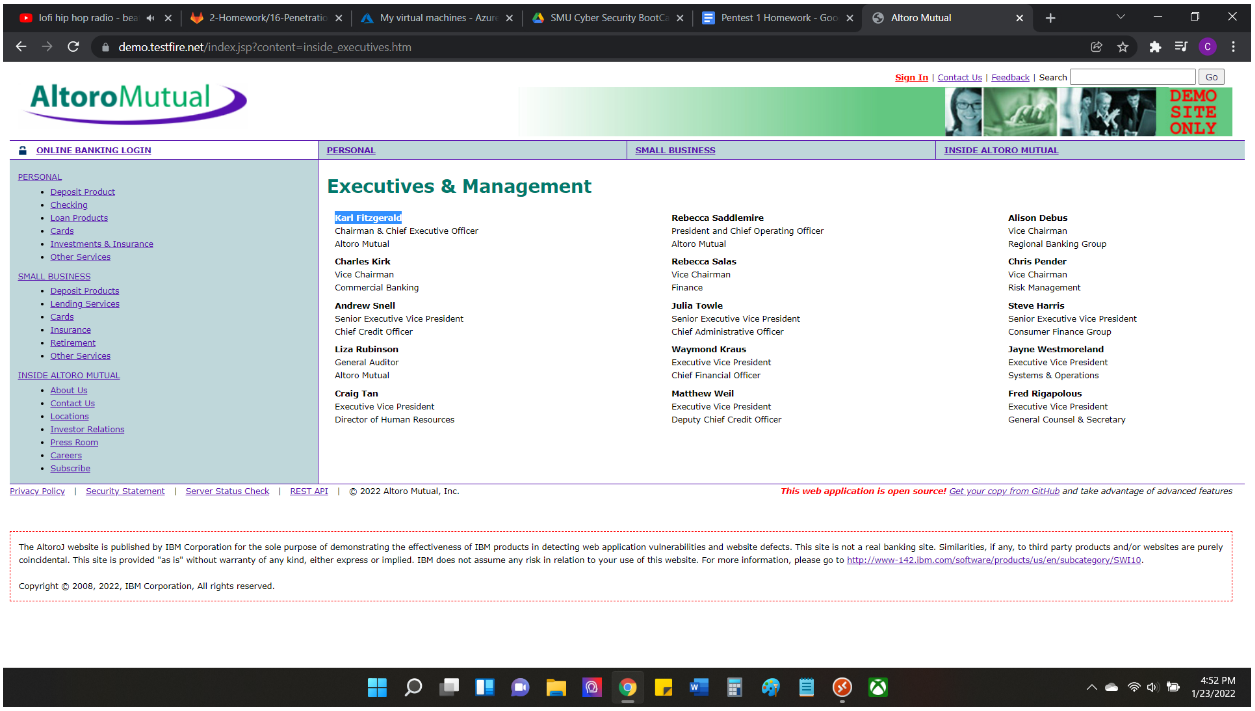
Step 1: Google Dorking

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?
    - Karl Fitzgerald is the Chief Executive Officer.



PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Executives & Management

Karl Fitzgerald
Chairman & Chief Executive Officer
Altoro Mutual

Charles Kirk
Vice Chairman
Commercial Banking

Andrew Snell
Senior Executive Vice President
Chief Credit Officer

Liza Rubinson
General Auditor
Altoro Mutual

Craig Tan
Executive Vice President
Director of Human Resources

Rebecca Saddlemire
President and Chief Operating Officer
Altoro Mutual

Rebecca Salas
Vice Chairman
Finance

Julia Towle
Senior Executive Vice President
Chief Administrative Officer

Waymond Kraus
Executive Vice President
Chief Financial Officer

Matthew Weil
Executive Vice President
Deputy Chief Credit Officer

Alison Debus
Vice Chairman
Regional Banking Group

Chris Pender
Vice Chairman
Risk Management

Steve Harris
Senior Executive Vice President
Consumer Finance Group

Jayne Westmoreland
Executive Vice President
Systems & Operations

Fred Rigapolous
Executive Vice President
General Counsel & Secretary

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

-

- How can this information be helpful to an attacker?
    - An Attacker can use this information to start a phishing attack letting the email look similar to the Chiefs name.

