



1



2



SOMMAIRE



Sécurité informatique
SOMMAIRE



Définition



Rappels légaux



Domaines de la sécurité



Les attaques



OSINT



Les outils



Comment apprendre la sécurité

Sécurité informatique
NOTIONS GÉNÉRALES

Définition



DÉFINITION



« La sécurité des systèmes d'information (SSI), ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. »

Source : https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d'information

DÉFINITION



OWASP :
<https://owasp.org/>

- **Open Web Application Security Project**
- L'OWASP est une organisation à but non lucratif qui se consacre à l'amélioration de la sécurité des logiciels.
- Elle fournit des ressources, des guides, des outils et des projets open source pour aider les développeurs, les ingénieurs en sécurité et les professionnels de la cybersécurité à identifier, à prévenir et à corriger les vulnérabilités dans les applications web.
- L'OWASP est surtout connue pour son projet « OWASP Top Ten », qui répertorie les dix principales vulnérabilités de sécurité dans les applications web, ainsi que pour de nombreux autres projets destinés à améliorer la sécurité des applications web à travers le monde.

DÉFINITION



ANSSI : l'Agence nationale de la sécurité des systèmes d'information
<https://www.ssi.gouv.fr/>

- L'ANSSI est une agence gouvernementale française créée en 2009, relevant du ministère de l'Économie, des Finances et de la Relance.
- Elle est chargée de protéger la sécurité des systèmes d'information de l'État, des administrations publiques, des entreprises d'importance vitale (comme les opérateurs d'énergie, de transport, de santé, etc.), et plus largement, de contribuer à la sécurisation de l'espace numérique en France.
- L'ANSSI accomplit sa mission en fournissant des conseils, des normes de sécurité, des audits, des formations, et en coordonnant la réponse aux incidents de sécurité informatique.
- Elle joue un rôle essentiel dans la sensibilisation et la protection contre les menaces cybernétiques et les attaques informatiques.

DÉFINITION



PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles




CNIL : Commission nationale de l'informatique et des libertés
<https://www.cnil.fr/>

- La CNIL est une autorité administrative indépendante française créée en 1978.
- Sa mission principale est de protéger les données personnelles et la vie privée des individus en veillant au respect de la législation sur la protection des données.
- La CNIL régule la collecte, le traitement, le stockage et la transmission des données personnelles en France, et elle assure également la sensibilisation du public, l'information sur les droits à la vie privée, et le contrôle du respect de la réglementation par les organisations et les entreprises.
- Elle joue un rôle essentiel dans la mise en œuvre du règlement général sur la protection des données (RGPD) au niveau national et travaille en collaboration avec d'autres autorités de protection des données en Europe.

DÉFINITION

CNIL

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles



Sécurité informatique
NOTIONS GÉNÉRALES

Budget de la CNIL par année

	2016 ¹⁰	2017 ¹¹	2018 ¹²	2019 ¹³	2020 ¹⁴	2021 ¹⁵	2022 ¹⁶
Budget alloué	16 964 049 €	17 161 536 €	16 838 254 €	18 506 734 €	20 143 890 €	21 780 782 €	23 950 763 €
Titre 2 (personnel)	13 842 841 €	14 088 832 €	14 402 426 €	15 162 970 €	16 710 552 €	18 017 267 €	20 000 658 €
Hors titre 2 (fonctionnement, investissement et intervention)	3 121 208 €	3 072 704 €	3 003 136 €	3 343 764 € (auxquels s'ajoutent 180 000 € de réallocation)	3 433 338 €	3 763 515 €	3 950 105 €


Nombre d'emplois par année

	2016 ¹⁷	2017 ¹⁸	2018 ¹⁹	2019 ²⁰	2020 ²¹	2021 ²²	2022 ²³
Nombre d'emplois (en fin d'année)	195	198	199	215	225	245	270
Proportion de juristes	38 %	36 %	44 %	48 %	34 %	33 %	N/A
Proportion d'assistants	22 %	26 %	25 %	22 %	13 %	12 %	N/A
Proportion d'ingénieurs et auditeurs des systèmes d'information	12 %	14 %	18 %	19 %	11 %	11 %	N/A

