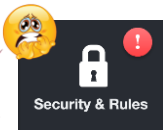
90 % des entreprises ont été confrontées à des problèmes de sécurité et n'ont pas su faire face

Sommaire

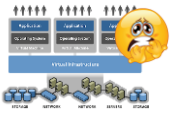
Sécurité : Pour mieux nous défendre contre les attaques
Utiliser les mêmes armes que nos adversaires

Les problèmes viennent de partout


Sécurité des mobiles



Réseaux d'anonymisation



Hyperviseurs

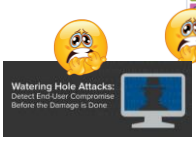

Piratage des capteurs de commande d'un véhicule

Conformité règlementaire

Sécurité des containers


Vol de données

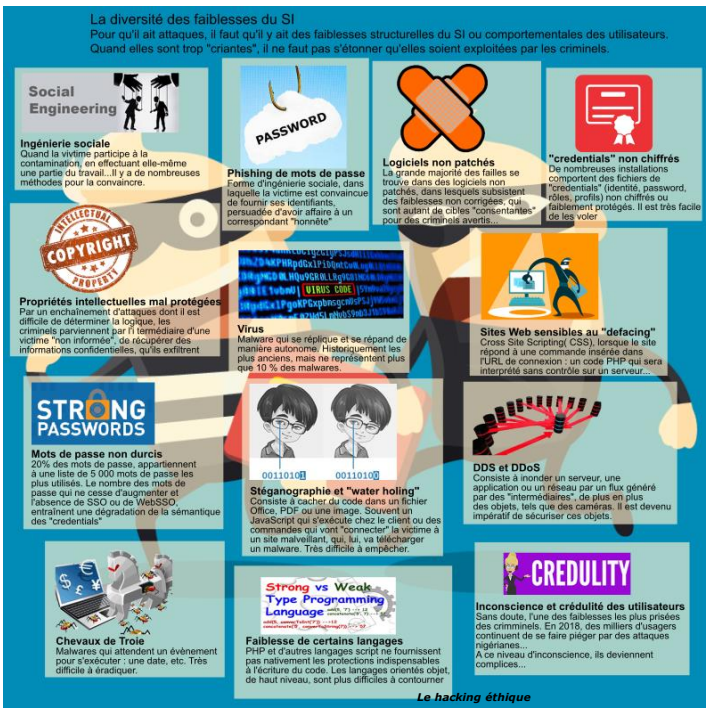

Paiement par mobile



Watering Hole

Attaques contre les structures industrielles

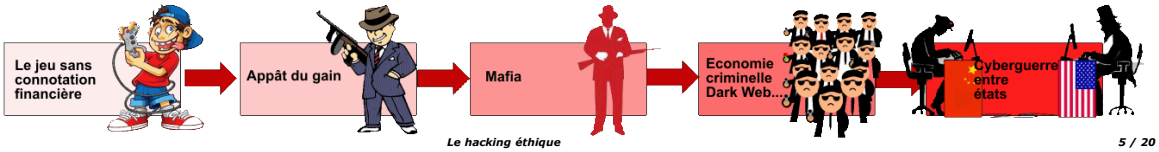
DoS et DDoS



Les principales faiblesses du TI

A qui avons-nous affaire ?

