MICHAEL THON PUR

CYBERSECURITY ANALYST

https://www.linkedin.com/in/michael-thon-pur

https://github.com/MichaelThon21

ekimikemignon21@gmail.com

+91 9606 807 411

BANGALORE - INDIA

ABOUT ME

Self-motivated BCA pass-out having keen interest in cyber security & cyber defense. Intrigued by learning about system attack mechanisms & defenses. Aiming to develop problem-solving skills in terms of identifying vulnerabilities, threat analysis, & contribution towards making more secured systems. Ambitious to build up my profile as a Cyber Security Analyst & make use of my technical acumen in securing an organization.

EDUCATION

Bachelor of Computer Applications, *T John College*
Aug 2022 – May 2025 | Bangalore,India

- ***Programming & Development Skills:*** Experienced in C, C++, Python, Java, HTML, CSS, JavaScript, and PHP Programming languages and have sound knowledge in Programming Concepts
- ***Database Management:*** Practical experience in designing, optimizing, and querying databases by MySQL
- ***Web Technologies:*** Developed end-to-end web applications involving front end as well as backend processing
- **Tools & Collaboration:** Git/GitHub professional with experience in using these tools as part of version control and team collaboration.

PROJECT

Academic Project, *AI-Based Traffic Analysis and Vehicle Counting System (YOLO)*
Feb 2025 – May 2025

- Developed an AI system for traffic analysis to detect, track, and count cars from live as well as recorded videos using object detection methods. Implemented multi-object tracking and virtual line crossing to enable accurate counting of cars without repetition. Used computer vision methods like region masking, frame processing, and bounding box visualization for accurate detection. Tested its performance for cars at night, at peak traffic hours, as well as on roads with varying environments. Designed to scale to traffic surveillance systems for smarter cities.
- **Tools & Technologies:** Python, Ultralytics YOLO, OpenCV, Machine Learning, Computer Vision.
- **Key Outcomes:** Accurate real-time vehicle detection • Improved traffic flow monitoring • Reduced manual traffic surveillance

LANGUAGES

English | Arabic

INTERNSHIP

TechByHeart, *CYBERSECURITY*
6 Months | Bangalore,India
Acquired hands-on experience with vulnerability scanning and penetration testing using prevalent tools under a controlled lab setting.

- **Network Security:** Performed active reconnaissance and vulnerability scans using Nmap and Nikto tools.
- **Web Application Security:** Identified vulnerabilities of the OWASP Top 10 in web applications using Burp Suite and OWASP ZAP, and carried out automated SQL injection scan using SQLMap.
- **Exploitation & Analysis:** Carried out ethical exploitation tests on the Metasploit platform, along with authentication by brute force attack with Hydra.
- **Defensive Monitoring:** Network traffic behavior analysis with Wireshark, simulating security log analysis with Splunk.
- **Methodology & Skill Development:** Experienced the entire vulnerability cycle from identification and analysis through exploitation and remediation using interactive platforms such as TryHackMe and Hack The Box.

SKILLS

Network Traffic Monitoring & Threat Detection
Examined real-time network traffic for anomalies, malicious data packets, and intrusion attacks in Wireshark, TcpDump software.

Network Scanning & Attack Surface Reconnaissance:
Identified open ports, running services, and vulnerable systems by scanning the network using Nmap and Netcat.

Vulnerability Assessment & Risk Identification:
Identified vulnerabilities in the target system and applications and proposed counter measures using Nmap, OpenVAS, Nessus.

Web Application Vulnerability Testing:
Identifies generic security risks such as SQL Injection & Cross-Site Scripting (XSS), performed in compliance with standards as defined by OWASP Top 10 & Burp Suite.

Web Traffic Interception & Analysis:
Analyzed HTTP/HTTPS traffic for vulnerable input processing, sessions, and authentication with Burp Suite and browser developer tools.

Ethical Hacking & Penetration Testing (Lab) :
Practical real-life methods for understanding attacker activity in controlled settings utilizing tools and technologies such as Kali Linux, Metasploit, Hydra.

Log Analysis & Incident Investigation:
Involved analysis of system and application logs to show how to recognize IoC using Linux system logs, Windows Event Viewer, SIEM Fundamentals.

Network Access Control & Firewall Configuration:
Prevented unauthorized access to the network and enhanced network traffic security through the use of "iptables" and Windows Firewall.

Operating System Hardening:
Inducted security in Linux and Windows by managing users, permissions, and services using Linus CLI/ Windows Security Policies.

System Monitoring & Event Tracking:
Managed system health and security events for early threat detection by writing shell scripts and using system monitoring tools.

Security Principles & Risk Management:
Applied foundational cyber security principles to enhance overall security posture by using the CIA Triad, risk assessment frameworks.