BISWADEB MUKHERJEE

Offensive Security Engineer

admin@official-biswadeb941.in · official-biswadeb941.in · github.com/Mr-Biswadeb-Mukherjee

linkedin.com/in/biswadeb-mukherjee

SUMMARY

Independent Offensive security researcher with 6+ years in custom tooling, adversary simulation and large-scale phishing infrastructure analysis, and producing actionable threat intelligence.

RESEARCH EXPERIENCE

Independent Security Researcher 2021 – Present

- Built Go-based domain intelligence system → **330K+ domains analyzed, 12K+ active infrastructure identified** (DOI published)
- Mapped phishing-as-a-service ecosystem targeting Indian government portals (CERT-IN Acknowledged)
- Built Hash-Based tamper proof logging attachable module in Nodejs, Golang
- Built adversary simulation web app in Flask → **validated OWASP vulnerabilities via real attack scenarios**

Technical Contributor & Mentor IEEE-IC Standard Hackathon, IEEE India · Dec 2024

- Co-developed FlowGuard (IDS/IPS benchmarking platform) → **Top 5, IEEE-IC Hackathon 2024**
- Automated API integrations in Python → **reduced benchmarking time by 30 hours/month**
- Achieved **Top 5 nationally** in IEEE-IC cybersecurity hackathon

RESEARCH & PUBLICATIONS

DIBs — Domain Intelligence & Behaviour Analysis Technical Whitepaper · 2026

DOI: 10.5281/zenodo.19432181

- Designed and executed a large-scale domain intelligence study: 500 brand keywords generated 330k+ domains, yielding 12k+ confirmed live infrastructure nodes. Published full reproducible dataset and methodology, built for independent replication.
- Revealed infrastructure concentration patterns across AWS, Cloudflare, and GCP that passive DNS monitoring would have missed. Demonstrated mutation-based proactive detection as a superior methodology.
- Automated DNS intelligence which reduced manual intervention time by several hours.

Passive Forensic Analysis of PAN & Aadhaar Portals Case ID: BM-PaaS-2026-001 · Jan 2026

github.com/Mr-Biswadeb-Mukherjee/CASE-ID-BM-PaaS-2026-001

- Identified a live Phishing-as-a-Service ecosystem across 8 domains impersonating Indian government identity portals. Mapped a tiered monetisation structure with retailer, distributor, and white-label tiers.

- Produced a forensic investigation with cryptographically signed evidence repository and full regulatory mapping. Acknowledged by CERT-In under two separate reference IDs.

TOOLS

DIBs — Domain Intelligence & Behaviour System Nov 2025 – Present

github.com/Mr-Biswadeb-Mukherjee/DIBs

- Built Go-based DNS intelligence pipeline → **330K+ domains analyzed, phishing detection via typosquatting/bitsquatting/homograph techniques**
- Automated large-scale analysis with Redis-backed concurrency → **high-throughput processing, reduced manual effort significantly**
- Applied ASN clustering and cloud correlation → **uncovered hidden infrastructure patterns, SIEM-ready telemetry pipeline for threat intel ingestion**

Linux C2 Framework 2025 – Present

Github: redacted

- Built research-grade C2 framework for Linux → **simulated persistence and post-exploitation workflows**
- Used as adversary simulation platform → **modeled and documented real attacker tradecraft**
- Extended for cross-platform capability → **Windows port in progress**

Incognito Vault — Hardened Web Application & Red Team Target August 2024 – June 2025

- Built and hardened Flask application against **SQLi, XSS, CSRF, session hijacking, and brute force attacks**
- Actively red-teamed the application → **validated defenses under real attack scenarios and iterated improvements**

FlowGuard — IDS/IPS Benchmarking Platform Dec 2024

- Built CLI-based IDS/IPS benchmarking platform with **real-time plotting and multi-engine threat simulation**
- Deployed on VPS for **continuous monitoring and evaluation at scale**
- Achieved **Top 5 nationally** at IEEE-IC Standard Hackathon

COMPETENCIES

Red Team / Offensive Security	Red Team Operations, Adversary Simulation, Penetration Testing, Privilege Escalation, Post-Exploitation
Malware Research	Malware Development (PE/ELF), C2 Design, Exploit Development, AV/EDR Evasion
Threat Intel & Forensics	OSINT & Reconnaissance, DNS Analysis
Engineering	Go, Python, Offensive Automation

CREDENTIALS

Certified Ethical Hacker (CEH) In Progress

BCA — Guru Nanak Institute of Technology, Kolkata

ISC / ICSE — St. Xavier's Institution