Reeti Agarwal

eWPT | eJPT | Cybersecurity Researcher | Penetration Tester | VAPT | AIML | CTF Player |

reeti05agarwal@gmail.com | linkedin.com/in/reeti-agarwal-cyber/ | github.com/Reeti05Agarwal |

reeti-agarwal-portfolio.vercel.app/

PROFESSIONAL SUMMARY

Cybersecurity engineering student (BTech CSE, Symbiosis Institute of Technology) with hands-on experience across offensive security, threat intelligence, digital forensics, and AI-driven defense systems. Certified eJPT penetration tester with real-world internship exposure to VAPT, dark web intelligence, SOC 2/GDPR compliance, and law enforcement digital forensics. CTF competitor with podium finishes at IIT Bombay and IIT Jammu. Passionate about building innovative security tools that bridge research and real-world impact.

TECHNICAL SKILLS

Offensive Security: Penetration Testing (Web/Network), VAPT, Privilege Escalation, Post-Exploitation, API Security, OSINT, Social Engineering, Cloud Security

Defensive & Forensics: Digital Forensics, SIEM, Threat Intelligence, Threat Detection. Network Security. Firewall. Cryptography, Cloud Security, MITRE ATT&CK framework

AI / ML Security: Threat Detection Models, Anomaly Detection, RAG, Data Analysis, Machine Learning, Knowledge Distillation, Differential Privacy

Languages: Python, Bash, PowerShell, Java, Rust, Go, C, C++, JavaScript, TypeScript

Frameworks & Stack: Apache Kafka, Elasticsearch, MySQL, MongoDB, PostgreSQL, React, NestJS, ExpressJS, NodeJS, Tailwind

Security Tools: Burp Suite, Nmap, Metasploit, Wireshark, Nessus, OWASP ZAP, Ghidra, Volatility, Zeek, Suricata, Splunk, Autopsy, Snort, SPIRE

Platforms & Infra: Docker, Xen Hypervisor, Ollama, N8N Workflows, GitHub, Cisco Packet Tracer, Linux, Windows, Kubernetes, Vagrant

ACHIEVEMENTS & COMPETITIONS

2nd Position in Women's CTF
IITB Trust Lab | *29th March 2025*

3rd Position in Operation Cipher Shadows
IIT Jammu | 11th April 2025

2nd Position in Cyber Security and Blockchain Hackathon
Cyber Secured India and India Blockchain Alliance | *15th-18th September 2023*

Quantum Computing Odyssey: Teleporting to the Realm of Unparalleled Possibilities
Research Paper Published in 2024 International Conference on ADICS

NPIIPC-AICTE Pentathon 2025
Rank: 500 out of 3500 | 5th-6th April 25

CyberShield Hackathon

MP Police

EXPERIENCE

Vice President - *Cyber Blockchain Club*
August 2024 - Present

- Lead the Cybersecurity and Blockchain wings of a 30+ member technical club as Vice President, overseeing technical direction, event planning, and member development.
- Designed and facilitated hands-on workshops on Linux, web penetration testing, network security tools, and blockchain, consistently improving members' practical skill levels.
- Organized and hosted internal CTF competitions, building a culture of applied security learning and fostering competitive problem-solving across the club.
- Mentored junior members on offensive and defensive security fundamentals, bridging the gap between academic theory and real-world practice.

AI Cyber Security Research Intern - *Deepcytes*
Feb 2025 - October 2025

- Conducted penetration testing engagements for clients, identifying and reporting critical vulnerabilities across web applications and network infrastructure.
- Researched AI-driven cyber threats and emerging attack vectors like ransomware.
- Investigated dark web forums and marketplaces to gather threat intelligence, tracking adversarial activity and surfacing actionable insights on cyber risks and compliance gaps.
- Conducted OSINT investigations to profile threat actors, map digital footprints, and support intelligence-led cybercrime analysis.
- Built and automated a RAG (Retrieval-Augmented Generation) pipeline using N8N workflows, streamlining threat intelligence aggregation and enabling faster, context-aware security research

Web Security Research Intern - *Rosche System*
Feb 2025 - June 2025

- Conducted structured vulnerability research on OWASP Top 10 attack vectors, including SQL injection, XSS, IDOR, authentication bypasses, and server misconfigurations to strengthen client application security posture.
- Analyzed web application architectures to identify weaknesses in input validation, session management, and access controls, providing detailed technical findings and remediation recommendations.
- Studied and applied cybersecurity governance frameworks including SOC 2, GDPR, and HIPAA and contributed to internal compliance documentation and control gap assessments.
- Gained practical exposure to security policy development and regulatory compliance initiatives within an enterprise security environment.

