## 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

* How can this information be helpful to an attacker:

Can used for reconan social engineering, phishing

#### 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

1. What is the NetRange IP address:

65.61.137.64 - 65.61.137.127

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

Rackspace Backbone Engineering

1. 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:

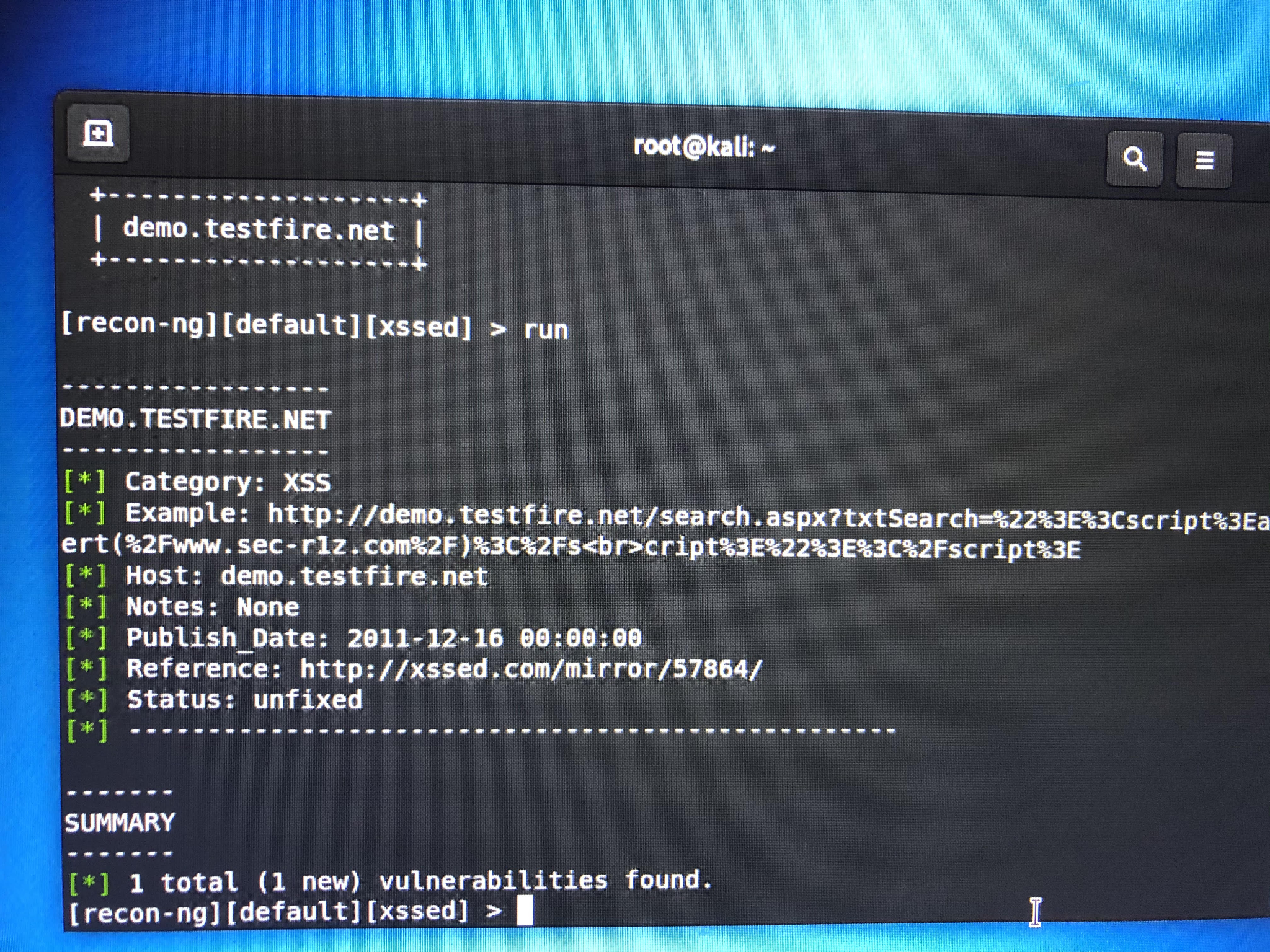
Open Ports: 80,443,8080

Services:Appache 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



### 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-v192.168.0.10

* Bonus command to output results into a new text file named zenmapscan.txt:
* Zenmap vulnerability script command:

nmap --script samba-vuln-cve-2012-1182 192.168.0.10

* Once you have identified this vulnerability, answer the following questions for your client:
  1. What is the vulnerability:

SMB 3 (samba)

* 1. Why is it dangerous:

It allows attackers to have access to directories, files, printers that are on the server and by them gaining access they can use it to bring down the company and steal personal information.

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

Block port 445

Course