**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:

**This would be part of the reconnaissance phase so an attacker would be able to target Karl specifically with something like phishing.**

**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: **San Antonio TX**
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: **akam.net**
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:

**The open ports are 80, 443 and 8080 running Apache Tomcat/Coyote JSP engine 1.1 in text/html format**

**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**

**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 -oN zenmapscan.txt --script smb-enum-shares 192.168.0.10**

Zenmap vulnerability script command:

**nmap --script 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: **Anonymous users have read/write access to their SAMBA shares.**
  2. Why is it dangerous: **Anonymous users can access company files and change them.**
  3. What mitigation strategies can you recommendations for the client to protect their server: **Update their SAMBA server to the newest version and to disable anonymous access.**