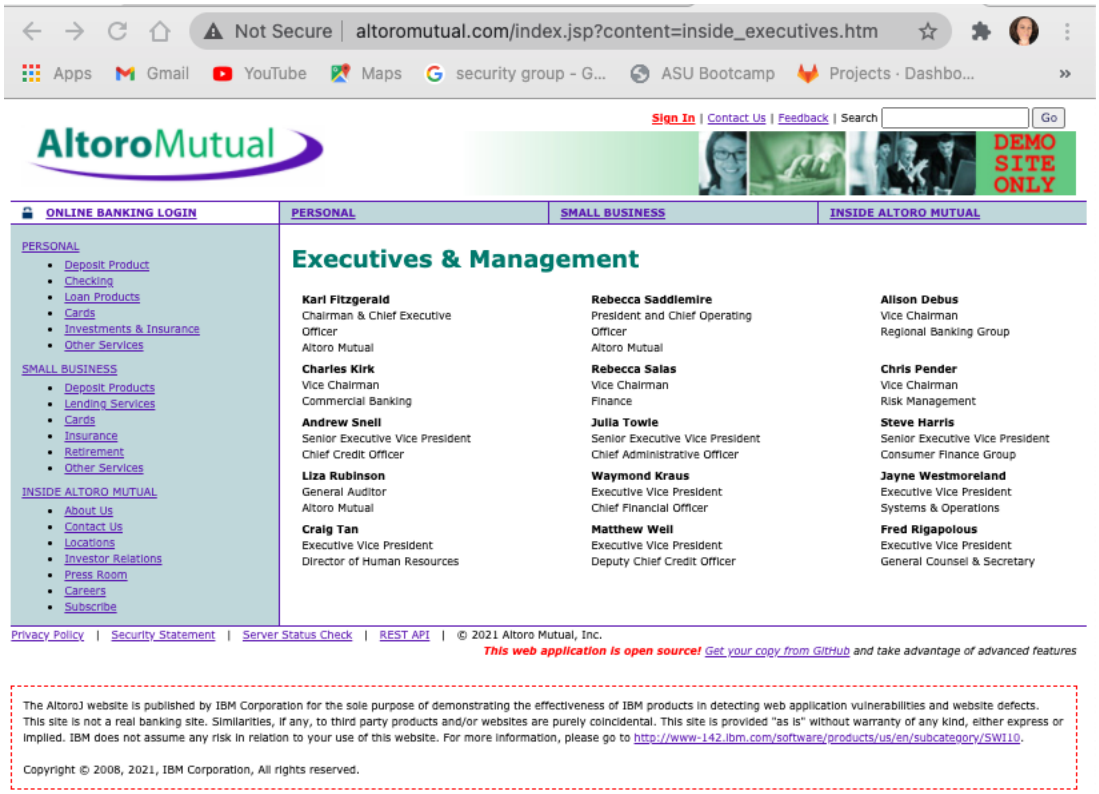
# Week 16 Homework: Penetration Testing 1

## Step 1: Google Dorking

Altoro Mutual wants to ensure that private information that is unavailable on their public website cannot be found by searching the web.

- For example, Altoro Mutual does not mention their executive remembers on the website. Using Google, can you identify who the Chief Executive Officer?




- How can this information be helpful to an attacker?

Google Dorking is a search technique that enables hackers to gain access to information that corporations and individuals did not intend to make publicly available. Using this technique, hackers are able to identify vulnerable systems and can recover usernames, passwords, email addresses, and even credit card details.

https://www.mcafee.com/blogs/enterprise/google-dorking/#:~:text=Google%20Dorking%20is%20a%20search,and%20even%20credit%20card%20details.

## Step 2: DNS and Domain Discovery

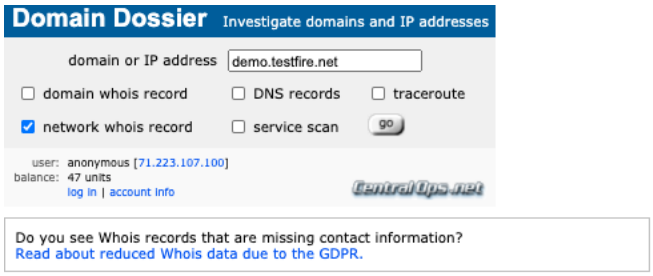
The reconnaissance phase of a penetration test is possibly the most important phase of the engagement. Without a clear understanding of your client's assets, vulnerabilities can go unnoticed and later exploited.

