JAMAL SHERIF

Minneapolis, Minnesota, United States jamalsherif2@gmail.com (612)458-5076 in/jamal-sherif-49495a33b jamalsheri-portforlio.base44.app

SUMMARY

Cybersecurity student pursuing a B.S. in Cybersecurity with strong foundations in threat detection, network security, and incident management. Experienced in applying access control, incident response, and compliance monitoring through professional security roles. Skilled in Wireshark, Nmap, and Microsoft Office Suite, with CompTIA Security+ and AWS Cloud Practitioner certifications. Dedicated to protecting digital and physical environments by combining technical expertise with proven leadership and communication skills.

EXPERIENCE

Security Officer (SOC)

Metro One Security **September 2022 - February 2025**

- Use tools like SIEM (Security Information and Event Management) systems to track network traffic, logs, and alerts for unusual behavior.
- Identify security incidents such as malware infections, phishing attempts, or data breaches, and take immediate action to contain and mitigate them.
- Investigate alerts, assess their severity, and determine whether they are real threats or false positives.
- Document incidents, findings, and responses in detailed reports for management or compliance purposes.
- Stay updated on new attack techniques and vulnerabilities to improve response strategies.
- Work with IT and cybersecurity teams to strengthen overall network defenses and prevent future incidents.

Security Guard (SOC)

Brosnan Risk Consultants **September 2021 - September 2022**

- Use tools like SIEM (Security Information and Event Management) systems to track network traffic, logs, and alerts for unusual behavior.
- Identify security incidents such as malware infections, phishing attempts, or data breaches, and take immediate action to contain and mitigate them.
- Investigate alerts, assess their severity, and determine whether they are real threats or false positives.
- Document incidents, findings, and responses in detailed reports for management or compliance purposes.
- Stay updated on new attack techniques and vulnerabilities to improve response strategies.
- Work with IT and cybersecurity teams to strengthen overall network defenses and prevent future incidents.

Support Help Desk

G4S Secure Solutions **March 2021 - September 2021**

- Served as the first point of contact for IT-related issues, providing technical support for hardware, software, and network connectivity.
- Logged, prioritized, and resolved user tickets through the internal help desk system, escalating complex issues to higher tiers when necessary.
- Assisted with account setup, password resets, and basic system administration tasks under security policy guidelines.
- Supported endpoint maintenance including device imaging, software installation, and Windows updates.
- Delivered prompt, customer-focused support while maintaining compliance with company security standards and data protection protocols.

PROJECT

Encryption to Enhance Confidentiality and Integrity

VmWare

- Created and exchanged asymmetric encryption key pairs and verified fingerprints using GPG.
- Applied asymmetric encryption to secure files, then decrypted them to confirm data integrity.
- Used symmetric encryption for file protection, documenting strong password practices
- Implemented hybrid cryptography by encrypting/decrypting secret keys and transferring them securely.
- Digitally signed and verified documents using Kleopatra, gaining hands-on experience with digital signatures, certificate management, and secure file exchange.

Assessing Common Attack Vectors

VmWare

- Simulated injection attacks (SQLi, XSS), capturing evidence of successful exploits like admin logins and DOM-based injections
- Executed a malware payload using Metasploit's msfvenom, analyzing system info and access gained.
- Performed a Distributed Denial-of-Service (DDoS) attack on a test target, observing network congestion and host recruitment into a botnet.
- Designed a social engineering phishing campaign using SET, successfully creating and testing phishing email payloads.
- Recommended layered defensive measures, including input validation, restricting active content, load balancing, botnet filtering, and security awareness training

Vulnerability Assessment and Penetration Testing

VmWare

- Performed network scanning with Nmap and Zenmap, identifying open ports, services, and OS details on lab servers
- Conducted vulnerability scans using Nessus and OpenVAS, documenting high-severity findings such as weak database credentials, outdated TLS protocols, and FTP backdoor vulnerabilities
- Developed a penetration test report that included CVSS scoring, risk evaluation, and remediation strategies (e.g., enforcing HTTPS, disabling anonymous FTP logins, patching vulnerable services)
- Delivered actionable recommendations to improve system security, demonstrating skills in vulnerability management and reporting.
- Engineered automated scripts to supplement manual penetration techniques, streamlining the identification and exploitation of application-level vulnerabilities while ensuring thorough documentation for compliance and audit purposes.

EDUCATION

Bachelor of Science, Cybersecurity

Metropolitan State University • St. Paul, Minnesota • 2026

CERTIFICATIONS

AWS Certified Cloud Practitioner

Network+

- In Progress...

AWS Certified Cloud Architect

- In Progress...

CompTIA Security+

2025

- Security+ is actually pretty useful because it shows I understand the basics of cybersecurity like how to protect data, recognize threats, and keep systems safe. Even outside of IT, it's relevant since almost every company deals with sensitive information now.

SKILLS

Skills 1: Wireshark, Nmap, CISCO (CIA triad), AAA, Encryption, Authentication, Access Control, Zenmap, SIEM, SQL, Python

Skills 2: Excel, Microsoft Word, Teams, Outlook,

Skills 3: English, Somali