DÉFINITION

CNIL

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles



Sécurité informatique
NOTIONS GÉNÉRALES

Mission de la CNIL :

- Contrôler le respect de la loi Informatique et Libertés
- Accompagner et conseiller les acteurs publics et privés
- Traiter les plaintes et les demandes des individus
- Sensibiliser et éduquer le public
- Assurer une veille technologique et juridique
- Représenter la France au niveau européen et international

DÉFINITION



Exemple d'intervention de la CNIL :

- La CNIL est par exemple intervenue sur des cas portant préjudice à des personnes figurant dans des fichiers de police : mention ne devant plus y figurer, acte ne devant pas être référencé, personne fichée à tort.
- La CNIL doit aussi vérifier que l'exploitation privée de données de masse préserve la protection des données de santé personnelles.

DÉFINITION



Loi Informatique et Libertés :

- C'est une loi française qui régit la protection des données personnelles et la vie privée des individus en France.
- Elle a été promulguée en 1978 et a été modifiée et mise à jour à plusieurs reprises pour s'adapter aux évolutions technologiques et aux normes de protection des données.
- La loi Informatique et Libertés est l'équivalent français de la directive européenne sur la protection des données de 1995.

DÉFINITION



RGPD (Règlement général sur la protection des données) :

<https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>

- Le RGPD est un règlement européen en matière de protection des données personnelles qui est entré en vigueur le 25 mai 2018.
- Il a pour objectif de renforcer la protection des données personnelles des individus au sein de l'Union européenne en établissant des règles strictes sur la collecte, le traitement et la conservation des données personnelles par les organisations et les entreprises.
- Le RGPD accorde aux individus des droits accrus sur leurs données, tels que le droit d'accès, le droit de rectification, le droit à l'effacement (ou droit à l'oubli), et le droit à la portabilité des données.
- Il impose également des obligations aux responsables du traitement des données, notamment en matière de transparence, de sécurité des données, de notification des violations de données, et de désignation d'un délégué à la protection des données (DPO).
- Les entreprises et les organisations qui ne respectent pas le RGPD peuvent être soumises à des amendes importantes.

Exemples de cyberattaques :



- Cyberattaque WannaCry en 2017
- Cyberattaque NotPetya en 2017
- Attaque contre Equifax en 2017
- Attaque SolarWinds en 2020
- Attaque Colonial Pipeline en 2021
- Attaque Kaseya VSA en 2021

RAPPELS LÉGAUX



Article 323-1 du Code pénal :

- Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **trois ans d'emprisonnement et de 100 000 € d'amende**.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **cinq ans d'emprisonnement et de 50 000 € d'amende**.
- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à **sept ans d'emprisonnement et à 300 000 € d'amende**.

Source : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047052655

Domaines de la sécurité



DOMAINES



Voici quelques domaines de la sécurité informatique :

- Cryptographie
- Sécurité des réseaux
- Sécurité des systèmes d'exploitation
- Sécurité des applications
- Sécurité physique
- Sécurité des données
- Gestion des identités et des accès

Il en existe beaucoup et certains domaines sont transversaux.
Exemple : la sécurité physique et la sécurité des données.

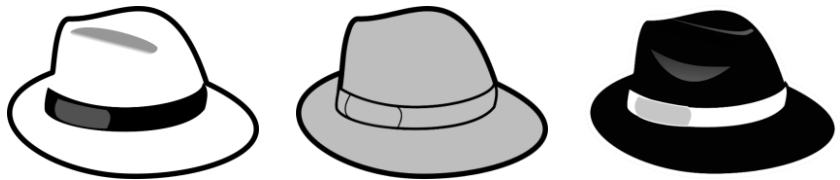


Les attaques



QUI ?

Les attaques sont souvent menées par des **hackers**.
Tous ne sont pas malveillants :



POURQUOI ?

- Le *pourquoi* est très variable.
- Il peut s'agir d'**argent** ou de **nuisance**.
- Parfois, le but recherché est l'**espionnage**, l'**obtention d'informations**.
- Mais une attaque peut aussi n'être qu'un **jeu**.



COMMENT ?

Tous les moyens sont bons !

