Juan Nemiña

Ingeniero de Seguridad Ofensiva
juan.nemina@outlook.com | LinkedIn | GitHub | Santiago, Chile

RESUMEN

Ingeniero en Ciencias de la Computación y profesional de Seguridad Ofensiva con 3 años de experiencia en evaluaciones de seguridad Web, API, Mobile y cloud en contextos empresariales. Experiencia identificando vulnerabilidades en sistemas reales, evaluando impacto técnico y de negocio, y comunicando hallazgos accionables a equipos técnicos y stakeholders de negocio. Actualmente enfocado en roles de Application Security, Product Security y Offensive Security.

EXPERIENCIA

NTT DATA **Enero 2022 – Presente**
Engineer | Marzo 2025 – Presente *Santiago, Chile*

- Ejecución de ejercicios de Ethical Hacking en entornos Web, API y Mobile como parte del equipo global de una empresa aseguradora multinacional, realizando auditorías para unidades de negocio en distintas regiones del mundo.
- Diseño e implementación de una máquina CTF vulnerable en Windows para apoyar procesos de evaluación técnica de nuevos pentesters, incorporando una cadena de ataque realista con explotación web avanzada, exposición de servicios internos y elevación de privilegios local.

Junior Engineer | Marzo 2023 – Marzo 2025

- Responsable del servicio de Ethical Hacking para una importante entidad gubernamental chilena, gestionando y ejecutando evaluaciones de seguridad en múltiples entornos: Web, API, Mobile, Thick Client y Wi-Fi.
- Ejecución de simulaciones avanzadas de ciberseguridad mediante playbooks ofensivos, incluyendo phishing, ingeniería social, compromiso de endpoints y escenarios de respuesta ante ransomware, con foco en evaluación de controles, concientización y respuesta organizacional.
- Apoyo al centro de Hacking de NTT DATA España en la ejecución de ejercicios de Ethical Hacking Web y API para clientes internacionales.

Práctica Profesional II | Enero 2023 – Marzo 2023

- Ejecución de ejercicios de Ethical Hacking Web, identificando vulnerabilidades, documentando hallazgos técnicos y proponiendo recomendaciones de remediación.
- Diseño e implementación de un sitio web vulnerable desplegado en máquina virtual con fines educativos, incluyendo elaboración de informe técnico de vulnerabilidades y walkthrough detallado como parte de un workshop de seguridad en la Universidad de Concepción.

Práctica Profesional I | Enero 2022 – Marzo 2022

- Apoyo en la documentación de un proyecto Cloud Zero Trust basado en Microsoft Azure.
- Desarrollo de artefacto de cumplimiento para controles de seguridad en APIs, orientado a apoyar la evaluación y documentación de buenas prácticas de seguridad.

PROYECTOS DESTACADOS

BINMO: Bullying is no more **Enero 2022 – Diciembre 2022**
Desarrollador Full Stack *Santiago, Chile*

- Diseñé e implementé componentes backend y móviles para una solución full-stack orientada a instituciones educativas, integrando APIs, persistencia de datos y lógica de aplicación.
- Proyecto reconocido con el Premio Excelencia Académica en la Feria de Software USM 30° Edición, 2022.

FORMACIÓN ACADÉMICA

Universidad Técnica Federico Santa María **Octubre 2024**
Ingeniería Civil Informática *Santiago, Chile*

- Tesis: "Alexandria: Web-App platform that stores mobile applications and the result of their analysis from a focus on information privacy". Nota máxima: 100/100.

CERTIFICACIONES

OSCP+ **Febrero 2026**
Offensive Security

eJPT **Marzo 2024**
eLearn Security

AZ-900 **Abril 2023**
Microsoft Azure

HABILIDADES TÉCNICAS

- **Cursos:** Android Application Security – Mobile Hacking Lab, 2026; Bug Bounty Hunter – Hack The Box, 2025; Introduction to Cybersecurity Tools & Cyber Attacks, 2020.
- ***Seguridad Ofensiva:*** Pentesting Web/API, pruebas de seguridad en aplicaciones móviles, pruebas de Thick Client, evaluaciones de seguridad Wi-Fi, Active Directory, enumeración de redes, explotación de servicios, escalamiento de privilegios en Linux/Windows, phishing, ingeniería social y OWASP Top 10.
- ***Herramientas:*** Burp Suite, Caido, Nessus, Nuclei, Metasploit, Nmap, ffuf, sqlmap, Wireshark, testssl.sh, Impacket, NetExec, BloodHound, Mimikatz, WinPEAS/LinPEAS, Kali Linux, Frida, Objection, MobSF, JADX.
- ***Desarrollo y Cloud:*** Python, JavaScript, TypeScript, Node.js, React, Bash, AWS, Azure, Docker, Serverless.
- ***Automatización e IA:*** Scripting e IA generativa aplicada al análisis técnico, documentación y flujos de trabajo de seguridad.
- **Áreas objetivo:** Application Security, Product Security, Mobile Security, Bug Bounty, CTFs y automatización aplicada a ciberseguridad**.**

IDIOMAS

- Español: Nativo.
- Inglés: C1 (TOEIC, 2022).