Mostafa Mahmoud Sayed

Junior Penetration Tester | VAPT & Web Application Security

Faisal, El Giza, Egypt | 01112264172 | m.mostafa5830@gmail.com | linkedin.com/in/mostafa-mahmoud-mmm | mostfa25.github.io/ewaptx_notes

SUMMARY

Junior Penetration Tester with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT), web application security testing, and network penetration testing. Practiced in identifying and exploiting SQL Injection, XSS, CSRF, IDOR, and Broken Authentication vulnerabilities using Burp Suite, Nmap, Metasploit, and OWASP ZAP. Documented 50+ machines on Hack The Box and TryHackMe simulating real-world attack scenarios. Skilled in Python for exploit automation and Active Directory security including Kerberos attacks and privilege escalation. Trained through NTI/MCIT Red Team and DEPI Penetration Testing programs, with a strong focus on technical reporting, remediation guidance, and continuous learning aligned with CEH standards.

EDUCATION

Bachelor of Computer Science Engineering — Modern Academy for Engineering and Technology *2020 – 2025*

Specialization: Cybersecurity Graduated with a top-grade project in Penetration Testing (A+)

Maadi, Cairo | Degree: B-

EXPERIENCE

Cybersecurity Instructional Assistant March 2026 – Present

Digilians - Egyptian Military Academy

Provided hands-on lab support, technical guidance, and practical cybersecurity instruction to learners in an MCIT-organized program hosted at the Egyptian Military Academy.

PROJECTS

Graduation Project — Practical Penetration Testing *09/2024 – 06/2025*

- Led a team of 4 to identify and remediate 12+ web vulnerabilities (SQLi, XSS, insecure authentication, insecure API endpoints) across simulated environments.
- Completed 50+ CTF-style penetration testing labs, producing clear vulnerability remediation reports for stakeholders.

Auto Hunter — Automated IP Scanner & Risk Prioritization Tool *09/2024 – 01/2025*

- Developed an automated vulnerability scanning tool using Nmap and ML-driven risk prioritization, improving triage efficiency by 60% and reducing manual reporting time by 40%.
- Tested and validated the tool across 500+ IP addresses with optimized scan performance for large-scale network assessments.

TRAINING

Cybersecurity / Red Team Training — National Telecommunication Institute (NTI), MCIT *09/2025 – 01/2026*

Smart Village, Cairo

- Completed intensive hands-on training in penetration testing techniques, web application security testing (SQLi, XSS, authentication flaws), network security, vulnerability assessment, and technical reporting.

Penetration Testing Track — Digital Egypt Pioneers Initiative (DEPI), MCIT *04/2024 – 10/2024*

Cairo

- Trained in penetration testing methodologies, web application security testing (SQLi, XSS, CSRF, IDOR), network penetration testing, ethical hacking techniques, and security findings documentation.

TECHNICAL SKILLS

Penetration Testing Tools: Burp Suite, SQLMap, Nikto, DirBuster, Metasploit, Nmap, Hydra, Netcat, Wireshark, Tcpdump, Netdiscover, Hashcat, John the Ripper, Subfinder, FFUF.

Web Application Security :OWASP top 10**,** Authentication & access control flaws, injections (OS, SQL), file upload issues, SSRF, path traversal, XSS, CSRF, CORS misconfigurations. Completed labs on PortSwigger, TryHackMe, and Hack The Box.

Networking: Cisco Routers & Switches, VPN, VLANs, ACLS, DNS, DHCP, IP Subnetting, TCP/IP, Network Hardening, Firewall & IDS/IPS Evasion

Network Security: Network scanning and enumeration, vulnerability assessment, password attacks, MITM, traffic analysis (Wireshark), service discovery (Nmap), exploitation (Metasploit), firewall/IDS evasion, and Linux privilege escalation.

Active Directory Security: Active Directory Enumeration, Kerberos Attacks, Pass-the-Hash, Pass-the-Ticket, Privilege Escalation, Lateral Movement.

Programming / Scripting: Python, PHP, MySQL, JavaScript, Bash.

Protocols & Cryptography: TCP/IP, HTTP/S, FTP, SSH, SNMP, SSL/TLS, AES, RSA, SHA, MD5, PKI, Digital Signatures, Secure Authentication & Encryption Practices

Operating Systems: Linux**,** Kali Linux, Ubuntu, Windows

Reporting & Methodology: Penetration Test Reporting, Security Auditing, Threat Modeling, Remediation Planning, Technical Documentation

SOFT SKILLS

Teamwork | Problem Solving | Communication | Creativity | Analytical Thinking | Technical Writing & Reporting | Continuous Learning

COURSES

Jr Penetration Tester, TryHackMe	01/2026 – 03/2026
eLearn Security Junior Penetration Tester (eJPT), NetRiders Academy	08/2023 – 10/2023
Certified Ethical Hacker (CEH), NTI	11/2023 – 01/2024
Introduction to Cybersecurity, Cyber Talen	12/2023 – 12/2023
Cisco Certified Network Associate (CCNA), NTI	05/2023 – 07/2023
System Administration, Self-study	02/2023 – 03/2023
Microsoft Certified Solutions Associate (MCSA), Self-study	07/2023 – 08/2023
Basic PHP, YAT Academy	08/2022 – 09/2022

LANGUAGES

English — Intermediate | Arabic — Native