- Ransomware
- Virus
- Cheval de Troie
- OSINT
- Cryptanalyse
- Rétro-ingénierie



DÉMONSTRATION

UPDA OSINT

Vidéo site immobilier Fred.

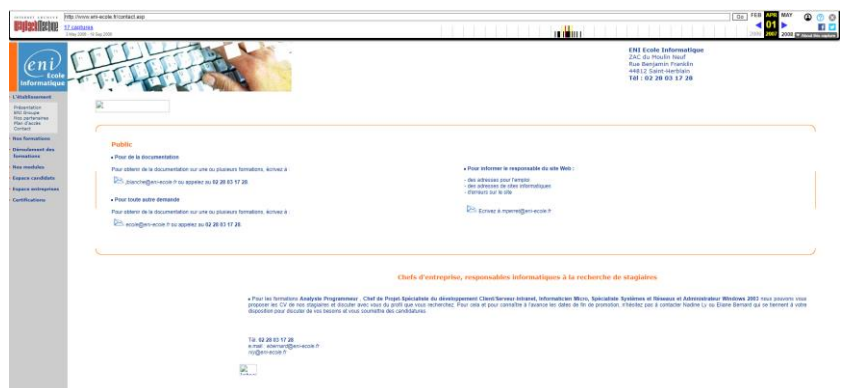
https://www.youtube.com/watch?v=nkz_qFa1Xbc



OSINT

Trouver le responsable du site web de l'ENI en mars 2007

23



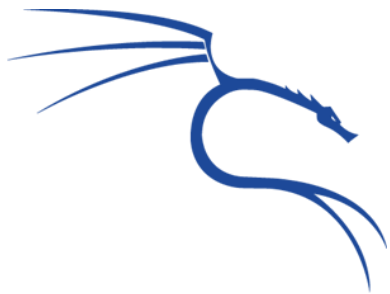
24

Les outils



LES OUTILS

L'outil le plus connu est **Kali Linux**.



LES OUTILS



- **Kali Linux** est une distribution Linux spécialisée dans la sécurité informatique.
- Elle est basée sur **Debian** et offre une vaste gamme d'outils de test de pénétration, de récupération de données, de sécurité des réseaux et d'analyse de vulnérabilités.

LES OUTILS



Origines :

- Kali Linux est dérivé de la distribution **BackTrack Linux**.
- En 2013, il a été rebaptisé Kali Linux par Offensive Security, une société de sécurité informatique.



LES OUTILS



Objectif principal :

- Kali Linux est conçu pour les professionnels de la sécurité informatique et les experts en test de pénétration.
- Son objectif principal est de fournir une plateforme complète pour les tests de sécurité, l'analyse de vulnérabilités, la récupération de données et la forensique numérique.



LES OUTILS



Outils de sécurité :

Kali Linux propose plus de **600** outils de sécurité préinstallés, regroupés dans différentes catégories telles que :

- la collecte d'informations,
- l'analyse des vulnérabilités,
- l'exploitation des failles,
- la gestion des mots de passe,
- la surveillance du réseau, etc.

Certains des outils populaires inclus sont Nmap, Wireshark, Metasploit Framework, Aircrack-ng, John the Ripper.



Comment apprendre la sécurité ?



31

APPRENTISSAGE



Bibliothèque numérique des Éditions ENI

- De nombreux ouvrages et vidéos sont disponibles !



32

APPRENTISSAGE

Sites spécialisés :

- Hack The Box : <https://www.hackthebox.eu>
- TryHackMe : <https://tryhackme.com>
- Root Me : <https://www.root-me.org>
- HackTheBox : <https://www.hackthebox.eu>
- The Black Side : <https://theblackside.fr/>
- Ozint : <https://ozint.eu/>



DÉMONSTRATION

UPDATE
Cryptographie





CODE CÉSAR

Cryptographie - Chiffrement par Substitution - Code César



Rechercher un outil

☐ Parcourir la liste complète des outils

Menu

- Déchiffrement du Code César
- Chiffrement par Code César
- Outils qui se code César
- Définition
- Comment encoder avec le chiffre de César (7 Principes de chiffrement)
- Comment décoder le chiffre de César (7 Principes de déchiffrement)
- Comment reconnaître le code César ?
- Comment reconnaître le code César sans connaître le code César ?
- Quelles sont les variantes du code César ?
- Comment encoder des mots et des chiffres avec le chiffre de César ?
- Pourquoi le code César n'aurait-il pas été inventé ?
- Quelles sont les autres noms du code César ?
- Comment chiffrer César avec le code César ?
- Comment tester l'algorithmique de César en pseudo-code ?
- Quand a été code César a-t-il été inventé ?

