Alejandro **López Aguilar**

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

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

Ingeniero de software especializado en ciberseguridad ofensiva, con experiencia en auditorías Black Box y Grey Box de aplicaciones web, APIs e infraestructura. Certificaciones CRTO, OSCP+, CPTS y CWP. Práctica en operaciones Red Team con C2, Active Directory y seguridad Wi-Fi, desarrollo de herramientas en Bash, Python y C, y redacción de informes orientados a la remediación.

Experiencia Profesional

Actualidad – feb. 2026 | **Pentester / Analista de Seguridad Ofensiva, Hispasec, Málaga, España**

- Auditorías Black Box y Grey Box de aplicaciones web, APIs, infraestructura y servicios expuestos.
- Validación y explotación controlada de fallos de autenticación, autorización, configuración y exposición de información.
- Pruebas de concepto, evaluación de impacto, retesting e informes con recomendaciones de remediación.
- Análisis de superficie de ataque externa: activos, tecnologías, dominios y subdominios.

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

jul. 2024 – jun. 2024 | **Técnico de Ciberseguridad (Prácticas), Grupo TOPdigital, Málaga, España**

- Monitorización, análisis de vulnerabilidades y revisión de seguridad de aplicaciones web.
- Revisión de configuraciones y medidas de hardening; elaboración de documentación técnica e informes.

Vulnerability Analysis | Web Security | Hardening | Security Monitoring

jun. 2023 – mar. 2023 | **Desarrollador Web (FCT), TYM, Málaga, España**

- Desarrollo y mantenimiento de funcionalidades web con TypeScript y Angular, utilizando Git y metodologías de trabajo colaborativo.

TypeScript | Angular | Git

Habilidades

Pentesting	Web, APIs REST/GraphQL, redes, infraestructura, Black/Grey Box, retesting, PoC y reporting técnico.
Red Teaming	Operación de C2 (Cobalt Strike, Sliver), Malleable C2, persistencia, evasión de AMSI, AppLocker y Defender, y OPSEC.
Active Directory	Kerberos (Kerberoasting, delegaciones, RBCD), AD CS, DPAPI, LAPS, MSSQL, trusts, movimiento lateral y pivoting (Ligolo-ng, Chisel).
Wireless Security	WPA/WPA2, 802.1X/EAP, rogue AP, PMF/MFP, MFP Scout y EAP Scout.
Malware Development	C/C++, Windows Internals, Process Injection, API Hooking, WinAPI, syscalls y fundamentos de evasión de defensas.
Herramientas	Burp Suite Pro, BloodHound, Rubeus, Mimikatz, Certify, Nmap, Metasploit, Wireshark, Docker y Git.
Scripting	Python, PowerShell y Bash.
Idiomas	Español nativo e inglés B2 técnico/profesional.

Alejandro López Aguilar Offensive Security Engineer

Certificaciones

Oct. 2026 **Certified Red Team Operator (CRTO)**, Zero-Point Security
Operaciones Red Team end-to-end con Cobalt Strike: acceso inicial, persistencia, escalada de privilegios, abuso de Kerberos y AD CS, movimiento lateral, pivoting, trusts entre dominios, evasión de defensas (AMSI, AppLocker, Defender) y OPSEC.

Jul. 2026 **Certified WiFiChallenge Professional (CWP)**, WiFiChallenge Academy
Auditoría de redes Wi-Fi, WPA/WPA2-Enterprise, ataques 802.1X/EAP, puntos de acceso maliciosos y evaluación de controles inalámbricos.

Feb. 2026 **OffSec Certified Professional Plus (OSCP+)**, OffSec
Puntuación: 100/100. Pentesting de redes, explotación de Active Directory, escalada de privilegios y pivoting en entornos corporativos.

2025 **HTB Certified Penetration Testing Specialist (CPTS)**, Hack The Box
Pentesting de aplicaciones web, redes y Active Directory, explotación avanzada y elaboración de informes técnicos.

2024 **Junior Penetration Tester (eJPTv2)**, INE Security
Pentesting web y de redes, pivoting, explotación y reporting técnico.

</> Proyectos Destacados

2026 MFP Scout, Proyecto personal, GitHub
- Analiza capturas Wi-Fi con tshark para comprobar si PMF/MFP es obligatorio y orientar pruebas de desautenticación.

Bash · tshark · Wi-Fi · 802.11w

2026 EAP Scout, Proyecto personal, GitHub
- Analiza capturas 802.1X/WPA-Enterprise para identificar métodos EAP, identidades visibles y pistas de negociación.

Bash · tshark · 802.1X · EAP

2025 Shellcode Injection, Proyecto personal, GitHub
- Implementación en C de enumeración de procesos e inyección de shellcode mediante WinAPI y syscalls nativas.

C · WinAPI · Syscalls · Windows Internals

2024 CheckGtfoBin, Proyecto personal, GitHub
- Consulta GTFOBins para detectar posibles vías de escalada con binarios Sudo/SUID.

Python · Linux · Privilege Escalation · Automation

Educación

2023 - 2026 **Grado en Ingeniería Informática**, UOC
Mención en Ingeniería de Software.

2023 - 2024 **Máster FP Ciberseguridad (Especialización)**, CPIFP Alan Turing
Hacking Ético, Análisis Forense y Bastionado de Redes.

2021 - 2023 **CFGS Desarrollo de Aplicaciones (DAM)**, Colegio San José
Java, Bases de Datos, Sistemas y entornos de desarrollo.