**Sécuriser communications**

Acheter ordinateur d’occasion

Connecter sur un wifi

Firewall – sécurité

Proxy

VPN – changer de serveur

OS – Linux

Thor -> internet parallel

Black hat -> mechant

White Hat -> Gentil

Dark web

Malware -> cyber arme rentrer dans un ordinateur discrètement

Jabber -> communication anonyme

Toujours faire des backups des bases de données

Dsi direction de système d’information

SI système d’information

SSI -> sécurité des systèmes d’informations

Machines Zombies -> ordinateurs avec un malware qui font la même action

Hard control -> puissance militaire : USA1#

Soft control -> puissance à rayonner culturellement, à influencer : France 1#

Risque = préjudice (argent, personnes...) x probabilité d’occurrence

**AVPA :** Amenez votre propre appareil -> Buy Your Own Device

Quand sauvegarde fichiers perso -> CONFIDENTIEL

Cible de sécurité -> contre quoi se prémunir (périmètre)

FAI fournisseurs français d’accès Internet

Habilitation : niveau d’accès à une donnée

Token : Signature -> informations de l’utilisateur

Man of the middle intercepte une communication non cryptée

Premier algorithme de cryptographie : chiffre de césar

**Empêcher les intrusions**

Identifier et détruire

Pare-feu (firewalls) filtrage des communication réseau

**Certificat SSL**: Secure Socket Layer (ne peut pas être gérer pas un organisme) certificat qui passe la page en Https donc crypté les données. SI le cadenas est rouge : Le ssl n’est pas sûr, sil il est vert c’est qu’il est sûr.

**DMZ**: machine coupée du réseau

**Bastion**: ce qui va faire front aux attaques

**IDS**

**IPS**: système de prévention d’intrusion -> autoscalé : poper instance virtuelle, bannir les premier IPs d’intrus

**CERT** computer emergency response teams, pour une description de ces centres

**RSSI** responsable de sécurité des systèmes d’Information

Hameçonnage : phishing

Structurer au maximum -> pour tenir au courant les utilisateurs

ANSSI

**Cybersqatting**: Réserver un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom ai profit de titulaire plus naturels ou légitimes.

**Canular Hoax**: information vraie ou fausse, souvent transmise par messagerie électronique -> fausse alerte ou virus.

**Capteur de clavier (Keylogger, keystroke logger)** enregistre tous les mots tapés sur l’ordinateur

**Cheval de Troie (Trojan Horse)**: Programme donnant l’impression d’avoir fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante. (Malware, virus).

**Clonage de serveur DNS (DNS Pharming)**: Site factice

**Code d’exploitation**: utiliser une vulnérabilité d’un logiciel à des fins malveillants.

**Code Malveillant, logiciel malveillant**: tout programme dvp dans le but de nuire à un système d’information.

**Défiguration, barbouillage**: modifie l’apparence ou le contenue d’un serveur internet.

**Déni de service**: saturer un serveur (mail bombing, réseau de machine zombie)

**Dépassement ou débordement de mémoire (buffer overflow)**: saturer la mémoire d’un système informatique

Elévation de privilège (privilege escalation)

**Spyware (logiciel espion)**: collecte les données d’un ordinateur

**Exécution de code arbitraire à distance**: mise en œuvre de commandes à distance sur un ordinateur, à l’insu de son utilisateur.

**Faute de frappe (Typosquatting)**: faute de frappe dans l’url qui amène à un site malveillant

**Hameçonnage ciblé (spearfishing)**: se faire passer pour quelqu’un, mail gohst : possibilité d’envoyer un mail avec une adresse celui qu’on veut

**Hameçonnage (phishing)**: vol d’identités ou d’informations confidentielles

**Man of the middle**: récupère des informations entre récepteurs et émetteurs

**Injection de code indirect (cross site scripting, css, xss)**

**Aware (logiciel publicitaire)** code ayant pour finalité d’afficher de bandeaux publicitaires par le biais du navigateur internet de l’utilisateur

**Moisson de couriels**: action qui consiste à parcourir un grand nombre de ressources publiques

**Mouchard internet**: support graphique implanté dans une page internet (spyware)

**Outil de dissimulation d’activité Rootkit**: tout programme permettant de dissimuler une activité, malveillante ou non sur une machine

**Backdoor**: porte ouverte pour rentrer dans un ordinateur

**Point d’eau :** type d’attaque destiné à infecter les ordinateurs de personnels œuvrant dans un secteur d’activité ou une organisation ciblée

**Polymorphe**: se dit d’un Ver ou d’un virus dont le code est chiffré, changeant le code de déchiffrement d’une infection à l’autre, et donc l’apparence et/ou la signature.

