

Aashirwad Verma

+91 97736 32552 aashirwadverma7@gmail.com linkedin.com/in/Aashirw4d github.com/Aashirw4d

Professional Summary

Cybersecurity graduate with hands-on experience in SOC operations, digital forensics, threat detection, incident documentation, and infrastructure security through internships at Infrastructure Gas Limited (IGL), Delhi Cyber Cell, and Verzeo. Experienced with Microsoft Defender, SIEM tools, Python, Windows/Linux administration, and OSINT investigations. Seeking Security Analyst, SOC Analyst, Incident Response, or Threat Intelligence roles.

Skills

Analysis & Scripting: Log Analysis, Event Correlation, Python, Bash, SQL, SPL, Analytical Problem Solving

Digital Forensics: LFTK Imager, Autopsy, Volatility, Wireshark, HxD Hex Editor, The Sleuth Kit, File System Analysis (FAT16/NTFS)

SOC Tools: SIEM, Security Tools, Microsoft Defender, CrowdStrike EDR, Email Analysis

Threat Detection: Use Case Understanding, Alert Triage, Incident Management, Phishing, Malware, Brute Force, MITRE ATT&CK

Security Operations: Windows/Linux Logs, TCP/IP, DNS, Ports, Protocols, Incident Notes, Reporting, Awareness Training

Experience

Indraprastha Gas Limited (IGL)

July'25 – Sep'25 | Delhi, India

- Valuated cybersecurity controls to ensure compliance with security standards.
- Reviewed cybersecurity controls and compliance documentation for industrial infrastructure environments, supporting security assessments and risk identification.
- Gained hands-on exposure to network infrastructure, system monitoring, and technical documentation while collaborating with engineering and operations teams.

Digital Forensics Intern | Delhi Cyber Cell (NCFL|IFSO)

July'24 – Aug'24 | Delhi, India

- Analyzed cybercrime cases by applying advanced **forensic techniques** and reporting findings to senior officers.
- Supported **Dark Web** training sessions for **60+ police officials** to build cybersecurity awareness.
- Assisted in digital evidence analysis, forensic reporting, and cyber incident investigations while gaining practical exposure to law enforcement workflows.

Verzeo Remote | Cyber Security Intern

Aug'22 – Oct'22 | Remote, India

- Performed OSINT on Amazon infrastructure using Shodan and Censys; identified 20+ exposed endpoints
- Simulated complete kill chain in lab environment: recon to post-exploitation using Kali Linux.
- Documented step-by-step attack vectors in 10-page report as part of major project.

Projects

SentryPot - Cyber Honeypot

- Developed a Python-based multi-service honeypot simulating SSH, HTTP, and FTP attacks.
- Built a Flask dashboard to visualize attacker IPs, login attempts, and executed commands.
- Collected and analyzed attack telemetry from Kali Linux simulations.
- Used SQLite for event storage and reporting.

FTK Imager - Digital Forensics Investigation

- Acquired and analyzed forensic disk images using FTK Imager while preserving evidence integrity.
- Verified file hashes, documented findings, and followed standard digital evidence handling procedures.
- Documented forensic findings and followed standard evidence handling procedures for investigation and reporting.

Security Research & Engineering

- Designed CTF challenges across forensics, OSINT, malware, and exploitation; produced security write-ups.
- Investigated Windows and Linux system artifacts to support digital forensic analysis and incident investigations.
- Completed 76+ practical cybersecurity labs on [tryhackme/Indian4don5](#) covering SOC, DFIR, Threat Hunting, Network Analysis, Web Security, Splunk, SIEM, and MITRE ATT&CK.

Education

B.Tech CSE with Cyber Security & Threat Intelligence, Manav Rachna University

Sep'22 - Jun'26

Senior Secondary School, Paramount International School

Apr'19 - Mar'21

Secondary School, Paramount International School

Apr'10 - Mar'20

Publications

Impact of Browser Extensions on Web Security: Analysis of Privacy and Security Risks of browser extensions using packet analysis tools

Feb'25

- Aashirwad Verma, Aayush Gupta, Dr. Shalu

Leadership & Recognition

- Reported an IDOR access control vulnerability during structured security testing; the issue was acknowledged and successfully fixed.
- Received **Appreciation & Recommendation** from **IEEE MRU** for contributions to cybersecurity events and growth.
- Practiced security awareness, operational discipline, clear reporting, and continuous learning of evolving threats.