Contribution ID: **144**

Type: **Oral**

Advanced Network Traffic Monitoring Tool

Growing cyber threats and the proliferation of complex network attacks present critical challenges for organizations seeking robust network defense. The Advanced Network Traffic Monitoring Tool is a Python-based solution engineered for real-time capture, analysis, and filtering of network traffic, with automated detection of suspicious activities. Integrating Wireshark command-line utilities and the Scapy library, it enables live packet capture, time-based filtering, trace merging, and multithreaded port scanning—all accessible via a streamlined Gradio web interface. This unified platform addresses usability gaps in traditional tools like Wireshark and Nmap, providing flexible monitoring, active probing, and instant threat alerts. Automated correlation of scanned ports with a database of high-risk indicators enhances detection of command & control, exfiltration, and lateral movement attempts. Modular architecture and customizable design ensure adaptability to emerging security requirements. The tool empowers both new learners and experienced security professionals to conduct comprehensive network audits, incident investigations, and proactive threat hunting efficiently.
Keywords: Network Traffic, Packet Capture, Wireshark CLI, Scapy, Port Scanning, Suspicious Activity Detection, Gradio Interface, Multithreading, Network Forensics, Real-Time Monitoring.

Authors: Mr ZACHARIAH, MOTTI (JAIN(Deemed-to-be-University)); CHAURISHIYA, sonali (JAIN(Deemed-to-be-University))

Co-author: Mr NATARAJAN, VISHNU VENKATESH (JAIN(Deemed-to-be-University))

Presenter: CHAURISHIYA, sonali (JAIN(Deemed-to-be-University))

Track Classification: Forensic Sciences