Ahmed Mahmoud

Penetration Tester

ahmedmahmoudhus@gmail.com +20 1096534894 6th of October, Giza

ahm-mahmoud ahme-mahmoud ahme-mahmoud Portfolio

Summary

Cybersecurity student and penetration tester focused on web, API, and network penetration testing, with hands-on experience in vulnerability assessment, digital forensics, and ML-based threat detection. Skilled in offensive security workflows, network traffic analysis, anomaly detection, and AI-driven security solutions.

EDUCATION

B.Sc. in Network and Cyber Security 2023 – 2027
Elsewedy University of Technology - Polytechnic of Egypt

WORK EXPERIENCE

Bug Bounty Researcher 2024 – Present
HackerOne
Identified and reported security vulnerabilities through bug bounty programs.

Offensive Security Internship 11/2025 – 03/2026
CyberThos Remote
Worked on web application penetration testing, vulnerability assessment, security monitoring, and log analysis using Splunk.

Machine Learning Intern 11/2025 – Present
Digital Egypt Pioneers Initiative - DEPI Cairo, Egypt
Built and trained machine learning models using Python

Cybersecurity training 08/2025 – 09/2025
NTI Smart Village, Egypt
Completed hands-on cybersecurity training in vulnerability assessment, web security, threat hunting, and security monitoring.

Cybersecurity Bootcamp Remote
Microsoft Summer Camp x Sprints
Completed training in SOC operations, OSINT, and penetration testing.

PROJECTS

ICS/OT Network Detection & Response
Built a network threat detection system for Industrial Control Systems (ICS/OT) using machine learning to detect malicious network activity.

Botnet Detection System
Furssah AI Competition (CrossRealms ME)
Built a machine learning system for detecting botnet traffic and analyzing malicious network behavior in real time.

Network Traffic Forensics for Intrusion Detection
Built a real-time IDS using Suricata, Wireshark, and XGBoost to classify malicious traffic. Designed a Streamlit dashboard for live monitoring and alerts.

AI-Powered Deepfake & Image Manipulation Detection System
Built a digital forensics system for detecting AI-generated, spliced, and manipulated images using machine learning.

Campus Net Compiler
Built an Infrastructure-as-Code platform for automated network deployment and simulation using GNS3 and YAML-based topology configurations.

SecureMerge – Cyber Risk Management for M&A
Developed a cybersecurity risk management framework for mergers and acquisitions (M&A) with risk assessment and governance tracking.

IoT Wi-Fi Honeypot
Developed an IoT Wi-Fi honeypot for monitoring device behavior during Evil Twin attacks.

Custom Firewall System
Created a Linux-based firewall using iptables and SQLite for persistent rule storage.

SKILLS

Offensive Security
Web & API Penetration Testing, Vulnerability Assessment, Burp Suite, OWASP ZAP, Nuclei, ffuf

Incident Response & Security Monitoring
ELK Stack, Splunk, SIEM, IDS/IPS, Log Analysis

Programming & Development
Python, Bash, JavaScript, PHP, Java, Flask, Laravel

Networking & Systems
Linux, TCP/IP, DNS, HTTP/HTTPS, Windows Server, Network Security

Machine Learning for Cybersecurity
Anomaly Detection, Network Traffic Analysis, Threat Detection Systems, Scikit-learn, XGBoost, LightGBM, TensorFlow, Pandas, NumPy

Soft Skills
Technical Research, Reporting, Team Collaboration

CERTIFICATIONS

eJPT
Self-study completed

eWPT
Self-study completed

eMAPT
In Progress – Self Study

Languages

English

Arabic

Interests

Penetration Testing | Vulnerability Research | Machine Learning for Security | Threat Detection & Network Monitoring