



Identifier : les fragilités de l'entreprise

Eric DUPUIS^{1,2*}

⊕ Résumé

Ce document présente la dynamique du travail sur les fragilités de l'entreprise, de la maîtrise des vulnérabilités à la surveillance des menaces de l'environnement

Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse compilé en un document unique.

Ce document ne constitue pas à lui seul le référentiel du cours. Ce sont des notes de synthèse mises à disposition comme support pédagogique.

⊕ Mots clefs

Veille, vulnérabilités, menaces, identification

¹ Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France

² RSSI Orange Cyberdefense

*email : eric.dupuis@cnam.fr – eric.dupuis@orange.com

— Introduction sur les vulnérabilités, chapitre 3.1 —

La notion de fragilités de l'entreprise est à prendre au sens large. Elle comprends les vulnérabilités, humaines, organisationnelle et technique mais aussi la sensibilité à des scénarios d'attaques. C'est en effet la susceptibilité d'une organisation à subir des défaillances dans le temps,

0.1 Détecter les fragilités de l'entreprise

La première tâche de fond pour une équipe cybersécurité est d'identifier de fragilités de l'ensemble de l'environnement numérique¹ de l'entreprise. Elle s'inscrit dans la dynamique de l'**anticipation** avec la recherche de fragilités ou de risques cyber dans l'entreprise et leur correction. Elle précède généralement la **détection** d'évènement à risque, d'attaques, de déviance dans l'environnement mais aussi à l'extérieur du périmètre de l'entreprise. Elle se positionne comme une activité qui peut déclencher des mécanismes de la **réaction** aux incidents, de la

1. systèmes d'information de l'entreprise, services dans les cloud, réseaux sociaux...



gestion de crise, par la nécessaire remédiation en cas de vulnérabilité critique.

On peut distinguer deux grandes typologies d'actions pour identifier ces fragilités :

- ▶ l'audit de sécurité, qui permet de détecter des fragilités exploitables. Ce type d'audit peut se dérouler sous la forme de scénario exécuter par des équipes de "tests d'intrusion" soit sous la forme de campagne exécuter avec des scanners de vulnérabilités.
- ▶ la veille en vulnérabilités associée à la cartographie de l'environnement technique qui permet de déclencher une alerte de sécurité si une vulnérabilité apparaissait sur un des produits, services ou logiciel surveillé.

La difficulté principale de ces activités est de bien définir les périmètres techniques et de responsabilités sur lesquelles elles portent.

L'audit de sécurité permet d'évaluer les fragilités des éléments (composants) de l'entreprise en ce mettant dans la peau de l'attaquant, afin de découvrir les scénarios potentiellement actifs sur l'environnement digital de l'entreprise.

0.2 Anticiper et surveiller les menaces

Comme nous l'avons vu, une grande partie des attaques sur l'entreprise est liée à l'exploitation de fragilités de celle-ci.

L'exploitation de ces fragilités, sont de deux grandes natures.

- ▶ attaques exploitant de manière **opportuniste** des fragilités cataloguées et sans ciblage particulier de l'attaqué ;
- ▶ attaques **ciblées** exploitant de manière spécifique des fragilités connues mais pas corrigées ou des fragilités non encore connus par les défenseurs.

On trouvera dans le chapitre 3, une description plus précise de ces notions de vulnérabilités connues et non connues. Les menaces sont généralement des scénarios, des codes malveillants, des mécanismes d'agression ... Le principe de gestion de la menace relève de la même dynamique de gestion que celle liée aux vulnérabilités.

1. Les bases sur les vulnérabilités

1.1 Fragilités HOT

Quand nous parlons de vulnérabilités, nous parlons globalement des fragilités dans l'environnement du numérique de l'entreprise. Nous pouvons distinguer trois grands classes de fragilités :

- ▶ Fragilités techniques, généralement dénommé vulnérabilités au sens où ces fragilités rendent vulnérable tout ou partie d'un système. Pour rechercher



ces vulnérabilités, on utilisera des techniques d'audit, de scan , de fuzzing ... Ce sont ces vulnérabilités informatiques et réseaux que nous présenterons en détail.

- ▶ Fragilités humaines, généralement des déviations comportementales, détournement d'usage légitime, sensibilité à l'ingénierie sociale, vulnérabilités sociales ou physiologiques que l'attaquant peut utiliser. Ces fragilités sont détectables avec des audits (exemple tests mail phishing). Elles sont réduites par des mécanismes de formations et de sensibilisation, ainsi que dans certains cas des processus d'habilitation
- ▶ Fragilités organisationnelles : Un attaquant peut utiliser des déficiences organisationnelles pour obtenir des éléments pour conduire son attaque (exemple : pas de processus de vérification d'identité lors de demande sensible par téléphone).

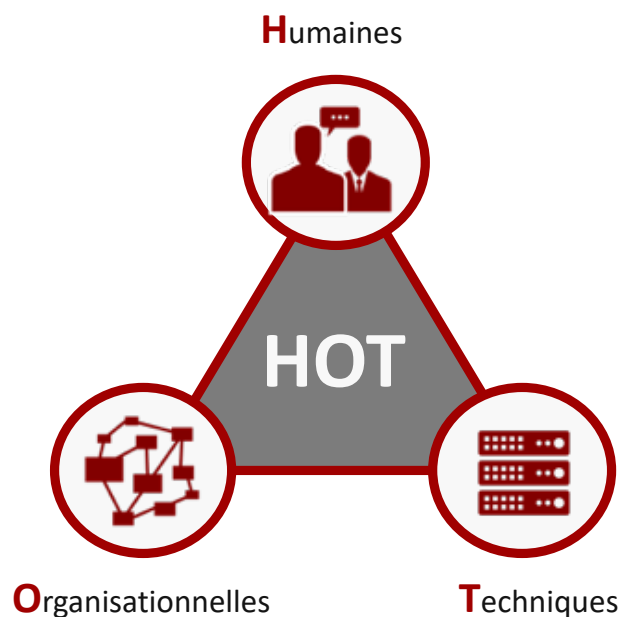


FIGURE 1. les types de vulnérabilités

Un attaquant utilisera bien entendu l'ensemble de ces fragilités pour conduire sa mission.

Dans le domaine technique de cette sécurité numérique, une vulnérabilité ou faille est une faiblesse dans un système, permettant à un attaquant de porter atteinte à la fonction de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, le dé-

ploiement, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système.

