Khalil Yahyaoui *Pentester*

khalilyahyaoui@proton.me khalil-yahyaoui khalil_yahyaoui

Profil

Consultant en cybersécurité avec près de 3 ans d'expérience, spécialisé dans les évaluations techniques et les tests d'intrusion. Expertise en sécurité offensive, Windows, tests Active Directory, et développement d'outils offensifs pour la simulation d'adversaires et techniques d'évasion EDR/AV dans un cadre red team. Diplômé en cybersécurité et réseaux informatiques.

Formation Académique

Diplôme d'ingénieur en réseaux informatiques et télécommunications - spécialité cybersécurité 2018 – 2023
Institut National des Sciences Appliquées et de Technologie (INSAT)

Expérience professionnelle

Testeur d'intrusion d'applications Web 04/2024 – aujourd'hui
Septeo
Réalisation de tests d'intrusion sur les solutions internes afin d'identifier et corriger les vulnérabilités avant mise en production, sur des applications couvrant différents secteurs d'activité. Automatisation des tâches de tests d'intrusion web, améliorant la couverture et réduisant le temps d'exécution de 50%. Développement d'outils internes contribuant au renforcement de la posture de sécurité de l'entreprise.

Consultant Cybersécurité 08/2023 – 03/2024
Trustable
Réalisation en équipe de tests d'intrusion sur applications web, réseaux et environnements Active Directory. Contribution au développement de trois outils open source intégrés aux offres commerciales de l'entreprise. Automatisation des audits de configuration Windows et Linux, réduisant de 50 % le temps consacré à ces missions.

Stage de fin d'études 02/2023 – 06/2023
Ernst & Young (EY)
Développement d'un outil de reconnaissance et d'analyse du réseau interne ayant élargi la surface d'attaque identifiée lors des tests d'intrusion et réduit de 50 % la phase de test manuel. Conception et déploiement d'une application web intégrant cet outil, réduisant de 25 % le temps d'exécution des tâches récurrentes de l'équipe.

Certificats

- RastaLabs Prolab - Red Team Operator I
- Certified Red Team Professional (CRTP)
- C-AI/MLPen
- Certified Professional Penetration Tester (eCPPTv2)
- Dante Prolab - Penetration Tester II
- Offshore Prolab - Penetration Tester III
- CWL - Multi-Cloud Red Team Analyst [MCRTA]

CTFs

- 14th Place Solo in Root-Me CTF 2022 out of 400 players
- 3rd Place in FwordCTF 2021 out of 400 teams
- Pragyan CTF 2022 Winner out of 225 Teams
- Hackfest Winner out of 20 Tunisian Teams
- Hack Zone-X Winner out of 20 Tunisian Teams
- 2nd Place in RaziCTF 2020 out of 300 teams

Compétences

- Web & API: Burp Suite Pro, OWASP ZAP, Nuclei, ffuf, sqlmap
- Reconnaissance & Infrastructure : Nmap, Masscan, Amass, Subfinder, httpx, Shodan, Metasploit
- Systèmes : Windows, Linux, Active Directory
- Active Directory & Red Team : BloodHound, NetExec (nxc), Impacket, Responder, CrackMapExec, Rubeus, Mimikatz, Cobalt Strike, Sliver, Evil-WinRM, Kerberos
- Développement offensif & évasion : Python, Go, PowerShell, Bash, C/C#, techniques d'évasion EDR/AV.
- Méthodologies & Standards : OWASP Top 10, OWASP WSTG, PTES, MITRE ATT&CK, CIS Benchmarks

Langues

Arabe — Langue Maternelle/Bilingue

Français — Courant

Anglais — Courant