## **Activity File: DHCP Attacks**

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

* Acme Corp employees are currently experiencing network access issues and are unable to connect to the internet.
* These employees are receiving error messages saying no local IP addresses are available, indicating a potential issue with DHCP.
* Acme believes an internal attack may have occurred and would like you to investigate by analyzing a packet capture to determine what type of attack may be causing the issue.
* <https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/09-Networking-Fundamentals-II-and-CTF-Review/1/Activities/04_DHCP_Attacks/unsolved>

### **Instructions**

Open the provided packet capture with Wireshark.

1. Create a filter to determine the count for *each* DHCP activity:  
   * DHCP Discover
     1. Dhcp.option.dhcp == 1
   * DHCP Offer
     1. Dhcp.option.dhcp == 2
   * DHCP Request
     1. Dhcp.option.dhcp == 3
2. Based on these results, summarize what type of attack may have occurred, and why you believe Acme Corp's employees are having network issues.
   * DHCP starvation attack due to multiple DHCP request and offer within a short period of time
   * Caused staff attempting to connect to the network to be unable to connect due to lack of public IP addresses

#### **Bonus**

* Analyze the source MAC addresses of the DHCP activities and summarize what the attacker is doing.
  + The attacker is using different MAC addresses