

Professional Summary

Entry-level Security Engineer and SOC Analyst with hands-on experience in penetration testing, SIEM monitoring (Splunk, LogRhythm), wireless network troubleshooting, and Linux/Windows administration. Strong practical knowledge of Active Directory operations, domain attacks, and hardening. Familiar with EDR, IDS/IPS concepts, detection logic, and incident response fundamentals. Motivated to grow in defensive security and enterprise infrastructure.

Experience

Estarta Solutions – Cisco TAC (Wireless Engineer) Amman, Jordan	<i>Aug 2025 – Oct 2025</i>
<ul style="list-style-type: none">Troubleshoot AP registration, roaming, RF interference, DHCP/DNS issues, and authentication failures.Performed diagnostics using CLI, packet captures, and Prime Infrastructure.	
NCSC JO – Nashama Cybersecurity Bootcamp (Cybersecurity Intern) Amman, Jordan	<i>Oct 2024 – Jan 2025</i>
<ul style="list-style-type: none">Conducted penetration testing on web apps, networks, and Active Directory using Kali Linux.Configured and monitored Splunk SIEM for threat detection and alert analysis.Delivered phishing awareness training and executed simulated phishing campaigns.Deployed FortiGate firewall policies, VPNs, web filtering, and application control.Configured FortiGate HA (Active-Passive), performed failover testing, and validated sync.	

Projects

Active Directory Exploitation & Defense Lab

- Executed DNS poisoning and ADCS ESC15 exploitation; analyzed attack paths and domain misconfigurations.
- Hardened the environment using GPOs, LDAP signing, and SIEM monitoring rules.

Vulnerable Web Application (QRB Training Project)

- Built a PHP/SQL training lab demonstrating SQLi, XSS, LFI, and common web vulnerabilities.

Phishing Campaign & Network Scanner

- Created Bash-based network scanner and executed internal phishing simulations.

Education

B.Sc. in Cybersecurity Yarmouk University — Irbid, Jordan	<i>2020–2024</i>
---	------------------

Certifications

• LogRhythm Security Analyst (LRSA)	• LogRhythm Platform Admin (LRPA)	• TCM Practical Ethical Hacking	• Linux Fundamentals	• Linux Privilege Escalation	• TryHackMe: Pre-Security Path	• TryHackMe: Cyber Security 101
-------------------------------------	-----------------------------------	---------------------------------	----------------------	------------------------------	--------------------------------	---------------------------------

Technical Skills

- Operating Systems:** Windows Server 2016–2022, Windows 10, Linux (Ubuntu, Kali)
- Networking:** TCP/IP, DHCP, DNS, VLANs, WLAN, routing/switching basics, packet analysis
- Security Technologies:** SIEM (Splunk, LogRhythm), EDR concepts (behavior-based detection, threat response), IDS/IPS concepts (signature/anomaly detection), FortiGate Firewall
- Security Tools:** Metasploit, Burp Suite, Nmap, Wireshark
- Active Directory:** Domain services, GPOs, Kerberos basics, ADCS, privilege escalation paths
- Web/DB:** PHP, HTML/CSS, MySQL