Alejandro **López Aguilar**

Offensive Security Engineer | CRTO | OSCP+ | CPTS | CWP

linkedin.com/in/alejandrolopezaguilardev
github.com/AleLopezDev
hackalex.com
alejandrolopezaguilar.dev@gmail.com
Málaga, Spain

Software engineer specializing in offensive security, with experience in black-box and gray-box assessments of web applications, APIs, and infrastructure. CRTO, OSCP+, CPTS, and CWP certified. Hands-on work in C2-driven red team operations, Active Directory, and Wi-Fi security, development of tools in Bash, Python, and C, and clear remediation-focused reporting.

Professional Experience

Present – Feb. 2026 | **Penetration Tester / Offensive Security Analyst, Hispasec, Málaga, Spain**

- Black-box and gray-box assessments of web applications, APIs, infrastructure, and exposed services.
- Validation and controlled exploitation of authentication, authorization, configuration, and information exposure issues.
- Proofs of concept, impact assessment, retesting, and reports with remediation recommendations.
- External attack surface analysis across assets, technologies, domains, and subdomains.

Web Security | API Security | Infrastructure Pentesting | External Attack Surface | Reporting

Jul. 2024 – Jun. 2024 | **Cybersecurity Technician (Internship), Grupo TOPdigital, Málaga, Spain**

- Security monitoring, vulnerability analysis, and web application security reviews.
- Configuration and hardening reviews, technical documentation, and findings reports.

Vulnerability Analysis | Web Security | Hardening | Security Monitoring

Jun. 2023 – Mar. 2023 | **Web Developer (Internship), TYM, Málaga, Spain**

- Developed and maintained web features with TypeScript and Angular, using Git in a collaborative workflow.

TypeScript | Angular | Git

Skills

Pentesting	Web applications, REST/GraphQL APIs, networks, infrastructure, black-box/gray-box testing, retesting, PoCs, and reporting.
Red Teaming	C2 operations (Cobalt Strike, Sliver), Malleable C2, persistence, AMSI, AppLocker, and Defender evasion, and OPSEC.
Active Directory	Kerberos (Kerberoasting, delegation, RBCD), AD CS, DPAPI, LAPS, MSSQL, trusts, lateral movement, and pivoting (Ligolo-ng, Chisel).
Wireless Security	WPA/WPA2, 802.1X/EAP, rogue APs, PMF/MFP, MFP Scout, and EAP Scout.
Malware Development	C/C++, Windows internals, process injection, API hooking, WinAPI, syscalls, and defense evasion fundamentals.
Tools	Burp Suite Pro, BloodHound, Rubeus, Mimikatz, Certify, Nmap, Metasploit, Wireshark, Docker, and Git.
Scripting	Python, PowerShell, and Bash.
Languages	Native Spanish; B2 English for technical and professional work.

Alejandro López Aguilar Offensive Security Engineer

Certifications

Oct. 2026 **Certified Red Team Operator (CRTO)**, Zero-Point Security
End-to-end red team operations with Cobalt Strike: initial access, persistence, privilege escalation, Kerberos and AD CS abuse, lateral movement, pivoting, domain trusts, defense evasion (AMSI, AppLocker, Defender), and OPSEC.

Jul. 2026 **Certified WiFiChallenge Professional (CWP)**, WiFiChallenge Academy
Wi-Fi security assessments, WPA/WPA2-Enterprise, 802.1X/EAP attacks, rogue access points, and wireless control reviews.

Feb. 2026 **OffSec Certified Professional Plus (OSCP+)**, OffSec
Score: 100/100. Network penetration testing, Active Directory exploitation, privilege escalation, and pivoting in enterprise environments.

2025 **HTB Certified Penetration Testing Specialist (CPTS)**, Hack The Box
Web, network, and Active Directory penetration testing, advanced exploitation, and technical reporting.

2024 **Junior Penetration Tester (eJPTv2)**, INE Security
Web and network penetration testing, pivoting, exploitation, and technical reporting.

Selected Projects

2026 MFP Scout, Personal project, GitHub
- Parses Wi-Fi captures with tshark to assess PMF/MFP requirements and guide deauthentication testing.

Bash | tshark | Wi-Fi | 802.11w

2026 EAP Scout, Personal project, GitHub
- Parses 802.1X/WPA-Enterprise captures to identify EAP methods, visible identities, and negotiation details.

Bash | tshark | 802.1X | EAP

2025 Shellcode Injection, Personal project, GitHub
- C implementation of process enumeration and shellcode injection using WinAPI and native syscalls.

C | WinAPI | Syscalls | Windows Internals

2024 CheckGtfoBin, Personal project, GitHub
- Checks GTFOBins for potential privilege escalation paths through Sudo/SUID binaries.

Python | Linux | Privilege Escalation | Automation

Education

2023 - 2026 **BSc in Computer Engineering**, UOC
Software Engineering track.

2023 - 2024 **Vocational specialization in Cybersecurity (Máster FP)**, CPIFP Alan Turing
Ethical hacking, digital forensics, and network hardening.

2021 - 2023 **Higher Vocational Diploma in Multiplatform Application Development**, Colegio San José
Java, databases, systems, and development environments.