- Navigate to centralops.net.
- 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?

Queried **whois.corporatedomains.com** with "**testfire.net**"...

```
Domain Name: testfire.net
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-02T11:59:50Z
Creation Date: 1999-07-23T09:52:32.000-04:00
Registrar Registration Expiration Date: 2021-07-23T13:52:32.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Sunnyvale
Registrant State/Province: CA
```

2. What is the NetRange IP address?

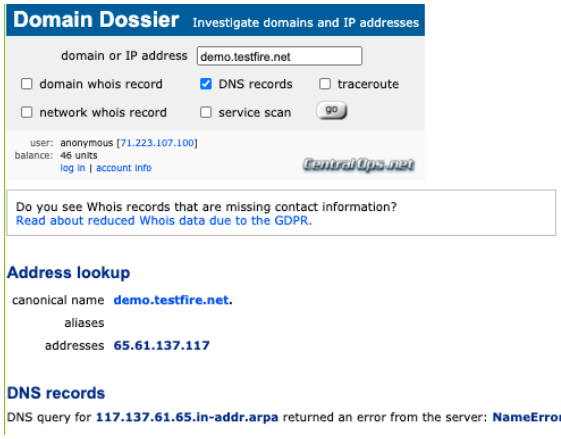



3. What is the company they use to store their infrastructure?

```
CustName:       Rackspace Backbone Engineering
Address:        9725 Datapoint Drive, Suite 100
City:           San Antonio
StateProv:      TX
PostalCode:     78229
Country:        US
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/entity/C05762718
```

## Underlying infrastructure in IT

4. What is the IP address of the DNS server?

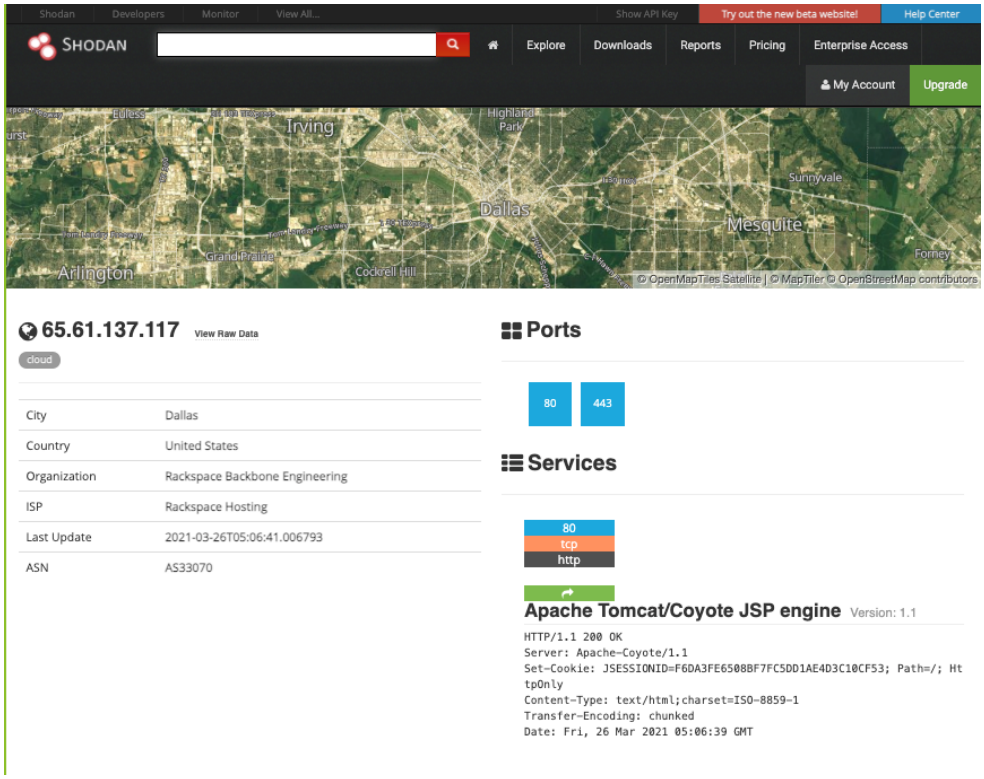


DNS is where it will query and DNS servers will change so wasn't sure if this is not right

## Step 3: Shodan

Using Shodan and the information gathered from Google Dorking, find any other useful information that can be used in an attack.

- Navigate to shodan.io.
- Run a scan against the IP address of the DNS server for demo.testfire.net.
    - What open ports and running services did Shodan find?




