## **Unit 16 Homework Submission File: Penetration Testing**

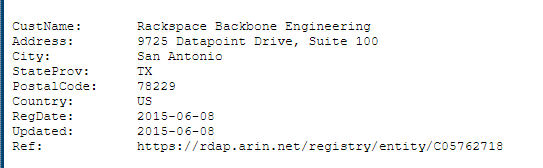
#### **Step 1: Google Dorking**

* 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:
  + Knowing the first and last names of the Executive and Management ([Executives & Management](http://www.altoromutual.com/index.jsp?content=inside_executives.htm)) is useful to an attacker because you can send phishing emails. A dedicated attacker can also use this information to research the individual further, whether that be on Social Media or Google, and use their findings to perform other attacks such as Brute Force.

#### **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:
   1. Sunnyvale, CA
2. What is the NetRange IP address:
   1. 65.61.137.64 - 65.61.137.127
3. What is the company they use to store their infrastructure:

**  
RACKSPACE BACKBONE ENGINEERING**

1. What is the IP address of the DNS server:
   1. 65.61.137.117

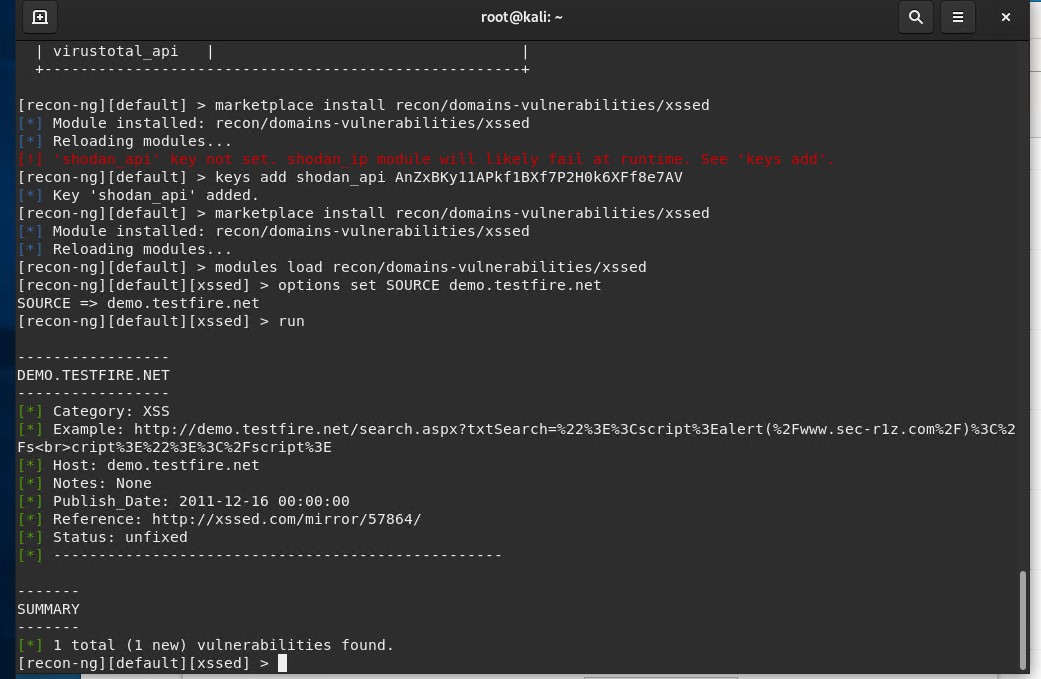
#### **Step 3: Shodan**

* What open ports and running services did Shodan find:
  + 80, 443, 8080

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

* Install the Recon module xssed.
  + marketplace install recon/domains-vulnerabilities/xssed
  + modules load recon/domains-vulnerabilities/xssed
* Set the source to demo.testfire.net.
  + options set source demo.testfire.net
* Run the module.

