SHLOMO ROSS

CYSA+ CERTIFIED CYBERSECURITY PROFESSIONAL

shlomozross@gmail.com | (516) 574-9563 | LinkedIn | Github | New York, NY

About Me

Cybersecurity professional with a deep understanding of **incident response, risk assessment, vulnerability management, and penetration testing**. Adept at problem-solving and skilled in using cutting-edge tools and technologies. Passionate about combining these new skills with my 13+ years of professional work experience to pursue a career within cybersecurity.

Technical Skills

Operating Systems - Windows, MacOS, Linux (Kali, Sift)
Networking – TCP/IP Protocols, Switches, Routers, VPN, LAN/WAN
Firewalls – Bitdefender, Cisco, Palo Alto, Windows Firewall
Malware Analysis – Wireshark, VirusTotal, AlienVault
Command Line Interfaces – Command Prompt, Powershell, Linux
Directory Services - Active Directory, LDAP, OpenLDAP
Hypervisors – VMWare, Oracle Virtualbox, Microsoft Hyper-V
Vulnerability Scanners – Nessus, Nmap, Burp Suite, Nuclei, Accunetix, OpenVAS

SIEMs – Splunk, Elastic Search
IDS and IPS – Snort, Suricata
Scripting Languages – Python, Bash
Cloud Computing– AWS, Azure
Forensics – Autopsy, PhotoRec, FTK, Recuva
PenTest Tools – Metasploit, SQLmap, Hydra, BeEF

Expertise

- Threat Intelligence
- Security Standards & Frameworks
- Penetration Testing
- Network & Endpoint Security
- Vulnerability Assessment & Management
- Compliance & Risk Management
- Security Architecture
- Complex Problem Solving
- Cross-Collaboration

Education, Licenses & Certifications

CompTIA CySA+ (DoD 8570 IAT II, Security+ equivalent), Tier 2 Cyber Security Analyst, *2021*
Fullstack Academy Cyber Bootcamp, Cybersecurity Certification, *2020*

Relevant Experience

BreachLock Inc., *Penetration Testing Intern (Remote)* *Dec 2022 - Mar 2023*

- Conducted penetration tests on various enterprise systems and applications and collaborated with senior penetration testers to identify security vulnerabilities while documenting test results and preparing reports for clients
- Utilized the OWASP Top 10, network and web application scanning, password cracking, and code analysis to identify vulnerabilities
- Developed scripts to automate tasks and improve testing efficiency, resulting in a more streamlined testing process
- Identified and exploited security vulnerabilities in over 25 enterprise systems and applications by demonstrating knowledge of networking protocols, operating systems, and web application architectures
- Provided recommendations for improving security processes and best practices in team meetings, demonstrating a solid understanding of industry standards and protocols

Fullstack Academy Cyber Bootcamp, *Instructional Associate (Remote)* *Oct 2020 - Nov 2022*

- Set up virtual machines, created Python Scripts, conducted penetration tests, monitored logs, established firewalls, prevented phishing attacks, and hardened systems from known vulnerabilities
- Leveraged AWS to create a SOC classroom environment, setting up networks, servers, VPNs, and Honeypots
- Conducted penetration tests based on the MITRE ATT&CK framework and taught students how to gather information, think critically, and understand Windows OS, Linux OS, and Python programming fundamentals