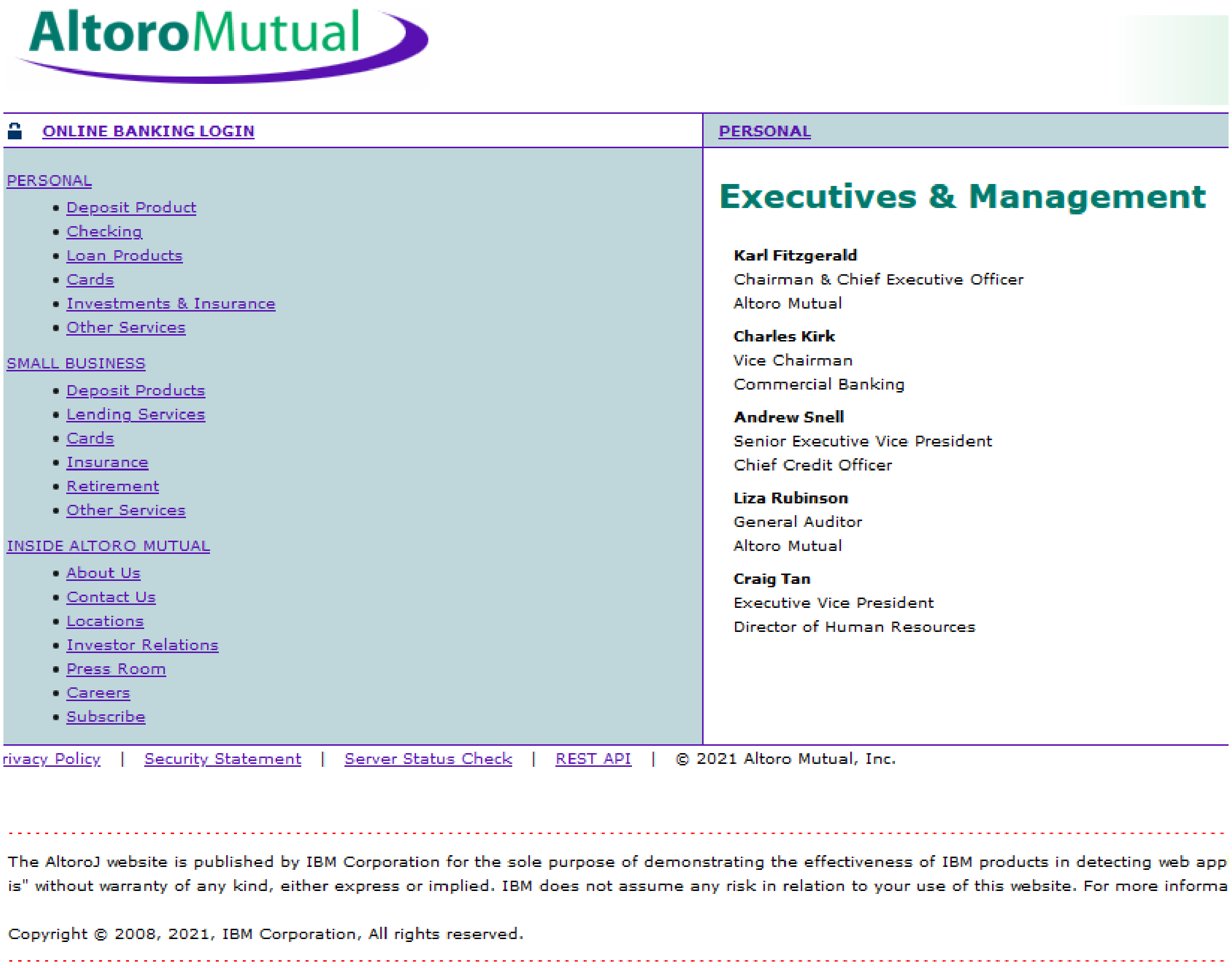
## Week 16 Homework Submission File: Penetration Testing 1

#### Step 1: Google Dorking

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

Karl Fitzgerald



AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

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

rivacy Policy | Security Statement | Server Status Check | REST API | © 2021 Altoro Mutual, Inc.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web app
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 informa