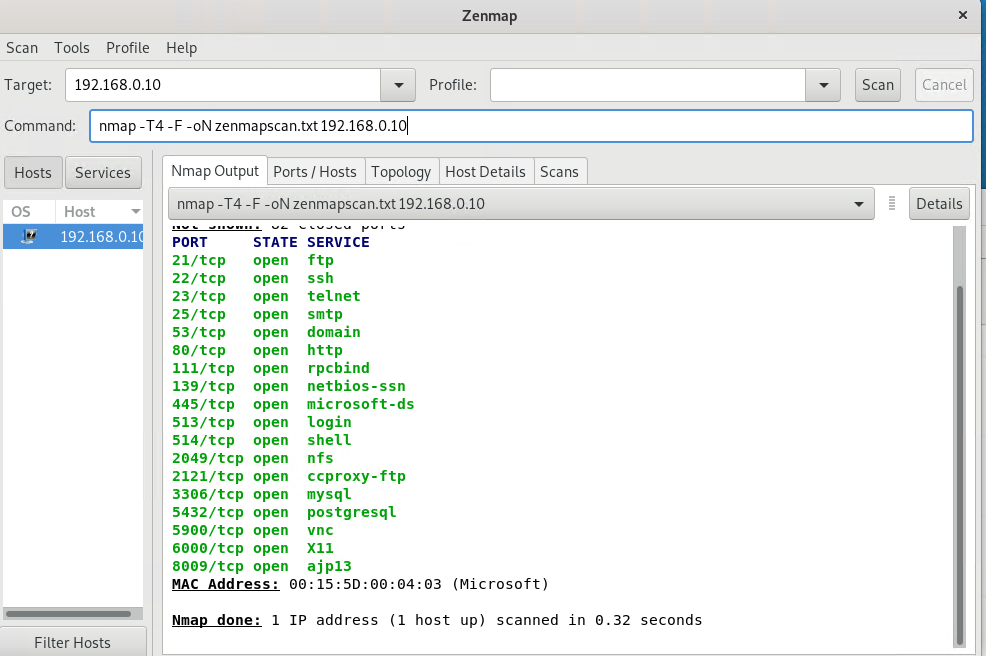
Is Altoro Mutual vulnerable to XSS: YES.



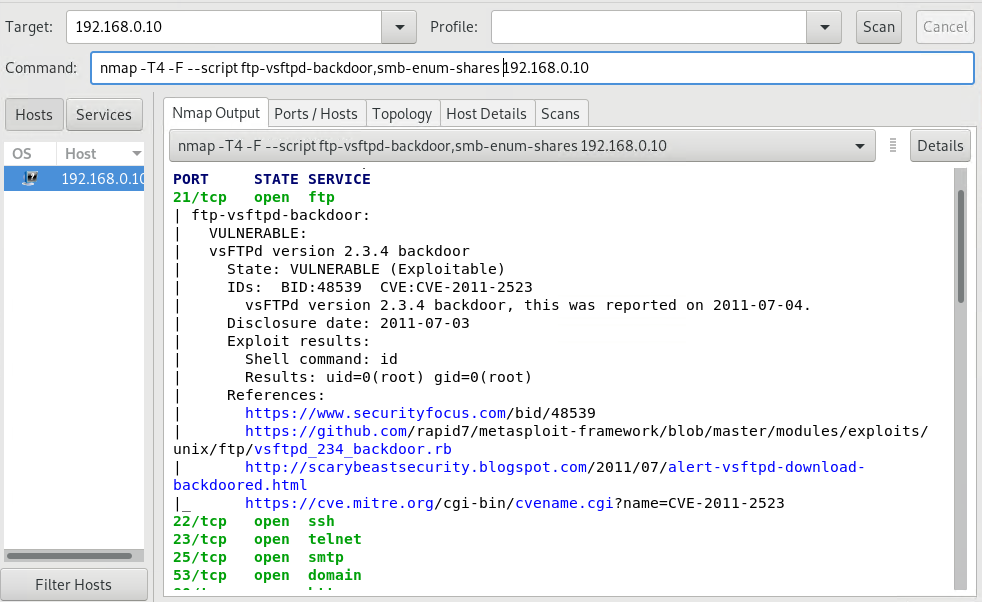
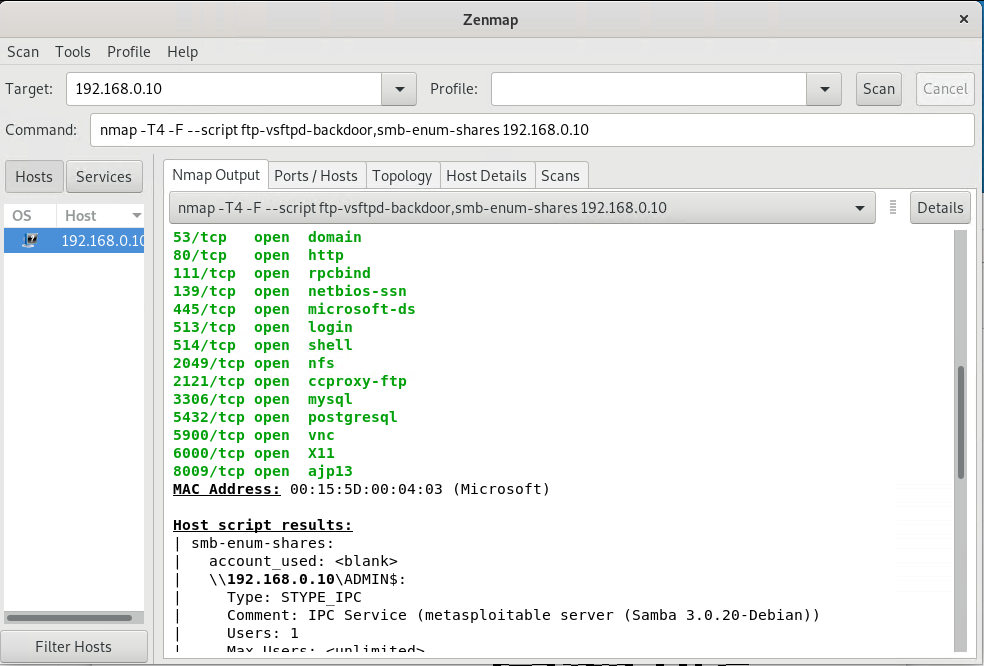
### **Step 5: Zenmap**

