

# Shay Mordechai

Cloud Security Researcher | DevSecOps & Network Specialist

☎ [052-306-4991](tel:052-306-4991) | ✉ [My E-Mail](#) | 💎 [LinkedIn: shay-mor](#) | 💎 [GitHub: shay-mor](#)

---

## Summary

**Passionate Security Researcher with exceptional learning agility, deep expertise in Network Analysis and Reverse Engineering.** Combines academic excellence (**GPA 89**) with hands-on experience in building custom security tools (Python/Scapy) and securing CI/CD pipelines. Currently focused on **Cloud-Native security research**, simulating attack vectors in Kubernetes environments. Highly motivated to leverage strong networking fundamentals into advanced Vulnerability Research roles.

---

## 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

**Kubernetes Security Home Lab** | *Self-Initiated Project*

- **Established an experimental environment** (Fedora/Ubuntu/Kubeadm) to explore Cloud-Native attack surfaces and virtualization.
- **Explored CNI** (Calico) implementations and Overlay Networks to understand Lateral Movement vectors and Network Policy bypasses.
- **Simulated security scenarios** such as Container Escapes and API Server misconfigurations to practice runtime threat detection using Falco.

**AI-Augmented Vulnerability Research (SBCL Compiler)** | ([GitHub](#)) - 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.

**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](#)]

**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 (*Graduating 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** (Advanced - Automation/Tooling), C/C++, Bash, SQL, Assembly

**Tools:** Wireshark, Burp Suite, IDA Pro, Checkmarx (SAST/SCA), Git, Linux (Fedora Atomic/Kali).

**Languages:** Hebrew (Native), English (Fluent).