2024.09.19 - Bloc 3 - Cours Sécurité informatique

**

La sécurité informatique est devenue fondamentale, elle n'est plus une option.

Cela s'applique autant dans le domaine professionnel que personnel. Nous allons évoquer des situations communes, que ce soit à la maison ou directement au travail.

La sécurité informatique est en constante évolution.

Il est important de prendre conscience de la responsabilité que nous aurons à assumer, que ce soit dans le cadre de nos travaux en entreprise ou à la maison. Un manque de vigilance peut entraîner des dégâts considérables et avoir de graves conséquences.

Réflexes de sécurité informatique

1. Avoir des mots de passe (mdp) de qualité

Il est important d'utiliser des mots de passe solides. Voici quelques bonnes pratiques à suivre :

- Un mot de passe doit comporter au moins 12 caractères, incluant une majuscule, une minuscule, un chiffre et des caractères spéciaux.
- Évitez d'utiliser des informations personnelles (dates de naissance, noms familiers, etc.).
- Ne pas utiliser le même mot de passe partout. Préférez des mots neutres et n'utilisez pas de langues courantes comme le français.

Exemple :
"Combien de temps faut-il à un pirate pour trouver votre mot de passe en 2024 ?"

Des outils comme Kaspersky peuvent vérifier la résistance de vos mots de passe.

2. Vérification des fuites de données

- Have I Been Pwned? est un site qui vous aide à savoir si votre adresse email ou numéro de téléphone a déjà été impliqué dans une fuite de données.
  👉 https://haveibeenpwned.com/
- WhatsMyName.app permet de vérifier sur quels sites vos informations sont potentiellement utilisées.
  👉 https://whatsmyname.app/

3. Gestionnaires de mots de passe : à éviter

Il est déconseillé d'enregistrer vos mots de passe dans des gestionnaires automatiques ou d'utiliser des générateurs de mots de passe. Jusqu'à présent, aucun des logiciels existants n'a réussi à passer tous les tests de sécurité. Aucune solution n'est 100 % sécurisée.

Astuce :
Utilisez des clés physiques, comme les clés Titan, qui peuvent servir de mots de passe. Il est conseillé d'en avoir deux, au cas où l'une serait perdue ou cassée.

4. Stratégie de création de mots de passe

Une méthode simple consiste à utiliser des phrases ou des éléments déjà connus. Par exemple, prenez la première lettre de chaque mot d'une phrase ou d'une chanson.

Phrase de départ : "Feel the magic in the air, Allez, allez, allez, Levez les mains en l'air, Allez, allez, allez"

Mot de passe créé :

- Ftmitaaaallmel’aaaa
- Ftm1t@@@@llm€l’@@@@

Ensuite, modifiez certains mots comme "air" par "amazon", "caf", ou autre selon vos besoins. (S’il faut modifier régulièrement les mdp sur différents sites internet.

Avoir un système d’exploitation et des logiciels à jour

Toujours garantir les mises à jour de votre système d'exploitation et de vos logiciels, et les appliquer dès qu'elles sont disponibles.

Outil recommandé :
Le site endoflife.date permet de suivre les mises à jour de vos systèmes d'exploitation, de vos logiciels ou même de vos téléphones. Il vous informe si ces systèmes sont encore à jour.

Astuce : utilisez la fonction Ctrl + F pour rechercher rapidement des informations sur une page web.

Effectuer des sauvegardes régulières

En entreprise, si le budget le permet, il est impératif de réaliser des sauvegardes régulières. Nous ne pouvons plus considérer qu'un système est infaillible aujourd'hui. Il est donc essentiel de faire des sauvegardes fréquentes et de ne pas prendre cela à la légère.

Rappel :
On ne peut pas empêcher une attaque informatique, mais on peut la repousser ou en limiter les effets. Il y aura toujours une faille quelque part.

Plateforme recommandée :
M. Jobard a créé une plateforme avec de nombreux outils utiles :
👉 mewo.r3z.frMot de passe : mewo mewo

Ne pas cliquer trop vite sur des liens

Soyez toujours vigilant avant de cliquer sur un lien ou d'ouvrir une pièce jointe, surtout si vous ne l'attendiez pas.

Outil recommandé pour vérifier les liens :
👉 virustotal.com

Toujours faire fonctionner son cerveau

Réfléchissez avant d'agir. Ne cliquez jamais trop vite sans avoir pris le temps de vérifier l'authenticité d'un lien ou d'une pièce jointe.

