**Week 16 Homework: 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:

Spear Phishing

Whaling

#### 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

4. What is the IP address of the DNS server:65.61.137.117

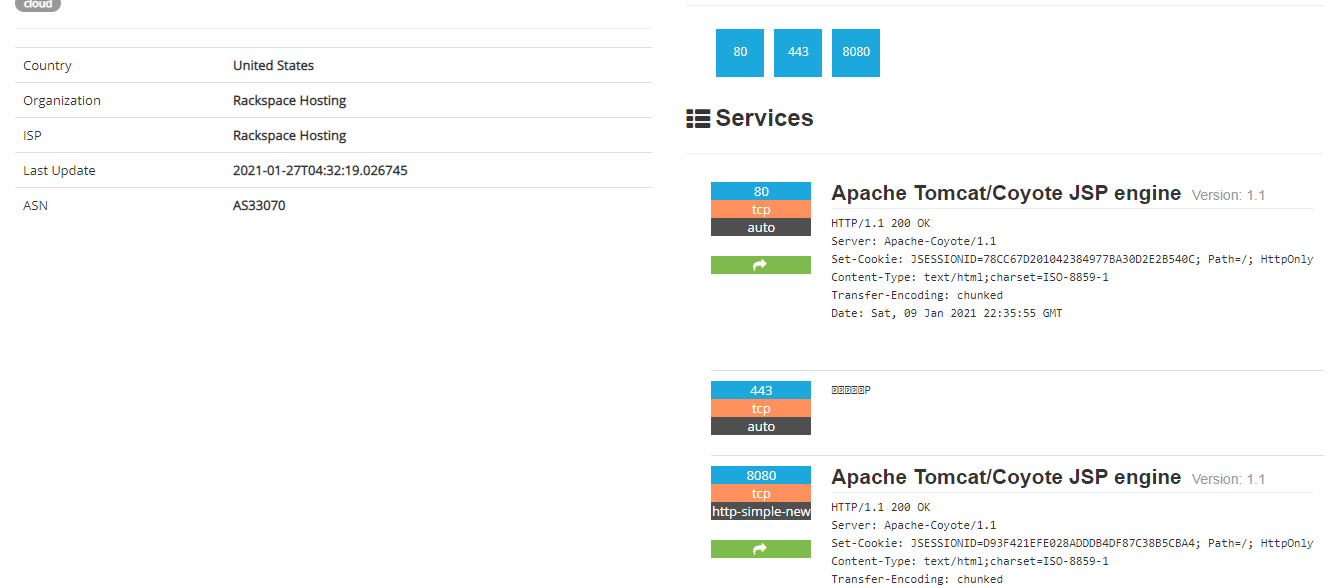
#### Step 3: Shodan

- What open ports and running services did Shodan find:

○ Port 80 - Apache HTTP

○ Port 443 - Apache HTTPS

○ Port 8080 - Apache HTTP



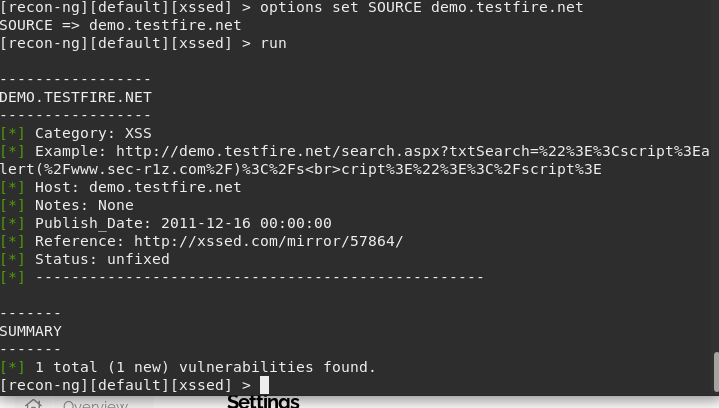
#### Step 4: Recon-ng

- Install the Recon module `xssed`.

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

- Run the module.

Is Altoro Mutual vulnerable to XSS:



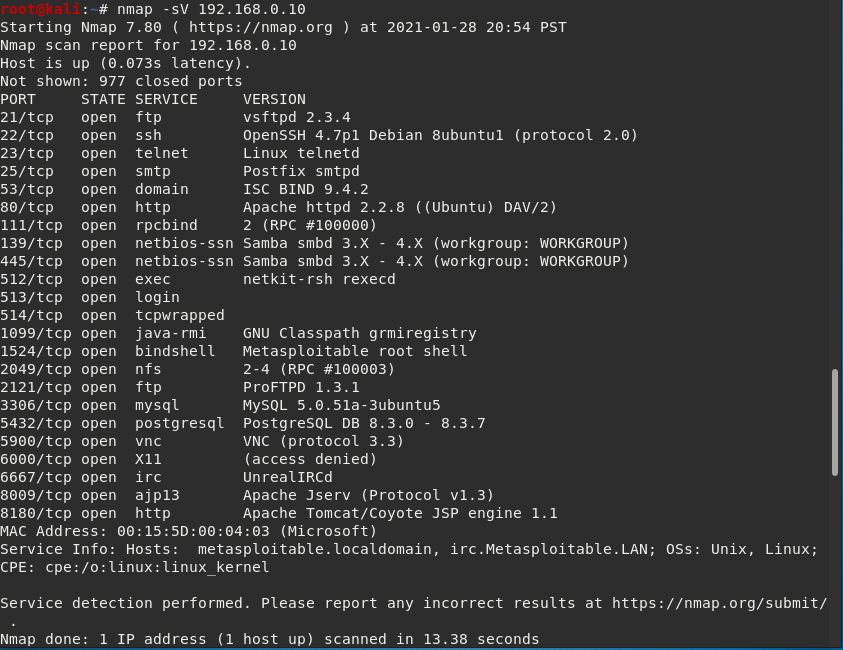
### Step 5: Zenmap

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:

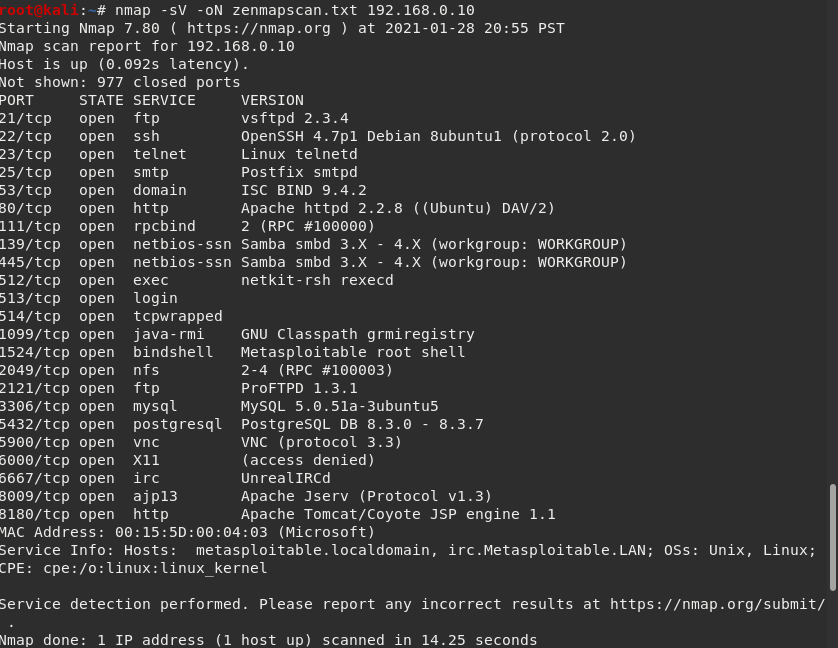
- Command for Zenmap to run a service scan against the Metasploitable machine:

Nmap -sV 192.168.0.10



**- Bonus**: Command to output results into a new text file named `zenmapscan.txt`:

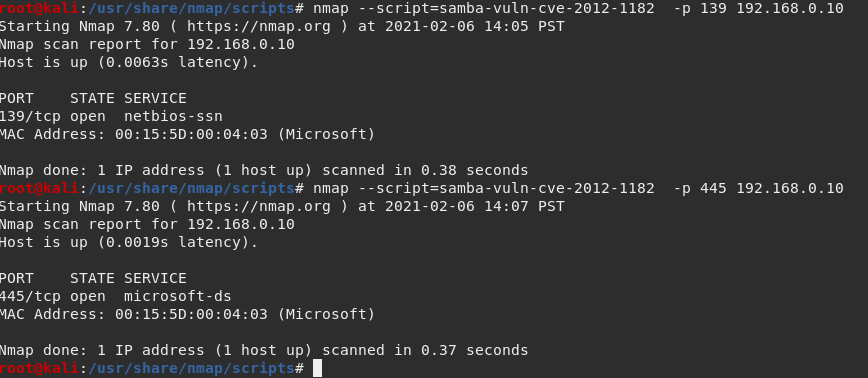
Nmap -sV -oN zenmapscan.txt 192.168.0.10



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

- Zenmap vulnerability script command: nmap --script=samba-vuln-cve-2012-1182 -p 139 192.168.0.10

nmap --script=samba-vuln-cve-2012-1182 -p 445 192.168.0.10



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

1. What is the vulnerability:Weakness in smb allowing unauthorized access

2. Why is it dangerous:it allows for exfiltration of data

3. What mitigation strategies can you recommendations for the client to protect their server:Update/patch the Samba version as soon as possible

---

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