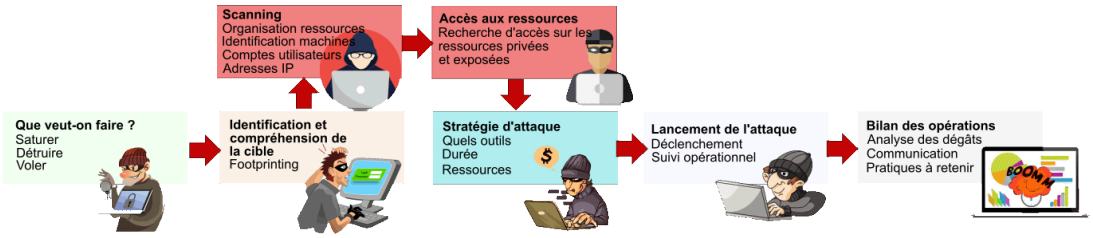
- Les « **Black Hats** » : les « crackers » qui détruisent, terroristes et maffieux. Leurs objectifs sont clairs et ils possèdent une grande compétence.
  - Le nerf de la guerre est.
  - Déstabilisation de la démocratie.
- Les « **White Hats** » : les hackers éthiques. Ils protègent les actifs de l'entreprise, que l'on pourra déployer en deux familles, « reds » ou « blues ».
- Les « **Gray Hats** » sorte d'intermédiaire entre les black et white hats. Ils ne cherchent pas à gagner de l'argent, ni à détruire la société, mais s'intéressent au sujet.
- Les « **Green Hats** » : des « Black Hats » incompétents, ceux qui posent des questions idiotes, auxquelles les vrais hackers répondent avec parcimonie et mépris.
- Le « **Red Hat** » est le Rambo de la sécurité, celui qui croit qu'il mettra fin aux activité des « black Hats », seul et sans armes.
  - Pour bien comprendre la dangerosité des malwares, il les télécharge et les incorpore dans son propre système.
  - Il arrive que l'un de des « Red Hats » fasse plier un hacker maladroit. Mais c'est en général au prix de 100 000 machines bloquées et de 3 millions $ de pertes de production.
- Le « **Blue Hat** » est une sorte de « script kiddie », pas plus compétent, mais animé d'un désir de vengeance inassouvi.



Qu'est-ce que le hacking éthique

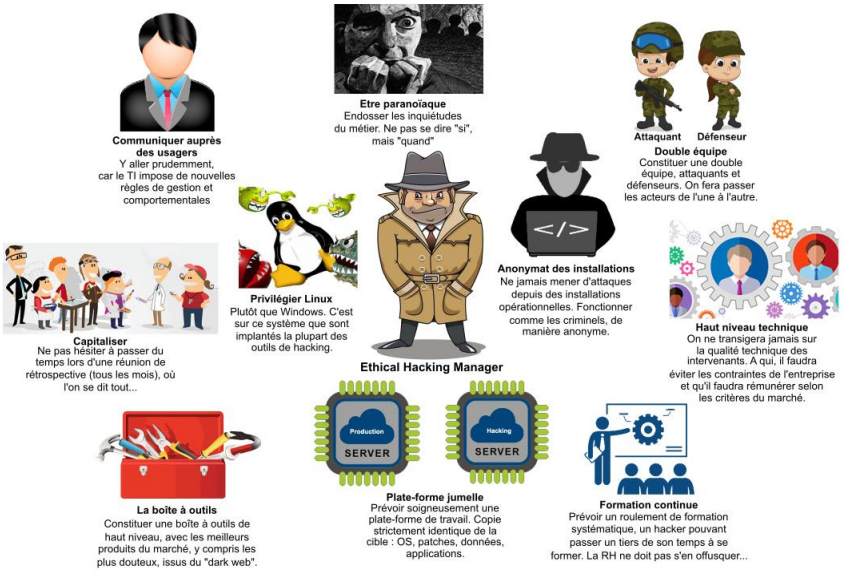
- Le temps du hacking "angélique" est terminé.
- Les pertes globales liées à la sécurité atteignent 6 000 milliards $.
- Etat de guerre.
- Les entreprises doivent mieux valoriser les responsables sécurité?
- **La meilleure manière de se protéger contre les entreprises criminelles menées contre le TI, est de pratiquer les mêmes techniques, méthodes et outils qu'elles.**
- Pour dresser des parades sur des protocoles qui ne garantissent rien en matière de sécurité : IP, TCP, UDP, SMTP, DNS, SNMP, CMIP…
- Les policiers ne peuvent pas fonctionner sans indicateurs chez les criminels. Pour le TI c'est pareil.
- L'arsenal juridique est à revoir, sanctions…
- Accentuer le rapprochement entre les polices.
- Le hacking éthique ou "White Hat Hacking", regroupe l'ensemble des solutions qui permettent à des équipes internes de se comporter comme des criminels, mais sans autre volonté que celle de protéger l'entreprise.
- Avec des solutions qui recouvrent deux concepts : les méthodes et les outils.
- La sécurité est une préoccupation permanente 7/24, d'où la nécessité de libérer les acteurs de certaines contraintes règlementaires, telles que les horaires

