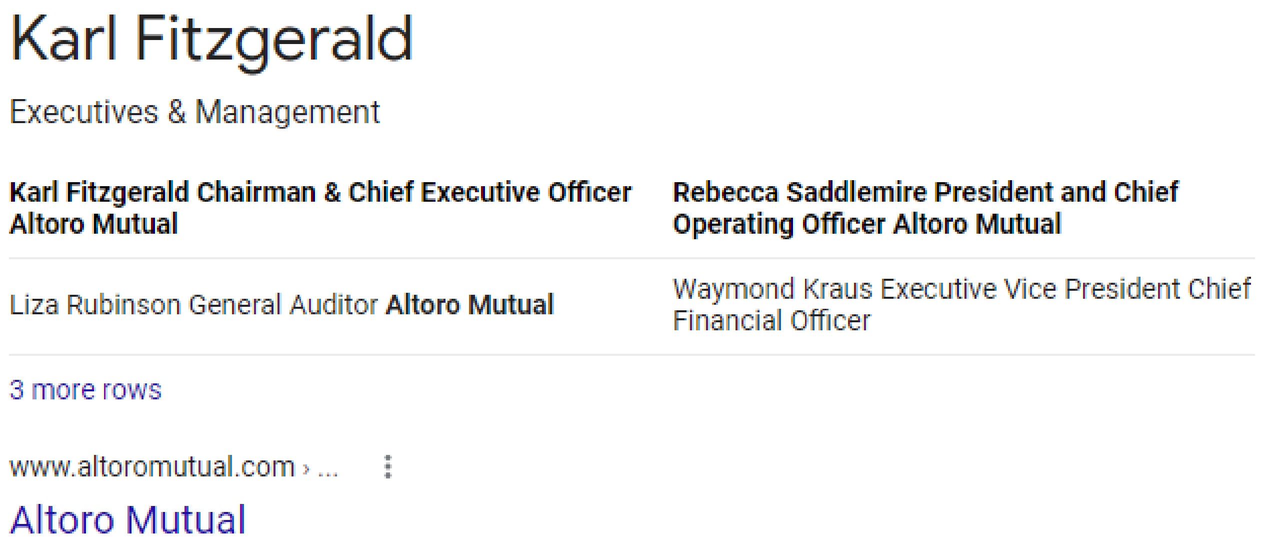
Week 16 Homework Submission File: Penetration Testing 1

Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:



Karl Fitzgerald

Executives & Management

Karl Fitzgerald Chairman & Chief Executive Officer Altoro Mutual	**Rebecca Saddlemire President and Chief Operating Officer Altoro Mutual**
Liza Rubinson General Auditor **Altoro Mutual**	Waymond Kraus Executive Vice President Chief Financial Officer

3 more rows

www.altoromutual.com › ...

Altoro Mutual

- How can this information be helpful to an attacker: **Found during Recon, can be a target of a whaling attack**

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: **`Registrant City: Sunnyvale, Registrant State/Province: CA, Registrant Postal Code: 94085, Registrant Country: US`**

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, Address:9725 Datapoint Drive, Suite 100, City:San Antonio, StateProv:TX, PostalCode:78229`**

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: **Ports: 80, 443, running 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: **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

