

FORUM

Myriam QUÉMÈNER
Amélie KÖCKE**Hacker « éthique »
et cybersécurité**
Opportunités et défisLGDJ Le Grand Débat Juridique
Lection

Hacker « éthique » et cybersécurité » Opportunités et défis

*Myriam Quéméner, magistrat
honoraire, docteur en droit*

1



Plan de la Présentation

- Introduction au hacking éthique
- Techniques et outils du hacker éthique
- Cadre légal et réglementation
- Ethique et responsabilités des hackers éthiques
- Impact et avenir du hacking éthique

2

Différences entre hacking éthique et hacking malveillant

Hacking éthique

Le hacking éthique est effectué avec l'autorisation des propriétaires de systèmes dans le but d'améliorer la sécurité.

Hacking malveillant

Le hacking malveillant est illégal et vise à exploiter les failles pour des gains personnels, souvent au détriment des autres.

Importance de la sensibilisation

Comprendre ces différences est essentiel pour protéger nos systèmes et nos données contre les menaces potentielles.



3

Cadre juridique actuel

- La signalisation spontanée de vulnérabilités à l'Autorité Nationale de la Sécurité des Systèmes d'Information (ANSSI) par les hackers éthiques est encadrée par l'article L.2321-4 du code de la défense. Cet article réserve l'appréciation de la bonne foi du hacker ayant effectué une signalisation aux collaborateurs du CERT de l'ANSSI (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).
- Il est en l'état complexe de concilier la défense face aux risques d'abus des hackers d'un cadre juridique trop protecteur et d'autre part le manque de garantie d'une absence de sanction pour les hackers en cas de signalement.
- Face aux cybermenaces grandissantes, rechercher et opter pour des solutions efficaces est aujourd'hui une priorité pour l'ensemble des organisations.

4

Les hackers face à la justice

- Les hackers qui sont identifiés au terme d'une enquête peuvent faire l'objet de poursuites, notamment sur le fondement des infractions d'atteinte au fonctionnement et aux données contenues dans un système de traitement automatisé de données (STAD). L'entreprise victime de l'acte malveillant pourrait également se prévaloir, selon les circonstances, d'un abus de confiance commis à son préjudice.
- Selon l'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 résulte 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 150000€ d'amende.

5

Hackers et risques juridiques

- Aux termes de l'article 323-3-1 du Code pénal «Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée». Les hackers éthiques ne sont pas toujours à l'abri de poursuites sur cette base juridique, par exemple s'ils diffusent des failles de sécurité sans respecter une procédure bien définie avec le client afin d'éviter de nuire à sa réputation numérique.
- L'infraction de collecte frauduleuse des données personnelles, punie par l'article 226-18 du Code pénal, qui a parfois été retenue cumulativement soit avec l'accès frauduleux dans un système de traitement automatisé de données soit avec l'extraction de données visée par l'article 323-3 du Code pénal.

6

Importance du hacking éthique dans la cybersécurité

Prévention des cyberattaques

Le hacking éthique permet d'anticiper les cyberattaques en identifiant les vulnérabilités dans les systèmes informatiques.

Renforcement de la sécurité

Les hackers éthiques aident à améliorer la sécurité globale des organisations en corrigeant les failles avant leur exploitation.

Identification des faiblesses

En analysant les systèmes, les hackers éthiques découvrent des faiblesses qui peuvent être exploitées par des hackers malveillants.



7

Outils courants utilisés par les hackers éthiques



Metasploit

Metasploit est un outil de test d'intrusion qui permet aux hackers éthiques de découvrir et d'exploiter des vulnérabilités dans des systèmes informatiques.

Nmap

Nmap est un scanner de réseaux qui aide à découvrir des hôtes et des services sur un réseau, essentiel pour effectuer une reconnaissance préalable.

Wireshark

Wireshark est un analyseur de protocole qui permet aux hackers éthiques d'observer le trafic réseau en temps réel pour détecter des anomalies.

8

Méthodologies de hacking éthique

Collecte d'information

La collecte d'information est la première étape cruciale du hacking éthique, permettant d'obtenir des données pertinentes sur la cible.

Analyse des vulnérabilités

L'analyse des vulnérabilités identifie les faiblesses dans les systèmes, ce qui est essentiel pour prévenir les cyberattaques.

Exploitation des failles

L'exploitation des failles consiste à tester les vulnérabilités identifiées pour évaluer la sécurité du système.



9

Législation sur la cybersécurité

Règles pour les entreprises

Les législations sur la cybersécurité établissent des règles claires que les entreprises doivent suivre pour protéger les informations sensibles.

Protection des données

Les lois de cybersécurité obligent les entreprises à mettre en œuvre des mesures efficaces pour protéger les données des utilisateurs contre les cybermenaces.

