

## Mohamed Mostafa Ali

Undergraduate Student, Bachelor of Computer Science  
Arab Academy for Science, Technology & Maritime Transport  
Major in Cybersecurity  
6 October City, Giza, Gamal Abd El-Nasser Axis, Egypt

**Phone:** +201097936088

**Email:** mohamedmostafa10110@gmail.com

**GitHub:** <https://github.com/MohamedMostafa010>

**LinkedIn:** <https://www.linkedin.com/in/mohamedmostafaali>

**Personal Website:** <https://mohamedmostafa010.github.io/>

## EDUCATION

- **Arab Academy for Science, Technology & Maritime Transport** Oct 2022 – Jul 2026  
*Bachelor of Computer Science; Major in Cybersecurity* Smart Village, Egypt  
**GPA:** 3.56/4.0 (Excellent)

## EXPERIENCE

- **Commercial International Bank Egypt (CIB)** Jul 2024 – Aug 2024  
*Internship Trainee · Internship (Online)* Cairo, Egypt
  - Explored banking operations, teamwork, and industry practices through a structured program.
- **National Bank of Egypt (NBE)** Aug 2024 – Sep 2024  
*Information Technology Trainee · Internship (On-site)* Cairo, Egypt
  - Gained hands-on experience in IT operations, software testing, and troubleshooting.
- **WE Innovate Bootcamp** Aug 2025 – Sep 2025  
*SOC Analyst Intern · Internship (Hybrid)* Giza, Egypt
  - Completed hands-on SOC training tasks including Active Directory setup, Bash scripting for IP/domain blocking, NFS server configuration, securing Nginx with ModSecurity, Cisco Packet Tracer network simulations, and implementing SIEM solutions.

## PROJECTS

- **University Financial System Threat Modeling and Security Testing** Nov 2024 – Dec 2024  
*Threat Modeling and Security Testing Project* AAST
  - Performed threat modeling for a financial system, mitigating 85% of identified threats.
  - **Skills:** STRIDE, MITRE ATT&CK, Microsoft Threat Modeling Tool.
  - **GitHub Repository (Click to View):** <https://github.com/MohamedMostafa010/SecurePortalModeling>
- **System Performance Monitor Project with Bash and Docker** Nov 2024 – Dec 2024  
*Containerized System Monitoring Tool* AAST
  - Developed a containerized monitoring tool to track system performance.
  - **Skills:** Bash Scripting, Docker, Report Generation.
  - **GitHub Repository (Click to View):** <https://github.com/MohamedMostafa010/MonitorMetrics.git>
- **Sliver C2 & Botnet Small Lab: Cloud-Based Red Teaming** Jan 2025 – Feb 2025  
*Cybersecurity Red Teaming Project* Self-initiated
  - Built a cloud-based red teaming lab with automated C2 setup using Terraform.
  - **Skills:** Sliver C2, Network Traffic Analysis, Detection Evasion, Azure & Terraform.
  - **GitHub Repository (Click to View):** <https://github.com/MohamedMostafa010/C2Lab.git>
- **SSH Honeypot for Intrusion Detection** Jan 2025 – Feb 2025  
*Deceptive SSH Service to Detect Unauthorized Access* Self-initiated
  - Designed a cloud-based low-interaction honeypot to log unauthorized SSH access attempts for analysis.
  - **Skills:** Cloud-Based Honeypot Deployment, API Integration, Azure & Terraform.
  - **GitHub Repository (Click to View):** [https://github.com/MohamedMostafa010/SSH\\_Honeypot\\_Project\\_Pshitt.git](https://github.com/MohamedMostafa010/SSH_Honeypot_Project_Pshitt.git)
- **TuxTrace - Forensic Artifact Generation Tool** Apr 2025 – May 2025  
*A tool to simulate user activity and generate forensic artifacts.* AAST
  - Developed and Dockerized a Python script that simulates user activity and generates forensic artifacts, including files like .bashrc, .bash\_history, auth.log, /tmp directories, and Cron jobs, for educational and forensic analysis.
  - **Skills:** Python, Forensic Analysis, Bash Scripting, Artifact Generation, Docker, Cron Jobs.
  - **GitHub Repository (Click to View):** <https://github.com/MohamedMostafa010/TuxTrace>
- **ExeRay - AI-Powered Malware Detection System** May 2025 – Jun 2025  
*Machine Learning Engine for Executable Analysis* AAST
  - Developed an AI system that analyzes PE file characteristics to detect malware with 92% accuracy.
  - Implemented feature extraction from executable headers, sections, and imports for machine learning analysis.
  - **Skills:** Machine Learning, Feature Engineering, PE File Analysis, Adversarial Machine Learning (Threat Detection), XGBoost, and Random Forest.
  - **GitHub Repository (Click to View, Research Paper Uploaded):** <https://github.com/MohamedMostafa010/ExeRay>

