Arctos Morei  
  
## 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:

The attacker now has a name and can do recon on the CEO, as well as know who to start targeting for phishing/whaling.

#### 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: Per Domain Whois record – 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: 117.137.61.65.in-addr.arpa

#### Step 3: Shodan

- What open ports and running services did Shodan find:

I couldn’t get anything to show up in Shodan?? I tried multiple IP’s too but kept getting the same result.   
Table

Description automatically generated

#### 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:

Ye

### 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: (we mostly used nmap in class, so that’s what I’ll be using instead of Zenmap.) Metasploitable machine is 192.168.0.10. So the command will be nmap -Ss 192.168.0.10

- Bonus command to output results into a new text file named `zenmapscan.txt`:  
After nmap -sS, you would add the -oN switch with the desired filename zenmapscan.txt afterwards.

- Zenmap vulnerability script command: nmap -sV -sC -p (specify a port, such as 6667) 192.168.0.10

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

1. What is the vulnerability:

For the example above, Port 6667 is open and allows irc traffic.

2. Why is it dangerous:

This is a very outdated and thus easily exploitable backdoor to download malicious software.

3. What mitigation strategies can you recommendations for the client to protect their server:

Consider why irc is still in use, and if it’s necessary for this system. If not, I would recommend disabling irc.