**Ranswome Ware**: chantage d’argent wannacry

**Sniffer**: capter des données (trames) sur un réseau wireshark, balise d’interception -> interception communication entre téléphone et antenne relais

**Usurpation d’adresse**: comme sniffer

**Ver**: cherche à répandre son code dans le plus d’ordinateur

**Virus**: Destruction

**OWASP**: recommandation de sécuriser son application, caritative -> 10 risques de sécurité les plus exploités par an.

Open web application Security Project

O2WASP

10 risques:

* Injection #1 -> PHP plus vulnerable
* Violation de Géstion d’Authentification
* Exposition de données Sensibles -> Big Data

Si on arrive à comprendre les vecteurs d’attaques on peut comprendre comment les éviter.

Passer par une Api pour un Web Service -> double vérification javascript + code d’erreur 400 API

**Fuzzer :** logiciel d’analyse de faille

2019 : les 10 attaques les plus répandu

* 1# **Injection** -> On considère que n’importe qui peut rentrer des données non fiables au système. Très vulnérable avec code ancien, les injections se font le plus avec SQL et NOSQL. White list/black list -> permet de lister les gens bannis ou non. Bien protéger les inputs.
* 2# **Broken Authentification** -> (casser une authentification) les attaquants ont des accès à des centaines de millions de login et mot de passe, des comptes par défaut d’administration, d’outils de force brut.
* 3# **exposition des données sensibles** -> man of the middle (Oublie de crypter les données en transit, génération de clés faible) -> la personne récupère les données en transit. Les GPUs permettent de paralléliser les actions. Comment les empêcher : Classifier les données, degrés de confidentialité, ne stocker pas les données sensibles inutiles, crypter toutes les données en transit, algorithme de cryptage à jour, chiffrement **PFS (Perfect Forward Secret)** ...
* 4# **XML External Entities (XXE)** -> attaquant peuvent exploiter des processeurs XML vulnérable s’ils peuvent le télécharger ou intégrer du code malveillant. Soit du XML ou du SVG. Logiciel SAST peuvent découvrir ces problèmes. Il faut utiliser JSON pour éviter ce problème
* 5# **Broken** **Access** **Control** -> casse l’accès au contrôle des permissions, élévation de privilège. Tout doit être bloqué par un token - un package qui parle à toute les APIs.
* 6# **Mauvaise configuration de sécurité** : mauvaise configuration des couches de sécurités : services des réseaux, la plateforme, le serveur Web, la base de données. Une telle intrusion fournis souvent aux attaquant un accès non autorisé. Structuré et sécuriser chaque composant de l’application. SSH -> moyen de rentrer dans un serveur avec login et mot de passe.
* 7# **Cross-Site Scripting (XSS) :** Menace **:** Des outils automatisés permettent de détecter et d’exploiter les trois types de XSS et des frameworks d’exploitation gratuits sont disponibles. Vulnérabilité : PHP JEE/JSE et ASP.NET. Bien sécuriser les inputs car l’attaquant peut écrire du HTML, du XML ou du javascript.
* 8# **Insecure Deserialization : deserialiser**: prendre des données pour les transformer en objet -> serveur à client. Empêcher : implémenter des contrôles d’intégrité tels que des signatures numériques. Appliquer des contraintes de typage.
* 9# **Utilisation de composants avec des vulnérabilités Connues**: vulnérabilité -> utilisation de trop de package (par exemple chaque package utilise des packages). Il faudrait crée soit même les packages pour ne pas avoir de faille de sécurité. Mais cela prend beaucoup de temps.
* 10# Supervision et journalisation insuffisante : Si on est pas au courant on ne peut pas empêcher l’intrusion. Donc il faut monitorer mettre des alertes de seuil d’erreur.