Il ya trois grandes classes de faiblesses ou vulnérabilités numériques :

- ▶ **Faillles de configuration** ou de défaut d'usage (utilisation d'un système en dehors de ses zones de fonctionnement stable et maîtrisé)
- ▶ **Faillles Logicielles** : Faillles de développement, de programmation qui conduisent généralement de l'exploitation de bugs logiciels. Il faut distinguer les logiciels développés de manière dédiée, et les logiciels dits sur étagère. Les dysfonctionnements des logiciels sur étagère (éditeurs logiciels) sont en général corrigés à mesure de leurs découvertes, mais il y a un délai entre le moment de la découverte et la correction.
- ▶ **Faillles de conception** : Faillles issus de défaut de conception. Ces faillles sont souvent liées à des faillles protocolaires issues de faille de conception d'un protocole de communications, ou de format de données.

Nous pouvons décomposer les faillles dites logicielles, en deux groupes

- ▶ Les faillles des logiciels ou codes sur mesures, développé dans l'entreprise ou par un tiers mais non édité en tant que logiciel indépendant. Nous pouvons y inclure tous les codes logiciels développés en interne.
- ▶ Les faillles logicielles de produits ou codes connus, reconnus souvent dénommées progiciels (produits logiciels). On peut aussi y distinguer deux sous classes les logiciels où les sources sont accessibles, et les codes dits fermés ou l'utilisateur ne dispose que du code binaire exécutable. Nous verrons que les démarches de recherche de faillles dans ces deux types de code sont un peu différentes.

Quand on parle de fragilités, il n'y pas que les faillles de conception ou de développement, mais aussi des faillles de configuration des systèmes d'information.

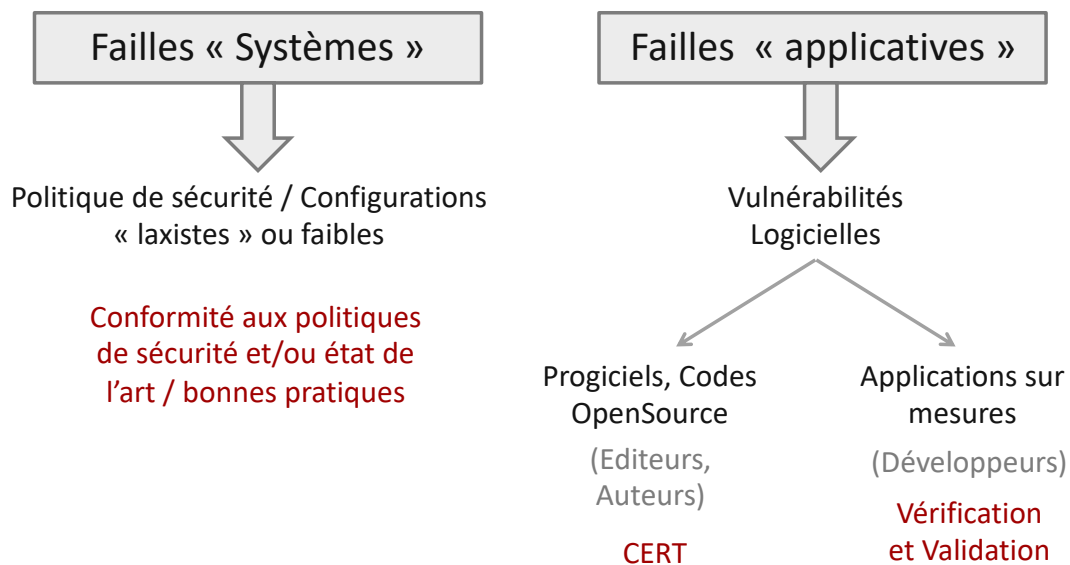
La recherche et découverte de ces vulnérabilités utilisent des outillages un peu différent. On distingue donc :

- ▶ les faillles systèmes
- ▶ les faillles applicatives

1.2 Exemples de vulnérabilités

A titre d'exemple et d'illustration je vous propose d'examiner rapidement des vulnérabilités techniques : deux faillles de conception et une de programmation. Nous ne rentrerons pas dans les détails des vulnérabilités. Ce chapitre a pour objectif de présenter concrètement ce qu'est une vulnérabilité, sur la base d'exemples simples.



**FIGURE 2.** Les types de vulnérabilités

La majorité des failles informatiques du domaine du Web et des applications sur mesures est due à une utilisation non prévue de l'applicatif. Un utilisateur peut envoyer une information plus longue que prévue (buffer overflow), ou une valeur non gérée (négative, quand le logiciel attend une valeur positive), ou quand il ajoute des symboles non attendus (des guillemets, caractères spéciaux alors qu'il était prévu seulement des lettres), si les vérifications des données ne sont pas faites correctes, alors le logiciel, programme ou l'application peut être détournée.

1.2.1 Faille type XSS

Si nous prenons par exemple, un code qui affiche une image avec un titre, que ce titre d'image soit saisi par un utilisateur et qu'aucun contrôle ne soit fait. Dans l'application, l'affichage se fait par un code PHP du style :

```
<?php ...
    $image = readimage(). "png";
    $title = readtitle();
    ...
    print '';
...?>
```

et permet de générer le code HTML suivant :



```
<html>...
    
...</html>
```

Un utilisateur malveillant pourrait avoir saisi autre chose qu'un simple titre, et faire en sorte que la variable **\$title** puisse contenir une chaîne de caractère un peu particulière. Le pirate aura entré, par exemple, comme titre de sa photo sur ce site un peu faible, une chaîne comme :

« un titre de mon image/"><script>...scriptmalveillant...;</script> »

```
<html>...
    <script>...scriptmalveillant...;</script>"
    ...
</html>
```

L'exécution du script javascript malveillant se fera à la lecture de cette page générée. Si cette donnée est stockée sur un serveur, l'action sera effective pour toutes les personnes qui consulteront l'image avec son titre piégé par un script malveillant.

1.2.2 Faille type SQL Injection

Nous allons rapidement explorer un grand classique des vulnérabilités sur les applications de sites Web sur Internet : l'injection SQL. Le principe est d'injecter dans une requête SQL (langage d'interrogation de base de données), utilisée dans une application PHP par exemple. Supposons que dans l'application, la requête suivante soit utilisée :

```
SELECT fieldlist
FROM table
WHERE field = ' $EMAIL ';
```

Supposons que la saisie de l'utilisateur, saisisse un email avec une chaîne un peu modifiée (ajout d'un simple « ' » en plus) :

```
SELECT fieldlist
FROM table
WHERE field = ' contact@test.com' ';
```

L'exécution de cette requête va générer une erreur, et en fonction de la gestion des erreurs du code PHP, l'utilisateur pourra apercevoir que cette requête a



provoqué une erreur d'exécution. Ceci permet à l'utilisateur de rapidement déterminer que le code est sensible à une attaque par injection SQL. Il peut alors à loisir trouver la meilleure manière de l'exploiter, en entrant un email forgé avec une chaîne plus malicieuse.

