Debangshu Roy

debang5hu.github.io | roydebangshu22@gmail.com | West Bengal, India

Objective

Experienced in network, web application (API-focused) and Active Directory penetration testing with hands-on-skills developed through solving Hack The Box ,developing CTF challenges and bug hunting. Proficient in automating workflows with Python and Bash, and possesses foundational knowledge of Docker security.

Technical Skills

- **Penetration Testing & Security Assessment:** Vulnerability Assessment & Penetration Testing (VAPT), Network Penetration Testing, Web Application Penetration Testing, API Security Testing, Active Directory Penetration Testing, OWASP Top 10
- **Compliance & Security Standards:** PCI DSS, HIPAA, ISO 27001, OWASP
- **Programming & Scripting Languages:** Python, C++, Bash
- **Operating Systems & Platforms:** Linux, Windows, Docker
- **Databases & Version Control:** MySQL, MariaDB, Git, GitHub
- **Tools & Frameworks:** Flask, Nmap, OpenVAS, Burp Suite, BloodHound, Metasploit, Wireshark, Postman

Education

B.Tech in Computer Science Engineering (2022 -2026)
Sister Nivedita University (CGPA: 7.9)

Techno India Group Public School (2020 - 2022)
Senior School Certificate Examination (Percentage: 85.4%)

Experience

ZeroDay Alliance – CTF developer
Aug 2024 - Jul 2025

- Designed and developed Capture The Flag (CTF) challenges focused on web, network penetration testing, and binary exploitation. Contributed to knowledge sharing by publishing detailed write-up.

Projects

Keylogger

- Developed a keylogger using Python 3 to capture keystrokes and collect unique clipboard data.
- Implemented periodic data exfiltration to an attacker's account for covert communication.
- Ensured persistence by scheduling execution on system reboot using cron jobs.

Wushi

- Developed honeypot services simulating HTTP (HTTPS) and SSH protocols by implementing an HTTP honeypot using Flask to capture client IPs, user agents, and login attempts with bot deterrence like CAPTCHA, along with an SSH honeypot built on Paramiko that logs login attempts and provides a restricted "jailed" shell environment for authenticated users.
- Enabled concurrent operation and coordination of both honeypots through a Golang based server with activity logging.

Certifications

- Microsoft Certified: Security, Compliance, and Identity Fundamentals
- FullHouse - Hack The Box