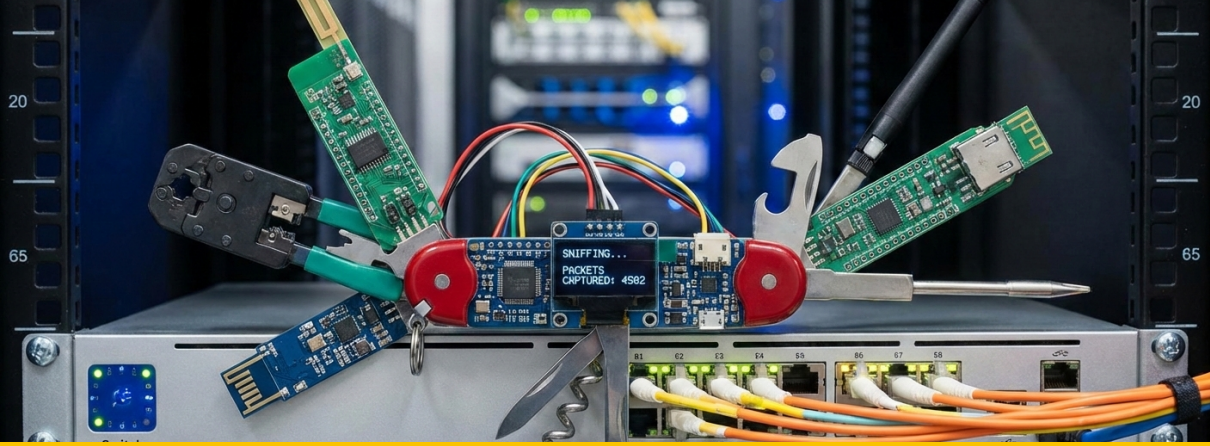

Swiss Army Knife Network Sniffer (NSAK)

Version 0.4

January 11, 2026

Lukas von Allmen (vonal3) and Frank Gauss (gausf1) | Bern University of Applied Sciences

Introduction

Motivation

Subtitle

- **Cyberangriffe nehmen zu** Angriffsbarrieren sinken, Automatisierung steigt
- **Sicherheit erfordert Sichtbarkeit** Netzwerkangriffe sind oft nur auf Layer 2–4 erkennbar
- **Bestehende Frameworks sind komplex** Hoher Konfigurations- und Betriebsaufwand
- **Unser Ansatz (PoC)** Modularer, kontrollierter Network-Sniffer für Angriffsszenarien

Eher alles als Bilder

Warum Network Sniffing

Color Wheel?

Design and Architecture

Was ist der Swiss Army Network Sniffer

NSAK Concepts

- **Devices** Physical machines used as attack and target hosts
- **Environments** Network infrastructure and topology
- **Scenarios** Sequence of drills (e.g. ARP spoofing, Packet Capture)
- **Drills** Individual attack or observation steps
- **Operator** Red / Blue team

Hardware Evaluation

Hardware Selection

Was braucht so ein Board

- At least two native Ethernet interfaces for inline packet sniffing
- Support for 2.5 GbE or higher
- Onboard Wi-Fi with access point (AP) and monitor mode support
- Low power consumption suitable for 24/7 operation
- Compact form factor for laboratory and prototype setups
- Strong community and software support
- Affordable cost (below 150 CHF)

Bild R4 und Nano PI

Implementation

Use Cases / Demo-Szenario

MITM ARP-spoofing / Transparent TCP Proxy

- Idee und Konzept auffrischen
- umsetzung erklären
- Demo

Use Cases / Demo-Szenario

Rogue AP

- Idee und Konzept auffrischen
- umsetzung erklären
- Demo am Ende

Evaluation and Discussion

Grenzen und Risiken Future Work

Subtitle

1 Folie

Fazit und Takeaways

Subtitle

1 Folie Repo Link

Demo Access Point

Subtitle

Keine Folien

Blocks

Block with a title

Content.

Without title

Block types

Exampleblock

Content.

Alertblock

Content.

Example (Example environment)

Content.