MSE | MASTER OF SCIENCE IN ENGINEERING

NFQUEUE Target

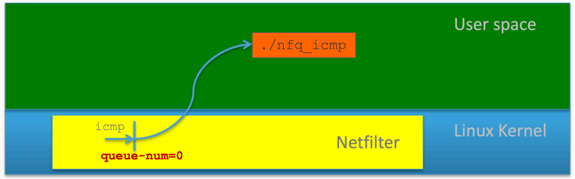
Luca Haab, Jean-Roland Schuler

November 23, 2025

NFQUEUE target (I)

The NFQUEUE target gives the opportunity to pass the packet to userspace. Namely

- NFQUEUE is a special iptables target that sends matching packets from the kernel's netfilter framework into a user-space queue.
- A userspace program (e.g. an intrusion-detection system like *Suricata* or *Snort*) can then read packets from that queue via libnetfilter_queue, decide what to do with each packet (modify it, drop it, accept it) and return a *verdict* back to the kernel.
- The queue number is selectable with the --queue-num option in the iptables rule; it's a 16-bit value (so between 0 and 65535).
- If no userspace process is listening on a queue, by default packets may be dropped.



NFQUEUE target (II)

Example: all `icmp` packets received in the kernel must be checked in the userspace.

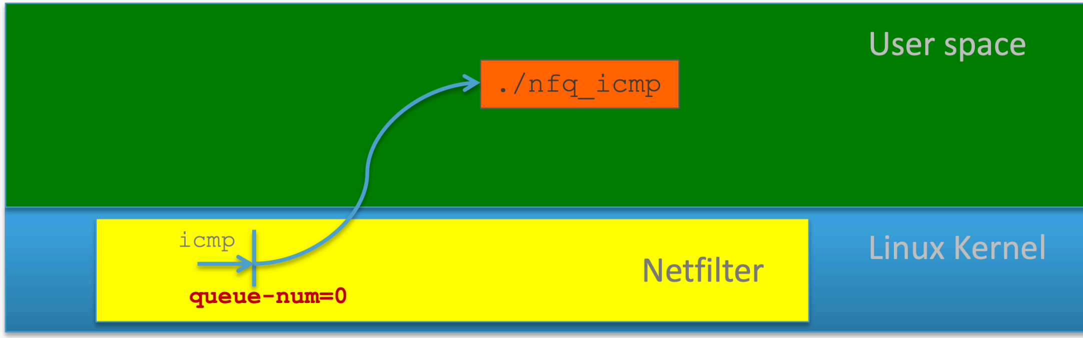
In order to do so, one has to

- create the target queue (in userspace)

```
# NFQUEUE queue-num = 0 for incoming ICMP
iptables -A INPUT -t filter -p icmp -j
NFQUEUE --queue-num=0
```

- write (or simply run if it exists already) the programme that reads from the queue the packets that hit the rule

```
  # nfq_icmp is program that checks all icmp
packets in the userspace
  ./nfq_icmp
```



Resources

- `iptables` documentation: https://www.netfilter.org/documentation/
- `libnetfilter_queue` Documentation: https://www.netfilter.org/projects/libnetfilter_queue/doxygen/html/
- *Writing Netfilter modules*, J. Engelhardt, N. Bouliane, http://inai.de/documents/Netfilter_Modules.pdf