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?

        - Admin City: Sunnyvale
        - Admin State/Province: CA
        - Admin Postal Code: 94085
        - Admin 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?
    - 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

4. What is the IP address of the DNS server?
    - 65.61.137.117

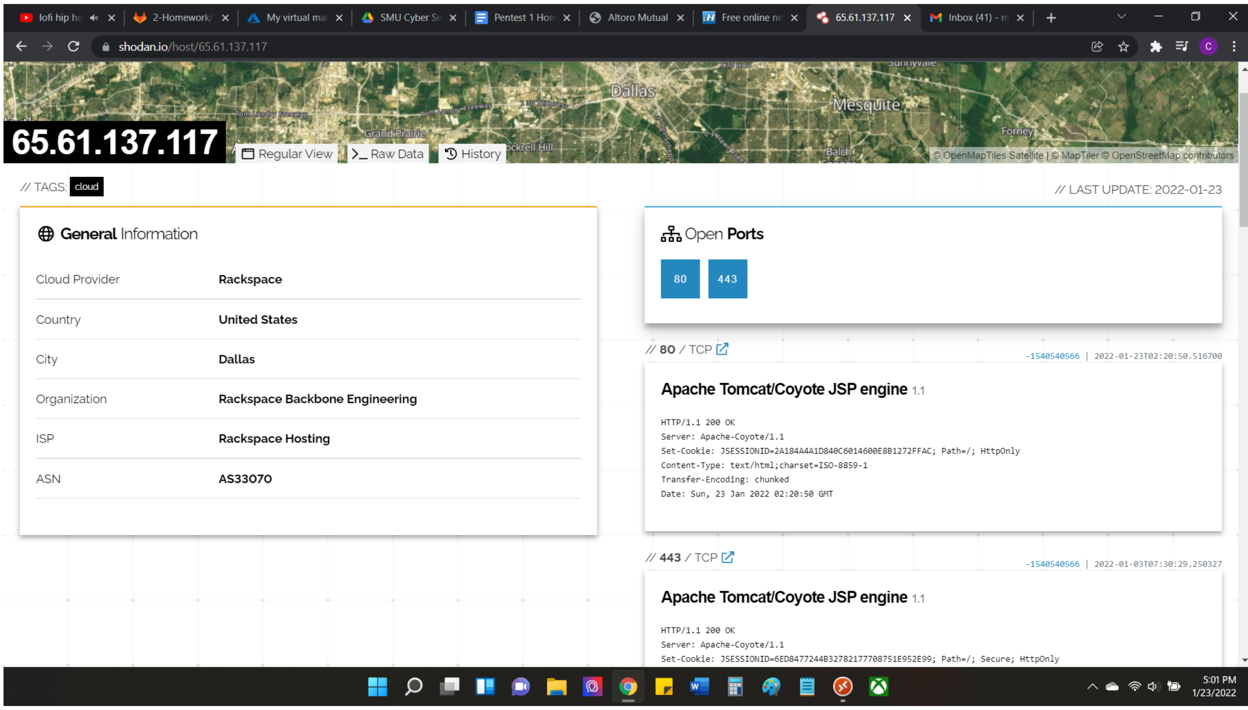
Step 3: Shodan

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?
        - 80, 443 Screenshot below.



65.61.137.117

// TAGS: cloud

// LAST UPDATE: 2022-01-23

General Information

Cloud Provider	**Rackspace**
Country	**United States**
City	**Dallas**
Organization	**Rackspace Backbone Engineering**
ISP	**Rackspace Hosting**
ASN	**AS33070**

Open **Ports**

80 443

// **80** / TCP

-1540540566 | 2022-01-23T02:20:50.516700

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=2A184A4A1D840C6014600E8B1272FFAC; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 23 Jan 2022 02:20:50 GMT
```

// **443** / TCP

-1540540566 | 2022-01-03T07:30:29.250327

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6ED8477244B32782177708751E952E99; Path=/; Secure; HttpOnly
```

