AMMAR ALKHAFAJI

Houston, TX | (832) 475-3384 | ammar@it365hub.com
LinkedIn: linkedin.com/in/ammar-alkhafaji-79a5b5136

PROFESSIONAL SUMMARY

OSCP-certified Red Team Lead with 5+ years of experience in enterprise offensive security, adversary emulation, and penetration testing across network, web application, and Active Directory environments. Proven ability to identify high-impact attack paths, simulate real-world adversaries using MITRE ATT&CK, and translate technical vulnerabilities into business risk for executive and technical stakeholders.

Experienced in strengthening detection capabilities, improving identity security controls, and collaborating with blue teams to enhance incident response maturity. Hands-on experience supporting vulnerability management and patch remediation efforts using enterprise tools. Currently advanced CISSP knowledge across core security domains.

CORE SKILLS

Offensive Security & Red Teaming
Red Team Operations, Adversary Emulation, Penetration Testing (Network/Web/AD), Privilege Escalation, Lateral Movement, Post-Exploitation, Attack Path Analysis

Enterprise Security & Architecture
Active Directory Security, Identity & Access Management (IAM), Security Architecture Review, Attack Surface Reduction, Network Security, Segmentation Analysis

Risk & Frameworks
MITRE ATT&CK, OWASP Top 10, CIS Controls (conceptual), Vulnerability Management, Risk-Based Security Assessment

Security Operations & Collaboration
Purple Team Engagements, Incident Response Support, Detection Engineering Feedback, Security Control Validation, Executive Reporting

Tools & Technologies
rapid7 insightvm, Pentera, Galacticscan, Metasploit, Burp Suite, BloodHound, Nessus, OpenVas, Nmap, Impacket, Wireshark, Tanium, NinjaOne , Arctic Wolf (SIEM), SecurityOnion

Systems & Scripting
Windows, Linux, Unix, TCP/IP, DNS, HTTP/S, VPNs, Firewalls, Python, Bash

PROFESSIONAL EXPERIENCE

Red Team Lead | Sep 2019 – Present

- Lead and execute red team and penetration testing engagements across enterprise environments.
- Perform adversary emulation, privilege escalation, and Active Directory attack path analysis.
- Collaborate with blue teams to improve detection capabilities and incident response effectiveness.
- Identify and validate high-risk attack paths and security weaknesses across networks and identity systems.
- Translate technical findings into risk-based insights to support remediation efforts.

Tools Used:
Kali OS, Metasploit, Burp Suite, OpenVAs, Impacket, Nmap, Wireshark, CrowdStrike, darktrace

Client Engagements:
Delivered services to multiple clients through dedicated contract engagements.

Cybersecurity Specialist | Jul 2023 – Jan 2024

- Evaluated security controls across prevention, detection, and response domains to identify gaps.
- Supported vulnerability management and patch remediation using Tanium and NinjaOne.
- Assisted incident response activities and SIEM monitoring using Arctic Wolf.

Network Penetration Tester | Sep 2022 – Jul 2023

- Conducted internal and external network penetration testing against enterprise environments using rapid7 insightvm, Pentera.
- Identified misconfigurations, weak authentication mechanisms, and segmentation gaps.
- Delivered risk-based findings with actionable remediation guidance.

LABS & PROJECTS

Active Directory Attack Lab

Designed and deployed a multi-domain Active Directory lab to simulate enterprise environments and practice real-world attack scenarios. Performed privilege escalation, Kerberoasting, Pass-the-Hash, and lateral movement techniques using tools such as BloodHound and Impacket.

Red Team Automation & Scripting

Built Python and Bash scripts to automate reconnaissance, enumeration, and post-exploitation tasks, improving efficiency during engagements and lab simulations.

Web Application Security Testing Lab

Conducted hands-on testing of vulnerable web applications (e.g., OWASP-based labs), identifying and exploiting vulnerabilities such as SQL injection, XSS, authentication flaws, and access control issues using Burp Suite.

Red Team vs Blue Team Exercises

Designed and executed red vs blue team scenarios aligned with MITRE ATT&CK techniques to simulate real-world adversary behavior. Evaluated detection and response capabilities and provided feedback to improve security controls and visibility.

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP)
- Master Certified Ethical Hacker (MCEH) – EC-Council
- Top 10 Global Ethical Hacker – EC-Council (2021)
- CISSP – In Progress (ISC^2)