IPS exercise

Jens Schønberg

April 2022

1 Exercise 1. Taking a look at iptables

If you haven't then I would recommend to install Wireshark or try a test case with tcpdump to start sniffing and detecting network traffic.

2 Exercise 2. Writing a TCP-state rule

iptables -A INPUT -m conntrack –cstate ESTABLISHED,RELATED -j ACCEPT

is just one example, but it allows to make connection based on the stateful TCP session.

You can also add dport such as 22 for ssh, and new for outgoing, then established for incoming.