Cybersécurité

- Cyber malveillance
- Zataz
- Data Security Breach
- Sensibilisation à la cybersécurité
- Guide des bonnes pratiques de confidentialité et de sécurité en informatique
- 15 liens utiles pour votre Sécurité & Cybersécurité
- Check if your email address is in a data breach
- Outils de sécurité informatique
- Documentaires
- 20 outils incontournables
- Moteurs de recherche
- 10 technologies

Cyber malveillance

https://www.cybermalveillance.gouv.fr/

Zataz

https://www.zataz.com/

Data Security Breach

https://www.datasecuritybreach.fr/

Sensibilisation à la cybersécurité

Guide :

https://kdrive.infomaniak.com/app/share/210579/863e3287-393f-4bdc-a6a5-57db8d1d8c0f

Guide des bonnes pratiques de confidentialité et de sécurité en informatique

Guide : https://kdrive.infomaniak.com/app/share/210579/985a1711-d5f9-4285-a96a-6337a8dfdcc7

15 liens utiles pour votre Sécurité & Cybersécurité

 Cambriolage - Bénéficier gratuitement du dispositif Opération tranquillité vacances - https://lnkd.in/eWS3RFYZ

 Signaler une violence conjugale ou sexiste - https://lnkd.in/eg5AkxHw

 Signaler un Cyber-harcelement - https://lnkd.in/eHjGnFXq

 Signaler un spam sur votre messagerie - https://www.signal-spam.fr

 Pharos - Signaler un contenu illégal sur Internet - https://lnkd.in/ehKCdngm

 Perceval - Signaler une fraude à la CB - https://lnkd.in/eHv7kdzW

 SignalConso - Signaler un problème avec un commerçant ou un service - https://lnkd.in/eSD3mFtj

 Signaler une discrimination - https://lnkd.in/eYQ3nunf

 Association e-Enfance/3018 - Suppression de contenus (chantage, revenge, usurpation d’identité…) - https://lnkd.in/esY_ja3S

 Allo 119 - Enfant en danger - https://lnkd.in/ezs6z9ZN

 CNIL - Plainte au régulateur des données personnelles - https://lnkd.in/e-uyi3e4

 Pre-Plainte - Déclaration pour des faits d'atteinte aux biens - https://lnkd.in/eRgVygXs

 Cybermalveillance - Conseils pratiques en cas de cyber attaque - https://lnkd.in/ey74MihW

 Discuter avec la Gendarmerie Nationale - https://lnkd.in/ey74MihW

 Défenseur des droits - https://lnkd.in/e56WqTdg

Check if your email address is in a data breach

https://haveibeenpwned.com/

Outils de sécurité informatique

Ces outils vous aideront à renforcer vos connaissances en sécurité et à auditer vos réseaux, applications et systèmes.

Piratage de réseaux sans fil:

- Aircrack-NG
- Wifite
- Kismet
- TCPDump
- Airsnort
- Netstumbler
- Reaver

Phishing et développement:

- GoPhish
- HiddenEye
- SocialFish
- EvilURL
- Evilginx

Exploitation:

- Burp Suite
- Metasploit Framework
- SQL Map
- ZAP
- ExploitDB
- Core Impact
- Cobalt Strike

Scan de vulnérabilités:

- OpenVAS
- Nessus
- AppScan
- LYNIS

- Retina
- Nexpose

Enquête et récupération de données:

- SluethKit
- Autopsy
- Volatility
- Foremost
- Binwalk
- Wireshark
- Test Disk

Évaluation des applications web:

- OWASP ZAP
- Burp Suite
- Nikto
- WPScan
- Gobuster
- App Spider

Collecte d’informations:

- Nmap
- Shodan
- Maltego
- TheHarvester
- Recon-NG
- Amass
- Censys
- OSINT Framework

Craquage de mots de passe:

- John The Ripper
- Hydra
- Hashcat
- OPHCrack
- Medusa
- Cain & Abel

Documentaires

Découvre les meilleurs documentaires pour plonger dans l’univers fascinant des hackers et de la cybersécurité :

1. We Are Legion - The Story Of The Hacktivists
2. 21st Century Hackers
3. Hackers Wanted
4. Hackers in Wonderland
5. The Internet’s Own Boy: The Story Of Aaron Swartz
6. Def Con: The Documentary
7. Hackers Are People Too
8. Secret History Of Hacking
9. Risk (2016)
10. Zero Days (2016)
11. Guardians Of The New World | Real Stories
12. A Origem dos Hackers
13. The Great Hack
14. The Network’s Dilemma
15. Web Warriors
16. Cyber War - Dot of Documentary
17. CyberWar Threat - Inside World’s Deadliest Cyberattack
18. The Future of Cyberwarfare
19. Dark Web: Fighting Cybercrime
20. Cyber Defense: Military Training for Cyber Warfare
21. Hacker Hunter: WannaCry, The Story of Marcus Hutchin
22. The Life Hacker Documentary

20 outils incontournables

Pour les pros et ceux qui débutent ...

