# Santiago González Osuna - Pentester Jr.

Correo: santijuan2404@gmail.com | LinkedIn: linkedin.com/in/santiago-gonzalez-006266369 /Ubicación: Mazatlán, Sinaloa | Disponibilidad: Inmediata - Horario flexible

## Perfil Profesional

Pentester junior certificado (eJPT) con sólida base técnica y experiencia práctica en entornos controlados. Apasionado por la ciberseguridad ofensiva, con habilidades en escaneo de redes, pruebas de penetración web, análisis de tráfico y automatización de tareas con Python. En constante aprendizaje de seguridad en la nube (AWS) y comprometido con ofrecer resultados útiles y profesionales. Destaco por mi responsabilidad, curiosidad técnica y capacidad para adaptarme rápidamente a nuevos entornos y herramientas.

## Certificación

eLearnSecurity Junior Penetration Tester (eJPT) - INE Security (ID verificable)

## Habilidades Técnicas

| Pentesting: | Nmap, Burp Suite, sqlmap, FFUF, Wireshark, Metasploit |
|---|---|
| Seguridad Web: | OWASP Top 10, pruebas en apps HTML/JS, interceptación HTTP |
| Redes: | TCP/IP, escaneo de puertos, auditoría WiFi |
| Sistemas operativos: | Kali Linux, Linux Debian, Windows |
| Programación: | Python (scripts), C++, HTML/CSS, Java (básico) |
| Virtualización y entornos: | VirtualBox, Docker (básico), Metasploitable, Hack The Box |
| Cloud: | Aprendizaje activo de AWS ofensivo (IAM, S3, EC2, configuración insegura) |

## Proyectos Técnicos

- BlitzScan - App de escaneo web (2025)
Desarrollé una herramienta propia que integra escaneos automáticos con Nmap, sqlmap, WhatWeb y FFUF a través de un frontend HTML y backend Flask, con resultados mostrados en tiempo real.

- Auditoría en la Universidad Politécnica de Sinaloa (UPSIN) (2025)
Realicé pruebas de seguridad en aplicaciones web internas y auditorías de red, aportando hallazgos que fortalecieron la seguridad de la institución. Colaboré con el área de TI en la implementación de medidas preventivas.

- Auditoría WiFi doméstica (2024)
Evaluación de seguridad en redes con herramientas como airodump-ng y aircrack-ng.

- Análisis de tráfico con Wireshark (2024)
Captura y análisis de tráfico HTTP/HTTPS e ICMP en entornos virtuales.

- Explotación de máquinas vulnerables (2024)
Uso de Metasploitable 2 para prácticas de explotación y post-explotación en entornos aislados.

## Formación Académica

Universidad Politécnica de Sinaloa (UPSIN) - Ingeniería en Tecnologías de la Información (En curso)

## Idiomas

Español: Nativo
Inglés: Intermedio (lectura técnica, documentación, herramientas ofensivas)