Juan Nemiña

Offensive Security Engineer
juan.nemina@outlook.com | LinkedIn | GitHub | Santiago, Chile

SUMMARY

Offensive Security professional and Computer Science Engineer with 3 years of experience performing Web, API, Mobile, and cloud security assessments in enterprise environments. Experienced in identifying real-world vulnerabilities, assessing technical and business impact, and communicating actionable findings to technical teams and stakeholders. Currently focused on Application Security, Product Security, and Offensive Security roles.

EXPERIENCE

NTT DATA **Jan. 2022 – Present**

Engineer | Mar. 2025 – Present *Santiago, Chile*

- Performed Ethical Hacking assessments across Web, API, and Mobile environments as part of the global security team of a multinational insurance company, supporting business units across multiple regions.
- Designed and implemented a vulnerable Windows-based CTF machine to support technical assessments for new hires, incorporating a realistic attack chain involving advanced web exploitation, exposure of internal services, and local privilege escalation.

Junior Engineer | Mar. 2023 – Mar. 2025

- Led and executed Ethical Hacking activities for a major Chilean government entity, managing security assessments across Web, API, Mobile, Thick Client, and Wi-Fi environments.
- Executed advanced cybersecurity simulations through offensive playbooks, including phishing, social engineering, endpoint compromise, and ransomware response scenarios, focused on control assessment, awareness, and organizational response.
- Supported NTT DATA Spain's Hacking Center in the execution of Web and API Ethical Hacking assessments for international clients.

Second Professional Internship | Jan. 2023 – Mar. 2023

- Executed Web Ethical Hacking assessments, identifying vulnerabilities, documenting technical findings, and proposing remediation recommendations.
- Designed and implemented a vulnerable website deployed on a virtual machine for educational purposes, including the preparation of a technical vulnerability report and a detailed walkthrough as part of a security workshop at the University of Concepción.

First Professional Internship | Jan. 2022 – Mar. 2022

- Supported the documentation of a Cloud Zero Trust project based on Microsoft Azure.
- Developed a compliance artifact for API security controls, aimed at supporting the assessment and documentation of security best practices.

SELECTED PROJECTS

BINMO: Bullying is no more **Jan. 2022 – Dec. 2022**

Full Stack Developer *Santiago, Chile*

- Designed and implemented backend and mobile components for a full-stack solution aimed at educational institutions, integrating APIs, data persistence, and application logic.
- Project recognized with the Academic Excellence Award at the 30th USM Software Fair, 2022.

EDUCATION

Universidad Técnica Federico Santa María **Oct. 2024**
B.S. in Computer Science *Santiago, Chile*

- Thesis: "Alexandria: Web-App platform that stores mobile applications and the results of their analysis from an information privacy perspective." Highest grade: 100/100.

CERTIFICATIONS

OSCP+ **Feb. 2026**
Offensive Security

eJPT **Mar. 2024**
eLearn Security

AZ-900 **Apr. 2023**
Microsoft Azure

SKILLS

- **Courses:** Android Application Security – Mobile Hacking Lab, 2026; Bug Bounty Hunter – Hack The Box, 2025; Introduction to Cybersecurity Tools & Cyber Attacks, 2020.
- ***Offensive Security:*** Web/API Pentesting, Mobile Application Testing, Thick Client Testing, Wi-Fi Security Assessments, Active Directory, Network Enumeration, Service Exploitation, Linux/Windows Privilege Escalation, Phishing, Social Engineering, OWASP Top 10.
- ***Tools:*** Burp Suite, Caido, Nessus, Nuclei, Metasploit, Nmap, ffuf, sqlmap, Wireshark, testssl.sh, Impacket, NetExec, BloodHound, Mimikatz, WinPEAS/LinPEAS, Kali Linux, Frida, Objection, MobSF, JADX.
- ***Development & Cloud:*** Python, JavaScript, TypeScript, Node.js, React, Bash, AWS, Azure, Docker, Serverless.
- ***AI & Automation:*** Scripting and generative AI applied to technical analysis, documentation, and security workflows.
- **Target Areas:** Application Security, Product Security, Mobile Security, Bug Bounty, CTFs, and cybersecurity automation.

LANGUAGES

- English: C1 English proficiency (TOEIC, 2022).
- Spanish: Native.