1. Kali Linux - Système d’exploitation avec des milliers d’outils préinstallés
2. Wireshark - Capture et analyse de protocoles réseau
3. Nmap - Scanner de ports (à utiliser avec précaution)
4. Burp Suite - Sécurité web
5. Gophish - Kit d’outils de phishing open source
6. Aircrack-NG - Sécurité Wi-Fi
7. Have I Been Pwned - Pour vérifier si vos emails ont été retrouvés dans un leak
8. Metasploit Framework - Outil de pentest polyvalent (à utiliser avec précaution)
9. Nikto - Scanner de vulnérabilités
10. HackTheBox - Entraînement à la cybersécurité
11. pfSense - Pare-feu/Routeur
12. Cyber Chef - Boîte à outils polyvalente, disponible en ligne et installable localement
13. Suricata - Système de détection d’intrusions (IDS)
14. Ghidra - Reverse engineering, développé par la NSA
15. Dehashed - Pour savoir si vous avez été compromis
16. OpenVAS - Scanner de vulnérabilités interne et externe (version open source de Nessus maintenue par l’armée allemande)
17. OSSEC - Détection et prévention des intrusions
18. SQLMap - Détection et exploitation d’injections SQL (à utiliser avec précaution)
19. REMnux - Reverse engineering et analyse, notamment pour la décompilation de malwares
20. Zed Attack Proxy (OWASP ZAP) - Scanner de sécurité des applications web

Moteurs de recherche

Vous cherchez un truc en cybersécurité ?

Si vous travaillez dans la cybersécurité, vous savez à quel point il est difficile d'avoir les bons outils pour explorer et analyser les données. Voici 10 moteurs de recherche un peut spéciaux que tout professionnel devrait connaître, avec une explication de ce que chacun permet de faire:

1. Shodan
Le moteur de recherche des objets connectés. Shodan vous permet d'explorer les serveurs, caméras, dispositifs IoT et autres appareils connectés à Internet. Parfait pour identifier les équipements vulnérables.
2. Censys
Analyse des services sur Internet. Censys cartographie les services exposés et fournit des informations détaillées sur les systèmes en ligne, facilitant la détection des failles de sécurité.
3. Hunter
Recherche d'adresses email. Hunter est idéal pour trouver les adresses email associées à un domaine. Utilisé souvent dans les campagnes de phishing ou d'investigation en cybersécurité.
4. urlscan.io
Analyse des URL suspectes. Ce service analyse les sites web pour identifier les comportements malveillants, les redirections, ou les contenus cachés. Très utile pour évaluer les menaces liées aux URL.
5. grep.app

Recherche dans le code source public. Grep.app vous aide à trouver des fragments de code partagés en public, ce qui peut révéler des informations sensibles ou des erreurs de configuration.
6. intelx.io
Outils d'OSINT. IntelX vous permet d'accéder à des bases de données, archives web et documents divulgués publiquement pour mener des enquêtes approfondies.
7. wigle.net
Cartographie des réseaux WiFi. Wigle vous aide à identifier les réseaux WiFi dans le monde entier. Utile pour les recherches sur les vulnérabilités réseaux.
8. FullHunt (Attack Surface)
Analyse de la surface d'attaque. FullHunt permet d'identifier et de surveiller les failles de sécurité dans les systèmes exposés sur Internet.
9. Vulners (Vulnerabilities)
Recherche de vulnérabilités. Vulners est un moteur de recherche de vulnérabilités connu qui compile les CVE (Common Vulnerabilities and Exposures).
10. viz.greynoise (Threat Intel)
GreyNoise aide à distinguer les activités malveillantes réelles des bruits de fond (scans automatisés, bots), permettant d'allouer vos ressources plus efficacement.

Ces outils couvrent tout, des serveurs vulnérables aux réseaux WiFi non sécurisés, en passant par la collecte d’informations OSINT. Ils sont incontournables pour tout professionnel de la cybersécurité !

10 technologies

1. SIEM (Security Information and Event Management)
Remontée de logs, analyse automatique et alertes en temps réel. Indispensable pour identifier rapidement les incidents de sécurité et réagir avant que la situation ne s’aggrave.

2. Firewall
L’indispensable filtre qui t’évite de te prendre des attaques sur ton infra. Sans ça, autant laisser la porte ouverte et sortir les petits fours.

3. EDR (Endpoint Detection and Response)
Pour que ton système détecte quand quelque chose qui ne devrait pas se passer se passe.

4. Solutions de Sécurité Cloud
Ah, le cloud. Là où tout est censé être sécurisé et flou. En vérité, la grande majorité des attaques aujourd’hui cible le cloud, normal, c’est là où tout se passe !

5. VPN (Virtual Private Network)
Parce que travailler depuis un salon de thé en toute sécurité, c’est le rêve de tout “hacker”. Aussi parce que tout le monde en télétravail est sur VPN, et que c’est un bon vecteur d’attaque.

6. IDS/IPS (Intrusion Detection/Prevention Systems)
IDS observe ce qui passe sur le réseau, IPS agit. Ça se bypass, mais surtout, ça se met en place et ça se configure comme il se doit.

7. Antivirus / Anti-Malware
Parce qu’en 2024, les virus ne sont pas encore obsolètes, désolé de te décevoir. Mais la majorité des anti-malwares aujourd’hui sont des EDR, et comme les commerciaux en ont vendu à toutes les boîtes, on a inventé les XDR.

8. Technologie de Chiffrement
Parce que les données sensibles, c’est mieux quand elles ne sont pas stockées en clair. Encore mieux quand elles ne sont pas transférées en clair non plus…

9. IAM (Identity and Access Management)
Pour gérer qui accède à quoi, même si toi-même tu t’y perds un peu et que tu n’as accès à pas grand-chose.

10. DLP (Data Loss Prevention)
Empêche les fuites de données, quand ça marche bien. Parce que partager, c’est sympa, mais pas les infos sensibles à des personnes non autorisées.