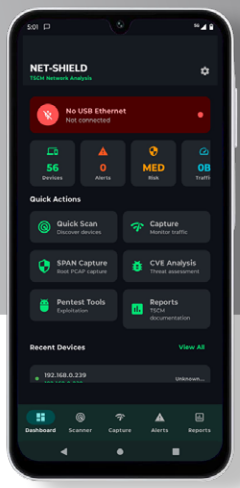
Net-Shield

TSCM network security analysis app



COUNTERMEASURES

NEW

Net-Shield delivers an instant snapshot of every device on your wire, leveraging root-level analysis to expose hidden threats that standard tools miss.

Net-Shield is a professional TSCM (Technical Surveillance Counter-Measures) network security analysis app for Android that uses a USB-OTG Ethernet adapter to discover, profile, and monitor wired networks. It provides host discovery, port scanning, real-time traffic insights, anomaly detection, and report generation. With root access and optional command-line tools, it enables true packet capture from a SPAN/mirror port and advanced diagnostic/pentest actions.

Core Capabilities

Network Discovery and Scanning

- Quick discovery (ping sweep).
- Full scan with common + high-risk ports, basic banner grabbing.
- Device fingerprinting: vendor (OUI), device type inference, risk scoring.

Traffic Monitoring and Analysis

- Non-root passive monitoring via /proc/net stats (TCP/UDP/ARP).
- Real-time stats: packet counts, protocol distribution, top talkers, ARP table, DNS queries.
- Anomaly detection: ARP spoofing, port scans, beaconing, suspicious ports, ICMP tunneling, potential data exfiltration, DNS tunneling indicators.

USB Ethernet (OTG) Support

- Detects and monitors USB-Ethernet interfaces (ASIX, Realtek, TP-Link, CDC class).
- Live connectivity/LinkProperties tracking and interface selection.

Packet Capture

- Baseline: Passive activity monitoring (no raw pcap).
- Root mode: Full packet capture via tcpdump to rolling PCAP with BPF filters; live packet feed and real-time stats.

Reporting

- Compose UI to assemble TSCM reports with devices, alerts, findings, and recommendations; export via FileProvider.

Threat/Vulnerability Insights

- Service fingerprinting and CVE lookups (local data), device risk summaries.

User Interface (Compose)
- Scanner: Start quick/full scans, view progress and device list with risk filter.
- Capture: Start/stop passive capture, traffic stats, protocol distribution, ARP/DNS views.
- Root Capture: Check root, select interface, start tcpdump with BPF filter, live packet feed, file rotation info.
- Anomalies: Severity chips, details, recommendations, dismiss actions.
- Reports: Create/view/export professional TSCM reports.

Installation & Compatibility
- Android: Min SDK 26 (8.0), Target/Compile SDK 34.
- Hardware: USB-OTG host required.
- Adapters: ASIX (AX88179), Realtek (RTL8153), TP-Link, and generic CDC Ethernet.
- Build: JDK 17, Kotlin 1.9.20, Compose compiler 1.5.5.

Permissions (runtime and manifest)
- Network: INTERNET, ACCESS_NETWORK_STATE, ACCESS_WIFI_STATE, CHANGE_WIFI_STATE, CHANGE_NETWORK_STATE.
- Foreground services: FOREGROUND_SERVICE, FOREGROUND_SERVICE_SPECIAL_USE (Android 14+).
- Notifications: POST_NOTIFICATIONS (Android 13+ prompt).
- Wake lock: WAKE_LOCK.
- Storage: Legacy READ/WRITE_EXTERNAL_STORAGE (maxSdkVersion-limited); exports via FileProvider.
- USB Host feature and vendor/class filters for Ethernet adapters.
- Cleartext traffic allowed for local analysis endpoints as needed.

Data Handling
- Local storage of scan results, anomalies, and PCAP files (app external files dir by default).
- Optional public PCAP directory when rooted (created under external storage via su).
- FileProvider to export reports and captures.

Performance & Limits
- Concurrency: up to ~50 hosts in parallel; up to ~20 ports per host chunk.
- Timeouts: ~1s ping; ~500ms TCP connect per port.
- PCAP capture: rolling files (default ~100 MB/file, keep last 10); PPS/BPS real-time updates.

Security & Compliance
- Intended for authorized TSCM/security operations only.
- Anomaly rules emphasize reconnaissance and exfil indicators.
- Root mode and pentest tools can disrupt networks; use only in controlled, permitted environments.

Known Limitations
- Without root: no raw packet capture; analysis relies on /proc/net and heuristics.
- External binaries must match device architecture and be in su PATH.
- Public PCAP directory creation requires root and permissive file modes.

