

# David Jiménez Salcedo

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

**Location:** 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>

## Professional Summary

Computer Engineer specialized in Cybersecurity with professional experience in a Security Operations Center (SOC Tier 1/2) and Digital Risk Protection (DRP) at Telefónica Tech. My Blue Team experience is complemented by strong hands-on training in Offensive Security, with a focus on Enterprise Active Directory, Internal Network Penetration Testing, and Web Application Security. I hold the eJPTv2 certification and am currently pursuing the Certified Penetration Testing Specialist (CPTS). I am seeking to join an Offensive Security team where I can bring a unique perspective by combining hands-on defensive operations experience in enterprise environments with solid penetration testing expertise to identify vulnerabilities, assess their detectability, and recommend effective mitigation strategies.

## Professional Experience

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

- Monitor, investigate and correlate security events using enterprise SIEM platforms including Microsoft Sentinel, Splunk, IBM QRadar, RSA NetWitness and Cortex XSIAM.
- Perform endpoint threat analysis using Cortex XDR, CrowdStrike Falcon and Microsoft Defender for Endpoint.
- Investigate, classify and prioritize cybersecurity alerts following operational procedures.
- Work in accordance with incident response procedures, service level agreements (SLAs) and operational playbooks.
- Perform initial incident analysis, validation and escalation to the appropriate response teams.
- Correlate security events and analyse Indicators of Compromise (IoCs).

- Execute Digital Risk Protection (DRP) activities to identify and assess external digital threats affecting organisations.
- Produce technical documentation and incident reports.
- Collaborate with Blue Team specialists during incident investigation and response.
- Continuously strengthen knowledge of Microsoft security technologies, cloud security and defensive operations.
- Produce technical documentation and incident reports.
- Collaborate with Blue Team specialists during incident investigation and response.
- Continuously strengthen knowledge of Microsoft security technologies, cloud security and defensive operations.

## **Technical Projects**

### Enterprise Active Directory Offensive Security Laboratory

- Designed and deployed a realistic enterprise Active Directory environment for Red Team simulations.
- Simulated enterprise attack scenarios aligned with real-world adversary techniques and MITRE ATT&CK tactics.
- Conducted vulnerability validation and exploitation against enterprise services and infrastructure.
- Executed the full attack lifecycle from enumeration to domain compromise.
- Performed Active Directory Enumeration, Password Spraying, Kerberoasting, AS-REP Roasting and NTLM Relay attacks.
- Executed SQL Server exploitation and privilege escalation using PrintSpoofer.
- Performed Pass-the-Hash, Pass-the-Ticket, DCSync, Golden Ticket and Silver Ticket attacks.
- Analysed Blue Team detectability throughout each attack phase as part of my Final Degree Project.
- Produced professional technical documentation describing findings, attack paths and mitigation recommendations.

### Hack The Box Academy

- Completed advanced training focused on Active Directory, Web Security, API Security, Pivoting and Post-Exploitation.
- Maintain and continuously expand a personal technical portfolio documenting labs, methodologies, writeups and offensive security notes

## Education

- Universidad Alfonso X el Sabio BSc Computer Science Engineering (2022–2026)
- **Final Degree Project:** Simulation of an Advanced Persistent Threat (APT) against an Enterprise Active Directory environment using Red Team methodologies and Blue Team detectability analysis.

## Certifications

- Certified Penetration Testing Specialist (CPTS) – Hack The Box Academy (Currently pursuing). Expected Completion: September 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

**Core Competencies**

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

**Languages**

Spanish: Native

English: B2