Bornov Shyam Kalita

+91-7576909883 | bornovofficial@gmail.com | LinkedIn | https://wizardbornov.github.io/Portfolio/

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. Knowledgeable in ISO 27001 standards through Google Cybersecurity Professional Certificate. Seeking investigative security roles combining threat actor behavior analysis with defensive detection and incident response.

EDUCATION

B.Tech in Electronics & Communication Engineering, National Institute of Technology Silchar Silchar, India 2024-2028

CGPA: 8.6 / 10

Senior Secondary (Class XII), Spring Dale International School (CBSE) May 2024

Awarded Student of the Year

TECHNICAL EXPERIENCE

Penetration Tester & DFIR Analyst, April 2025 — Present

- 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, lateral movement, and network traffic analysis using Wireshark to identify malicious traffic patterns and establish persistent access
- Performed blue team incident response, leveraging SIEM (Splunk) to analyze 100+ authentication, system, and web server log events alongside native Linux tools.
- Applied Microsoft Defender XDR and Defender for Cloud workload protections in lab environments to detect and remediate cloud and on-premises threats
- 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, August 2025 — Present

- 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, November 2025 — Present

- 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

LEADERSHIP & COMMUNICATION

Host, NITSHACKS 8.0 NIT Silchar Jan 2025

- Hosted opening and closing ceremonies for North-East India’s largest technical hackathon with 3,000+ participants.

CTF Player,

- Led and coordinated 3-member teams during high-pressure CTF competitions, managing task delegation, time optimization, and team collaboration.
- Developed documentation and technical write-ups for security findings, translating complex vulnerabilities into actionable insights for diverse audiences.

CERTIFICATIONS & TRAINING

Google Cybersecurity Professional Certificate, Google

In Progress – Comprehensive training in network security, incident response, threat detection, security operations, and risk assessment concepts

TryHackMe – Cyber Security 101, TryHackMe

PortSwigger Web Security Academy, PortSwigger

60+ completed labs in web application security testing

Microsoft Certified: Security Operations Analyst Associate, Microsoft

Investigate, search for, and mitigate threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender.

TryHackMe – SOC Level 1, TryHackMe

In progress – hands-on labs and exercises covering SOC operations, monitoring, and incident response

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