Shay Mordechai

Security Researcher | OS Internals & Network Specialist

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

Summary

Security Researcher with a deep focus on **OS Internals**, **Binary Analysis**, and **Network Protocols**. Specializing in vulnerability discovery through custom tooling, including the development of an AI-augmented fuzzer that identified **3 Zero-Day vulnerabilities** in compiler infrastructure. Proven track record of engaging with **Enterprise PSIRT teams** to validate and implement architectural network-layer mitigations. Passionate about deconstructing complex system primitives - from **JIT engines** to **Linux Kernel namespaces -** to bridge the gap between theoretical architecture and practical exploitation.

Professional Experience

DevSecOps Intern | Israel Tax Authority | 2024 - 2025

- **Defense in Depth & AppSec**: Orchestrated a multi-layered security strategy across the SDLC. Conducted Threat Modeling (Design), integrated **SAST/SCA** pipelines (Build), and enforced **JSON**/XML schema hardening *on IBM DataPower (Runtime). Collaboration:* Partnered with SOC/SIEM teams on secure system design, code reviews, and incident response procedures.

Combat Soldier | Intelligence Gathering Unit, IDF

Technical Projects

AI-Augmented Vulnerability Research - SBCL Compiler

- **Discovery:** Identified critical **Logic Flaws** in the Macro Expansion engine leading to **Stack Exhaustion** and **Memory Corruption**.
- **Methodology:** Developed a custom **AI-Augmented Fuzzer** to generate recursive macro structures that bypassed compiler hygiene checks.
- **Status:** Reported to **MITRE** (Tracking ID: 1977672) and **Israel National CERT**.

LSaaS Platform - Zero Trust: Engineered a "Dark Server" on AWS with zero public ports using Cloudflare Argo tunnels and implemented rootless Podman containers on Fedora.

Network Protocol & Traffic Analysis Toolset: Built core protocols (HTTP/DNS/SMTP) from scratch using Raw Sockets and developed a Python-based CTF platform simulating MITM attacks on CAs.

Education

B.Sc. Computer Science | Jerusalem College of Technology | ***2021-2025*** | GPA: 89
Relevant coursework: Network Analysis (97)**,** Reverse Engineering (93), Information Security (90)

Technical Skills

Security Research: Focused on **JIT internals**, **Memory Corruption**, and **RSC** protocol logic.
Operating Systems: Daily **Fedora Kinoite** user; deep understanding of **Linux Internals** (Namespaces, Cgroups).
Network Analysis: L2-L7 protocol research; implemented protocols via **Raw Sockets** and **Scapy**.
Core Capabilities: Research Automation, Binary Analysis, Anomaly Detection, and Threat Hunting.
Stack: Python, C/C++, Assembly (x86), JavaScript, IDA Pro, Burp Suite.