## COURSES, CERTIFICATIONS, AND DIPLOMAS

---

• AMIT Learning SOC Diploma	AMIT
• CCNA 200-301	AMIT & Self-study
• CCNA Network Security	AMIT
• Cisco CyberOps	AMIT
• MCSA (Active Directory Part)	Self-study
• Red Hat System Administration Level 1	Mahara Tech
• CompTIA Linux+ XK0-005	Cybrary
• (ISC) <sup>2</sup> CC (Certified in Cybersecurity)	(ISC) <sup>2</sup> Obrizum
• CompTIA Security+ SY0-601	Netriders Platform
• Junior Penetration Tester (eJPTv1)	Netriders Platform
• THM Complete Beginner Learning Path	TryHackMe
• THM Introduction to Cyber Security Learning Path	TryHackMe
• THM Pre Security Learning Path	TryHackMe
• Microsoft Certified: Azure Fundamentals AZ-900	Self-study
• Certified Incident Responder (eCIR)	Netriders Platform
• Secure Software Development Lifecycle (SSDLC)	Mahara Tech
• CompTIA Cybersecurity Analyst (CySA+ CS0-003)	Netriders Platform

## TECHNICAL SKILLS AND STRENGTHS

---

- **SOC Field** - Experienced in **Detection Engineering** and **SOC Analysis** using **ELK**, **Splunk**, and **EDRs**.
- **Scripting and Automation** - Basic scripting and automation in Python, Bash, and PowerShell for security.
- **Networks and Security** - Advanced knowledge of networks and network security.
- **Operating Systems** - Highly proficient in Linux and Windows Management (Especially Linux).
- **Penetration Testing** - Basic penetration testing skills.
- **Programming Languages** - Proficient in Python, C/C++, Java, OOP, and Data Structures & Algorithms.
- **Web Programming** - Basic knowledge in web programming (HTML, CSS, PHP, JavaScript, etc.).

## SOFT SKILLS

---

- **Proactive Learning** - Proactive in learning and researching new technologies.
- **Adaptability** - Quickly adapts to new tools and methodologies.
- **Stress Management** - Effectively handles high-pressure situations.
- **Self-Discipline** - Self-disciplined and focused on achieving goals.
- **Communication** - Good communication abilities, both written and verbal.
- **Language Proficiency** - Native Arabic speaker with professional working proficiency in English.

## PROFESSIONAL ACCOMPLISHMENTS

---

- **AMIT Learning SOC Diploma Final Project** - Completed with a perfect score of **100%**.
- **TryHackMe Ranking** - Ranked in the **Top 2% worldwide** on **TryHackMe (THM)** (**150+ Rooms**).
- **IUGRC-9 Research** - Presented "*ExeRay: Windows Malware Classifier*" at the **9th IUGRC, MTC, Cairo**.

## BOOKS READ

---

- **Bash Idioms** - A book on advanced Bash scripting techniques and best practices.