Sécurité des systèmes d'information

Ces lois jouent un rôle crucial pour garantir la sécurité globale des systèmes d'information dans un environnement numérique de plus en plus complexe.



10



Normes et certifications pour les hackers éthiques

Certifications reconnues

Les hackers éthiques peuvent obtenir des certifications telles que CEH et OSCP, témoignant de leur compétence professionnelle.

Expertise et conformité

Ces certifications démontrent l'expertise des hackers éthiques et leur conformité aux normes établies par l'industrie.

11



Réglementations internationales et conformité

Importance du RGPD

Le RGPD en Europe protège les données personnelles et impose des règles strictes sur leur gestion.

Conformité nécessaire

La conformité aux réglementations internationales est essentielle pour éviter des sanctions financières et protéger la réputation.

Rôle des hackers éthiques

Les hackers éthiques jouent un rôle clé dans la protection des données tout en respectant les réglementations en vigueur.

12

Tests d'intrusion et évaluation des vulnérabilités

Simulations d'attaques

Les tests d'intrusion impliquent des simulations d'attaques pour évaluer les défenses d'un système informatique.

Identification des vulnérabilités

Ce processus aide à identifier les vulnérabilités critiques dans les systèmes avant qu'une attaque réelle ne se produise.

Prévention des attaques

Les tests d'intrusion sont essentiels pour renforcer la sécurité et prévenir les cyberattaques potentielles.



13

Code de conduite et bonnes pratiques

Intégrité des hackers éthiques

Les hackers éthiques doivent agir avec intégrité et respect envers les données qu'ils manipulent.

Confidentialité des données

Il est crucial que les hackers éthiques respectent et protègent la confidentialité des données qu'ils examinent.

Lignes directrices du code de conduite

Un code de conduite fournit des directives claires pour aider les hackers à naviguer éthiquement dans leur travail.

14

Les Plateformes De Bug Bounty

Rôle des plateformes

Les plateformes de bug bounty facilitent la connexion entre entreprises et chercheurs en matière de sécurité. Elles aident à identifier et à corriger les vulnérabilités de manière proactive.

Gestion des rapports

Ces plateformes gèrent la soumission des rapports de vulnérabilités, rendant le processus plus structuré et accessible pour tous les acteurs impliqués.

Évaluation et récompenses

Elles évaluent les vulnérabilités soumises et distribuent des récompenses aux chercheurs, encourageant ainsi la participation au programme de bug bounty.



15

Responsabilités légales et éthiques

Obtention de l'autorisation

Les hackers éthiques doivent toujours obtenir l'autorisation préalable avant de tester ou d'évaluer la sécurité d'un système.

Normes éthiques

Ils doivent adhérer à des normes éthiques strictes pour s'assurer qu'aucun dommage n'est causé pendant leurs tests.



16



Défis et dilemmes éthiques

Signalement des failles

Les hackers éthiques doivent décider s'ils doivent signaler les vulnérabilités découvertes lors de leurs tests, ce qui pose un dilemme moral.

Impact sur la confiance

La décision de signaler ou non peut affecter la confiance et la réputation des hackers éthiques dans l'industrie.

Équilibre éthique

Les hackers éthiques doivent trouver un équilibre entre la responsabilité professionnelle et leurs implications éthiques.

17

Tendances actuelles en cybersécurité

Demande de hackers éthiques

Il y a une demande croissante pour les hackers éthiques, qui jouent un rôle essentiel dans la protection des systèmes informatiques.

Impact de l'intelligence artificielle

Les technologies émergentes comme l'intelligence artificielle transforment le paysage de la cybersécurité, améliorant la détection des menaces.



18

L'avenir du hacking éthique et des réglementations

Évolution des menaces numériques

Les menaces numériques continuent d'évoluer, ce qui nécessite une adaptation constante des pratiques de hacking éthique pour répondre à ces défis.

Réglementations et lois

Le développement de réglementations entourant le hacking éthique est essentiel pour garantir que les pratiques respectent des normes éthiques et légales.

Pratiques de hacking éthique

L'avenir du hacking éthique dépendra de l'innovation dans les pratiques, visant à améliorer la sécurité tout en respectant les lois établies.



19

Conclusion

Importance du hacking éthique

Le hacking éthique est devenu indispensable pour protéger les systèmes numériques contre les cybermenaces croissantes.

Cadre légal et éthique

Le cadre légal et éthique est essentiel pour assurer que les hackers éthiques agissent dans le respect des lois et de la moralité.

Techniques de hacking éthique

Les techniques employées par les hackers éthiques sont cruciales pour identifier les vulnérabilités des systèmes et renforcer leur sécurité.

20