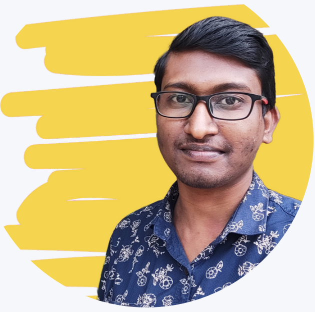

ANOOP B

Vulnerability Assessment & Penetration Tester

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

ABOUT ME

A skilled and dynamic Red Team Specialist with over 1 year of hands-on experience in Penetration Testing and Red Teaming, complemented by 4+ years of dedicated involvement in cybersecurity. Proficient in emulating adversary behavior and conducting full-scope simulated attacks, I excel in assessing organizational resilience against real-world threats. Leveraging expertise in Red Teaming methodologies and various programming languages, I provide actionable results to fortify digital infrastructures and enhance security posture. Passionate about continuous learning and adapting to the dynamic landscape of cybersecurity.

WORK EXPERIENCE

Associate Penetration Tester

Tricon Infotech , Bangalore September 2022 - Present

Roles and Responsibilities:

- Spearheaded Red Teaming exercises, orchestrating full-scope simulated attacks to assess the organization's defensive capabilities against real-world threats.
- Demonstrated proficiency in penetration testing and ethical hacking activities using Metasploit and Kali Linux.
- Conducted Host Network and Service Enumeration, Blind Web, Network, and Application Assessments to identify vulnerabilities and potential attack vectors.
- Implemented Red Team Activities including Bypassing User Account Control, creating and Impersonating Tokens, and executing Lateral Movement via SMB Protocol.
- Proficient in Credential Dumping, Kerberoasting, Pass-the-hash with Mimikatz, LDAP Reconnaissance, and BloodHound Reconnaissance.
- Conducted successful Phishing Campaigns to evaluate susceptibility to social engineering attacks, followed by comprehensive training sessions to improve awareness and resilience.
- Conducted Automated Security Scans and Manual Vulnerability Reproduction and Exploitation to uncover and remediate security weaknesses.
- Actively engaged in Client interaction & Handling, ensuring effective communication and understanding of security requirements.
- Played a key role in conducting thorough security audits, identifying vulnerabilities, and recommending appropriate mitigation measures.
- Streamlined operational tasks through automation using Bash scripting, enhancing efficiency and productivity.
- Provided comprehensive security awareness training to employees, empowering them to recognize and mitigate potential security threats.

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 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.
- Phishing Attack simulation.
- Bash and Python Scripting
- Threat Surface Analysis
- MITRE ATT&CK Framework
- 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

PROJECTS:

Invincione (Phishing Campaign) Duration: Mar 2023 - Sep 2023

Organization: Tricon Infotech

Orchestrated successful Phishing Campaigns to assess the organization's susceptibility to social engineering attacks and conducted subsequent training to improve awareness.

MiniOrange Multi-Factor Authentication (MFA) Implementation Duration: July 2023 - Present

Organization: Tricon Infotech

MiniOrange MFA project is implemented to strengthen the security posture of user systems, providing an additional layer of protection against unauthorized access and potential security threats. By incorporating Multi-Factor Authentication (MFA), it aims to safeguard sensitive data and prevent unauthorized entry, thereby ensuring the privacy and integrity of the system's resources.

TOOLS:

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.

Red Team Operations

- Mimikatz
- BloodHound
- Caldera
- Metasploit

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.