Usama Ghawji

(416) 877-4388 • LinkedIn • My Website • u.ghawji@gmail.com

OBJECTIVE

Usama is a detail-oriented creative thinker, a problem solver, and a life-long learner. As a recent graduate with an Honors B.Sc. in Computer Science, Usama is seeking to start his career focusing on detecting threats, remediating vulnerabilities, and proactively securing networks - making distinctive, lasting, and substantial improvements to the threat landscape. Usama is experienced in network intrusion prevention and detection, vulnerability management, threat hunting, and security compliance. A meticulous cybersecurity enthusiast, Usama works independently and thrives in a fast-paced, team-oriented environment.

EDUCATION

York University | Honours B.Sc. - Computer Science Specialized in Cybersecurity June 2017- April 2022

- **Relevant Coursework**
  - Network Security & Forensics
  - Computer Security Lab
  - Introduction to Computer Security
  - Computer Network Protocols
- **Experience Venture Award** | YSpace
  - Awarded for excellence in disruptive innovation, entrepreneurial thinking, and leadership skills
- **Graduation Project**
  - **Developing & Securing Helpdesk WebApp** | *HTML, PHP, SQL, Hydra, BurpSuite, ZAP, SHA-256, SALT*
    - The aim of this project was to develop a helpdesk web application that is secure from the ground up. The project lasted 4 months, which is why I broke it into 4 phases. Phase 1 included using Agile methodology to utilize one server, one SQL database, develop the front-end in HTML, CSS, and JavaScript, and the backend code in PHP. Phase 2 included conducting penetration testing through Hydra, Burp Suite, and ZAP where I tested the web-app against various attacks such as: password cracking, brute-force attacks, dictionary attacks, SQL injection, XSS, and CSRF. Phase 3 included patching the vulnerabilities found after the penetration testing reports, where I sanitized the code, added an extra layer of security by hashing & salting passwords. In Phase 4, I presented a 20-minute presentation to 40+ students including a live demo of the web-app, the penetration testing report, the fixes, and what future enhancements I would make.
    - Over the course of this project, I conducted pen-testing, vulnerability management, and utilized excellent communication skills to present my findings to the class.

EXPERIENCE

SOC Analyst Intern June 2019 - Sept. 2019

Johns Hopkins Aramco Healthcare | Saudi Aramco, KSA

- Constructed informative dashboards and reports in **SPLUNK** based on use cases to identify vulnerabilities, resulting in intercepting an .exe file before any malicious code was executed
- Engineered **SPLUNK** threat detection queries to cover **7** areas of the **MITRE ATT&CK** framework and further cyber threat hunting capabilities.
- Configured **Next-Gen Firewall** rules to block malicious traffic and filter out phishing emails, reducing DoS attempts by 15%
- Identified areas of weakness in business processes and suggested improvements, ensuring compliance with industry standards and slashing risks by an average of 30%

Co-Founder & Director of Operations Aug. 2020 - April 2022

Lassonde Security Club @ York University | Toronto, Canada

- Co-founded the first cybersecurity club at YorkU, gaining over 100 members in 3 months
- Educated 20+ students on the basics of **Wireshark** including UI, capture filters, and analyzing network
- Created and implemented cyber security-specific workshops, tools, and guest speakers for university students

CERTIFICATIONS

- **Splunk Fundamentals 1** - April 2021
- **Splunk User Behavior Analytics (UBA)** - May 2021

- **Fortinet Network Security Expert** - March 2021
- **CompTIA CySA+, ISO/IEC 27001** - *In progress*

PROJECTS

- **Snort - NID and IPS |** *Snort, Network Intrusion Detection, Intrusion Prevention System, Wireshark* **April 2022**
  - Configured Snort rules to detect intrusions. Created custom ICMP rules and ran them against the York University server to trigger alerts.
  - Installed Snort onto Kali Linux VM and established correct network address range
  - Used Wireshark to track custom-made ICMP packets

- **Reconnaissance and Exploitation |** *Kali Linux, Nmap, Metasploit, Azure Virtual Lab, Vsftpd, Samba, SMTP* **February 2022**
  - Conducted a port scan using Nmap to identify all open ports/services running on the target machine
  - Used Nmap with -A flag: this option enables OS detection, version detection, script scanning and traceroute
  - Utilized Metasploit to conduct attacks on Vsftpd, Samba, and SMTP
  - Reviewed payloads and their effects on the target machines after exploit

- **Social Engineering |** *Kali Linux, SEToolKit* **January 2022**
  - Conducted a watering hole attack on common websites with the aim of gathering unsuspecting users' credentials
  - Used the SEToolkit in a Kali Linux Virtual Machine to clone websites such as Facebook, Gmail, and Twitter to harvest credentials
  - Learned the social engineering techniques used by malicious attackers

SKILLS

- **Softwares:** Splunk, Wireshark, Kali Linux, Palo Alto Next-Generation Firewall, Power BI, Microsoft Suite
- **Frameworks:** ISO 27001, MITRE ATT&CK, Cyber Kill Chain, Zero Trust Network Architecture
- **Knowledge:** Industrial Security, GRC, Incident Response, Vulnerability Management, CIA, Social Engineering, Risk Management, TCP/IP, Networking, TLS, HTTPS, Certificates, OSI, Firewalls, VPNs, Routers, Proxy, IPsec, Indicator Management, Threat Hunting, Malware, Indicators of Compromise.