Pratiquer les mêmes techniques que les adversaires



- Il faut les apprendre…
- Participer à des groupes de hackers… sous un faux nom… si possible
- Se mettre "dans la peau" d'un criminel, comprendre ses motivations…
- Se faire aider par des partenaires sûrs : tests de pénétration réguliers, veille permanente
- Faire appliquer les bonnes pratiques de programmation
- Tester au plus près de la vraie grandeur les scénarii d'attaques

Les recommandations du hacking éthique



S’organiser pour faire face

Une équipe et une plate-forme d'attaque

- Rattacher l'équipe sécurité directement auprès du patron du TI, sans intermédiaire
- Faire de la **paranoïa** une qualité et ne pas se demander si notre entreprise **va** être attaquée, mais **quand**.
- **Ne jamais mener d’attaques, depuis notre propre machine**. JAMAIS.
- Il faut nous familiariser avec Linux et certaines de ses distributions (Kali.
- Pour les cibles, on aura généralement affaire à Windows, mais **on ne confondra pas les moyens d’attaques avec les cibles**.
- Il faudra prévoir une **plate-forme strictement identique** (twin), avec les mêmes données et les mêmes configurations systèmes et les principaux process à surveiller.
  - On prendra soin de « détacher » cette plate-forme des domaines de production.
  - Cela va coûter beaucoup d’argent, mais il faudra aussi savoir ce que l’on veut.
  - Globalement une plate-forme de test, qui pourra aussi servir de reprise dans le cadre d’un PCA/PRA (Continuité et Reprise d’Activités), peut représenter jusqu’à 20 % du budget alloué à l’informatique.
- Il y a plusieurs niveaux de reproduction, depuis la simple application jusqu'au site "twin".
- **Communiquer auprès des usagers**
  - Ca ne sert à rien de dépenser des fortunes, s’ils continuent d’avoir des pratiques provocatrices.

L'organisation du hacking éthique

- Distinguer **deux natures de fonctions de hacking**
  - Celles que l’on répètera selon un scénario peaufiné à l’avance, pour s’assurer que la situation ne se dégrade pas.
  - Celles que l’on improvisera en fonction des évènements, pour répondre à une inquiétude ou une épidémie.
- **L'équipe de hacking est bicéphale :** ceux qui attaquent et ceux qui défendent.
  - Nous suggérons de confier la responsabilité de la première à un technicien et la seconde à un manager.
  - La première est une force d’attaque dont les préoccupations seront exclusivement techniques, alors que la seconde exprimera le ressenti des usagers, plus métier que TI.
- On veillera à maintenir le contact avec la RH, car ce métier nécessite une constante remise à niveau, avec les **formations adéquates**. Il n’y a aura rien d’étonnant à ce qu’un technicien passe le quart de son temps en éducation, la formation étant ici à prendre au sens large et pas nécessairement dans des cursus institutionnels.

