Hemal Maniar
hemalmaniar23@gmail.com | LinkedIn | Website
OSCP | Security+ | eJPT

CAREER BREAK

Family Care & Personal Leave **November 2023 – May 2024**

- Took a six-month break to manage family care responsibilities during a critical time.
- Developed time management and multitasking skills to balance family obligations and professional development.
- Stayed engaged with latest tools and techniques by solving challenges on Hack The Box, TryHackMe, OffSec Playground, and participating in CTFs.

Offensive Security Certified Professional (OSCP) **June 2024 – October 2024**

- Committed to completing PEN-200 training and preparing for the OSCP certification.
- Gained hands-on expertise in penetration testing on Windows and Linux systems, along with reporting.
- Achieved OSCP Certification in October 2024.

PROFESSIONAL EXPERIENCE

Citizens Bank, ***Providence, RI, USA*** **May 2023 – October 2023**
Senior Cyber Threat Defense Operations Specialist

- Analyzed logs in Splunk SIEM, including dashboarding, event triage, and incident analysis.
- Conducted threat analysis using Crowdstrike EDR to identify and mitigate endpoint and network security risks.
- Performed security alert investigation and incident response using AWS GuardDuty, CloudTrail, and CloudWatch.
- Successfully tuned down 40% of Data Loss Prevention alerts, significantly improving incident response times.

Northeastern University - Information Technology Services, ***Boston, USA*** **September 2022 - December 2022**
Security Engineer

- Developed web application scanner using open-source tools to identify and report OWASP Top 10 vulnerabilities.
- Deployed scanner using CI/CD pipelines to enable vulnerability detection and streamline scanning capabilities.
- Developed scripts for efficient data parsing and leveraged KQL for Log Analytics in Azure Sentinel.

Southworth International Group Inc., ***Portland, ME, USA*** **January 2022 - August 2022**
Cybersecurity Analyst

- Led a comprehensive review of the organization's security policies and infrastructure, advocating for the creation of PO&M and SSP to comply with CMMC 2.0 standards.
- Configured Graylog server for data aggregation & forwarding to AlienVault SIEM for enhanced threat detection.
- Strengthened cybersecurity culture by deploying KnowBe4 modules for security awareness training, resulting in increased employee engagement and reduced security threat.
- Identified and resolved a bug on organization’s website, preventing exposure of 100+ PII records.

HackersEra Cybersecurity Consultancy and Training, ***Pune, India*** **June 2019 – December 2019**
Cybersecurity Associate

- Identified and exploited various vulnerabilities through responsible disclosure on public platforms, including active participation in bug bounty hunting, contributing to a more security digital environment.

EDUCATION

Master of Science in Computer Science and Information Security (Cybersecurity) December 2022
Northeastern University, *Boston, USA* GPA: 3.7/4

Bachelor of Engineering in Information Technology May 2020
Savitribai Phule Pune University, *Pune, India* GPA: 7.58/10

CORE SKILLS AND TOOLS

- Vulnerability Assessment: Nessus, SonarQube, Semgrep, Nuclei, Trivy, Nikto, Helio
- Incident Response: Splunk, Crowdstrike, Symantec, FireEye, Firepower, Netskope, Anomali ThreatStream
- Penetration Testing: BurpSuite, OWASP ZAP, Metasploit, Nmap, Bloodhound
- Cloud Security: AWS GuardDuty, AWS CloudTrail, AWS CloudWatch, MVISION Cloud, Cisco Firepower
- Governance & Compliance: Archer GRC, PDQ Deploy, ScoutSuite
- Languages: Python, PowerShell, Bash