

ht8440@proton.me · Paris, France · 34zy.red
github.com/34zY · huggingface.co/34zY
linkedin.com/in/hamza-t-355765314

PROFIL

Senior penetration tester et ingénieur en sécurité offensive avec plus de 4 ans d'expérience en web, Active Directory, embarqué / IoT et OT/ICS, sans fil et systèmes IA. Mène les évaluations de bout en bout, en boîte blanche comme en boîte noire, avec des rapports directement adressés aux équipes techniques et aux services conformité. Spécialiste sécurité produit en environnements réglementés : EN 18031 (RED delegated act) et préparation CRA, sécurité IoT ETSI EN 303 645, IEC 62443 IACS/OT, audits ANSSI CSPN et FDA. Tests sans fil sur produits connectés (WiFi WPA2/WPA3-EAP, BLE, RF). Certifié OSCP et CRTP, auteur du PoC CVE-2025-52970. Chaque finding démontré par un proof-of-concept fonctionnel.

EXPÉRIENCE

Expert sécurité / Testeur d'intrusion

Mars 2025 - Présent

BYCYB (ex CRYPTON.IT, filiale LNE) · audit cyber, certification & formation · Paris



- Évaluations multi-domaines (boîte blanche, grise et noire)** : web et API, Active Directory, Android/iOS, IoT/OT/ICS/SCADA et appareils médicaux ; UART/I2C/JTAG/USB, ingénierie inverse de firmware et mises à jour.
- Sécurité sans fil & RF** : WiFi (WPA2/WPA3-EAP), Bluetooth Low Energy, analyse spectrale RF, injection de paquets et tests de protocoles sans fil sur produits connectés.
- Conformité produit & industrielle** : évaluations de conformité EN 18031 (RED delegated act) et préparation CRA, sécurité IoT ETSI EN 303 645, évaluations IEC 62443 IACS/OT, audit ANSSI CSPN et registre cash-register LNE.
- Recherche sécurité offensive & LLM** : moteurs d'inférence locaux, optimisation des modèles, fine-tuning et évaluation ; tests OWASP GenAI (prompt injection, guardrails, fuites de système-prompt, workflows agent/MCP).
- Livraison senior** : scopes et mène les évaluations de bout en bout, du kick-off au retest, avec reporting direct vers les parties prenantes techniques et conformité ; outillage Python custom et 79 findings sur cinq engagements 2026 (14 critiques).
- Transfert de compétences** : formations internes et externes sur le reverse engineering de malwares Android, le pentest LLM/MCP, la migration EN 18031 vers CRA, et la sécurité IACS/OT/SCADA.

Expert sécurité / Testeur d'intrusion

Mars 2025 - Juil. 2025

CRYPTON.IT - consulting cybersécurité · Paris · équipe rebrandée BYCYB en août 2025



- Consulting cybersécurité sur web, Active Directory et systèmes embarqués/IoT** : tests boîte blanche et grise, exploits Python custom et rapports.
- Fondamentaux IoT & conformité** : préparation EN 18031, évaluation de dispositifs IoT et premiers tests WiFi/BLE sans fil sur produits connectés.

Testeur d'intrusion en alternance

Sept. 2021 - Juil. 2024

Département des Hautes-Alpes - Gap

- Pentest web et Active Directory en boîte grise**, exploits Python/HTML/JavaScript custom et rapports.
- 22 zero-days** sur applications internes ; développement de malwares (Python/C#/ASM), contournement EPP/EDR, tests BOF et détection MDE.
- Exercice red-team autorisé** : intrusion physique, déploiement de 70+ clés USB et 30 % de rappel ; Cyberwatch gestion de vulnérabilités et gouvernance ISO 27002.

