Abdelrahman Magdy

Ismailia, Egypt | +20 1289 228 560 | **Email**: AbdelrahmanMagdy0x0@proton.me
LinkedIn:linkedin.com/in/abdomagdy00 **Blog**: vipa0z.github.io | **GitHub**: github.com/vipa0z

SUMMARY

Junior Penetration Tester with 1.5+ years of experience in network security assessments, Active Directory penetration testing, and web application vulnerability analysis. Demonstrated expertise in network protocols, routing/switching concepts, and systematic security testing methodologies across enterprise environments. **Currently pursuing HTB CPTS certification** while contributing to the cybersecurity community through detailed technical writeups and knowledge sharing.

EDUCATION

Bachelor's Degree in Computer Science | Future Academy, Cairo | 09/2021 – 06/2025
GPA: 3.08

Courses/Certifications

- **Hackthebox Certified Penetration Testing Specialist (HTB CPTS) | HTB**
- **Cisco CyberOps & CCNA | Cisco | DEPI**

Experience

Volunteer Penetration Tester | Web Application Testing | Mar 2025 – Jun 2025

- Secured community gaming platform serving 5,000+ users through comprehensive penetration testing and vulnerability assessment
- Prevented potential data breach by discovering and reporting 5+ critical SQL injection vulnerabilities affecting user database integrity
- Enhanced platform security posture by identifying API authentication flaws that could enable unauthorized user impersonation across comment systems
- Improved application resilience through discovery of input validation vulnerabilities including improper parameter filtering and unused attack vectors
- Accelerated remediation timeline by delivering actionable security reports with prioritized findings and step-by-step mitigation guidance to development team

Skills

Penetration Testing & Security Assessment

- Penetration testing processes and methodologies using OWASP, NIST, and OSSTMM frameworks
- Vulnerability assessment and comprehensive security risk analysis
- Information gathering and reconnaissance through OSINT and network enumeration

Skills

- Manual and automated exploitation techniques

Systems & Infrastructure Security

- Windows and Linux target assessment and penetration testing
- Active Directory penetration testing including domain enumeration, ACL attacks, Trust attacks, and Kerberoasting
- Windows and Linux privilege escalation techniques and exploitation
- Pivoting and lateral movement
- Post-exploitation enumeration and system reconnaissance

Web Application Security

- Web application penetration testing covering OWASP Top 10 vulnerabilities
- Application security assessment including API testing and authentication bypass
- Injection attacks, cross-site scripting, and client-side vulnerability exploitation

Communication & Reporting

- Vulnerability and risk communication for technical and executive audiences
- Security documentation including detailed findings and remediation guidance
- Technical report writing and compliance reporting

Tools

- Web Application: Burp Suite, OWASP ZAP, SQLMAP, XSSER, XXEIJNECTOR
- Active Directory: BloodHound, Impacket, PowerView, Mimikatz, Certipy
- Network & Reconnaissance: Nmap, NetExec, DNSRecon, RustScan
- Vulnerability Assessment: Nessus, OpenVAS
- Exploitation: Metasploit Framework, John the Ripper, Hashcat
- Scripting: PowerShell, Python, Bash

LANGUAGES

English: Proficient, Arabic: Native