Ahmed Emad Shahen

ahmed.e.shahen@gmail.com | +201062323523 | LinkedIn | TryHackMe | Credly

SUMMARY

Highly motivated and detail-oriented Penetration Tester with hands-on experience in vulnerability assessment, exploitation, and securing systems. Skilled in ethical hacking, network security, and application security testing, including buffer overflow and privilege escalation attacks, with expertise in Android and web application penetration testing. Adept at writing comprehensive penetration test reports and working collaboratively in teams. Focused on continuous learning to stay updated on the latest cybersecurity trends and passionate about safeguarding systems against evolving threats.

EXPERIENCE

Offensive Security Trainee @ WE INNOVATE Academy — September 2024 : November 2024

- Conducted Web Application Penetration Testing, focusing on vulnerabilities such as SQL Injection, XSS, CSRF, SSRF, and application logic flaws to identify and mitigate critical security risks.
- Performed Android Application Penetration Testing, including APK analysis, exploiting exported components, bypassing SSL pinning, and analyzing traffic interception for vulnerabilities.
- Engaged in Infrastructure Penetration Testing, utilizing tools like Nmap and PSExec to identify security gaps, execute privilege escalation on Windows and Linux systems, and conduct Active Directory attacks.
- Conducted Operating Systems Penetration Testing, including exploiting Windows and Linux buffer overflows and executing wireless network attacks for comprehensive system assessments.

System Administrator @ Ministry Of Manpower — March 2024 : September 2024

- Configure and manage Windows Server environments, including installation, maintenance, and upgrades.
- Implement and administer Active Directory, SQL Manager, IIS, Group Policies, and user account management.
- Provide technical support and troubleshoot issues for Windows-based systems and applications.
- Ensure system security through configuration, monitoring, and applying patches and updates.
- Conduct system backups and recovery processes to maintain data integrity and availability.

CyberSecurity Trainee @ ITI — Summer 2023

As a Cyber Security trainee at ITI Institute, I gained hands-on experience and theoretical knowledge in network fundamentals, Windows server administration, Red Hat system administration , firewall technologies, and cloud computing.

EDUCATION

Bachelor of Computer Engineering, Menoufia University 2019 – 2024 — Grade: Very Good
Faculty of Electronic Engineering, Cyber Security and Data Analytics department.

CERTIFICATES

- CyberOps -- Cisco
- Cybersecurity Essentials -- Cisco
- Ethical Hacking -- Cisco
- Ethical Hacking -- ITI
- CyberSecurity Trainee -- ITI
- Wireless Networks Penetration Testing -- ITI
- Advanced Malware Analysis -- ITI

COURSES

- CCNA
- MCSA
- RHCSA
- OWASP Top 10 (Web) 2021
- eJPTv1 Prep
- API Penetration Testing -- APISEC University

SKILLS

Networking Protocols & Security Principles
- Strong understanding of networking protocols and security principles.

Operating Systems
- Proficient with Linux and Windows environments.

System Administration
- Skilled in Windows Server administration and Red Hat system administration.

Cloud Computing
- Knowledgeable in cloud technologies, architecture, and security implementations.

Penetration Testing
- Network Penetration Testing.
- Web Application Penetration Testing.
- Mobile Application Penetration Testing.
- Wireless Network Penetration Testing.

Vulnerability Assessments
- Identifying and Exploiting Vulnerabilities.
- Conducting Comprehensive Vulnerability Assessments.
- Exploiting Network Services.
- Web Application Exploitation.
- Buffer Overflows.
- Privilege Escalation Techniques.
- Post-Exploitation Techniques.

OSINT (Open-Source Intelligence)
- Skilled in gathering and analyzing public information for reconnaissance.

Network Scanning and Enumeration
- Expertise in service detection, enumeration, and vulnerability discovery.

Active Directory
- Knowledgeable in Active Directory attacks and post-compromise persistence techniques.

Scripting and Exploits
- Proficient in scripting with Python, Bash, and PowerShell for automation and exploitation tasks.

Reporting
- Adept at writing detailed penetration testing reports with actionable mitigation strategies.

LANGUAGE

Arabic: Mother Tongue

English: Upper-intermediate