fritzbox-capture

Voraussetzungen schaffen um eine FRITZ!BOX an ein IDS anbinden

Grundlage

- FRITZ!BOX hat kein „Mirror-Port“ :-(
- In FRITZ!BOXen kann man über die URL https://fritz.box/html/capture.html PCAP-Dumps der verschiedenen Netzwerkschnittstellen herunterladen
- Start und Stop des Dumps wird manuell gesteuert

Wie gehts?

- PCAP-Dump via curl oder wget herunterladen
- Ausgabe von curl oder wget in tcpreplay „pipen“
- tcpreplay die Ausgabe an ein dummy-Interface machen lassen
- NIDS auf dem dummy-Interface „hören“ lassen

Herausforderungen

- Session mit der FRITZ!BOX aushandeln und herstellen
- Automatisierung: https://github.com/pditzel/scripts/blob/master/fritzbox-capture/fritzbox-capture.sh
  - Viele versch. Skripte für das Sessionhandling
  - Developertools unter Firefox

Ende

Quellen:

- https://github.com/pditzel/scripts/blob/master/fritzbox-capture/fritzbox-capture.sh
- https://www.administrator.de/wissen/fritzbox-reboot-ohne-telnet-bash-shell-script-f%C3%BCr-aktuelle-firmware-versionen-6-6-3-274710.html