Nicholas Lanza

IT Technician (Penetration Tester)

215-459-1090
nicholas.lanza@proton.me

Skills

- Burpsuite
- Metasploit
- OWASP Top 10
- Impacket Toolkit
- Bloodhound
- Impacket Toolkit
- Docker
- VirtualBox
- Python

Summary

OSCP-certified IT Technician with 5 years of hands-on experience in Windows, Active Directory, and Microsoft 365 support. Proven offensive security skills through the OSCP Certification, Hack The Box competitions and full AD attack labs. Seeking a position where I can apply and continue developing practical exploitation skills

Work Experience

IT Technician — New Life of Community Health 2020–2025

- Supported over 30 Windows users across the main office, resolving hardware, software, and network issues.
- Managed user accounts in Microsoft 365 Admin Center, handling onboarding, offboarding, and credential updates.
- Assisted with maintaining Microsoft 365 security configurations, with awareness of CISA SCuBA baseline recommendations.
- Conducted bi-weekly system performance tests, improving network reliability, and reducing downtime.
- Performed monthly server maintenance, applying firmware, and software updates while managing changes to maintain reliable operations.
- Provided basic website updates and maintenance in Wix, keeping pages functional and up to date.
- Supported IT systems and cloud services handling Protected Health Information (PHI) in compliance with organizational policies.

Certifications

Offensive Security Certified Professional Plus (OSCP+) 2025

- Identified, exploited, and documented a wide range of vulnerabilities under time constraints across Windows, Linux, and Active Directory.
- Compiled detailed reports using the outlining findings, exploitation steps, and recommended remediation actions.
- Actively maintained OSCP+ skills and certification through OffSec's renewal program by completing regular practical exercises to stay current with offensive security techniques.

Projects

Hack The Box Season 8 (Team Competition) 2025

- Worked with a team and achieved a Top 25 global team ranking and a Top 800 individual ranking among thousands of competitors.
- Completed 13 machines across Windows and Linux, demonstrating strong capability in a variety of techniques.
- Utilized Burpsuite and the OWASP Top 10 to exploit 5 different web-hosts testing and using techniques like local file inclusion, remote code execution, And template injection.
- Used Metasploit on 4 machines to gain user level access and enumerate multiple privilege escalation vectors.

VirtualBox Active Directory Homelab 2024

- Built a Virtual Active Directory lab environment using VirtualBox and Docker, including 2 forests, 3 Domains and both Windows and Linux hosts to strengthen Active Directory Exploitation Techniques.
- Utilized Bloodhound to enumerate Access Control Entries and achieve Domain Compromise.
- Extracted and cracked the Security Manager Database hashes using the Impacket Toolkit and Hashcat.