La chaîne « `OU 'x' = 'x'` » étant toujours VRAI, on pourrait obtenir des informations complètes de certaines tables. Bien entendu, l'usage de vulnérabilité SQL injection n'est généralement pas trivial, mais avec un peu d'habitude, il est possible de construire des attaques sophistiquées sur des codes vulnérables.

```
SELECT fieldlist
FROM table
WHERE field = 'somebody' OU 'x' = 'x' ;
```

1.2.3 vulnérabilités WEB

Vous trouverez sur le site Open Web Application Security Project [🔗](https://www.owasp.org)², le top TEN des vulnérabilités découvertes sur les sites WEB et pour ceux qui souhaitent creuser un peu plus, il existe de nombreux sites présentant en détail des vulnérabilités et des manières de les exploiter (à des fins pédagogiques!). Par exemple, le site de Pixis (Hackndo) [🔗](https://beta.hackndo.com)³ vous donnent quelques partages particuliers d'un Ethical hacker.

1.3 Faille de programmation

On peut trouver des vulnérabilités dans des produits et services très connus, et déployés depuis très longtemps.

Parmi les vulnérabilités les plus célèbres, la classe de vulnérabilités du protocole SMB en version 1, est celle qui continue encore à faire des victimes. Le protocole SMB (Server Message Block) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows. Sa version 1 du protocole SMB, vulnérable à la faille EternalBlue.

Dans la base de données du système CVE on retrouve l'identifiant de cette vulnérabilité : **CVE-2017-0144**.

1.4 vulnérabilités et exploits

Il arrive que la procédure d'exploitation d'une faille d'un logiciel soit documentée et utilisable soit sous la forme d'un code logiciel et/ou de procédure des-

2. <https://www.owasp.org>

3. <https://beta.hackndo.com>



Windows : une faille 0-day révélée dans SMB, le correctif ...

<https://www.nextinpact.com/news/103173-windows-faille-0-day-revele...> ▼

6 févr. 2017 - Une faille 0-day existe dans Windows, plus spécialement dans la manière dont le système gère le trafic **SMB**. Un prototype d'exploitation est déjà en circulation, ... **Analyses** de la rédaction. ...

Faille critique dans le protocole SMB de Windows ...

cybersecurite.over-blog.com/article-faille-critique-dans-le-protocole-smb... ▼

17 févr. 2011 - La société de sécurité Vupen émet une alerte jugée comme "critique" sur une vulnérabilité concernant le système d'exploitation Windows pour ...

MS17-010 - Security Update for Microsoft Windows SMB ...

<https://www.sophos.com/threat-analyses/vulnerabilities/VET-001035> ▼

14 mars 2017 - MS17-010 - Security Update for Microsoft Windows **SMB** Server. Pour plus ... de test des SophosLabs. **Faillles** connues, Aucune **faille** connue.

Analyse des attaques des ransomware Wannacry et Jaff ...

<https://www.vadesecure.com/analyse-attaques-ransomware-wannacry-jaff>

15 mai 2017 - Ce ransomware se propage au travers d'une **faille** du protocole de partage **SMB** v1 (Server Message Block) non patchée au moment de ...

FIGURE 3. Tempo faille SMB - google

criptive détaillée appelée « exploit ». Ces exploits ne sont pas systématiquement publiés.

1.5 vulnérabilités et divulgation

La divulgation publique des vulnérabilités est soumise un modèle de divulgation de vulnérabilité dans lequel une vulnérabilité ou un problème est révélé uniquement après une période permettant à la vulnérabilité ou au problème d'être corrigée ou corrigée. Cette période distingue le modèle de la divulgation complète.

Tout fournisseur de logiciels de sécurité, de services et de recherches de vulnérabilité, se doit de prendre des précautions vis à vis de vulnérabilités découvertes, en particulier les délais de publication. On parle généralement de *Vulnerability Disclosure Policy*.

En effet , développeurs de matériel et de logiciels ont souvent besoin de temps et de ressources pour corriger ces vulnérabilités.


Dans certains cas, lorsque la découverte n'a pas été faite via une recherche commanditée (Audit, Pentest, BugBounty), la communauté sécurité et les scientifiques estiment qu'il est de leur responsabilité sociale de sensibiliser le public aux vulnérabilités ayant un impact important en les publiant. Cacher ces problèmes pourrait créer un faux sentiment de sécurité. Pour éviter cela, les parties impliquées unissent leurs forces et s'accordent sur un délai pour réparer la vul-



néralité et prévenir tout dommage futur. En fonction de l'impact potentiel de la vulnérabilité, du temps requis pour qu'un correctif d'urgence ou une solution de contournement soit développé et appliqué, ainsi que d'autres facteurs, cette période peut varier de quelques jours à plusieurs mois.

Par ailleurs, la confidentialité des découvertes est généralement requise lors des audits. Le commanditaire et l'expert signent un accord dénommé *Vulnerability Non Disclosure Agreement*, qui permet de s'assurer que la publication des vulnérabilités restera à la main du commanditaire.

Dans un mode public avec mode de divulgation de vulnérabilités ouverts les experts en sécurité s'attendent à être indemnisés financièrement, mais avec le risque que signaler ces vulnérabilités au fournisseur avec l'exigence d'une indemnisation soit considéré comme une extorsion.

Un marché des vulnérabilités s'est développé Zerodium ⁴ (Voir fig. 4 page 10), mais la commercialisation des vulnérabilités reste un sujet très controversé lié au concept de divulgation des vulnérabilités. C'est normalement dans le rôle de CERT d'assurer cette coordination des divulgations.

2. CVE, CVSS et CWE

2.1 Common Vulnerabilities and Exposure (CVE)

De nombreuses vulnérabilités sont découvertes chaque année dans des produits et logiciels. Les informations techniques sur ces vulnérabilités permet de les détecter, et de les caractériser. Il était important dans le monde des technologies de l'information qu'elles puissent être identifiées et décrites de manière unique, accessibles à tous.

L'objectif fondamental de la création du CVE est de constituer un dictionnaire qui recense toutes les failles avec une description succincte de la vulnérabilité, ainsi qu'un ensemble de liens que les utilisateurs peuvent consulter pour plus d'informations. Cette base est proposée pour consultation et reste maintenue par le Mitre Corporation. Cet organisme à but non lucratif américaine a pour l'objectif est de travailler dans des domaines technologique comme l'ingénierie des systèmes, les technologies de l'information, la sécurité.

