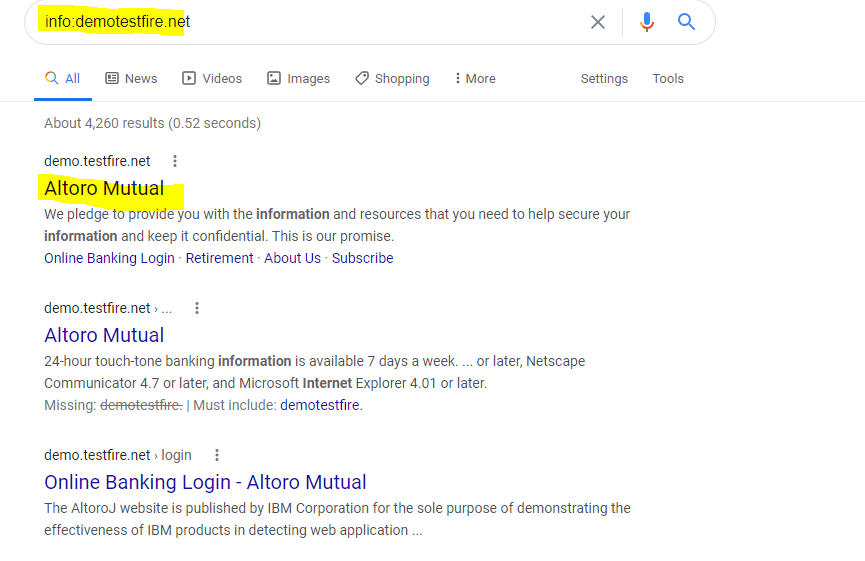
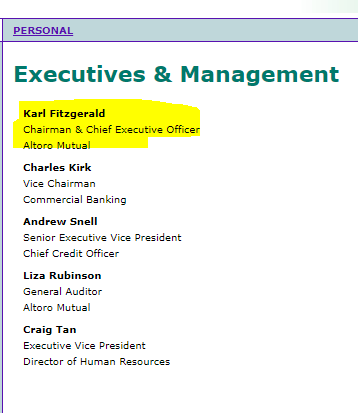
#### **Step 1: Google Dorking**

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

The Chief executive Officer of the Altoro Mutual organization is **Karl Fitzgerald**. Using the command, **info:demotestfire.net** on google, the information was retrieved.





* How can this information be helpful to an attacker:

The Information can enable an attacker to carry out different attacks such as **Social Engineering.**

