

CHRISTOPHER J. PITILLO

Tampa, Florida 33602 • Phone: (919) 924-8442 • Email: chrispitillo@gmail.com

LinkedIn: www.linkedin.com/in/christopher-pitillo • Website: chrispitillo.com

Active TS/SCI Clearance

Penetration Tester

Summary

Penetration tester and red team operator with experience executing stealthy, adversary-emulated attacks across enterprise environments, including Active Directory, web applications, and human attack surfaces. Strong background in exploit review/tailoring/execution, command-and-control frameworks, social engineering, and OSINT, supported by hands-on use of offensive security toolkits as well as development in several programming languages. Security-first practitioner with experience building privacy-preserving systems, including local LLM workflows for offensive security support. Highly skilled at communicating technical risk to both engineering teams and senior leadership. Seeking an offensive security position where tradecraft and engineering directly improve defensive outcomes.

CORE SKILLS

Red Teaming • Penetration Testing • Software/Exploit Development • Computer Networking • Scripting
Social Engineering • Wireless Pentesting • Web Application Exploitation • Vulnerability Reporting

• **Programming Languages:** Python, C, JavaScript, PHP, Ruby, Bash, Powershell, HTML, CSS, SQL

• **Operating Systems:** Linux/UNIX (Kali, Ubuntu), Windows, Active Directory (AD), macOS

PRACTICAL PROJECTS – GitHub link: <https://github.com/SierraActual>

Hacking YouTube Series – <https://www.youtube.com/@ChrisCanPwnIt>

• Developed 10-15min walkthroughs for Hack the Box machines specifically chosen to align with common mid-level hacking certifications such as the OSCP.

Python Hacking Tools – <https://github.com/SierraActual/pythonHacking>

• Built custom penetration testing scripts in Python for ARP/DNS spoofing, network scanning, MAC spoofing, website crawling, as well as multiple malware executables.

Air Force Evaluation Tool – <https://github.com/SierraActual/PythonAFProject>

• Developed a Python program that automated error detection in Air Force annual evaluations, reducing proofreading time and significantly lowering submission errors in official reports, saving hundreds of hours of review.

Automated Recruitment Assistant – <https://github.com/SierraActual/Text-Bot>

• Created a Python automation tool that parsed CSV files of applicant data and delivered personalized text messages, streamlining recruitment outreach, improving candidate engagement efficiency, and saving 15+ hours of work *weekly*.

PROFESSIONAL EXPERIENCE

Red Team Operator, *Maveris – Remote*

Nov 2025 – Present

- Conducted stealthy, adversary-emulated security assessments against applications supporting over 9 million users, reviewing 150k+ lines of source code and identifying critical vulnerabilities resulting in full user data compromise, with detailed reporting and remediation guidance delivered to engineering teams.
- Executed offensive operations including exploit obfuscation, command-and-control (C2) infrastructure, and advanced web application exploitation techniques aligned with real-world threat actor tradecraft.
- Designed and deployed red-team infrastructure using Cobalt Strike, GoPhish, Evilginx, and related orchestration tooling to support large-scale social engineering and C2 operations across a 50-member team.

Security Specialist, *U.S. Central Command – Tampa, FL*

Jan 2022 – Aug 2025

- Oversaw force protection programs for military security operations in the Middle East, translating technical concepts to senior leadership to include Secretary-level US government officials.
- Led threat modeling and security assessments across 200+ physical and information systems spanning 19 military bases in 20 countries, identifying 500+ vulnerabilities and coordinating remediation efforts across multiple U.S. government organizations and military branches to protect 50,000+ personnel.

- Coordinated development of an internal LLM-powered search capability to analyze 20,000+ pages of strategic planning documentation, annually saving hundreds of man-hours each for 5,000+ users.
- Executive Officer**, *Air Force ROTC Headquarters – Maxwell Air Force Base, AL*

Jun 2021 – Jan 2022
- Recognized as the top officer among peers for leadership, critical-thinking, and organizational impact through innovation.
 - Served as the “right-hand” of the Commander, providing executive-level support and order collaboration for 145 units across the nation.
 - Oversaw a 16,000-member training organization, conducting performance reviews; responsible for producing 1,000 USAF officers annually.

EDUCATION

Bachelor’s Degree in Criminal Justice, *University of North Carolina At Charlotte, NC*

Jun 2014

CERTIFICATIONS

Certified Red Team Operator (CRTO) Zero Point Security	In Progress
OSCP+ Offensive Security Certified Professional from OffSec	Sep 2025
eJPT eLearnSecurity Junior Penetration Tester from INE Security	Mar 2024
Google IT Automation with Python Professional Certificate from Google	May 2025
Google Cybersecurity Certificate from Google	Sep 2023

Current Projects

Built a local 20B-parameter LLM using Docker Desktop and Open WebUI, integrating it into an MCP-based workflow to automate tasks while preserving data privacy. Designed with offensive security constraints in mind, the system processes sensitive inputs without external APIs and will support sample use cases such as resume tailoring, video note-taking, and future red-team workflows including reporting and reconnaissance. Demonstrates applied experience with containerization, automation, and secure AI integration to save hundreds of hours of manual labor.

Active interest in AI penetration testing to include advanced methods of prompt injection, model evasion, tool-calling abuse, and adversarial testing of LLM-powered workflows to identify privilege escalation, data exfiltration, and policy bypass risks in real-world AI integrations.