Tools POC Report – Innonup Inter

Date: 25 July 2025

Author: Supriya Santosh Jaiswal Intern ID: 244

Purpose: Assignment as an intern at Digisuraksha Parahari Foundation

# Tool Name

Innonup Inter

# History

Innonup Inter was developed as a modular, lightweight network inspection and anomaly detection tool for cybersecurity analysts and researchers. Initially designed for academic research, it has now gained traction in industry use for real-time incident analysis and network forensics.

# Description

Innonup Inter is an open-source CLI-based tool designed to monitor and analyze network traffic for security threats, anomalies, and unauthorized transmissions. It provides packet-level inspection and intelligent tagging based on AI-driven detection rules.

# What Is This Tool About?

Innonup Inter captures, logs, and analyzes live or recorded network traffic to detect intrusions, anomalies, or behavioral changes in data flow. Its goal is to simplify threat identification in complex environments like enterprise LANs or IoT networks.

# Key Characteristics / Features

* • Real-time packet inspection
* • Anomaly detection via AI rule engine
* • Protocol decoding (TCP/UDP/HTTP/DNS/IoT)
* • Custom rule scripting
* • Log tagging for alerts
* • Traffic pattern visualization (via plugin)
* • PCAP replay and injection support
* • CLI & API interface
* • Works on Linux and Windows
* • Lightweight footprint

# Types / Modules Available

* • Live Capture Module
* • Anomaly Detection Engine
* • Rule Engine (Script-based)
* • PCAP Loader & Replayer
* • Alert Tagging System
* • Plugin Visualizer (Graph & Timeline)

# How Will This Tool Help?

* • Detects unauthorized network behavior
* • Identifies malware C2 traffic in real-time
* • Pinpoints DNS tunneling and data exfiltration
* • Helps trace lateral movement in compromised networks
* • Supports PCAP replay for retroactive forensics

# 15-Liner Summary

* • CLI network forensics
* • AI anomaly engine
* • Open-source
* • Lightweight & fast
* • PCAP compatible
* • Scripting support
* • Real-time alerts
* • DNS, HTTP, TCP inspection
* • Linux/Windows friendly
* • Modular design
* • Timeline graph plugin
* • Rule-based filtering
* • Traffic tagging
* • Simple log structure
* • Forensics-ready