Ludovic HAVARD

INFOS CONTACT

Linkedin :
https://www.linkedin.com/in/ludovic-havard-541ba4231

Porfolio :
https://havard-ludovic.github.io/Porfolio/

LANGUES

Anglais (B2) Allemand (B1)

FORMATION

HACK THE BOX ACADEMY
Techniques de cybersécurité offensive
Job Role Path « Penetration Tester » complété

2024 – ECE PARIS-LYON – 75015 Paris
Ecole d'ingénieurs généralistes et hightech - Majeure cybersécurité

Sept-Déc 2021 : Edimbourg
Cours d'IA, d'Analyse de données et de Software Engineering

2019 – LYCEE CARNOT – 75017 Paris
Baccalauréat S – Mention Assez Bien

CENTRES D'INTERETS

- Veille technologique : suivi régulier de l'actualité cybersécurité via le magazine MISC et LinkedIn.
- Stratégie & réflexion (échecs)
- Discipline & persévérance (tennis)

CONSULTANT CYBERSECURITE OFFENSIVE

Ingénieur en cybersécurité spécialisé en pentests. Passionné par les audits techniques et l'analyse de vulnérabilités, j'aborde chaque mission avec curiosité et rigueur pour sécuriser au mieux les systèmes d'informations. Je renforce mes compétences quotidiennement via les CTF et le Bug Bounty.

COMPETENCES

PENTEST & SECURITE

- **Distributions :** Kali Linux, Parrot OS
- **Reconnaissance :** Nmap, Ffuf, Smbmap
- **Analyse & Exploitation :** Metasploit, Burp Suite, SQLmap, Wireshark, LinPEAS, Sn1per, XSStrike
- **Bruteforce :** Hashcat, John the Ripper, CrackMapExec, Hydra
- **Site Web**: Gtfobin, Crackstation, Revshell
- **Post-exploitation :** Netcat, Mimikatz, BloodHound, Evil-WinRM, Impacket

STACK TECHNIQUE & OUTILS

- C, C++, C#, Java, Python, Bash, HTML, PHP, JavaScript, React, Next.js, SQL, NoSQL
- Git, Visual Studio, VS Code, Power Apps, Power BI, Office (Excel avancé)

EXPÉRIENCES

SECURITE OFFENSIVE, BUG BOUNTY & CTF

Depuis 2023 | PROJET PERSONNEL

Bug bounty : activité quotidienne sur HackerOne / Vulnérabilités Web trouvées et validées / Rédaction de rapports incluant : type de vulnérabilité, niveau de criticité, risques associés, et propositions de remédiation
(Profil: https://hackerone.com/0daylight)

CTF & challenges techniques : résolution régulière de machines sur Hack The Box (pseudo : lud7515) et Root Me (www.root-me.org/lud7515)

Compétitions : participation aux événements comme HackDay, ComCyber et UofTCTF, organisés par des communautés de cybersécurité.

Audit technique : exploitation du site vulnérable OWASP Juice Shop (tests d'intrusion Web), rédaction du rapport associé

GESTION DES VULNERABILITES - Mission chez un client international

Février – Août 2024 | HEADMINDS PARTNERS – Paris (75)

- Suivi des vulnérabilités des ressources Azure (central, régions et leurs échanges)
- Création de dashboards de suivi des audits, remédiations et budgets (Power BI)
- Amélioration de l'application de suivi des régions (Power Apps)
- Scripts Python pour automatiser des activités récurrentes

CERTIFICATS CRYPTOGRAPHIQUES – Projet d'archivage numérique

Mai – Août 2023 | BANQUE DE FRANCE – Paris (75)

Production de certificats X509 sur des supports physiques / Gestion du projet d'archivage numérique des demandes de certificats / Refonte de statistiques

PHISHING - Mise en œuvre d'une application de campagnes de phishing

Septembre 2022 – Avril 2023 | LGM – Vélizy (78)

Projet en partenariat avec la société : Génération des mails avec un lien hypertexte / Création de fausses pages de connexion avec les pages pédagogiques associées / Affichage des résultats de la campagne (nombre de mails envoyés, de clics sur le lien et de mots de passe entrés)