Résultats

Mots Fournis :

N°	Outil
#17 (+)	Le Flag Is a long rope for the intruder
#18 (+)	Nou zhuu ca
#19 (+)	vayguyjvlgltlcnaymufmnoh
#20 (+)	Gur vrf nrvzencenayegvhevrfrnygnag
#21 (+)	Car oup jo
#22 (+)	vayguyjvlgltlcnaymufmnoh
#23 (+)	Pda lhuw oc
#24 (+)	vayguyjvlgltlcnaymufmnoh
#25 (+)	Eqr dfr tl
#26 (+)	vayguyjvlgltlcnaymufmnoh
#27 (+)	Hst lshn pz
#28 (+)	hctylshnpyvayguyjvlgltlcnaymufmnoh
#29 (+)	Hsu tzoay w
#30 (+)	vayguyjvlgltlcnaymufmnoh
#31 (+)	Ouv pvlva sc
#32 (+)	vayguyjvlgltlcnaymufmnoh
#33 (+)	Fag rnuw uc
#34 (+)	vayguyjvlgltlcnaymufmnoh
#35 (+)	Uyf gmlh ts
#36 (+)	vayguyjvlgltlcnaymufmnoh

DÉCHIFFREMENT DU CODE CÉSAR

☐ Historique comment ne Code César (2)
[Ouv rve ts](#) [vayguyjvlgltlcnaymufmnoh](#)

Tester tous les décalages possibles (ajustez de 26 lettres A-Z)

► DÉCHIFFRER AUTOMATIQUEMENT

DÉCHIFFREMENT MANUEL ET PARAMÈTRES

☐ DÉCALAGE (du 1 au 25) : 1

☒ **UTILISER L'ALPHABET FRANÇAIS (26 LETTRES DE A à Z)**

☐ **UTILISER L'ALPHABET FRANÇAIS ET DÉCALER AUSSI LES CHIFFRES 0-9**

☐ **UTILISER L'ALPHABET LATIN (26 LETTRES DE A à Z, 10 0-9, 11 A, 12 U, 13 V, 14 W, 15 X, 16 Y, 17 Z)**

☐ **UTILISER LA TABLE CÉSAR (DU 12753 COMME ALPHABET)**

☐ **UTILISER UN ALPHABET PERSONNALISÉ (CARACTÈRES à 260-9999)**

0232454789ABCDEF GHIJKLMNOPQRSTUVWXYZ

► DÉCHIFFRER

Nou aouf - Chiffre Rot (Rotation) - Chiffre par Décalages

CHIFFREMENT PAR DÉCALAGES

☐ HISTORIQUE CLASSE à CHIFFRER PAR CODE CÉSAR (7)
 CODE CÉSAR



37



38

APPRENTISSAGE : OSINT



Site incontournable : ozint.eu

- <https://youtu.be/9bEoHw6wACg> Durée de la vidéo : 1h06
- https://ozint.eu/challenge_detail.cgi?id_challenge=37

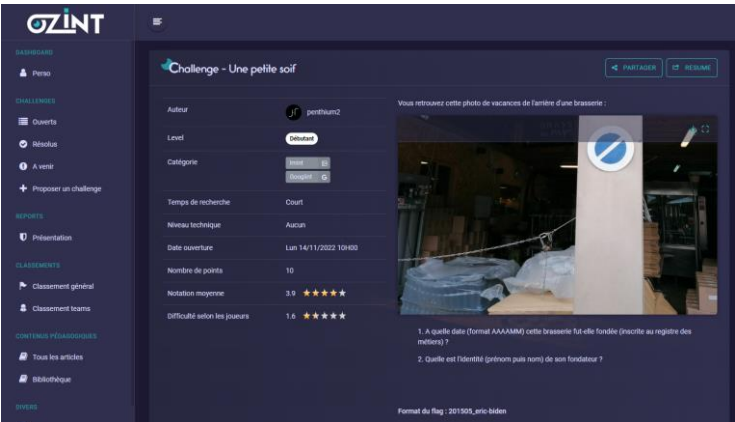


APPRENTISSAGE : OSINT



Site incontournable : ozint.eu

https://ozint.eu/challenge_detail.cgi?id_challenge=9



APPRENTISSAGE

Bug bounty (prime aux bogues)

