Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:
  - Used the following command:
    - site:demo.testfire.net ceo
  - Got the following result from "http://demo.testfire.net/index.jsp?content=inside_executives.htm" which was the top result in the Google search:
    - Karl Fitzgerald
- How can this information be helpful to an attacker:
  - Getting his name could make his company email easy to guess since most company emails follow the "<First Initial><Last Name>@<Domain>.com" format.
    - Getting his email could then make him the target of a "whaling phishing" attack.
    - Attackers could spoof his email and pose as him in emails to employees in order to use his position to get information from him.
  - Getting his name could lead to getting his home address which would make his home computer and/or home network a target.
  - Attackers could phone employees and say they're him and get information from them.

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:

- Where is the company located:
  - Sunnyvale, CA 94085, US
- What is the NetRange IP address:
  - 65.61.137.64 - 65.61.137.127
- What is the company they use to store their infrastructure:
  - Rackspace Backbone Engineering
- What is the IP address of the DNS server:

- I got the primary names server from the following Powershell command:

```
PS C:\Users\Justin> nslookup -type=ns demo.testfire.net
Server:  cdns01.comcast.net
Address:  75.75.75.75

testfire.net
        primary name server = asia3.akam.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1366025606
        refresh = 43200 (12 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

- I found the primary in the list displayed from "Domain Dossier":

testfire.net	IN	NS	eur2.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	ns1-206.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	ns1-99.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	usc3.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	usc2.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	asia3.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	usw2.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	eur5.akam.net	86400s (1.00:00:00)

- So, I decided to find the IP for only the primary instead of all eight name servers:

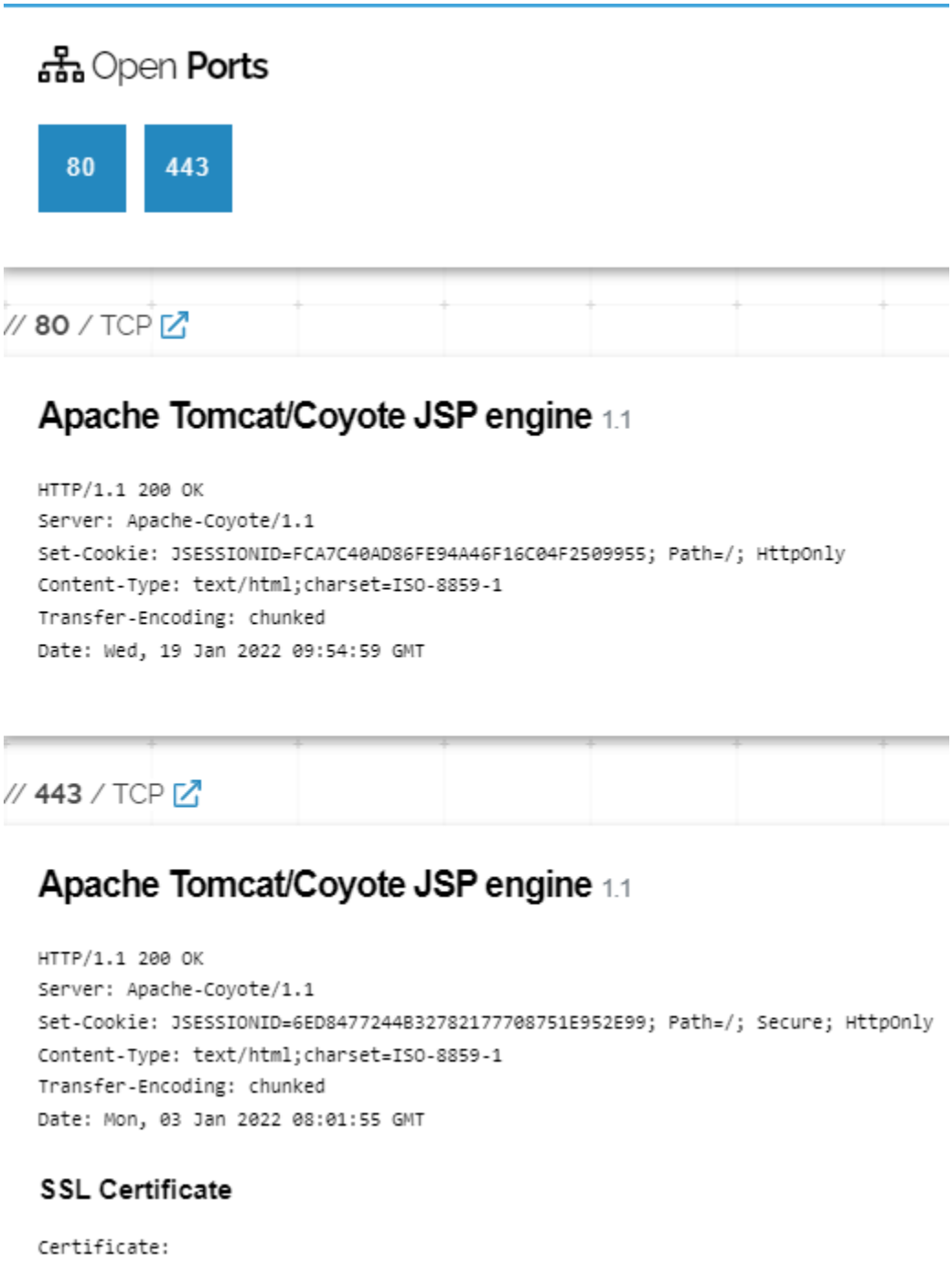
```
PS C:\Users\Justin> nslookup asia3.akam.net
Server:  cdns01.comcast.net
Address:  75.75.75.75

