QASIM TAWALBEH

Amman, Jordan | *+962 782023773* | *QasimTawalbeh.0@gmail.com*

NOTION | *LinkedIn* | *Portfolio* *Github*

CAREER SUMMARY

Cybersecurity professional with expertise in offensive and defensive security, penetration testing, and SOC operations, SIEM tools (Splunk, LogRhythm), network security (FortiGate, VLANs), and scripting (Python, Bash). *Skilled in leveraging AI tools like ChatGPT to accelerate tasks such as writing and debugging code, developing scripts, creating documentation, and building* websites**.** Hands-on experience in CTF competitions, cybersecurity bootcamps (NCSCJO NASAMA 5), and security automation projects. Passionate about strengthening infrastructure resilience and mitigating cyber threats while utilizing AI-driven tools to enhance efficiency and productivity.

PROFESSIONAL EXPERIENCE

NCSC JO (NASAMA Bootcamp 5) Jordan — Oct 2024 – Jan 2025

Cybersecurity Intern

- Conducted penetration testing to exploit vulnerabilities in web applications, networks, and Active Directory environments, utilizing tools like Kali Linux and Metasploit.
- Installed, configured, and maintained Windows-based systems and network infrastructure (Windows Server 2016/2019/2022), troubleshooting software, hardware, and network issues in both physical and virtual environments.
- Configured and fine-tuned Splunk SIEM for log analysis, threat detection, and incident response, improving alert accuracy.
- Designed and executed phishing simulation campaigns to identify risks and educate users on mitigating social engineering attacks, effectively communicating technical procedures to non-technical stakeholders during awareness sessions.
- Deployed and configured FortiGate firewalls, implementing policies for VPN, web filtering, and application control to enhance network security.
- Gained hands-on experience with Docker, deploying containers and leveraging containerization for secure application hosting and isolation, also utilizing VirtualBox for isolated test environments.
- Strengthened foundational skills in Linux system administration, including CLI proficiency, automation, and troubleshooting across multiple distributions.
- Developed expertise in Windows environments and Active Directory, including setup, user management, and securing roles and permissions.
- Acquired solid knowledge of networking fundamentals, including IP addressing, subnetting, and network protocols, to secure local and wide-area networks with a focus on segmented network design.
- Built beginner-level proficiency in offensive security (penetration testing, vulnerability enumeration) and defensive security (log analysis, threat detection, system hardening).
- Committed to further developing skills in penetration testing, network security, and vulnerability management to secure critical digital infrastructures.

Orange at Yarmouk University. Jordan — Jul 2024 – Aug 2024

Website Development

- Developed full-stack web applications using HTML, CSS, Bootstrap, PHP, MYSQL, optimizing application efficiency by 70%.
- Applied PHP, and database management principles to improve system security and performance.

EDUCATION

- **BSc Cybersecurity | *Yarmouk University***
  2020 – 2024 | Irbid, Jordan
- Relevant coursework: **Networking fundamentals (IP, subnetting)**, Ethical Hacking, Digital Forensics.
-

PROJECTS

1. **Active Directory Exploitation & Defense Lab**
   - Simulated DNS Poisoning (mitm6/NTLM relay) and ADCS ESC15 exploitation.
   - Hardened Active Directory using GPOs, and SIEM monitoring.
   - and documented mitigation steps in clear, non-technical language for non-security stakeholders
2. **Vulnerable Web Application**
   - Developed a PHP/SQL-based platform with intentional SQLi and XSS, LFI, vulnerabilities Also lessons on each vulnerability for cybersecurity training.
3. **Phishing Campaign & Network Scanner**
   - Automated network reconnaissance using Bash scripting.
   - Executed phishing simulations, tracking user interaction metrics.

CERTIFICATIONS

1. **LogRhythm:** Security Analyst (LRSA), Platform Admin (LRPA)
2. **TCM Security:** Linux Fundamentals
3. **TCM Security:** Linux Privilege Escalation
4. **TCM Security:** Practical Ethical Hacking

EXTRACURRICULAR ACTIVITIES

CTF Competitor | NCSC Jordan (Jun 2022) - Ranked in national cybersecurity challenges.
Cyber Range Labs: Studying Junior/Senior Penetration Tester/ SOC Tier 1 roles (In Progress 30%).

Skills& Others

- **Operating Systems:** Windows Server 2016/2019/2022, Windows 10, Linux (Ubuntu, Kali)
- **Networking:** IP addressing, subnetting, gateways, DHCP, VLANs, DHCPv6, LDAP, DNS Poisoning Mitigation
- **Virtualization & Containers:** Docker, VMware, VirtualBox
- **Productivity Tools:** Microsoft Office (Word, Outlook, PowerPoint)
- **Offensive Security:** Penetration Testing (Web, Network, Active Directory), Kali Linux, Metasploit, Burp Suite, OWASP Top 10
- **Defensive Security:** SIEM (Splunk, LogRhythm), Firewalls (FortiGate), GPO Management, System Hardening
- **Active Directory Security:** GPO Management, LDAP Hardening, Protected User Group Implementation
- **SIEM Operations:** Configured custom Splunk rules for detecting DNS spoofing and unauthorized certificate requests
- **Programming & Scripting:** Python, Bash, PHP, HTML/CSS, Bootstrap
- **Soft Skills:** Strong organizational skills, task prioritization, and effective communication with both technical and non-technical personnel