Mohnish Shende

OSINT RESEARCHER | CYBERSECURITY ANALYST

+91 7020172261 · mohnish@mohnish.ink · mohnish.ink · GitHub · Nagpur, Maharashtra, India · Indian

Cybersecurity and OSINT researcher with experience in vulnerability assessment, Linux infrastructure, security analysis, intelligence-style research, and independent interdisciplinary research. Experienced with Nessus, Burp Suite, Nmap, Python security tooling, Docker-based infrastructure, and self-hosted systems. MSc Cyber Security graduate from an NCSC-certified degree programme with peer-reviewed research experience. Research work spans cybersecurity, forensic psychology, intelligence analysis, political psychology, influence systems, and structured evidence assessment. Experienced in source verification, evidence evaluation, qualitative document analysis, comparative case analysis, construct operationalization, framework development, and communicating uncertainty in technical and research reporting

EXPERIENCE

Project Associate I
12/2024 – 03/2025

CSIR National Environmental Engineering Research Institute (CSIR-NEERI) — Nagpur, Maharashtra, India

- Assessed internal research networks for vulnerabilities using Nessus and Burp Suite
- Supported network segmentation, access-control configuration, and Linux privilege management
- Documented network baselines, secure-configuration practices, and system-hardening measures
- Produced technical reports and conducted OSINT-based research using SearXNG and other research tools

EDUCATION

MSc Cyber Security, Merit
09/2023 – 09/2024

University of Plymouth — United Kingdom

- National Cyber Security Centre (NCSC)-certified degree programme

Bachelor of Engineering (B.E.) in Information Technology, Distinction
02/2018 – 07/2022

St. Vincent Pallotti College of Engineering and Technology

SKILLS

- Cybersecurity: Nmap · Nessus · Burp Suite · Vulnerability Assessment · Security Reconnaissance · OSINT · Passive Reconnaissance · Command Allowlisting · Scan-Result Analysis

SKILLS

— Systems & Infrastructure: Linux · Debian · Ubuntu · Docker · Docker Compose · Caddy · Pi-hole · Unbound · Tailscale · Samba · SSH · fabric · systemd · Self-Hosted Infrastructure · Internal DNS · Reverse Proxying

— Development & Data: Python · Flask · REST APIs · XML · JSON · Markdown · requests · xmltodict · tracemalloc · Ollama · Local LLM Integration

— Research & Intelligence Analysis: OSINT Research · Source Verification · Evidence Evaluation · Source Triangulation · Confidence Assessment · Chronology Reconstruction · Qualitative Document Analysis · Comparative Case Analysis · Process Tracing · Mechanism Coding · Construct Operationalization · Framework Development · Structured Evidence Assessment · Research Writing · Technical Reporting

PROJECTS

NodeZero — Self-Hosted Homelab Infrastructure

https://github.com/MohnishShende/NodeZero-A-complete-homelab-document

A reproducible self-hosted infrastructure environment designed around Linux, Docker, internal DNS, HTTPS, remote access, monitoring, backup, and recovery

- Built and operated a Docker-based self-hosted infrastructure environment
- Implemented internal DNS using Pi-hole and Unbound
- Implemented internal HTTPS and reverse-proxy services using Caddy
- Configured remote access through Tailscale and network file sharing through Samba
- Integrated monitoring through Uptime Kuma and containerized application services
- Documented system architecture, networking, DNS/HTTPS configuration, security controls, services, backups, recovery procedures, and operational runbooks
- Maintained rebuild-from-zero documentation to support reproducibility and disaster recovery

Nmap LLM — AI-Assisted Network Scanner and Triage Tool

https://github.com/MohnishShende/nmap-llm

Python-based security tool integrating Nmap with a locally hosted LLM through Ollama

- Converts natural language scanning requests into controlled Nmap commands using a local LLM
- Implements command allowlisting and checks for disallowed operations before execution
- Supports explicit scan execution and structured processing of Nmap results
- Parses Nmap XML output into structured JSON and Markdown reports
- Designed for offline/local operation without dependence on cloud-hosted LLM services
- Developed in Python using Ollama/Mistral and structured scan-result processing

PROJECTS

NIA OSINT Security Reconnaissance Dossier

Independent security reconnaissance assessment of nia.gov.in submitted to CERT-In

- Conducted OSINT and externally observable security reconnaissance of public-facing infrastructure
- Documented service exposure, web metadata, Drupal version disclosure, installation-path information, authentication portal and resource structures, publicly accessible files, analytics exposure, and HTTP security-header configuration
- Classified findings by evidence, severity, potential risk, positive security controls, and remediation
- Produced a structured technical dossier separating observations from interpretation and recommendations
- Submitted findings to CERT-In and received a response

ECI EVM Engineering Assurance Assessment

https://github.com/MohnishShende/ECI-EVM-Engineering-Assurance

Engineering assessment using evidence analysis on Indian Electronic Voting Machines claims

- Extracted and normalized technical claims from source material
- Developed traceability between claims, evidence, and analytical conclusions
- Distinguished directly supported evidence from inference, uncertainty, and unsupported assertions
- Applied structured evidence evaluation to produce an auditable engineering-assurance framework

Somerton Man Research Dossier

Independent evidence-based investigation and long-form research dossier

- Conducted source analysis, claim verification, chronology reconstruction, and uncertainty assessment
- Classified sources and analytical conclusions by evidentiary strength and confidence
- Maintained a version-controlled research dossier designed to preserve traceability between evidence and conclusions

Identity-Based Identification Schemes

https://github.com/MohnishShende/IBI-schemes

Python implementation of identity-based identification and zero-knowledge authentication concepts

- Implemented educational demonstrations of EZKP, Fiat-Shamir, Sakai-Kasahara, TNCIBI, and TwinSchnorr-related schemes
- Developed Flask endpoints and supporting clients for protocol experimentation
- Used timing and memory measurements, including tracemalloc, for implementation analysis
- Developed as an educational/research implementation rather than a production authentication system

PUBLICATIONS

Psychological Appropriation: A Dimensional Model of Surrogate-Moral Violence — 12/2025

Published online 5 December 2025 — https://doi.org/10.1080/24732850.2025.2599908

Shende, M

LANGUAGES

English — *Native* Marathi — *Native* Hindi — *Native*

AWARDS

MSc Cyber Security, NCSC-Certified Degree Programme — Academic Year 2023–2024

FIND ME ONLINE

ORCID

orcid.org/0009-0000-9466-3056

Google Scholar

https://scholar.google.com/citations?user=Qu1HDUIAAAAJ&hl=en

ONGOING

Research Manuscripts / Working Papers

Shende, M. — "Covert Thought Reform: Adapting Classical Models Across Political, Cultural, and Organizational Contexts."

Shende, M. — "Subtle Affective Deficit Evaluation (SADE) Protocol: Theoretical Foundations, Validation, and Field-Ready Tools." (Ongoing research)

Shende, M. — "The Inescapable Chain: Human Nature, Exploitation, and the Illusion of Freedom."

Books

Shende, M. — The Operating Manual: Meditations on the Mind, Judgment, and Living Well