David Rodríguez Ramírez

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

davidrodriguezscout@gmail.com | +34 645 457 266

Resumen Profesional

Especialista en **ciberseguridad ofensiva** con experiencia práctica en entornos simulados mediante **HackTheBox**, centrado en **Active Directory**, **Kerberos**, **Impacket**, técnicas de **post-explotación** y **Privilege Escalation** en Windows y Linux. Capacidad demostrada en análisis, troubleshooting avanzado, reconstrucción de vectores cuando el camino intended falla y explotación manual sin herramientas automáticas. Formación híbrida entre ciberseguridad, automatización en Python e ingeniería cloud, con experiencia en despliegue y mantenimiento de infraestructura técnica real.

Experiencia en Ciberseguridad Ofensiva

Active Directory & Windows Attacks

- Kerberos: TGT/ST manipulation, AS-REP, SPN enumeration, S4U2Self.
- SPN Hijacking y abuso de cuentas de servicio.
- Explotación de MSSQL: `xp_cmdshell`, impersonation, escaladas.
- Abuso de WinRM para acceso y post-explotación.
- Enumeración avanzada de LDAP y análisis de ACLs.
- Extracción de credenciales con herramientas de Impacket.

Técnicas de Red Teaming

- Pivoting mediante **Ligolo-ng**.
- Explotación manual de servicios sin Metasploit.
- Reconocimiento avanzado: Nmap NSE, fingerprinting, ffuf.
- Reverse shells en Bash, PowerShell y Python.
- Bypass de restricciones en PowerShell e interpretación de logs.
- Privilege Escalation Windows/Linux: SUID, PATH hijacking, servicios, capabilities.

Troubleshooting & Investigación

- Depuración de fallos de Impacket (errores Kerberos, clock skew, tickets corruptos).
- Reconstrucción de exploit chains en máquinas donde el vector intended falla.
- Análisis de configuraciones erróneas en Windows y servicios corporativos.

HackTheBox — Práctica Ofensiva Real

Máquinas resueltas (selección): Gavel · MonitorsFour · Editor · Eighteen · Previous · DarkZero · HackNet · Giveback · Outbound

Técnicas aplicadas:

- Kerberos TGT/ST, AS-REP, SPN abuse.
- Abuso de ACLs y cuentas de servicio.
- MSSQL exploitation y escalada mediante servicios.
- WinRM exploitation y movimiento lateral.
- LDAP enumeration, pivoting con Ligolo-ng.
- PrivEsc avanzada en Windows y Linux.
- Troubleshooting profundo en entornos AD.

Proyectos Técnicos Relevantes

gemsy.es — Plataforma Full-Stack + IA gemsy.es

Desarrollo desde cero de un sistema completo basado en Python y Google Cloud: automatización, consultas semánticas con GPT, API propia, bases de datos y despliegue seguro en cloud. Enfoque en escalabilidad, modularidad y buenas prácticas técnicas.

drscout.es — Infraestructura Web & Optimización drscout.es

Sitio optimizado para rendimiento, SEO y seguridad básica. Automatización de procesos técnicos y despliegue en infraestructuras cloud.

Experiencia Profesional

Desarrollo Full-Stack e IA — gemsy.es 2025 – Actual

- Diseño, desarrollo e infraestructuras del producto.
- Integración de IA (GPT) para automatización y análisis.
- Backend modular en Python y APIs seguras.
- BBDD PostgreSQL y despliegue en Google Cloud.

Desarrollador Web — drscout.es 2024 – Actual

- Desarrollo técnico, mantenimiento e infraestructura.
- Optimización de rendimiento y estabilidad.
- Automatización de procesos.

Habilidades Técnicas

Ciberseguridad	Active Directory, Kerberos (TGT/ST), SPN abuse, Impacket, MSSQL exploitation, WinRM, PrivEsc Linux/Windows, pivoting, troubleshooting avanzado.
Herramientas	Impacket, Evil-WinRM, Ligolo-ng, Nmap NSE, ffuf, BurpSuite, Kerbrute, LDAPSearch, Python scripting.
Desarrollo	Python, APIs REST, automatización ofensiva, integración GPT.
Cloud	Google Cloud: App Engine, Firestore, CloudSQL, Storage, IAM, SSL.
Web	HTML/CSS, optimización, SEO técnico.

Formación

2025 Ciberseguridad en la Empresa — **Centro Virtual Formación Murcia**
2021 Bachillerato — **IES Los Boliches**

Idiomas

Español	Nativo
Inglés	Avanzado
Francés	Intermedio
Catalán	Básico