Week 16 Project 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
- How can this information be helpful to an attacker:

  Enabling an attacker to launch an EMAIL whaling phishing attack against the CEO of Altoro Mutual

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

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:

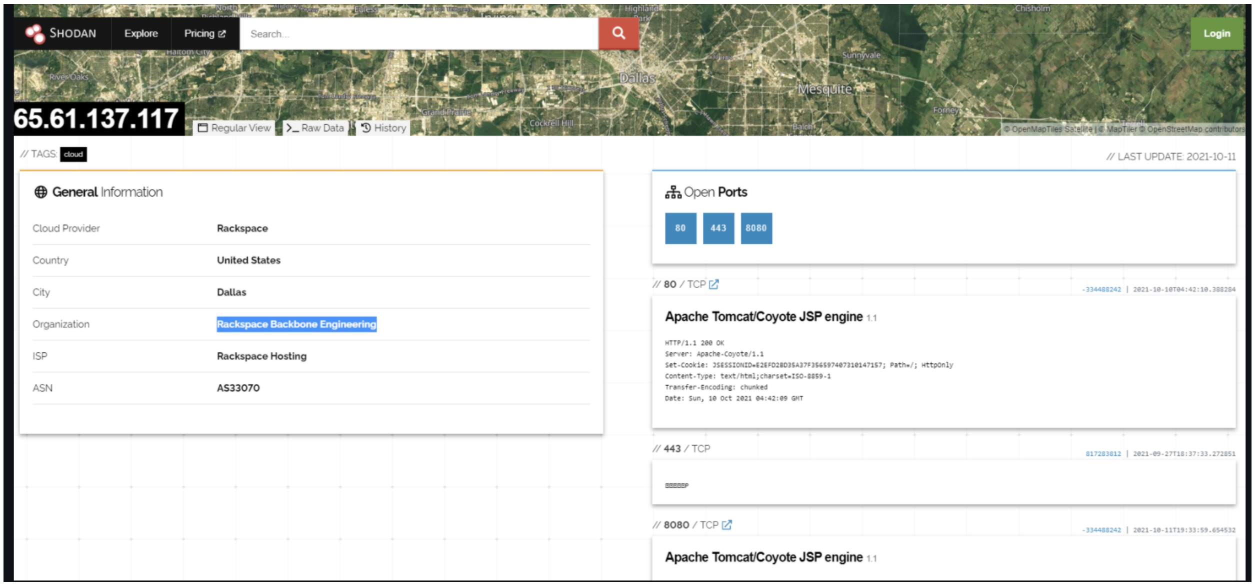
   Rackspace Backbone Engineering

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:
- Port 80 - Apache tcp, HTTP
- Port 443 - Apache tcp, HTTPS
- Port 8080 - Apache tcp, HTTPS



65.61.137.117

// TAGS: cloud

// LAST UPDATE: 2021-10-11

General Information

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

Open **Ports**

80 443 8080

// 80 / TCP
-334488242 | 2021-10-10T04:42:10.388284

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E2EFD2BD35A37F356597407310147157; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sun, 10 Oct 2021 04:42:09 GMT
```

// 443 / TCP
817283812 | 2021-09-27T18:37:33.272851

