MOSTAFA AKKAD

Lebanon mostafaakkad@protonmail.com +961 76379304

SUMMARY

Security professional with a background in both offensive and defensive security. I've built my skills from the ground up from studying penetration testing and Active Directory attacks to working daily in a live SOC environment handling real incidents across multiple client environments. I'm comfortable on both sides of the fence and I pick things up really fast.

EDUCATION

Information Technology, Sidon Technical School.

CERTIFICATIONS

Practical Ethical Hacking (PEH), Windows Privilege Escalation (WPE), Linux Privilege Escalation (LPE) — TCM

Junior Penetration Tester, Introduction to Cyber Security, Web Fundamentals — TryHackMe

External Pentest Playbook (EPP), Open Source Intelligence Fundamentals (OSINT) — TCM

Python 101 for Hackers, Python 201 for Hackers, Linux 101 — TCM

CompTIA Pentest+, A+, Network+ | Cisco CCNA

EXPERIENCE

SOC Analyst
Capital Outsourcing
- Conduct advanced incident investigations beyond typical L1 scope, performing root cause analysis and coordinating remediation across affected systems.
- Execute proactive threat hunting across endpoints and networks using MITRE ATT&CK techniques to identify sophisticated adversary behavior before alert escalation.
- Monitor, triage, and investigate security alerts across FortiEDR, Microsoft Sentinel, Wazuh, Defender XDR, and CRM platforms.

SOC Analyst
Potech-Consulting
- Monitored network traffic and SIEM alerts, identifying and escalating potential threats in a timely manner.
- Responded to security incidents to contain and resolve issues.
- Analyzed suspicious activity patterns using SIEM tooling to support detection rule tuning.

Network Technician
MK Technology
- Installed and maintained surveillance systems and LAN networks.
- Diagnosed and optimized installations for seamless performance.

PROJECTS

AD Home Lab
- Built an Active Directory lab environment, including domain controller setup, user machine configuration, and Group Policy implementation.
- Applied AD attack vectors including LLMNR poisoning, SMB relay attacks, IPv6-based attacks, and various pass-the-hash/ticket techniques.
- Performed post-compromise enumeration and domain mapping using BloodHound, PlumHound, and PingCastle.
- Implemented post-compromise attacks such as credential dumping, NTDS.dit extraction, Kerberoasting, token impersonation, and Golden Ticket attacks.

LABS & CTF EXPERIENCE
TryHackMe
Completed 199 rooms and obtained 25 badges, placing me in the top 1% of users.

HackTheBox
Smashing through HackTheBox CTF's, and preparing for the CPTS certification as well as many others.