

NOLAN PUJOL

ETUDIANT EN INFORMATIQUE

CONTACT

06.85.80.21.08

nolanpujol.pro34@gmail.com

Villetelle

portfolio-nolan-pujol.vercel.app

Permis B

COMPÉTENCES

DEVELOPPEMENT & DATA

- Java & Spring Boot
- JS/TypeScript, Vue.js, PHP
- Python + (FAST api)
- SQL, PL/SQL & NoSQL

RÉSEAU & SÉCURITÉ

- BurpSuite,Nikto,Metasploit
- Wireshark,Nmap,PfSense
- GNS3 & VirtualBox,OpenVpn

DEVOPS & INFRA

- Docker
- Ansible & Terraform
- Bash
- N8N, Opencode

LANGUAGES

- Anglais B2
- Espagnol B2

CENTRES D'INTÉRÊT

Cybersécurité	En activité sur TryHackMe Bug Bounty sur Hackerone
Sport	Handball, Squash
Musique	Piano soliste et en groupe, Production sur FL studio

PROFIL

Actuellement en BUT Informatique (parcours DACS), je souhaite poursuivre mes études en intégrant à la rentrée prochaine une formation de niveau Bac+5 spécialisée en cybersécurité, en alternance. Selon mon admission définitive, ce cursus sera réalisé au CNAM (24 mois) ou à CESI Mauguio (36 mois). Mon objectif est de mettre ma polyvalence technique et mon expérience terrain au profit de projets concrets en entreprise tout en approfondissant mes compétences académiques en cybersécurité.

MES EXPÉRIENCES

Stagiaire Analyste Cybersécurité (ENGIE GREEN) AVRIL 2026 – AOÛT 2026

- Développement et déploiement d'une sonde d'audit réseau open source permettant la réalisation de scans distants des parcs industriels Engie via VPN, l'inventaire automatisé des équipements et la collecte de données techniques dans le cadre des projets de migration vers des infrastructures Modern Network et Cloud.
- Conception d'un laboratoire de simulation des environnements industriels Engie sous VirtualBox et GNS3, intégrant une segmentation réseau (VLAN, Trunk, DMZ), un pare-feu pfSense, un proxy Squid SSL ainsi qu'une infrastructure Active Directory (AD, DNS, GPO).
- Participation à l'élaboration des cahiers des charges dans le cadre des projets de migration de serveurs métier et d'infrastructures SD-WAN, avec identification des besoins techniques, des outils et des parties prenantes.
- Réalisation d'audits techniques et de sécurité, incluant l'analyse des risques, la cartographie des actifs et la production de la documentation associée aux projets de migration.

Plateforme sécurisée multi-services avec authentification centralisée 2025 - 2026

- Déploiement & Services : Déploiement conteneurisé (Docker) d'outils collaboratifs et DevOps (Nextcloud, GitLab) avec automatisation des configurations.
- Sécurité & Réseau : Architecture hybride (LAN et Tunnels Cloudflare) exposée via Traefik (Reverse Proxy) et protégée par un WAF (Web Application Firewall).
- Gestion des Identités (IAM) : Authentification centralisée via Keycloak et annuaire LDAP (SSO, 2FA, intégrations OAuth/SAML multi-services).
- Continuité & Résilience (PRA/PCA) : Sauvegardes automatisées, chiffrées et réplication multi-postes avec Docker Swarm et Gluster Fs pour le système de fichiers distribué.

Système de vote sécurisé avec chiffrement homomorphe 2024 - 2025

- Architecture client-serveur (Java Spring Boot / Vue.js) avec communication TLS et chiffrement homomorphe ElGamal
- Déchiffrement distribué via PZK pour assurer confidentialité et intégrité des votes Interfaces distinctes : électeurs, administrateurs, scrutateurs
- Déploiement automatisé avec : Docker pour la conteneurisation CI/CD GitLab pour le build et la mise en production

STAGIAIRE INFORMATICIEN – RADIO AVIVA JANVIER 2025 – MARS 2025

- Sécurité Offensive & Gouvernance : Sécurisation des données internes et externes via des tests d'intrusion (pentest), identification et correction de failles de sécurité, contrôle des versions des outils utilisés et mise en place de nouveaux processus de sécurité ainsi que de sessions sécurisées sur postes Windows.
- Développement & Automatisation : Développement d'applications d'automatisation Java Spring Boot avec l'API Google, applications conteneurisées et déployées sur serveurs internes

Pentest : TryHackMe - HackerOne - YesWeHack EN CONTINUE

- Pratique régulière (Labs/CTFs) : Reconnaissance et exploitation via Nmap, Metasploit, Burp Suite. Automatisation des phases de scan et exploitation d'agents IA pour assister la remédiation et l'analyse de vulnérabilités.
- Bug Bounty : Analyse de périmètre, découverte de sous-domaines, tests d'applications web et identification de failles logiques/systèmes IA. Rédaction de rapports techniques de vulnérabilités.

EDUCATION

BUT Informatique (obtenu) – Parcours Déploiement d'Applications Communicantes et Sécurisées (DACS) 2023 - 2026

BAC Terminale scientifique (NSI/MATHS) mention bien 2022 - 2023

Diplôme national du brevet 2019 - 2020