Atharva Shirude

(240) 398-7708 | sec.atharvashirude@gmail.com | College Park, MD | Open to Relocation | LinkedIn | GitHub | **Blog:** https://rootissh.in

SUMMARY

I'm a Security Engineer with 2 years of hands-on experience in penetration testing across Active Directory, web, and thick client applications, along with threat detection and response. I bring curiosity, creativity, and just enough paranoia to keep things safe and interesting.

EDUCATION

University of Maryland, College Park *August 2023 – May 2025*

Master of Engineering in Cybersecurity, CGPA: 3.77

Relevant Coursework – Digital Forensics and Incidence Response, Penetration Testing, Cloud Security, Virtualization & Container

MIT World Peace University, Pune *August 2019 – June 2022*

Bachelor of Technology in Computer Science and Engineering, CGPA: 3.4

Relevant Coursework – Computer Networks, Information Security, Digital Forensics, Cyber Laws, Cryptography

WORK EXPERIENCE

Graduate Research Assistant, University of Maryland ***November 2023 – May 2025***

- Built a research pipeline to analyze cybersecurity risk disclosures, improving compliance data extraction efficiency.
- Applied NLP and automation to extract security governance insights from 10,000+ regulatory documents.
- Assessed cybersecurity risks and governance trends to support policy development and risk mitigation strategies.

Security Engineer, PKF Algosmic Pvt Ltd ***August 2022 – July 2023***

- Performed Vulnerability Assessment and Penetration Testing on web applications, identifying vulnerabilities (SQL injection, XSS, SSRF).
- Achieved Domain Controller compromise in 100% of Active Directory assessments through privilege escalation and lateral movement.
- Utilized core tools across 90% of engagements, including Burp Suite, Nmap, Metasploit Framework, Nessus, and Wireshark.
- Enhanced security posture of thick client applications, resulting in 80% reduction in vulnerability findings during subsequent assessments.
- Managed incident response by refining detection rules, and improving log analysis for threat detection and vulnerability management.
- Performed Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to identify vulnerabilities.

Security Engineer Intern, PKF Algosmic Pvt Ltd ***February 2022 – July 2022***

- Led 6 successful VAPT projects, identifying and remediating 15+ critical vulnerabilities, leading to reduction in attack surface.
- Enhanced problem-solving skills by developing automated solutions for security challenges.
- Produced a series of in-depth security blogs delving into the intricate world of malware and vulnerabilities, providing insights and analysis.

Associate Security Consultant, HACKX Security Pvt Ltd ***July 2021 – January 2022***

- Led VAPT engagements for critical financial applications, working closely with compliance teams to remediate risks.
- Authored 10+ technical blogs on penetration testing, increasing cybersecurity awareness and generating over 10,000 cumulative reads.
- Developed a secure software development lifecycle (SDLC) framework.

PROJECTS

Honeypot Deployment for Threat Detection & Logging

- Deployed a honeypot simulating SSH, HTTP, and FTP services to attract and log unauthorized access attempts.
- Configured Cowrie honeypot to capture attacker activities on SSH and FTP ports.
- Set up an HTTP server with intentional vulnerabilities (SQL injection, XSS) to analyze web-based attack attempts.
- Integrated Elasticsearch, Logstash, and Kibana (ELK stack) to collect, process, and visualize logs for threat analysis.
- Developed automated alerting mechanisms for detecting and responding to suspicious activities.

Secured a Cloud-based Healthcare Application Platform

- Conducted risk assessments and identified 20+ security vulnerabilities using AWS security tools. Implemented encryption and access controls.
- Implemented robust security measures, including encryption and access controls.
- Provided recommendations for HIPAA and PCI-DSS compliance.

Deployment of OpenTelemetry Demo with Terraform Automation and Kubernetes

- Automated multi-phase OpenTelemetry demo deployment on AWS using Terraform, Docker, and Kubernetes.
- Deployed application via Docker Compose on EC2 and validated service health through logs and endpoints.
- Configured Prometheus alerts with email notifications and set up CI/CD pipeline with rollback support using GitHub Actions.

ACHIEVEMENTS

- Secured 1st place at a Capture the Flag (CTF) competition hosted by the Army Institute of Technology, Pune.
- Achieved 9th place nationwide in the in-person Amazon CTF 2024, held across Seattle, Washington, DC, and New York.
- Vice President of the Cybersecurity Club, led the initiatives that enhanced engagement and expanded knowledge in the field.

CERTIFICATIONS

CEH Master, INE Junior Penetration Tester v2, Offensive Security Certified Professional (OSCP) (In progress)

TECHNICAL SKILLS

Programming Languages: Shell scripting, Python, PHP, JavaScript

Fields of Interest: Web Application and API Testing, Red Team Operations, Incident Response and SIEM, Cloud Security, AI Security

Technology: OWASP Top 10, Risk Management, SIEM, Threat Modelling, IAM, TCP/IP, UDP, IPSEC, HTTP, BGP, OSINT, EDR, Terraform

Security Tools: Nmap, Burp Suite, Wireshark, Nessus, Kali Linux, Shodan, KQL, Splunk, Elasticsearch, Docker, Kibana

Penetration Testing: Web Application, Thick Client, API, Social Engineering, OSINT, Windows Active Directory

Soft Skills: Ethical Judgment and Confidentiality, Creative Thinking, Problem-Solving, Team Collaboration, Time Management and Prioritization