David Rodríguez Ramírez

linkedin | gemsy.es | drscout.es | portfolio | github | HTB

davidrodriguezscout@gmail.com | +34 645 457 266

Professional Summary

Offensive Security specialist with hands-on experience in **Active Directory attacks**, **Kerberos abuse**, **Impacket tooling**, and **post-exploitation** across Windows and Linux environments. Skilled in troubleshooting complex attack paths, reconstructing broken vectors, and performing manual exploitation without automated frameworks. Strong background combining cybersecurity, Python automation, and cloud engineering, with real-world technical deployment experience.

Offensive Security Experience

Active Directory & Windows Attack Surface

- Kerberos: TGT/ST manipulation, AS-REP abuse, SPN enumeration, S4U2Self attacks.
- SPN Hijacking and service account privilege escalation.
- MSSQL exploitation: `xp_cmdshell`, impersonation, chained escalations.
- WinRM exploitation for remote code execution and post-exploitation.
- LDAP advanced enumeration and ACL analysis.
- Credential extraction using Impacket-based tooling.

Red Teaming Techniques

- Pivoting through **Ligolo-ng**.
- Manual exploitation of services without Metasploit.
- Advanced reconnaissance: Nmap NSE, fingerprinting, ffuf.
- Reverse shells in Bash, PowerShell, and Python.
- PowerShell restriction bypass and log interpretation.
- Privilege Escalation (Windows/Linux): SUID, PATH hijacking, services, capabilities.

Troubleshooting & Technical Investigation

- Debugging Impacket failures (Kerberos errors, clock skew, corrupted tickets).
- Reconstructing exploit chains when intended attack paths fail.
- Analysis of misconfigurations across Windows services and corporate environments.

HackTheBox — Real Offensive Practice

Selected Machines Solved: Gavel · MonitorsFour · Editor · Eighteen · Previous · DarkZero · HackNet · Giveback · Outbound

Techniques Used:

- Kerberos TGT/ST, AS-REP abuse, SPN attacks.
- ACL abuse and service account exploitation.
- MSSQL exploitation with privilege escalation.
- WinRM exploitation and lateral movement.
- LDAP enumeration, pivoting with Ligolo-ng.
- Advanced Windows/Linux privilege escalation.
- Deep troubleshooting in AD environments.

Technical Projects

gemsy.es — Full-Stack Platform + AI gemsy.es

End-to-end development of a cloud-based system using Python, GPT-powered semantic automation, custom APIs, secure deployment pipelines, and PostgreSQL on Google Cloud. Focus on scalability, modularity, and reliability.

drscout.es — Infrastructure & Performance Optimization drscout.es

Cloud-hosted platform with performance optimization, SEO improvements, and technical automation. Experience with secure deployment and cloud architecture.

Professional Experience

Full-Stack Development & AI Engineering — gemsy.es 2025 – Present

- System design, backend development, and cloud infrastructure.
- GPT-based automation and advanced filtering systems.
- API development and modular Python backend.
- PostgreSQL management and Google Cloud deployment.

Web Development — drscout.es 2024 – Present

- Technical development, maintenance, and infrastructure.
- Performance optimization and stability improvements.
- Automation of site processes.

Technical Skills

Cybersecurity	Active Directory, Kerberos (TGT/ST), SPN abuse, Impacket, MSSQL exploitation, WinRM, Linux/Windows PrivEsc, pivoting, advanced troubleshooting.
Tools	Impacket suite, Evil-WinRM, Ligolo-ng, Nmap NSE, ffuf, BurpSuite, Kerbrute, LDAPSearch, Python scripting.
Development	Python, REST APIs, automation tooling, GPT integration.
Cloud	Google Cloud (App Engine, Firestore, CloudSQL, Storage, IAM, SSL).
Web	HTML/CSS, performance optimization, SEO.

Education

2025 Cybersecurity in the Enterprise **CVFM (Murcia)**
2021 High School Diploma **IES Los Boliches**

Languages

Spanish Native
English Advanced
French Intermediate
Catalan Basic