MD ZISHAN FIROZ

Patna, Bihar | P: +91 9006776876 | zishanfiroz@gmail.com
LinkedIn: linkedin.com/md-zishan-firoz-405031204

EDUCATION

Dehradun Institute of Technology — Dehradun, India
Bachelor of Technology (B.Tech) — July 2024
Computer Science & Engineering; Specialization in **Cyber Security and Privacy** — (Graduated)

WORK EXPERIENCE

Cybersecurity Research Intern — Remote
PurpleSynapz — Feb 2025- Present

- Analyzed and investigated security logs from **Zeek** for **intrusion detection** and network monitoring.
- Refined and customized **Zeek scripts** for better automation of network monitoring and incident detection.
- Conducted in-depth analysis of **network logs** generated by Zeek to identify anomalies and investigate security incidents.

Cyber Security Intern — Noida, UP
Qunit Technologies — Dec 2023 – Mar 2024

- Actively **monitored and analyzed** security alerts using **SIEM** tool.
- Learned about **threats and vulnerabilities** in web application and network.
- Researched on innovative **API Security** Tool from scratch.
- Authored insightful blogs for the company website.

Cyber Security Administrator Intern — Remote
Virtually Testing Foundation — Jan 2023 – Mar 2023

- Conducted regular **security assessments** and **identified vulnerabilities**.
- Managed user **access and permissions**, ensuring least privilege principles are followed.
- Utilized security tools and software to **monitor and analyze** network traffic for potential threats.
- Worked with IT teams and management to integrate security measures into daily operations.

Technical Skills

Security Tools: Burp Suite, Splunk, Wazuh, Nessus, Nmap, Wireshark, pfSense, Zeek
Skills/Expertise: Incident Response, SIEM, VAPT, SOC, Identity and Access Management (IAM), Web Application Security, SOAR, IDS/IPS, Network Security Monitoring
Language: Bash scripting

Projects

SOC Homelab for Threat Hunting and Incident Response :

- Built a SOC homelab environment using **VirtualBox**, **Wazuh, Suricata**, **pfSense.**

Achievements

- Hall Of Fame – **CERT- EU European Union**
- Received acknowledgment from companies/government platforms for responsible disclosure of critical data leaks and misconfigurations. **(Verizon, IITD, IITB, Telangana Govt, Kerala Govt).**
- Contributed to strengthening the cybersecurity posture of organizations by uncovering sensitive information exposure, including **personal details, credentials, and internal documents**.

Courses and Certifications

- Certified Cyber Security Analyst (C3SA) - CWL
- Cyber Incident Response - Coursera