Amr Mohamed Mousa

Cairo, Egypt • amr27mm@gmail.com • 01001806578 • linkedin.com/in/amr-mousa-0990a0219
github.com/amr12m

PROFILE

Cybersecurity graduate and eWAPTX-certified penetration tester, specializing in advanced web application security testing, vulnerability research, and exploit development. Experienced in real-world attack simulations, malware analysis, and network security.

EDUCATION

Menoufia University, Faculty of Electronic Engineering

Bachelor of Cyber Security, Computer Science Department

GPA: Very good (3.55)

EXPERIENCE

National Telecommunication Institute NTI EME 4M

Professional Security Administrator February 2025 – May 2025

Network Security Engineer

- Designed and implemented secure network architectures using **Cisco Firepower** NGFW and **Cisco ASA** firewalls.
- Configured secure VPNs (IPsec/SSL) for encrypted communication, ensuring remote access security.
- Developed and enforced policies to secure network traffic, applying **AAA** for authentication and authorization.
- Conducted network segmentation with **ACLs** and implemented **Zone-Based Policy Firewalls** for enhanced defense.

Ethical Hacker & Penetration Tester

Conducted vulnerability assessments, penetration testing, and exploitation using **Kali Linux** and **Metasploit**.

- Analyzed network traffic with **Wireshark** to identify security risks and provide mitigation strategies.
- Tested network defenses against attacks including SQL injection, DoS, and session hijacking.
- Performed hands-on testing of web applications for common OWASP Top 10 vulnerabilities, including XSS, SQLi and IDOR.
- Conducted in-depth penetration tests on internal web applications focusing on server-side vulnerabilities (XXE, API flaws, Injection attacks).
- Identified and exploited misconfigurations and authentication flaws in real-world scenarios via PortSwigger labs (completed50%).
- Documented findings with detailed PoCs and remediation suggestions in professional reports

CyberOps Engineer

- Utilized **Wireshark** for in-depth network traffic analysis, detecting anomalies and identifying potential security threats in real-time.
- Employed **Cisco Packet Tracer** for simulating network environments and testing security configurations.
- Leveraged **Security Onion** In **Security Onion**, the following tools are used for monitoring, threat detection, and incident response:
  - **ELK Stack** (Elasticsearch, Logstash, Kibana):
    - **Elasticsearch**: A search and analytics engine for storing and querying large volumes of log data.
    - **Logstash**: A tool for collecting, parsing, and forwarding logs to Elasticsearch.
    - **Kibana**: A visualization tool for analyzing and presenting the data stored in Elasticsearch.
  - **SGUIL**:
    - SGUIL is an open-source GUI for interacting with **Snort** and **Suricata** intrusion detection systems (IDS), allowing security analysts to view alerts and take action in real-time.
    - Provides features such as managing alert data, creating event summaries, and performing event correlation.

AWARDS

3rd Place – Zinad-IT CTF Competition by Zinad-IT April 2024

- Tackling challenges in web exploitation, reverse engineering, cryptography, and forensics.
- Demonstrated strong problem-solving skills, team collaboration, and cybersecurity expertise to secure a top position.

Top 5% on Try Hack Me

Solved 50% on port swigger

PROJECTS

GUI AI searching algorithms

- Engineered and implemented AI-based search algorithms such as A*, BFS, and DFS.
- Developed an interactive visualization to demonstrate algorithm performance
- Optimized execution time for large datasets.

JANDA

- Developed and implemented an advanced malware analysis tool to automate static and dynamic analysis.
- Integrated key security features to detect and analyze malicious patterns.
- Optimized performance for efficient detection and enhanced reporting capabilities for better insights.

Packet analysis

- Conducted in-depth network traffic analysis to identify anomalies and security threats.
- Developed custom scripts to automate packet filtering and analyzed network behavior to detect potential vulnerabilities.

VulnHunter (Graduation Project)

- Designed and developed a custom automation tool to perform reconnaissance, subdomain enumeration, and vulnerability scanning for web applications and external networks.
- Integrated multiple recon tools such as Amass, Sublist3r, Assetfinder, httpx, waybackurls, and combined outputs via Python scripts.Implemented scanning modules for common vulnerabilities like SQL Injection, XSS, and misconfigurations.
- Implemented web vulnerability scanning modules targeting common OWASP Top 10 issues such as SQL Injection, XSS and misconfigurations.
- Built reporting engine that generates professional security reports with detailed vulnerability descriptions, PoCs, and remediation advice.

Advanced Network Security Architecture Implementation

- Designed and implemented a secure network architecture with Cisco Firepower NGFW, configuring IPS to detect and block malicious traffic.
- Deployed secure IPsec VPNs for encrypted remote communication, enforced network segmentation with OSPF authentication, implemented AAA protocols for access control.
- Applied Layer 2 security measures to protect against threats like VLAN hopping and MAC spoofing.

SKILLS

- **Programming & Scripting:** Python (Security Scripting, Automation), C++
- **Network Security:** Cisco Firewalls (ASA, Firepower), VPN configuration (IPSec/SSL), AAA implementation, ACLs.
- **Linux Administration:** System management, SSH, file security, and user/group management.
- **Ethical Hacking:** Footprinting, vulnerability analysis, penetration testing, and system exploitation.
- **Cryptography**: Symmetric & asymmetric encryption, PKI, cryptographic attacks
- **Virtualization:** VMware, Virtual Machine configuration, and cloning
- **Soft Skills:** Problem-Solving ,Teamwork & Collaboration, Self-Learning & Adaptability, Persistence & Resilience

CERTIFICATIONS

- eWAPTX – eLearnSecurity Web Application Penetration Tester eXtreme (2025)
- CCNA certificate by National Telecommunication Institute NTI
- Introduction to Cybersecurity bootcamp by cyber Talents

LANGUAGES

- **Arabic**
- **English**

ORGANIZATIONAL & VOLUNTEER EXPERIENCE

University Cybersecurity Club

- Organized and led cybersecurity workshops, increasing student participation by 50% over the semester.
- Planned and hosted (CTF) Capture The Flag competitions, engaging 100+ participants and improving hands-on security skills.
- Mentored junior members in penetration testing and ethical hacking, leading to a 30% improvement in their performance in national CTFs.
- Collaborated with faculty and industry professionals to organize lectures for student exposure enhancement to real-world cybersecurity challenges.
- Developed and structured training sessions on web security and networking, resulting in 70% of attendees reporting improved skills in post-event surveys.