Ne jamais utiliser un compte administrateur pour naviguer

Il est déconseillé d'utiliser un compte administrateur pour naviguer sur Internet. En cas de piratage, vous exposez votre système à des risques majeurs.
Solution : créez un compte utilisateur pour minimiser l'impact d'une éventuelle attaque.

Contrôler la diffusion d'informations personnelles

Il est important de se déconnecter des sites sur lesquels vous êtes inscrits et de fermer les comptes inutilisés, même ceux des services qui ne sont plus actifs. Cela réduit le risque de divulguer vos informations.

Sur chaque site, vérifiez les paramètres de confidentialité pour vous assurer qu'ils correspondent à vos attentes et à vos besoins.

Soyez vigilant sur ce que vous partagez en ligne.

Utilisation de cartes bancaires virtuelles

L'utilisation de cartes bancaires virtuelles peut également limiter les risques de piratage lors des transactions en ligne.

HoaxBuster : vérifier les informations trompeuses

Le site HoaxBuster vous permet de vérifier la véracité des informations diffusées sur Internet, notamment les rumeurs ou les canulars.
👉 hoaxbuster.comAstuce : Ce site est particulièrement utile pour détecter les fausses informations diffusées dans les médias (par exemple, le Gorafi, parodie du Figaro).

Précaution avec les pièces jointes

Si vous ne vous attendez pas à recevoir une pièce jointe, ne l'ouvrez pas.

Réflexes orientés PRO

1. Ne pas mélanger le professionnel et le personnel

Depuis la généralisation du télétravail, la frontière entre le monde professionnel et personnel s'est estompée, ce phénomène s'appelle le blurring. Il est d'ailleurs important de noter que nous ne sommes plus obligés de répondre à notre employeur en dehors des heures de travail.

Si votre compte personnel est piraté, il y a un risque que votre compte professionnel le soit aussi, et inversement. D'où l'intérêt de ne pas mélanger les deux et de bien sécuriser cette frontière.

---

2. Protéger ses données en déplacement

Lorsque vous êtes en déplacement, soyez particulièrement attentif aux données que vous transportez, qu'elles soient celles de vos clients ou les vôtres.

Quelques bonnes pratiques :

- Ne laissez jamais votre ordinateur ou vos documents sans surveillance (par exemple, éviter de laisser son PC ouvert et déverrouillé si vous quittez brièvement votre espace, comme pour aller aux toilettes dans un train).
- Évitez de vous connecter à des Wi-Fi publics sans utiliser un VPN pour protéger vos données.

3. Communiquer sur les méthodes d'échange

En cas d'arnaques visant à soutirer de l'argent, il est primordial d'établir des règles et des procédures claires pour les transactions financières comme les virements bancaires.

Exemple de procédure à suivre :

- Envoi d'un mail avec devis
- Pièce jointe incluse
- Validation par une tierce personne

---

4. Respecter la charte de l’entreprise

Il est essentiel de bien lire et comprendre la charte informatique de l'entreprise. En général, vous la signez automatiquement lors de votre entrée dans l'entreprise. Si elle ne vous est pas fournie, n'hésitez pas à la réclamer.

5. Signaler toute anomalie au service compétent

Ne restez jamais seul face à une difficulté ou une anomalie. Si vous rencontrez un problème, rapprochez-vous de votre tuteur ou du service compétent pour obtenir de l'aide.

Les acteurs du monde de la cybersécurité

(Site qui permet de voir les cyberattaques en temps réel : cyber map.kaspersky.com)

1. Script kiddies (“lamer”)

Ce terme désigne généralement une personne assez jeune, sans formation spécifique en informatique, mais ayant acquis certaines connaissances en suivant des tutoriels douteux, souvent trouvés sur YouTube.

- Caractéristiques : Il agit de manière imprévisible, sans réellement comprendre ce qu'il fait, souvent au hasard. Il n'a aucune conscience des conséquences de ses actes.
- Particularité : Ces individus sont souvent mineurs, ce qui les rend pratiquement intouchables légalement.

---

2. Hacktivistes

L'hacktiviste est souvent une personne ordinaire, comme un père ou une mère de famille, ayant des convictions très fortes. Il pense défendre une cause juste, ce qui motive ses actions de piratage.

- Exemple : Un militant végan qui déteste une marque de viande comme Charal et décide de mener des actions contre eux durant son temps libre.
- Point positif : Il est généralement prévisible.
- Point négatif : Sa détermination est alimentée par ses convictions, et il n'hésitera pas à dépenser son propre argent pour faire avancer sa cause.