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:
  1. nmap -T4 -F 192.168.0.10
* Bonus command to output results into a new text file named zenmapscan.txt:



* Zenmap vulnerability script command:
  1. nmap -T4 -F - -script ftp-vsftpd-backdoor,sub-enum-shares 192.168.0.10
* Once you have identified this vulnerability, answer the following questions for your client:
  1. What is the vulnerability:
     + Port 139: netbios-ssn
     + Port 445: microsoft-ds

* 1. Why is it dangerous:
     + netbios-ssn (CVE-2017-0174) is a dangerous Denial of Service vulnerability that exists “when Microsoft Windows improperly handles NetBIOS packets. An attacker who successfully exploited this vulnerability could cause a target computer to become completely unresponsive” (<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0174>).
     + “Port 445 (SMB) is one of the most commonly and easily susceptible ports for attacks. Port 445 is a TCP port for Microsoft-DS SMB file sharing. Many (to most) Windows systems, as well as Linux, have this port open by default, with unsecured shares and un-patched systems unknowingly exposed to everyone” (<https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/>).
     + An attacker may use port 445 to perform NetBIOS attacks as it would on port 139 (<https://www.beyondsecurity.com/scan-pentest-network-vulnerabilities-smb-listens-on-port.html>).
  2. What mitigation strategies can you recommendations for the client to protect their server:
     + Staying up to date on patches and security updates as well as monitoring/updating new versions consistently are necessary to protect the server. Microsoft also recommends users to “block TCP port 139 at the firewall” for the netbios-ssn vulnerability.

RESOURCES:

“Executives & Management.” *Altoro Mutual*, IBM, http://www.altoromutual.com/index.jsp?content=inside\_executives.htm.

“Finding and Fixing Vulnerabilities in SMB Listens on Port , a Medium Risk Vulnerability.” *Beyond Security*, 2 Feb. 2022, https://www.beyondsecurity.com/scan-pentest-network-vulnerabilities-smb-listens-on-port.html.

machn1k. “Metasploit SMB – Exploitation of Port 445.” *machn1k.Wordpress.com*, 4 Feb. 2013, https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/.

“Windows NetBIOS Denial of Service Vulnerability.” *Security Update Guide - Microsoft Security Response Center*, Microsoft , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0174.

GITHUB UNIT 16 CLASS ACTIVITIES/STUDENT GUIDE