○

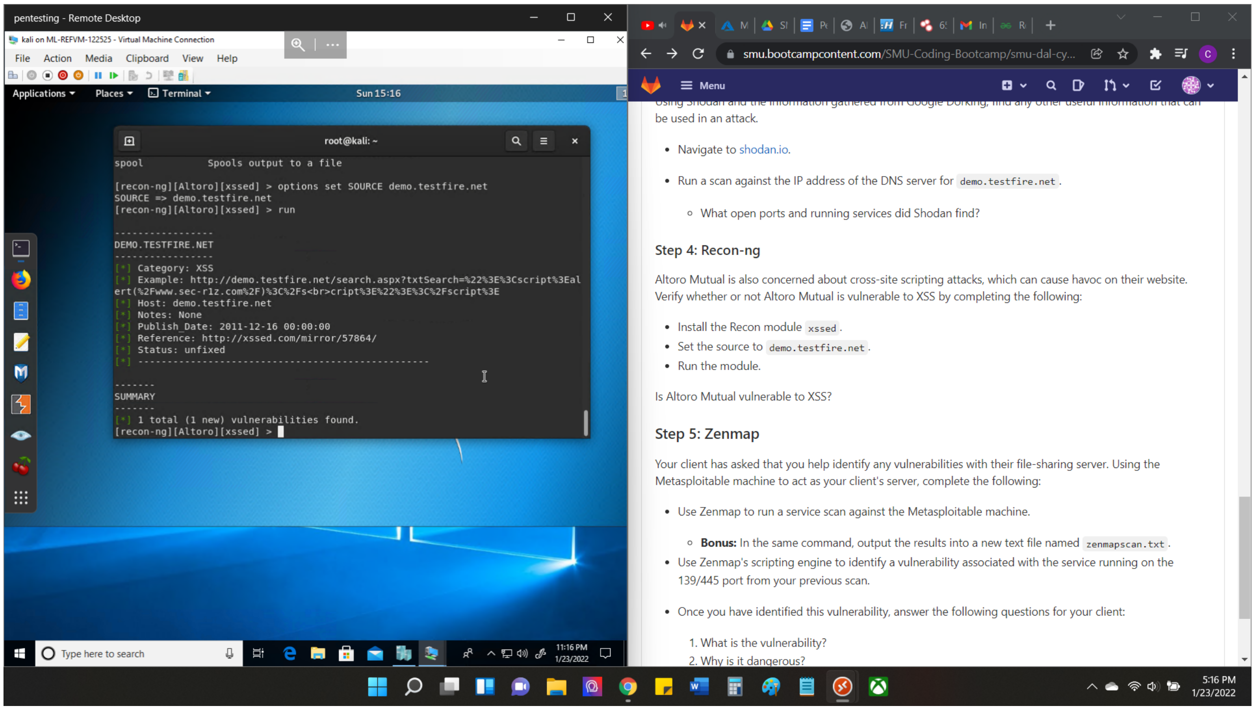
Step 4: Recon-ng

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.
- Set the source to demo.testfire.net.
- Run the module.

Is Altoro Mutual vulnerable to XSS?

Yes Altoro Mutual is vulnerable to XSS. Screenshot below.


pentesting - Remote Desktop
kali on ML-REFVM-122525 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Applications
Places
Terminal
Sun 15:16
root@kali: ~
Type here to search
11:16 PM
1/23/2022
smu.bootcampcontent.com/SMU-Coding-Bootcamp/smu-dal-cy...
Menu
5:16 PM
1/23/2022

```
spool            Spools output to a file

[recon-ng][Altoro][xssed] > options set SOURCE demo.testfire.net
SOURCE => demo.testfire.net
[recon-ng][Altoro][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][Altoro][xssed] >
```

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?

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`.
- Set the source to `demo.testfire.net`.
- Run the module.

