

# VEILLE TECHNOLOGIQUE

---



## L'ETHICAL HACKING

---

Par Marville Dovan BTS Services informatiques aux organisations  
option B solutions logicielles et applications métiers (SIO SLAM)

---



## Table des matières

<b>Qu'est-ce que c'est un hacker éthique ?.....</b>	<b>3</b>
L'origine des hackers.....	3-4
Les différents hackers et quels sont leurs rôles ?.....	5
<b>Les outils les plus utilisé par les hackers.....</b>	<b>6</b>
Kali linux.....	6
Flipper Zero.....	6
Raspberry PI.....	6-7
Kali NetHunter.....	7
<b>Les moyens que j'utilise pour suivre l'actualité.....</b>	<b>7</b>
Krebs On Security.....	7
The Hacker News.....	7
Instagram.....	8
Threapost.....	8
Owasp Top 10.....	8
Dark Reading.....	8

# INTRODUCTION

Dans l'univers de la technologie, le terme "hacker" évoque souvent des images de menaces, d'intrusions malveillantes et de cybercriminalité de la part d'un individu mal intentionné. C'est exact, ça peut être le cas effectivement. Cependant, il est essentiel de comprendre que le monde du hacking n'est pas un territoire exclusivement réservé aux acteurs mal intentionnés. Au contraire, l'ethical hacking, ou hacking éthique en français, représente une facette cruciale de la sécurité informatique, prônant la bienveillance et la protection des systèmes contre les attaques potentielles.

Dans cette veille technologique dédiée à l'ethical hacking, nous explorerons les principes fondamentaux de cette pratique.

## Qu'est-ce que c'est un hacker éthique ?

### I. L'origine des hackers

Les premiers hackers notables de l'histoire informatique étaient souvent des passionnés de technologie qui ont contribué au développement des premiers ordinateurs et des réseaux. Voici quelques figures emblématiques :

\* Alan Turing (1912-1954) : Mathématicien et logicien britannique, Turing a joué un rôle crucial pendant la Seconde Guerre mondiale en déchiffrant les codes ennemis allemands. Il est souvent considéré comme le père de l'informatique et a jeté les bases du concept de machine universelle, qui a grandement influencé le développement ultérieur des ordinateurs.

\* Richard Stallman (né en 1953) : Programmeur et militant du logiciel libre, Stallman a fondé le projet GNU (GNU's Not Unix) dans les années 1980, visant à créer un système d'exploitation entièrement libre. Sa philosophie du logiciel libre a eu une influence significative sur la communauté hacker et le développement de logiciels open source.

\* Kevin Mitnick (né en 1963) : Mitnick était un hacker notoire dans les années 1980 et 1990. Il a été impliqué dans diverses activités

de piratage, mais après avoir été capturé, il est devenu un consultant en sécurité et un défenseur de l'éthique hacker.

\* Linus Torvalds (né en 1969) : Créateur du noyau Linux, Torvalds a été un acteur majeur dans le développement du système d'exploitation Linux, qui est largement utilisé dans le domaine du serveur et de l'informatique embarquée.

L'origine du terme "hacker" remonte aux premières décennies de l'informatique. Initialement, le mot "hacker" désignait simplement un individu passionné par la compréhension des systèmes informatiques et la recherche de solutions créatives à des problèmes complexes. Ces premiers hackers étaient souvent des adeptes de la programmation et de l'exploration des possibilités offertes par les nouveaux ordinateurs.

Cependant, au fil du temps, la perception du terme a évolué, et il a été associé à des activités illégales, notamment le piratage informatique. Les médias ont souvent dépeint les hackers comme des individus mal intentionnés cherchant à exploiter des failles de sécurité pour des gains personnels ou pour causer des dommages.

C'est dans ce contexte que le concept de "hacker éthique" a émergé. Les hackers éthiques, également appelés "pentesters" (testeurs d'intrusion) ou "professionnels de la sécurité", ont adopté les compétences techniques des hackers traditionnels, mais avec une intention différente. Leur objectif est de mettre en lumière les vulnérabilités des systèmes informatiques de manière légale et constructive. Les hackers éthiques travaillent souvent en collaboration avec des organisations pour identifier et corriger les faiblesses de leurs infrastructures, renforçant ainsi la sécurité globale.

## II.Les différents hackers et quels sont leurs rôles ?

Le terme "hat" dans le contexte du hacking est souvent utilisé pour décrire les différentes attitudes et intentions des individus impliqués dans des activités liées à la sécurité informatique. Ces termes sont basés sur les couleurs des chapeaux, une métaphore utilisée pour représenter les différentes perspectives. Voici quelques-uns des principaux types de "hat" dans le hacking :



**White Hat (Chapeau Blanc)** : Les "chapeaux blancs" représentent l'éthique et la légalité dans le hacking.



**Black Hat (Chapeau Noir)** : À l'opposé, les "chapeaux noirs" incarnent la face obscure du hacking. Leur objectif est souvent malveillant, cherchant à exploiter des failles de sécurité à des fins personnelles ou nuisibles.