```
▯▯▯▯▯P
```

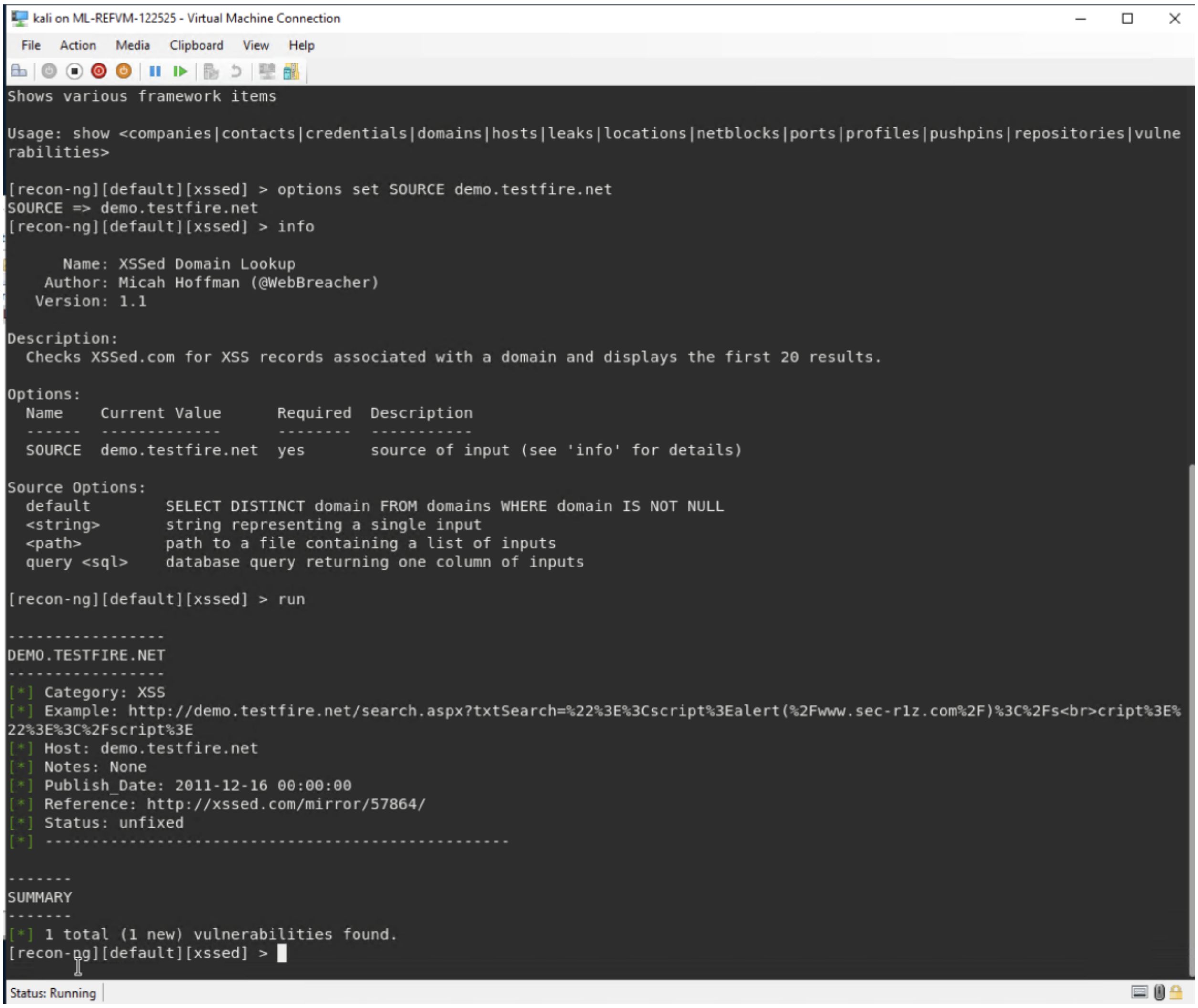
// 8080 / TCP
-334488242 | 2021-10-11T19:33:59.654532

Apache Tomcat/Coyote JSP engine 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



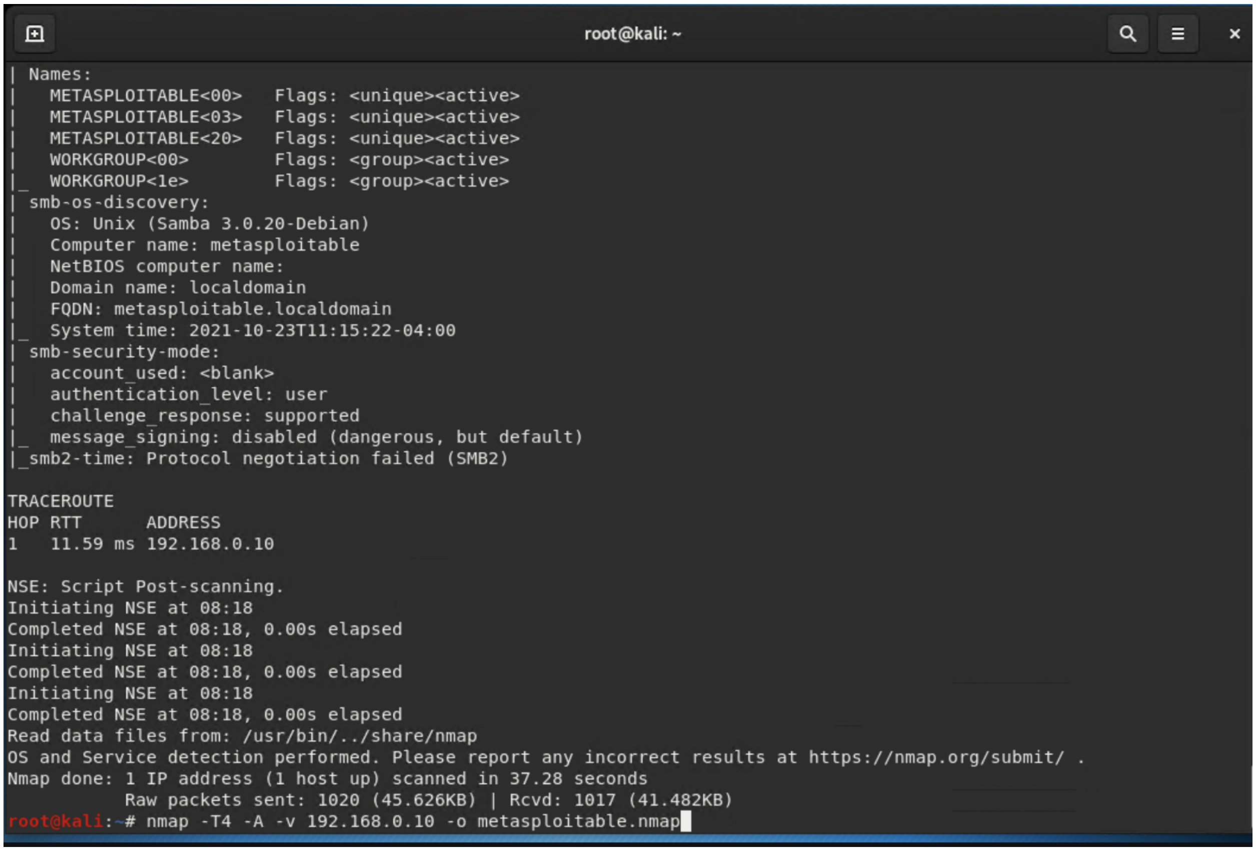
```
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulne
rabilities>

