

LAN ANALYZER

- •OMER PORTNOY, 207251018
- •Ruben Ventura, 328759675
 - •ESTY BRANDES, 209021211

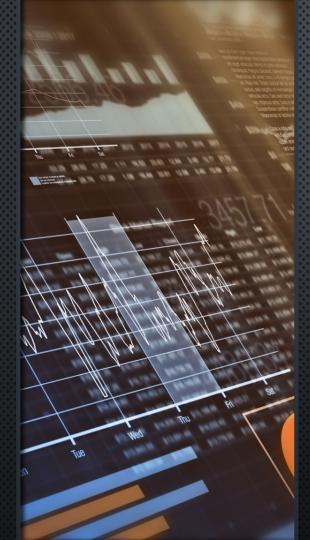
INTRODUCTION



Simplifying Network Analysis for Security: Our LAN analyzer tool provides essential functionalities to enhance network security.



Streamlining Monitoring with Integrated Tools: Integration of Nmap, P0F, and Scapy simplifies network traffic monitoring rule based detections.



RATIONALE AND OBJECTIVES

- ENHANCE NETWORK SECURITY BY IDENTIFYING POTENTIAL VULNERABILITIES.
- PROVIDE BASIC NETWORK TRAFFIC MONITORING.
- SIMPLIFY NETWORK ANALYSIS WITH A STRAIGHTFORWARD GRAPHICAL INTERFACE.
- DETECT ANOMALIES OVER PROCESSES AND NETWORK TRAFFIC

MAIN FUNCTIONALITY



PORT SCANNING: USE NMAP FOR IDENTIFYING OPEN PORTS.



FINGERPRINTING: USE POF FOR OS AND SERVICE FINGERPRINTING.



BASIC TRAFFIC ANALYSIS: USE SCAPY TO CAPTURE AND DISPLAY NETWORK PACKETS.



USER INTERFACE: PROVIDE A SIMPLE UI USING TKINTER.



Integration of Functionalities:

Use a modular design to efficiently combine port scanning, fingerprinting, traffic and behavioral analysis.



Real-time Processing:

Leverage optimized libraries like Scapy for efficient real-time traffic analysis.



UI Development:

Implement a straightforward and responsive GUI using the Tkinter framework.

CHALLENGES AND SOLUTIONS

DEVELOPMENT ENVIRONMENT AND TOOLS

1

Leveraging Python for Networking and GUI Development: Python's libraries empower robust networking functionalities and streamlined GUI development. 2

Optimizing Network Analysis with Scapy, POF and WMI: Scapy and POF enhance network analysis accuracy and efficiency for robust security.

3

Enhancing User Experience Through Tkinter GUI: Tkinter simplifies UI development, ensuring user-friendly interface for tool usage.