Mahdi Amin Alabdallah

Cybersecurity Engineer | Network Security Specialist | Penetration Tester

mahdiesta@gmail.com +962 799 27 11 46 Amman, Jordan linkedin.com/in/shammari

github.com/xl337x

Summary

Offensive Security Consultant and Penetration Tester specializing in Active Directory, hybrid identity environments, and enterprise attack-path assessments. Currently delivering network, Active Directory, and web application security engagements at Wizard Cyber. Holder of OSCP+, eCPPT, eWPT, and eCIR certifications, combining hands-on offensive security expertise with a background in detection engineering and threat hunting. Published cybersecurity researcher focused on phishing tradecraft and trusted-infrastructure abuse, with a proven ability to translate complex security risks into actionable remediation for technical and executive stakeholders.

Experience

Penetration Tester 09/2025 – Present

Wizard Cyber

- Deliver penetration test engagements across internal and external networks, Active Directory, and web applications for enterprise clients.
- Build full attack paths across on-premises Active Directory, Entra ID, and hybrid identity environments, including ADCS certificate-template chains, Kerberos delegation abuse, ACL-based privilege escalation, and credential-relay attacks leading to domain compromise.
- Test web applications across modern stacks, focusing on authentication, authorization, server-side request forgery, file handling, business logic flaws.
- Validate network segmentation and defense in depth by establishing controlled multi-hop access from external footholds through DMZ into segmented internal zones.
- Maintain internal offensive methodology, attack playbooks, and reusable workflows that standardize engagement delivery across the team.

Cybersecurity Analyst - Detection, CTI Team Member 07/2024 – 09/2025

Wizard Cyber

- Developed and tuned custom detection rules in Microsoft Sentinel using KQL, improving visibility across ATT&CK techniques.
- Performed proactive threat hunting across cloud and endpoint environments using KQL and threat intelligence data.
- Researched emerging threats, phishing campaigns, and attacker TTPs to support detection and response activities.
- Identified, validated, and blocked malicious IoCs, including IPs, domains, URLs, and file hashes.
- Simulated attack scenarios in Microsoft's ACME lab environment to test and improve detection coverage.
- Produced threat intelligence reports and security advisories for internal teams and MSSP clients.
- Supported incident investigations, alert triage, and detection engineering initiatives.
- Contributed to phishing awareness and security improvement efforts through analysis and recommendations.

Education

B.Sc. Network Engineering and Security 2019 – 2024 | Irbid, Jordan

Jordan University of Science and Technology

Areas of Expertise

Network and Active Directory Penetration Testing

Internal and external network assessment, AD attack-path analysis, Kerberos abuse, certificate services security, delegation review, ACL-based privilege escalation, and post-exploitation across enterprise environments.

Post-Exploitation and Privilege Escalation

Windows and Linux post-exploitation, credential extraction, token abuse, lateral movement, persistence, and segmentation validation.

Web Application Security

Manual testing across the OWASP Top 10, authentication and session management, access control, server-side request forgery, file handling, business logic flaws, and AI chatbots security.

Detection Engineering, Threat Hunting, and Research

Detection content development, KQL log analytics, hypothesis-driven hunting, MITRE ATT&CK aligned coverage, adversary tradecraft research, and technical writing.

Certifications

OSCP/OSCP+, Offensive Security Certified Professional+

eCPPT, Certified Professional Penetration Tester

Microsoft AZ-500, Azure Security Engineer Associate

Microsoft SC-200, Security Operations Analyst Associate

eWPT, Web Application Penetration Tester

eCIR, Certified Incident Responder

Microsoft SC-300, Identity and Access Administrator Associate

Languages

Arabic
Native

English
Professional working proficiency

Publications

Invisible Threats: How SVG Files Are Weaponized for Phishing Attacks.
Wizard Cyber

iCloud Calendar Exploited to Deliver Phishing Emails from Apple Infrastructure.
Wizard Cyber

Rising Threat: Phishing Campaigns Exploiting .es and .com.br Domains.
Wizard Cyber

Technical Projects

Offensive Security Tooling and Research
Maintain a public repository of offensive security tooling, references, and methodology guides at github.com/xl337x, covering Active Directory attack paths, web exploitation, and operator workflows.

AWARDS AND RECOGNITION

Top 3 Finalist, Cybersecurity Project Competition 01/12/2023
Jordan Second Cybersecurity Summit (NCSCJO)
Project showcased under the patronage of HRH Crown Prince Hussein bin Abdullah II.

2nd Place
Jordan National Cybersecurity CTF (CyberTalents)

3rd Place
MetaCTF, Princess Sumaya University for Technology

3rd Place
JUST University Cybersecurity CTF