Daniel Miranda Barcelona

Pentester | Seguridad Ofensiva | Vulnerability Research | eJPTv2 · eWPT | OSCP en curso

daniel.mirandabarcelona@gmail.com · +34 697 38 23 93 · danielmb.es · github.com/ex-cal1bur · linkedin.com/in/daniel-miranda-barcelona · Zaragoza, España

[NASA VDP] Reconocimiento oficial — Abril 2026

Vulnerabilidad P2 en *SBN-Client*, librería C open source de NASA para comunicación con el Core Flight System (cFS). Stack buffer overflow de 32.767 bytes por campo de red sin validar. Confirmada, parcheada y cerrada en 26 días. CVE en proceso con MITRE.

Perfil Profesional

Pentester con experiencia en auditorías reales (interna y externa) sobre infraestructura y aplicaciones web, metodología PTES y reporting basado en CVSS v3. Investigador de seguridad activo: PoC publicada en Exploit-DB (**EDB-ID: 52325**, CVE-2025-24071), contribuidor oficial de Hak5 y redactor técnico en Araintel. Base sólida en desarrollo (PL/SQL, Python, Bash) que acelera scripting de reconocimiento y explotación. OSCP en curso. Busco incorporarme a un equipo de seguridad ofensiva en Zaragoza (presencial/híbrido) o remoto en España.

Logros y Proyectos Destacados

- **NASA VDP Recognition** (Abr. 2026) — Vulnerabilidad P2 en *SBN-Client* (librería C open source, Core Flight System). Stack buffer overflow de 32.767 bytes. Confirmada, parcheada y cerrada en 26 días. CVE en proceso con MITRE.
- **PoC publicada en Exploit-DB** — EDB-ID: 52325 (CVE-2025-24071): identifiqué un caso no cubierto en implementaciones públicas y desarrollé la PoC mejorada, aceptada tras revisión.
- **Artículos técnicos publicados en Araintel** — Análisis de CVEs activos (CVE-2025-32463, CVE-2025-55182, CVE-2025-24071) con cobertura técnica de vectores de ataque, explotación y mitigación orientada a equipos de seguridad.
- **Contribuidor oficial Hak5** — Payloads aceptados en el repositorio oficial de USB Rubber Ducky.
- **TryHackMe Top 6% Global** · **Hack The Box — Rango Hacker**.

Experiencia

Pentester e Investigador de Seguridad Ofensiva
Jun. 2025 – Presente

The Dumpster / Freelance — España

- Investigación activa de vulnerabilidades en software real: identificación, explotación y documentación con PoCs reproducibles e informes de impacto real.
- Cadena de ataque completa sobre entorno Active Directory: LLMNR/NBT-NS poisoning, Pass-the-Hash, Kerberoast, AS-REP roasting, volcado de NTDS y Golden Ticket — documentada en informe técnico de 49 páginas (ver portfolio).
- NASA VDP Recognition (P2) por vulnerabilidad en *SBN-Client* (Core Flight System); PoC publicada en Exploit-DB (EDB-ID: 52325, CVE-2025-24071).
- Contribuidor activo al repositorio oficial de Hak5 y redactor técnico en Araintel y The Dumpster sobre vulnerabilidades, explotación y pentesting.
- Divulgación responsable coordinada con INCIBE-CERT sobre plataforma del sector público español (Security Misconfiguration, OWASP A05).

Redactor Técnico de Ciberseguridad
Oct. 2025 – Presente

Araintel — Zaragoza (Remoto)

- Artículos técnicos sobre pentesting, explotación de vulnerabilidades y análisis orientados a Red Team y Blue Team en entornos corporativos (Araintel y The Dumpster).

Software Engineer — Oracle / PL/SQL
Nov. 2022 – Presente

Ayesa / Minsait (Indra) — Zaragoza

- Desarrollo y mantenimiento de plataformas empresariales críticas en Oracle Forms y PL/SQL; participación en migración 10g a 12c.
- Reducción de errores en producción y del tiempo de resolución de incidencias mediante depuración sistemática y automatización.
- Formación técnica de tres perfiles junior, mejorando la autonomía del equipo.
- Base en desarrollo aplicada al pentesting de aplicaciones — entender cómo está construido un sistema es parte de saber cómo romperlo.

Security Content Tester
Sep. 2024 – Abr. 2025

HackJourney — Remoto

- Validación de entornos CTF y laboratorios (Linux, Windows, AD) en fases alfa/beta, asegurando coherencia técnica y realismo ofensivo.

Stack Técnico

Pentesting	Burp Suite, Nmap, Nessus, Sqlmap, FFUF, Gobuster, Nuclei, Dirsearch
Post-explot. / AD	Impacket, BloodHound, Mimikatz, CrackMapExec, Evil-WinRM, Responder, SharpHound
Web	OWASP ZAP, JWT Inspector, XSStrike
Scripting / Dev	Python, Bash, PowerShell, JavaScript, PL/SQL, MySQL, Git
Sistemas	Kali Linux, Debian, Parrot, Windows Server, Active Directory, Wireshark, VMware
Gestión	JIRA, Redmine

Certificaciones

- OSCP — Offensive Security Certified Professional — En curso
- eJPTv2 — eLearnSecurity / INE — Abr. 2024–2027
- eWPT — Web Application Penetration Tester, INE — Oct. 2024–2027
- ICCA — INE Certified Cloud Associate — Jul. 2024–2027
- Google Cybersecurity Professional Certificate — Sep. 2024

Formación Académica

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Sep. 2026 – En curso

Universitat Oberta de Catalunya (UOC)

Máster en Ciberseguridad
May. 2025 – Dic. 2025

TSSciberseguridad — Auditorías de seguridad, hacking ético, gestión de vulnerabilidades

Incluye 2 auditorías reales (interna + externa) sobre entornos de clientes reales, siguiendo metodología PTES con reporting técnico y ejecutivo basado en CVSS v3.

CFGS — Desarrollo de Aplicaciones Web (DAW)
2020–2022

CPIFP Los Enlaces

CFGM — Sistemas Microinformáticos y Redes (SMR)
2017–2020

CPIFP Los Enlaces

Idiomas

Español — Nativo | **Inglés** — B2 (EF-SET 65/100, equivalente C1)