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: 65.61.137.117

#### Step 3: Shodan

- What open ports and running services did Shodan find:

Open Ports – 80 / TCP, 443 / TCP, 8080 / TCP

Running Services – 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:

Text

Description automatically generated

Ye, it’s susceptible to XSS.

### 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-T4 -F 192.168.0.10

- Bonus command to output results into a new text file named `zenmapscan.txt`:  
Add the -oN switch with the desired filename (zenmapscan.txt) afterwards.

- Zenmap vulnerability script command:

nmap-T4 -F –script ftp-vsftpd-backdoor,smb-enum-shares 192.168.0.10

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

1. What is the vulnerability:  
CVE-2011-2523

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

2. Why is it dangerous:

This is a very dangerous exploit, rated 9.8 in severity because the backdoor on port 21/tcp can be used to open a shell on port 6200/tcp.

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

Use the most updated version of vsFPTd to prevent this exploit from happening, as this one affects v 2.3.4