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

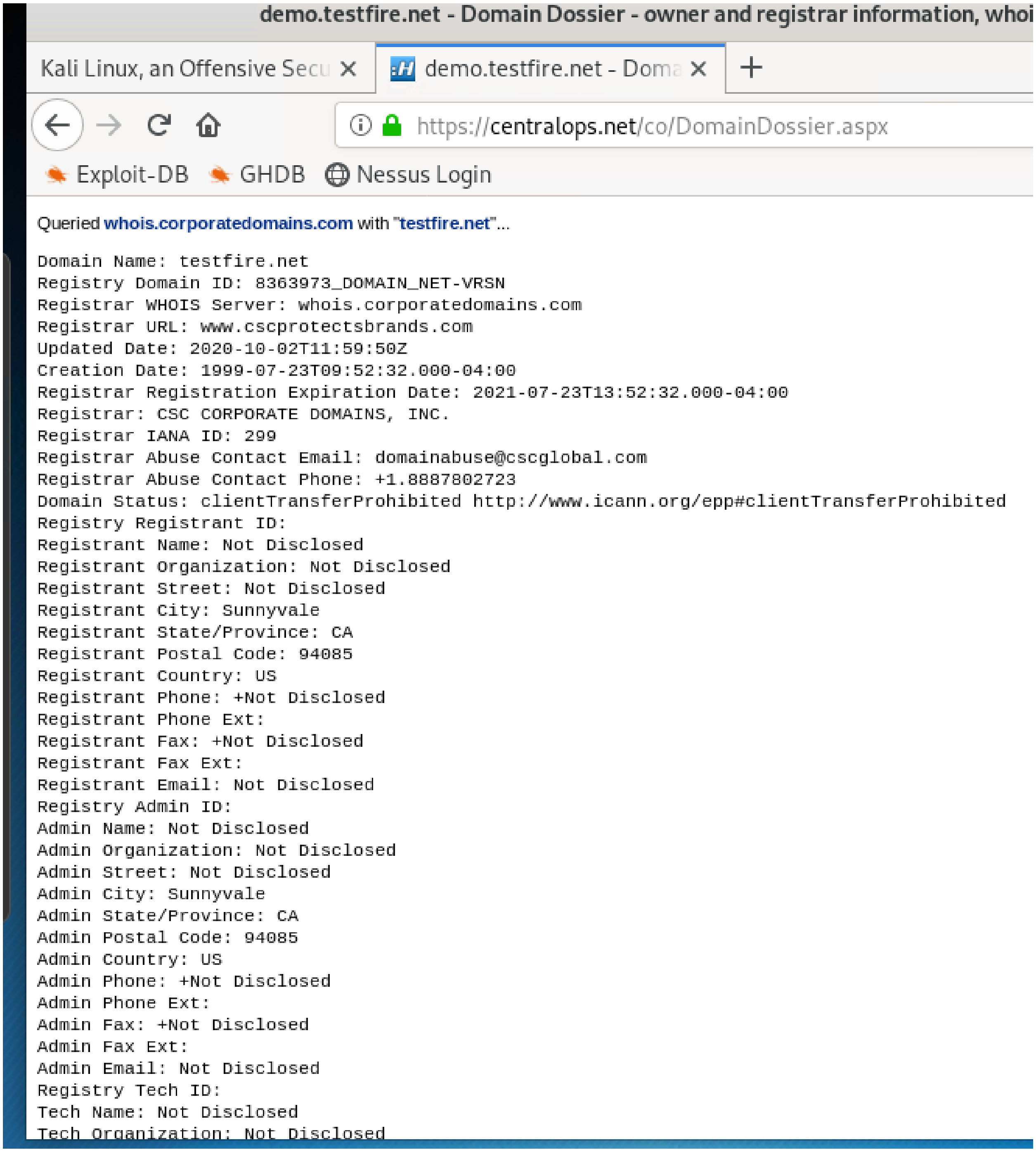
- How can this information be helpful to an attacker:
Emails, social engineering, knowing who you are attacking, good for research