- Participer à un programme de récompenses



APPRENTISSAGE

Veille

- Faire de la veille tout le temps !



Security By Design



43

SECURITY BY DESIGN



Security by Design (Sécurité par la conception)

- Est un concept de sécurité informatique qui promeut l'intégration de la sécurité dès le début du processus de conception et de développement d'un système, d'une application, ou d'un produit.
- Plutôt que d'ajouter la sécurité comme une réflexion après-coup, le « Security by Design » encourage à envisager et à intégrer les principes de sécurité dès les premières phases de planification et de conception.
- L'objectif est de créer des systèmes et des produits qui sont intrinsèquement sécurisés, réduisant ainsi les risques de vulnérabilités et d'attaques.

44

SECURITY BY DESIGN



Intégration précoce de la sécurité

- Le « Security by Design » implique que les aspects de sécurité sont pris en compte dès le début d'un projet.
- Cela signifie que les architectes, les développeurs, et les concepteurs intègrent des contrôles de sécurité dès la phase de conception plutôt que de les ajouter après avoir développé un produit ou un système.

45

SECURITY BY DESIGN



Identification des menaces et des vulnérabilités

- Le processus de « Security by Design » commence par l'identification des menaces potentielles et des vulnérabilités qui pourraient affecter le système.
- Une analyse des risques est réalisée pour déterminer les scénarios de menace possibles.

46

SECURITY BY DESIGN



Choix des technologies et des pratiques sécurisées

- Les choix technologiques et les pratiques de développement sécurisé sont intégrés dans la conception.
- Cela peut inclure l'utilisation de bibliothèques de sécurité, la mise en œuvre de contrôles d'accès robustes, et la gestion appropriée des données sensibles.

SECURITY BY DESIGN



Tests de sécurité continus

- La sécurité est continuellement testée tout au long du développement, avec des évaluations de sécurité, des analyses de vulnérabilité, et des tests de pénétration.
- Les vulnérabilités identifiées sont corrigées rapidement.

SECURITY BY DESIGN



Sensibilisation à la sécurité

- Le personnel impliqué dans le projet est sensibilisé à l'importance de la sécurité et formé pour adopter des pratiques sécurisées.



Gestion des incidents

- Le « Security by Design » inclut également des plans de réponse aux incidents en cas de failles de sécurité.
- Il est essentiel de savoir comment réagir en cas de compromission potentielle.

SECURITY BY DESIGN



Conformité aux réglementations

- Le « Security by Design » vise également à garantir que le système est conforme aux réglementations de sécurité et de protection des données en vigueur.

En résumé :

- C'est une approche proactive de la sécurité qui cherche à éviter les lacunes et les vulnérabilités en intégrant la sécurité dès le début du processus de conception.
- Cette approche est de plus en plus importante à mesure que les cybermenaces deviennent plus sophistiquées et que la protection des données personnelles devient une préoccupation majeure pour les organisations.

NOUVEAU
PROJET DE LOI

<https://www.vie-publique.fr/loi/289345-securiser-et-reguler-lespace-numerique-projet-de-loi-sren>

REPUBLIQUE FRANÇAISE

Logo

Vie publique

Au service du citoyen public

Rechercher

Actualités

Les Fiches

Ressources

Multimédia

Publications

Qui sommes-nous ?

Accueil

Actualités

Panorama des lois

Projet de loi visant à sécuriser et réguler l'espace numérique

← Panorama des lois

Projet de loi visant à sécuriser et réguler l'espace numérique

Où en est-on ?

Conseil des ministres

10 mai 2023

51