Scenario

You’re a network analyst who needs to use `tcpdump` to capture and analyze live network traffic from a Linux virtual machine.

The lab starts with your user account, called `analyst`, already logged in to a Linux terminal.

Your Linux user's home directory contains a sample packet capture file that you will use at the end of the lab to answer a few questions about the network traffic that it contains.

Here’s how you’ll do this: **First**, you’ll identify network interfaces to capture network packet data. **Second**, you’ll use `tcpdump` to filter live network traffic. **Third**, you’ll capture network traffic using `tcpdump`. **Finally**, you’ll filter the captured packet data.