Looking for version # for published exploits https://www.exploit-db.com/exploits/43008

## Step 4: Recon-ng

Altoro Mutual is also concerned about cross-site scripting attacks, which can cause havoc on their website. Verify whether or not Altoro Mutual is vulnerable to XSS by completing the following:

- Install the Recon module xssed.

```
[recon-ng][default] > marketplace install xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See 'keys add'.
[recon-ng][default] > modules load xssed
[recon-ng][default][xssed] >
```

- Set the source to demo.testfire.net.

```
[recon-ng][default][xssed] > info

      Name: XSSed Domain Lookup
    Author: Micah Hoffman (@WebBreacher)
   Version: 1.1

Description:
  Checks XSSed.com for XSS records associated with a domain and displays the fir
st 20 results.

Options:
  Name    Current Value      Required  Description
  ------  -------------      --------  -----------
  SOURCE  demo.testfire.net  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

- Run the module.

```
[recon-ng][default][xssed] > run

-----------------
DEMO.TESTFIRE.NET
-----------------
[*] Category: XSS
[*] Example: http://demo.testfire.net/search.aspx?txtSearch=%22%3E%3Cscript%3Eal
ert(%2Fwww.sec-r1z.com%2F)%3C%2Fs<br>cript%3E%22%3E%3C%2Fscript%3E
[*] Host: demo.testfire.net
[*] Notes: None
[*] Publish_Date: 2011-12-16 00:00:00
[*] Reference: http://xssed.com/mirror/57864/
[*] Status: unfixed
[*] ---------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (1 new) vulnerabilities found.
[recon-ng][default][xssed] >
```


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

- Is Altoro Mutual vulnerable to XSS?

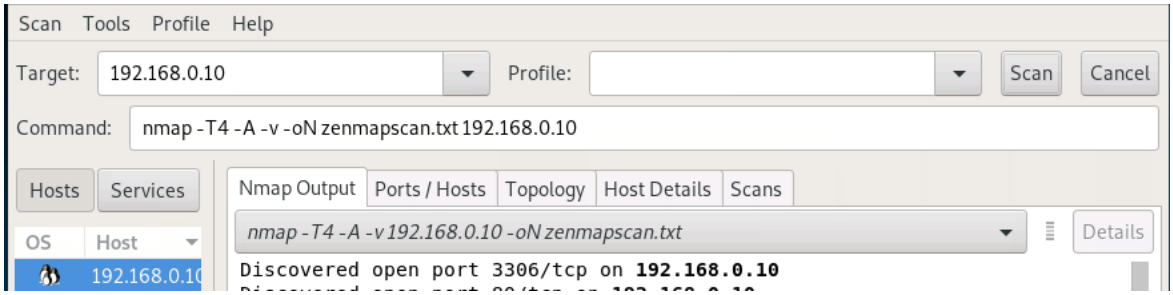
Yes!!

## 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:

- Use Zenmap to run a service scan against the Metasploitable machine.

```
86  ifconfig
87  nmap -F 192.168.0.0/24
88  nmap
```




```
NSE: Script Post-scanning.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.73 seconds
           Raw packets sent: 1292 (57.594KB) | Rcvd: 1017 (41.482KB)
```

  - **Bonus:** In the same command, output the results into a new text file named zenmapscan.txt.

```
root@kali:~# ls
Desktop    Downloads  Music     Public     version.txt  zenmapscan.txt
Documents  hack.exe   Pictures  Templates  Videos
```

- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.

```
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

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

    Samba smbd 3.X -4.X

    https://www.exploit-db.com/exploits/16320

    https://www.cvedetails.com/vulnerability-list/vendor_id-102/product_id-171/version_id-41384/Samba-Samba-3.0.20.html

- Why is it dangerous?

This exploit triggers a heap overflow in the Samba dameon, specifically in the SMB which is the Server Message Block which is a protocol for sharing files, printers, serial ports and data on a network. In essence the way computers talk to one another. These ports need to remain secure, however, it is ok to leave them open because they are necessary for communication across the internet so they need remain secure including making sure they are configured correctly, patched when necessary, strict security rules in place and monitored frequently to avoid exploits.

https://www.upguard.com/blog/smb-port

- What are your recommendations for the client to protect their server?

These ports need to remain secure and open as they are necessary for communication across the internet. Therefore, my recommendations for the client is to keep them secure by making sure they are configured correctly, patched when necessary, strict security rules put into place and monitored frequently to avoid exploits.