#### 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:

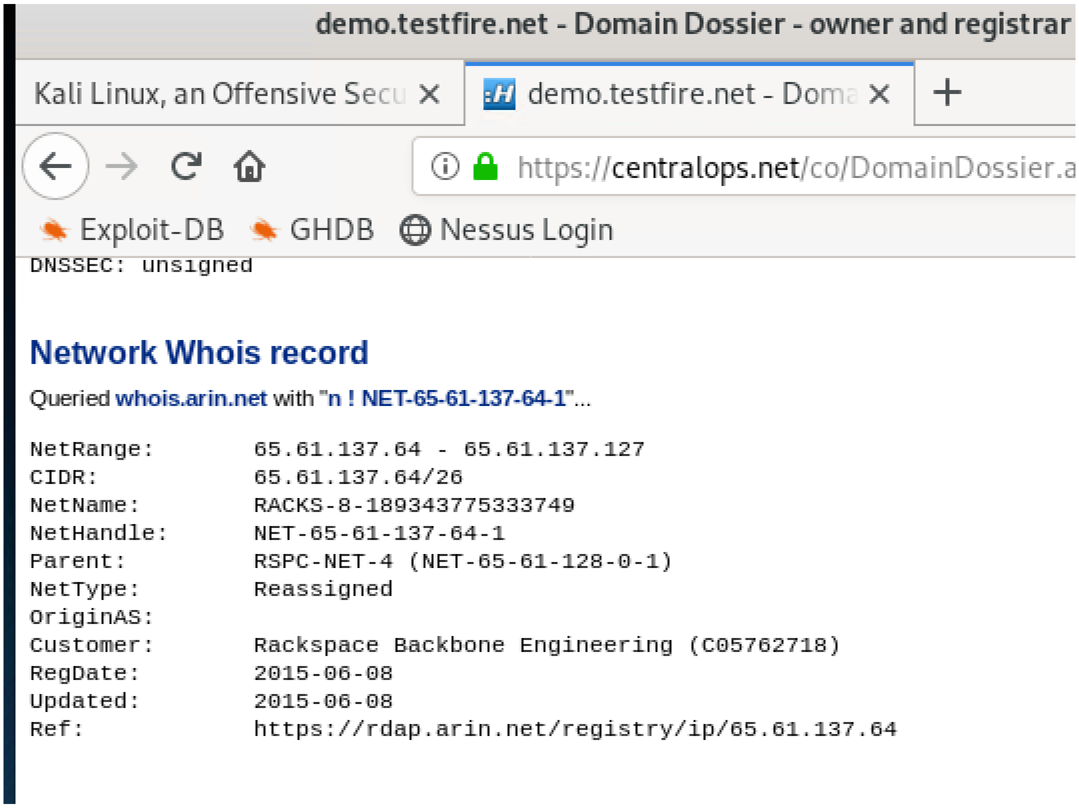
Sunnyvale, Ca


demo.testfire.net - Domain Dossier - owner and registrar information, whoi
Kali Linux, an Offensive Secu
demo.testfire.net - Doma
https://centralops.net/co/DomainDossier.aspx
Exploit-DB
GHDB
Nessus Login

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
Registrant Postal Code: 94085
Registrant Country: US
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
Registry Admin ID:
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94085
Admin Country: US
Admin Phone: +Not Disclosed
Admin Phone Ext:
Admin Fax: +Not Disclosed
Admin Fax Ext:
Admin Email: Not Disclosed
Registry Tech ID:
Tech Name: Not Disclosed
Tech Organization: Not Disclosed
```

2. What is the NetRange IP address:
65.61.137.64 - 65.61.137.127


demo.testfire.net - Domain Dossier - owner and registrar
Kali Linux, an Offensive Secu
demo.testfire.net - Doma
https://centralops.net/co/DomainDossier.a
Exploit-DB
GHDB
Nessus Login

