#### **Step 1: Google Dorking**

Altoro Mutual wants to ensure that private information that is unavailable on their public website cannot be found by searching the web.

* For example, Altoro Mutual does not mention their executive remembers on the website. Using Google, can you identify who the Chief Executive Officer is?

Answer: **The Chief Executive Officer is Karl Fitzgerald**

* How can this information be helpful to an attacker?

Answer: **This information can help the hacker send out phishing emails to all executive members**

#### **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?

Answer: **Sunnyvale, CA**

* 1. What is the NetRange IP address?

Answer: **65.61.137.64 - 65.61.137.127**

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

Answer: **Rackspace Backbone Engineering is the company they use to store their infrastructure**

* 1. What is the IP address of the DNS server?

Answer: The IP address of the DNS server is **65.61.137.117**

#### 

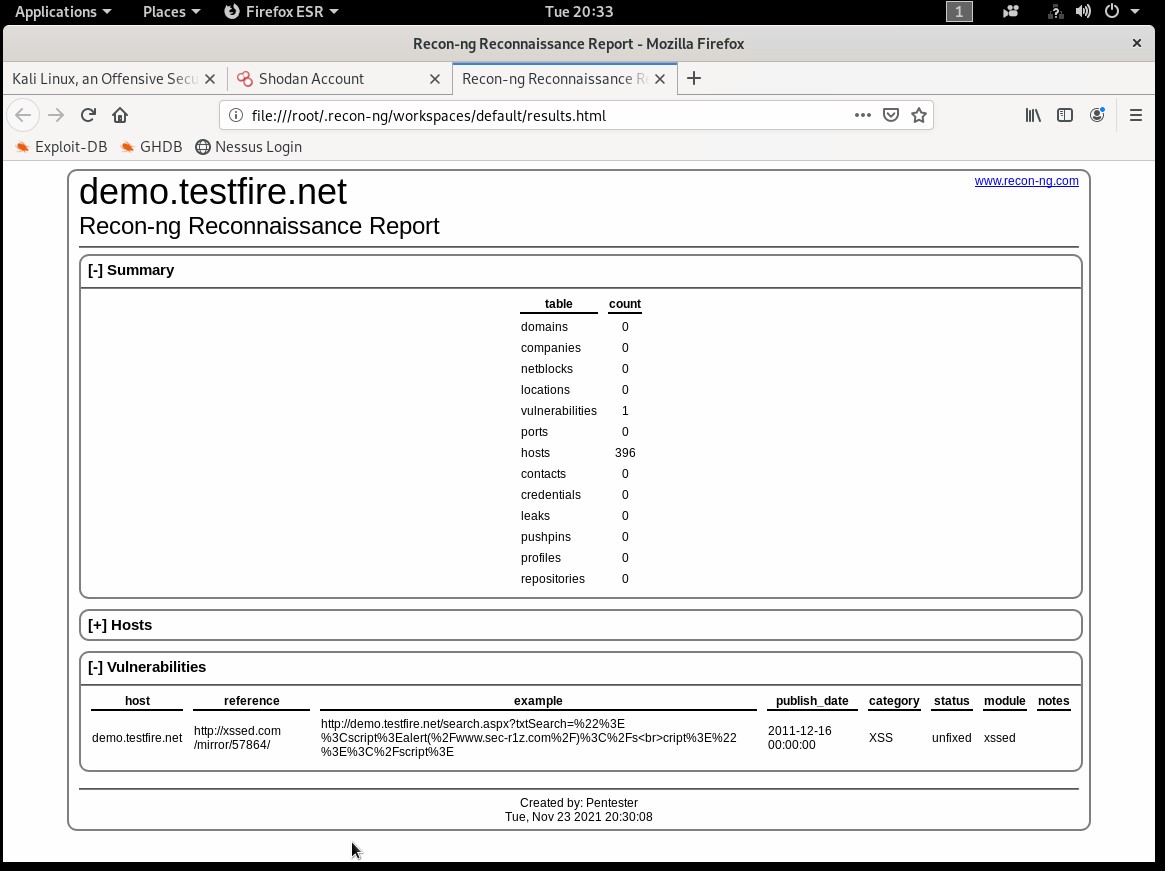
#### **Step 3: Shodan**

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?