Common Vulnerabilities and Exposures ou CVE est une base de données (Dictionnaire) des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN

Pour consulter les CVE, il suffit de se rendre sur [CVE.mitre.org](https://cve.mitre.org) ⁵

4. <https://zerodium.com>

5. <https://www.cve.mitre.org>



Changelog / Sep 3rd, 2019

Sep. 3, 2019 - Payouts for major mobile exploits have been modified. Changes are highlighted below:

Category	Changes
New Payouts (Mobiles)	\$2,500,000 - Android full chain (Zero-Click) with persistence (New Entry) \$500,000 - Apple iOS persistence exploits or techniques (New Entry)
Increased Payouts (Mobiles)	\$1,500,000 - WhatsApp RCE + LPE (Zero-Click) <u>without</u> persistence (previously: \$1,000,000) \$1,500,000 - iMessage RCE + LPE (Zero-Click) <u>without</u> persistence (previously: \$1,000,000)
Decreased Payouts (Mobiles)	\$1,000,000 - Apple iOS full chain (1-Click) with persistence (previously: \$1,500,000) \$500,000 - iMessage RCE + LPE (1-Click) <u>without</u> persistence (previously: \$1,000,000)
Desktops/Servers	No modifications.

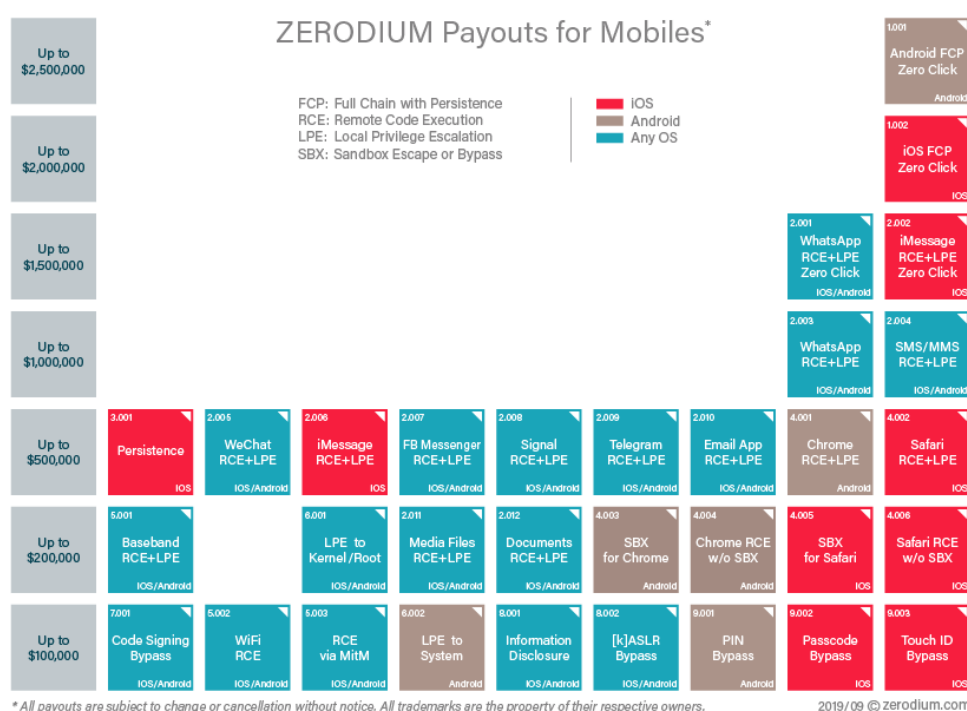


FIGURE 4. Le marché des failles mobiles avec Zerodium

2.2 Common Vulnerability Scoring System (CVSS)

Bien entendu, disposer d'un identifiant d'une vulnérabilité est important, mais un gestionnaire de sécurité dans l'entreprise, doit aussi disposer d'éléments pour juger de la gravité de cette vulnérabilité.

Le *Common Vulnerability Scoring System (CVSS)* à sa version 3 issu des travaux du FIRST, Forum of Incident Response and Security Teams ⁶, est un cadre mé-

6. <https://www.first.org/cvss/>



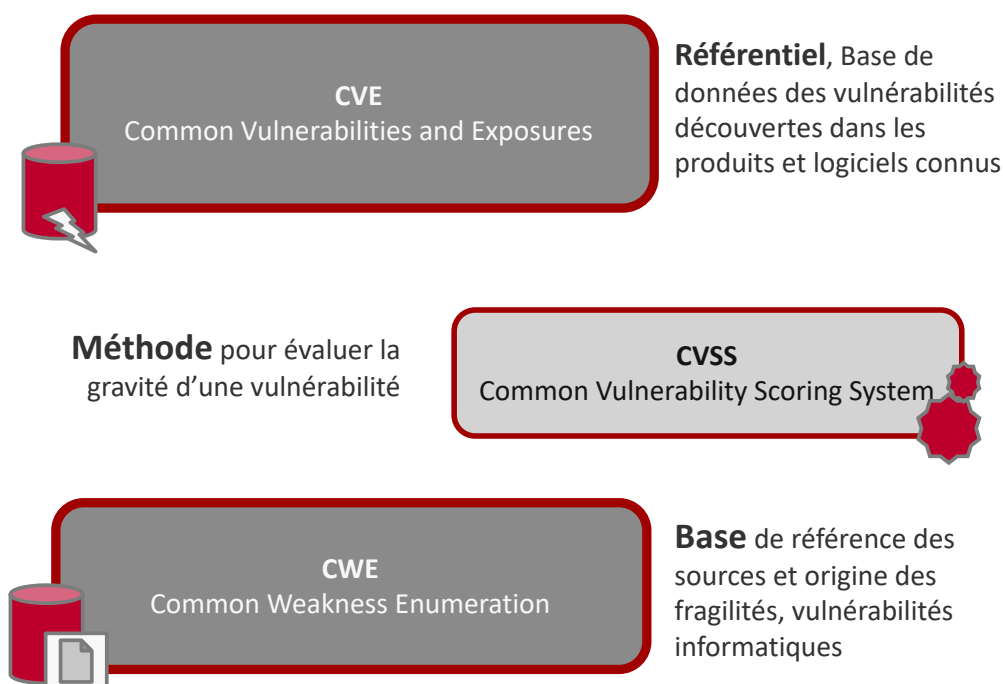


FIGURE 5. Quelques concepts de gestion sur les vulnérabilités

thodologique permettant d'évaluer en particulier la criticité d'une vulnérabilité.

C'est un système permettant de calculer une note évaluant la criticité d'une vulnérabilité, et de construire une chaîne de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité, et les critères utilisés pour ce calcul.

