## **Week 16 Homework Submission File: PenetrationTesting1**

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

* Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is: Karl Fitzgerald
* How can this information be helpful to an attacker: knowing who you are attacking,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:
* 80: Apache Tomcat/Coyote JSP engine
* 443: Apache Tomcat/Coyote JSP engine
* 8080: Apache Tomcat/Coyote JSP engine
* 8443: : Apache Tomcat/Coyote JSP engine

#### **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. Status is unfixed

### **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 192.168.0.10 -oN zenmapscan.txt
* Zenmap vulnerability script command: nmap --script smb-enum-shares -p139,445 192.168.0.10
* Once you have identified this vulnerability, answer the following questions for your client:  
  1. What is the vulnerability: Users don't have the right privileges.
  2. Why is it dangerous: They can write and execute dangeers commands that can harm the system.
  3. What mitigation strategies can you recommend for the client to protect their server: Keep updating SAMBA.