(312) 555-4567

maria.perez@gmail.com

United States, Chicago, IL

Maria Perez

EDUCATION

Bachelor of Science in Cybersecurity, DePaul University, United States, Graduated: May 2016

Certifications

- **Offensive Security Certified Expert (OSCE)**, November 2021
- **Certified Red Team Professional (CRTP)**, July 2020
- **Certified Ethical Hacker (CEH)**, March 2018

SKILLS

Red teaming and adversary emulation	**Expert**
Physical security testing	**Expert**
Social engineering and phishing	**Expert**
Exploiting network and web application vulnerabilities	**Expert**
Scripting and automation (Python, Bash)	**Expert**
Security control testing and bypass techniques	**Expert**
Post-engagement reporting and presentations	**Expert**
Security monitoring and detection evasion	**Expert**

AWARDS

Outstanding Red Team Achievement Award – January 2023

Employee of the Year – December 2018

LANGUAGES

Spanish – Native

Italian – Fluent

Lead Red Team Pentester

PROFESSIONAL SUMMARY

Proactive and creative Red Team Pentester with experience in simulating adversarial attacks, exploiting vulnerabilities, and testing security controls to improve organizational security posture. Passionate about mimicking real-world threat actors to identify potential gaps in security defenses.

EXPERIENCE

Lead Red Team Pentester, Advanced Security Solutions, Chicago, IL

January 2021 - Now

- Lead red team engagements for multiple high-profile clients, simulating advanced persistent threats (APT) and spear-phishing attacks.
- Execute complex attack chains, including initial exploitation, lateral movement, privilege escalation, and exfiltration of sensitive data.
- Develop custom attack tools and scripts to bypass security defenses and test detection mechanisms.
- Provide detailed after-action reports with recommendations for strengthening organizational security.
- Mentor junior pentesters and red team members on attack tactics and methodologies.

Red Team Pentester, Cyber Defense Solutions, Chicago, IL

June 2016 - December 2020

- Simulated adversarial techniques to test security systems and assess vulnerability management processes.
- Engaged in threat emulation exercises, including physical security testing, social engineering, and wireless network attacks.
- Conducted post-engagement debriefings with clients to improve defensive measures.
- Automated penetration testing tasks and developed scripts to streamline security assessments.