

Bornov Shyam Kalita

📍 India | ✉ bornovofficial@gmail.com | 📞 +91-7576909883

🌐 LinkedIn | 🛠 TryHackMe | 🛠 HackTheBox

Professional Summary

Cybersecurity engineering student specializing in offensive security, Digital Forensics & Incident Response (DFIR), and Open Source Intelligence (OSINT). Proven expertise through 100+ hours of hands-on lab work, CTF competitions, and a self-built enterprise-grade security HomeLab. Analyzed attack vectors, reconstructed intrusion timelines and identified indicators of compromise across Linux and Windows environments in over 50 lab scenarios, contributing to improvements in incident response strategies and security protocols.. Seeking investigative security roles combining threat actor behavior analysis with defensive detection and incident 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

Technical Experience

Penetration Tester & DFIR Analyst

Security Homelab & Penetration Testing

2025 – Present

Kali Linux, Metasploit, Wireshark, Splunk

- Architected enterprise-simulated security homelab with 5–7 VMs modeling real-world attack scenarios across segmented Linux and Windows networks
- Executed 20+ red team exercises including enumeration, service exploitation, privilege escalation, and lateral movement to establish persistent access
- Performed blue team incident response by analyzing 100+ authentication, system, and web server log events using Splunk and native Linux tools
- Reconstructed 10+ complete intrusion timelines identifying TTPs (Tactics, Techniques, and Procedures), persistence mechanisms, and IOCs
- Documented post-exploitation findings and security misconfigurations, developing remediation strategies aligned with MITRE ATT&CK framework

Web Application Penetration Tester

Web Application Security Testing

2025 – Present

Burp Suite, OWASP Top 10, PortSwigger Academy

- Completed 60+ practical labs covering SQL Injection, Cross-Site Scripting (XSS), Broken Access Control, CSRF, and authentication bypass techniques
- Identified and exploited 20+ authorization flaws, insecure input validation vulnerabilities, and session management weaknesses
- Mapped discovered vulnerabilities to OWASP Top 10 categories and underlying application design flaws affecting CIA triad

OSINT/Threat Intelligence Analyst

Open Source Intelligence (OSINT) Operations

2025 – Present

Maltego, theHarvester, Social Engineering

- Conducted 15+ OSINT investigations leveraging public records, social media platforms, and open databases for intelligence gathering
- Applied cross-verification methodology using 3–5 independent sources per investigation to ensure attribution accuracy and minimize false positives
- Synthesized disparate data points into actionable intelligence reports following intelligence cycle methodology

Technical Skills

Security Specializations: DFIR, Penetration Testing, Vulnerability Assessment, OSINT, Threat Hunting, SecOps

Security Tools: Burp Suite, Nmap, Wireshark, Ghidra

DFIR & Analysis: Splunk, Autopsy, Volatility, Redline, KAPE, EZ Tools, FTK Imager, Log Analysis (Syslog, Auth.log, Apache/Nginx)

Operating Systems: Kali Linux, Ubuntu, Parrot OS, Windows Server, Active Directory, VMware Workstation

Programming Languages/Scripting: Python, Bash/Shell, C/C++, SQL, JavaScript, Solidity

Frameworks & Methodologies: MITRE ATT&CK, OWASP Top 10, Kill Chain, NIST Cybersecurity Framework, Incident Response Lifecycle, Cyber Kill Chain

Tools & Technologies: Git/GitHub, Docker, Virtualization, Firewalls, IDS/IPS

Competitive Achievements

- **Hack The Box University CTF 2025:** Ranked **Top 200 globally** and **Top 5 in India** among 5,000+ participating teams (3-member team)
- **TryHackMe Industrial Intrusion:** Achieved **Top 5% globally** in advanced industrial control systems (ICS) security challenge competing against international cybersecurity professionals and students
- **AICTE National Ethical Hacking Hackathon:** Competed in comprehensive multi-domain challenges across Linux, Windows, cloud security, and network exploitation

Certifications & Training

- **Google Cybersecurity Professional Certificate:** In Progress – Comprehensive training in network security, incident response, threat detection, and security operations
- **TryHackMe – Cyber Security 101:** Foundational cybersecurity principles and practical skills
- **PortSwigger Web Security Academy:** 60+ completed labs in web application security testing

Leadership & Communication

- **NITSHACKS 8.0 Host:** Hosted opening and closing ceremonies for North-East India's largest technical hackathon with 3,000+ participants
- **Team Leadership:** Led and coordinated 3-member teams during high-pressure CTF competitions, managing task delegation, time optimization, and team collaboration
- **Technical Communication:** Developed documentation and technical write-ups for security findings, demonstrating ability to translate complex vulnerabilities into actionable insights for diverse audiences