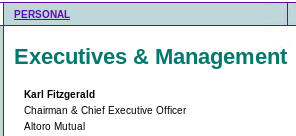
## **CSpencer HW 16 1/12/2021**

## **Homework Submission File: Penetration Testing 1**

#### **Step 1: Google Dorking**

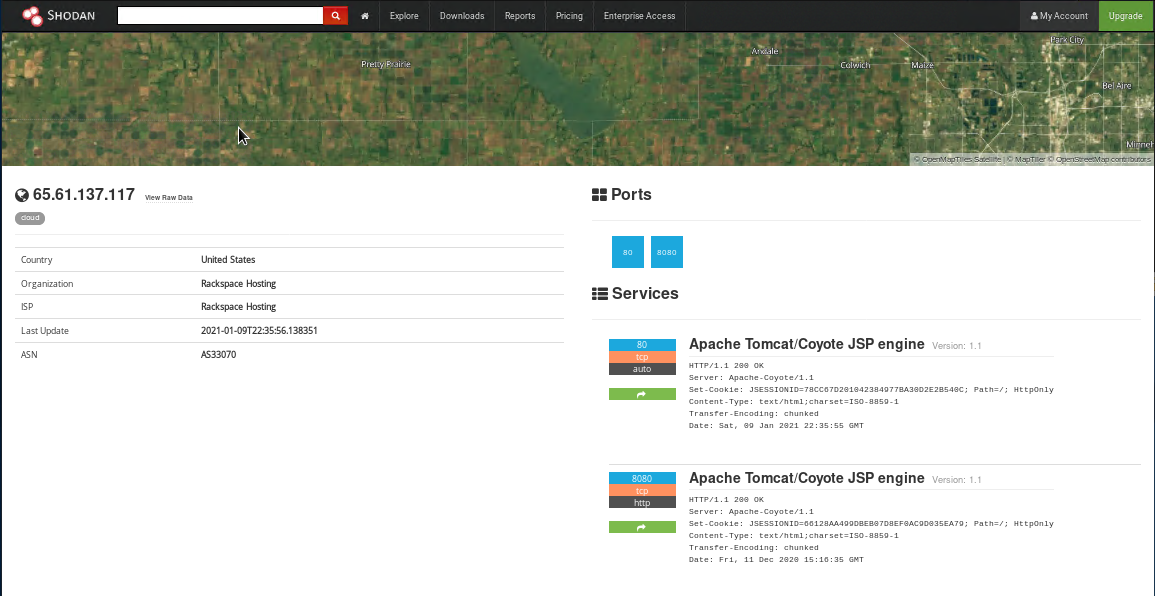
* Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:
  + site: altoro mutual intext:chief executive officer
  + Karl Fitzgerald - Chairman and Chief Executive Officer
  + 
* How can this information be helpful to an attacker:
  + This information can be used in a whaling attack of the CEO and in social engineering of staff by impersonation of the CEO.

#### **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

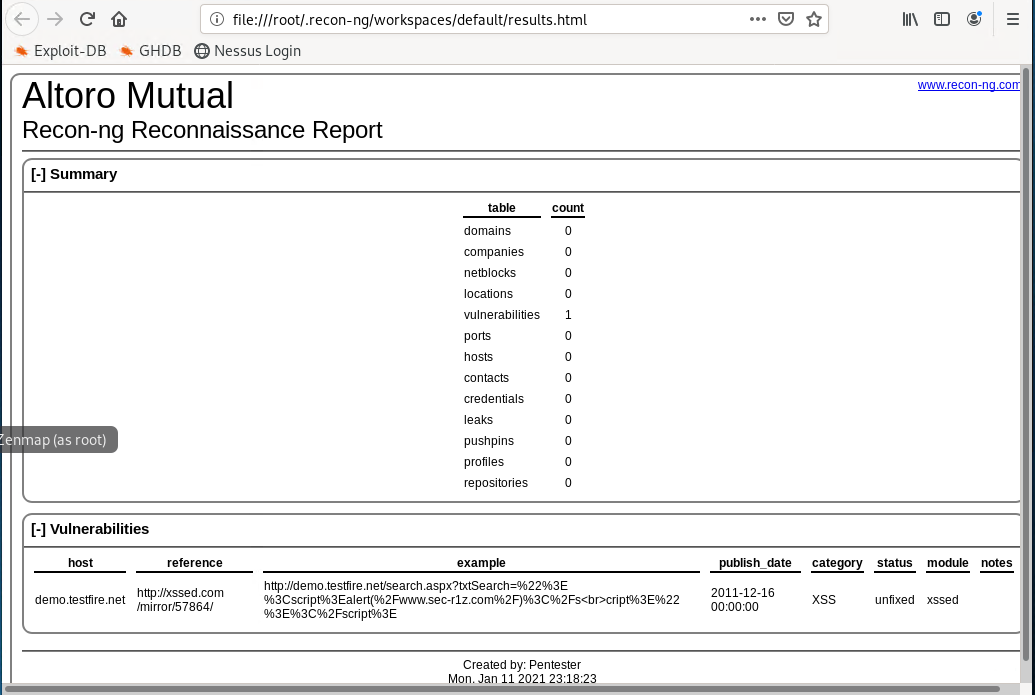
#### **Step 3: Shodan**

* What open ports and running services did Shodan find:  
   Ports: 80, 8080  
   Services: Apache Tomcat/Coyote JSP engine  
   Server: Apache-Coyote/1.1
* 

