



# 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 (Franky)

# 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

(Lücku)

# 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 (Franky)

# Implementation

# NSAK Framework

- Core:
- CLI: Frontend which uses the API exposed by the core to enable user interaction
- Resource Repository: Python implementation of Scenarios, Drill,  
(Lücku)

# Scenario: MITM ARP-spoofing / Transparent TCP Proxy

Use Cases / Demo-Szenario

## Drills:

- Discover Hosts: Scans the target network
- ARP Spoof: Spoofs the MAC Addresses of discovered hosts
- Transparent TCP Proxy:
  - Creates a TCP client and server
  - Redirects traffic with IPTables / NFTables
  - Reads and modifies intercepted packages

## Environment:

- Simulation with podman/docker compose
- Instructions for building a lab with two Raspberry PIs and a switch

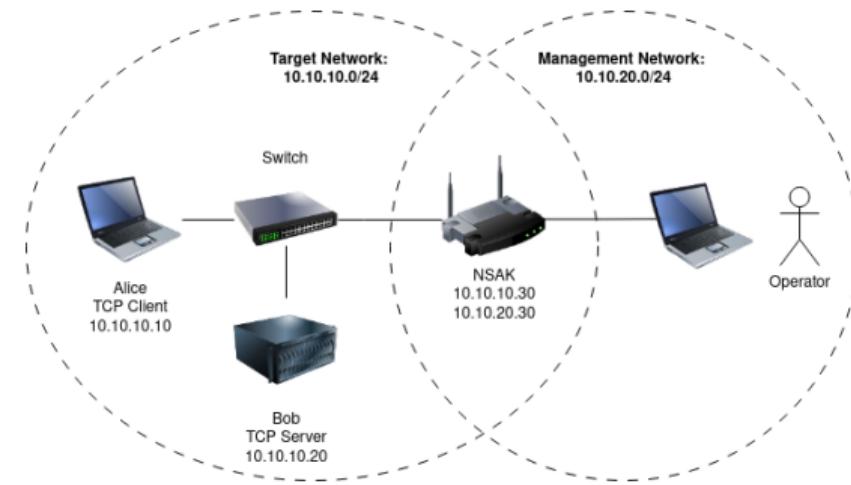


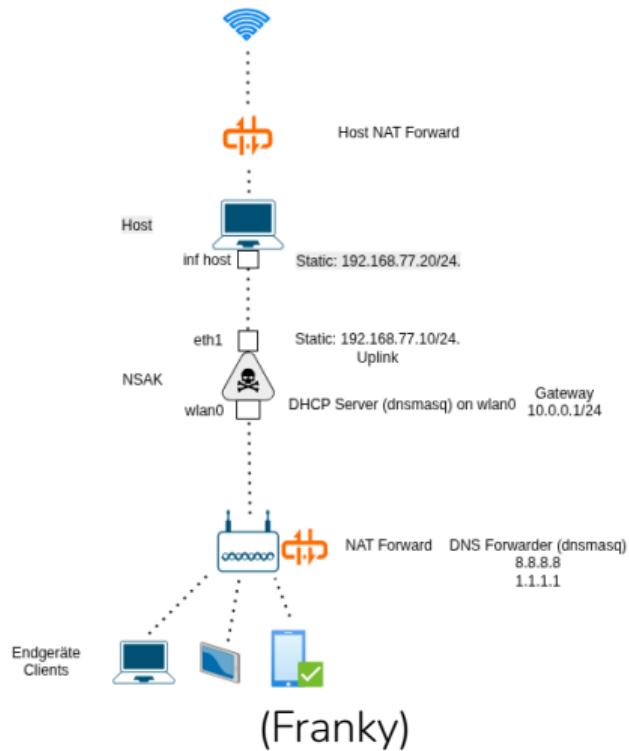
Figure: Simple TCP client - server environment

Demo Video

(Lücku)

# Demo-Szenario

## Rogue AP



# Evaluation and Discussion

# Conclusion and Future Work

Key insights and Takeaways

1 Folie (Lücku)

# Questions

Demo Access Point

(Lücku / Franky)