Qasim Tawalbeh

Cyber Security Jordan, Amman, Irbid | +962 782023773 | [kasemtawalbeh56@gmail.com](mailto:kasemtawalbeh56@gmail.com)

**LinkedIn:**  [www.linkedin.com/in/qasim-tawalbeh-a3b75522b](http://www.linkedin.com/in/qasim-tawalbeh-a3b75522b%20)

**GitHub**: <https://github.com/H3x0ra>

# PROFESSIONAL SUMMARY

Proactive Cybersecurity graduate with hands-on expertise in offensive/defensive security, penetration testing, and SOC operations. Skilled in vulnerability assessment, SIEM tools (Splunk, LogRhythm), network security (FortiGate, VLANs), and scripting (Python, Bash). Certified in LogRhythm, and TCM Security. Proven experience in CTF competitions, bootcamps (NCSCJO Nashama 5), and collaborative projects. Passionate about automating security processes and enhancing infrastructure resilience.Technical Relevant Coursework

# TECHNICAL SKILLS

* **Offensive Security:** Penetration Testing (Web, Network, AD), Kali Linux, Metasploit, Nmap, Burp Suite, OWASP Top 10
* **Defensive Security:** SIEM (Splunk, LogRhythm), Firewalls (FortiGate), GPO Management
* **Network Security:** DHCPv6, LDAP, DNS Poisoning Mitigation
* **Tools:** Wireshark, Docker, Certipy, John the Ripper, Impacket, XAMPP
* **Programming/Scripting:** Python, Bash, C#, PHP, HTML/CSS, MVC Framework
* Active Directory Security & GPO Management

# Experience

**Cybersecurity Intern | NCSC JO (Nashama Bootcamp 5) *Oct 2024 – Jan 2025***

* Conducted penetration testing , exploiting web, network, and AD vulnerabilities.
* Configured Splunk SIEM for log analysis, threat detection, and incident response; fine-tuned alert rules.
* Mitigated phishing risks by designing simulations, reducing employee susceptibility.
* Deployed FortiGate firewalls with policies for VPN, web filtering, and application control.
* Acquired practical skills in Docker, containerization, and Fortigate firewall configuration.
* Developed expertise in Linux system administration, Windows environments, and Active Directory.
* Strengthened networking fundamentals, including IP addressing, subnetting, and protocols.

**Asp.NET Trainee | Orange at Yarmouk University** *Jul 2024 – Aug 2024*

* Developed full-stack web applications using MVC architecture.

# PROJECTS

**1. Active Directory Exploitation & Defense Lab**

* Simulated DNS Poisoning (mitm6/NTLM relay) and ADCS ESC15 exploitation.
* Mitigated attacks via GPOs, LDAP signing, and **Splunk** monitoring.

**2. Vulnerable Web Application**

* Built a PHP/SQL platform with deliberate vulnerabilities (SQLi, XSS) for training purposes.

**3. Phishing Campaign & Network Scanner**

* Automated network reconnaissance using Bash; executed phishing simulations with tracked metrics.

# EDUCATION

* **BSc Cybersecurity | Yarmouk University** *2020 – 2024 | Irbid, Jordan*
* Relevant Coursework: Ethical Hacking, Cryptography, Digital Forensics, Risk Management

# CERTIFICATIONS

* **LogRhythm:** Security Analyst (LRSA), Platform Admin (LRPA)
* **TCM Security:** Linux Fundamentals
* **TCM Security**: Practical Ethical Hacking **(In Progress)**
* **Cyber Range Labs:** Soc Tier **1 (In Progress)**
* **CCNA: (In Progress)**

# EXTRACURRICULAR

* **CTF Competitor | NCSC Jordan** (Jun 2022): Ranked in national cybersecurity challenges.
* **Cyber Range Labs:** Studying for Junior/Senior Penetration Tester and SOC Tier 1 roles.

# TECHNICAL HIGHLIGHT

* **Automation:** Scripted network scans and log analysis workflows in Python/Bash.
* **SIEM:** Deployed Splunk rules to detect DNS spoofing and unauthorized certificate requests.
* **AD Hardening:** Secured environments via GPOs, LDAP channel binding, and Protected Users Group.