

NETSCAN: Prototype Summary & Visibility Report

1. Platform & Technical Architecture

Strategic Choice: Windows + Npcap

To achieve comprehensive network visibility, the prototype was developed for Windows using the Npcap driver. Mobile platforms (iOS/Android) utilize strict application sandboxing that prevents cross-device traffic monitoring. By leveraging Promiscuous Mode via Npcap, NetScan can capture and analyze packets from any device on the local network, bypassing the limitations of standard mobile environments.

2. Data Acquisition Capabilities

The prototype successfully isolates and extracts high-value plain-text metadata from ambient network traffic:

- **DNS Resolution (Browsing History):** By monitoring DNS queries, the tool identifies the specific domains devices are requesting (e.g., facebook.com or internal-server.local), providing a footprint of user activity even when the session itself is encrypted.
- **Service Discovery (Device Identification):** Through mDNS and SSDP broadcast analysis, the tool extracts human-readable identifiers such as "John's iPhone," "Kitchen-Sonos," or "Office-Printer-04."
- **Unencrypted Web Traffic (HTTP):** Full URL strings and header data are captured for any legacy or unsecured traffic transmitted via Port 80.
- **Geospatial Mapping:** Every packet is cross-referenced with IP geolocation databases to visualize the global destination of data flows in real-time.

3. The Encryption Boundary (TLS/SSL)

It is critical to distinguish between payload and metadata in the current security landscape:

Category	Status	Visibility Details
Protected Content	Encrypted	Private messages, passwords, financial data, and email bodies remain inaccessible due to TLS/SSL.
Network Metadata	Exposed	Server Name Indication (SNI), source/destination

		IPs, packet frequency, and server location remain visible.
--	--	--

Demo Impact: For demonstration purposes, this metadata is sufficient to construct a comprehensive behavioral profile of any target device on the network without needing to break encryption.

4. Security & Ethical Guardrails

The NetScan prototype is designed with a "Privacy-First" technical framework:

- **Passive Operation:** The tool functions exclusively as a listener. It does not perform Man-in-the-Middle (MitM) attacks, packet injection, or any active "hacking" techniques.
- **Volatile Storage:** To prevent data persistence, all captured information is stored strictly in system RAM.
- **Automated Purge:** All session data is permanently wiped the moment the application process is terminated. No local logs or historical databases are maintained.