**Threat Eye (v0.1)**

By - **Rajat Kundu**

Release Date: **26.02.2025**

Threat Eye (v0.1) – A Comprehensive Network Security Scanner for Kali Linux

Threat Eye is an advanced network scanning and security monitoring tool built for Kali Linux, designed to detect and respond to network anomalies, unauthorized device connections, and Man-in-the-Middle (MITM) attacks in real time. With a strong emphasis on automated detection, alerting, and mitigation, Threat Eye enhances network security by actively monitoring network traffic and providing instant threat intelligence via Telegram and email notifications.

This tool is designed for cybersecurity professionals, ethical hackers, penetration testers, and network administrators, helping them analyze, detect, and mitigate various types of network threats. It combines real-time packet analysis, an interactive GUI-based dashboard, and automated response mechanisms to offer a holistic cybersecurity solution for network protection.

* **Key Features :**

**1. Network Anomaly Detection**

Threat Eye continuously monitors network traffic and detects suspicious behavior, such as unusual packet size variations, unexpected spikes in data transmission, and unauthorized access attempts. It helps identify potential intrusions, malware infections, and network breaches before they cause harm.

**2. Unauthorized Device Detection & Blocking**

Any new or unauthorized device connecting to the network is immediately detected. Threat Eye provides the option to automatically block these devices, ensuring only whitelisted or authenticated devices can access the network.

**3. Man-in-the-Middle (MITM) Attack Detection**

MITM attacks are one of the most dangerous threats to network security, allowing attackers to intercept, alter, or steal sensitive data. Threat Eye can detect MITM attempts such as ARP spoofing, DNS spoofing, and SSL stripping and immediately notify the user while taking necessary countermeasures.

**4. Real-Time Alerts via Telegram & Email**

Whenever a network anomaly, unauthorized device, or MITM attack is detected, Threat Eye sends an immediate alert through:  
✅ **Telegram bot (threat\_eye) –** Instant notification on a dedicated Telegram account.  
**✅ Email Alerts –** Detailed security alerts sent to the configured email address.

These instant notifications allow users to take action promptly, minimizing potential security risks.

**5. GUI-Based Dashboard for Easy Monitoring**

Threat Eye comes with an interactive, user-friendly web dashboard hosted on localhost, making network security monitoring simple and efficient. The dashboard includes:  
**🔹 User Authentication System –** Secure sign-up & login functionality for users.  
**🔹 Real-Time Graphs –** Displays network packet data (packet size vs. time) for deep traffic analysis.  
**🔹 Unauthorized Devices Section –** Lists all unknown devices detected and blocked.  
**🔹 MITM Detection Panel –** Displays ongoingMITM attacks with relevant details.  
**🔹 Live Notification Panel –** Showcases all network events and security alerts in real time.

* **Future Scope & Enhancements in Threat\_Eye\_V0.2 :**

While Threat Eye v0.1 is a powerful security tool, future updates aim to further enhance its capabilities. Planned improvements include:

**🔹 Forgot Password Feature** – Implement a password recovery mechanism for the user login system.  
**🔹 OTP Verification for Sign-Up & Password Recovery** – Add an extra layer of security to prevent unauthorized account creation and recovery. **🔹 More Advanced Threat Detection –** Improve anomaly detection algorithms for more accurate results. **🔹 Custom Domain & Port Forwarding** – Enable secure remote access to the dashboard via custom domain or port forwarding.  
**🔹 HTTPS & Cloudflare Protection –** Secure the dashboard with SSL encryption and Cloudflare security to prevent DDoS attacks and unauthorized access.

* **Why Choose Threat Eye?**

Threat Eye is a lightweight yet highly effective tool designed to proactively monitor and protect networks from unauthorized access and cyber threats. Unlike traditional network scanners, Threat Eye not only detects threats but also takes automated actions like blocking unauthorized devices and sending real-time alerts to administrators.

**Ideal For:**

**✅ Network Security Professionals –** Monitor enterprise networks and detect anomalies.  
**✅ Ethical Hackers & Penetration Testers** – Identify security weaknesses and perform network analysis.  
**✅ IT Administrators** – Prevent unauthorized access and secure internal network infrastructure.  
**✅ Cybersecurity Enthusiasts** – Learn and experiment with real-world network security challenges.

* **Conclusion :**

Threat Eye v0.1 is a powerful, real-time network security tool that helps organizations and individuals protect their networks from unauthorized access and cyber attacks. With features like network anomaly detection, automatic device blocking, MITM attack detection, and instant alert notifications, it provides an all-in-one security solution for modern network environments.

With planned enhancements such as OTP-based authentication, advanced detection mechanisms, and Cloudflare protection, future versions of Threat Eye will further strengthen its capabilities.

🚀 Stay ahead of cyber threats with **Threat Eye** – Your Ultimate Network Security Companion!