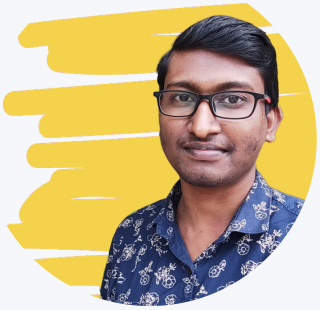

ANOOP B

Vulnerability Assessment & Penetration Tester

91 9605218790 | anup99bose@gmail.com | https://darkshadow04.github.io/Anoop.github.io

ABOUT ME

Cybersecurity professional specialized in Vulnerability Assessment and Penetration Testing (VAPT) with expertise in API, web, infrastructure, and endpoint security. Experienced across both offensive (Red Teaming, penetration testing) and defensive (vulnerability management, patch governance, compliance monitoring) operations. Skilled in managing vulnerability data, enforcing remediation timelines, and reducing critical exposures through risk-based prioritization. Proficient in leveraging AI-driven analytics and automations to enhance security reporting, operational efficiency, and enterprise risk posture.

WORK EXPERIENCE

Associate Penetration Tester

Tricon Infotech , Bangalore, India September 2022 - August 2024

Roles and Responsibilities:

- Led Red Teaming exercises and simulated attack scenarios to evaluate and enhance organizational defense mechanisms.
- Performed network, web, and application penetration testing, identifying and exploiting vulnerabilities using Metasploit and Kali Linux.
- Executed phishing campaigns to assess user awareness and conducted post-assessment training sessions to improve resilience.
- Conducted automated and manual vulnerability assessments, delivering detailed reports and mitigation strategies.
- Automated repetitive security tasks through Bash scripting, improving efficiency and reporting accuracy.
- Collaborated directly with clients to understand security requirements and deliver tailored VAPT solutions.

Security Delivery Analyst

Accenture , Bangalore, India August 2024 - ongoing

Roles and Responsibilities:

- Led API and web application penetration testing engagements, identifying and validating critical vulnerabilities to proactively reduce enterprise risk exposure.
- Operated across both offensive and defensive security functions, aligning penetration testing insights with patch governance and remediation strategy to strengthen overall security posture.
- Directed end-to-end vulnerability lifecycle management, including scan analysis, SPI matrix reporting, risk-based prioritization, and enforcement of patch SLAs to minimize Red-rated exposures.
- Applied AI-driven analytics to improve vulnerability triage, detect risk trends, and enhance remediation decision accuracy across large-scale technology environments.
- Optimized endpoint security controls by enhancing Tanium Application Control and File Integrity Monitoring (FIM), increasing threat visibility and compliance adherence.
- Secured cloud transformation initiatives by performing risk assessments and security validation during on-prem to SaaS migrations.
- Automated executive-level security reporting and dashboards through ServiceNow and AI integrations, improving audit readiness, transparency, and operational efficiency.

Recognitions & Achievements:

- Appreciated under the InfoSec Senior Managers Shout Out Program for consistent dedication and contribution to the Tanium migration project.
- Recognized by leadership for technical excellence, initiative, and reliability in project execution and delivery
- Acknowledged for technical proficiency, attention to detail, and professionalism, achieving P3+ ratings in API and web application security testing with 100% chargeability across projects.

EDUCATION

Bachelor's Degree, Industrial Microbiology and Zoology

Sub-subjects: Computer Science and Bio-Chemistry

VNS College of Arts and Science, Konni, Kerala.

June 2016 - March 2019

Post Graduate Diploma in Computer Applications

LBS Centre for Science & Technology, Adoor, Kerala

Sep 2021 - May 2022

Post Graduate Diploma in Cyber Forensics

Institute of Human Resources Development, Thiruvalla, Kerala

Aug 2022 - Feb 2023

SKILLS

- Vulnerability Assessment & Penetration Testing (VAPT)
- Red Team Operations.
- API penetration Testing
- Phishing Attack simulation.
- Bash and Python Scripting
- Attack Surface Management
- Threat Hunting
- Vulnerability Management
- Ethical Hacking
- Metasploit Framework
- Web Application Security Testing.
- Network Penetration Testing
- Defense Evasion
- Active Directory (AD) Attacks
- Deep web/Dark web exploration.
- Report Writing and Documentation

CERTIFICATIONS

- Certified Ethical Hacker (CEH v11) – Skillsoft
- API Penetration Testing – APIsec University
- Postman API Fundamentals Student Expert – Postman
- Digital Forensics Essentials (DFE) – EC-Council Learning
- Practical Web Application Security & Testing – TCM Security

PROJECTS:

Bank of America - Vulnerability Management.

