

DAVID JIMÉNEZ SALCEDO

PENTESTING | SEGURIDAD OFENSIVA | RED TEAM | ACTIVE DIRECTORY | WEB & API SECURITY

Madrid, España | david.jim.salc@gmail.com | +34 646 736 205 | [linkedin.com/in/david-jimenez-salcedo](https://www.linkedin.com/in/david-jimenez-salcedo) | davidjim.dev

PERFIL PROFESIONAL

Ingeniero Informático especializado en ciberseguridad, certificado eJPTv2 y con experiencia profesional en SOC N1/N2 y Digital Risk Protection (DRP) en Telefónica Tech. Orientado a la seguridad ofensiva, con experiencia práctica en laboratorios corporativos de Active Directory, pentesting de redes internas, aplicaciones Web/API y simulación de adversarios mediante MITRE ATT&CK.

Participo activamente en programas de Bug Bounty y Vulnerability Disclosure Programs (VDP), realizando reconocimiento, análisis de superficies de ataque, validación de vulnerabilidades y documentación de hallazgos en entornos autorizados.

Combino conocimientos ofensivos con experiencia profesional en detección de amenazas, análisis de incidentes, evaluación de riesgos y elaboración de informes técnicos. Actualmente profundizo en técnicas avanzadas de penetración mediante la preparación de la certificación HTB CPTS, con el objetivo de desarrollar mi carrera profesional en proyectos de Penetration Testing, Red Team y Adversary Simulation.

ÁREAS DE ESPECIALIZACIÓN Y HERRAMIENTAS

Pentesting de infraestructuras: evaluación de seguridad de redes internas y externas, reconocimiento, enumeración de servicios, identificación y explotación controlada de vulnerabilidades, escalada de privilegios, movimiento lateral, pivoting, post-explotación y análisis de rutas de ataque en entornos Windows y Linux.

Seguridad Web/API y metodologías: reconocimiento de superficies de ataque, enumeración de directorios y endpoints, análisis de vulnerabilidades, validación de hallazgos y pruebas de seguridad basadas en OWASP Top 10.

Metodologías y simulación de adversarios: MITRE ATT&CK, técnicas y procedimientos utilizados por atacantes reales (TTPs), simulación de campañas APT y documentación de cadenas de ataque. Familiaridad con las metodologías de evaluación de seguridad ofensiva.

Herramientas de seguridad ofensiva: Burp Suite, Nmap, Metasploit, Wireshark, BloodHound, SharpHound, Impacket, NetExec, Responder, Mimikatz, Hashcat, John the Ripper, FFUF, Gobuster, Evil-WinRM, Rubeus y Proxychains.

Sistemas, protocolos y automatización: Windows, Windows Server, Kali Linux, Ubuntu y Debian; TCP/IP, DNS, HTTP/HTTPS, SMB, LDAP, Kerberos, WinRM, SSH y RDP. Scripting y programación con Python, PowerShell, Bash, SQL, JavaScript y Java.

Análisis defensivo, gestión de riesgos y reporting: análisis y correlación de eventos, investigación de indicadores de compromiso (IoCs), validación de alertas y descarte de falsos positivos, evaluación de criticidad e impacto, documentación de evidencias, informes técnicos y recomendaciones de mitigación. Experiencia con Microsoft Sentinel, Splunk, QRadar, NetWitness, XSIAM, Cortex XDR, CrowdStrike Falcon y Defender for Endpoint.

PROYECTOS DE SEGURIDAD OFENSIVA

Laboratorio empresarial de Active Directory | Proyecto de Fin de Grado – Red Team / Blue Team

Diseñé e implementé un laboratorio empresarial de Active Directory para reproducir una campaña de amenaza persistente avanzada (APT), evaluar vulnerabilidades y analizar el ciclo de ataque desde las perspectivas ofensiva y defensiva.

