TRAAM STI 2023-2025

Cybersécurité

Secteurs Financiers

Darknet

- Définition
  - Une zone d'Internet non indexée par les moteurs de recherche, accessible via des réseaux anonymes et fréquemment associée à des activités illégales.
- Réseaux anonymes
  - Tor
  - I2P
  - Freenet
- Accès au Darknet
  - Navigateurs spécifiques (Tor Browser)
  - Réseaux privés virtuels (VPN)
  - Marchés en ligne spécialisés
- Contenus et services
  - Forums de discussions anonymes
  - Vente de drogues, armes, et autres produits illégaux
  - Journalisme d'investigation
  - Protection de la vie privé
- Risques et controverses
  - Activités illégales
  - Menaces à la sécurité et à la vie privé
  - Surveillance gouvernementales
  - Éthique de l'anonymat en ligne
- Répression légal
  - Lois et réglementations sur le Darknet
  - Arrestations de criminels en ligne
  - Évolution de la législation
- Utilisations légales
  - Protection de la vie privée
  - Défense de la liberté d'expression
  - Recherche sur la cybersécurité
- Conseils de sécurité
  - Utilisation responsable
  - Protection de l'identité
  - Éviter les risques
- L'avenir du Darknet
  - Évolutions technologiques
  - Débats sur la régulation
  - Impacts sur la société

Les types de hackeurs

- Les 3 principaux
  - Hackeur au chapeau blanc
    - Aussi connus sous le nom de « hackers éthiques », ces individus sont des professionnels de la cybersécurité. Ils travaillent pour le gouvernement et les entreprises afin de les aider à identifier les failles de leur réseau et à y remédier. Ils évitent ainsi les menaces éventuelles et renforcent leur cybersécurité.
  - Hackeur au chapeau noire
    - Également connus sous le nom de « crackers », c'est généralement à ce groupe d'individus qu'on fait référence quand on parle de hackers. Contrairement aux hackers éthiques qui se conforment à la loi et aux réglementations en vigueur, les crackers ne respectent aucun code d'honneur. Ils s'engagent dans des activités criminelles pour voler, extorquer, espionner… tous les coups sont permis !
    - Les black hats sont largement associés aujourd'hui aux organisations criminelles qui mènent des attaques
  - Hackeur au chapeau gris
    - Rien n'est jamais tout noir ou tout blanc ; il en est de même dans le monde du hacking. Les gray hat hackers utilisent les mêmes techniques de piratage que les hackers black hat pour découvrir les failles de sécurité des systèmes cibles, sans l'autorisation du propriétaire.
    - Ces personnes peuvent se livrer à des pratiques qui ne sont pas tout à fait honnêtes, mais agissent souvent pour le bien commun. Les gray hat hackers représentent le juste milieu entre les white hats, qui agissent pour maintenir des systèmes sécurisés, et les black hats qui agissent de manière malveillante pour exploiter les vulnérabilités des systèmes.
    - Pour être clair, ce type de piratage est toujours illégal, car, même si les intentions sont bonnes, l'infiltration dans les réseaux et la récupération de données ne sont pas autorisées.
- Les autres moins connus
  - Script kiddies ou skiddies
    - Ce sont des hackers amateurs qui ne créent pas leur propre code, mais utilisent des scripts écrits par des programmeurs chevronnés. Les skiddies sont donc souvent des personnes qui n'ont pas de compétences en programmation et sont motivés par l'expérimentation et le vandalisme.
  - Les hacktivistes
    - Ils représentent un groupe de hackers militants anonymes qui accèdent sans autorisation aux fichiers et réseaux informatiques du gouvernement. Ils exploitent des informations confidentielles pour des motifs souvent politiques et sociaux.
    - Le mouvement hacktiviste le plus connu est le groupe Anonymous. Ses membres se présentent masqués et défendent généralement le droit à la liberté d'expression sur internet ou en dehors.
  - Hackeur au chapeau rouge
    - Leurs intentions sont semblables à celles des white hats ; leur objectif est de protéger les entreprises contre les menaces et les attaques. Mais contrairement à ces derniers, les red hat hackers sont prêts à transgresser les règles et deviennent alors impitoyables pour défendre l'entreprise.
    - Les red hats vise également à freiner les activités des black hat hackers ; au lieu de signaler ces activités malveillantes aux autorités, ils prennent les choses en main et utilisent des techniques d'attaques agressives telles que la DDoS, une des types de cyberattaques les plus populaires.
  - Hackeur au chapeau bleu
    - A l'instar des script kiddies, il s'agit d'une autre catégorie de pirates novices dont l'objectif est de se venger de toute personne qui les contrarie. Réellement, ils n'ont aucun désir d'apprendre et d'acquérir des compétences en développement informatique et peuvent alors utiliser des techniques de cyberattaques simples.
  - Les hackeurs parrainés par l'Etat
    - Ce sont des personnes engagées par l'Etat pour espionner et s'infiltrer dans les réseaux des grandes entreprises, des départements ou des gouvernements. Ils disposent en effet de budget illimité et d'outils très avancés pour mener leurs attaques.

