TAMEEN KASSEM

Toronto, Canada • tameenyt@gmail.com • + 1 (647) 325-9717 • https://www.linkedin.com/in/tameen-kassem-88a09226a/

PROFESSIONAL EXPERIENCE

PARTYSOCIAL **Dubai, UAE**
Network Solutions Consultant **October 2024 - January 2025**

- Seamlessly connected multiple networks, allowing devices to communicate across them efficiently.
- Designed a Layer 2 Wi-Fi bridging solution, and implemented Access Points (AP) to bridge the networks.
- Manually assigned static IPs to key devices, and tested to ensure efficient communication.
- Conducted latency tests and optimized network settings, reducing network response time by 50%.
- Implemented email protection for phishing on Google Workspace.
- Created SPF, DKIM and DMARC records, adding them to the DNS to prevent email spoofing.
- Performed incident response and remediation, quarantining a system following an email-based attack.
- Performed analysis using DeepBlueCLI and Windows Event Viewer on a compromised system.
- Used hashing tools via PowerShell and CMD to generate file hashes to cross-reference with OSINT tools.

LOG IMPACTFUL TECH SOLUTIONS **Lisbon, Portugal**
Cyber Security Analyst **June 2024 -August 2024**

- Learned and utilized GVM and OpenVAS, a network security scanner, to configure and deploy a vulnerability scanner, which was used to perform reconnaissance and assess exposure via specific ports and hosts on the target network.
- Disabled unused ports and services and eliminated false reports to address vulnerabilities in the network.
- Developed a virtual machine (VM) with a pre-configured vulnerability scanner for company-wide use.
- Wrote official documentation to conduct system scanning, standardizing deployment and ensuring operational efficiency.

VOGACLOSET **Amman, Jordan**
Network Security Analyst **May 2023 - May 2024**

- Conducted phishing analysis using OSINT tools (URL2PNG, VirusTotal, domain analysis) to verify email authenticity.
- Reduced phishing email delivery by 30% through email quarantining, email filtering and sender blocking.
- Investigated suspicious attachments in sandboxed VMs, identifying malicious executables via Autopsy.
- Analyzed PCAP logs in Wireshark, isolating malicious traffic and attack patterns.
- Used Splunk to detect anomalies, visualize security threats, and analyze persistence mechanisms in compromised systems.
- Recommended remediation steps to address varying levels of security incidents.

MACDONALD SAGER MANIS LLC **Toronto, Canada**
Law Firm Summer Internship **2018 and 2019**

CERTIFICATIONS

SECURITY BLUE TEAM **February 2025**
Blue Team Level 1 Junior Defensive Cybersecurity Certification | **Gold Coin Recipient**

GOOGLE CLOUD PROFESSIONAL **November 2024**
Associate Cloud Engineer Certification

COMPTIA **February 2024**
Security+ (Plus) Certification

EDUCATION

UNIVERSITY OF TORONTO SCHOOL OF CONTINUING STUDIES; ***Cybersecurity Program*** **February-August 2023**

UNIVERSITY OF TORONTO; ***Bachelor of Arts, Major in Criminology; Major in Sociology*** **2017-2022**

PROJECTS

HACKTHEBOX
Cybersecurity Practitioner **February 2024-Present**

- Ranked top 800 globally in vulnerability assessment and penetration testing, developing skills in cryptography, reverse engineering and forensic analysis.
- Conducted over 20 penetration tests, identifying critical vulnerabilities (SQL injection, XSS, buffer overflows).
- Performed network reconnaissance using Nmap and Burp Suite for web security testing.
- Exploited vulnerabilities via Metasploit payloads and documented remediation strategies.
- Developed PowerShell & Bash scripts for reverse-shell attacks and persistence techniques.

TECHNICAL SKILLS

- **Security & Forensic Tools:** Splunk, TheHive, DeepBlueCLI, Windows Event Viewer, Autopsy, FTK Imager, Volatility, CyberChef, Scalpel, KAPE, PECMD, Virustotal, URL2PNG, WannaBrowser, ProcDump
- **Network Security & Penetration Testing**: Wireshark, Burp Suite, Nmap, Metasploit, Powershell/Bash Scripting
- **System & Incident Response:** Case Management, Digital Forensics, Windows Event Logs, File Recovery, Browser History Analysis, MITRE ATT&CK, SIEM analysis