## **Activity File: Analyzing DNS Record Types**

<https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/09-Networking-Fundamentals-II-and-CTF-Review/2/Activities/03_DNS_Record_Types/unsolved>

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

* Acme Corp recently updated the DNS records for several of their sites and needs you to confirm the updates worked.
* Your task is to use nslookup to validate the DNS records for each of the domains provided.

### **Instructions**

1. Acme Corp owns the following domains:  
   * splunk.com
   * fireeye.com
   * nmap.org
2. For each website, determine the following DNS records and document your findings:  
   * A record
     1. Nslookup -type=A splunk.com
   * NS record
     1. Nslookup -type=NS fireye.com
   * MX record
     1. Nslookup -type=MX nmap.com
3. Answer the following questions:  
     
    a. Did any of the domains have more than one MX record? If so, why do you think that is? They all have more than one MX records for redundancy  
     
    b. For nmap.org, list the mail servers, from the highest to lowest priority.
   * Lowest number has a higher priority

#### **Bonus**

* Look up the SPF record for nmap.org and explain what it indicates.
  + Nslookup -type=txt nmap.org
  + The SPF record shows a range of IP address that are allowed to send emails as and representing as nmap