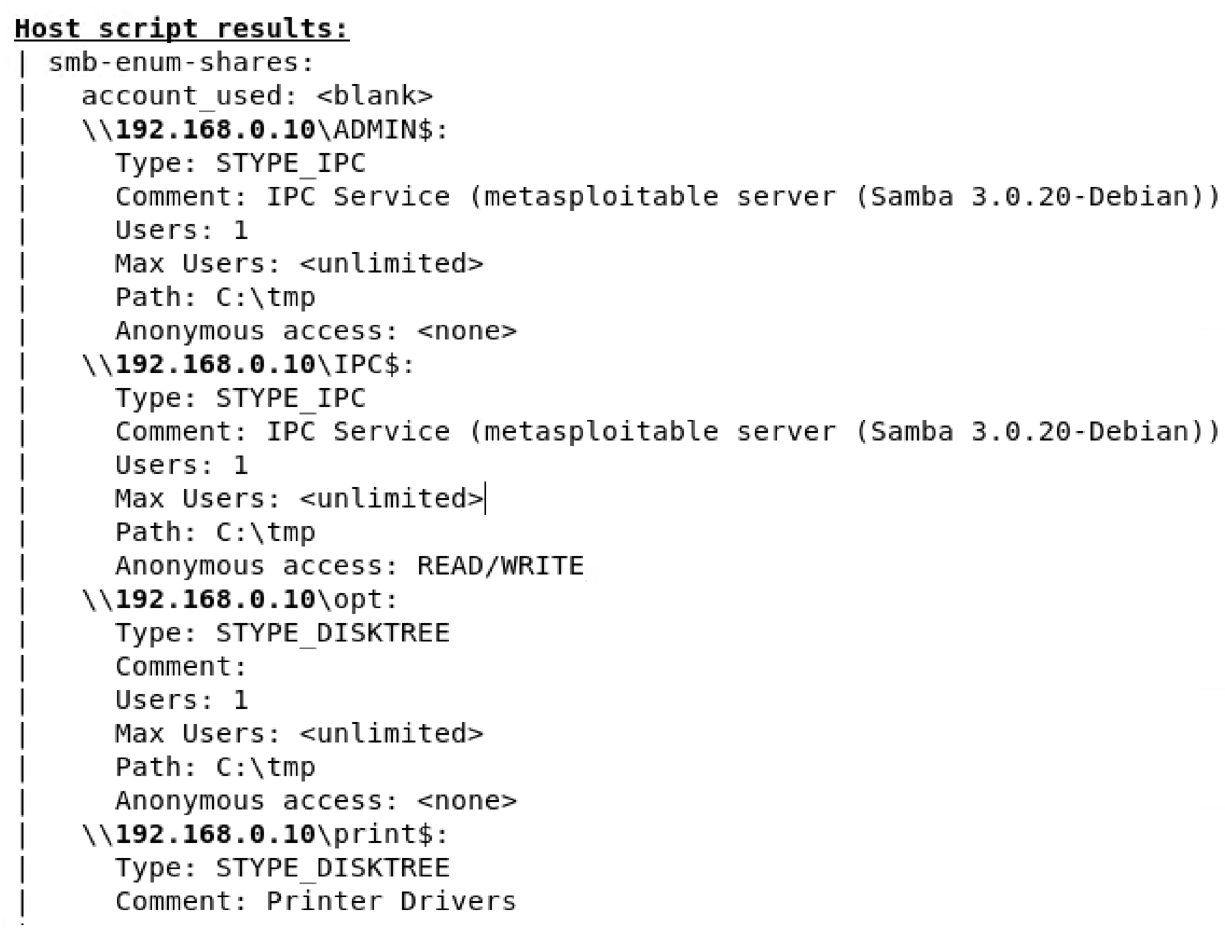
- Bonus command to output results into a new text file named zenmapscan.txt:
  nmap -sV -oN zenmapscan.txt --script smb-enum-shares 192.168.0.10

- Zenmap vulnerability script command:

  Nmap -sV --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:
     Gives attacker READ/WRITE ACCESS



```
Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.0.10\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.0.10\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.0.10\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.0.10\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
```

2. Why is it dangerous: **it gives an attacker the ability to manipulate files and change them**

3. What mitigation strategies can you recommendations for the client to protect their server: **restrict access to server through only(close as many ports as possible to keep secure) SECURE SHELL or port 22, require difficult login credentials and not allow a user to have root privileges as soon as they login, have a separate login for root access. Another thing would be to regularly update the server and patch security updates while disabling anonymous access.**