

DAVID JIMÉNEZ SALCEDO

PENTESTING | OFFENSIVE SECURITY | 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

PROFESSIONAL PROFILE

Computer Engineer specializing in cybersecurity, eJPTv2 certified, with professional experience in SOC N1/N2 and Digital Risk Protection (DRP) at Telefónica Tech. Focused on offensive security, with hands-on experience in enterprise Active Directory labs, internal network penetration testing, Web/API applications, and adversary simulation using MITRE ATT&CK.

I actively participate in Bug Bounty and Vulnerability Disclosure Programs (VDP), performing reconnaissance, attack surface analysis, vulnerability validation, and findings documentation in authorized environments.

I combine offensive security knowledge with professional experience in threat detection, incident analysis, risk assessment, and technical report writing. I am currently deepening my advanced penetration testing skills through preparation for the HTB CPTS certification, with the goal of developing my professional career in Penetration Testing, Red Team, and Adversary Simulation projects.

AREAS OF EXPERTISE AND TOOLS

Infrastructure penetration testing: security assessment of internal and external networks, reconnaissance, service enumeration, vulnerability identification and controlled exploitation, privilege escalation, lateral movement, pivoting, post-exploitation, and attack path analysis in Windows and Linux environments.

Web/API security and methodologies: attack surface reconnaissance, directory and endpoint enumeration, vulnerability analysis, findings validation, and security testing based on the OWASP Top 10.

Methodologies and adversary simulation: MITRE ATT&CK, techniques and procedures used by real-world attackers (TTPs), APT campaign simulation, and attack chain documentation. Familiarity with offensive security assessment methodologies.

Offensive security tools: Burp Suite, Nmap, Metasploit, Wireshark, BloodHound, SharpHound, Impacket, NetExec, Responder, Mimikatz, Hashcat, John the Ripper, FFUF, Gobuster, Evil-WinRM, Rubeus, and Proxychains.

Systems, protocols, and automation: Windows, Windows Server, Kali Linux, Ubuntu, and Debian; TCP/IP, DNS, HTTP/HTTPS, SMB, LDAP, Kerberos, WinRM, SSH, and RDP. Scripting and programming with Python, PowerShell, Bash, SQL, JavaScript, and Java.

Defensive analysis, risk management, and reporting: event analysis and correlation, investigation of indicators of compromise (IoCs), alert validation and false-positive elimination, severity and impact assessment, evidence documentation, technical reports, and mitigation recommendations. Experience with Microsoft Sentinel, Splunk, QRadar, NetWitness, XSIAM, Cortex XDR, CrowdStrike Falcon, and Defender for Endpoint.

OFFENSIVE SECURITY PROJECTS

Enterprise Active Directory Lab | Final Degree Project – Red Team / Blue Team

I designed and implemented an enterprise Active Directory lab to reproduce an advanced persistent threat (APT) campaign, assess vulnerabilities, and analyze the attack lifecycle from offensive and defensive perspectives.

- Performed reconnaissance, enumeration, and domain compromise techniques using Password Spraying, Kerberoasting, AS-REP Roasting, NTLM Relay, SQL Server exploitation, and privilege escalation with PrintSpoofer.
- Simulated lateral movement and advanced compromise techniques using Pass-the-Hash, Pass-the-Ticket, DCSync, Golden Ticket, and Silver Ticket.
- Mapped the techniques used to MITRE ATT&CK, assessing their detection through Blue Team tools and procedures.
- Documented attack paths, technical evidence, vulnerability impact, and mitigation recommendations.

Hack The Box Academy, Labs, and Bug Bounty / VDP | Independent Technical Practice

I conduct penetration tests in HTB corporate network labs involving Active Directory and Web/API applications, applying reconnaissance, enumeration, exploitation, privilege escalation, pivoting, and post-exploitation methodologies.

I participate in Bug Bounty and Vulnerability Disclosure Programs (VDP), analyzing attack surfaces and validating potential vulnerabilities within authorized scope. I document procedures, results, and technical evidence through a portfolio of hands-on exercises and write-ups.

PROFESSIONAL EXPERIENCE

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

I monitor and analyze security alerts and incidents in a 24x7 SOC, using SIEM, EDR, and XDR solutions to identify anomalous behavior and potential malicious activity. The tools I currently use are Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness, and Cortex XSIAM, as well as Cortex XDR, CrowdStrike Falcon, and Microsoft Defender for Endpoint.

I investigate and correlate indicators of compromise, validate alerts to rule out false positives, and assess incident severity, impact, and scope. I carry out containment and response procedures, including IP address blocking and endpoint actions, and document investigations in accordance with service playbooks and SLAs.

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

I participated in security alert monitoring, investigation, and prioritization, event correlation, and Digital Risk Protection to analyze external digital threats and potential risks to corporate assets.

I worked with more than seven SIEM tools and six EDR/XDR tools for endpoint investigation. I documented findings, evidence, and response actions following established operational procedures.

EDUCATION AND CERTIFICATIONS

- **Bachelor's Degree in Computer Engineering | Universidad Alfonso X el Sabio | 2022–2026.**
- **Final Degree Project – Red Team / Blue Team:** simulation of an APT campaign in an enterprise Active Directory environment.
- **LPIC-1 – Linux Professional Institute:** GNU/Linux systems administration, networking, services, and security.
- **eJPTv2 – INE Security:** practical certification in penetration testing, enumeration, exploitation, and pivoting.
- **Cisco Ethical Hacker:** reconnaissance, vulnerability analysis, and ethical hacking techniques.
- **Hack The Box Academy – Penetration Tester Job Role Path:** advanced hands-on training in infrastructure penetration testing, Active Directory, privilege escalation, and post-exploitation.
- **HTB CPTS – Certified Penetration Testing Specialist (in preparation):** advanced practical certification in enterprise penetration testing, with a technical and methodological scope comparable to OSCP+ and particular emphasis on corporate scenarios and professional report writing.

LANGUAGES

Spanish: native | English: B2 (reading technical documentation).