**Grey Hat (Chapeau Gris)** :

Naviguant entre le bien et le mal, les "chapeaux gris" défient parfois la légalité pour tester des systèmes sans autorisation.



**Red Hat (Chapeau Rouge)** :

Les "chapeaux rouges" sont les experts en tests de pénétration, simulant des attaques réalistes pour évaluer la résilience des systèmes.



**Chapeau Bleu (Blue Hat)** :

Les "chapeaux bleus" sont les gardiens de la sécurité au sein d'une organisation qui est chargée de vérifier l'absence de bogues et de corriger d'éventuels exploits avant le lancement d'un système d'exploitation sur le marché.



**Chapeau Vert (Green Hat)** : Enfin, les "chapeaux verts" peuvent représenter des novices ou des apprenants dans le monde du hacking.

## Les différents outils les plus utilisé par les hackers

### I.Kali linux



Kali Linux est une distribution de systèmes d'exploitation basée sur Debian, spécialement conçue pour les tests de sécurité informatique et la pénétration. Elle est développée par Offensive Security, une entreprise spécialisée dans la formation en sécurité informatique. Kali Linux est largement utilisée par les professionnels de la sécurité, les chercheurs en sécurité, les pentesteurs (testeurs d'intrusion) et les hackers éthiques pour effectuer des évaluations de sécurité sur les systèmes informatiques. Kali Linux est livré avec une vaste collection d'outils dédiés aux tests de pénétration. Ces outils couvrent divers domaines tels que la surveillance réseau, l'analyse des vulnérabilités, l'ingénierie sociale, la récupération de mot de passe, et plus encore. [Nmap](#)

### II.Flipper Zero

Un petit gadget très intéressant est le Flipper Zero qui est un multi-outil portable pour les pentesters dans un corps semblable à un jouet. Il permet de pirater des éléments numériques, tels que des protocoles radio, des systèmes de contrôle d'accès, du matériel informatique, des télévisions etc. Il est entièrement open source et personnalisable, vous pouvez donc l'étendre comme vous le souhaitez.



### III.Raspberry PI

Le Raspberry Pi est une série d'ordinateurs monocartes peu coûteux et développés par la fondation Raspberry Pi. Ces ordinateurs sont conçus pour promouvoir l'éducation en informatique et fournir une

plateforme pour des projets de bricolage. Les cartes Raspberry Pi sont de la taille d'une carte de crédit et intègrent un système sur une puce (SoC) de Broadcom, divers ports d'entrée/sortie et en charge différents systèmes d'exploitation. Pour les hackers, cet outil peut permettre les attaques par force brute, l'espionnage, attaques de déni de service (DDoS), Intrusion dans les réseaux...



#### IV.Kali NetHunter

Kali NetHunter est une plateforme de test de pénétration pour Android développée par l'équipe Offensive Security, la même équipe derrière Kali Linux. Elle est conçue pour les appareils mobiles et permet aux professionnels de la sécurité et aux passionnés d'utiliser la puissance de Kali Linux sur leurs smartphones ou tablettes. Kali NetHunter est livré avec une variété d'outils et de fonctionnalités spécialement conçus pour les tests de pénétration sur mobile.



#### Les moyens que j'utilise pour suivre l'actualité

Pour suivre l'actualité sur le hacking j'utilise :

**Krebs on Security** : <https://krebsonsecurity.com>

Tenu par le journaliste Brian Krebs, ce site couvre une variété de sujets liés à la sécurité informatique.

**The Hacker News** : <https://thehackernews.com>

C'est une source d'informations sur les dernières actualités en matière de cybersécurité, de piratage éthique et de technologies.

**Instagram** : <https://www.instagram.com>

Réseau social où je suis les experts en cybersécurité comme (David Bombal, Network Chunk, CyberTech Society...).

**Threapost** : <https://threatpost.com>

Couvrant les actualités en cybersécurité, Threatpost propose des articles, des analyses et des rapports sur les dernières menaces.

**OWASP TOP 10** : <https://owasp.org>

Ou est publié régulièrement une liste des dix principales vulnérabilités de sécurité des applications web. Cette liste est mise à jour pour refléter les nouvelles menaces et vulnérabilités émergentes.

**Dark Reading** : <https://www.darkreading.com>

Un site Web qui propose des actualités, des analyses et des articles sur la sécurité informatique, y compris des sujets tels que le pentest, les vulnérabilités, et les meilleures pratiques en matière de sécurité.