Organization: Accenture | Duration: Dec 2025 – ongoing

- Led vulnerability governance under the **Vulnerability Simplification Program** within Global Market Technologies at Bank of America, managing **SPI matrices, vulnerability databases, and patch timelines** to maintain Green/Amber compliance.
- Analyzed **asset scan data**, validated **patch cycles**, and partnered with cross-functional teams to remediate security gaps and reduce Red-rated exposures.
- Implemented **automation and AI enhancements** in ServiceNow to streamline reporting, improve data accuracy, and optimize monthly security dashboards.

Tanium Security Tool Optimization

Organization: Accenture | Duration: Oct 2024 – Nov 2025

- Conducted **proof-of-concept (POC) testing and validation** for **Tanium Application Control** and **File Integrity Monitoring (FIM)** modules to evaluate readiness, stability, and effectiveness prior to enterprise rollout.
- Analyzed module performance, usability, and accuracy to ensure alignment with security objectives and operational requirements.
- Collaborated with engineering teams to identify bugs, optimize configurations, and validate module functionality under real-world conditions.
- Supported the migration testing from **on-premises to SaaS environment**, focusing on module performance, scalability, and reliability.

Invincione (Phishing Campaign)

Organization: Tricon Infotech | Duration: Mar 2023 – Sep 2023

- Orchestrated **phishing campaigns** to measure employee awareness and identify social engineering risks.
- Conducted **post-campaign training sessions**, increasing staff awareness and reducing phishing susceptibility.
- Delivered detailed **risk reports and recommendations**, improving organizational resilience against phishing threats.

MiniOrange Multi-Factor Authentication (MFA) Implementation

Organization: Tricon Infotech | Duration: Jul 2023 – Aug 2024

- Implemented **Multi-Factor Authentication (MFA)** to strengthen access control and protect against unauthorized logins.
- Improved overall **system security and data integrity** by integrating MFA into existing authentication workflows.
- Collaborated with stakeholders to ensure secure rollout and minimize authentication errors during deployment.

TOOLS:

Hands-on experience with industry-standard offensive and defensive security tools used for comprehensive vulnerability assessment, penetration testing, and threat detection.

Offensive Security:

- **Burp Suite Professional:** Advanced web and API penetration testing platform.
- **Metasploit:** Framework for exploitation, payload delivery, and Red Team simulations.
- **Kali Linux / Kali Purple:** Security-focused OS for penetration testing and defensive lab environments.
- **OWASP ZAP & Vooki:** Open-source and commercial DAST tools for web and API vulnerability scanning.
- **OpenVAS & Nessus Professional:** Network vulnerability scanners for identifying and validating security flaws.
- **HostedScan:** Cloud-based vulnerability scanning tool for asset exposure checks.
- **Postman:** API testing and validation tool used in security assessments.

Defensive Security Tools:

- **Tanium:** Endpoint management and security platform for Application Control and File Integrity Monitoring (FIM).
- **Security Onion & Wazuh:** SIEM and intrusion detection platforms for real-time monitoring and log analysis.
- **Trend Micro XDR & Email Security:** Threat detection and prevention solutions for endpoints and communication layers.
- **Trend Micro Attack Surface Management:** Continuous visibility into exposed assets and vulnerabilities.
- **ManageEngine:** IT operations management suite supporting configuration, auditing, compliance and Patch.

SOCIAL ENGAGEMENTS

GITHUB

GitHub Repositories: https://github.com/DarkShadow04

Curated collection of cybersecurity tools, projects, and resources demonstrating expertise in penetration testing, vulnerability assessment, and proactive defense strategies