**## Week 16 Homework Submission File: Penetration Testing 1**

**#### 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 things like the CEO name an attacker could create emails to look like they are from them but are malicious emails to hack into the system.

**#### 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:

65.61.137.64/26

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, 443, 8080

**#### 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, there is 1 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 192.168.0.8

- Bonus command to output results into a new text file named `zenmapscan.txt`:

- Zenmap vulnerability script command: nmap -T4 -A -v 192.168.0.8

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

1. What is the vulnerability: They have open tcp port 22

2. Why is it dangerous: This allows attackers to get into into the system and possibly take over certain systems or get information

3. What mitigation strategies can you recommendations for the client to protect their server: I would suggest closing port 22