[recon-ng][default][xssed] > options set SOURCE demo.testfire.net
SOURCE => 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 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:

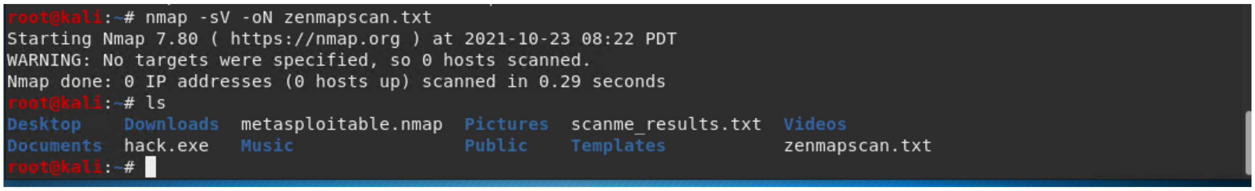
- Command for Zenmap to run a service scan against the Metasploitable machine:

  nmap -T4 -A -v 192.168.0.10 -o metasploitable.nmap



```
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-10-23T11:15:22-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1   11.59 ms 192.168.0.10

NSE: Script Post-scanning.
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 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 37.28 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1017 (41.482KB)
root@kali:~# nmap -T4 -A -v 192.168.0.10 -o metasploitable.nmap
```

