Atharva Sardesai

Cybersecurity Intern

+91 94235 21051 atharvapsardesai@gmail.com
Pune, Maharashtra, India CyberWithAtharva cyberwithatharva.com

Summary

Cyber defender with a sharp eye for threats—skilled in cloud security, malware analysis and reverse engineering . I blend research, automation, and hands-on defense to stay one step ahead.

Experience

Cybersecurity Intern *06/2024 - Present*
Be4Breach

- Conducted comprehensive security assessments across AWS and Azure environments, uncovering misconfigurations and critical vulnerabilities, mapping them to their respective risks, leading to a 35% improvement in cloud compliance posture.
- Leveraged tools such as Prowler, and commercial CSPM platforms to validate environments against CIS benchmarks, NIST standards, and client-specific policies.
- Developed 10+ Python and Bash automation scripts to streamline cloud assessments, reduce manual overhead by 40%.
- Contributed to malware analysis and reverse engineering efforts, identifying and classifying malicious artifacts from incident samples using tools like Ghidra and CyberChef.
- Authored detailed vulnerability and assessment reports with root cause analysis, MITRE ATT&CK mapping, and tailored remediation plans, improving stakeholder clarity and actionability.

Skills

Cloud Security
- Assessed security misconfigurations in AWS, Azure, and GCP environments using Prowler and CloudSploit.
- Implemented least privilege access controls and IAM role policies to secure cloud assets.
- Monitored and analyzed cloud infrastructure logs to detect anomalous behavior and unauthorized access.

Malware Analysis & Reverse Engineering
- Conducted in-depth static and dynamic analysis of malware using IDA Pro, Ghidra, and Radare2.
- Reverse-engineered malware binaries across Windows, and Linux to uncover obfuscation techniques.

Threat Intelligence & Attribution
- Investigated cyber threats by analyzing attack infrastructure with Shodan, Censys, and VirusTotal.
- Mapped attacker TTPs to the MITRE ATT&CK framework for proactive threat hunting.

Network Security & Traffic Analysis
- Analyzed network traffic using Wireshark and Zeek to detect malicious C2 communication.

Cryptography & Evasion Techniques
- Researched anti-analysis mechanisms including sandbox evasion and VM detection.
- Reverse-engineered malware packing techniques to extract payloads from obfuscated binaries.

Online Courses & Certifications

- Google Cybersecurity Certificate - Google
- AWS Security Fundamentals - AWS Skill Builder
- Blue Team Junior Analyst - Security Blue Team

Education

B.Tech Information Technology *Vishwakarma Institute of Information Technology* **Pune** *(2021-2025)*
12th HSC *Arihant Junior College of Arts, Commerce and Science* **Pune** *(2021)*
10th CBSE *Sainik School Satara* **Satara** *(2019)*

Projects

Security Operations Center (SOC) Lab using ELK Stack

- Designed and implemented a SOC lab on Oracle Cloud using Elasticsearch, Logstash, and Kibana (ELK).
- Developed custom log parsers and alert rules to detect security misconfigurations and attacks.

Cloud Native Portfolio Website :

- Designed and deployed a responsive portfolio website using AWS Amplify.
- Integrated an AWS Lambda function to dynamically update blog posts from Medium.
- Configured AWS API Gateway for efficient API request handling.