Les notes et vecteurs CVSS sont toujours le résultat de trois groupes de critères d'évaluation (« Base », « Temporel » et « Environnemental ») ayant chacun leur note ainsi que leur vecteur :

- ▶ Le groupe des critères de « **Base** » évalue l'impact maximum théorique de la vulnérabilité.
- ▶ Le groupe des critères « **Temporel** » pondère le groupe « Basic » en prenant en compte l'évolution dans le temps de la menace liée à la vulnérabilité (par exemple, l'existence d'un programme d'exploitation ou d'un correctif).
- ▶ Le groupe des critères « **Environnemental** » pondère le groupe « Temporel » en prenant en compte les caractéristiques de la vulnérabilité pour un Système d'Information donné.


La richesse du modèle apporte une complexité dans sa lecture rapide, toutefois globalement, on peut lire un score CVSS en terme de criticité avec la grille de lecture suivante :

- ▶ Un score de 0 à 3.9 correspond à une criticité basse



- ▶ Un score de 4 à 6.9 correspond à une criticité moyenne
- ▶ Un score de 7 à 10 correspond à une criticité haute

2.3 Common Weakness Enumeration (CWE)

L'Énumération des faiblesses ordinaires c'est ainsi qu'il faudrait traduire CWE publié par le MITRE ⁷ qui listent par ailleurs, le top 25 des erreurs de programmation dangereuses et fréquentes. En effet, les développeurs font souvent les mêmes erreurs. La plupart des vulnérabilités applicatives viennent d'une poignée d'erreurs bien connues, qui reviennent régulièrement et pour lesquelles les adapter n'ont qu'à adapter des attaques existantes. C'est le but de la CWE (Common weakness Enumeration) que de recenser les erreurs de programmation commises. On y retrouve des grands classiques, comme la validation des champs d'un formulaire, la célèbre injection SQL, les problèmes de gestion du système, les contrôles d'accès mal gérés, les tests réalisés par le client plutôt que par le serveur... Le but du top 25 est d'attirer l'attention des programmeurs sur leurs propres erreurs les plus courantes, mais également de faire réfléchir les formateurs : trop souvent, ces problèmes courants sont oubliés des cours de programmation et de sécurité. Après une brève présentation de chaque problème, la CWE propose des principes généraux pour l'éviter ; le tout est clarifié autant que possible et devrait être compréhensible avec un peu d'effort par la plupart des développeurs. On explorera un peu plus ces éléments dans le chapitre sur la sécurité applicative. En 2019, les 3 premières faiblesses ordinaires ont été :

1. CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer à 75.56%
2. CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') à 45.69%
3. CWE-20 Improper Input Validation à 43.61%

3. gérer ses vulnérabilités

Dans le paysage numérique de plus en plus complexe , nous sommes exposés à des terminologies variées souvent soutenues par les modes du moment. Les termes «analyse de vulnérabilités», «évaluation des vulnérabilités» et «gestion des vulnérabilités» sont souvent utilisés et restent une source de confusion pour nombre d'entre nous. Pour nous assurer de se concentrer sur les tactiques les plus efficaces pour gérer les vulnérabilités, nous donnerons les principales différences entre l'évaluation des vulnérabilités et la gestion des vulnérabilités. Mais en posant comme principe que l'important est d'agir quand sont identifiées des failles dans un système.

7. <http://cwe.mitre.org>



- ▶ La gestion des vulnérabilités (**Vulnerability Management**) est un processus continu servant à identifier, classer, corriger et réduire les vulnérabilités, en particulier dans les logiciels. La gestion des vulnérabilités fait partie intégrante des processus de gestion de la cybersécurité dans l'entreprise. Contrairement au projet d'évaluation ponctuelle des vulnérabilités, une stratégie de gestion des vulnérabilités fait référence à un processus ou programme complet et continu qui vise à gérer les vulnérabilités d'une organisation de manière globale et continue. Nous avons rassemblé quelques caractéristiques et éléments clés d'une approche standard de la gestion des vulnérabilités. La gestion des vulnérabilités comprend aussi le processus par lequel les risques associés ces vulnérabilités sont évalués. Cette évaluation conduit à corriger les vulnérabilités et éliminer le risque ou une acceptation formelle du risque par le gestion d'une organisation (par exemple, au cas où l'impact d'une attaque serait faible ou la le coût de la correction ne dépasse pas les dommages éventuels pour l'organisation).
- ▶ Il est souvent confondu avec l'évaluation des vulnérabilités (**Vulnerability Assessment**), dont l'objectif est de rechercher les fragilités d'un système ou d'une entreprise. Ces vulnérabilités connues sont recherchées sur le système. Une évaluation de vulnérabilité n'est pas une analyse, c'est un projet ponctuel avec une date de début et une date de fin définies. En règle générale, un consultant externe en sécurité de l'information examine votre environnement d'entreprise et identifie diverses vulnérabilités potentiellement exploitables auxquelles vous êtes exposé dans un rapport détaillé. Le rapport répertoriera non seulement les vulnérabilités identifiées, mais fournira également des recommandations concrètes pour la résolution. Une fois le rapport final préparé, l'évaluation de la vulnérabilité est terminée. Malgré le fait que les deux sont liés, il existe une différence importante entre les deux. La recherche de vulnérabilités consiste à utiliser par exemple un programme informatique pour identifier les vulnérabilités dans réseaux, infrastructure informatique ou applications. La gestion de la vulnérabilité est la processus entourant ce scan de vulnérabilités, prenant également en compte d'autres aspects tels que acceptation des risques, remédiation, etc. On verra en outre que le scan de vulnérabilités n'est qu'un sous partie de l'évaluation des vulnérabilité.
- ▶ L'analyse des vulnérabilités est un processus de recherche ces fragilités et des scénario qui vont permettre de les exploiter. Les tests d'intrusion sont un exemple de cette dynamique d'analyse des fragilités afin d'en définir un scénario permettant d'atteindre l'objectif que l'attaquant s'est assigné.



