Khalil Yahyaoui *Penetration Tester*

khalilyahyaoui@proton.me khalil-yahyaoui khalil_yahyaoui

Profile

Cybersecurity consultant with nearly 3 years of experience, specialized in technical assessments and penetration testing. Expertise in offensive security, Windows, Active Directory testing, and the development of offensive tools for adversary simulation and EDR/AV evasion techniques within red team engagements. Degree in Cybersecurity and Computer Networks.

Education

Engineering Degree, Computer Networks and Telecommunication - CyberSecurity Specialty 2019 – 2023
National Institute of Applied Sciences and Technology

Professional Experience

Web Application Penetration Tester Apr 2024 – Present
Septeo
Conducted penetration tests on internal solutions to identify and remediate vulnerabilities prior to production release, across applications covering various business sectors. Automated web application penetration testing tasks, improving coverage and reducing execution time by 50%. Developed internal tools contributing to the strengthening of the company's security posture.

CyberSecurity Consultant Aug 2023 – Mar 2024
Trustable
Collaborated within a team to conduct multiple penetration tests on web applications, networks, and Active Directory environments. Contributed to the development and extension of three open-source cybersecurity tools, supporting the enhancement and commercialization of the company's proprietary solutions. Automated cybersecurity tasks, notably Windows and Linux configuration audits, reducing time spent on these engagements by 50%.

End of study internship Feb 2023 – Jun 2023
Ernst & Young (EY)
Developed an internal network reconnaissance and analysis tool that expanded the attack surface identified during penetration tests and reduced manual testing time by 50%. Designed and deployed a web application integrating this tool, cutting execution time for the team's recurring tasks by 25%.

Certificates

- 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]

Capture The Flag Competitions

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

Skills

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

Languages

Arabic — Native/Bilingual

French — Fluent

English — Fluent