Bhushan Ladgaonkar

+91 9152963095 | bhushanladgaonkar@gmail.com | LinkedIn | github.com/beeth73

Professional Summary

Security Researcher and Machine Learning Engineer specializing in **Adversarial AI** and **Offensive Security**. Proven experience in engineering ML-based Network Intrusion Detection Systems (NIDS) for enterprise infrastructure and researching autonomous decision-making agents using Reinforcement Learning. Seeking to leverage expertise in simulation, modeling, and security architectures.

Education

Fr. Conceicao Rodrigues College of Engineering Mumbai, India
Bachelor of Technology (B.Tech) in Computer Engineering *Expected May 2028*

Experience

Oil and Natural Gas Corporation (ONGC) Mumbai, India
Summer Intern | Database & Security Group *May 2025 – June 2025*

- Developed a prototype NIDS using the UNSW-NB15 dataset to demonstrate ML capabilities for threat detection **Network Intrusion Detection System (NIDS)** to identify zero-day threats and malicious traffic patterns, addressing specific limitations in traditional signature-based detection.
- Optimized data pipelines for the **UNSW-NB15 dataset** (2M+ records), performing advanced feature engineering to enhance model accuracy for enterprise-grade network traffic.
- Implemented and evaluated **Random Forest** and **XGBoost** algorithms, successfully reducing false positive rates while maintaining high detection sensitivity for anomalous packets.
- Collaborated with the Database Group to document threat detection methodologies, bridging the gap between raw data analysis and actionable security intelligence.

Technical Projects

MendikotZero: AI Agent for Complex Trick-Taking Card Game | *Python, PyTorch, RL* Oct 2025

- Architected a Reinforcement Learning agent capable of strategic decision-making in imperfect-information environments using the **AlphaZero architecture**.
- Implemented **Monte Carlo Tree Search (MCTS)** guided by a Dual-Head Neural Network (Policy & Value) to simulate future game states and optimize move selection.
- Designed a **Self-Play** training loop where the agent evolved strategies from random noise to advanced probability-based gameplay without human data input.

Technical Skills

Languages: Python, C, SQL, Java
AI & Simulation: Machine Learning, Reinforcement Learning, MCTS, PyTorch, Scikit-learn, Pandas, XGBoost
Security: Network Intrusion Detection (NIDS), Offensive Security, OSINT, Linux (Kali/Ubuntu), Reconnaissance
Developer Tools: Git, GitHub, VS Code, Jupyter Notebooks

Certifications

Offensive Security Operations – Cybrary
Open Source Intelligence (OSINT) – Cybrary
Cyber Kill Chain – Cybrary