#### **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:

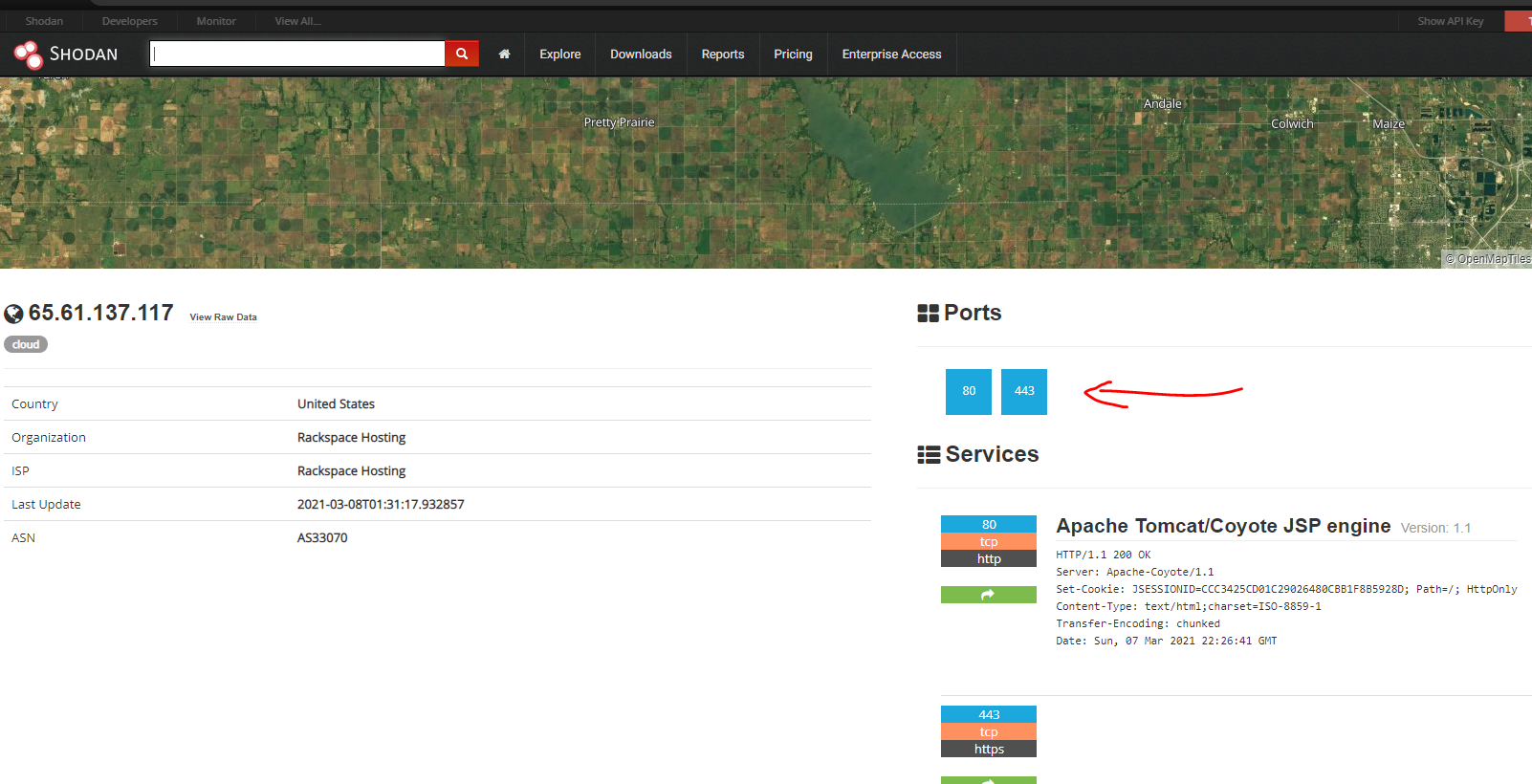
1. Where is the company located: **Sunnyvale CA**
2. What is the NetRange IP address: **65.61.137.64 - 65.61.137.127**
3. What is the company they use to store their infrastructure: **Rackspace Backbone Engineering**
4. What is the IP address of the DNS server: **65.61.137.117**

|  |  |
| --- | --- |
|  |  |
|  |  |

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

* What open ports and running services did Shodan find: **Ports 80 and 443**

The command **shodan.io 65.61.137.117**

****

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

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

Command **modules search** to confirm if the module xssed is already installed

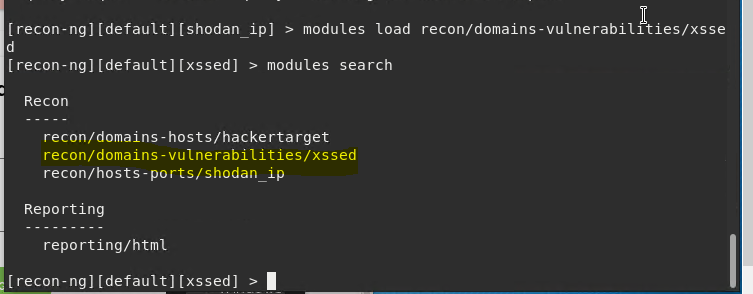
Command **marketplace install xssed** to install the recon module xssed

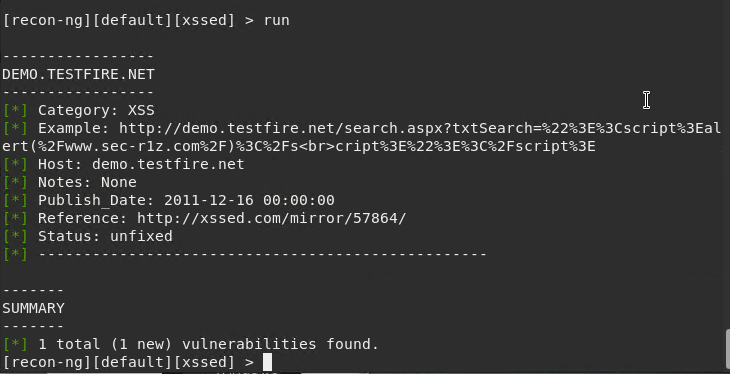
Run **options set SOURCE demo.testfire.net** to set the source as as demo.testfire.net

Command **modules load recon/domains-vulnerabilities/xssed** this will change the directory

