AMMAR ALKHAFAJI

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

PROFESSIONAL SUMMARY

OSCP-certified cybersecurity professional with 5+ years of experience across red teaming, penetration testing, and enterprise security assessments, with strong exposure to vulnerability management and security operations in complex enterprise environments.
Experienced in identifying, validating, and exploiting security weaknesses across network, web, and Active Directory systems, and translating technical findings into risk-based insights aligned with business impact.
Strong ability to prioritize vulnerabilities based on exploitability, exposure, and asset criticality rather than severity alone.
Skilled in supporting remediation efforts, improving security posture, and collaborating with IT and security teams to reduce risk exposure. Strong understanding of threat-driven security models, MITRE ATT&CK, and secure architecture principles, with hands-on experience in security monitoring and analysis using enterprise tools and SIEM platforms.

CORE COMPETENCIES

Vulnerability Management & Risk
- End-to-End Vulnerability Management
- Risk-Based Prioritization (beyond CVSS)
- Vulnerability Validation & False Positive Reduction
- Threat-Informed Risk Analysis
- Patch & Remediation Coordination

Offensive Security
- Red Team Operations & Adversary Emulation
- Network / Web / Active Directory Penetration Testing
- Privilege Escalation & Lateral Movement
- Post-Exploitation & Attack Path Analysis
- Exploit Validation

Enterprise Security
- Active Directory & Identity Security (IAM)
- Network Security & Segmentation
- Attack Surface Reduction
- Security Architecture (conceptual)

Security Operations
- SIEM Monitoring & Log Analysis (Arctic Wolf, Splunk)
- Incident Response Support
- Purple Team Collaboration
- Security Control Validation
- Executive & Technical Reporting

Tools & Technologies
- Rapid7 InsightVM, Pentera, Metasploit, Burp Suite, BloodHound, OpenVAS, Nmap, Impacket, Wireshark, Tanium, NinjaOne, Security Onion

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

EXPERIENCE

Red Team Lead | Sep 2020 – Present

- Lead and execute red team and penetration testing engagements across enterprise environments
- Perform adversary emulation aligned with MITRE ATT&CK to simulate real-world attack scenarios
- Conduct privilege escalation, lateral movement, and Active Directory attack path analysis
- Identify and validate high-risk vulnerabilities and misconfigurations across enterprise systems
- Translate technical findings into risk-based insights for remediation and business decision-making
- Collaborate with blue teams to enhance detection capabilities and incident response maturity

Vulnerability Management Contributions

- Validated scan results and reduced false positives
- Prioritized vulnerabilities based on exploitability, exposure, and business impact
- Identified critical misconfigurations (e.g., default credentials) leading to potential data exposure
- Supported remediation through secure configurations and access control improvements
- Applied compensating controls when immediate patching was not feasible

Cybersecurity Specialist (Jul 2023 – Jan 2024):

- Evaluated security controls across prevention, detection, and response domains
- Supported vulnerability remediation and patch coordination efforts
- Assisted incident response investigations using SIEM platforms
- Provided risk-based security recommendations to improve overall posture

Network Penetration Tester (Sep 2022 – Jul 2023)

- Conducted internal and external penetration testing in enterprise environments
- Identified misconfigurations, weak authentication, and segmentation gaps
- Validated exploitability to improve vulnerability prioritization accuracy
- Delivered clear remediation guidance aligned with business risk

PROJECTS / LABS / SECURITY RESEARCH

Active Directory Attack Lab

- Designed a multi-domain Active Directory environment simulating enterprise systems. Performed Kerberoasting, Pass-the-Hash, privilege escalation, and lateral movement using BloodHound and Impacket.

Red Team Automation & Scripting

- Developed Python and Bash scripts to automate reconnaissance, enumeration, and post-exploitation tasks.

Web Application Security Testing

- Performed security testing on OWASP-based applications, identifying SQL injection, XSS, authentication flaws, and access control issues using Burp Suite.

Red vs Blue Team Exercises

- Simulated adversary behavior aligned with MITRE ATT&CK to evaluate detection and response effectiveness.

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP+)
- Master Certified Ethical Hacker (MCEH) – EC-Council
- Top 10 Global Ethical Hacker – EC-Council (2021)
- (In Progress) CISSP – ISC²