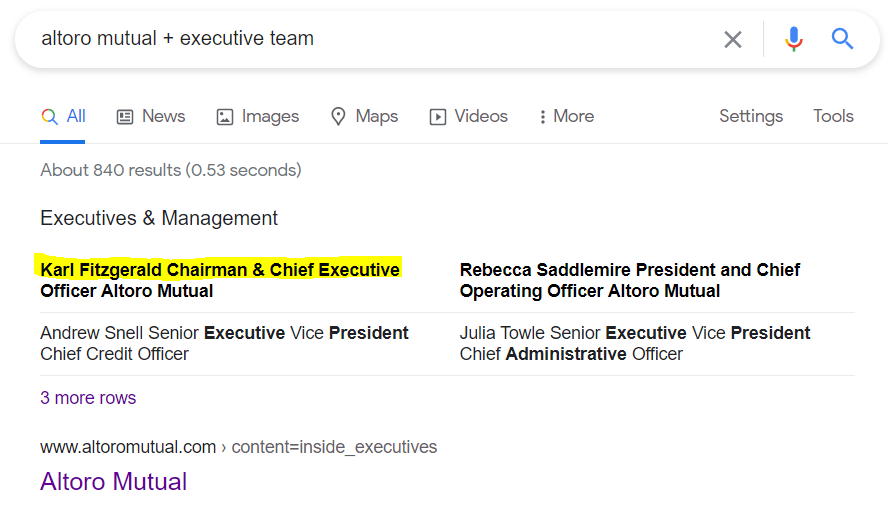
**## Week 16 Homework: Penetration Testing 1**Altoro Mutual wants to ensure that private information that is unavailable on their public website cannot be found by searching the web.

Using Google, can you identify who the Chief Executive Officer?  


How can this information be helpful to an attacker?

**Help in the sense that it can assist a hacker in performing social engineering. The ability to identify the prime target who has full access to the system might yield the attacker access when the target is in a compromised unsuspecting position.**

**#### Step 2: DNS and Domain Discovery**

The reconnaissance phase of a penetration test is possibly the most important phase of the engagement. Without a clear understanding of your client's assets, vulnerabilities can go unnoticed and later exploited.

- Navigate to `centralops.net`.

- 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 94085**

2. What is the NetRange IP address?

**65.61.137.64- 65.61.137.127**

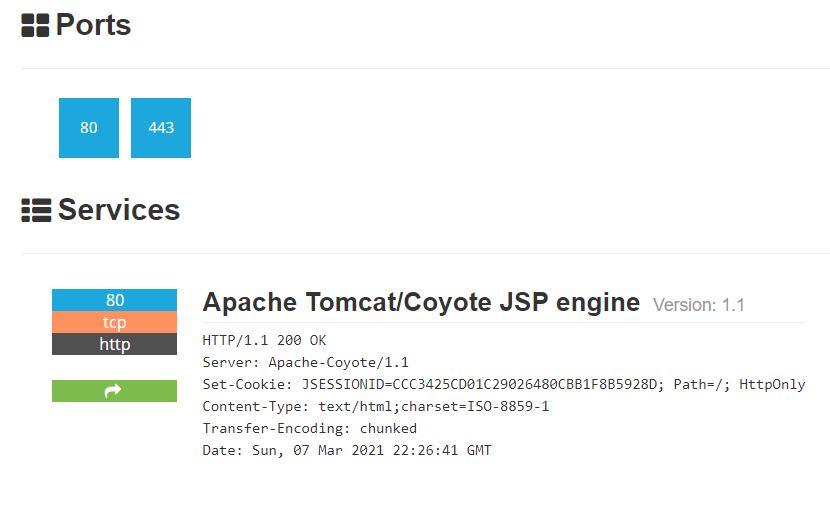
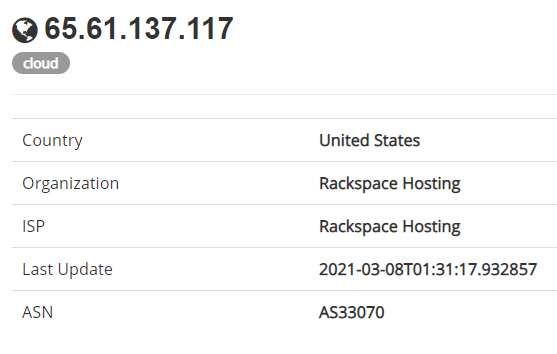
3. What is the company they use to store their infrastructure?