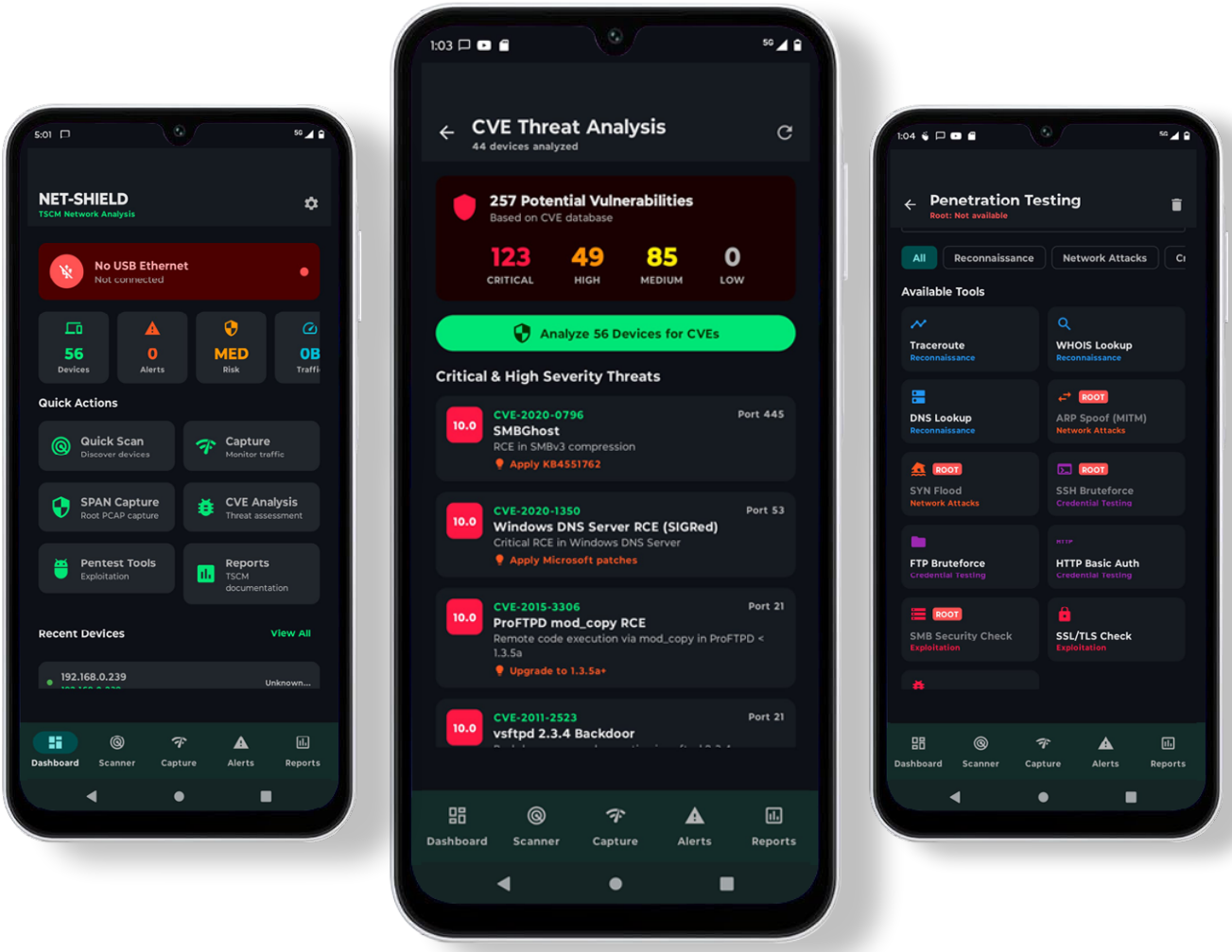
USB Adapter Support (examples)
- ASIX AX88179 (0×0B95).
- Realtek RTL8153 (0×0BDA).
- TP-Link (0×2357).
- Generic CDC class Ethernet.

Android 14 Foreground Service Notes
- Uses FGS special use subtype for scanning/capture services when available.
- Falls back to standard FGS on older Android versions.

Net-Shield

TSCM network security analysis app

COUNTERMEASURES



It takes a super snap shot of all networked devices. Allowing for real-time or post processing of network analysis and threat assessment

Requirements Summary

Baseline (no root)

- Android 8.0+ with USB-OTG host.
- USB-Ethernet adapter (ASIX/Realtek/CDC).
- Permissions: Network, Notifications (13+), Foreground Service.
- Features: discovery, full/port scans, passive monitoring, anomaly detection, reports.

Advanced (rooted device)

- Stable root (e.g., Magisk).
- CLI tools in su PATH: tcpdump (mandatory for raw capture); optional: arping, hping3/nping, nmap, smbclient, snmpwalk, sshpass, traceroute, whois, nslookup, host.
- Enables SPAN-grade packet capture with BPF filters, per-IP iptables stats, and pentest utilities.

Deliverables and Status

- Comprehensive app analysis completed from source.
- Sales-ready spec sheet provided here, including root requirements and optional tooling.