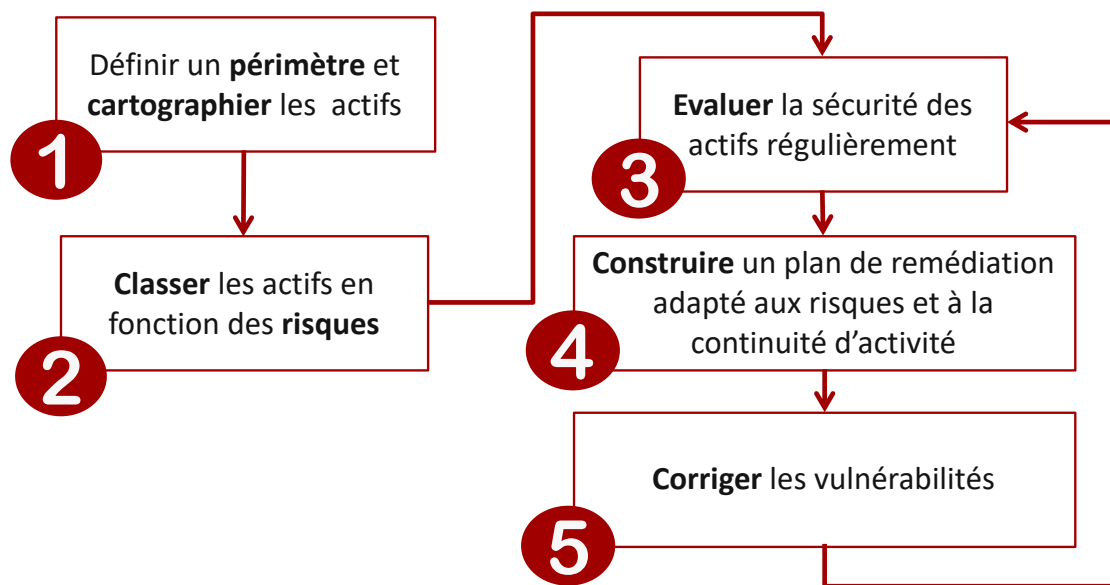


FIGURE 6. Les types de vulnérabilités

3.1 Processus de gestion des vulnérabilités

La gestion des vulnérabilités est un processus continu. Elle apparaît en toile de fond du cycle de vie du Maintien en Condition de Sécurité :

- ▶ Cartographier, cataloguer l'environnement ;
- ▶ Identifier les fragilités et les menaces ;
- ▶ Corriger, remédier, améliorer la protection et la défense ;
- ▶ Mesurer et suivre l'efficacité des mesures déployées.

3.1.1 ISO 27001

Un chapitre de la norme parle de Veille de la vulnérabilité, que nous pouvons classer dans le domaine de la gestion des vulnérabilités et donne des éléments méthodologiques :

- ▶ 1. **DÉCOUVRIR** : Catalogage de l'existant, des actifs, des ressources du système d'information.
- ▶ 2. **PRIORISER** : Classifier et attribuer des valeurs quantifiables aux ressources, les hiérarchiser.
- ▶ 3. **ÉVALUER** : Identifier les vulnérabilités ou les menaces potentielles sur chaque ressource.
- ▶ 4. **SIGNALER** : Signaler, publier les vulnérabilités découvertes.



- ▶ 5. **CORRIGER** : Éliminer les vulnérabilités les plus sérieuses des ressources les plus importantes.
- ▶ 6. **VÉRIFIER** : S'assurer que la vulnérabilité a bien été traitée.

3.2 Processus d'analyse/recherche des vulnérabilités

3.3 Processus d'évaluation des vulnérabilités

L'évaluation permet de définir l'impact d'une vulnérabilités sur les risques courus par l'entreprise.

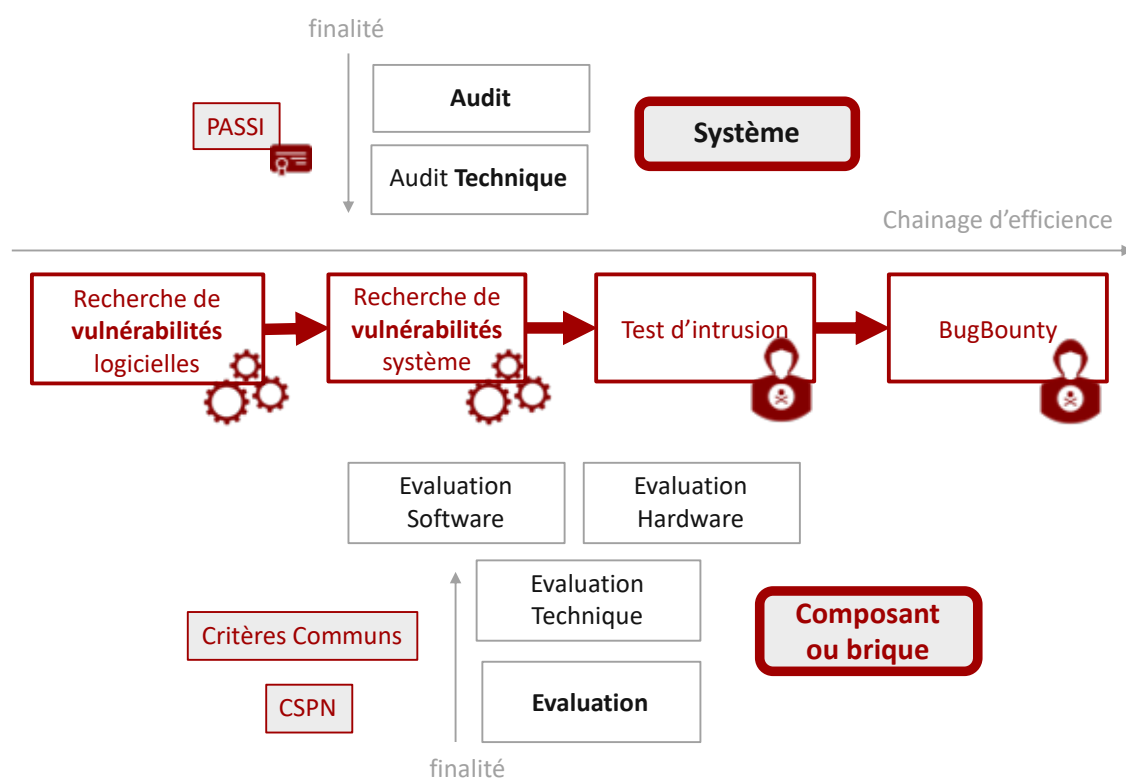


FIGURE 7. Rechercher ses vulnérabilités

3.4 Audit sécurité des vulnérabilités

1. Scan de vulnérabilités, permettant de manière automatisée à rechercher les vulnérabilités sur un système donné.
2. Audit technique et pentest

3.4.1 Scan de Vulnérabilités

Un processus nécessaire qui peut être utilisé de manière récurrente.



3.4.2 Scan de Vulnérabilités système

Les vulnérabilités peuvent être découvertes à l'aide d'un scanner de vulnérabilités, qui analyse un système informatique à la recherche de vulnérabilités connues, telles que les ports ouverts, les configurations logicielles non sécurisées et la vulnérabilité aux infections par logiciels malveillants. Des tests de fuzz peuvent permettre de détecter des vulnérabilités inconnues, telles que le jour zéro, permettant d'identifier certains types de vulnérabilités, telles qu'un débordement de mémoire tampon avec des cas de test pertinents. Une telle analyse peut être facilitée par l'automatisation des tests.

