Emad Elshareef

Penetration Testing Team Lead

OSCE3 - OSED - OSEP – OSWE – OSCP – OSWP – CRTL- CRTO – CRTE – CRTP – CEH – ECSA – eMAPT

☎ +966 533 046 181 LinkedIn

✉ noip515@gmail.com My website

PROFILE

With over 9 years of experience in Information Security, I've honed my skills as a Penetration Testing Team Lead. My expertise spans various domains, including Web, Mobile, App, API, Active Directory, and Network security testing. This breadth of knowledge reflects my commitment to staying at the forefront of the dynamic landscape of cybersecurity.

EDUCATION

Bachelor of Science, IT
University of Science and Technology, **2015**

Master of Science, IT
University of Science and Technology, **2017**

ACHIEVEMENT

- **5th place BlackHat** International CTF Competition 2021-KSA
- **2nd Place GroupIB CTF** 2023.
- **5th place at Hyatt** Hotels Bug Bounty Program.
- PlayStation Network Wall of Fame
- AT&T Wall of Fame

LANGUAGES

- Arabic
  Native Speaker
- English
  Professional

PROFESSIONAL EXPERINECE

Penetration Testing Team Lead **Aug 2023 – Present**
Confidential

- Spearheaded a team of cybersecurity experts tasked with executing comprehensive penetration tests across diverse systems, applications, and networks, ensuring robust security protocols.
- Identified security vulnerabilities, meticulously assessed findings, and facilitated the deployment of strategic security enhancements to fortify sensitive data and systems against potential breaches.
- Conducted hands-on Web Applications, mobile app and AD penetration testing, meticulously scrutinizing applications utilized within the organization to pinpoint vulnerabilities and reinforce security measures.
- Review and update yearly Penetration Testing plan.
- Establish Clear Communication Channels: Maintain open lines of communication with vendors to ensure timely receipt of reports and facilitate any necessary clarifications or additional information.
- Conduct Red Teaming as per regulations.

Senior Information Security Consultant **May 2021 – August 2023**
SecurEyes KSA

- **Web Application Penetration Testing:** Conduct in-depth security evaluations of web applications, scrutinizing their architecture, APIs, data storage mechanisms, and authentication processes to detect and exploit vulnerabilities using custom and public Tools.
- **Security Controls Assessment:** Conduct comprehensive evaluations of security controls implemented within the organization's IT infrastructure. This includes assessing the effectiveness of access controls, authentication mechanisms, encryption protocols, logging and monitoring systems, and other defensive measures to identify gaps and weaknesses that could be exploited by attackers.
- **Red Teaming Engagement:** Lead Red Team exercises aimed at simulating real-world cyber-attacks to test the organization's overall security posture and incident response capabilities. Coordinate with stakeholders to plan and execute sophisticated attack scenarios, including social engineering, advanced persistent threats (APTs), and lateral movement techniques, to identify weaknesses in defensive measures and improve resilience to targeted attacks.
- **Mobile App Penetration Testing:** Perform comprehensive security assessments of mobile applications deployed on various platforms, including iOS and Android. Analyze application binaries, API endpoints, data storage mechanisms, and authentication mechanisms to uncover vulnerabilities such as insecure data storage, improper session management, and insecure

EXPERTISE

- Adversary Simulation & Red Teaming
- Security Metrics & Reporting
- Programming & Scripting
- AD Security Assessment
- Regulatory Compliance
- Security Frameworks
- Active Directory Assessment
- Penetration Testing
- Control Assessment
- Application Security
- Disaster Recovery
- Incident Handling
- 3rd Party Vendors
- Risk Assessment
- Security Policies
- Bug Bounty
- Security Audit
- Cloud Security

SOFTSKILLS

Problem-Solving: Methodically uses logic and analysis to come to a solution

Communication: Strong communication and data presentation skills

Critical Thinking: Actively and skilfully analyses information collected from multiple disciplined processes

Adaptability: Swiftly adjusts to changing settings and obstacles to suit the needs of the task at hand

communication channels.

- **Network Penetration Testing:** Execute thorough assessments of network infrastructure components, including routers, switches, firewalls, and servers, to identify vulnerabilities and misconfigurations that could compromise the confidentiality, integrity, and availability of critical assets. Utilize techniques such as port scanning, vulnerability scanning, and exploitation of network.