```
DNSSEC: unsigned
```

Network Whois record

Queried whois.arin.net with "n ! NET-65-61-137-64-1"...

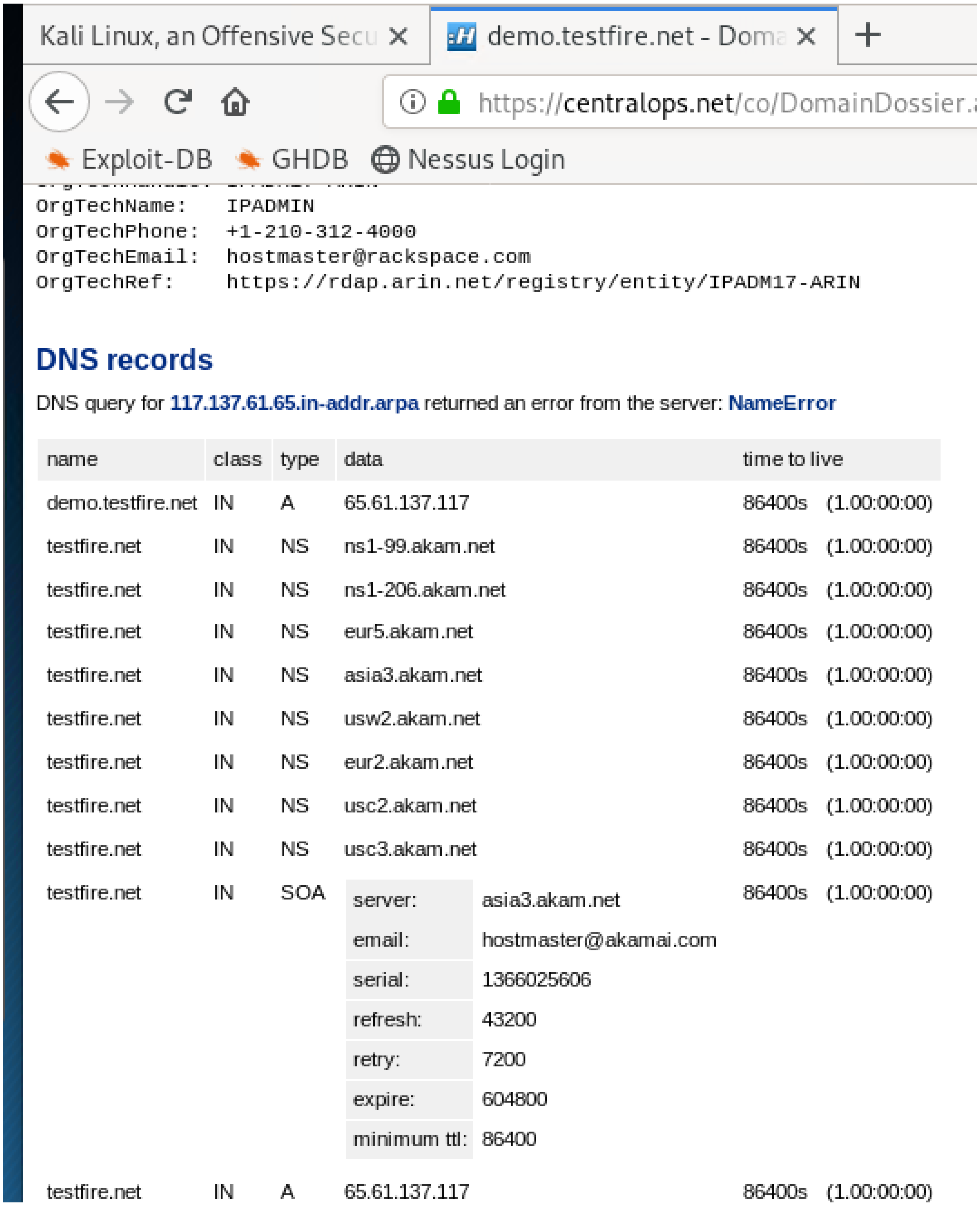
```
NetRange:       65.61.137.64 - 65.61.137.127
CIDR:           65.61.137.64/26
NetName:        RACKS-8-1893437753337 49
NetHandle:      NET-65-61-137-64-1
Parent:         RSPC-NET-4 (NET-65-61-128-0-1)
NetType:        Reassigned
OriginAS:
Customer:       Rackspace Backbone Engineering (C05762718)
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/ip/65.61.137.64
```

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

Rackspace Backbone Engineering

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

65.61.137.117


Kali Linux, an Offensive Secu
demo.testfire.net - Doma
https://centralops.net/co/DomainDossier.a
Exploit-DB
GHDB
Nessus Login

