Motiranjan Barik
Bengaluru, India
Phone: +91 98274 14805
Email: motiranjan.barik@aol.com
LinkedIn: linkedin.com/in/motiranjan-barik-72ab60155
Portfolio: sudoxploit.github.io

Career Objective

Passionate and detail-oriented cybersecurity professional with a Bachelor's in Information Technology & Management and hands-on internship experience in red teaming, network security, and VAPT. Skilled in identifying vulnerabilities, exploiting flaws, and delivering actionable remediation plans. Seeking a Red Team or Penetration Testing role to help strengthen and safeguard enterprise infrastructure.

Education

Bachelor of Information Technology & Management
Ravenshaw University, Cuttack
Completed: 2021

Internship Experience

Cybersecurity Intern (VAPT & Red Teaming)
CyberSapiens LLP | June 2024 – January 2025

- Performed penetration tests on networks, web applications, and APIs using tools such as Nmap, Nessus, Metasploit, and Burp Suite
- Conducted vulnerability assessments using both automated scanners and manual testing techniques
- Executed password attacks (brute-force, dictionary, credential stuffing)
- Analyzed network traffic using Wireshark and sniffing tools to detect anomalies
- Performed mobile application security testing for Android and iOS platforms
- Participated in firewall and router security audits and testing
- Documented technical reports outlining vulnerabilities, impact, and mitigation strategies

Technical Skills

Offensive Security & Penetration Testing

- Network & Web Application Pentesting (OWASP Top 10)
- API Security Testing
- Mobile Application Pentesting (Android & iOS)
- Password Attacks: Brute-force, Dictionary, Credential Stuffing
- Post-Exploitation: Persistence, Privilege Escalation
- Pentesting Protocols/Services: FTP, SSH, SMB, RDP, Telnet, SMTP, DNS, DHCP

Network Security & Assessment

- Vulnerability Assessment & Exploitation
- Firewall Ruleset Review
- Router, Switch & Wireless Security Testing
- Packet Sniffing & Traffic Analysis
- DoS & MITM Simulation

Tools & Frameworks

- Recon & Scanning: Nmap, Masscan, ZMap, Fierce, DNSenum
- Vulnerability Scanning: Nessus, Qualys, OpenVAS
- Web/API Testing: Burp Suite, Postman, Nikto, SQLmap
- Password Cracking: Hydra, Medusa, John the Ripper, Hashcat
- Wireless Attacks: Aircrack-ng
- Exploitation: Metasploit, Responder
- Traffic Analysis: Wireshark

Operating Systems & Scripting

- Windows & Linux Security
- Basic Bash & PowerShell Scripting

Key Projects

API Penetration Testing

- Offensive security testing of REST APIs focusing on auth bypass, data exposure, and rate-limiting issues

Mobile Application Security Testing

- Security assessment of Android & iOS apps targeting insecure storage, permissions, and runtime behaviors

Network Vulnerability Assessment

- Conducted vulnerability scanning, validation, and exploitation in a simulated enterprise environment

---

Certifications & Training

- CompTIA Security+
- GIAC Penetration Tester (GPEN)
- OSINT & Threat Intelligence Essentials
- Mobile Application Security Testing Training
- Certified Ethical Hacker (CEH) – *Pursuing/Recommended*
- Offensive Security Certified Professional (OSCP) – *Recommended*

Core Competencies

- Time Management
- Communication & Collaboration
- Adaptability & Learning Agility
- Problem Solving
- Patience under Pressure

Languages

- English
- Hindi
- Odia