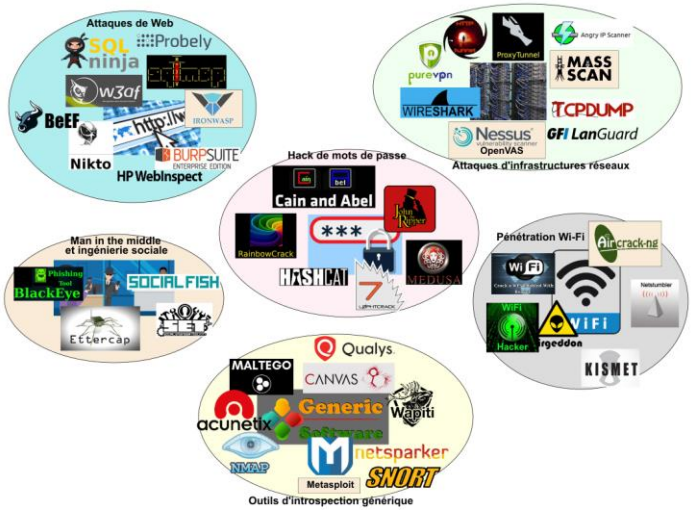
Le profil d'un spécialiste interne

- Personnage à part
- Hacker honnête
- Il faut le libérer des contraintes de l'entreprise : dans son métier tout se passe dans les forums, certains dans le dark web et pas pendant les "heures de bureau"
- Participe à des organisations "douteuses"
- Exploite les outils interdits et l'entreprise doit lui donner les moyens de les utiliser sans nuire aux ressources qu'il est censé protéger
- Il est allergique à la rigidité de l'entreprise, c'est un contestataire, souvent en butte avec sa hiérarchie, qu'il accuse de ne rien comprendre…
- Curieux de tout
- Oublie de venir au bureau parce qu'il a passé la nuit sur un plugin dangereux ou un script malveillant : inutile de le faire pointer, il dort…
- Il n'a pas d'âge et les diplômes n'ont aucune importance
- Il doit se former par des certifications pointues
- La RH doit trouver un moyen d'intégrer ce profil atypique
- **Compétences** : on est ici dans l'un des domaines les plus techniques du TI et qu'il faudra trouver des **praticiens de haut niveau**, passionnés par leur mission et rompus à la programmation système, assembleur, C ou équivalent, pour qui les architectures réseaux et machines n'auront pas de secrets.
- Problème de salaires : difficile de faire entrer l'équipe de hacking éthique dans le cadre des rémunérations de l'entreprise. Ca ne passera pas.
  - Il faut à la fois des compétences très pointues et des comportements spécifiques.
  - Le hacking ne se pratique pas à heures fixes. Il est une préoccupation permanente 7/24. Ce n'est pas un habit que l'on quitte à 5 PM. D'où la nécessité de libérer ces acteurs de certaines contraintes règlementaires, telles que les horaires…

Un hacker "interne", peu compatible avec les règles de l'entreprise

Plus de deux mille produits exploitables

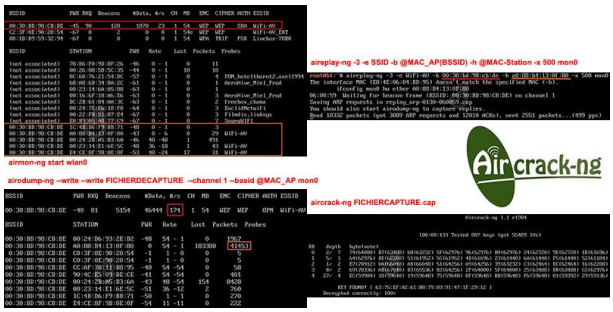
- Il existe sur le marché plus de 2 000 produits susceptibles de nous aider dans la compréhension des techniques de hacking et de mise en œuvre des parades appropriées.
- Certains sont éphémères et disparaissent au gré des modes et pandémies.
- Proposition de classification
  - Pénétration et détection des vulnérabilités Web
  - Introspection des ressources réseaux
  - Hack des mots de passe et autres moyens d'authentification
  - Outils d'introspection génériques
  - Moyens de pénétration Wi-Fi
  - Systèmes d'ingénierie sociale dont « man in the middle ».
- La plupart des outils sont Open Source, parfois gratuits avec des versions "premium"
- Le choix doit être effectué avec soin, par des gens compétents
- Ils vont vous permettre d'endosser en toute légalité, les habits « étroits » du hacker.
- Les "stars" : Aircrack-ng, TCH Hydra, John the Ripper, Nmap (Network Mapper).



Les stars du hacking légal

Aircrack-ng

- Refonte du bien connu Aircrack, dont il est un fork, toujours gratuit.
- Sa vocation est de retrouver les clés utilisées dans les réseaux Wi-Fi, jusqu'au mode de protection WPA-2.
- Suite de plusieurs programmes, parmi lesquels trois sont très importants :
  - Airmon-ng, qui fait passer la carte réseau de la machine de test en mode « monitor », obligatoire pour lui permettre d'écouter le trafic Wi-Fi de proximité et récupérer les paquets Wi-Fi, sans avoir besoin de s'enregistrer
  - Airodump-ng, le bras armé d'Airmon-ng chargé de « sniffer » les paquets
  - Aireplay-ng, qui joue un rôle actif, en réinjectant des paquets ARP, de manière à augmenter les chances de l'attaquant, de retrouver les clés de connexion.
- On estime que 5 à 10 % des routeurs Wi-Fi sont encore équipés d'une simple protection WEP.



