HACKING SWISS ARMY KNIFE

A PENETRATION TESTER'S BEST FRIEND!

You are working on a penetration testing contract, and you have social-engineered your way through to the server room …

The Liability of Clutter

The Scenario: you are in a server closet. Time is running out, and you need an outstanding need to install a Network Tap on a switch's port.

The Friction: As a part of your earlier social-engineering efforts, you have brought your trusty technician bag, packed to the rim with network cables, ethernet hubs, external ethernet adapters, and so on. Every second counts, and with every item you push aside, your anxiety level increases with it …

The Risk: Your trusty Raspberry Pi is overheating, in spite of its loud-sounding fan going overboard to cool it down. The fan's sound is loud enough to be heard by anyone who decides to wander in for a glance.

The Feeling: We have a fine mixture of anxiety, increased risks of exposure and a feeling of sluggishness …

The Operative's Edge

The Scenario: you are in the same server closet, tasked with the same objective.

The Flow: You slide **the device** from your pocket. It is cool to the touch, due to the effective heat dissipation due to the incorporation of a dense passive cooler in the design, along with heat resistant plastics and silicon grips.

The Action: You need Ethernet? You push-click the Wi-Fi module out and snap the Ethernet module in. The **E-Ink display** confirms the new interface instantly. Due to the design of E-Ink, it does not need to refresh unless there is new information to be displayed. More power saved!

The Result: No fans. No light bleed. No fumbling. You switch the **Hardware OS Toggle** to choose Kali Linux, plug the ethernet cable into the Ethernet Module and walk out before anyone knows you were there.

The Feeling: *Invisible. Surgical. Ready.*

The Anatomy

The Stealth Core (Hardware)

Chassis: Heat-dissipating aluminum alloy with heat-resistant ABS grip.

Thermal: Passive cooling pads + heat shield (Silent/No Fans).

Display: Low-power Color E-Ink (Sunlight readable, no suspicious glow).

Control: Physical Hardware Switch for Multi-OS Boot

(Kali / OpenWRT / Bjorn).

The Modular Bay (Connectivity)

Push-Click Hub: Hot-swappable USB-C ports for instant module changes.

Included Modules: Wi-Fi Monitoring, Bluetooth Sniffing, LTE modem and Ethernet.

Expansion Ready: GPIO access, Sub-GHz, NFC/RFID (Future Addons).

The Command Center (Software)

Mobile Uplink: Dedicated Phone App for remote menu control & log processing.

Data Pipeline: Auto-send captured data to phone storage.

Network Suite: Pre-configured DNS, TOR, remote access with Wireguard VPN , and Pi-hole integration for use as a portable privacy router

Detection Suite: Possible additions would be a microphone unit to detect changes in decibels in the room, utilization of the Bluetooth model to detect proximity of other Bluetooth devices and a GPS location-tracking unit