## **Activity File: Analyzing ARP**

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

* CompuCom, a software company, has hired Acme Corp to do a security assessment of their network.
* Your task is to analyze ARP activity from a CompuCom packet capture to determine if any vulnerabilities exist
* <https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/08-Networking-Fundamentals/3/Resources>

### **Instructions**

1. Open the packet capture provided to you and filter out for ARP activity.
2. Document the physical addresses found for each of the following IP addresses:  
   * 192.168.47.1
     1. Duplicate IP address detected for 192.168.47.1 (00:0c:29:1d:b3:b1) - also in use by 00:50:56:c0:00:08 (frame 298)
   * 192.168.47.2
     1. [Duplicate IP address detected for 192.168.47.2 (00:0c:29:1d:b3:b1) - also in use by 00:50:56:fd:2f:16 (frame 304)]
   * 192.168.47.200
     1. Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 224)
   * 192.168.47.254
     1. Duplicate IP address detected for 192.168.47.254 (00:0c:29:1d:b3:b1) - also in use by 00:50:56:f9:f5:54 (frame 278)
3. Further analyze the packet capture to determine if these IPs present any potential security vulnerabilities, and write a summary of your findings to provide to CompuCorp.

#### **Bonus**

1. Name a few ways to protect against this vulnerability.
   1. Create static arp entries in the servers
2. Determine the primary vendor for the MAC addresses.
   1. The web tool at aruljohn.com/mac.pl identifies all the MAC addresses vendors as VMWare.