Senior Penetration Tester **July 2017 – February 2021**
GSK Information Technology

- **Leading Penetration Testing Projects:** Taking charge of penetration testing projects from initiation to completion, including scoping, planning, execution, and reporting. You'll oversee the entire testing process, ensuring that it aligns with project objectives and client requirements.
- **Developing Customized Attack Scenarios:** Creating and executing customized attack scenarios to simulate real-world cyber threats and emulate the tactics, techniques, and procedures (TTPs) of malicious actors. This includes conducting Red Team engagements to assess the organization's detection and response capabilities.
- **Providing Remediation Recommendations:** Generating detailed reports outlining identified vulnerabilities, potential risks, and recommended remediation actions. You'll communicate findings to clients in a clear and concise manner, providing actionable recommendations for improving their security posture.
- **Mentoring Junior Team Members:** Providing mentorship and guidance to junior penetration testers, helping them develop their technical skills, methodology adherence, and professional growth within the field of penetration testing.
- **Staying Abreast of Emerging Threats:** Keeping abreast of the latest cybersecurity trends, emerging threats, and attack techniques.
- Collaborated seamlessly with procurement and legal teams to meticulously assess vendor contracts, ensuring they met stringent security and compliance prerequisites, safeguarding the organisation's interests and information
- **Engaging with Clients and Stakeholders:** Engaging with clients, stakeholders, and other relevant parties to understand their security concerns, requirements, and objectives. You'll collaborate closely with clients to tailor testing approaches that meet their specific needs and address their unique security challenges.
- **Contributing to Thought Leadership:** Contributing to thought leadership initiatives within the cybersecurity community through research, publications, conference presentations, and participation in industry forums. You'll share insights, best practices, and lessons learned to advance the field of penetration testing and enhance overall cybersecurity awareness.
- **Contributing to Team Knowledge:** Sharing knowledge and expertise with colleagues, participating in team discussions and knowledge-sharing sessions, and continuously learning new skills to enhance the effectiveness of the penetration testing team.

Penetration Tester **Jan 2015 - June 2017**
Gateway to IT and Innovation
Oman

- Conducting Security Assessments: Performing comprehensive security assessments on systems, applications, and networks to identify vulnerabilities and weaknesses that could be exploited by attackers.
- Utilizing Testing Tools and Techniques: Utilizing a variety of automated scanning tools, as well as manual testing techniques, to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure configurations.
- Executing Penetration Tests: Performing penetration tests to simulate real-world cyber-attacks, including network attacks, web application attacks, and social engineering attacks, to assess

Leadership: Cross-collaboration, inclusiveness and diversity are valued.

Relationship Building: Works to build and maintain relationships in order to help achieve work-related goals

the organization's security posture.

- Adhering to Ethical Guidelines: Conducting penetration tests in an ethical and responsible manner, ensuring that testing activities do not cause harm to systems or violate legal or ethical standards.
- Analyzing Results: Analyzing the results of security assessments and penetration tests to prioritize vulnerabilities based on severity and potential impact on the organization's systems and data.
- Generating Reports: Creating detailed reports documenting identified vulnerabilities, including their descriptions, risk ratings, and recommended remediation actions. Reports may also include evidence of exploitation to demonstrate the impact of vulnerabilities.

PROFESSIONAL DEVELOPMENT

- Offensive Security Certified Expert (OSCE3)
  Digital Badge: Here
- Offensive Security Exploit Developer (OSED)
  Digital Badge: Here
- Offensive Security Experienced Penetration Tester (OSEP)
  Digital Badge: Here
- Offensive Security Web Expert (OSWE)
  Digital Badge: Here
- Offensive Security Certified Professional (OSCP)
  Digital Badge: Here
- Offensive Security Wireless Professional (OSWP)
  Digital Badge: Here
- Certified Red Team Expert (CRTE)
  Digital Badge: Here
- Certified Red Team Operator (CRTO)
  Digital Badge: Here
- Certified Ethical Hacker (CEH)
  Digital Badge: Here
- EC Council Certified Security Analyst (ECSA)
  Digital Badge: Here
- eLearnSecurity Mobile Application Penetration Tester (eMAPT)
  Digital Badge: Here
- Certified Red Team Lead (CRTL)
  Digital Badge: Here

REFERENCES

Available upon request.