

# David Jiménez Salcedo

Cybersecurity Engineer | Offensive Security | Penetration Testing | Active Directory Security | Web & API Security

Localización: Madrid, Spain

Mail: david.jim.salc@gmail.com

Tlf: +34 646 736 205

LinkedIn: <https://linkedin.com/in/david-jimenez-salcedo>

Portfolio web: <https://davidjim.dev>

## Perfil Profesional

Ingeniero Informático especializado en Ciberseguridad con experiencia profesional en un Security Operations Center (SOC N1/N2) y Digital Risk Protection (DRP) en Telefónica Tech. Mi experiencia en Blue Team se complementa con una sólida formación práctica en Offensive Security, centrada en Enterprise Active Directory, Pentesting interno y Web Security. Certificado eJPTv2 y actualmente cursando el Certified Penetration Testing Specialist (CPTS). Busco incorporarme a un equipo de Offensive Security donde aportar una perspectiva diferencial, combinando la experiencia adquirida en operaciones defensivas y entornos corporativos con una sólida base técnica en Pentesting para identificar vulnerabilidades, comprender su detectabilidad y proponer medidas de mitigación eficaces.

## Experiencia Profesional

**Telefónica Tech – Talentum Cyber & Cloud Cybersecurity Analyst (SOC N1/N2 & Digital Risk Protection) Enero 2026 – Presente**

- Monitorización, investigación y correlación de eventos de seguridad mediante plataformas SIEM corporativas como Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness y Cortex XSIAM.
- Análisis de amenazas en endpoints utilizando soluciones EDR/XDR como Cortex XDR, CrowdStrike Falcon y Microsoft Defender for Endpoint.
- Investigación, clasificación y priorización de alertas de ciberseguridad conforme a procedimientos operativos establecidos.
- Trabajo siguiendo procedimientos de Incident Response, Service Level Agreements (SLAs) y playbooks operativos.
- Análisis inicial, validación y escalado de incidentes de seguridad a los equipos correspondientes.

- Análisis y correlación de Indicators of Compromise (IoCs) para apoyar la detección e investigación de amenazas.
- Ejecución de actividades de Digital Risk Protection (DRP) para identificar, analizar y evaluar amenazas digitales externas que puedan afectar a organizaciones.
- Elaboración de Technical Reporting e informes técnicos relacionados con incidentes de seguridad y riesgos detectados.
- Colaboración con equipos Blue Team durante los procesos de investigación, contención y respuesta ante incidentes.
- Formación continua en tecnologías de seguridad Microsoft, Cloud Security y operaciones defensivas.

## **Proyectos Técnicos**

### Enterprise Active Directory Offensive Security Laboratory

- Diseño e implementación de un entorno empresarial de Active Directory para la simulación de escenarios Red Team.
- Simulación de escenarios de ataque basados en técnicas reales de adversarios y alineados con el framework MITRE ATT&CK.
- Validación y explotación de vulnerabilidades sobre servicios e infraestructuras corporativas.
- Ejecución del ciclo completo de un ataque, desde la fase de Enumeration hasta el compromiso completo del dominio.
- Desarrollo de ataques Active Directory Enumeration, Password Spraying, Kerberoasting, AS-REP Roasting y NTLM Relay.
- Explotación de SQL Server y Privilege Escalation mediante PrintSpoofer.
- Ejecución de técnicas Pass-the-Hash, Pass-the-Ticket, DCSync, Golden Ticket y Silver Ticket.
- Análisis de la detectabilidad de cada fase del ataque desde la perspectiva Blue Team, como parte del Trabajo Fin de Grado.
- Elaboración de Technical Reporting, documentando hallazgos, rutas de ataque y recomendaciones de mitigación.

### Hack The Box Academy

- Formación avanzada en Active Directory, Web Security, API Security, Pivoting y Post-Exploitation.
- Desarrollo y mantenimiento de un portfolio técnico con laboratorios, metodologías, write-ups y documentación sobre Offensive Security.

## Educación

- Universidad Alfonso X el Sabio Grado en Ingeniería Informática | 2022 – 2026
- **Trabajo Final de Grado:** Diseño e implementación de un laboratorio empresarial de Active Directory para la simulación del ciclo completo de un Advanced Persistent Threat (APT) mediante metodologías Red Team, evaluando la capacidad de detección desde la perspectiva Blue Team.

## Certifications

- Certified Penetration Testing Specialist (CPTS) – Hack The Box Academy (Currently pursuing). Finalización estimada: septiembre de 2026
- eJPTv2 – INE Security
- Penetration Tester Job Role Path – Hack The Box Academy
- Cisco Ethical Hacker
- LPIC-1 – Linux Professional Institute

## Technical Skills

- **Offensive Security:** Penetration Testing, Active Directory Security and Enumeration, Web Application Security, OWASP Top 10, API Security, Vulnerability Assessment, Vulnerability Validation, Privilege Escalation, Lateral Movement, Pivoting, Post-Exploitation, Windows and Linux Security, Internal Infrastructure Penetration Testing
- **Blue Team:** SOC Operations, Incident Response, Alert Triage, Digital Risk Protection (DRP), IoC Analysis, Threat Analysis, Technical Reporting, Security Monitoring, SIEM and EDR Tools (Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness, Cortex XSIAM, CrowdStrike Falcon, Cortex XDR, Microsoft Defender for Endpoint)
- **Operating Systems:** Windows, Windows Server, Kali Linux, Ubuntu, Debian
- **Networking:** TCP/IP, DNS, HTTP/HTTPS, SMB, LDAP, Kerberos, WinRM, SSH, RDP
- **Programming & Scripting:** Python, PowerShell, Bash, Java, SQL, HTML, CSS, JS
- **Tools:** Burp Suite, Nmap, Wireshark, Metasploit, SharpHound, BloodHound, Impacket, NetExec, Mimikatz, Responder, Hashcat, John the Ripper, FFUF, Gobuster, Evil-WinRM, Proxychains, Rubeus, Enum4Linux-ng, VMware Workstation, VirtualBox, LOLBins

### **Competencias Clave**

Enterprise Penetration Testing, Active Directory Security, Web & API Security, SOC Operations, Digital Risk Protection, Incident Response, Threat Analysis, Technical Reporting

### **Idiomas**

Español: Nativo

Inglés: B2