Lian Mark

Ramat Gan, Israel | 050-9532222 | Lianmark00@outlook.com

ABOUT

Cybersecurity student (HackerU, 9 months — as of 09/2025) specializing in network defense, monitoring and SOC workflows. Hands-on experience with Python scripting, log analysis, and defensive testing in isolated lab environments. Started using PCs at age 8–9 — built and administered game servers 2012–2015 VIA File Protocol Transfer(FileZilla) — comfortable installing complex software and quickly learning new tools and libraries. Seeking a Junior SOC Analyst role.

EXPRIENCE

TDX-Arena Labs (Cybersecurity Training Environment) – Completed 40+ labs

• Used SOC tools (Splunk, Snort) to detect and respond to threats.

• Hands-on experience with Kali Linux: applied Linux fundamentals, performed Nmap scans, and analyzed traffic with Wireshark.

• Gained practical experience with attack tools such as John the Ripper, Hashcat, Mimikatz, Bettercap, ARPspoof, Metasploit (msfconsole), and more to understand attacker methods and defenses.

Python and C++ Codes

• Projects: UDP load simulator (lab-only); baseline file-hash scanner; TCP-SYN detector (alerts + JSON logs); network capture + Windows-FW blocking; process/resource monitor with signature checks; getAddresses.cpp (WIP pointer scanner) — all tested in controlled/lab environments.

EDUCATION (Hands-On)

HackerU — Cybersecurity Course (2025–2026)

Linux fundamentals: user & group management, file permissions, basic system administration.

Windows Server: Active Directory administration, Group Policy (GPO) lifecycle**.**

Network & infrastructure: packet analysis (Wireshark), network scanning & enumeration (Nmap, Hping3).

Offensive & defensive tooling: Metasploit (exploitation & post-exploitation), password/hash recovery and cracking (John the Ripper — including pdf2john/ssh2john, hashcat).

Endpoint & privilege escalation: NT AUTHORITY / Domain user privileges, registry & SAM, LSASS memory analysis, Mimikatz (lab only), memory dumps and log clearing concepts.

SIEM & SOC basics: agent deployment, log generation & collection (Windows Event Viewer), hands-on with Snort and Splunk via lab exercises. Also see my Github Projects.

Web fundamentals: HTML, CSS, JavaScript basics.

(All offensive techniques practiced in isolated lab/personal PC environments under ethical guidelines.)

PROJECTS & SKILLS

NOTE: Used AI guidance only for snippets and debugging support (never full scripts), ensuring I fully understood the code. As someone new to Python libraries, I quickly learned and applied them through hands-on practice.

projects link: https://github.com/lianmark/offense-defense-tools

- **Simple-DDoS-Attack.py:** Performed controlled stress-testing of internal services (Ports flood via UDP)

- Baseline_scan.py: Scans all files on the computer and extracts file hashes to check against a malicious-hash database.

- nmap_detector_v2.py: Monitors TCP-SYN packets — if an IP sends more than 100 packets within 5 seconds, an alert is shown. Saves all IPS history to a JSON file.

- **nmap&Ddos.py:** Captures inbound TCP/UDP packets and flags possible Nmap scans or DDoS floods, then blocks the source IP with Windows firewall.

- **processesMonitor.py**: Monitors Windows CPU/RAM and process network connections, logging high-resource processes, their remote endpoints and code-signature checks to logs.txt file inside Botnet_logs folder(self-created).

- **getAddresses.cpp** — WIP (requires pointer scanner). Opens a target process by PID, scans memory for a user-entered integer, tracks repeated matches, and overwrites frequently matched addresses with a chosen value. **NOTE: built and tested only on my own open-source game.**

TOOLS & TECHNOLOGIES

Linux (Ubuntu), Windows Server, Active Directory, Wireshark, Nmap, Hping3, Snort, Splunk, Metasploit, John the Ripper, hashcat, Python, C++, psutil, Scapy, WinDivert

LANGUAGES

- HEBREW - Native

- ENGLISH - Advanced