Ahmad Abou El Kheir *Cyber Security*

ahmad_k2001@hotmail.com
+961 70048296
linkedin.com/in/ahmad-abou-el-kheir

EDUCATION

BS in Computer Science

Lebanese American University 01/2022 - 05/2024 | Beirut, Lebanon

CERTIFICATIONS

Google Cybersecurity Professional Certification

eJPTv2 (in progress, almost done)

PROJECTS

- **Malware Analysis**
  Investigated a malicious Android application to understand its behavior and impact. I started by setting up Genymotion, an Android emulator, to safely test the app without risking my actual device. Using Burp Suite, I intercepted and analyzed network requests made by the application to uncover its communication patterns and potential data exfiltration methods. Through this analysis, I was able to identify the app's malicious activities, including unauthorized data transmission and potential security vulnerabilities.
- **Incident Handler's Journal**
  Reviewed the details of a security incident and documented the incident using the incident handler's journal. included a description of the journal entry, outlined the details of the incident investigation using the 5 W's, Included the tools used such as Chronicle and Virus Total, included additional thoughts or questions.
- **Other Practical Security Projects**

TryHackMe

Active user on TryHackMe for 2+ years, where I gained practical experience and knowledge in the following areas:

- Penetration Testing & Vulnerability Assessment
  Hands-on experience in identifying and exploiting vulnerabilities through interactive challenges and labs.
- Network Security
  Practical skills in network scanning, traffic analysis, and threat detection.
- Cyber Security Tools
  Proficiency with tools such as Burp Suite, Metasploit, Nmap, Wireshark, Kali Linux and Many more.
- Security Hardening
  Application of security best practices to strengthen systems and applications against threats.
- Threat Analysis & Incident Response
  Experience in analyzing security incidents and responding.

SKILLS AND TECHNOLOGIES

Network Security Groups, Firewalls, ACLs, VMs, Active Directory, File Permissions, Linux, Vulnerability Scanning and Assessment, Python, SQL, Wireshark, Nmap, Various Password Cracking Tools, Operating Systems, Cryptography, OWASP, Privilege Escalation, Incident Escalation, Log Analysis and Reporting, Threat Detection, Incident Documentation, OSINT, Risk Assessment, Security Mindset, Verbal and Written Communication Skills, Web App Technologies, Quick Learning Abilities, Continuous Learning.