Non-authoritative answer:
Name:    asia3.akam.net
Address:  23.211.61.64
```

Step 3: Shodan

- What open ports and running services did Shodan find:

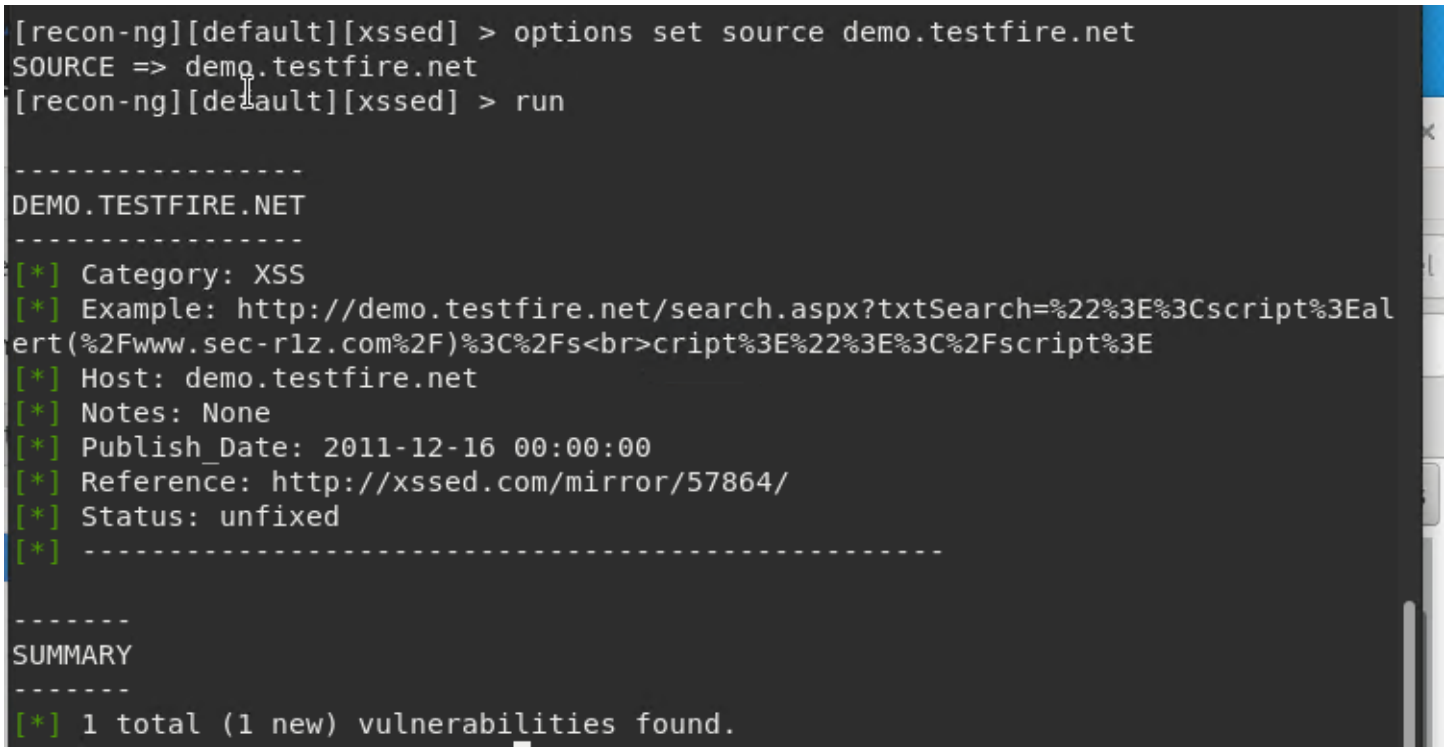
- Shodan showed HTTP and HTTPS running on ports 80 and 443 respectively:



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, according to “recon-ng”:



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 192.168.0.10
    - This will create the file in the logged in user's home directory.
- Zenmap vulnerability script command:
  - nmap -p 445 --script smb-enum-shares 192.168.0.10
    - Found the above script from "https://nmap.org/nsedoc/scripts/smb-enum-shares.html".
  - Keep in mind that I got the same results from the following:
    - nmap -p ***139*** --script smb-enum-shares 192.168.0.10
- Once you have identified this vulnerability, answer the following questions for your client:
  - What is the vulnerability:
    - The server is allowing anonymous read/write access on two shares – \IPC$ and \tmp.
  - Why is it dangerous:
    - Because they're allowing anonymous read/write access…

        - Any user can read any sensitive information on those shares.
        - Any user can modify anything – most likely destroy anything – in those two shares.
    - What mitigation strategies can you recommendations for the client to protect their server:
        - Configure the SMB services on those ports to NOT allow anonymous access to the set up shares. Or if the data isn't sensitive then at the very least don't allow write access.