

# JAMAL SHERIF

📍 Minneapolis, MN ✉ jamalsherif2@gmail.com 📞 (612)458-5076

---

## 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

#### Metro One Security

Sep 2022 – Feb 2025

- Monitored CCTV and managed facility access, applying principles of access control to prevent unauthorized entry.
- Responded to and documented incidents, creating reports that aligned with compliance and regulatory standards.
- Trained and mentored new personnel on safety protocols, improving team readiness and operational performance.

### Security Guard

#### Brosnan Risk Consultants

Sep 2021 – Sep 2022

- Conducted regular patrols to enforce policy compliance and reduce security risks.
- Collaborated with law enforcement during incidents, ensuring rapid and effective resolution.
- Oversaw site entry points, maintaining a secure environment and preventing unauthorized access.

### Security Guard

#### G4S Secure Solutions

Mar 2021 – Sep 2021

- Patrolled facilities to deter unauthorized access and security breaches.
- Logged and reported emergencies and incidents for organizational review and follow-up.
- Supported access control processes and maintained compliance with site regulations.

---

## PROJECT

### Encryption to Enhance Confidentiality and Integrity

May 2025 – September 2025

- 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**.
- Engineered a robust encryption workflow leveraging hybrid cryptographic techniques, facilitating secure file transfer and digital signature validation to reinforce confidentiality and data integrity throughout collaborative processes.

### Assessing Common Attack Vectors

May 2025 – September 2025

- 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

May 2025 – August 2025

- 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 • Minneapolis, MN • Expected Graduation: 2026

---

## CERTIFICATIONS

### CompTIA Security+

### AWS Certified Cloud Practitioner

### Network+

• In Progress...

### AWS Certified Cloud Architect

• In Progress...

---

## SKILLS

Wireshark, Nmap, CISCO (CIA triad), AAA, Encryption, Authentication, Access Control

Microsoft Office Suite

English, Somali

---