

David Rodríguez Ramírez

[linkedin](#) | [gemsy.es](#) | [drscout.es](#) | [portfolio](#) | [github](#) | [HackTheBox](#)
davidrodriguezscout@gmail.com | [+34 645 457 266](#)

PROFESSIONAL SUMMARY

Junior Security Analyst with a **hands-on and practical** approach to offensive cybersecurity, with experience in **enumeration, exploitation and post-exploitation** across Windows and Linux environments through personal labs and training platforms such as Hack The Box.

Experience working with **simulated Active Directory environments**, web services and Windows systems, applying structured enumeration methodologies, testing attack vectors and performing privilege escalation in controlled environments.

Profile oriented toward continuous learning, with a strong interest in understanding how vulnerabilities materialize in real-world scenarios, improving offensive reasoning and strengthening technical foundations through constant practice.

CYBERSECURITY EXPERIENCE

Offensive Security (Hands-on Practice)

- Enumeration of Windows and Linux systems: services, users, permissions and attack surface.
- Practice in simulated Active Directory environments: LDAP and SMB enumeration, basic Kerberos attack vector testing.
- Exploitation of common Windows services (MSSQL, WinRM) in laboratory environments.
- Gaining initial access and using reverse shells in Bash, PowerShell and Python.
- Privilege Escalation on Windows and Linux through analysis of insecure configurations (SUID, services, permissions).

Defensive Security Fundamentals

- Identification of common misconfigurations and vulnerabilities in systems and services.
- Basic understanding of vulnerability impact and its relationship with defensive controls.
- Fundamental concepts of system hardening and attack surface reduction.

HACK THE BOX — SIMULATED ENVIRONMENT PRACTICE

Solved machines (selection): Gavel · MonitorsFour · Editor · Eighteen · Previous · DarkZero · HackNet · Giveback · Outbound

- Solved enterprise-like machines using structured enumeration, exploitation and privilege escalation workflows.
- Practice of offensive reasoning: hypothesis testing, error correction and alternative attack path evaluation.
- Progressive improvement of technical judgment through analysis of failed and successful attack paths.

RELEVANT TECHNICAL PROJECTS

Active Directory Offensive Homelab

[GitHub](#)

Design and deployment of an isolated Active Directory lab focused on practicing enumeration, identifying misconfigurations and understanding attack paths in controlled environments.

Hands-on practice of authenticated and unauthenticated enumeration (LDAP, SMB), basic Kerberos attack vector testing and analysis of insecure permissions (ACLs) to understand their security impact.

Personal documentation of attack paths, common mistakes and potential mitigation strategies as part of the learning process.

gemsy.es — Full-Stack + AI Platform

[gemsy.es](#)

Designed and developed from scratch a Python-based platform on Google Cloud, including modular backend architecture, automation, REST APIs, GPT integration and cloud deployment.

drscout.es — Web Infrastructure

[drscout.es](#)

Development and maintenance of a website with a focus on performance, stability and basic security. Automation of technical processes.

PROFESSIONAL EXPERIENCE

Full-Stack Development & AI — [gemsy.es](#)

2025 – Present

- Product design and development.
- Modular Python backend and REST APIs.
- Basic identity, permissions and service management on Google Cloud.
- Process automation and business logic implementation.

Web Developer — [drscout.es](#)

2024 – Present

- Technical development, maintenance and infrastructure.
- Performance and stability optimization.
- Process automation.

TECHNICAL SKILLS

Offensive Security Enumeration, basic/intermediate exploitation, Windows/Linux Privilege Escalation, Active Directory (simulated environments).

Tools Nmap, ffuf, Burp Suite, Evil-WinRM, Impacket (practical usage), Ligolo-ng.

Cloud Google Cloud: App Engine, Firestore, CloudSQL, IAM (fundamentals).

Development Python scripting, REST APIs, basic automation, GPT integration.

EDUCATION

2025 Cybersecurity in Enterprise Environments

Centro Virtual Formación Murcia

2021 High School Diploma

IES Los Boliches

LANGUAGES

Spanish Native

English Advanced

French Intermediate

Catalan Basic