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

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

NSAK Framework
MITM ARP-spoofing / Transparent TCP Proxy

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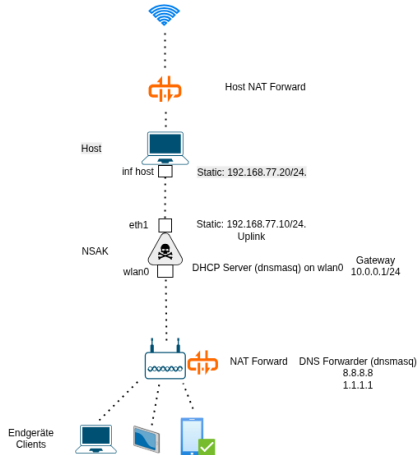- Resource Repository: Python implementation of Scenarios, Drill,

Use Cases / Demo-Szenario
Data Link Layer ARP MitM

- Idee und Konzept auffrischen
- umsetzung erklären
- Demo

Demo-Szenario

Rogue AP

Host NAT Forward

Host
inf host   Static: 192.168.77.20/24.

eth1   Static: 192.168.77.10/24.
Uplink

NSAK

wlan0   DHCP Server (dnsmasq) on wlan0   Gateway
10.0.0.1/24

NAT Forward   DNS Forwarder (dnsmasq)
8.8.8.8
1.1.1.1

Endgeräte
Clients

Evaluation and Discussion

Conclusion and Future Work

Key insights and Takeaways

1 Folie

Questions

Demo Access Point