Abhiram T.G

Mysore, Karnataka | +91 9482606828 | **abhiramtg506@gmail.com** | **LinkedIn** | **GITHUB**

Executive Summary :

Motivated Computer Science Graduate with hands-on experience in Security Operations Center (SOC) environments, specializing in incident triage, SIEM configuration, and threat detection. Seeking to apply practical skills in incident response and vulnerability management to a Tier 1 SOC Analyst position.

Technical Skills :

Programming/Scripting : Python, Bash
Operating Systems : Linux (Kali, Ubuntu), Windows
Security Information & Event Management (SIEM) : Splunk, Wazuh
Intrusion Detection/Prevention Systems (IDS/IPS) : Snort, Suricata
Network Analysis: Wireshark
Vulnerability Assessment & Penetration Testing (VAPT) Tools : Metasploit, Nmap, Burp Suite, OWASP ZAP
Web Technologies : HTML, CSS, JavaScript (Basics), ReactJS (Basics)
Databases : MySQL, MongoDB

Education :

Bachelor of Engineering in Computer Science
Maharaja Institute of Technology Mysore
Graduated: July 2024 | **GPA**: 7.2

Professional Experience :

Cyber Security Analyst | CyberLancers Pvt.Ltd

Sept 2025 - Present

1. SOC Trainee - Cyberverse Foundation - CyberLancers.Pvt.Ltd **Feb 2025 - Aug 2025**

- Triaged and categorized security incidents, reducing false positives and ensuring timely escalation to senior analysts.
- Configured SIEM backends, developed custom dashboards, and performed detailed log analysis to identify and investigate security events.
- Developed and deployed Python scripts to generate simulated security logs using soc-faker, enabling comprehensive testing and validation of SIEM configurations.
- Configured and deployed custom decoders and rules within the SIEM to accurately parse, normalize, and alert on various log types
- Designed and implemented custom rule sets for specific log entries, enhancing threat detection capabilities within the SIEM.
- Documented and Maintained up-to-date knowledge of current cyber threats, attack techniques, and security best practices.
- Contributed to the testing and refinement of SIEM functionalities, focusing on improving alert fidelity and reducing false positives.
- Developed and delivered comprehensive educational content on Kali Linux including detailed screen captures of lab exercises and theoretical explanations.

2. Cybersecurity Intern - Future Interns [Remote] **Jan 2025 - Feb 2025**

- Performed Web Application Security Testing on a sample web application to identify vulnerabilities like SQL injection, XSS, and Authentication flaws using tools like Nmap, OWASP Zap and Burp Suite
- Built a User Friendly Interface based Password Strength Analyzer Tool using Python alongside a report explaining the Algorithm and its effectiveness
- Analyzed and Responded to a Simulated Cybersecurity Incident with an incidence response report with the help of tools like Splunk and Wireshark

3. Cybersecurity Intern - Forage - Commonwealth Bank [Virtual] **June 2024**

- Completed a job simulation specializing in fraud detection and prevention for the Commonwealth Bank Cybersecurity team.
- Developed Splunk dashboards for analyzing customer data to aid in fraud detection.
- Conducted penetration testing, identified vulnerabilities, and recommended remediation measures.
- Enhanced security awareness by creating infographics for password management based on Australian Cybersecurity Centre guidance.

Personal Projects :

Project 1 - Basic SOC Home Lab

Tools/Technologies : Nmap, Metasploit, Splunk, Sysmon, Snort, Suricata, Zeek

- Installed **Virtual environments** with **Windows10** as my **Target machine** and **Kali Linux** as my **Attacker machine**.
- Configured both the **Virtual Machines** for **Malware Analysis**
- Installed **Splunk** and **Sysmon** for **log collection** on my **Windows Machine**
- Scanned the **Windows machine** for any open ports using **Nmap**
- Conducted **Malware analysis** and created **Malware** by using a **Meterpreter Reverse Shell** as a **payload** on my **Kali machine** using **Metasploit**
- **Bypassed Windows real-time protection**, and established a **meterpreter shell** for investigation.
- **Detected the generated telemetry data in Splunk** which helped me in **Threat Detection.**
- Deployed and configured network security monitoring tools like **Snort, Suricata, and Zeek** to **analyze network traffic** and **investigate malicious PCAP** files within a home SOC lab environment.

Project 2 - Ethical Penetration Testing

Tools/Technologies : Metasploit, Nmap

- Used **Nmap** to perform **port scans** and **identify vulnerabilities** for reporting.
- Conducted vulnerability research and enhanced search capabilities using **Google dorks**.
- Loaded **Metasploit** modules to exploit vulnerabilities on target machines.
- Monitored systems for **unauthorized backdoor accounts** and potential threats.
- Created detailed **penetration testing reports**, helping the company address and **fix security vulnerabilities.**

Project 3 - Malware Analysis Lab

Tools/Technologies : FlareVM, RemnuxVM, PEStudio, TriDnet, Wireshark, Procmon, Virustotal

- Architected and managed a secure, virtualized analysis environment using **FLARE VM** and **REMnux**, enabling comprehensive **Static and Dynamic Analysis** of Malware samples, including **WannaCry Ransomware** and **ElectroRAT**.
- Uncovered critical Indicators of Compromise (**IOCs**) for the WannaCry sample by intercepting its **kill-switch domain** with **Wireshark** and documenting its unique file system artifacts with **ProcMon**.
- Analyzed and documented the advanced malicious behaviors of **ElectroRAT**, tracing its **keylogging** and **data exfiltration** capabilities with **ProcMon** and **Wireshark** to identify **unauthorized data transfer**.

Certifications :

- **Google Cybersecurity | Coursera**
- **CompTIA Security + | CompTIA**
- **Foundation Level Threat Intelligence Analyst | ArcX**

Languages :

Tamil, English, Kannada, Hindi

Hobbies/Interests :

- **Solving Courses, Challenges, CTF'S on platforms like OverTheWire, LetsDefend and HackTheBox**
- **Enrolling in the Latest Virtual Cybersecurity Simulations provided by Forage**
- **Listening to Music**
- **Reading Manga and Light-Novels**