Red Team vs Blue Team: AI Simulation for Cybersecurity Defense

By Modi Nitya & Malde Roshni
Internship: Digisuraksha Parhari Foundation
Powered by Infinisec Technologies Pvt. Ltd.

Github Links:
https://github.com/Roshni1603/Red-vs-Blue-AI-Simulation.git
https://github.com/nityamodi0810/Red_Blue_AI_Simulate.git

Introduction

- Red vs Blue Teaming:
- Red Team: Simulates attackers to test vulnerabilities.
- Blue Team: Defends systems by detecting and responding to threats.
- AI Simulation:
- Using AI to create virtual environments that mimic real-world scenarios for training, testing, and improving models.
- AI can help automate attack and defense strategies.

Problem Statement

- Increasing frequency of cyber attacks
- Manual Red vs Blue exercises lack scalability and consistency.
- Need for automated, ethical, and safe testing environments.
- Difficulty in modeling AI-driven cyberattacks and defenses.

Solution

- Red Team agent simulates offensive actions across common services (HTTP, FTP, SSH).
- Blue Team agent monitors, detects, and responds to threats using predefined logic.
- Logs and system alerts are generated for analysis and evaluation.
- Supports cybersecurity education, enterprise training, and strategic planning.

Objective

- Build an AI-based simulation of Red (attacker) vs Blue (defender)
- Provide a scalable, ethical training ground for cybersecurity.
- Track and evaluate performance metrics (detection, compromise rate).

Architecture Overview

- Red Agent ↔ Environment ↔ Blue Agent
- Interaction loop between agents and environment
- Virtual hosts simulate SSH, HTTP, FTP services.
- Each step logs system status and alerts.

Code & Tool Breakdown

Programming Language: Python

Key Files:

- red_team_agent.py – Implements offensive logic for simulating attacks
- blue_team_agent.py – Handles defensive strategies and monitors system activity
- environment.py – Controls the simulation environment and coordinates agent actions

Libraries Used:

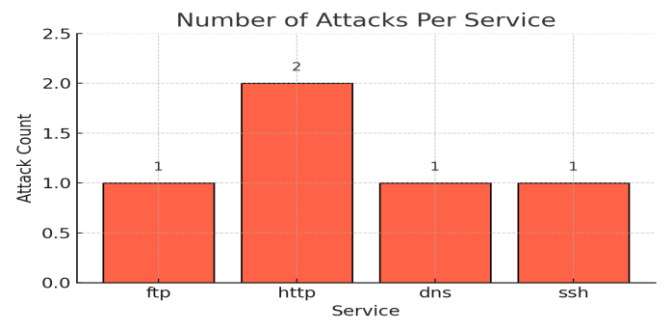
- random – For generating unpredictable behavior in simulations
- os: Provides functions to interact with the operating system
- sys: Provides access to system-specific parameters and functions

Output:

- Logs – Record each action taken by agents
- Alerts – Notify about detected attacks or anomalies
- System Status – Provides snapshot of the network during simulation

Results & Observations

- Chart: Number of Attacks Per Service



- - HTTP had the highest number of attacks (2)
- - FTP, DNS, and SSH each had 1
- - Suggests HTTP is more vulnerable or targeted

Real-World Use Cases

Cybersecurity Training Environments

- Used by enterprises, military, and academia for safe cyber defense training.

Red & Blue Team Operations

- Your AI system can automate this model for consistent and scalable testing.

Educational Platforms

- Your project fits perfectly in learning environments and cyber bootcamps.

Future Enhancements

- **Smarter AI**: Add reinforcement learning for adaptive attack/defense.
- **Real Tools**: Integrate Metasploit, Snort, Wireshark,Kali.
- **Larger Networks**: Use Docker/GNS3 for scalable setups.
- **Live Dashboards**: Visualize attacks/defense with Grafana & Streamlit.
- **Educational Mode**: Add Purple Team & learning competitions.

Conclusion

- Showcased realistic cyber scenarios
- Scalable and ethical AI-based simulation.
- Effective for training and strategy testing.
- Contributes to adaptive cybersecurity systems.

THANK YOU!!!