3.4.3 Scan de Vulnérabilités logicielles

La correction des vulnérabilités peut impliquer de différentes manières l'installation d'un correctif, une modification de la stratégie de sécurité du réseau, la reconfiguration du logiciel ou la formation des utilisateurs à l'ingénierie sociale.

4. les audits

4.1 Types d'audit

4.1.1 Audit Organisationnelle

4.1.2 Audit technique

4.2 Processus d'audit

4.2.1 Audit de conformité

4.2.2 Audit ponctuels et campagnes

4.2.3 Audit continu

5. La relation avec un CSIRT Interne

Une méthodologie efficace de gestion des vulnérabilités comprend une équipe d'intervention en cas d'incident de sécurité informatique (CSIRT). Le CSIRT est responsable de la publication des avis de sécurité, de la tenue d'information régulières pour échanger sur les activités malveillantes et des dernières attaques du jour zéro, de la simplification et de la diffusion des alertes de sécurité et de l'élaboration de directives compréhensibles et efficaces en matière de réaction aux incidents pour tous les salariés. De cette manière, chacun seront en mesure de réagir aux indicateurs de compromis potentiels conformément aux pratiques recommandées par l'équipe CSIRT.

6. Compléments



6.1 Périmètre sous responsabilité de l'entreprise

6.1.1 la notion de responsabilité

6.1.2 Inventaire des actifs

6.2 L'environnement digital externe

6.3 Veille et alerte sur les vulnérabilités

6.3.1 abonnement au CERT

6.3.2 Le marché de la vulnérabilité

CERT, veille en vulnérabilités Une vulnérabilité et sa cotation

6.4 La chasse aux vulnérabilités

Checking versus Pentest

Corriger une vulnérabilité au plus tot

6.5 Le marché de l'insécurité chronique

Sécurité applicative et le pire avec les DEVOPS et le WEB (Owasp co)

7. Les équipes

8. les tests d'intrusion

8.1 généralités

Le terme PENTEST est devenu tellement courant, que l'on oublie quelques fois qu'il est l'abréviation de : "Penetration Testing", qui veut littéralement dire tests d'intrusion. L'expression "test de pénétration" est parfois rencontrée, mais les professionnels du PENTEST n'apprécie par trop cette expression.

Il est toujours un peu complexe de catégoriser l'activité de pentests. Il aura assez rapidement des détracteurs pour soulever le fait que la catégorie n'est pas la bonne, qu'elle n'est pas représentative du métier. Je vais donc faire rentrer cette activités dans plusieurs catégories (métier de l'audit, métiers d'expertise, métiers du tests). Dans le cadre de ce cours, cette activité je propose de relier cette activité métier se situe comme un des outils du processus de gestion des vulnérabilités (*Vulnerability Management*). Mais il est plus courant de classer les activités de PENTESTS dans les activités d'audit.



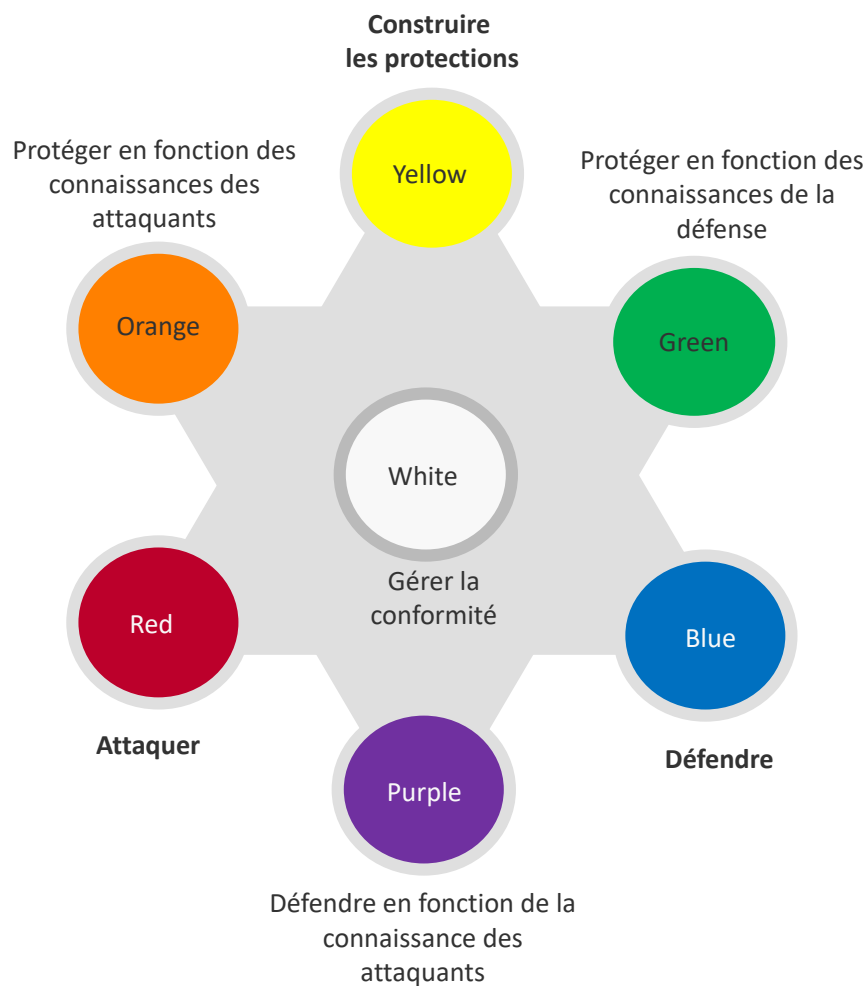


FIGURE 8. Les branches du test

8.2 le métier de Pentesteur

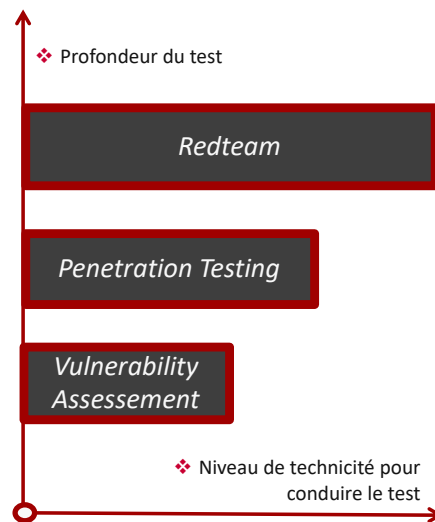
Le métier du PENTEST est lié aux métiers techniques de l'informatique et télécom. Les origines des Pentesteur sont très variées. Ce sont des métiers qu'il est possible d'exercer avec différents niveaux de formation. Etre Ethical Hacker fait partie du mythe de la cybersécurité.

