

Bornov Shyam Kalita

India

bornovofficial@gmail.com — +91-7576909883 — LinkedIn — TryHackMe — HackTheBox

Professional Summary

Cybersecurity-focused engineering student with hands-on experience in offensive security, Digital Forensics and Incident Response (DFIR), and OSINT through labs, CTFs, and a self-built security homelab. Designed and analyzed simulated attack scenarios involving exploitation, log analysis, and incident reconstruction across Linux and Windows environments. Strong interest in investigative security roles that combine attacker behavior analysis with defensive detection and response.

Education

National Institute of Technology Silchar

B.Tech in Electronics & Communication Engineering

2024 – 2028

CGPA: 8.6 / 10

Spring Dale International School (CBSE)

Senior Secondary (Class XII)

2022 – 2024

Awarded Student of the Year

Experience & Projects

Cybersecurity Practice & Labs (Offensive → Defensive Focus)

Self-directed

2023 – Present

- Architected and maintained a **5–7 VM security homelab**, modeling **15+ attack and investigation scenarios** across Linux-based systems.
- Configured attacker, victim, and investigation hosts (Kali Linux, vulnerable servers, analysis VMs) to emulate small enterprise network behavior.
- Conducted **20+ exploitation exercises** spanning enumeration, service abuse, and privilege escalation to establish attacker footholds.
- Performed **post-compromise investigations** by analyzing **100+ authentication, system, and web log events**.
- Reconstructed **10+ intrusion timelines**, identifying attacker actions, persistence techniques, and indicators of compromise.
- Documented investigation findings and security misconfigurations to reinforce DFIR workflows.

Web Security & Exploitation

- Completed **60+ labs** on PortSwigger Web Security Academy covering SQL Injection, XSS, Broken Access Control, and CSRF.
- Explored exploitation paths across **20+ vulnerable workflows** to identify authorization flaws, insecure input handling, and session weaknesses.

- Mapped web vulnerabilities to underlying design and configuration issues affecting application security.

OSINT & Investigation

- Completed **15+ OSINT challenges** involving open-source data discovery across public records and social platforms.
- Validated findings through **3–5 independent sources per case** to minimize false attribution.
- Synthesized fragmented open-source data into coherent investigative narratives.

Technical Skills

Security Domains: DFIR, OSINT, Web Application Security, CTF Methodology, Incident Analysis

Tools & Platforms: Linux (Kali, Ubuntu), Wireshark, tcpdump, Burp Suite, Metasploit, Netcat, Hashcat, John the Ripper, Splunk (log analysis on **100+ events**), Autopsy, EZ Tools, Kape, Redline, Volatility (memory artifact exploration), Git/GitHub, VMware

Programming & Scripting: Python, Bash, C/C++, JavaScript (basic), Solidity

Leadership & Communication

- Hosted the opening and closing ceremonies of NITSHACKS 8.0, the largest technical hackathon in North-East India.
- Comfortable with public speaking, cross-team coordination, and working under pressure.
- Experience leading and collaborating within small technical teams during hackathons, CTFs, and projects.

Achievements

- Hack The Box University CTF: Ranked Top 200 globally and Top 5 in India (3-member team).
- TryHackMe Global CTF: Led a team ranked among the Top 5% globally.
- AICTE National Ethical Hacking Hackathon: Participated in multi-domain challenges involving Linux, Windows, and cloud environments.

Certifications

- TryHackMe – Industrial Intrusion (Top 5% globally)
- TryHackMe – Cyber Security 101
- Hack The Box University CTF: Ranked **Top 200 globally** and **Top 5 in India** among **5,000+ participating teams**.