#### **Step 4: Recon-ng**

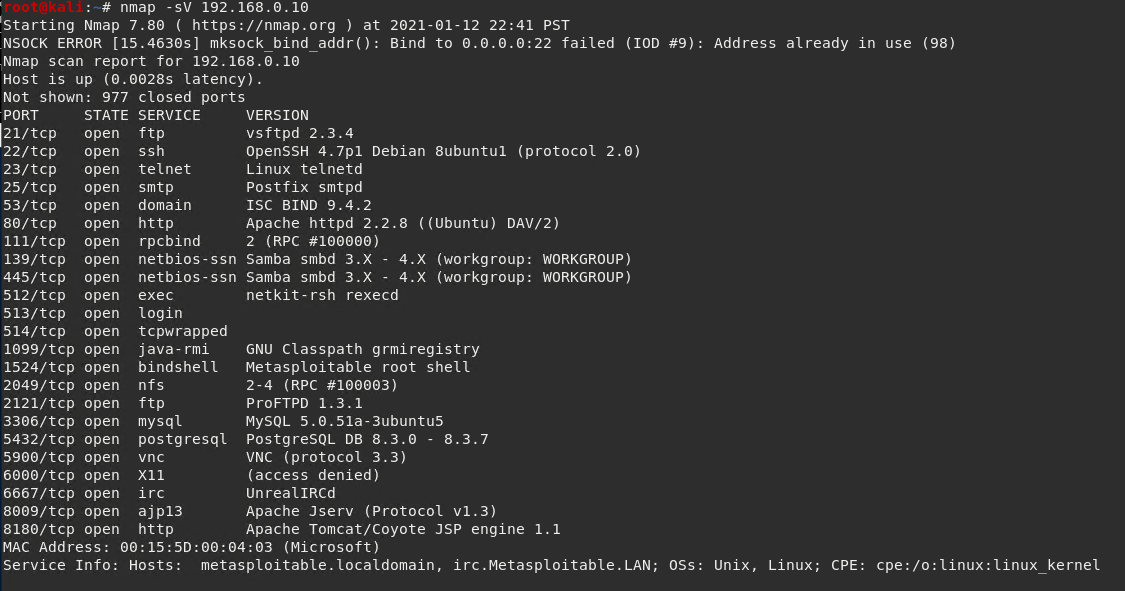
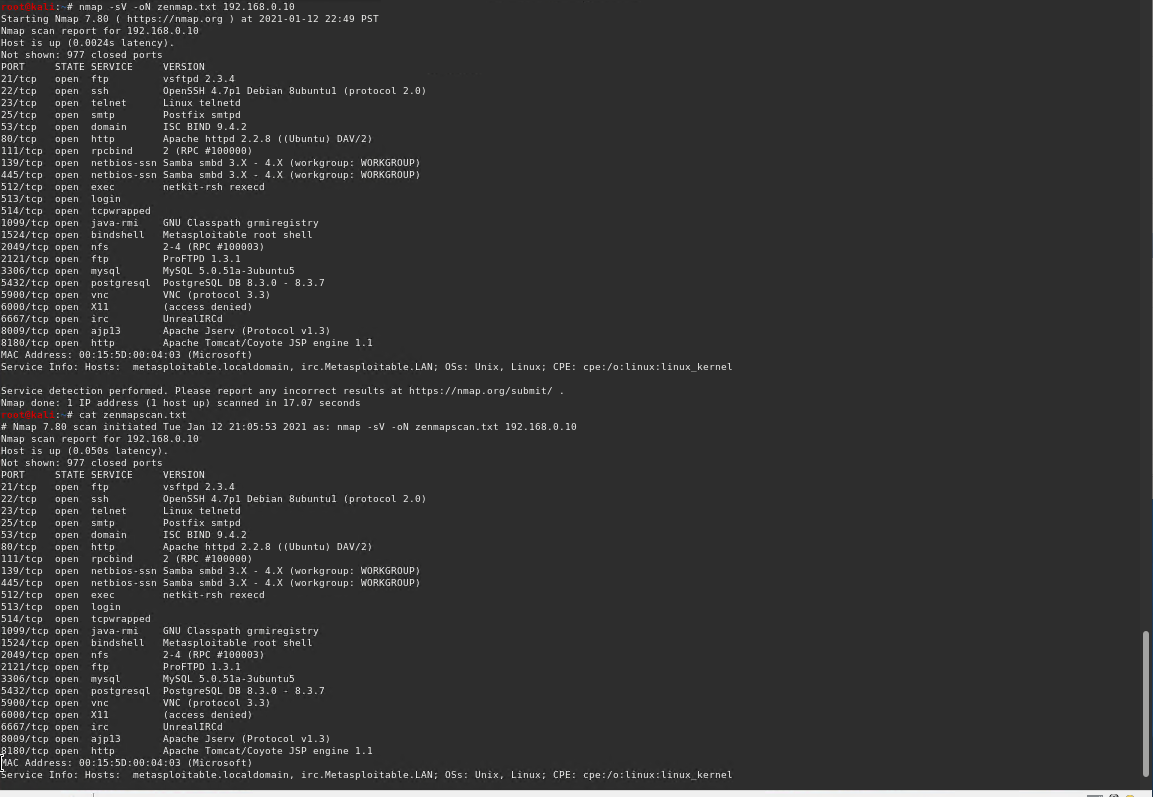
* Install the Recon module xssed.
* Set the source to demo.testfire.net.
* Run the module.

