Mohamed Ashraf Abdallah Mohamed
Cybersecurity Student | SOC & Network Forensics Enthusiast
Zagazig University – Faculty of Computers and Information Technology | Expected Graduation: 2027
Email: mohamed.ashraf.abdallah65@gmail.com | LinkedIn: linkedin.com/in/mohamed-mooka | Phone: +20 112 115 4504 | Location: Egypt

---

Profile

Motivated and detail-oriented cybersecurity student with a strong foundation in networking, SOC operations, and digital forensics. Hands-on experience in network traffic analysis, SIEM monitoring (Wazuh & Splunk), and threat detection. Proven ability to apply theoretical knowledge in practical lab environments and real-world scenarios, including vulnerability discovery and responsible disclosure. Skilled in Python scripting for automation and log parsing. Passionate about continuous learning and advancing in cybersecurity defense and threat hunting.

Technical Skills

- **Networking & Protocols:** Deep understanding of OSI & TCP/IP models, protocol behavior, port numbers, and common vulnerabilities.
- **SOC & Threat Detection:** Wireshark (packet capture and analysis), Wazuh SIEM, Splunk (log monitoring, search, alerting), Windows event log analysis, network forensics.
- **Operating Systems:** Linux (command-line proficiency), Windows (Active Directory, domain basics).
- **Programming:** C++ (OOP fundamentals), Python scripting for automation and log parsing.
- **Cybersecurity Concepts:** Threat hunting, incident triage, vulnerability assessment, Security+ fundamentals.
- **Tools:** Wireshark, Wazuh, Splunk, VirtualBox/VMWare, fuzzing tools, Windows Event Viewer, Sysmon, Burp Suite.

Education

Zagazig University – Faculty of Computers and Information Technology
Bachelor's Degree in Computer Science | Expected Graduation: 2027

Certifications

- Network Security Practitioner (CNSP) – The SecOps Group
- Google Cybersecurity Professional Certificate
- Studied CompTIA Security+, SANS SEC450 (Blue Team Fundamentals), and eJPT content

---

Practical Experience & Projects

Ethical Hacking Trainee
National Telecommunication Institute (NTI) | Cairo, Egypt | Nov 2025 – Present

- Participating in an intensive training program focused on offensive security, penetration testing, and ethical hacking methodologies.
- Gaining hands-on experience with security tools and techniques used in real-world vulnerability assessment and exploitation scenarios.
- Enhancing understanding of network security, web application security, and defensive countermeasures.

Personal SOC Lab (Virtual Machines):

- Built and managed a custom SOC lab simulating SIEM monitoring, log analysis, and incident response workflows.
- Practiced real-time alert triage, threat detection, and containment strategies using **Wazuh and Splunk**.
- Developed Python scripts to automate log analysis and streamline SOC operations.

CyberDefenders – SOC Tier-1 & Network Forensics Labs:

- Completed practical labs in SOC operations and network forensics.

- Performed packet-level analysis, incident triage, and log correlation using Wireshark and virtual environments.

CTF Participation:

- Engaged in CTF challenges on CyberDefenders and other platforms, focusing on network analysis and digital forensics.

Vulnerability Discovery – netriders.academy:

- Conducted web security testing using fuzzing techniques and discovered a hidden sensitive file (info.php) exposing critical server information.
- Performed responsible disclosure and received a reward. Gained experience in web reconnaissance, fuzzing methodologies, and ethical reporting.

Additional Strengths

- Strong analytical and investigative mindset with practical SOC exposure.
- Calm and focused under pressure; capable of working independently or in teams.
- Excellent communication skills and technical documentation writing.
- Actively pursuing advanced blue team certifications and cybersecurity specialization.

Languages

- Arabic: Native
- English: Professional working proficiency (CEFR Level B2)