Les stars du hacking légal

TCH Hydra

- L'horreur absolue.
- L'outil s'attaque aux « credentials » d'authentification de plus de 50 protocoles : Cisco, FTP, FTP, HTTPS, IMAP, IRC, LDAP, MS-SQL, MYSQL, NNTP, plusieurs protocoles Oracle, POP3, RDP, SAP/R3, SIP, SMTP, SSH, Subversion, Telnet, VMWare-Auth, VNC, etc.
- Il est le seul à proposer une telle diversité.
- Type d'outil d'attaque par force brute.
  - Nécessite des interventions précises de l'utilisateur, pour aider TCH Hydra dans son cheminement pour aboutir (peut-être) à l'obtention d'un mot de passe.
  - Il faudra lui indiquer soit une adresse IP, soit une famille d'IP, le protocole qui nous intéresse, voire un fichier contenant des mots de passe que TCH Hydra pourra tester en priorité, voire limiter le périmètre d'introspection pour des mots de passe ayant une certaine longueur, 8 caractères par exemple, mais pas 6 ou 7, la position des caractères numériques, spéciaux et majuscules, etc.
- On utilisera l'outil comme une console de commandes très puissante.
- Attention, éviter de le mettre entre n'importe quelles mains.

Les stars du hacking légal

John the Ripper

- John The Ripper est au hacking ce qu'est Pelé au soccer. La référence absolue.
- A l'origine, John the Ripper était un cracker de mots de passe, mais il est devenu une véritable suite, capable de mener des attaques par force brute, grâce à toute la panoplie des outils et techniques, connus à ce jour.
- Pour retrouver les mots de passe, il se sert des artefacts habituels : des dictionnaires (le sien par défaut comporte plus de 3 000 occurences). Il tente toutes les combinaisons possibles en associant l'identifiant et en effectuant toutes sortes de permutations, avec des caractères majuscules, minuscules, numériques et des symboles.
- JTR, est très à l'aise avec les techniques de chiffrement et il est capable, dans certains cas, de déchiffrer une empreinte (hash) MD5, par exemple et intervenir dans un processus de fédération d'identités de type ADFS de Microsoft ou Kerberos. Dans certains contextes et avec de la patience, il peut y parvenir…
- Avantage : sa disponibilité sur une cinquantaine de plates-formes.

Les stars du hacking légal

John the Ripper

- Nmap peut faire tomber les protections d'un réseau et constituer un excellent outil de maintenance, tests de vulnérabilités et simuler des attaques.
- Nmap est un « sniffer » de cibles, qui dresse une carte des ressources réseaux, avec de nombreuses informations sur chacune d'elles.
- Nmap peut être actionné par une interface graphique (il en existe plusieurs), mais aussi en mode commande.
  `nmap -option1 -option2 -optionN [cible]`, la cible pouvant être un DNS, une adresse IP, une plage d'adresses IP, une adresse réseau avec son filtre de sous-réseau.
- On peut détecter l'OS qui équipe la cible :
  `nmap -A domaine` : OS de la cible
  `nmap -sV domaine` : services actifs avec n° de port
- Tests d'intrusion : on pourra associer la commande Nmap à un véritable script, écrit en Lua
  `nmap -Pn –script de vulnérabilité domaine`
- C'est la fonctionnalité la plus utilisée via un script publié par la communauté.
- Simulations d'attaques de type DOS (Denial of Service), sur les cibles sensibles à la faiblesse Slowloris, par exemple :
  `nmap 192.168.X.Y -max-parallelism 800 -Pn --script http-slowloris --script-args http-slowloris.runforever=true`
- Attaques par force brute :
- Sur une cible WordPress :
  `nmap -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.X.Y`
- ou sur une base de données SQL :
  `nmap -p 1433 --script ms-sql-brute --script-args userdb=customuser.txt,passdb=custompass.txt 192.168.X.Y`
- Nmap est le couteau suisse, dont un hacker (légal) ne pourra pas se passer.