3. Hackers

Le terme hacker est souvent mal utilisé (et ne veut pas forcément dire grand chose), il englobe en réalité plusieurs catégories :

3.1 White hats (Chapeaux blanc)

Ce sont les hackers éthiques, souvent employés par des entreprises ou des organisations gouvernementales pour protéger les systèmes informatiques.

- Exemple : Alain, qui travaille à la DGSI, est un hacker qui veille au bon fonctionnement et à la sécurité des infrastructures informatiques. C'est un "gentil" qui travaille pour l'État.

3.2 Black hats (Chapeaux noir)

Les black hats sont des hackers malveillants qui cherchent à nuire pour le plaisir, sans motivation financière.

- Exemple : Jérôme, 26 ans, éprouve une haine profonde envers les autres et souhaite utiliser ses compétences informatiques pour causer des dommages sans raison valable.

3.3 Grey hats (Chapeaux gris)

Ce sont des hackers ambigus, parfois "gentils", parfois "méchants", en fonction de leurs intérêts ou de leur humeur.

- Exemple : Adrien, 28 ans, découvre accidentellement un accès à des données sensibles sur un site web. Il hésite à savoir s'il doit agir de manière éthique ou non. Ses actions dépendent de son état d'esprit du moment.

---

4. Crackers

Les crackers sont des experts dans le "cassage" de mots de passe. Ils possèdent des compétences spécialisées pour briser les systèmes de protection par mot de passe.

- Exemple : Il existe une entreprise israélienne réputée pour ses capacités dans ce domaine.

5. Phreakers

Les phreakers sont des experts dans le piratage d'équipements mobiles, qu'il s'agisse de smartphones Android ou iPhone. Leur spécialité est de manipuler les téléphones pour en tirer profit.

Types d'attaques informatiques

1. Casse de base de données (BDD)

Cette attaque consiste à compromettre une base de données, permettant aux attaquants d'accéder à des informations sensibles. Cela peut inclure des données personnelles, financières ou d'entreprise.

---

2. MITM (attaque de l'homme du milieu)

L'attaque de l'homme du milieu consiste à intercepter les communications entre deux parties, souvent dans un réseau, sans que celles-ci s'en rendent compte. Le pirate se positionne "au milieu" pour capturer les informations échangées, comme des mots de passe ou des données sensibles.

---

3. Malware (Maliciels)

Les malwares sont des logiciels malveillants conçus pour nuire à un système informatique. Voici quelques types courants de malwares :

- Ransomware : Ce type de malware chiffre les données de la victime et bloque l'accès à la machine, exigeant une rançon en échange de la restitution des données. Cependant, rien ne garantit que les données seront réellement rendues après paiement.
  Outil recommandé : Nomoreransom.org peut aider à lutter contre les ransomwares.
- Ver (worm) : Un logiciel qui infecte un PC avec pour objectif principal de se reproduire et de se propager à d'autres machines, souvent sans intervention humaine.
- Keylogger : Ce dispositif espion suit en temps réel ce que l'utilisateur tape sur son clavier, enregistrant potentiellement des informations sensibles comme des mots de passe ou des

données personnelles.

- Cheval de Troie : Un logiciel qui se présente comme légitime mais qui, une fois installé, permet à l'attaquant de prendre le contrôle du système.
- Adware : Ce type de malware affiche des publicités indésirables sur l'ordinateur de l'utilisateur, parfois en ralentissant le système ou en recueillant des données à des fins publicitaires.

---

4. Faille XSS (Cross-Site Scripting)

L'attaque XSS consiste à injecter du code malveillant dans un site web vulnérable, souvent via des formulaires ou des champs de saisie, afin d'exécuter ce code sur le navigateur des utilisateurs visitant le site.

---

5. Injection SQL

L'injection SQL permet aux attaquants de manipuler une base de données via une faille dans une application web. En exploitant cette vulnérabilité, ils peuvent exécuter des requêtes non autorisées pour extraire, modifier ou supprimer des données.

---

6. Dépassement de tampon (Buffer Overflow)

Le dépassement de tampon survient lorsque trop de données sont envoyées dans une zone de mémoire tampon, entraînant un dysfonctionnement du programme. Cette faille peut être exploitée pour exécuter du code malveillant.

