NeuralTrace
Overview

NeuralTrace is a production-ready network forensic tool for red team operations, powered by xAI's Grok 3 with Retrieval-Augmented Generation (RAG). It performs real-time anomaly detection, intrusion analysis, and OSINT attribution using live packet capture, Zeek logs, and real APIs (xAI, WhoisXML, Bright Data). Designed for enterprise-grade engagements, it maps to MITRE ATT&CK T1071.001 and supports authorized penetration testing.
Features

```
Live Packet Capture: Scapy/Libpcap with Zeek log generation.
RAG Pipeline: FAISS/LlamaIndex for telemetry indexing.
Anomaly Detection: SVM and Grok 3, trained on CICIDS-2017/UNSW-NB15.
OSINT Attribution: X API and WhoisXML via Bright Data proxies.
Log Correlation: FastAPI routes with AWS S3 backups.
Real-Time Dashboard: Streamlit for visualization.
CLI Interface: Simple commands for analysis.
Stealth: Tor and Bright Data proxies.
```

Installation
Prerequisites

```
Ubuntu/Debian
Python 3.9+
PostgreSQL, Tor, Libpcap, Zeek
GPU (24GB VRAM)
API Keys: xAI, X API, WhoisXML, Bright Data
AWS S3 credentials
CICIDS-2017/UNSW-NB15 datasets (/data/cicids2017.csv)
```

Single Command
bash
sudo apt update && sudo apt install -y git && git clone https://github.com/sunnythakur25/neuraltrace.git && cd neuraltrace && bash setup.sh
Manual Setup

```
Clone repository:
bash
```

git clone https://github.com/sunnythakur25/neuraltrace.git
cd neuraltrace
Install dependencies:

bash
sudo apt install -y python3 python3-pip postgresql postgresql-contrib tor libpcap-dev zeek
pip3 install -r requirements.txt
Set up PostgreSQL:
bash
sudo -u postgres psql -c "CREATE DATABASE neuraltrace;"
sudo -u postgres psql -c "CREATE USER neuraltrace WITH PASSWORD 'securepass';"
sudo -u postgres psql -c "GRANT ALL PRIVILEGES ON DATABASE neuraltrace TO neuraltrace;"
Configure Zeek:
bash
sudo zeekctl install
sudo zeekctl deploy
Configure .env with API keys and AWS credentials.
Run setup:
bash

```
bash setup.sh
```

Usage
CLI

Run analysis:
bash
python3 -m neuraltrace.cli --interface eth0 --count 10 --x-handle target_handle

Options:

```
--interface: Network interface (required).
--count: Packet count (default: 100).
--x-handle: X username (optional).
--init-db: Initialize database.
--report: Report file (default: neuraltrace_report.jsonl).
```

Dashboard
bash
streamlit run neuraltrace/dashboard.py
API
bash
uvicorn neuraltrace.api.log_correlator:app --host 0.0.0.0 --port 8000

Endpoints:

```
GET /logs/{data_type}: Retrieve logs.
POST /analyze: Analyze packet (placeholder).
```

Example Output

text

```
2025-05-26 10:45:23 - INFO - Captured 10 packets
2025-05-26 10:45:24 - INFO - Analyzed packet: {'anomaly_score': 0.89, 'attack_type': 'C2'}
2025-05-26 10:45:25 - INFO - Report saved to neuraltrace_report.jsonl and S3
```

Testing

```
Sandbox: AWS EC2 (g4dn.xlarge, ~$0.526/hour).
Traffic: CICIDS-2017, UNSW-NB15, or authorized enterprise traffic.
Metrics: Accuracy (>90%), false positives (<5%), latency (<1s).
Compliance: Audit logs (neuraltrace.log) and S3 backups.
```

Security

```
Red Team Only: Authorized use only (CFAA/GDPR compliance).
API Security: Store keys in .env and config.json.enc.
Proxies: Use Bright Data residential proxies.
Data Privacy: GDPR/CCPA compliance.
```

Contributing

```
Fork repository.
Create branch: git checkout -b feature/new-detection.
Test in sandbox with real traffic.
Submit pull request.
```

License

MIT License. See LICENSE.

Acknowledgments

Sunny thakur

xAI Grok 3

CICIDS-2017, UNSW-NB15 datasets

Nexphisher inspiration