Les stars du hacking légal

Metasploit

- Metasploit est une plate-forme complète.
- Elle comporte un framework écrit en Ruby, dont l'objet est de développer des exploits, censés utiliser au mieux les anomalies et faiblesses, éventuellement détectées par d'autres produits, tels que Nmap ou John The Ripper, avec lesquels Metasploit est « connectable ».
- Dès qu'une vulnérabilité est connue, on développe un exploit qui l'utilise, de manière à comprendre l'étendue des dégâts potentiels et en déduire la meilleure parade possible.
- Metasploit agit comme un vaccin, en ce sens qu'il « valide » une faiblesse dans le système.
- Les dernières versions de Metasploit ont évolué vers des fonctions dites de « fuzzing » (*), de détection des anomalies et ne se contente plus de se positionner en aval des découvertes, effectuées par d'autres produits.

* : injection de données aléatoires

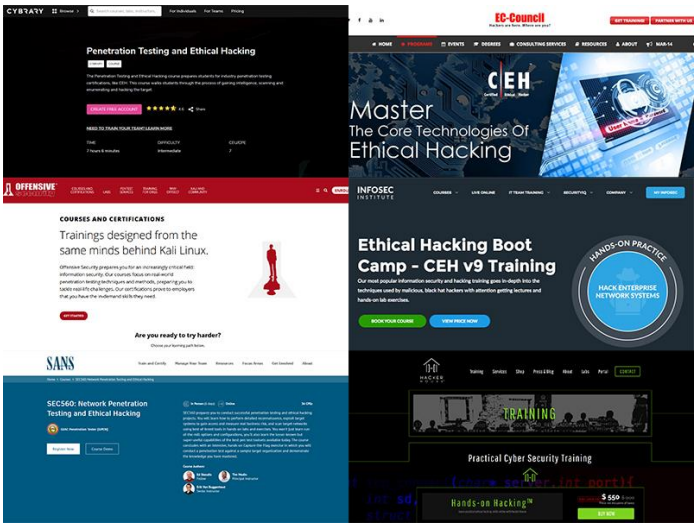
Les forums interdits

(mais je ne vous ai rien dit...)

- Une bonne manière de se maintenir au courant des technologies sécuritaires est de fréquenter certains sites du « deep web.
- On peut avoir des réticences à visiter ces sites (conséquences), mais ce n'est pas illégal.
- On y trouve tous les outils, quasiment gratuits mais bien souvent eux-mêmes pollués, d'où la nécessité de se connecter depuis une plate-forme anonyme et indépendante (navigateur TOR).
- Il existe des centaines de sites dédiés à la criminalité en col blanc, avec quelques vedettes :
- **Torum** (torum6uvof666pzw) : plus de 6 000 membres (référence ésotérique au nombre 666, celui du diable…)
- **KickAss** (kickassugvgoftuk), l'un des plus connus, où il n'est pas facile de se faire admettre, une vaste place de marché, à laquelle nous devons contribuer…
- **Hack this site** (https://www.hackthissite.org/forums)
- **https://hackforums.net/index.php**, va un peu plus loin et héberge de véritables projets consacrés à la lutte contre la cybercriminalité. Très intéressant, plus récent, sans que l'on puisse exclure sa dangerosité. 500 000 adhérents, énorme compte tenu de la matière « douteuse » et le fait que pour être enregistré, il faut décliner son identité, qui devient publique et accessible par les autres membres. Délicat…
- Et de nombreux autres plates-formes, où nous côtoyons la criminalité de près. Sans risque légal, tant que nous ne nous lançons pas dans des opérations illicites :
- **https://forums.hak5.org/**, riche d'une FAQ de plus de 60 000 questions
- **https://forum.exploit.in/**, un site russe d'une très grande richesse (on y parle anglais)
- **http://hackerw6dcplg3ej.onion/**, plutôt un grand catalogue d'outils de hacking, très diversifié. On rappelle que les .onion constituent un domaine de premier niveau auquel on ne peut accéder qu'avec le browser TOR.
- **http://mvfjfugdwgc5uwho.onion,** à la fois une place de marché et un forum où l'on débat des techniques de hacking les plus avancées**.**
- Les entreprises les plus sérieuses et renommées, banques, structures gouvernementales, manufacturiers, opérateurs de télécommunications, ont tous intérêt à « oublier » ce qu'elles sont et s'intéresser de près à ces sites. Evidemment, on évitera de se connecter avec la console d'administration du mainframe…

Des formations spécialisées

Parfois avec une certification



Cybrary
Nombreuses ressources, dont un guide d'étude pour le hacking éthique, un micro cours et des tests de pénétration avec Kali Linux.