Answer: **The open ports and running services of 80, 443, & 8080 were found**

#### **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 completing the following:Is Altoro Mutual vulnerable to XSS?

Answer: **Yes, Altoro Mutual is vulnerable to XSS**

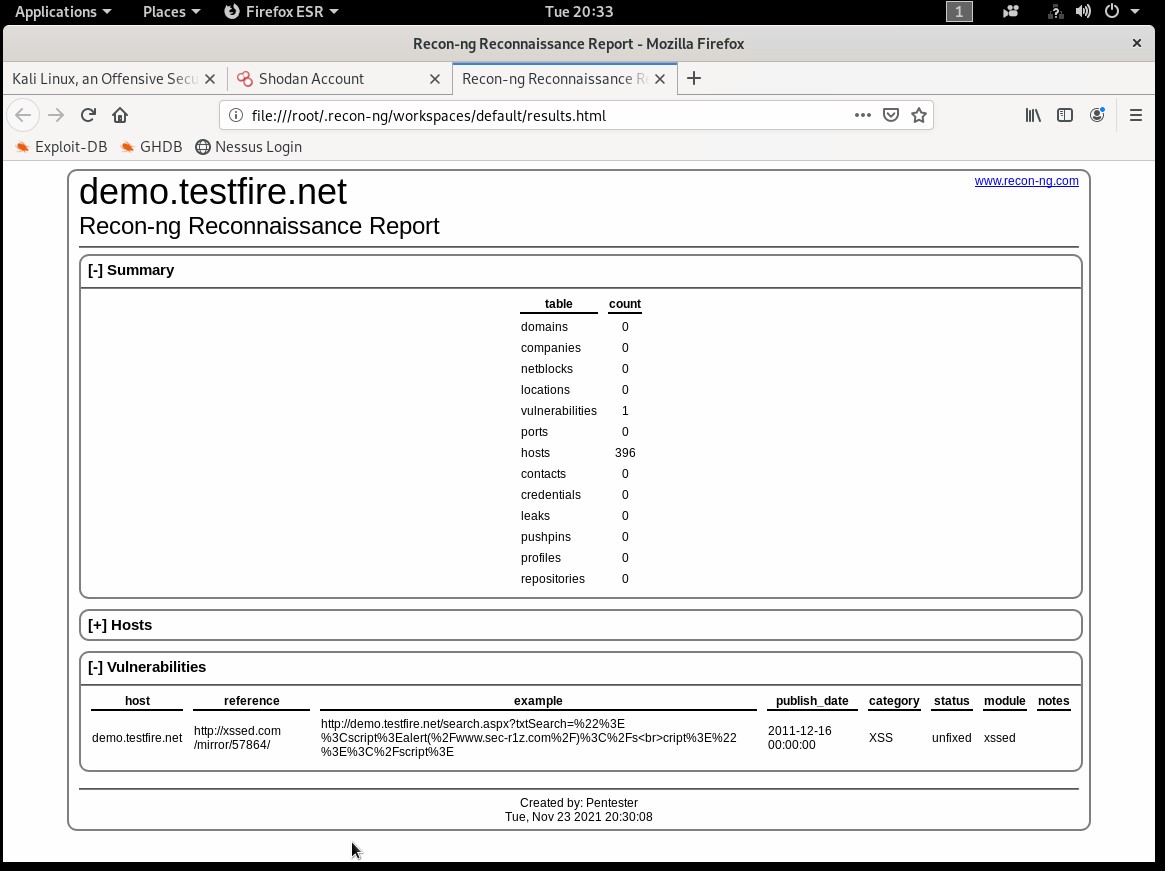
### **Step 5: Zenmap**

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.

Answer: **The Zenmap would use the command of nmap -T4 -A -v192.168.0.10 to run a service scan against the Metasploitable machine**

* 1. **Bonus:** In the same command, output the results into a new text file named zenmapscan.txt.
* Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.



* 1. What is the vulnerability?

Answer: **The vulnerability of both ports 139 / 445 are left open for read and write exectutions**

* 1. Why is it dangerous?

Answer: **Anyone that logs in can make changes as they want to because both ports have been left open**

* 1. What are your recommendations for the client to protect their server?

Answer: **My recommendations are for the client to update, patch their servers, and to not leave any ports to read and write**