## **Penetration Testing 1**

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

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

**Karl Fitzgerald - CEO**

* How can this information be helpful to an attacker:

**An attacker can use this information through social engineering by manipulating and deceiving employees that work for Altoro Mutual. Also an attacker user can use this information to send phishing emails.**

#### **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**

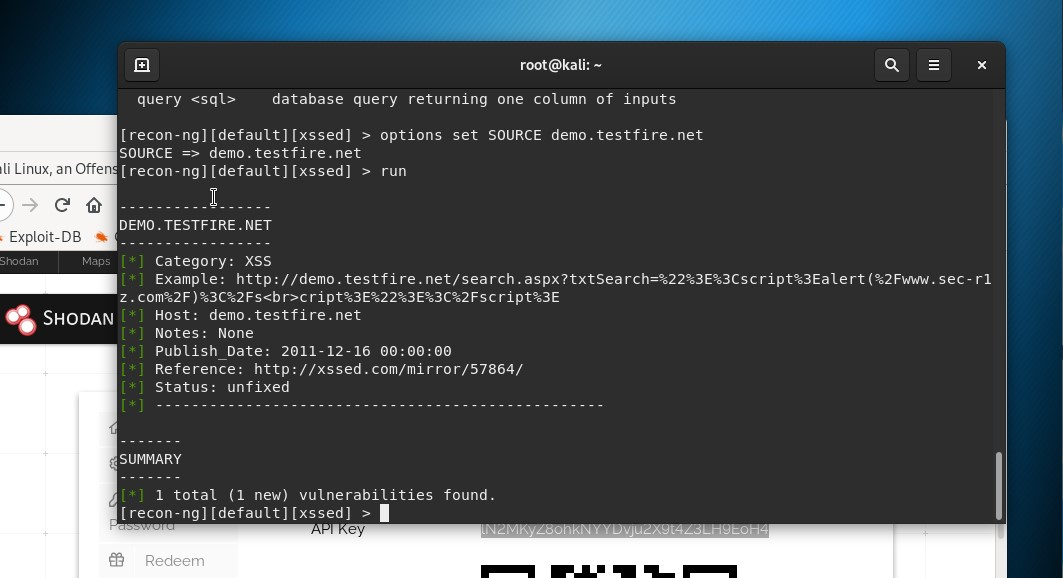
* What open ports and running services did Shodan find:

**Open ports: 80, 443, 8080 (Apache Tomcat/Coyote JSP engine 1.1)**

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

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

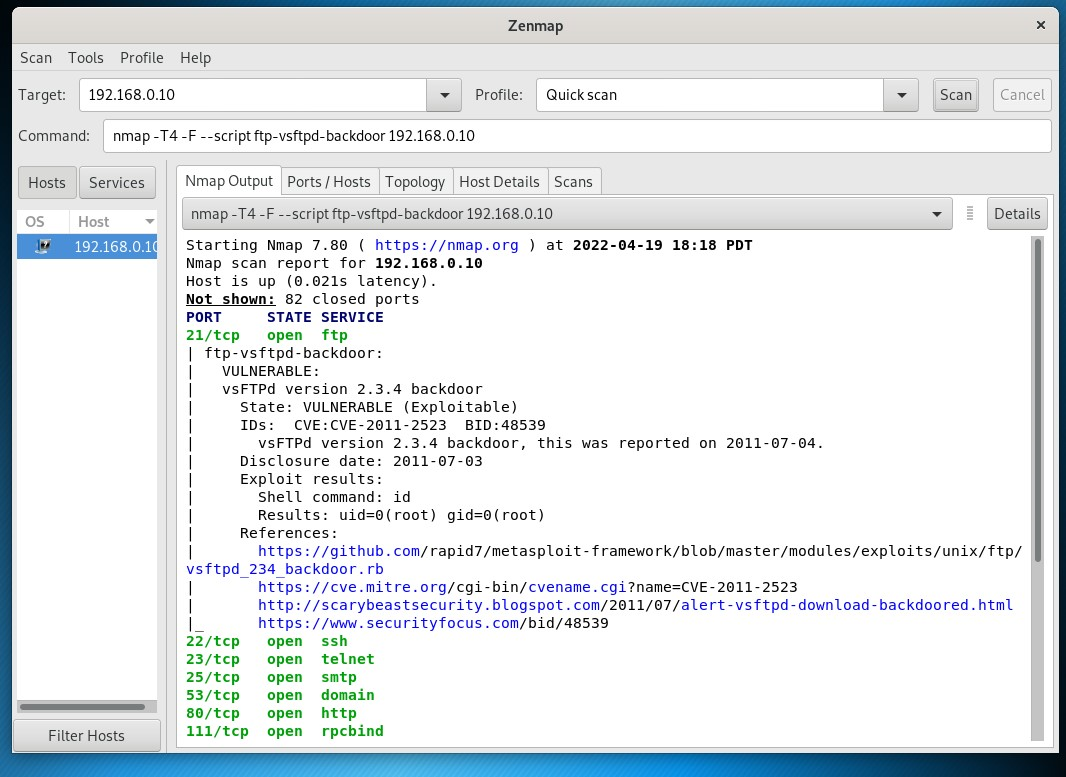
Is Altoro Mutual vulnerable to XSS: **Yes it is vulnerable.**

****

### **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:
* Bonus command to output results into a new text file named zenmapscan.txt:
* Zenmap vulnerability script command:



* Once you have identified this vulnerability, answer the following questions for your client:  
  1. What is the vulnerability: **CVE-2011-2523**
  2. Why is it dangerous: **This type of vulnerability contains a backdoor which opens a shell on port 6200/tcp. CIA is impacted: Integrity – there is total information disclosure, resulting in all system files being revealed; Availability - there is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised; Availability - There is a total shutdown. The attacker can render the resource completely unavailable.**
  3. What mitigation strategies can you recommendations for the client to protect their server:

f vsftpd 2.3.4 was downloaded between the 30th of June 2011 and the 3rd of July 2011, the new version has to be downloaded:

<https://security.appspot.com/downloads/vsftpd-2.3.4.tar.gz>

<https://security.appspot.com/downloads/vsftpd-2.3.4.tar.gz.asc>

Reference:

<https://www.cvedetails.com/>

https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805