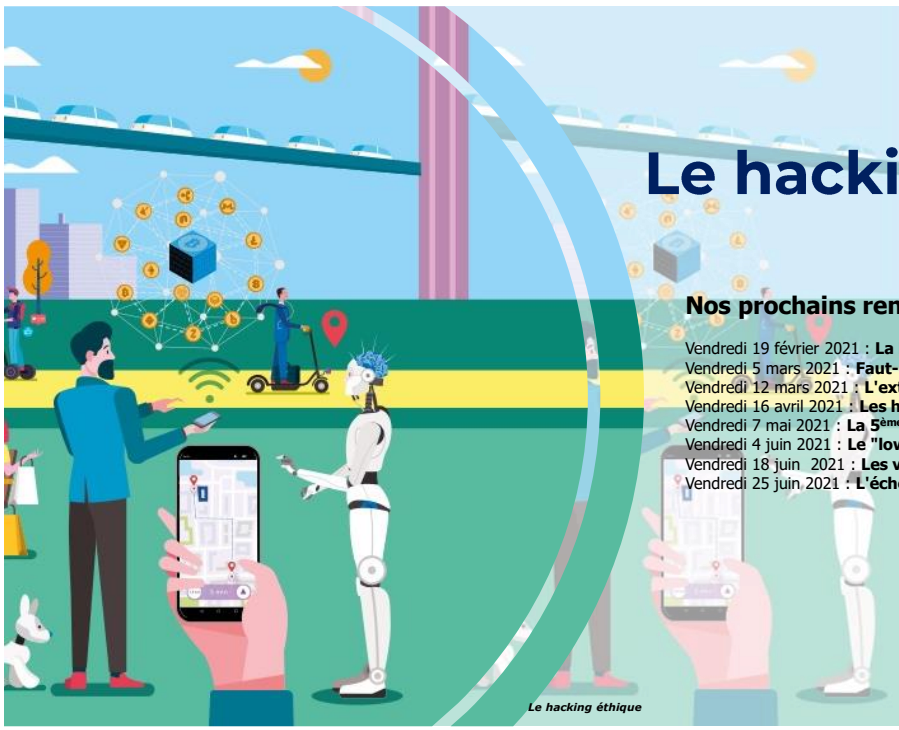
EC-Council
International Council propose le programme CEH (Certified Ethical Hacking), l'un des cours les plus complets du marché : 18 modules, 140 ateliers, 270 technologies et 2 200 outils de hacking connus.

Infosec Institute
Deux cours : Ethical Hacking Boot Camp et sa version avancée avec 31 ateliers.

Offensive Security
Certification OSCE (Offensive Security Certified Expert), pour repérer les vulnérabilités des systèmes. Se termine par un examen où il faut en 48 h, compromettre un réseau distant.

SANS
Le très connu SANS propose un cours de tests de pénétration de réseaux et de hacking éthique. 30 ateliers pour apprendre les méthodes, outils et techniques. Le cours se termine par un test de pénétration réel.

Hacker House
Collection très connue de ressources de formation, dont un cours pratique de hacking.



Le hacking éthique

Devenir des hackers

12 février 2021

Nos prochains rendez-vous

Vendredi 19 février 2021 : **La bataille des fibres sous-marines**
Vendredi 5 mars 2021 : **Faut-il sauver le soldat DSI ?**
Vendredi 12 mars 2021 : **L'extraordinaire retour de la gestion de fichiers**
Vendredi 16 avril 2021 : **Les hologrammes dans la communication**
Vendredi 7 mai 2021 : **La 5ème génération des bases de données**
Vendredi 4 juin 2021 : **Le "low code", comment peut-on y croire ?**
Vendredi 18 juin 2021 : **Les vrais coûts du Cloud**
Vendredi 25 juin 2021 : **L'échec de la modélisation**