

DANIEL DAYAN

054-912-0911 | danieldayan2512@gmail.com | [LinkedIn](#) | [GitHub](#) | [ctftracker.com](#)

PROFESSIONAL SUMMARY

Entry-level cybersecurity professional targeting **Junior SOC Analyst** and **Junior Penetration Tester** roles. Rooted **50+ Hack The Box machines** (2 active) and completed **30 HTB Academy modules**, backed by ITQ's **650-hour Cyber Security Implementer program** (Cisco, Windows Server, FortiGate NGFW, IBM QRadar SIEM, Splunk SOAR). Built **ZeroBox (ctftracker.com)**, a pentest workspace with **4,000+ visitors**. Preparing for **HTB CPTS** and **CWES**. 3 years of IDF service handling sensitive cases under strict SLAs.

EDUCATION

Cyber Security Implementer Program, ITQ (650 hours, Cisco and Fortinet specialization)

2024 - 2025

Hands-on training in Cisco network infrastructure, Microsoft servers, firewalls and SIEM/SOC in an enterprise lab environment.

- Configured and hardened **Cisco IOS XE** routers and switches: VLANs and 802.1Q trunking, inter-VLAN routing, DHCP, OSPF, RIPv2, HSRP, ACLs, port security, NAT, and GRE and IPsec VPN tunnels.
- Set up and configured **FortiGate NGFW** for a simulated two-site network (Israel and USA): firewall policies, address objects, Virtual IPs (static NAT), antivirus and web filtering profiles, and a site-to-site **IPsec VPN**.
- Configured and hardened **Windows Server 2022**: Active Directory, Group Policy (GPO), NTFS permissions, disk quotas and DHCP with MAC filtering; studied **LPI Linux Essentials** and administered Kali and Ubuntu (Netplan, SSH, SCP, tcpdump).
- Set up and configured **IBM Security QRadar SIEM** with the WinCollect agent, Windows audit policies and syslog forwarding through the FortiGate, and set up **Splunk SOAR**.

High School Diploma, Computer Science Major (10 Units)

2020 - 2022

Final project: native Android app in Java for real-time cryptocurrency prices and currency conversion (USD/EUR/ILS); web development with HTML and CSS.

PROJECTS

Hack The Box, Labs and Academy

2025 - Present

- Rooted **50+ Hack The Box machines**, including **2 active machines**, taking each from reconnaissance and initial access through privilege escalation to full system compromise.
- Completed the **Cracking into Hack The Box** path and **30 Academy modules** using Nmap, Burp Suite, OWASP ZAP, ffuf, SQLMap, Metasploit, Hydra and Hashcat.
- Identified and exploited **OWASP Top 10** web vulnerabilities, including SQL injection (SQLi), cross-site scripting (XSS), command injection, file upload flaws, file inclusion (LFI/RFI), SSRF, SSTI, XXE, IDOR and broken authentication.
- Practiced the full **penetration testing process** and **vulnerability assessment** methodology: footprinting, shells and payloads, file transfers, password attacks and documenting findings.

ZeroBox, CTF Tracker and Penetration Testing Workspace | [ctftracker.com](#)

2026 - Present

- Designed, built and launched an offline-first penetration testing workspace (web app and Tauri desktop app) in **React and TypeScript**, reaching **4,000+ visitors**; includes a catalog of 1,000+ Hack The Box and TryHackMe machines, 131 reverse shell templates and an 8-phase methodology.
- Developed a multi-host **Nmap XML** importer and one-click attack graph generation, removing manual transcription of hosts, ports and services during reconnaissance.
- Built a masked credential and hash evidence vault, a **CVSS v3.1** Markdown report generator, and a timed exam simulator for OSCP, CPTS, CRT0, OSEP and CRTP that exports a one-click ZIP submission bundle.

MILITARY SERVICE

Service Coordinator, Soldier Benefits, Israel Defense Forces (IDF)

2022 - 2025

- Investigated and resolved hundreds of sensitive soldier entitlement cases in **SAP**, maintaining strict data confidentiality and high accuracy under daily SLAs.
- Prioritized and tracked complex escalations to resolution through **CRM and ticketing** workflows, writing clear case notes that sped up coordination between soldiers, commanders and external agencies.

TECHNICAL SKILLS

Security Operations: IBM QRadar SIEM, WinCollect, Splunk SOAR, Windows Event Logs, Windows Audit Policy, log analysis, Syslog, firewall configuration (FortiGate NGFW), antivirus and web filtering, access control, network security, Cyber Kill Chain

Penetration Testing: Web application security, OWASP Top 10, SQL injection, XSS, command injection, LFI/RFI, file upload, SSRF, SSTI, XXE, IDOR, broken authentication, privilege escalation, password attacks, reconnaissance and OSINT, vulnerability assessment, CVSS v3.1

Networking: TCP/IP, OSI model, DNS, DHCP, HTTP/HTTPS, SMB, FTP, SSH, VLANs (802.1Q), OSPF, RIPv2, HSRP, ACLs, NAT, port security, IPsec and GRE VPNs, Cisco IOS XE, FortiGate

Systems and Tools: Windows Server 2022 (Active Directory, GPO), Linux (LPI Linux Essentials, Kali, Ubuntu), VMware, Nmap, Burp Suite, OWASP ZAP, ffuf, SQLMap, Metasploit, Hydra, Hashcat, Wireshark, tcpdump

Programming: TypeScript, React, JavaScript, SQL, Bash, Git, Python (basic)

Professional: Working under pressure, multitasking, teamwork and independent work, service orientation, fast self-learning

Languages: Hebrew (Native), English (Very Good)