---

7. Insecam.org

Ce site malveillant permet de regarder en direct les vidéos de caméras de surveillance mal sécurisées à travers le monde. Cela montre à quel point il est important de sécuriser correctement les dispositifs connectés.

(Le phishing (ou hameçonnage en français) est une technique de cyberattaque qui vise à tromper une personne pour qu'elle divulgue des informations sensibles, comme des mots de passe, des numéros de carte bancaire ou des données personnelles. Cela se fait généralement par l'envoi de courriels ou de messages qui imitent des communications légitimes (banques,

réseaux sociaux, services en ligne), incitant la victime à cliquer sur un lien frauduleux ou à fournir des informations sur un faux site web. L'objectif est de voler ces informations pour ensuite les utiliser à des fins malveillantes.)

Éléments clés à retenir

- 1987 : Première apparition d'un virus informatique capable de détruire des données.
- 2000 : Le virus "I love You" infecte 10 % des ordinateurs dans le monde.
- 2017 : Invention du premier ransomware de grande ampleur, WannaCry, qui affecte des milliers de systèmes à travers le monde.

À retenir :

- 1987 : Lehigh première destruction de données (virus)

Le virus Lehigh est l'un des premiers exemples de virus informatique. Découvert en 1987 à l'Université Lehigh en Pennsylvanie, ce virus ciblait spécifiquement les disquettes DOS. Lehigh infectait les fichiers exécutables COMMAND.COM, utilisés par DOS pour gérer les commandes. Une fois infecté, le virus se répliquait chaque fois que la disquette était insérée. Après un certain nombre d'infections (quatre précisément), Lehigh commençait à détruire des fichiers en mémoire, marquant ainsi l'un des premiers cas de destruction de données par un virus. Ce virus n'a pas eu une propagation massive, mais il a alerté la communauté sur les dangers que les virus pouvaient poser aux systèmes.

- 2000 : I love you, premier ver massif (10% de machine contaminée)

Le ver ILOVEYOU, également connu sous le nom de Love Bug, est apparu en mai 2000 et a eu un impact mondial. Il se propageait principalement par e-mail, avec un objet trompeur indiquant "ILOVEYOU" et un fichier joint nommé "LOVE-LETTER-FOR-YOU.txt.vbs". Ce fichier était en réalité un script malveillant écrit en VBScript. Lorsque l'utilisateur ouvrait le fichier, le ver se copiait dans le système et se répliquait en envoyant des copies de lui-même à tous les contacts de l'utilisateur. En quelques heures, il a infecté environ 10 % des ordinateurs dans le monde (environ 45 millions de machines). Il causait des pertes de données importantes en remplaçant des fichiers sensibles comme des images ou des documents. Les dégâts économiques étaient estimés à plus de 10 milliards de dollars.

- 2017 : WannaCry, premier ransomware massif

En mai 2017, le ransomware WannaCry a ravagé des centaines de milliers d'ordinateurs dans le monde entier. Ce malware exploite une vulnérabilité dans les versions non mises à jour de Microsoft Windows (connue sous le nom d'EternalBlue, une faille découverte par la NSA et divulguée par un groupe de hackers). WannaCry chiffrait les fichiers des utilisateurs et exigeait une rançon en bitcoin pour les déverrouiller. Il a paralysé des infrastructures critiques, y

compris des hôpitaux au Royaume-Uni, des réseaux de télécommunication et des entreprises. Plus de 230 000 machines dans 150 pays ont été touchées en quelques jours. WannaCry a mis en évidence l'importance des mises à jour de sécurité et de la protection des systèmes contre les cyberattaques de grande ampleur.

Botnets

Un botnet est un réseau de machines compromises (ou "bots") qui peuvent être contrôlées à distance par un attaquant. Voici quelques utilisations courantes des botnets :

- Envoyer du spam : Utilisation des bots pour envoyer des courriels indésirables à grande échelle.
- Vol d'informations sensibles : Les botnets peuvent intégrer des keyloggers pour espionner et voler des informations sensibles, telles que des mots de passe ou des données bancaires.
- Installer des spywares : Les machines infectées peuvent être utilisées pour installer des logiciels espions sans que l'utilisateur ne s'en rende compte.
- Paralyser un réseau (DDoS) : Les botnets peuvent effectuer des attaques par déni de service distribué (DDoS), qui consistent à submerger un réseau ou un site web de trafic, rendant le service inaccessible.
- Installer des sites web malveillants : Les botnets peuvent être utilisés pour héberger des sites de phishing, trompant ainsi les utilisateurs pour leur voler des informations.
- Truquer des statistiques : Ils peuvent également être utilisés pour fausser des sondages en ligne ou augmenter artificiellement le nombre de clics sur des bannières publicitaires, ce qui peut générer des revenus frauduleux.

