JAVIER DURÁN GARCÍA

Especialista en Ciberseguridad Ofensiva | Pentester | Red Team

654 142 576
nexusfireman@proton.me
linkedin.com/in/javierdurangarcia
Madrid, España

PERFIL PROFESIONAL

Especialista en Ciberseguridad Ofensiva con más de 15 años de experiencia en IT. Mi ventaja competitiva es única: he construido, administrado y defendido los sistemas que ahora audito desde una perspectiva ofensiva. Esta experiencia 360° me permite identificar vectores de ataque que otros profesionales pueden pasar por alto.

Implemento soluciones SIEM (Security Onion, Wazuh), realizo auditorías de seguridad, ejecuto hardening de infraestructuras y analizo vulnerabilidades en aplicaciones y redes. Desarrollo automatizaciones con Python y PowerShell para optimizar la detección de amenazas y exploro activamente aplicaciones de IA en análisis de seguridad.

ÁREAS DE EXPERTISE

🎯 Seguridad Ofensiva

Pentesting, Red Team, OSINT, Vulnerability Assessment, Exploit Analysis, Web Application Security

🛡️ Seguridad Defensiva

SIEM (Security Onion, Wazuh), Análisis de logs, Detección de amenazas, Incident Response, Hardening

💻 Sistemas & Redes

Windows Server, Linux, Active Directory Security, Virtualización (Hyper-V, VMware), Segmentación de red

⚙️ Desarrollo & Automatización

Python, PowerShell, Bash, C# (.NET), Secure Coding, Scripts de automatización, APIs seguras

EXPERIENCIA PROFESIONAL

Técnico de Sistemas y Seguridad

Jul 2021 - Actualidad

R.G.H. Cofer, S.L. | Madrid

Logros en Ciberseguridad

- Implementé y gestiono soluciones **SIEM con Security Onion y Wazuh**, reduciendo el tiempo de detección de incidentes en un 60% mediante configuración de alertas personalizadas
- Ejecuté proyecto completo de **hardening** aplicando CIS Benchmarks en infraestructura Windows Server y Linux, reduciendo significativamente la superficie de ataque
- Desarrollé **scripts de automatización en Python y PowerShell** para análisis de logs y detección de anomalías, aplicando técnicas básicas de machine learning
- Realizo **auditorías internas de seguridad** identificando vulnerabilidades en aplicaciones web corporativas con enfoque en OWASP Top 10

Administración de Infraestructura

- Gestión de **Active Directory** con políticas de grupo avanzadas, control de accesos basado en roles y auditoría continua de eventos de seguridad
- Administración de virtualización segura (**Hyper-V, VMware**) con segmentación de red y aislamiento de entornos críticos
- Diseño de estrategia de **backups cifrados** con planes de disaster recovery (RPO < 4 horas)

Desarrollo Seguro

- Desarrollo de aplicaciones en **C# (.NET) y Flutter** aplicando secure coding practices y validación exhaustiva de inputs
- Implementación de **autenticación segura y RBAC** en aplicaciones internas

Security Onion | Wazuh | Kali Linux | Python | PowerShell | Active Directory | Hyper-V | C# | Metasploit | Nmap

Programador Senior

May 2019 - Abr 2020

ConeXtaSoft Soluciones Empresariales | Jaén (Remoto)

- Desarrollo de aplicaciones empresariales críticas donde la disponibilidad y seguridad de datos eran fundamentales
- Diseño de arquitecturas de software con enfoque en integridad y disponibilidad
- Implementación de WordPress corporativo con configuraciones de seguridad avanzadas

Experiencia IT Previa (13+ años)

2006 - 2019

Múltiples empresas | 2006-2019

Mi carrera incluye roles progresivos en desarrollo de software (Velneo V7, VB.NET), administración de sistemas Windows Server, gestión de Active Directory, soporte técnico y gestión de redes. Esta base me proporciona una comprensión profunda de infraestructuras IT desde su diseño hasta su operación.

- **Responsable IT** - Ayuntamiento Añover de Tajo: Administración servidores, gestión red corporativa, formación técnica
- **Analista & Desarrollador** - Despacho Entreplazas, ERIDDES, Montemar: Desarrollo ERPs, soluciones empresariales
- **Técnico Informático** - Ingenia, Sermicro: Soporte 24/7, resolución incidencias, gestión infraestructuras

PROYECTOS DESTACADOS

Implementación de SIEM Empresarial

Despliegue completo de Security Onion y Wazuh con configuración de reglas personalizadas, integración con Active Directory y documentación de procedimientos de respuesta a incidentes. Resultado: monitorización 24/7 con reducción del 60% en tiempos de detección.

Laboratorio Personal de Pentesting

Entorno virtualizado para práctica continua de técnicas ofensivas en plataformas como HackTheBox y TryHackMe. Desarrollo de exploits propios en Python y documentación de metodologías de ataque y defensa.

Automatización de Análisis de Seguridad

Scripts en Python/PowerShell para automatizar escaneos de vulnerabilidades, análisis de logs y generación de informes. Experimentación con modelos de IA para detección de patrones anómalos en tráfico de red.

CERTIFICACIONES & FORMACIÓN

- ✓ ISO 27001 Fundamentals
- ✓ Introducción al Hacking (Cisco, HTB)
- ✓ Introduction to Cybersecurity
- ✓ Ciberseguridad y Hacking Ético
- ✓ Endpoint Security
- ✓ Networking Cisco (múltiples)

En preparación: CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional)
Práctica continua: HackTheBox, TryHackMe, CTF Competitions, análisis de CVEs

INFORMACIÓN ADICIONAL

Idiomas	Disponibilidad	Movilidad
Español: Nativo	Remoto, híbrido	Carnet B
Inglés: Técnico	o presencial	Vehículo propio

"La mejor defensa comienza entendiendo cómo ataca el adversario. Mi objetivo es aportar esa perspectiva ofensiva para construir entornos más seguros."