Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:

  The CEO of Altoro Mutual is Karl Fitzgerald

- How can this information be helpful to an attacker:

  This information is useful to an attacker when used as part of a spear phishing email. This kind of attack directly to a CEO is known as whaling.

Step 2: DNS and Domain Discovery

Enter the IP address for `demo.testfire.net` into Domain Dossier and answer the following questions based on the results:

1. Where is the company located:

   Sunnyvale California

2. What is the NetRange IP address:

   65.61.137.64 – 65.61.137.127

3. What is the company they use to store their infrastructure:

   Rackspace

4. What is the IP address of the DNS server:

   65.61.137.117

Step 3: Shodan

- What open ports and running services did Shodan find:

  Shodan found Port 80 – Apache HTTP, Port 443 – Apache HTTPS, and Port 8080 Apache HTTP

Step 4: Recon-ng

- Install the Recon module `xssed`.
- Set the source to `demo.testfire.net`.
- Run the module.

Is Altoro Mutual vulnerable to XSS: Yes

Step 5: Zenmap

Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

- Command for Zenmap to run a service scan against the Metasploitable machine:

nmap -sV 192.168.0.10

- Bonus command to output results into a new text file named `zenmapscan.txt`:

  nmap -sV -oN zenmapscat.txt 192.168.0.10

- Zenmap vulnerability script command:

  nmap –script smb-vuln* -p 139.445 192.168.0.10

- Once you have identified this vulnerability, answer the following questions for your client:

  1. What is the vulnerability: The vulnerability is a weakness in smb, which allows unauthorized access
  2. Why is it dangerous: It is dangerous because it allows for data to be extracted
  3. What mitigation strategies can you recommendations for the client to protect their server: Recommended mitigation would be updating or patching Samba as soon as possible.