Définition

- Cybersécurité
  - La cybersécurité est le domaine de protection des systèmes informatiques et des données contre les menaces, incluant des pratiques et technologies pour préserver la confidentialité et l'intégrité. Elle est cruciale pour la sécurité des données et de l'infrastructure en constante évolution.
- Hackeur
  - Un hacker est une personne qui utilise des compétences informatiques pour accéder, modifier ou manipuler des systèmes informatiques, des réseaux ou des données, souvent dans des contextes variés, allant de l'éthique à la malveillance.
- DDOS
  - Une attaque en déni de service ou DDoS vise à rendre inaccessible un serveur afin de provoquer une panne ou un fonctionnement fortement dégradé du service.
- Par-feu
  - Un dispositif de sécurité qui filtre le trafic réseau entrant et sortant pour empêcher les accès non autorisés.
- Logiciels Antivirus
  - Un programme conçu pour détecter, bloquer et supprimer les logiciels malveillants.
- Chiffrement de données
  - La transformation des données en un format illisible sans la clé correspondante pour les protéger contre l'accès non autorisé.
- Cyberattaque
  - Une action délibérée visant à compromettre la sécurité des systèmes informatiques ou à voler des données.
- Vulnérabilité
  - Une faiblesse ou une faille dans un système ou une application qui peut être exploitée par des attaquants.
- Authentification à deux facteurs
  - Un mécanisme de sécurité qui exige deux méthodes d'identification pour accéder à un compte (par exemple, un mot de passe et un code SMS).
- Mises à jour de sécurité
  - Des correctifs logiciels qui résolvent les vulnérabilités connues pour renforcer la sécurité.
- Réseau privé virtuel (VPN)
  - Une technologie qui crée un tunnel sécurisé pour les communications en ligne.
- Hackers éthiques
  - Des experts en sécurité qui testent les systèmes de manière légale pour améliorer la sécurité.
- IA (intelligence artificielle)
  - L'Intelligence Artificielle (IA) est un domaine de l'informatique qui vise à créer des systèmes informatiques capables d'imiter certaines fonctions cognitives humaines.
- Phishing
  - Le phishing est une méthode d'attaque informatique où les cybercriminels se font passer pour des entités de confiance pour tromper les victimes et obtenir des informations sensibles.

Gouvernance

- Méthodes
  - PSSI
    - Politique de sécurité des systèmes d'information
    - Dérogations
    - https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/
  - EBIOS
    - https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
  - MEHARI
  - RGS
    - https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
- Bonnes pratiques
  - Des utilisateurs
  - Veille
  - Référentiels
    - ISO
- Inventaire du SI
  - Cartographie
  - Urbanisation

RGPD

- Sujet secondaire
- Traitement des données
  - Responsable du traitement
  - Sous-traitance du traitement des données
- Sanctions
  - Sujet secondaire
  - Sujet secondaire
- https://www.ssi.gouv.fr/entreprise/reglementation/rgpd/

Surveillance

Pentest

- Nmap
- WireShark
- Sqlmap
- Kali Linux
- Metasploit
- John the Ripper
- Hydra
- Burp Suite
- Zed Attack Proxy
- Aircrack-ng

Sensibilisation formation

Certifications

- https://www.nist.gov/cyberframework
- https://www.offensive-security.com/
- https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
- https://certification.comptia.org/certifications/security
- https://www.giac.org/certification/security-essentials-gsec
- http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
- https://www.globalknowledge.com/fr-FR/Formation/ISC2/Security/CCSP
- Certifications privées
  - Google
    - https://cloud.google.com/certification/cloud-architect
  - Oracle
  - IBM
  - Microsoft
  - Cisco
- https://cloudsecurityalliance.org/education/ccsp/#_overview

Normes

- ISO
  - Certification
  - 00/10/20/30/40/50/60/90/95
    - ISO 14001
      - Management environnemental
      - https://www.iso.org/fr/iso-14001-environmental-management.html
    - ISO 20000-1
      - Technologies de l'information
      - https://www.iso.org/fr/standard/70636.html
    - ISO 27000
      - Système de Management de la Sécurité de l'Information 27001
      - Code bonnes pratiques pour le management de la sécurité de l'information 27002
        - 115 mesures réparties sur 14 chapitres
      - Gestion des risques 27005
      - Classification des informations
      - Gestion des ressources humaines
      - Mise en place
        - Plan
        - Do
        - Check
        - Act
      - https://www.ssi.gouv.fr/uploads/2016/05/cyberedu_module_4_cybersecurite_organisation_02_2017.pdf
    - ISO 9000
      - Management de la qualité
      - https://www.iso.org/fr/iso-9001-quality-management.html
- CASCO
  - Certification
  - Comité pour l'évaluation de la conformité
- ORGANISME DE CERTIFICATION
  - https://www.afnor.org/

Audit

Organismes

- ANSSI
- CLUSIF
- CNIL

Se protéger des attaques

Antivirus

- Sujet secondaire

Actifs

- Réseaux
- SI
- Applicatif
  - Logiciels
  - https://www.isc2.org/Certifications/CCSP
  - Webapp
  - Dev
  - OWASP
- Matériel
  - IoT
  - BYOD
- Humains

Cryptographie

- Sujet secondaire

HELPDESK

- Support Niveau 1
  - Interventions support utilisateurs
- Support Niveau 2
  - Téléassistance intermédiaire
- Support Niveau 3
  - Assitance Technique spécialisée
- https://www.promosoft.fr/les-differents-niveaux-dintervention-du-support-aux-utilisateurs-dans-le-cadre-de-la-maintenance-informatique/

Concepts

- GRC
  - Gouvernance
  - Risques
  - Conformité
- DIC(P)
  - Intégrité
  - Disponibilités
  - Confidentialité
  - Preuve
  - Traçabilité
- PRA
- PCA
- Classification de l'Information
- Sûreté/Sécurité
- Vulnérabilité / menaces / attaques
- BCR (Binding Corporate Rules)
  - https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr
- Hygiène informatique
  - https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/