

# SATYA SAGAR NAGESH

Cybersecurity Undergraduate

☎ +91-7381718378 ✉ [satyasagarofficial@gmail.com](mailto:satyasagarofficial@gmail.com) 📄 [satyasagar6087](#) 🌐 [HTB-A8C5273C12](#) 🌐 [sudo-satya.medium.com](#)

## EDUCATION

Vellore Institute of Technology

Oct 2022 – Ongoing

B.Tech in CSE (Specialization in Cybersecurity & Digital Forensics) - **CGPA - 8.42** Madhya Pradesh, India

## TECHNICAL SKILLS

**Security Tools & Frameworks:** Nessus, OpenVAS, Metasploit, Burp Suite, Wireshark, Nmap, Cisco Packet Tracer, SIEM Tools, Incident Response, NIST Cybersecurity Framework, OWASP Top 10, CIA Triad

**Operating Systems & Networking:** Windows, Linux, Computer Networks, Networking Tools & Devices

**Programming & Scripting:** Python, C++, Java, Bash

## PROJECTS

**Phishing Simulation Forensic Email Analysis** | Gophish, VirusTotal, Kasm

Oct 2025

- **Offensive Phase:** Deployed **GoPhish** via **Kasm Docker** to run 2 phishing campaigns, creating a deceptive email and fake login page that tracked delivery, opens, and credential submissions.
- **Defensive Phase:** Analyzed phishing email headers and identified 3 spoofing alerts by Gmail. Scanned the malicious attachment with **VirusTotal**, resulting in 13 detections, and performed static analysis using the **Rabin** sandbox tool to extract key indicators of compromise (IOCs).
- Documented the complete end-to-end attack lifecycle in a comprehensive report. The analysis determined that the malicious payload possessed advanced system-level capabilities, including memory inspection and enumeration, and could deploy persistent threats such as keylogging, screen capture, and the creation of fake GUI elements to deceive users.

**Operation Deep Packet** | Wireshark, NetworkMiner, Snort

Nov 2025

- Analyzed a collection of 15 PCAP files within a simulated Security Operations Center (SOC) environment.
- Utilized tools like **Wireshark**, **NetworkMiner**, and **Snort** to identify malicious network activity and security threats.
- Key discoveries during the assessment included the EternalBlue exploit, ARP poisoning, and malformed TCP packets (Broken TCP ACK in SYN Packet).

## ACHIEVEMENTS

- **Bug Bounty:** Acknowledged vulnerability reported to Coderzcolumn & a duplicate reported to Immutable Bug Bounty Program.
- **TryHackMe & HackTheBox:** Enhanced technical skills by solving over 30 badges, 90+ rooms and machines across both platforms.
- **Medium:** Authored 8 detailed medium writeups documenting methodologies and solutions for security lab exercises.

## CERTIFICATIONS

- **Google Cybersecurity Professional Certificate – Coursera (2025):** Completed 8 practical courses studies involving Python, Linux, SQL, Security Information & Event Management (SIEM) Tools and IDS to identify and mitigate threats, risks, and vulnerabilities.
- **Certified Network Security Practitioner (2025):** Foundational certification validating core knowledge in network security principles, threat detection, and defensive security measures.
- **ISC2 Certification (2024):** Foundational knowledge in security principles, network security, access controls, security operations, and incident response with business continuity & disaster recovery concepts.

## Hobbies & Languages

- **NCC Cadet (2015-2022:)** Trained in Arms & Ammunition, Map Reading, Drills, First Aid.
- Brown Belt holder in Karate.
- **Languages:** English, Hindi, Odia & Russian