

ABBAS BADREDDINE

Junior Cybersecurity Analyst

abbasbadredin@gmail.com | +961 81974936 | Nabatieh, Lebanon | www.linkedin.com/in/abbas-badreddine-14a74b273

PROFESSIONAL SUMMARY

Junior Security Analyst with hands-on experience in security operations center environments. Monitored and analyzed 500+ daily security events using SIEM tools including Splunk. Proficient in incident response following NIST 800-61 framework, threat analysis using MITRE ATT&CK, and vulnerability assessment. Strong knowledge of network protocols including TCP/IP, UDP, SNMP, Active Directory, LDAP, TLS, VPN, and IPSec. Experience with offensive security testing and exposure management. Seeking to leverage technical skills and cybersecurity knowledge in a Junior SOC Analyst role.

TECHNICAL SKILLS

Security Tools: Splunk, SIEM, Wireshark, Burp Suite, OWASP ZAP, Nmap, Nikto, Gobuster, ffuf.

Operating Systems: Kali Linux, Ubuntu, Windows, Windows Server.

Network Protocols: TCP/IP, UDP, OSI Model, HTTP, HTTPS, SSH, FTP, SMTP, SNMP, TLS, SSL, VPN, IPSec, LDAP.

Programming Languages: Python, Bash, PowerShell, JavaScript.

Security Frameworks: NIST Cybersecurity Framework, NIST 800-61, MITRE ATT&CK, OWASP Top 10.

Additional Skills: Active Directory, AWS Security, IAM, Cloud Security, Incident Response, Threat Intelligence, Scripting, Automation.

PROFESSIONAL EXPERIENCE

SOC Analyst Intern Wilses Cyber Security, Nabatieh, Lebanon Aug 2024 - Oct 2024

- Monitored and analyzed 500+ daily security events using SIEM platforms (Splunk), identifying malware, phishing attempts, and unauthorized access attempts.
- Performed incident response and triage following NIST 800-61 guidelines, documenting investigation steps and escalating high-priority security incidents.
- Conducted log analysis and root cause investigation to determine security breach origins and threat vectors.
- Applied MITRE ATT&CK framework to improve threat detection capabilities and security event classification.
- Utilized threat intelligence sources to stay current on emerging cybersecurity threats and attack patterns.
- Participated in offensive security exercises and penetration testing activities to understand attacker methodologies.
- Gained hands-on experience with AWS cloud security architecture and exposure management.
- Worked with network protocols including TCP, UDP, SNMP, Active Directory, LDAP, TLS, VPN, and IPSec.

Penetration Testing Trainee Bug Bounty Hunting Bootcamp Feb 2025 - Mar 2025

- Completed intensive 30-hour penetration testing and web application security bootcamp.
- Identified and exploited 15+ web vulnerabilities, including XSS, SQL Injection, CSRF, IDOR, and authentication bypass.
- Gained proficiency with security testing tools: Burp Suite, OWASP ZAP, Nmap, Nikto, ffuf, Gobuster.
- Conducted reconnaissance and information gathering for security assessments.
- Created detailed vulnerability reports following responsible disclosure practices.

EDUCATION

Bachelor of Science in Computer Science, Lebanese International University

Graduated: June 2024

Relevant Coursework: Network Security, Cryptography, Secure Software Development, Information Security. Participated in multiple Capture The Flag (CTF) competitions and cybersecurity challenges.

Information Technology Diploma, CIS College

Graduated: June 2019

Honor Student - Strong foundation in networking and system administration.

CERTIFICATIONS

In Progress: OSCP - Offensive Security Certified Professional (Expected 2026)

ADDITIONAL INFORMATION

- Core Competencies: Security Event Monitoring, Incident Response, Threat Analysis, Vulnerability Assessment, Log Analysis, SIEM Operations, Penetration Testing, Security Documentation
- Languages: English (Professional Working Proficiency), French (Professional Working Proficiency), Arabic (Native)
- Professional Attributes: Strong analytical and problem-solving skills, fast learner, excellent communication skills, team collaboration, attention to detail.