- Ejecuté reconocimiento, enumeración y técnicas de compromiso del dominio mediante Password Spraying, Kerberoasting, AS-REP Roasting, NTLM Relay, explotación de SQL Server y escalada de privilegios con PrintSpoofer.
- Simulé movimiento lateral y técnicas avanzadas de compromiso mediante Pass-the-Hash, Pass-the-Ticket, DCSync, Golden Ticket y Silver Ticket.
- Relacioné las técnicas empleadas con MITRE ATT&CK, evaluando su detección mediante herramientas y procedimientos Blue Team.
- Documenté las rutas de ataque, evidencias técnicas, impacto de las vulnerabilidades y recomendaciones de mitigación.

Hack The Box Academy, laboratorios y Bug Bounty / VDP | Práctica técnica independiente

Desarrollo pruebas de intrusión en laboratorios de redes corporativas en HTB de Active Directory y aplicaciones Web/API, aplicando metodologías de reconocimiento, enumeración, explotación, escalada de privilegios, pivoting y post-explotación.

Participo en programas de Bug Bounty y Vulnerability Disclosure Programs (VDP), analizando superficies de ataque y validando posibles vulnerabilidades dentro del alcance autorizado. Documento procedimientos, resultados y evidencias técnicas mediante un portfolio de prácticas y write-ups.

EXPERIENCIA PROFESIONAL

Telefónica Tech | Cybersecurity Analyst – SOC N1 24x7 | Sep. 2026 – Actualidad

Monitorizo y analizo alertas e incidentes de seguridad en un SOC 24x7, utilizando soluciones SIEM, EDR y XDR para identificar comportamientos anómalos y posibles actividades maliciosas. Las herramientas que actualmente uso son: Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness y Cortex XSIAM, así como con Cortex XDR, CrowdStrike Falcon y Microsoft Defender for Endpoint

Investigo y correlaciono indicadores de compromiso, valido alertas para descartar falsos positivos y evalúo la criticidad, el impacto y el alcance de los incidentes. Ejecuto procedimientos de contención y respuesta, incluyendo bloqueo de direcciones IP y actuaciones sobre endpoints, y documento las investigaciones conforme a playbooks y SLAs del servicio.

Telefónica Tech – Talentum Cyber & Cloud | Cybersecurity Analyst – SOC N1 y DRP | Ene. – Sep. 2026

Participé en tareas de monitorización, investigación y priorización de alertas de seguridad, correlación de eventos y Digital Risk Protection para el análisis de amenazas digitales externas y posibles riesgos sobre activos corporativos.

Trabajé con Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness y Cortex XSIAM, así como con Cortex XDR, CrowdStrike Falcon y Microsoft Defender for Endpoint para investigación de endpoints. Documenté hallazgos, evidencias y actuaciones de respuesta siguiendo los procedimientos operativos establecidos.

FORMACIÓN Y CERTIFICACIONES

- **Grado en Ingeniería Informática | Universidad Alfonso X el Sabio | 2022–2026.**
- **TFG – Red Team / Blue Team:** simulación de una campaña APT en un entorno empresarial de Active Directory.
- **LPIC-1 – Linux Professional Institute:** administración de sistemas GNU/Linux, redes, servicios y seguridad.
- **eJPTv2 – INE Security:** certificación práctica en pentesting, enumeración, explotación y pivoting.
- **Cisco Ethical Hacker:** reconocimiento, análisis de vulnerabilidades y técnicas de hacking ético.
- **Hack The Box Academy – Penetration Tester Job Role Path:** formación práctica avanzada en pentesting de infraestructuras, Active Directory, escalada de privilegios y post-explotación.
- **HTB CPTS – Certified Penetration Testing Specialist (en preparación):** certificación práctica avanzada de pentesting empresarial, con un alcance técnico y metodológico comparable al OSCP+ y especial énfasis en escenarios corporativos y elaboración de informes profesionales.

IDIOMAS

Español: nativo | Inglés: B2 (lectura de documentación técnica).