Kasem Shibli

Cyber Security Specialist | SOC & Penetration Tester

Country: Israel | Email: kasemshibli545@gmail.com | Phone: +972522886130

Linkedin: kasemshibli | Github: kasem545

Professional Summary

Hands-on cybersecurity professional with advanced practical experience in penetration testing, security monitoring, and incident response. Certified in ethical hacking, web application testing, and red teaming, with a proven record of building and managing enterprise-level SOC and pentesting labs. Skilled in SIEM log analysis, malware investigation, and network defense through real-world simulations, CTF competitions, and independent research.

Core Skills

- SOC & Monitoring: SIEM (Splunk, ELK, Wazuh), EDR tools, MITRE ATT&CK
- Incident Response: Log correlation, phishing analysis, malware sandboxing
- Penetration Testing: AD attacks, privilege escalation, web app exploitation, OWASP Top 10, OWASP API Top 10
- Networking: TCP/IP, DNS, DHCP, firewall rules, IDS/IPS tuning
- Operating Systems: Windows Server, Linux (Debian, Arch)
- Programming & Scripting: Python, Bash, Powershell
- Security Tools: Nmap, Metasploit, Burp Suite, Wireshark, Zeek, etc…

Practical Experience & Projects

Cybersecurity Operations & Threat Analysis Lab (2024–2025)

• Designed and operated a SOC homelab replicating enterprise security operations.
• Configured SIEM dashboards for log ingestion, correlation, and threat detection.
• Performed incident triage and escalation for simulated phishing, malware, and insider threat scenarios.
• Developed threat hunting playbooks for brute force detection, privilege abuse, and persistence.
• Integrated Suricata IDS for network anomaly alerts.

Red Team & Penetration Testing Projects (2023–2025)

• Built multi-domain Active Directory environments for privilege escalation testing.
• Executed internal/external attack simulations and post-exploitation scenarios.
• Performed web application and API assessments using OWASP methodology.
• Produced professional pentest reports with remediation recommendations.

Capture The Flag (CTF) & Challenges (Ongoing)

• Completed advanced HackTheBox Pro Labs (FullHouse, Solar) simulating real enterprise environments.
• Specialized in Windows privilege escalation, lateral movement, and persistence techniques.
• Ranked highly on HackTheBox and TryHackMe leaderboards through solving realistic exploitation challenges.

Additional Tools & Platforms

• Cloud Security: AWS GuardDuty, Azure Security Center, GCP SCC
• Container & DevSecOps: Docker, Kubernetes security basics, CI/CD pipeline security
• Forensics & Reverse Engineering: Volatility, Ghidra, IDA Free

Certifications

- Certified Red Team Analyst (CRTA) - Oct 2025
- DANTE HackTheBox ProLab - Oct 2025
- P.O.O HackTheBox ProLab - Oct 2025
- MCRTA – Multi Cloud Red Teaming Analyst -Oct 8 2025
- PT1 TryHackMe Practical - Oct 2025
- Certified Professional Penetration Tester (eCPPT) – Mar 2025
- Practical Network Penetration Tester (PNPT) – Sep 2024
- Web Application Penetration Tester (eWPT) – Oct 2024
- Junior Penetration Tester (eJPT) – Sep 2024
- Certified Ethical Hacker – Oct 2024
- CEH Master – Dec 2024
- Linux Essentials (LPI) – Nov 2024
- PCEP – Certified Python Programmer – Oct 2024
- HackTheBox FullHouse ProLab – Nov 2024
- HackTheBox Solar ProLab – Dec 2024

Education

• B.Sc. in Computer Science – Specialization in Cyber Security (2025 -) Open University of Israel Ra'anana
• Cyber Security Course (2021–2022), HackerU – 465 hours
• EC Council University (2022 – 2024) Certified Ethical Hacker Master

Languages

• Arabic (Native)
• English (Fluent)
• Hebrew (Fluent)