```
OrgTechName:    IPADMIN
OrgTechPhone:   +1-210-312-4000
OrgTechEmail:   hostmaster@rackspace.com
OrgTechRef:     https://rdap.arin.net/registry/entity/IPADM17-ARIN
```

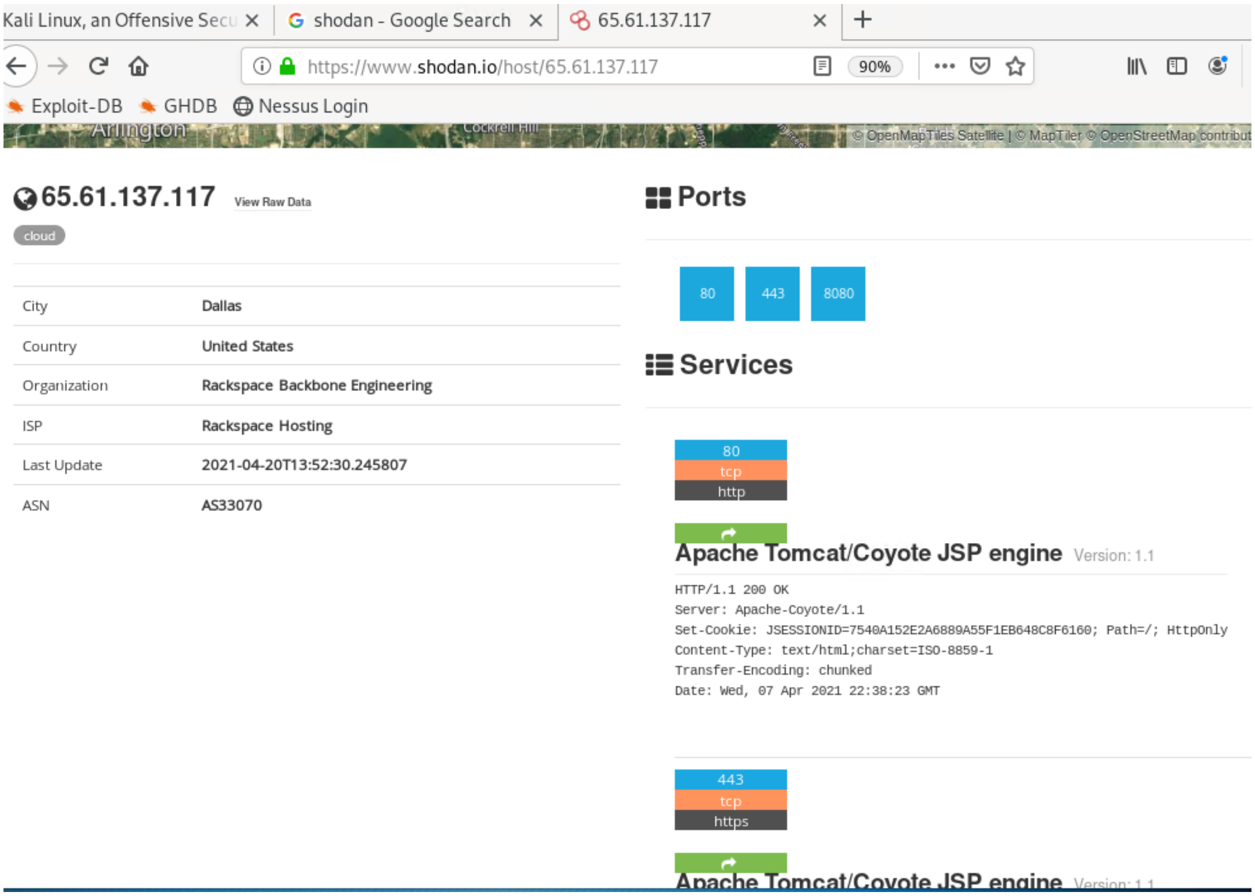
DNS records

DNS query for 117.137.61.65.in-addr.arpa returned an error from the server: NameError

name	class	type	data	time to live
demo.testfire.net	IN	A	65.61.137.117	86400s (1.00:00:00)
testfire.net	IN	NS	ns1-99.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	ns1-206.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	eur5.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	eur2.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	usc2.akam.net	86400s (1.00:00:00)
testfire.net	IN	NS	usc3.akam.net	86400s (1.00:00:00)
testfire.net	IN	SOA	server: asia3.akam.net email: hostmaster@akamai.com serial: 1366025606 refresh: 43200 retry: 7200 expire: 604800 minimum ttl: 86400	86400s (1.00:00:00)
testfire.net	IN	A	65.61.137.117	86400s (1.00:00:00)

#### Step 3: Shodan

- What open ports and running services did Shodan find:
Apache Tomcat/Coyote JSP engine: 80,443, 8080


Kali Linux, an Offensive Secu
shodan - Google Search
65.61.137.117
https://www.shodan.io/host/65.61.137.117
90%
Exploit-DB
GHDB
Nessus Login
Arlington
Cockrell Hill
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contribut

65.61.137.117 View Raw Data

cloud

City	Dallas
Country	United States
Organization	Rackspace Backbone Engineering
ISP	Rackspace Hosting
Last Update	2021-04-20T13:52:30.245807
ASN	AS33070

Ports

80 443 8080

Services

80
tcp
http

Apache Tomcat/Coyote JSP engine Version: 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=7540A152E2A6889A55F1EB648C8F6160; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 07 Apr 2021 22:38:23 GMT
```

