ANOOP B

Vulnerability Assessment & Penetration Tester

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

ABOUT ME

Experienced Vulnerability Assessment and Penetration Tester with a strong background in cybersecurity. Over 1 year of hands-on experience in Penetration Testing and Red Teaming, complemented by 4+ years of dedicated involvement in the field through bug bounty programs, CTF challenges, and active cybersecurity research. Proficient in various programming languages and tools to uncover vulnerabilities, strengthen defenses, and enhance cybersecurity posture. Passionate about continuously learning and adapting to the dynamic landscape of cybersecurity.

WORK EXPERIENCE

Associate Penetration Tester

Tricon Infotech , Bangalore

September 2022 - Present

Roles and Responsibilities:

- **Utilized expertise in Extended Detection and Response (XDR) technologies to enhance threat detection capabilities within the organization.**
- **Orchestrated successful Phishing Campaigns to assess the organization's susceptibility to social engineering attacks and conducted subsequent training to improve awareness.**
- **Leveraged tools like Manage Engine and Trend Micro Email Security to bolster email security measures and protect against potential threats.**
- **Demonstrated proficiency in using Metasploit and Kali Linux for penetration testing and ethical hacking activities.**
- **Conducted thorough Vulnerability Assessment and Penetration Testing (VAPT) on various systems, networks, and applications, identifying vulnerabilities and recommending appropriate remediation measures.**
- **Led Vulnerability Management efforts by overseeing the identification, prioritization, and mitigation of security vulnerabilities across the organization.**
- **Played a pivotal role in Incident Response activities, contributing to the containment, eradication, and recovery processes during security incidents.**
- **Implemented and managed Security Information and Event Management (SIEM) solutions to monitor and respond to security events in real-time.**
- **Conducted regular Vulnerability Scanning to proactively identify and address potential security weaknesses.**
- **Actively participated in Red Teaming exercises, simulating real-world attack scenarios to assess defensive capabilities and identify areas of improvement.**
- **Contributed to defense side operations, collaborating with internal teams to enhance security posture and protect against cyber threats.**
- **Demonstrated proficiency in automation using Bash scripting, streamlining routine tasks and enhancing operational efficiency.**

CERTIFICATIONS

- CEH (Certified Ethical Hacker)
- Practical Web Application Security and Testing - TCMSECURITY
- Complete Metasploit Course: Beginner to Advance - Udemy
- Ethical Hacking Practical Course - Udemy

EDUCATION

Bachelor's Degree, Industrial Microbiology and Zoology

Sub-subjects: Computer Science and Bio-Chemistry

VNS College of Arts and Science, Konni, Kerala.

June 2021 - May 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

- **Endpoint Security**
- **Patch and IT Management**
- **Security Operations Center (SOC)**
- **SIEM/SOC Operations**
- **Vulnerability Assessment & Penetration Testing (VAPT)**
- **Bash Scripting**
- **Cyber Forensics**
- **Threat Surface Analysis**
- **Ethical Hacking**
- **Web Design and Development (HTML, CSS, JavaScript, Bootstrap)**
- **Metasploit Framework**
- **Report Writing and Documentation**
- **Red Teaming**

SKILL TOOLS:

Endpoint Security

- Apex One Endpoint Protection- Endpoint security solution.
- Trend Micro Email Security Std. - Email security solution by Trend Micro.
- Trend Micro Cloud App Security - Cloud application security solution.
- Trend Micro Apex One™ as a Service - Cloud-based endpoint security service.
- XDR Endpoint Sensor - Extended Detection and Response (XDR) endpoint sensor.

Patch & IT Management

- Manage Engine Endpoint Central - Comprehensive IT management tool for patching, threat and vulnerability management, IT asset management, remote control, and endpoint security.

Security Operations Center (SOC)

- Kali Purple OS - Operating system for security research and testing.
- Suricata - Open-source network threat detection engine.
- Wazuh - Open-source security monitoring and intrusion detection system.
- Snort - Open-source intrusion detection and prevention system.

SIEM (Security Information and Event Management)

- Security Onion - Open-source SIEM platform for monitoring and analyzing security events.

Vulnerability Assessment and Penetration Testing (VAPT)

- Nessus Professional - Professional vulnerability scanner.
- OpenVAS (Open-source) - Open-source network penetration testing tool.
- OWASP ZAP (Open-source) - Open-source web application penetration testing tool.
- Vooki - Web App & API Scanner - Dynamic Application Security Testing (DAST) tool for web apps and APIs.
- HostedScan (Open-source) - Online vulnerability scanner.

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

BLOG

Blog: https://arfortech.wordpress.com

Ethical hacking and cybersecurity insights, tutorials, and tools for penetration testing and vulnerability assessment using Termux on Android and Linux environments.