

MOHAMMED HABIBUR RAHMAN

Ainz.Mhr@gmail.com | +91 9841080909 | linkedin.com/in/mhr-ainz | github.com/AinzAmour | Chennai, IN

OBJECTIVE

Cybersecurity-focused BCA final-year student with hands-on experience in SIEM monitoring, digital forensics, SOC homelab environments, and competitive CTFs. Seeking an internship or entry-level role in SOC, cybersecurity, or IT operations to apply practical skills in threat detection, incident response, log analysis, and system security.

EXPERIENCE

Cyber Secured India | *Cybersecurity & Digital Forensics Intern* | Remote Apr 2025 – Jul 2025

- Analyzed 400+ system logs weekly to identify security threats, supporting SIEM monitoring and threat detection efforts.
- Assisted with digital forensics tasks including disk imaging, evidence preservation, and file recovery.
- Engaged in cyber labs and simulated attack scenarios to practically apply cybersecurity and incident response strategies.
- Documented attack patterns and developed mitigation strategies to support effective incident response.

Freelance IT Consultant | *IT Support Technician* | Chennai Jul 2023 – May 2025

- Configured and Installed operating systems, drivers, and productivity tools while executing routine maintenance, virus removal, and software troubleshooting to enhance cybersecurity.
- Set up Wi-Fi routers, firewalls, and home networks with a focus on initial security configurations.
- Delivered comprehensive technical support, Resolved 50+ hardware/software tickets for local clients.

PROJECTS

SOC Homelab with Splunk and Sysmon

- Built a virtual SOC using VirtualBox with Splunk Enterprise on Ubuntu and Windows 10 endpoint with Sysmon.
- Configured Splunk Universal Forwarder for log ingestion, performed log analysis, and created custom threat detection dashboards (SPL) for simulated incident response.

Adaptive Web Application Firewall (WAF) with Lightweight SIEM – Final Year College Project

- Developed a custom WAF solution integrated with a lightweight SIEM to detect and block web-based attacks in real-time.
- Implemented real-time credential strength analysis against a banned password list to prevent common brute-force attacks.
- Built a containerized WAF using Docker and Integrated a SIEM for real-time log analysis.

CERTIFICATES

Cyber Security & Digital Forensics Achievement Certificate

Cyber Secured India Aug 2025

CTRL. ALT. ACT. - Open-Source Intelligence (OSINT) Certificate

Cyber Secured India & .MKITOS Sep 2025

Python, Flask Complete Course

Horizon Tech - Udemy Dec 2024

EDUCATION

Bachelor of Computer Applications, BCA **CGPA:7.55** 2023 - 2026

Dr MGR Educational and Research Institute

HSE +2, 77% 2023

Sir M.C.T.M Boys Higher Secondary School

SKILLS

Cybersecurity & Tools : Splunk, Sysmon, Nmap, Wireshark, Burp Suite, Metasploit, OSINT, and other security utilities.

Programming & Scripting : Python, PowerShell, SQL, Web Development (HTML/CSS/JS).

Cloud & Virtualization : AWS, Docker, VirtualBox.

Operating Systems : Windows, Linux, and Server Administration.

Networking : TCP/IP, DNS, LAN/WAN, Wi-Fi, Firewalls, Network Configuration & Troubleshooting.

Version Control: Git, GitHub, Command-Line Operations.

EXTRA CURRICULARS

CTF Achievements: “Jeopardy-style” :

- 1st ARCANÉ 2K25 - *B.S. Abdur Rahman Crescent Institute of Science and Technology* - National - Oct 2025
- 2nd TECHA STRA '25 - *Dr. M.G.R. Educational and Research Institute* - National - Sep 2025
- 3rd ZERODAY CTF 2025 - *Z3R0_LOG0N - JGEC's - 24hr online* - Global - Oct 2025
- 3rd Hackers Asylum CTF - *SSN College of Engineering* - National - Sep 2025
- Top25 Finalist H7CTF - *S.R.M UNIVERSITY -K.T.R Campus* - National - Oct 2025