Piyush Pote

8144098786 | piyush.pote@outlook.com | Linkedin

Cyber Security Analyst| Vulnerability Management| Penetration Tester| SOC Analyst

SUMMARY

Cybersecurity specialist with 2 years of hands-on experience in vulnerability management, penetration testing, and incident response. I specialize in designing policies and conducting threat assessments, leveraging tools like Qualys, Microsoft Defender, and Splunk to mitigate threats. Master's Degree in Cybersecurity Operations from Penn State and Certified in CEH, Security+, and Microsoft Security Operations.

WORK & EXPERIENCE

Merck Sharp and Dohme LLC — **Rahway, New Jersey**

Cybersecurity Analyst, ITRMS(Intern) — June – August 2023

- Engineered a groundbreaking integration system for Qualys, Wiz, and Microsoft Defender, the company's primary EDPs, using API technologies. Developed a single script that retrieves asset information affected by specific CVEs across all three platforms, significantly streamlining vulnerability management processes resulting in a 30% faster mitigation of critical vulnerabilities and bolstering endpoint protection across the enterprise.
- Designed and implemented interactive dashboards for real-time vulnerability tracking and remediation, increasing cross-team engagement and accelerating potential vulnerability identification by 20%.
- Developed a Python-based Linux Vulnerability Management System with MongoDB integration, automating CVE triage and reducing critical vulnerability response time by 20%.
- Orchestrated automation scripts based on vulnerability scan results from the integrated platforms, enhancing asset visibility by 10% and streamlining threat detection capabilities.
- Collaborated with Incident Response teams, utilizing the integrated data from SIEM tools like Microsoft Sentinel and Splunk to conduct advanced security log analysis and threat hunting.

ERSEGMENT — **Mumbai, India**

Penetration Tester, Red Team — April 2021 – June 2022

- Led high-stakes security investigations on government websites, employing advanced Vulnerability Assessment and Penetration Testing (VAPT) methodologies to uncover and mitigate critical OWASP Top 10 vulnerabilities earning 7 recognitions from NCIIPC (Government of India) for identifying and patching critical vulnerabilities.
- Designed and implemented an advanced web application security Capture The Flag (CTF) challenge for incoming interns, incorporating OWASP Top 10 vulnerabilities and industry-standard tools like Burp Suite and OWASP ZAP, effectively enhancing the company's penetration testing training program and fostering practical skills development.
- Developed comprehensive penetration testing scenarios and executed detailed test cases for diverse client websites, producing thorough documentation and proof-of-concept demonstrations as part of company attestation processes for multiple organizations.
- Executed comprehensive security assessments using Nessus scans and custom-tailored penetration testing strategies, identifying and exploiting system weaknesses to provide actionable remediation strategies, resulting in a 30% boost in overall system security and significantly enhancing clients' threat detection capabilities and security posture.
- Demonstrated advanced penetration testing skills by utilizing techniques such as privilege escalation, network pivoting, and exploit development successfully earning me a global ranking of #532 on the Hack The Box platform enhancing my threat detection capabilities.
- Specialized in Linux system security and web application vulnerability assessment through intensive practical challenges on TryHackMe, gaining proficiency with tools like Metasploit, Wireshark, and SQLmap. This culminated in ranking within the top 5% among over 1 million learners.

SDG-RAIT — **Mumbai, India**

Security Engineer, Backend Team(Intern) — April – November 2021

- Led security initiatives for a web application development project (VET appointments and bookings), implementing OWASP Top 10 security controls and conducting regular threat modeling sessions.
- Integrated automated security scanning tools like OWASP ZAP and SonarQube into the CI/CD pipeline, resulting in a 30% reduction in security vulnerabilities.
- Orchestrated security testing procedures, including penetration testing and vulnerability assessments using Burp Suite and Nessus, identifying and mitigating critical security flaws.
- Developed and enforced security policies for API endpoints, implementing robust authentication and authorization mechanisms using OAuth 2.0 and JSON Web Tokens (JWT).

CERTIFICATIONS & TECHNICAL SKILLS

Certifications: CompTIA Security+ Certification (SY0-701)**|**Certified Ethical Hacker (CEH V11)**|** ISC2 Certified in Cybersecurity (CC)

Security Tools: Qualys **|** Wiz **|** Microsoft Defender **|** Entra ID | Intune **|** Sentinel | Splunk **|** Crowdstrike Falcon | Wireshark **|** Nessus

Programming Languages: Python **|** C++ **|** Java **|** Javascript

Additional Skills: PowerBI **|** MongoDB **|** Docker **|** Azure **|** Cloud Security **|** Metasploit **|** Burp Suite **|** Wireshark **|** Active Directory

EDUCATION

Pennsylvania State University — **University Park, Pennsylvania**

Master of Science in Cybersecurity Operations and Analytics (3.8 GPA) — May 2024

Coursework: Web & E-Commerce Application Security, Offensive Security, Software Security, Network Security, Cloud Security.

Research Work: Securing the Smart: Exploring Optimal Defense Strategies Against Man-in-the-middle Attacks in IoT Networks.