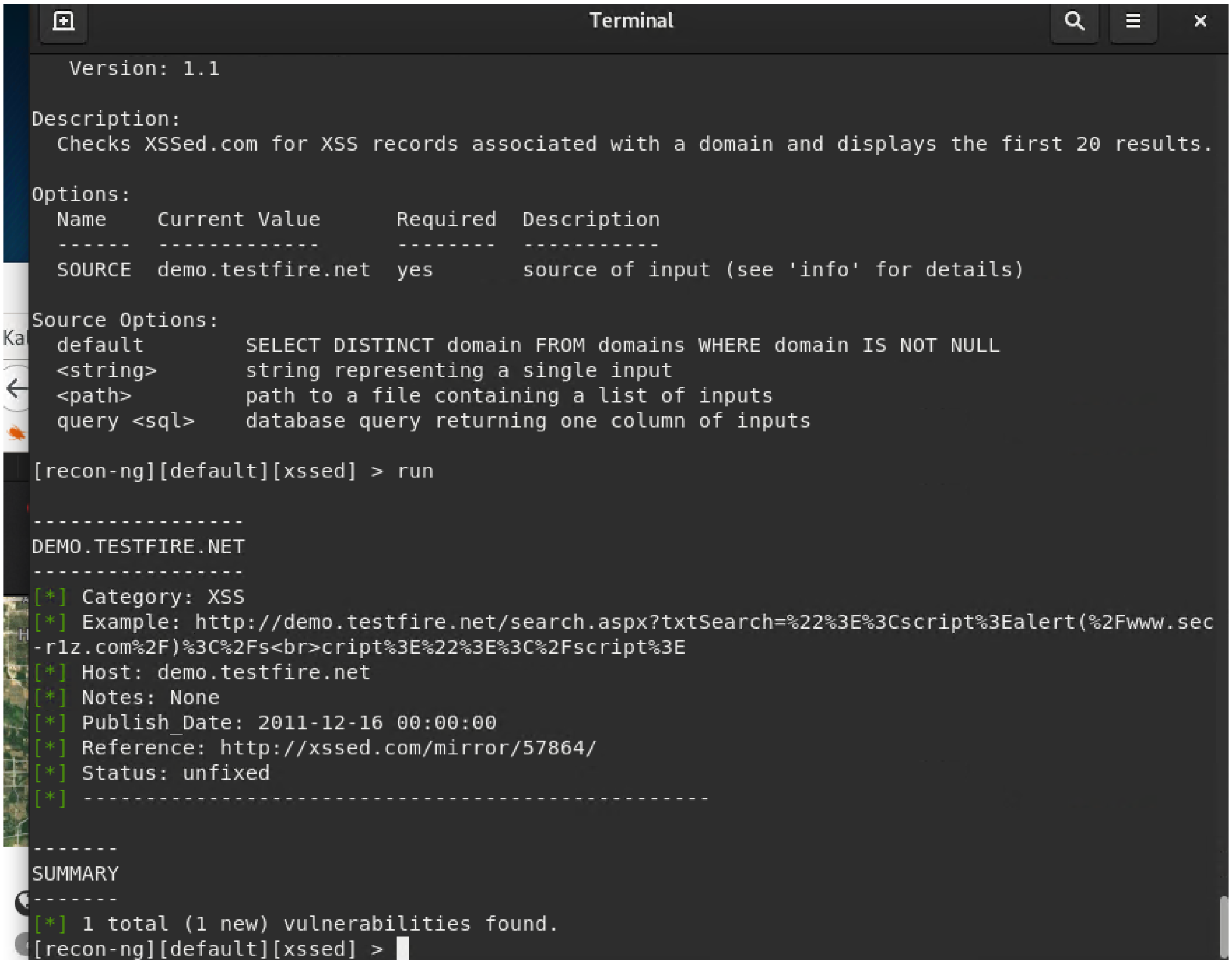
443
tcp
https

Apache Tomcat/Coyote JSP engine Version: 1.1

#### 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



```
   Version: 1.1

Description:
  Checks XSSed.com for XSS records associated with a domain and displays the first 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

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

-----------------
DEMO.TESTFIRE.NET
-----------------
[*] Category: XSS
[*] Example: http://demo.testfire.net/search.aspx?txtSearch=%22%3E%3Cscript%3Ealert(%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] >
```

### 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
- Zenmap vulnerability script command:
nmap --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:
Samba
  2. Why is it dangerous:

It allows the attacker to upload a shared library and have the server load and execute it. Complete impacts to the CIA triad (system files being shared, loss of system protection, totall shutdown of affected source).

3. What mitigation strategies can you recommendations for the client to protect their server:
Update SAMBA && Block port 445
