Yasser EL KARCH

Ingénieur Cybersécurité

Paris, France | +33 7 59 27 50 94 | yasser.elkarch@gmail.com
linkedin.com/yasser-el-karch | github.com/YasserElkarch

À Propos

Ingénieur en Réseaux et Télécommunications, étudiant en Master 2, avec une spécialisation affirmée en sécurité offensive. Certifié eJPTv2, PEH et EHE, doté d'une expérience en tests d'intrusion, audits de sécurité et protection des systèmes d'information. Actuellement à la recherche d'un **stage de fin d'études de 6 mois a partir de Mars** afin de mettre à profit mon expertise pour la détection, l'analyse et la prévention des vulnérabilités.

Études et formations

Université Paris Saclay — Orsay, France
Master 2 Professionnel en Réseaux et Télécoms — *2025 – Présent*

- **Cours pertinents :** Sécurité réseaux et systèmes, Virtualisation Réseau (SDN, NFV), Python pour les réseaux, Internet of Things, Coeur du réseaux

École Nationale des Sciences Appliquées (ENSA) — Tanger, Maroc
Diplôme d'Ingénieur en Génie des systèmes de Télécommunications et Réseaux — *2018 – 2024*

Expériences professionnelles

La Banque Populaire — Dec 2024 – Août 2025
Auditeur sécurité SI — *Casablanca, Maroc*

- Réalisation de +10 audits techniques sur Active Directory et Microsoft Exchange, incluant revue de configuration, détection de mauvaises pratiques et tests d'intrusion internes.
- Conduite de tests d'intrusion applicatifs (OWASP Top 10) sur plusieurs applications critiques, menant à l'identification de vulnérabilités à impact élevé (XSS, RFI, auth bypass).
- Exploitation contrôlée des failles via Burp Suite, Nessus, SQLmap, suivie de la rédaction de rapports exécutifs et techniques avec priorisation des risques
- Évaluation de la posture de sécurité selon ISO 27001 et COBIT 5, contribuant à une réduction mesurable du risque cyber.
- Suivi de 70 % des plans de remédiation via eFront ERM jusqu'à validation des correctifs.

La Banque Populaire — Fév 2024 – Juin 2024
Pentester & Sécurité Active Directory - stage — *Casablanca, Maroc*

- Conception et déploiement d'un lab Active Directory, simulant un environnement d'entreprise réel pour tests d'intrusion internes.
- Réalisation de campagnes complètes de pentest AD : énumération, exploitation d'abus de privilèges, élévation locale et compromission de domaine.
- Identification et validation de chemins d'attaque critiques (Kerberoasting, ACL abuse, lateral movement)
- Rédaction de rapports techniques détaillés incluant preuves d'exploitation (PoC) et recommandations de durcissement AD.
- **Initiative personnelle en complément du projet :** déploiement autonome de **Tenable Identity Exposure** pour l'identification automatisée de vecteurs d'attaque internes, et intégration d'**IBM QRadar SIEM** pour la corrélation des événements d'attaque simulés et l'amélioration de la détection.

INWI (Opérateur Télécom) — Juil 2023 – Août 2023
Ingénieur Sécurité SI — *Casablanca, Maroc*

- Déploiement d'une architecture VPN site-à-site haute disponibilité.
- Configuration sécurisée des routeurs, pare-feu et équipements réseau gérant IPSec.
- Gestion des clés de chiffrement et des mécanismes d'authentification.
- Analyse des risques et renforcement de la sécurité des communications inter-sites.

Projets

Pentest d'Active Directory | *BloodHound, Impacket, Kerberoasting, PowerShell*
* Réalisé l'énumération complète de l'AD et la cartographie des chemins d'attaque avec BloodHound.
* Exploité des vulnérabilités Kerberos (Kerberoasting, AS-REP Roasting) et effectué du lateral movement.
* Proposé des mesures de durcissement AD suite aux findings (GPO, ACL, politiques Kerberos)

Audit & Exploitation Wi-Fi (WiCrack.py) | *Python, Aircrack-ng, Scapy*
* Développement d'un outil Python automatisant le scan des réseaux Wi-Fi et la détection des clients connectés.
* Intégration d'un menu interactif permettant de lancer des attaques DoS ou de capturer un 4-Way Handshake.
* Implémentation d'attaques automatisées (deauth, MDK4) et génération de fichiers de capture pour analyse de sécurité.

Pentest Machines Vulnérables | *(TryHackMe, VulnLab, Metasploitable 2/3)*
* Réalisé l'énumération et l'analyse des services exposés (SMB, FTP, SSH, Web).
* Exploité des vulnérabilités réseau et applicatives, puis effectué l'escalade de privilèges Linux/Windows.
* Produit des preuves d'exploitation et rapporté les failles avec leurs mesures correctives.

Compétences Techniques

Sécurité Offensive (Pentest) : Pentest Réseau & Système (Linux/Windows), Pentest Active Directory, Web Application Pentesting (OWASP Top 10), Enumeration, Exploitation, Privilege Escalation, Lateral Movement, Post-Exploitation, Reporting de vulnérabilités, Metasploit, Burp Suite, Nmap, Gobuster, SQLmap, BloodHound, Impacket, CrackMapExec, ZAP Proxy, OpenVAS.
Sécurité Défensive & Gouvernance : Nessus, Tenable Identity Exposure, IBM QRadar (SIEM), Active Directory Security, Détection d'attaques, Analyse de logs, ISO 27001, COBIT 4, IAM, eFront ERM, Wireshark.
Programmation & Scripting : Python (outils d'automatisation sécurité), Bash, PowerShell (bases), Java, SQL (MySQL), C.
Systèmes & Réseaux : Linux, Windows, TCP/IP, VPN (IPSec, Site-to-Site), Routage, Firewalling, WLAN Security (WPA2/WPA3), Analyse réseau, Protocoles réseau.
Virtualisation & Environnements de test : VMware, VirtualBox, Labs Pentest (Hack The Box, TryHackMe, Root-Me, VulnHub).

Compétences Transversales

Soft Skills : Pensée offensive, Analyse et résolution de problèmes, Autonomie, Rigueur,Rédaction de rapports, Communication, Travail en équipe, Apprentissage continu.

Langues

Anglais : Bilingue
Français : Courant
Arabe : Langue maternelle

Certifications & Formations

INE Security 2025
Junior Penetration Tester (eJPTv2)

Formations & Parcours Techniques En continu

* **TCM Security :** Practical Ethical Hacking (PEH)
* **TryHackMe :** Junior Penetration Tester Path
* **EC-Council :** Ethical Hacking Essentials (EHE)