Thimoty LAY

Pentester | Consultant en cybersécurité | Analyste SOC

Mail : rattack@thimoty.com

Root-Me (1060 points) : Rattack | **Github** : Rattack-Hack | **Linkedin :** LAY Thimoty | **Site :** thimoty.com

PROFIL

Fort d'une expérience de 5 ans en alternance combinant administration système et sécurité offensive/défensive, je souhaite approfondir mes compétences dans le domaine et apprendre des autres. Passionné par la culture du challenge et le dépassement de soi (Root-Me, CTF). Expérience en tests d'intrusion, déploiement SIEM, analyse SOC, hardening AD, sécurisation et administration Linux/Windows.

EXPÉRIENCE PROFESSIONNELLE

Consultant en cybersécurité et administrateur système et réseau - Performance Conseil Informatique, Savenay, 05/2021 – Présent

- **Contrat d'alternance** (fin prévue en décembre 2026).
- **Pentesting :** Réalisation de tests d'intrusion internes en greybox : identification, exploitation et remédiation des vulnérabilités.
- **Sécurité Défensive (SOC) :** Déploiement de 3 SIEM Wazuh pour un centre opérationnel de sécurité.
- **Audits & Hardening :** Audit de 2 Active Directory via Pingcastle, application des mesures de hardening Windows, application des mesures de hardening Linux sur des serveurs en interne.
- **Sécurisation Réseau :** Audit et remédiation de pare-feu (appliance OPNsense).
- **Protection Web & Périmétrique :** Sécurisation de 5 reverse proxies avec WAF (Naxsi, Crowdsec) et intégration d'IPS (Crowdsec).

FORMATIONS & CERTIFICATIONS

- **Expert en sécurité digitale (BAC +5 en cours, niveau 7, RNCP 36399, en alternance) –** En cours / 08/2026 - ENI École Informatique, Nantes
- **Administrateur système et réseau (BAC +4, niveau 6, RNCP 41776, en alternance)** - 04/2025 - ENI École Informatique, Nantes
- **Certifications techniques :** CSNA Stormshield – 08/2024 - ENI École Informatique, Nantes | CCNA Academy - 05/2024 - ENI École Informatique, Nantes | Crowdsec Fundamentals – 07/2023 - Crowdsec Academy

COMPÉTENCES

- **Compétences techniques : Exploitation de vulnérabilités** (Nmap, Burp Suite, BloodHound, OpenVAS, Responder, NetExec) dans des environnements Windows, Linux et Docker - **Analyse de surface d'attaque et reporting sécurité** avec les matrices OWASP, MITRE ATT&CK, référentiels ANSSI - **Scripting** (Python, Bash, PowerShell) - **Analyse d'alertes** en environnement Windows et Linux (SIEM Wazuh, IPS/IDS Crowdsec, WAF Naxsi).
- **Environnements techniques :** Linux (Debian, Ubuntu et Red Hat), Windows, Docker, Active Directory, Wazuh, Crowdsec, Naxsi, OPNsense, Proxmox, VMware, Python, Bash, PowerShell, FreeBSD, Azure/Entra ID, Microsoft 365, Ansible.
- **Soft Skills :** Travail en équipe, esprit d'analyse et de synthèse, curiosité, rédaction de rapports techniques.
- **Langues :** Français (Langue maternelle) - Anglais (B2 - Avancé), Espagnol (B2 - Avancé), Portugais (A2 - Débutant).