**Rackspace Hosting**

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

**65.61.137.117**

**#### Step 3: Shodan**



Using Shodan and the information gathered from Google Dorking, find any other useful information that can be used in an attack.

- Navigate to [shodan.io](https://www.shodan.io/).

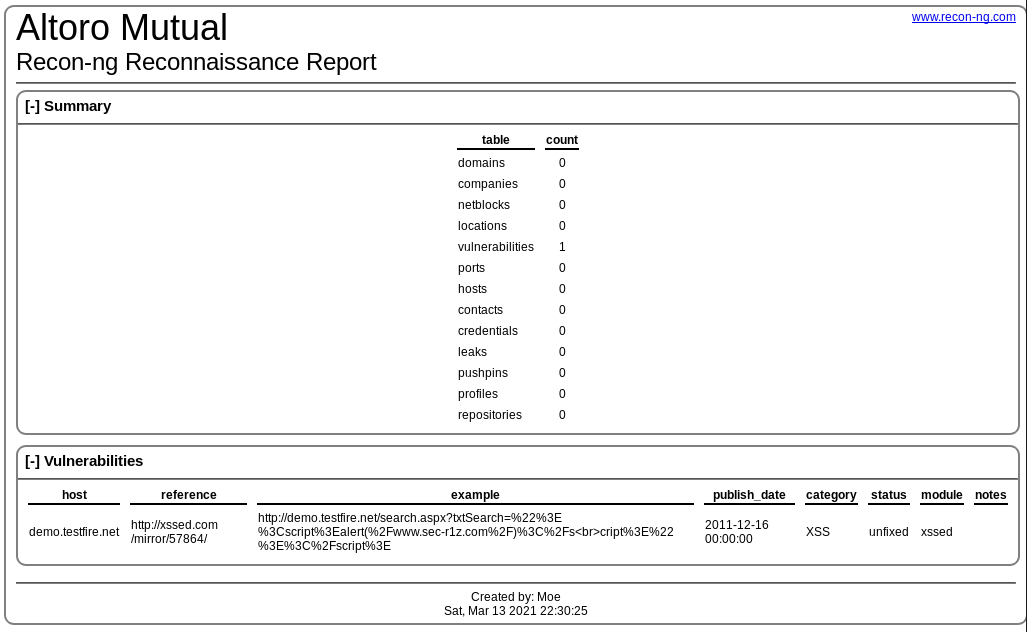
- Run a scan against the IP address of the DNS server for `demo.testfire.net`.

- What open ports and running services did Shodan find?

**80,443,8080  
Service: Apache Tomcat/Coyote JSP Engine (version 1.1)set**

**#### Step 4: Recon-ng**

Altoro Mutual is also concerned about cross-site scripting attacks, which can cause havoc on their website. Verify whether or not Altoro Mutual is vulnerable to XSS by installing the Recon module `xssed`, and setting the source to `demo.testfire.net`.

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:

- Use Zenmap to run a service scan against the Metasploitable machine.

**Nmap -T4 -A -v192.168.0.10**

- \*\*Bonus:\*\* In the same command, output the results into a new text file named `zenmapscan.txt`.

**Nmap -T4 -A -v -oA zenmapscan 192.168.0.10**

- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.  
**CVE-2012-1182**

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

1. What is the vulnerability?   
**SMB 3(Samba)**

2. Why is it dangerous?  
**Allows remote code execution as the “root” user from an anonymous connection**

3. What are your recommendations for the client to protect their server?   
**Patch the system and upgrade to the newer versions available**

---

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.