**Week 16 Homework: Penetration Testing 1**

**Step 1: Google Dorking**

* Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is: Karl Fitzgerald Chairman & **Chief Executive Officer Altoro Mutua**
* How can this information be helpful to an attacker: This can help an attacker do a social engineering campaign.

**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: Apache-Coyote
4. What is the IP address of the DNS server: ASIA3.AKAM.NET

**Step 3: Shodan**

* What open ports and running services did Shodan find: 80,443

**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 -p 139,445 -T4 -A -v 192.168.0.10
* Bonus command to output results into a new text file named **zenmapscan.txt**: -oN /tmp/zenmapscan.txt
* Zenmap vulnerability script command: --script smb-os-discovery,smb-vuln-cve-2017-7494,smb-vuln-cve2009-3103
* Once you have identified this vulnerability, answer the following questions for your client:
  1. What is the vulnerability: Detects Microsoft Windows systems vulnerable to denial of service
  2. Why is it dangerous: Can take the server off line
  3. What mitigation strategies can you recommendations for the client to protect their server: Keep up with patches, do not expose the server to the internet, and filter out 445 and 139 port requests