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: 3.61/4.0 (Excellent)

EXPERIENCE

- **WE Innovate Bootcamp** *Aug 2024 – Sep 2024*
  SOC Analyst Intern · Internship (Hybrid) Giza, Egypt
  – Completed hands-on SOC training: AD setup, Bash scripting, NFS config, Nginx security, Cisco simulations, SIEM implementation

- **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

- **Commercial International Bank Egypt (CIB)** *Jul 2024 – Aug 2024*
  Internship Trainee · Internship (Online) Cairo, Egypt
  – Explored banking operations, teamwork, and industry practices through structured program

PROJECTS

- **DroneSentinel: AI-Based Security Gap Monitoring System** *Nov 2025 – Present*
  Graduation Project - Specialized drone detection for security vulnerabilities AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/DroneSentinel

- **IoTCPS-AI-IDS: AI-Based Intrusion Detection System** *Nov 2025 – Dec 2025*
  Deep learning IDS for IoT Cyber-Physical Systems (99.6% accuracy) AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/IoTCPS-AI-IDS

- **Conpot ICS Honeypot Analysis** *Nov 2025 – Dec 2025*
  Industrial Control Systems honeypot deployment and analysis AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/Conpot_ICS_Honeypot_Lab

- **Metasploitable 2 Security Assessment – 46 Findings** *Nov 2025 – Dec 2025*
  Comprehensive penetration testing report AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/Metasploitable2_Pentest_46Findings

- **Decentralized IoT Authentication on Ethereum** *Nov 2025 – Dec 2025*
  Solidity smart contract for secure IoT authentication AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/DecentralizedIoTAuth

- **ExeRay - AI-Powered Malware Detection System** *May 2025 – Jun 2025*
  Machine Learning Engine for Executable Analysis (92% accuracy) AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/ExeRay

- **TuxTrace - Forensic Artifact Generation Tool** *Apr 2025 – May 2025*
  Tool to simulate user activity and generate forensic artifacts AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/TuxTrace

- **University Financial System Threat Modeling** *Nov 2024 – Dec 2024*
  Threat Modeling and Security Testing Project AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/SecurePortalModeling

- **System Performance Monitor with Bash and Docker** *Nov 2024 – Dec 2024*
  Containerized System Monitoring Tool AAST
  – **Github Repo Link:** github.com/MohamedMostafa010/MonitorMetrics

- **Sliver C2 & Botnet Lab: Cloud-Based Red Teaming** *Jan 2025 – Feb 2025*
  Cybersecurity Red Teaming Project Self-initiated
  – **Github Repo Link:** github.com/MohamedMostafa010/C2Lab

- **SSH Honeypot for Intrusion Detection** *Jan 2025 – Feb 2025*
  Deceptive SSH Service to Detect Unauthorized Access Self-initiated
  – **Github Repo Link:** github.com/MohamedMostafa010/SSH_Honeypot

Technical Skills

- **Security Operations:** SOC Analysis, Detection Engineering, ELK, Splunk, EDRs, Incident Response
- **Networking & Infrastructure:** CCNA-level networking, Linux/Windows Administration, Docker, Cloud (Azure)
- **Security Tools:** Metasploit, Nmap, Wireshark, Honeypots (Conpot), SIEM, Threat Intelligence (MISP)
- **Programming:** Python, C/C++, Java, Bash, PowerShell, Solidity, OOP, Data Structures
- **ML/AI Security:** TensorFlow, Scikit-learn, Feature Engineering, Model Evaluation
- **Web Technologies:** HTML, CSS, JavaScript, PHP, Nginx, ModSecurity

Certifications

- AMIT SOC Diploma
- CCNA 200-301
- CCNA Network Security
- Cisco CyberOps
- MCSA (Active Directory Part)
- Red Hat System Administration Level 1
- CompTIA Linux+ XKO-005
- (ISC)² CC (Certified in Cybersecurity)
- CompTIA Security+ SY0-601
- Junior Penetration Tester (eJPTv1)
- THM Complete Beginner Learning Path
- THM Intro to Cyber Security Learning Path
- THM Pre Security Learning Path
- Microsoft Certified: Azure Fundamentals AZ-900
- Certified Incident Responder (eCIR)
- MaharaTech Secure Software Development Lifecycle
- CompTIA Cybersecurity Analyst (CySA+ CS0-003)
- THM SOC Level 1 Learning Path
- THM SOC Level 2 Learning Path

Accomplishments & Strengths

- **Top 1% TryHackMe** worldwide (300+ rooms completed and 40+ badges)
- **Research Presentation:** "ExeRay: Windows Malware Classifier" at 9th IUGRC, MTC Cairo
- **100% Score** on AMIT SOC Diploma final project
- **Soft Skills:** Proactive learner, adaptable, stress-resistant, self-disciplined, strong communicator
- **Languages:** Native Arabic, Professional English