Analyse de cas

Empêcher l’entreprise de fonctionner
Cela peut se faire via des attaques par déni de service (DDoS), rendant les systèmes ou réseaux inaccessibles, ou en utilisant des ransomwares pour bloquer l'accès aux données essentielles de l'entreprise.

Diffuser des informations confidentielles
Une attaque visant à voler et publier des informations sensibles de l'entreprise peut se faire par phishing, par l'exploitation de failles de sécurité ou via des fuites internes. Cela peut gravement nuire à la réputation de l'entreprise.

Fraudes financières
Cela inclut des attaques visant à modifier des transactions financières, détourner des fonds, ou encore voler des informations bancaires par l'intermédiaire de malwares ou de techniques d'ingénierie sociale comme le Business Email Compromise (BEC).

Les trois en même temps
Une attaque de grande envergure, comme celle orchestrée par des groupes bien organisés, peut simultanément paralyser l'entreprise (DDoS, ransomware), diffuser des informations sensibles et détourner des fonds pour maximiser les dommages.

Vengeance concurrentielle

Une entreprise concurrente peut organiser ou encourager des cyberattaques pour nuire à la réputation ou aux capacités opérationnelles d'un rival, en ciblant ses systèmes ou en volant des informations clés pour l'exploiter à des fins concurrentielles.

Opportunisme

Un attaquant peut exploiter une vulnérabilité découverte par hasard, comme dans le cas des grey hats, pour accéder à des systèmes et en tirer profit, que ce soit pour des gains financiers ou simplement pour tester ses compétences.

Spéculation économique

Des cyberattaques peuvent être utilisées pour manipuler les marchés financiers, en affectant directement les entreprises cotées en bourse (par exemple, en rendant publiques des informations sensibles) pour créer une fluctuation des prix des actions.

Casse interne

Un employé mécontent ou un ancien employé pourrait délibérément nuire à l'entreprise en volant des informations, sabotant des systèmes ou révélant des données confidentielles à des tiers, causant ainsi des pertes importantes.

Mise en place de correctifs

- Gestion des sauvegardes
- NAS, Cloud
- Correctif d’investissement, (externaliser via le Cloud peut être une solution mais peut également être contre productif) Il faut quand même faire attention avec le cloud étant donné que l’on partage des données sur internet.
- NAS* Network Attached Storage (Stockage attaché au réseau) edf: Le NAS, ou Network Attached Storage, est un dispositif de stockage connecté à un réseau qui permet de stocker et de partager des fichiers de manière centralisée. Il fonctionne comme un serveur de fichiers, offrant un accès permanent aux données pour les utilisateurs et facilitant la collaboration au sein d'un réseau. Le NAS utilise souvent la technologie RAID pour assurer la redondance et la sécurité des données en cas de défaillance d'un disque. Il peut remplacer facilement un windows serveur, à la maison il peux etre considerer un peut

comme un Cloud à la maison (généralement pour les particulier ce sont les blanc de la marque Synology, certain fonctionne avec 1GB de RAM)
-Pour en faire un à moindre coût avec un second ordinateur, un système d'exploitation qui va avoir l'orientation de proposer une solution de stockage (TrueNAS, OpenMediaVault)

- Bug bounty/HoneyPot

Le principe est d'inciter les entreprises à faire tomber les pirates du bon côté, le but est de faciliter le fait de passer "du bon côté" la société en France s'appelle "Yes We Hack" elle récompense les informaticiens trouvant des failles.
Le HoneyPot c'est un peu comme un piège, le pirate tombe dedans et nous arrivons à le repérer. L'exemple du pot de miel, qui l'a touché ? Celui dont la main est pleine de miel. Une fois repéré, ils bloquent l'adresse IP du pirate.

- Suivi CMS
- Pentest interne ou externe, continu ou non

Cela veut dire, pour éprouver sa défense, il faut attaquer. Le Pentest peut être interne (qui peut tester mewo, c'est mewo) But du jeu, voir les fails, les anomalies et pouvoir les corriger. Elle peut être aussi de l'extérieur, un contrat avec tel entreprise pour se faire attaquer et voir les failles.
L'interne va être plus discret, l'idée est d'organiser ça comme on veut tout en gardant la confidentialité et former les équipes mais il peut y avoir des problèmes, il y a du mal a faire des critiques sur ce que nous connaissons, le deuxième gros problème c'est que nous ne pouvons plus nous concentrer sur nos sujets courent.

