## **Activity File: Network Security**

In this activity, you will play the role of a security analyst at Acme Corp.

* Several suspicious activities have occurred on Acme's products and systems.
* For each suspicious activity, you must list out the client and servers, and then describe the request and response in simple terms.

### **Instructions**

Review the three suspicious incidents at Acme Corp. For each, document the client and server, and describe the request and response in simple terms.

1. A hacker logged into Microsoft Outlook with the stolen username and password of Acme's CFO. The hacker sent an email to the head of accounting asking them to wire $10,000 to a foreign account owned by the hacker.
   1. Server: Email Server or mail exchange server.
   2. Client: Microsoft Outlook
   3. Request: Wire $10,000.00 to a foreign account sent via email
   4. Reponse: confirmation from exchange email that the email was recieved
2. A hacker used Firefox to visit the administrative website of Acme Corp, where they attempted to log into the CFO's account multiple times, until they correctly guessed the password.
   1. Server: Webserver hosting admin webpage
   2. Client: Firefox
   3. Request: Login attempts to CFO account
   4. Reponse: Brute force attacks until entering correct password and login is accepted
3. A hacker stole the Acme CFO's mobile phone. Login credentials were saved on the phone, allowing the hacker to log into Acme Corp's mobile admin application.
   1. Server: mobile web server
   2. Client: server hosting mobile admin application
   3. Request: Accessing Acme Corp’s mobile admin application
   4. Response: Confirmation for login credentials

**Use the internet to assist in your research.**