8.2.1 Ethical Hackers

8.2.2 Peut-on faire confiance à des pentesteurs ?

Parmi les grandes questions que se posent les "commanditaires" de tests d'intrusion se trouve celle de la confiance. En effet, le principe des tests d'intrusion est d'ouvrir un peu les portes de ses systèmes informatique à des "intrus" qui vont certainement découvrir des fragilités. Certains, peut être plus paranoïaque que



**FIGURE 9.** Les types de tests

d'autres, peuvent se poser la question de savoir ce que vont devenir ces informations sensibles dans "les mains" de Hackers. Parmi les commanditaires on trouve bien entendu les RSSI, mais aussi les chefs de projet d'application ou de produits embarquant des technologies de informatique ou de communication (Objets intelligents, connectés).

8.3 Les sociétés de confiance

On notera que l'ANSSI, a créé il y a quelques années dans le cadre du Référentiel Général de Sécurité, un référentiel spécifique d'exigences qui permet de certifier les sociétés d'audit. Ce référentiel est dénommé PASSI pour "Prestataire d'audit de la sécurité des systèmes d'information"

Les auditeurs sont certifiés sur une (ou plusieurs) compétences. La société est certifiée sur la base des processus de conduite des audits, et sur sa capacité à protéger les données sensibles de ses clients. Elle peut être certifiée sur différents domaines d'audit.

- ▶ Audit d'architecture
- ▶ Audit de configuration
- ▶ Audit de code source
- ▶ Tests d'intrusion
- ▶ Audit organisationnel et physique
- ▶ Audit d'un système industriel



Le niveau de sécurité du système d'information et des outils permettant de réaliser les audits sont vérifiés et validés par une société de certification (LSTI, AMOS-SYS ...). A l'issue de certification, l'ANSSI prononce la qualification de la société d'audit au titre de ce PASSI. Il existe une extension pour les audits liés à la loi de programmation militaire (LPM). c'est à dire pour les audits sur les SIIV (Système d'information d'importance vitale) des Opérateur d'importance Vitale. (Voir chapitre sur la Cyberdefense)

8.3.1 Formation des Pentests

8.4 Certifications professionnelles

8.5 le cadre méthodologique

8.6 les rapport d'audits

Au coeur de l'activité "professionnelle" des pentesteurs se situe le rapport d'audit. En effet, si l'objectif est bien d'identifier des fragilités (des vulnérabilités), et les scénarios qui permettent de les exploiter à des fin concrètes et relevant d'un menace présentant un risque pour l'entreprise. il n'en demeure pas moins important de "rendre compte" de ce qui a été trouver. Ce rapport doit aussi contenir des préconisations, car il est important face à une ou des fragilité(s) de proposer des solutions.

9. Les CERTs

J'ai traité les CERTs dans le chapitre sur le svulnérabilités, toutefois l'évolution des fonctions et services des CERTs s'est rapidement élargie ces dernières années. Au delà des de la diffusion et alerte sur des vulnérabilités, ils couvrent maintenant avec précision les menaces (analyse et alerte sur codes malveillants, ...) et les incidents.

9.1 Les CERTs commerciaux



10. Contributions

10.1 Comment contribuer

Les notes et les présentations sont réalisées sous \LaTeX .

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBER-DEF101). Les contributions peuvent se faire sous deux formes :

- ▶ Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- ▶ Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBER-DEF) [↗](https://github.com/edufaction/CYBERDEF)⁸ . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.

Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

10.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

10.2.1 Années 2019

- ▶ **François REGIS** (Orange) : CyberHunting

10.2.2 Années 2018

- ▶ **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

8. <https://github.com/edufaction/CYBERDEF>



Table des matières

0.1	Détecter les fragilités de l'entreprise	1
0.2	Anticiper et surveiller les menaces	2
1	Les bases sur les vulnérabilités	2
1.1	Fragilités HOT	2
1.2	Exemples de vulnérabilités	4
	Faible type XSS • Faible type SQL Injection • vulnérabilités WEB	
1.3	Faible de programmation	7
1.4	vulnérabilités et exploits	7
1.5	vulnérabilités et divulgation	8
2	CVE, CVSS et CWE	9
2.1	Common Vulnerabilities and Exposure (CVE)	9
2.2	Common Vulnerability Scoring System (CVSS)	10
2.3	Common Weakness Enumeration (CWE)	12
3	gérer ses vulnérabilités	12
3.1	Processus de gestion des vulnérabilités	14
	ISO 27001	
3.2	Processus d'analyse/recherche des vulnérabilités	15
3.3	Processus d'évaluation des vulnérabilités	15
3.4	Audit sécurité des vulnérabilités	15
	Scan de Vulnérabilités • Scan de Vulnérabilités système • Scan de Vulnérabilités logicielles	
4	les audits	16
4.1	Types d'audit	16
	Audit Organisationnelle • Audit technique	
4.2	Processus d'audit	16
	Audit de conformité • Audit ponctuels et campagnes • Audit continu	
5	La relation avec un CSIRT Interne	16
6	Compléments	16
6.1	Périmètre sous responsabilité de l'entreprise	17
	la notion de responsabilité • Inventaire des actifs	
6.2	L'environnement digital externe	17
6.3	Veille et alerte sur les vulnérabilités	17
	abonnement au CERT • Le marché de la vulnérabilité	
6.4	La chasse aux vulnérabilités	17
6.5	Le marché de l'insécurité chronique	17
7	Les équipes	17
8	les tests d'intrusion	17
8.1	généralités	17
8.2	le métier de Pentesteur	18
	Ethical Hackers • Peut-on faire confiance à des pentesteurs ?	



TABLE DES FIGURES	23
8.3 Les sociétés de confiance	19
Formation des Pentests	
8.4 Certifications professionnelles	20
8.5 le cadre méthodologique	20
8.6 les rapport d'audits	20
9 Les CERTs	20
9.1 Les CERTs commerciaux	20
10 Contributions	21
10.1 Comment contribuer	21
10.2 Les contributeurs/auteurs du cours	21
Années 2019 • Années 2018	

Table des figures

1 les types de vulnérabilités	3
2 Les types de vulnérabilités	5
3 Tempo faille SMB - google	8
4 Le marché des failles mobiles avec Zerodium	10
5 Quelques concepts de gestion sur les vulnérabilités	11
6 Les types de vulnérabilités	14
7 Rechercher ses vulnérabilités	15
8 Les branches du test	18
9 Les types de tests	19