RÉSULTATS SÉLECTIONNÉS

- Secrets mobile vers Firebase**, exposition backend RH et chaîne de prise de compte (finding client critique, sanitisé).
- IDOR/BOLA multi-domaine à grande échelle** : enregistrements utilisateurs, employés et documents exposés (critique, finding client sanitisé).
- Firmware de borne de recharge non signé**, accès debug ouvert et commandes privilégiées non authentifiées.
- Escape kiosk workstation médicale** et faiblesse d'analyse de jeton pré-authentification.
- Bypass SAML assertion** contournant l'authentification WordPress ; **bypass U-Boot / HAB** menant à un RCE non authentifié.
- Diffusions publiques** incluant endpoint REST WordPress non authentifié (ElementsKit Lite) et chaîne reflected XSS sur Dorksearch.
- Évaluations 2025** : DoS parsing DICOM non authentifié, persistance AdminSDHolder, stored XSS via validation upload et broken access control dans workflows enterprise.

OUTILS OPEN-SOURCE & CONTRIBUTIONS

Outils : [GitHarvest3r](#) · [Nerv0usR4bbit](#) · [Ping-Of-Death](#) · [Soft-Script-V.2](#). Exploit Ruby Metasploit (2021) : [Microsoft Office Word MSHTML RCE](#). Contributions : [CrackEverything6 \(2023\)](#) · [malicious-wordpress-plugin \(2024\)](#).

Laboratoire LLM local construit et maintenu pour déploiement de modèles, évaluation de moteurs d'inférence et recherche sécurité : quantification et optimisation performance, fine-tuning, benchmarking, harnois d'évaluation reproductible et workflows agent/outils. Étudié et testé les vulnérabilités IA incluant prompt injection, injection indirecte, fuite de système-prompt, bypass guardrail, usage dangereux d'outils, exfiltration de données et sécurité MCP/agent. Outillage offensif développé et expériences répétables pour modèles locaux, appliqué à la recherche de vulnérabilités et analyse défensive. Fine-tuné de Kairos, modèle de décision 0,3 B Apache-2.0 pour le scoring de décision zéro-génération et le routage sémantique en déploiement cascade, [disponible sur Hugging Face](#). Étude technique publique : analyse integer-overflow dans Apple CoreGraphics (iOS / macOS), [CVE-2026-86950](#).

COMPÉTENCES

Web & API	Burp Suite Pro, SQLMap, ffuf, Nuclei, OWASP WSTG
Active Directory	BloodHound, Mimikatz, Rubeus, Impacket, PingCastle, PurpleKnight
Embarqué / IoT / OT	UART, I2C, JTAG, RS232, binwalk, Ghidra, U-Boot, IEC 62443
Sans fil / RF	WiFi, RF, analyse spectrale, protocoles sans fil, injection de paquets
Red Team	Metasploit, Havoc, BOF, SysWhispers, Hell's Gate, contournement EPP/EDR
IA / LLM	Moteurs d'inférence locaux, optimisation, quantification, fine-tuning, évaluation, OWASP Top 10 GenAI, MCP, Kairos (propre modèle de décision 0,3 B fine-tuné, huggingface.co/34zY/Kairos)
Recon / threat intel	Subfinder, httpx, Shodan, MITRE ATT&CK, recherche CVE et zero-day
Conformité / normes	EN 18031 (RED), ETSI EN 303 645, IEC 62443, ANSSI CSPN, préparation CRA, ISO 14971 / IEC 62304
Langages	Python, PowerShell, Bash, C, C#, JavaScript, x86-64 ASM

CERTIFICATIONS



OSCP · Offensive Security, 2024



CRTP · Certified Red Team Professional, 2025



Red Hat · System Administration II & III, 2022



PentesterLab · HTTP, Essential, White, Blue, Serialize, 2023

FORMATION

ESEE-IT - école d'ingénieur (Paris) - Ingénieur Cybersécurité, 2021-2024

Lycée Philippe de Girard - BTS Systèmes Numériques, Électronique & Communications, 2019-2021

LANGUES

Français (maternel) · Anglais (professionnel) · Espagnol et Allemand (basique)