Activity Overview

As a security analyst, it's important to know how to capture and filter network traffic in a Linux environment. You'll also need to know the basic concepts associated with network interfaces.
In this lab activity, you'll perform tasks associated with using tcpdump to capture network traffic. You'll capture the data in a packet capture (p-cap) file and then examine the contents of the captured packet data to focus on specific types of traffic.
Let's capture network traffic!