ADVANCED INTRUSION DETECTION SYSTEM (IDS) USING DEEP LEARNING

PRESENTED BY:

TEAM NETWORK NEXUS
JIVANT L
MANO VARSHA S
VISHAAL T D

CareerTiQ

PROBLEM STATEMENT

Modern networks face complex challenges in cybersecurity, from the difficulty of detecting and responding to threats in real-time to the need for accurate threat assessment amid increasingly sophisticated attacks, all while maintaining comprehensive monitoring capabilities that can establish baseline behaviors and minimize false positives while tracking attack origins.

USE CASES

- Network security montioring
- Security Incident Detection
- Service Baseline Learning
- Threat score analysis
- Early warning system

PROPOSED SOLUTION

- Network Packet Monitoring
- Malicious Packet Detection
- Threat Alerts
- Traffic Statistics and Monitoring
- Sound Feature for Alerts

WORKFLOW

- **Initialization** - Program begins with enhanced startup animations
- **Packet Sniffing** - Scapy is used to capture real-time network packets
- **Packet Analysis** - source and destination IPs, protocol, and payload are extracted
- **Classification** - Based on the analysis, the packet is classified as normal traffic & malicious traffic
- **Threat Alerts** - If a packet is classified as malicious, an alert is added to the system

TECHNICAL STACK

CareerTiQ

★ **Programming Language**

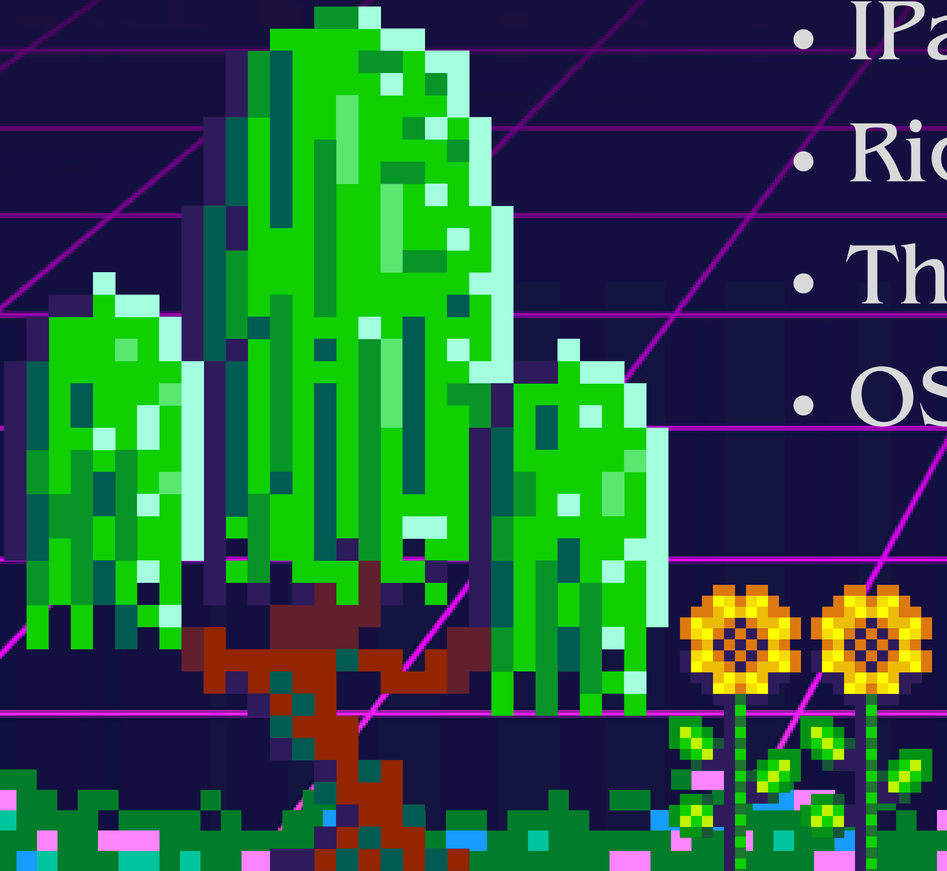
- Python 3.x

★ **Libraries:**

- Scapy
- IPaddress
- Rich
- Threading
- OS

★ **Operating System**

- Kali Linux - requires root privileges



CareerTiQ

SUGGESTIONS FOR FUTURE ENHANCEMENT?

CareerTiQ

THANK YOU

EXIT