## **Activity File: DNS Spoofing**

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

* In the previous activity, you determined that the hacker is trying to access Acme Corp's trade secrets.
* Acme Corp is concerned the hacker may try to access a website called acmetradesecrets.com. Acme must prevent the hacker from accessing this website.
* Your task is to create and test out a DNS spoof record that will redirect any hacker trying to visit acmetradesecrets.com to another website.
* This will first be tested on on your machine, but later it will be added to the hacker's computer.

### **Instructions**

Log into your Linux server.

1. Create a DNS spoof record for acmetradesecrets.com, to be redirected to the IP address of 52.202.62.206 (zoom.us).
   1. Cd /etc
   2. Ls -alt #To find the host file
   3. Sudo nano hosts
   4. 52.202.62.206 acmetradesecrets.com #at the bottom of the scripts
2. Open up a browser in your Linux server, and validate that when you access acmetradesecrets.com, it redirects correctly.

#### **Bonus**

* Research how to apply the same DNS spoof record on a Windows machine or VM.
* If you don't have access to a Windows machine, simply document the steps to create a DNS spoof record on a Windows system. If you do have access to a Windows machine, apply the spoof record on it.
  + User
  + Windows
  + System32
  + Drivers
  + Etc
  + services