MOSTAFA AKKAD

Lebanon   mostafaakkad@protonmail.com   https://medium.com/@av3rnuz

OBJECTIVE

Tech enthusiast with a strong background in ethical hacking, penetration testing, vulnerability analysis, and network security. Seeking a cybersecurity role to leverage my skills and contribute to the organization's success while continuing to grow and learn

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
Potech-Consulting

- Monitored network traffic and alerts for potential threats.
- Responded to security incidents to contain and resolve issues.
- Utilized SIEM to detect and analyze suspicious activity

Network Technician
MK Technology

- Installed and maintained surveillance systems and LAN networks.
- Diagnosed and optimized installations for seamless performance.

Technical Support
Scope Gaming Lounge

- Addressed client technical problems and ensured smooth functioning of lounge server.
- Oversaw technical operations for client satisfaction and operational efficiency.

PROJECTS

AD Home Lab

- Successfully built an Active Directory lab environment, demonstrating proficiency in domain controller setup, user machine configuration, and policy implementation.
- Applied various attack vectors including LLMNR poisoning, SMB relay attacks, IPv6 attacks, and pass attacks.
- Conducted post-compromise enumeration using tools like Bloodhound, Plumhound, and PingCastle.
- Implemented post-compromise attacks such as Kerberoasting, token impersonation, and credential dumping using tools like Mimikatz.
- Developed and executed post-compromise attack strategies, including dumping the NTDS.dit file and executing Golden Ticket attacks.

Capture the Flag (CTF) Challenges
TryHackMe

Completed 192 rooms and obtained 21 badges, placing me in the top 1% of users.

GitHub Projects
https://github.com/0Pa1

- InfiltraSSH : Username and Password SSH Brute-Force
- Crack256 : SHA256sum hash cracker
- BruteForceBuddy : Username and Password Web login Brute-Force