L'externe, les points forts sont que l'entreprise est spécialisée dans ce sujet et donc arrive avec tous le matériel nécessaire, et nous accompagne dans la chose. Les points faibles c'est qu'on laisse un intru rentrer chez soi et cela peut être très coûteux.

Et donc ce Pentest, qu'il soit interne ou externe est continue, la personne est en permanence sur le sujet, c'est son boulot à plein temps.

- Kali (kalilinux)(parrot-os)

C'est une distribution Linux mais qui nativement par défaut va inclure des milliers d'outils. Kali Linux est une distribution Linux basée sur Debian, conçue pour les tests de pénétration et l'audit de sécurité. Elle est open-source et préinstallée avec de nombreux outils de sécurité, tels que Nmap et Metasploit. Kali Linux peut être exécuté en mode live depuis un CD/USB ou installé sur un disque dur pour une utilisation permanente.

- Proxy/ReverseProxy

A chaque fois qu'une demande est envoyée, le contenu est analysé et filtré, s'il répond aux exigences de l'entreprise ça passe sinon c'est bloqué. C'est du réseau

- OpenPGP (sécurisation des emails)

Les mails transitent en clair sur internet et ne sont donc pas sécurisés. OpenPGP permet de chiffrer nos e-mails. C'est ce principe là qui garantit la confidentialité de nos données et il est utilisé pour Telegram par exemple.

- Let's Encrypt

Quand on utilise internet ou utilise le port Http, il n'est pas sécurisé et pas chiffré donc on a créé le Https*. Il y a un certain temps il fallait payer ces certificats (et ca couter très cher) Ainsi un mot d'ordre a était créer Let's Encrypt, il a proposé une solution de chiffrement libre et gratuit

- Chiffrement forcé

Les chiffrements ça se casse, renforcer son chiffrement permet de gagner le bras de fer avec les pirates.

VEILLE TECHNOLOGIQUE

- https://www.root-me.org/
- NDH / LeHack

Le hack est le grand événement à Paris, tous les pro de la cybersécurité y sont. Il y en a d'autres un peu partout aussi (FIC à Lille) Il peut y avoir aussi des conférences un peu partout, à voir aussi sur LinkedIn.

- CWE/CERT/CVE/CVSS

CWE (Common Weakness Enumeration) : c'est le fait d'avoir des organismes qui vont toute la journée surveiller et identifier les failles.

CERT : C'est le centre européen de réponse Cyber, sur leur site on peut voir toutes les attaques et les patch en temps réel. Un CERT (Computer Emergency Response Team) est une équipe spécialisée en cybersécurité qui gère les incidents de sécurité informatique. Les CERT ont pour rôle de prévenir, détecter et répondre aux cyberattaques, en centralisant les demandes d'assistance et en coordonnant les réponses. En France, le CERT-FR, géré par l'ANSSI, est le principal acteur national pour la défense des systèmes d'information.

CVE : C'est une vulnérabilité identifiée et classée. Les CVE (Common Vulnerabilities and Exposures) sont des identifiants attribués à des vulnérabilités de cybersécurité publiquement

divulguées. Elles sont gérées par des Autorités de Numérotation CVE (CNA) qui examinent, documentent et publient des informations sur ces vulnérabilités. Les CVE permettent aux utilisateurs d'accéder à des données critiques sur les failles de sécurité, facilitant ainsi la gestion des risques informatiques.

CVSS : Le Common Vulnerability Scoring System (CVSS) est un standard ouvert pour évaluer la gravité des vulnérabilités de sécurité, avec des scores allant de 0 à 10.

- WebGoat (TP à tester !)

OWASP : organisme mondial de la cyber pour s'entraîner. Il ne faut pas utiliser sur son PC avec internet d’ouvert

- Zerodisclo.com

C’est un site anonyme ou nous pouvons signaler des vulnérabilités, on peux faire un signalement sécurisé dans risqué d’aller en prison ou d’avoir des problèmes.

Méthodologie

La sécurité repose sur de la logique, des attitudes et de réflexions.

https://castor-informatique.fr/

(code d'accès : 3wafdthb) score 310 (bfqdrayr)

**