

# Dry running iptables-legacy scripts – a PoC

William Robinet

2023-07-04

#pts23 – Rump sessions

# The plot

- ▶ “iptables-legacy” based firewalls
- ▶ Rules are loaded at boot time via a bash script
- ▶ You want to keep meaningful variable names and shell facilities
- ▶ Large ruleset
- ▶ No check mechanism available

# The PoC

- ▶ We want to profit from the parsing abilities of “iptables-legacy” without actually modifying anything on the running kernel
- ▶ We want to profit from the shell error reporting
- ▶ Solution: mask syscalls via dynamic library preloading
- ▶ Demo

# Contact

project page

<https://github.com/wllm-rbnt/iptwrap>

social media

@wr@infosec.exchange

email

willi@mrobi.net

slides

<https://www.github.com/wllm-rbnt/iptwrap/blob/main/pts2023/iptwrap.pdf>