

Pluvigner, 56330

06 73 66 12 84

roystraque@protonmail.com



ULMANN JONATHAN

PENTESTER JUNIOR – PROFIL AUTODIDACTE

FORMATION

2014 - (2SIA) Administration systèmes & réseaux
bases systèmes, réseaux et sécurité

Formation Autodidacte En cybersécurité et
administration système

EXPERIENCE PROFESSIONNELLE

2014 – Aujourd'hui

indépendant – service techniques & informatiques

- Mise en place et sécurisation de réseaux d'entreprise
- Administration de systèmes Linux et Windows
- Déploiement et configuration de services (web, accès distants, serveurs internes)
- Configuration de firewall, règles de filtrage et segmentation réseau
- Sécurisation des accès (SSH, services exposés, limitations IP)
- Interventions sur des environnements variés (PME, structures indépendantes)

PROJETS & LABORATOIRES PERSONNELS

- Conception et déploiement d'infrastructures virtualisées vulnérables
- Réalisation d'audits de sécurité complets en environnement de laboratoire
- Exploitation de vulnérabilités et production de preuves de compromission
- Mise en œuvre de mesures de durcissement post-audit
- Rédaction de rapports d'audit structurés (méthodologie, risques, recommandations)

 <http://youtube.com/@casagency6057>

 <https://gitlab.com/users/roystraque/projects>

PENTEST RAPPORT AUDIT ICI

PROFIL

Pentester junior autodidacte, spécialisé dans l'audit de sécurité des infrastructures réseau, systèmes et applications web. Approche méthodologique complète intégrant reconnaissance, énumération, exploitation, post-exploitation et recommandations. Solide compréhension des mécanismes défensifs (segmentation réseau, filtrage, durcissement), permettant une analyse réaliste des risques et des impacts. Habitué aux environnements virtualisés et aux laboratoires de test.

COMPÉTENCES TECHNIQUES

Pentest & Sécurité

- Reconnaissance passive et active (OSINT)
- Énumération de services, versions et surfaces d'attaque
- Exploitation de vulnérabilités web, réseau et – systèmes
- Post-exploitation et preuves de compromission
- Rédaction de rapports d'audit et recommandations correctives

Vulnérabilités

- SQL Injection (classique)
- Cross-Site Scripting (XSS)
- Faiblesse d'authentification
- Mauvaises configurations réseau et services exposés
- Exposition d'informations sensibles et fuites de configuration

Réseaux & infrastructure

- TCP/IP, UDP, NAT, Routage
- Segmentation réseau et sous-réseaux
- Firewall, filtrage IP, limitation d'accès aux services
- Notion IDS / Détection d'intrusions

Systèmes & virtualisation

- Linux & Windows (administration, services, permissions)
- Active Directory (bases)
- Proxmox, VMware ESXi, VMware Workstation, VirtualBox
- Mise en place de laboratoires virtualisés
- Installation et configuration de firewall IPfire, Pfsense

Outils

- Nmap, Metasploit, Burp Suite
- SQLmap
- Hydra, John The Ripper, Hashcat
- Wireshark (analyse basique)
- Bash, Python (scripts utilitaires et automatisation)