechercher les pics suspects de l’activité *(suppression des données, connexions illicite)*

## Les trois notions en sécurité

* **Vulnérabilité =>** Faiblesse au niveau d’un bien
* **Menace** **=>** cause potentiel d’un incident qui pourrait causer des dommages par l’exploitation d’une vulnérabilité.
* **Attaque =>** a des chances de réussir que si elle exploite une vulnérabilité

Ainsi tout le travail des expert cyber est de savoir si le S.I. a des vulnérabilités

Menaces

* Hameçonnage & Ingénierie social
* Fraude interne
* Violation d’accès non autorisé
* Virus informatique
* Déni de service

**Extraction, fuite ou suppression de données**

Consiste à copier, transférer, ou supprimer sans autorisation des données hors du domaines. Via fraude interne ou extradition des données par un programme malveillant.

**Attaque interne malveillante**

Commise par administrateur approuvé de votre organisation qui a sciâmes transférer des informations sensibles en dehors de l’entreprise.

**Violation de compte**

Accès non autorisé au compte d'un utilisateur ou d'un administrateur du domaine. Elle se produit lorsqu'un utilisateur non autorisé dérobe des identifiants de connexion. Dans ce scénario, un compte du domaine est piraté de telle sorte qu'il peut être utilisé par une personne malveillante pour interagir avec des ressources. Le harponnage représente une méthode courante de vol d'identifiants. Dans ce cas, les pirates informatiques envoient frauduleusement un e-mail qui semble provenir d'une personne ou d'une entreprise que vous connaissez et en qui vous avez confiance.

**Violations du droit**

Fait référence au cas où une personne malveillante réussit à pirater un ou plusieurs comptes dans votre domaine et tente de tirer parti d'autorisations limitées pour accéder à des comples qui disposent d'autonsations plus étendues. Ce type de pirate informatique tente généralemerit d'accéder à des droits d'administrateur généraux pour mieux prendre le contrôle des ressources de votre domaine.

**Cassage de Mot de passe**

Est un processus de récupération de MDP qui s’effectue à l’aide

**Hameçonnage**

**Spoofing**

Falsification d’un entête de mail par un pirate destinée à faire croire que le message provient d’une personne autre que la véritable source. Usurpation d’adresse mail.

**Fraude interne**

**Déni de service**

Utilisation de botnet pour des attaques de 34h en moyenne.

## Déroulement d’une attaque

A : envoie un courriel à sa cible

C : est crédule, ouvre le mail => annonce de la compromission

A : Prend le contrôle de la cible

A : Connexion

C : Attaque et prise de contrôler d’un serveur

A : Prise de contrôle des machines qui trafic par le serveur de commandes

C : Demande de contenu du répertoire cible

S : Fournie les données

C : Efface les traces en sens inverse

## L’aspect éthique de la sécurité informatique

* Ne pas utilisez de techniques malveillantes pour accéder à des systèmes informatiques ou à des données
* Respecter les lois et les réglementations applicables
* Respecter la vie privée des utilisateurs
* Éviter de causer des dommages ou des perturbations aux services informatiques
* Obtenir du propriétaire du système informatique avant d’y accéder

## Respecter les lois lors de l’utilisation d’outils de sécurité

Définition de la cybercriminalité : Ensemble des actes contrevenant aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d’informations comme moyen de réalisation d’un délit, d’un crime, ou les ayant pour cible.

**La loi Godfrain** : 1988 stipules que l’accès ou la manipulation frauduleux dans tout ou une partie d’un système de traitement automatisé de données est puni de 2 ans & 30.000€ d’amande

**Entraver ou de fausser le fonctionnement** d’un tel système est puni de 5ans de prison & 75.000€ d’amande.

**L’introduction, la suppression ou la modification frauduleuse** **de données** dans un système de traitement automatisé, est puni de 5ans et 75.000€ d’amende.

**Le fait d’importer, céder ou de mettre à disposition**, sans motif légitime, un programme ou un moyen permettant de commettre les infractions ci-dessus.

# Introduction au pentesting

## Définitions

**Le pentesting** est également appelé test d’intrusion ou test de pénétration. C’est une technique qui consiste à analyser une cible en se comportant comme un pirate informatique.

Objectif

L’objectif est de réparer les potentielles failles et vulnérabilités de votre système. Il permettra de corriger les vulnérabilités afin de sécuriser vos infrastructures.

## Les types de test d’intrusion

### Boite noire

* C’est le test le plus proches des conditions réelles
* Le Pentester n’a aucune information sur le système
* Collecte d’information et recherche approfondie
* Recueille les informations accessibles au public : domain / ip
* Une partie considérable du temps est passé à la reconnaissance foot print & ingénierie social
* Cela prend du temps et coûte cher

### Boite blanche

* Le test d’intrusion en boite blanche est réalisé avec un maximum d’information sur le system d’information.
* Permet de trouver les bug et vulnérabilité plus rapidement

### Boite grise

* Informations sur le fonctionnement de la cible
* Fournies des comptes utilisateurs sur la plate-forme à accès restreinte
* Donner accès à une cible non accessible au public
* L’évaluation et le test de sécurité sont effectué en interne
* Il est réalisé le plus souvent lorsqu’un pentester qui fait une boite noire considère qu’il a besoin de quelques informations préalable pour réaliser son audit.

## Les phases d’un test d’intrusion

* Planification
* Reconnaissance => comprendre les besoins et objectif du pentest le testeur doit recueillir des informations sur la cible :
  + Son architecture
  + Ses systèmes d’exploitation
  + Ses applications
  + Ses protocoles de communication
  + Ses points d’entrée potentiels
* Analyse des vulnérabilités et Post-exploitation
* Élaboration du rapport
* Nettoyage et suivie
  + Proposer des recommandations & des recommandation alternative *(pas cher)*
  + Passer 3 semaines / 3 mois plus tard pour vérifier l’application des mesures corrective

### La planification et préparation

Définir les objectifs du pentest & Obtenir les autorisations nécessaires

*(Préparatif du contrat)*

* Identification des objets et des attentes
* Les parties prenantes
* Les limites du test *(définie le type de boite + interdiction du tester)*
  + Sans autorisation de modification du réseau pas de boite noir ou grise, seul la blanche *(repérage des failles uniquement)*
* Les règles d’engagement *(ROE)*
* Définir les équipes de travail
  + Directeur des opérations
* Procédure à suivre
* Réunions de travail