Diego Espejo

despejo1507@gmail.com | linkedin.com/in/diego-espejo-spiegel | github.com/spiegelin | +61 414 831 235

Education

Instituto Tecnológico y de Estudios Superiores de Monterrey — Guadalajara, Mexico
B.S. in Computer Science and Technology (GPA: 97/100) — *Aug. 2022 – May. 2025*

Macquarie University — Sydney, Australia
M.S. in Information Technology in Cyber Security — *Jul. 2025 – Jul. 2026 (expected)*

Certifications & Credentials

Offensive Security Certified Professional (OSCP+), CompTIA Security+, SC-200, Google Cybersecurity Specialization.

Experience

Cybersecurity Intern — February 2024 - July 2025
Avertium — *Phoenix, US*

- Attained practical expertise in configuring and securing operating systems, networks, and cloud services.
- Employed Security Information and Event Management (SIEM) tools (Splunk, AlienVault, Sentinel, LogRhythm) to safeguard networks, devices, and data.
- Identified and analyzed common risks, threats, and vulnerabilities, while acquiring proficiency in applying mitigation techniques, incident response, and threat hunting.
- Gain knowledge in Intrusion Detection Systems (IDS), Network Intrusion Detection Systems (NIDS), NIST CSF, GRC, TTPs, and scripting languages.
- Managed and monitored Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions to detect, investigate, and respond to advanced threats.
- Performed enterprise penetration tests and analyzed potential vulnerabilities by using security tools like Nessus, Burp Suite, Bloodhound, PowerView, Cobalt Strike, and Nmap.
- Utilized PlexTrac for documenting findings, streamlining reporting, and collaboration.

Projects

PyFuscator | *Python, AST, Powershell, C#, Regex* — May 2025

- Designed and implemented a cross-language code obfuscation tool supporting Python, PowerShell, and C#.
- Developed a solution to bypass modern security tools and signature-based detection systems.
- Supported red team operations by creating obfuscated payloads that evade endpoint protection platforms (EPPs) and traditional antivirus solutions.
- Engineered multiple encryption methods including RSA-like algorithms, XOR with key arrays, and multi-layer ciphers to protect sensitive code and intellectual property from reverse engineering attempts.

Nessus Mobile | *Docker, FastAPI, React-Native, Tenable, Dehashed, Hunter, Shodan, Crawler* — November 2024

- Developed an Integrated Multi-Tool Scanning Solution offering active and passive vulnerability scanning.
- Leveraged OSINT techniques to collect and analyze data on domains, IPs, and individuals, providing comprehensive reports to discover security risks.
- Implemented real-time detection of web vulnerabilities and associated CVEs, offering mitigation strategies.
- Performed automated reports with tailored recommendations.

LLMNR/NBT-NS Poisoning Tool | *Python, Network Protocols, OS Sockets, Impacket, Hashcat* — August 2024

- Developed a tool for LLMNR/NBT-NS poisoning, intercepting network traffic to harvest NTLM hash credentials.
- Enabled SMB relay attacks by integrating Impacket's ntlmrelayx, allowing captured credentials to be relayed for unauthorized access.
- Automated NTLM hash cracking by triggering hashcat upon capture, thus, accelerating post-exploitation.
- Created efficient logging for captured and cracked credentials, enhancing post-attack analysis and reporting.

Technical Skills

Programming Languages: C/C++, C#, JavaScript, Python, Go.
Developer Tools: Git, Wireshark, VS Code, Ghidra, Burp Suite, Impacket, Nmap, Hashcat.
Frameworks & Libraries: Cobalt Strike, Sliver, Metasploit, BeEF, Bloodhound, NetExec.
Languages: Spanish (Native), English (C1), German (B1).