Command **info** will display result of change

Command **exploit or run** will run the module





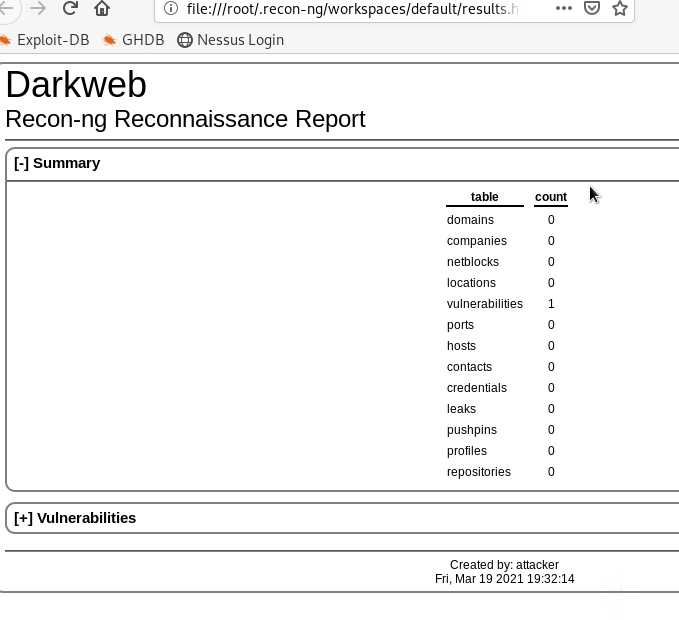
The result of the output is stored in a file following the below steps

**Modules load reporting/html**

**Set creator to attacker and customer as Darkweb**

**Use the command run to save the output in a file**

**To read the file use the syntax xdg-open /root/.recon-ng/workspaces/default/results.html**



Is Altoro Mutual vulnerable to XSS: **Yes.** **The output shows it has one vulnerability**

### **Step 5: Zenmap**

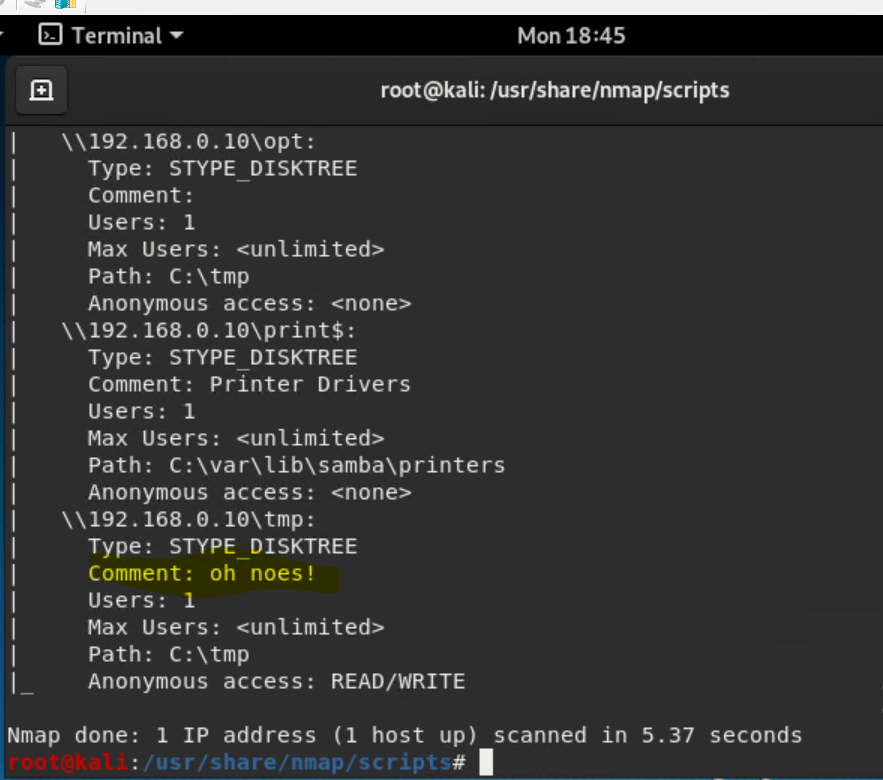
Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

* 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 zenmap.txt 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.

The service running on both ports is **Samba smbd 3.X version**, and in order to identify the vulnerability associated to both ports using the Zenmap scripting engine; **in the usr/share/nmap/scripts/ directory use the command nmap --script - smb-enum-shares.nse 192.168.0.10**



* Once you have identified this vulnerability, answer the following questions for your client:  
  1. What is the vulnerability: **anonymous users has read and write access to the sumba shares**
  2. Why is it dangerous: **they can access company’s files and make changes to them.**
  3. What mitigation strategies can you recommend for the client to protect their server: **disable anonymous access, and patch the server.**