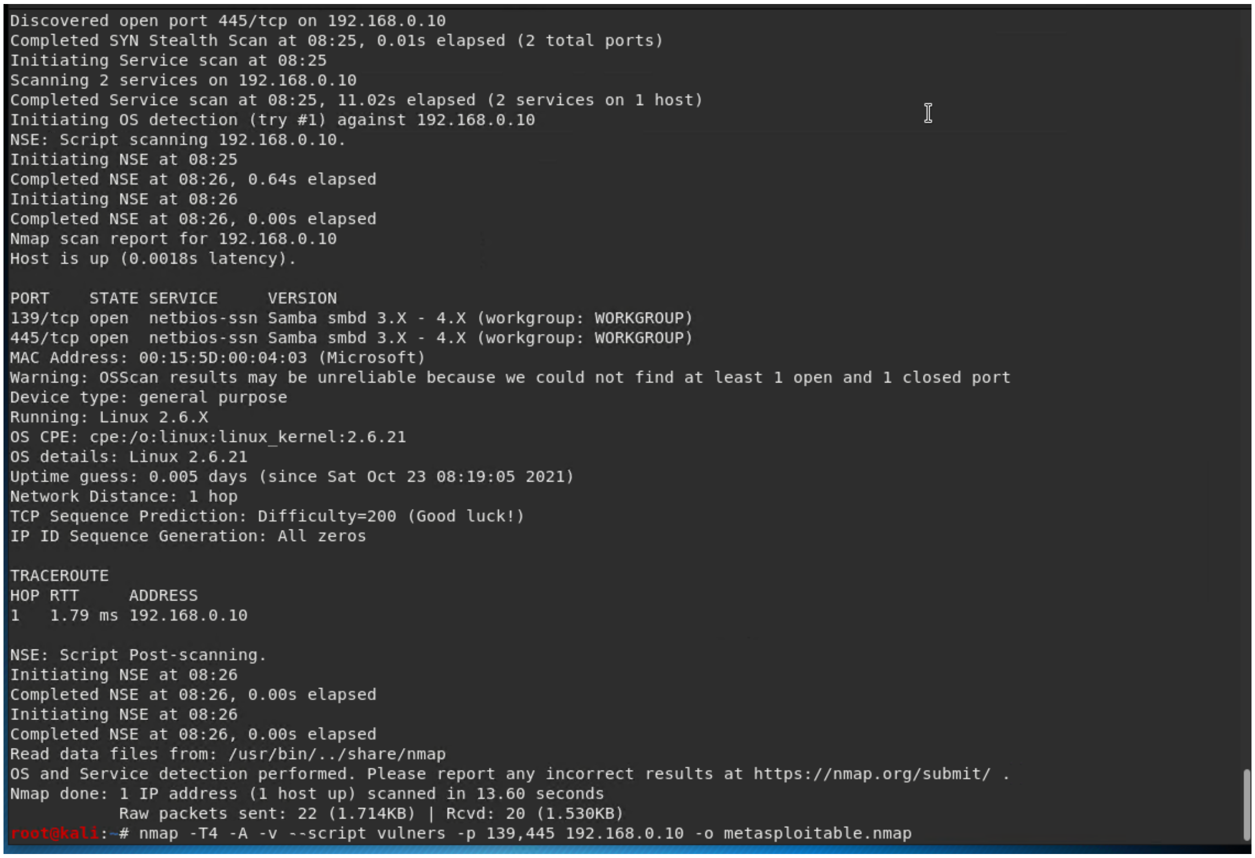
- Bonus command to output results into a new text file named zenmapscan.txt:
  nmap -sV -oN zenmapscan.txt



```
root@kali:~# nmap -sV -oN zenmapscan.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-23 08:22 PDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.29 seconds
root@kali:~# ls
Desktop    Downloads  metasploitable.nmap  Pictures  scanme_results.txt  Videos
Documents  hack.exe   Music                Public    Templates           zenmapscan.txt
root@kali:~# 
```

- Zenmap vulnerability script command:

  nmap -T4 -A -v --script vulners -p 139,445 192.168.0.10 -o metasploitable.nmap



```
Discovered open port 445/tcp on 192.168.0.10
Completed SYN Stealth Scan at 08:25, 0.01s elapsed (2 total ports)
Initiating Service scan at 08:25
Scanning 2 services on 192.168.0.10
Completed Service scan at 08:25, 11.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.10
NSE: Script scanning 192.168.0.10.
Initiating NSE at 08:25
Completed NSE at 08:26, 0.64s elapsed
Initiating NSE at 08:26
Completed NSE at 08:26, 0.00s elapsed
Nmap scan report for 192.168.0.10
Host is up (0.0018s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.21
OS details: Linux 2.6.21
Uptime guess: 0.005 days (since Sat Oct 23 08:19:05 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   1.79 ms 192.168.0.10

NSE: Script Post-scanning.
Initiating NSE at 08:26
Completed NSE at 08:26, 0.00s elapsed
Initiating NSE at 08:26
Completed NSE at 08:26, 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 13.60 seconds
           Raw packets sent: 22 (1.714KB) | Rcvd: 20 (1.530KB)
root@kali:~# nmap -T4 -A -v --script vulners -p 139,445 192.168.0.10 -o metasploitable.nmap
```

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

1. What is the vulnerability:

   The 192.168.0.10\tmp fileshare allows for user Anonymous: READ/WRITE access

2. Why is it dangerous:

   This could result in a hacker gaining access to the host server and install malicious code

3. What mitigation strategies can you recommendations for the client to protect their server:

   -Keep Software Up-to-Date.

   -Install Anti-Virus Protection Software.

   -Backup Critical Data.

   -Invest in Security Training for Employees.