Shay Mordechai

Security Researcher | OS Internals & Network Specialist

❖ 052-306-4991 | ❖ My E-Mail | ❖ My LinkedIn | ❖ My GitHub

Summary

High-performing Computer Science student (Graduating 2025) with deep-rooted expertise in **Network Protocols and Traffic Analysis (97)**. Expert in building custom network tools from scratch using Python/Scapy and **Raw Sockets**. Leveraging a strong systemic understanding of **Linux Internals** and Defense-in-Depth to research and secure Cloud-Native architectures (K8s/AWS). Skilled in bridging the gap between low-level networking and modern infrastructure.

Professional Experience

DevSecOps Intern | *Israel Tax Authority* | *2024 – 2025*

- **Implemented a Defense-in-Depth strategy:** Enforced **Schema Hardening**, conducted rigorous **Secure Code Reviews**, and provided debugging guidance to developers.
- Integrated SAST/SCA tools (Checkmarx) into CI/CD pipelines within Azure DevOps.
- Collaborated with SOC, SIEM, and InfoSec teams on secure system design and incident handling within Agile workflows.

Combat Soldier | Intelligence Gathering Unit, IDF

Technical Projects

Network Protocol & Traffic Analysis | Developed a comprehensive network research portfolio including:

- **CTF Platform**: Developed a custom challenge platform (3,400+ LoC in Python) simulating ICMP Exfiltration and TLS Spoofing. [GitHub]
- **TLS Traffic Generator**: Built a traffic generation tool using Scapy for custom handshake manipulation and packet crafting. [GitHub]
- **Core Protocols Implementation**: Built HTTP, DNS, and SMTP servers from scratch using Raw Sockets to analyze low-level packet structures. [GitHub]

AI-Augmented Vulnerability Research (SBCL Compiler) | (Private Repo - Responsible Disclosure in Progress) - Orchestrated an experimental research workflow to fuzz the SBCL compiler, identifying **3 potential zero-day vulnerabilities** (Memory Corruption/Stack Exhaustion). Validated findings through crash analysis, demonstrating deep understanding of **memory layout** and input validation mechanisms.

Kubernetes Security Home Lab | *Self-Initiated Project* - Built a nested virtualization environment (Fedora/Kubeadm) to explore Cloud-Native architecture. Currently **implementing Calico CNI and Falco** to study network policy enforcement and runtime system-call monitoring.

Cloud Automation: Developed Python automation scripts for AWS & GCP APIs, focusing on asset management and configuration validation.

Education

B.Sc. Computer Science | Jerusalem College of Technology | ***2021-2025*** | GPA: 89

Relevant coursework: Reverse Engineering (93), Network Analysis (97), Information Security (90).

Technical Skills

Cloud & Containers: Kubernetes (K8s), Docker, Minikube, AWS, Azure DevOps, rclone
Security Research: Network Protocol Analysis, Reverse Engineering, Malware Analysis, Fuzzing
Development: Python C/C++, Bash, SQL, Assembly
Tools: Wireshark, Burp Suite, IDA Pro, Checkmarx (SAST/SCA), Git, Linux (Fedora Atomic/Kali)

Languages: Hebrew (Native), English (Fluent)