Is Altoro Mutual vulnerable 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:

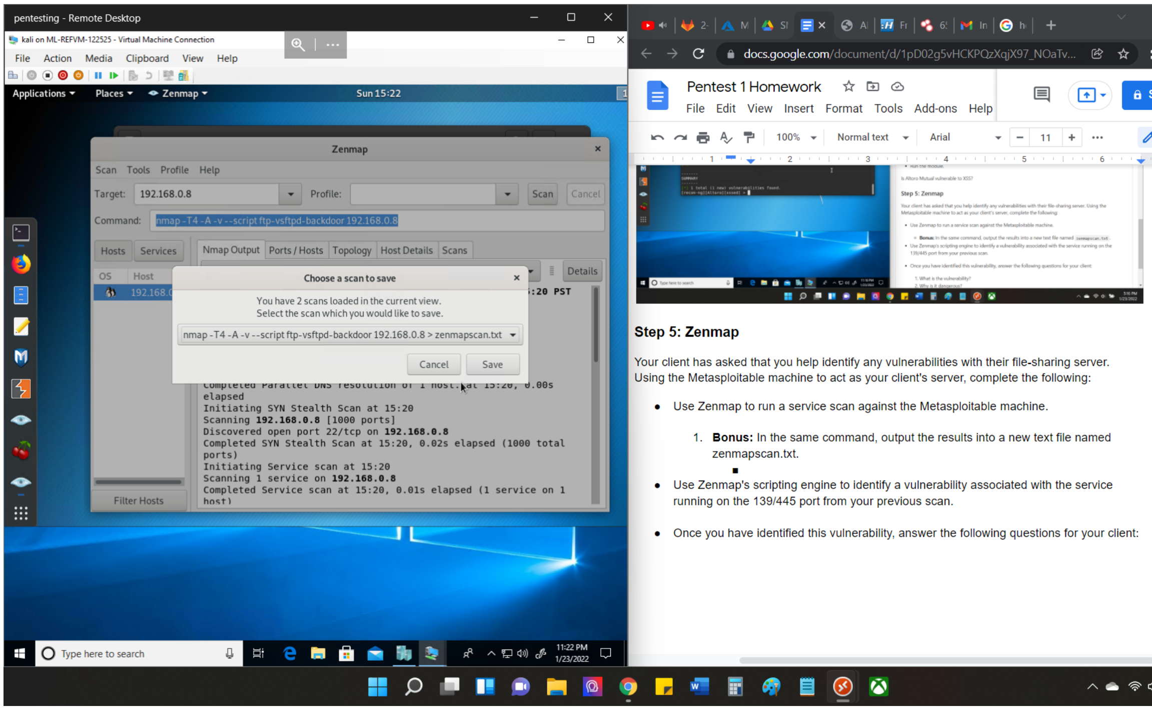
- Use Zenmap to run a service scan against the Metasploitable machine.
  - **Bonus:** In the same command, output the results into a new text file named `zenmapscan.txt`.
- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.
- Once you have identified this vulnerability, answer the following questions for your client:
  1. What is the vulnerability?
  2. Why is it dangerous?

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.

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



pentesting - Remote Desktop

kali on ML-REFVM-122525 - Virtual Machine Connection

Target: 192.168.0.8

Profile:

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.0.8

Choose a scan to save

You have 2 scans loaded in the current view.
Select the scan which you would like to save.

nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.0.8 > zenmapscan.txt

Cancel | Save

```
Completed Parallel DNS resolution of 1 host. at 15:20, 0.00s
elapsed
Initiating SYN Stealth Scan at 15:20
Scanning 192.168.0.8 [1000 ports]
Discovered open port 22/tcp on 192.168.0.8
Completed SYN Stealth Scan at 15:20, 0.02s elapsed (1000 total
ports)
Initiating Service scan at 15:20
Scanning 1 service on 192.168.0.8
Completed Service scan at 15:20, 0.01s elapsed (1 service on 1
host)
```

docs.google.com/document/d/1pD02g5vHCKPQzXqjX97_NOaTv...

