## **Activity File: OSI**

In this exercise, you'll continue to play the role of a security analyst at Acme Corp.

* You will be analyzing 10 suspicious network-related activities that have occurred at Acme Corp, which may be associated with Sally Stealer.
* Your task is to document at which OSI layer each of these situations occurred to help the Networking team pull the necessary logs for investigation.
* <https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/08-Networking-Fundamentals/2/Resources>

### **Instructions**

Review the list of 10 suspicious activities and determine which of the seven OSI layers each falls under:

1. A networking cable was cut in the Data Center and now no traffic can go out.
   1. Layer 1
2. A code injection was submitted from an administrative website, and it's possible that an attacker can now see unauthorized directories from your Linux server.
   1. 7
3. The MAC address of one of your network interface cards has been spoofed and is preventing some traffic from reaching its destination.
   1. 2
4. Your encrypted web traffic is now using a weak encryption cipher and the web traffic is now vulnerable to decryption.
   1. 6
5. The destination IP address has been modified and traffic is being routed to an unauthorized location.
   1. 3
6. A flood of TCP requests is causing performance issues.
   1. 4
7. A SQL injection attack has been detected by the SOC. This SQL injection may have deleted several database tables.
   1. 7
8. A switch suddenly stopped working and local machines aren't receiving any traffic.
   1. 1
9. An ethernet cable was disconnected and the machine connected isn't able to receive any external traffic.
   1. 1
10. Traffic within the network is now being directed from the switch to a suspicious device.
    1. 2