Intern - *Cyber Crime Department, Indore*
16 Dec - 24 Dec 2024

- Observed live cybercrime investigations into phishing campaigns, QR code scams, and WhatsApp-based social engineering attacks under supervising investigators.
- Analyzed 10+ active cases using digital forensics tools and social media tracking techniques, contributing findings to cybercrime prevention and case documentation efforts.
- Gained exposure to evidence preservation protocols, chain of custody procedures, and forensic analysis methodologies used in law enforcement investigations.

Network Security Intern - *Cisco Virtual Internship*
May - July 2024

- Completed intensive training in TCP/IP networking fundamentals, routing protocols, VPN configuration, and cybersecurity principles through Cisco's learning platform.

- Designed and validated secure multi-layer network topologies incorporating firewall rules, VLAN segmentation, and device hardening configurations.
- Practiced real-world troubleshooting of network device failures, configuration errors, and security misconfigurations using Cisco Packet Tracer simulations.
- Developed foundational knowledge of network security architecture principles applicable to enterprise environments.

Intern - *Cyber Secured India*

2023

- Gained practical experience in core cybersecurity domains including system security, network security, and Linux fundamentals through structured labs and real-world simulations.
- Applied both offensive and defensive security techniques that covered threat modeling, vulnerability identification, attack simulation, and mitigation strategies.
- Completed hands-on exercises in penetration testing methodology, security hardening, and incident response fundamentals, reinforcing theoretical concepts with practical application.

PROJECTS

Maya: Autonomous Decoy Networks for Adversarial Behavior Analysis

- Architected a CRDT-synchronized distributed deception platform that maintains persistent attacker sessions across isolated honeypots, creating seamless adversarial containment
- Implemented multi-tier decoy engagement (low/medium/high interaction) with RL-driven adaptation based on real-time threat actor fingerprinting and clustering
- Achieved zero false-positive detection by design, instrumenting all commands, file access, and lateral movement with MITRE ATT&CK TTP mapping
- Target metrics: <10 min time-to-detection (vs. 10-day industry average), 300–500% increase in attacker dwell time, and <50ms redirection latency

NexGuard

- Delivered real-time fraud detection (0.908 AUC, 87.3% accuracy) and churn prediction (0.897 AUC) using knowledge-distilled TabNet models on AWS serverless stack
- Secured pipeline with AES-256/TLS 2.0 encryption, zero-trust architecture, and differential privacy; integrated LIME for regulatory-compliant explainability
- Optimized for cost-efficiency: leveraged AWS free tier (750 hrs RDS, 1M Lambda requests, 5GB S3) to support 100K+ MAU authentication via Cognito

TraceProbe

- Built a scalable streaming analytics engine on Apache Kafka + Elasticsearch + Docker, ingesting and normalizing millions of raw IPDR records across 3+ formats (CSV/JSON/XML) for real-time digital forensics
- Developed Python-based threat enrichment modules performing geolocation lookups, reverse DNS validation, TTL/hop-count anomaly detection, and blacklist correlation to surface hidden criminal networks
- Delivered Kibana investigative dashboards with geo-mapping of A↔B Party communications, session heatmaps, and top protocol/domain analysis, accelerating cybercrime anomaly detection
- Hardened platform with TLS-in-transit, role-based access control, index-level field security, and immutable audit trails to meet law enforcement evidence-handling and privacy standards

Network Intrusion System

- Developed a 4-layer system architecture (Collection, Processing, Storage, Visualization) using Java, Pcap4J, MySQL, and JavaFX, capturing live traffic with real-time protocol categorization (TCP, UDP, HTTP) and deep packet inspection

- Engineered an AI anomaly detection engine with firewall/blacklist validation to flag 200+ daily suspicious packets, detecting zero-day threats alongside signature-based patterns and reducing security incidents by 15%
- Modeled a comprehensive relational database schema with PK/FK constraints across 12+ entities (Packets, Anomalies, Network Devices, Bandwidth, Latency Logs), applying Codd's relational rules to ensure data integrity and sub-second query performance
- Delivered interactive JavaFX dashboards displaying bandwidth trends, protocol distribution, and real-time security alerts, while supporting multi-format report export and RBAC authentication for forensic teams

EDUCATION

BTech in Computer Science & Engineering

Symbiosis Institute of Technology, Pune | 2023-27

CERTIFICATIONS

Web Application Penetration Tester (eWPT) - INE Security

Junior Penetration Tester (eJPT) - INE Security

Google Cybersecurity Professional Certificate - Coursera

Cisco Cybersecurity Course

OPSWAT Academy Certifications