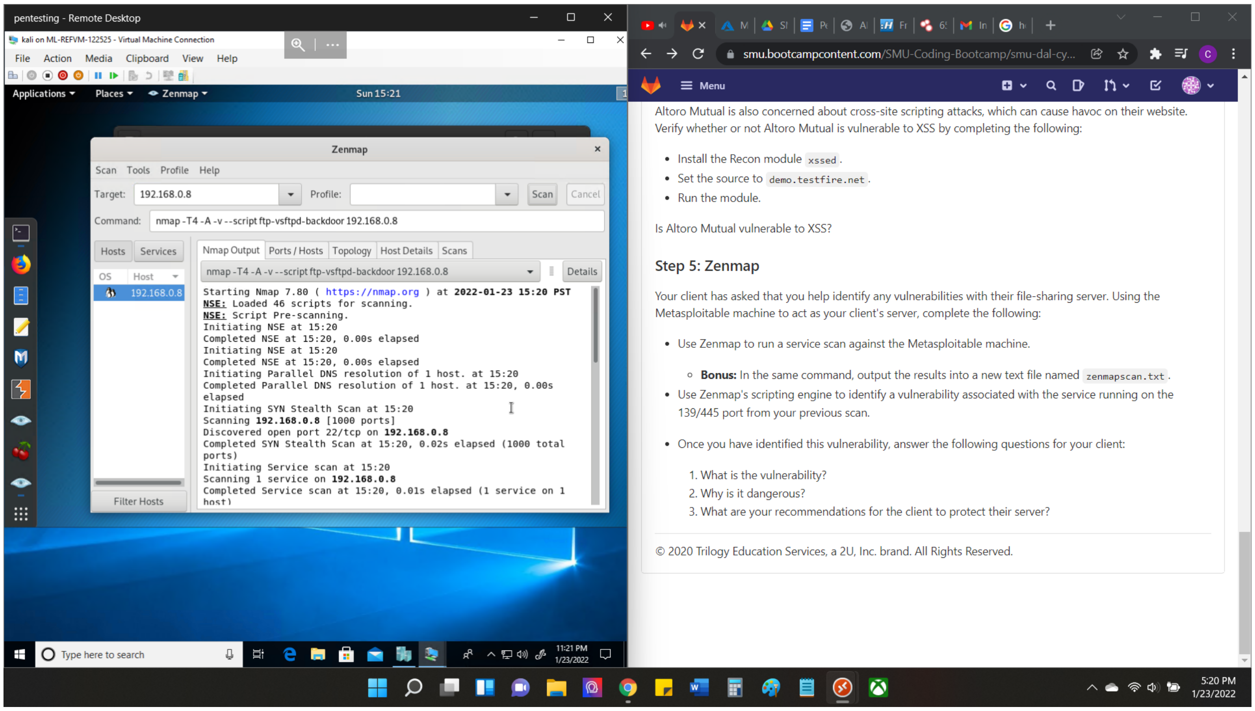
Step 5: Zenmap

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.
    1. **Bonus:** In the same command, output the results into a new text file named zenmapscan.txt.
- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.
- Once you have identified this vulnerability, answer the following questions for your client:

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

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



pentesting - Remote Desktop

kali on ML-REFVM-122525 - Virtual Machine Connection

Target: 192.168.0.8

Profile:

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.0.8

nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.0.8

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-23 15:20 PST
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:20
Completed NSE at 15:20, 0.00s elapsed
Initiating NSE at 15:20
Completed NSE at 15:20, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:20
Completed Parallel DNS resolution of 1 host. at 15:20, 0.00s
elapsed
Initiating SYN Stealth Scan at 15:20
Scanning 192.168.0.8 [1000 ports]
Discovered open port 22/tcp on 192.168.0.8
Completed SYN Stealth Scan at 15:20, 0.02s elapsed (1000 total
ports)
Initiating Service scan at 15:20
Scanning 1 service on 192.168.0.8
Completed Service scan at 15:20, 0.01s elapsed (1 service on 1
host)
```

smu.bootcampcontent.com/SMU-Coding-Bootcamp/smu-dal-cy...

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`.
- Set the source to `demo.testfire.net`.
- Run the module.

Is Altoro Mutual vulnerable 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:

- Use Zenmap to run a service scan against the Metasploitable machine.
    - **Bonus:** In the same command, output the results into a new text file named `zenmapscan.txt`.
- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.
- Once you have identified this vulnerability, answer the following questions for your client:
    1. What is the vulnerability?
    2. Why is it dangerous?
    3. What are your recommendations for the client to protect their server?

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

1. What is the vulnerability?
    - Port 22 is

2. Why is it dangerous?
    - Port 22 is open and it used for remote access. If an attacker knows this port is open they can gain access to the system remotely and may disguise as one of the users on the system.
3. What are your recommendations for the client to protect their server?
    - Close the port and encrypt the access to the port to use it.