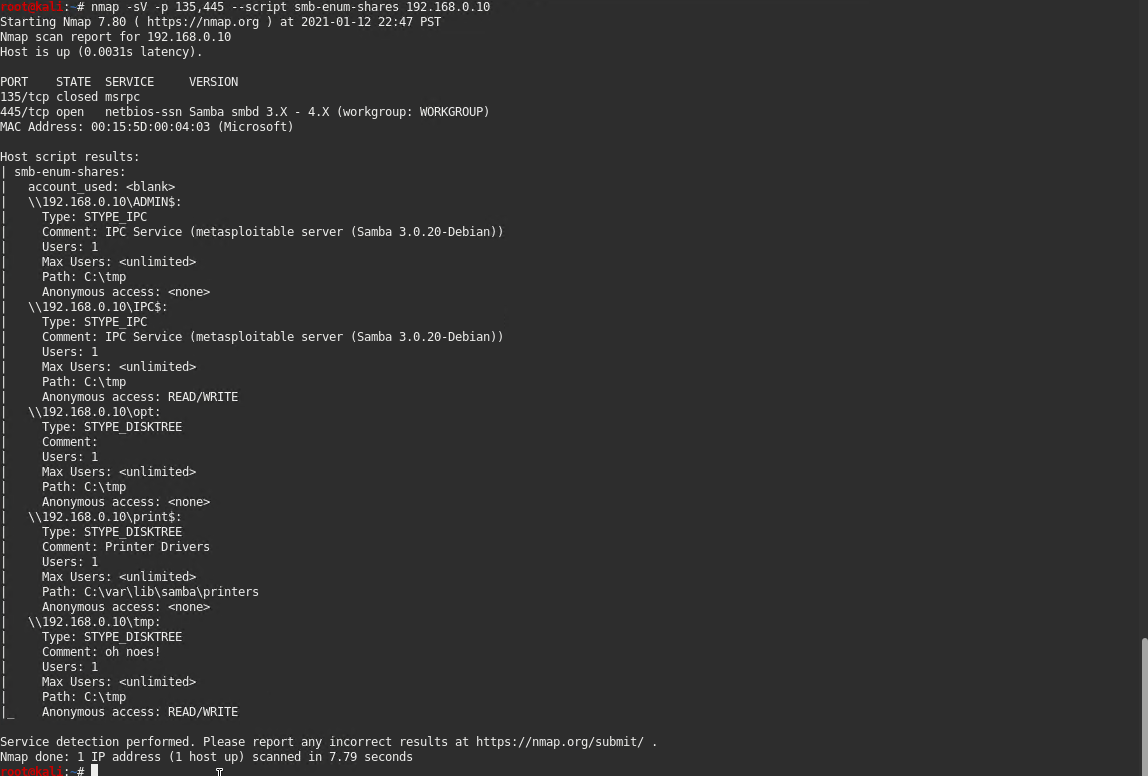
Is Altoro Mutual vulnerable to XSS:

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 -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  
  
* Zenmap vulnerability script command:

Nmap -sV -p 135,445 --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 3.0.20-Debian (CVE-2007-2447)

<https://www.cvedetails.com/cve/CVE-2007-2447/>

* 1. Why is it dangerous:  
     This exploits a command execution vulnerability that allows attackers to execute arbitrary commands; authentication is not required because the option is used to map usernames prior to authentication.  
     <https://www.cvedetails.com/cve/CVE-2007-2447/>  
       
     It is possible to get anonymous, root level access and further enumerate the machine.  
     <http://www.rwbnetsec.com/samba-3-x/>
  2. What mitigation strategies can you recommend for the client to protect their server:  
     Upgrade to the latest version of samba at http://www.samba.org/samba/download