**Week 16 Homework Submission File: Penetration Testing 1**

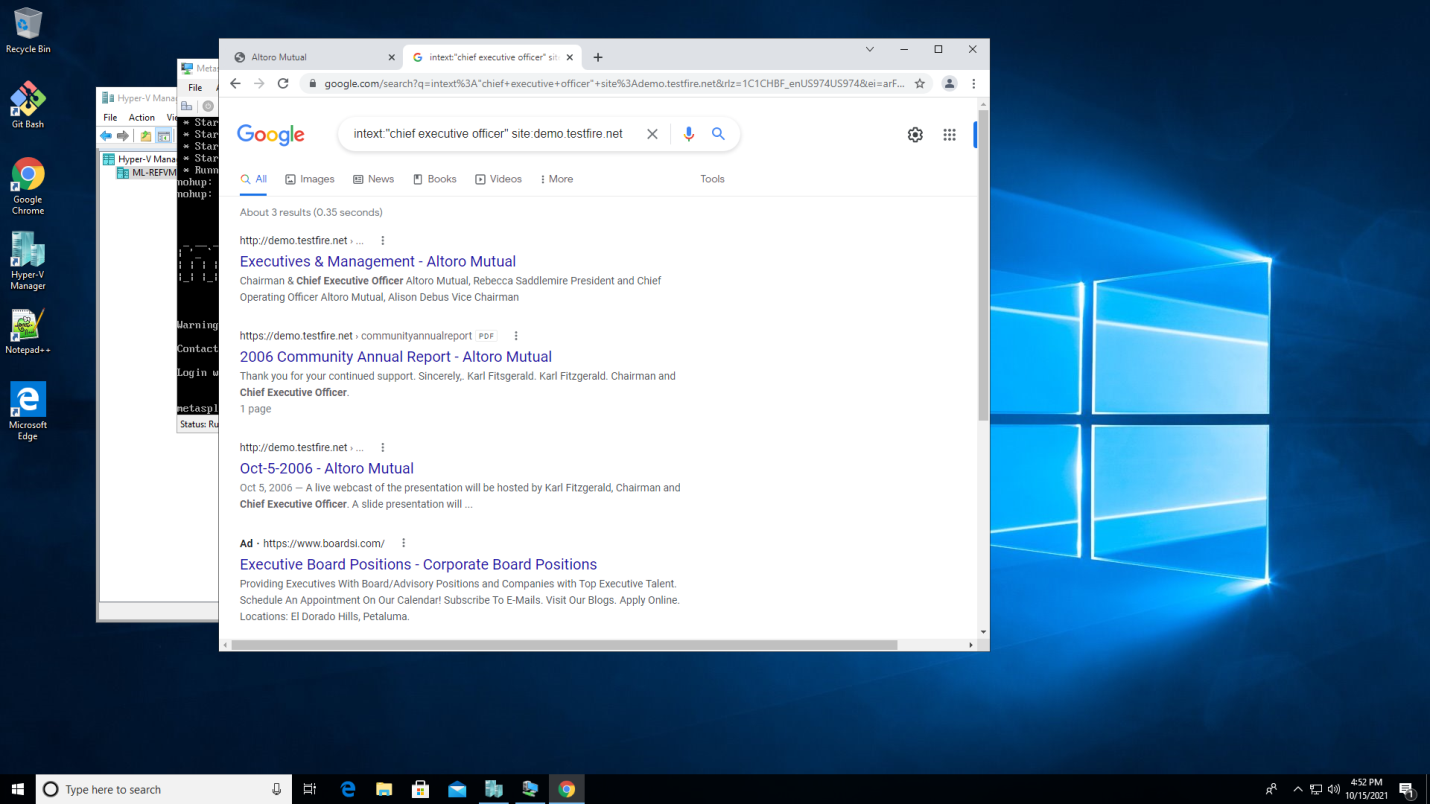
**Step 1: Google Dorking**

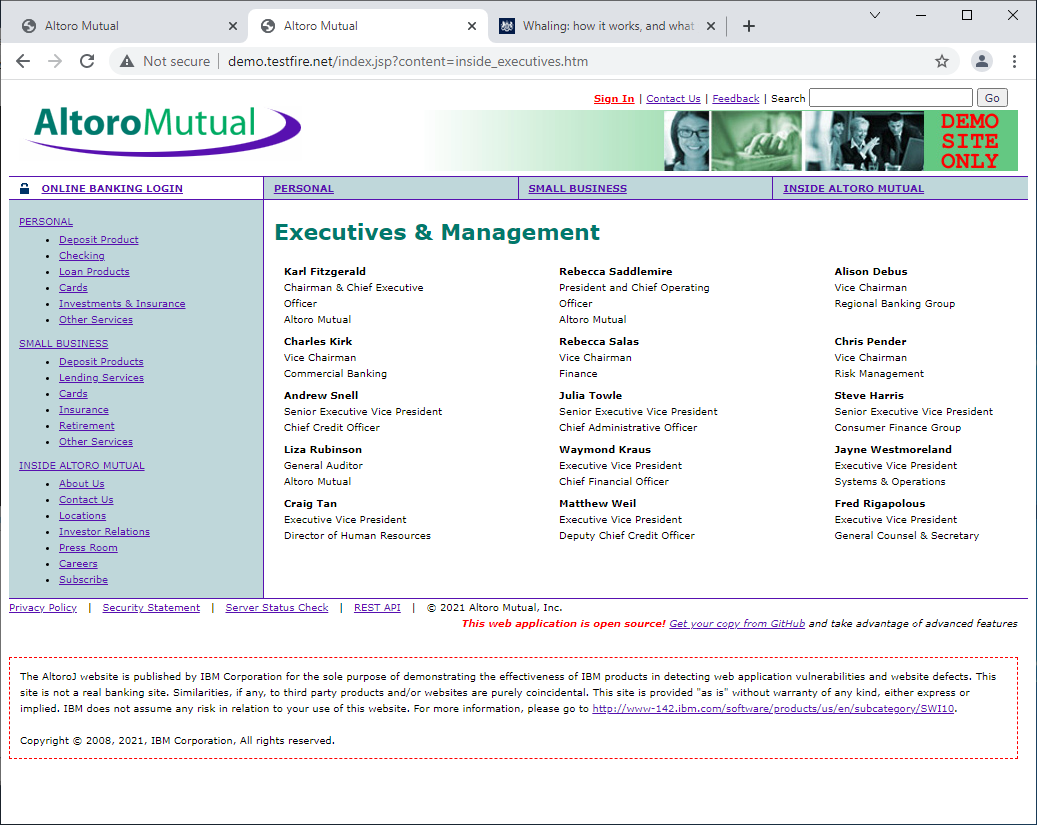
* Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:

*Alturo Mutual*

*intext:”chief executive officer” site:demo.testfire.net*

*resulted in:*





* How can this information be helpful to an attacker:

*This information can be used to prompt a whaling attack by bad actors. Whaling is aimed at senior executives, and comes disguised as legitimate email, but is in fact, an attempt to defraud the company through social engineering. Whaling is an attempt to encourage victims to perform actions like; approving transactions for billing, transferring funds, etc…*

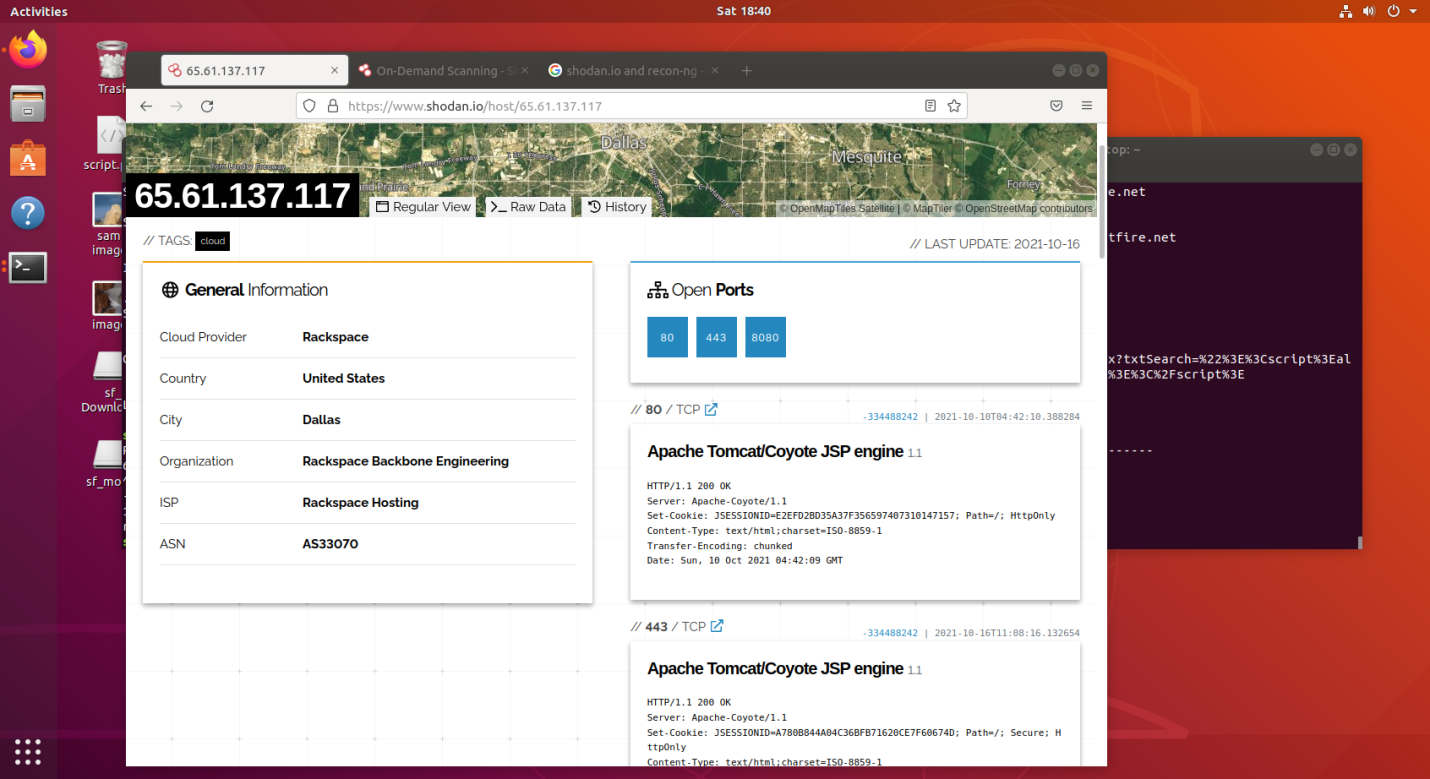
**Step 2: DNS and Domain Discovery**

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: *CIDR: 65.61.137.64/26*
3. What is the company they use to store their infrastructure: *Rackspace Backbone Engineering, 9725 Datapoint Drive, Suite 100, San Antonio, TX 78229, US*
4. What is the IP address of the DNS server: 65.61.137.117

**Step 3: Shodan**

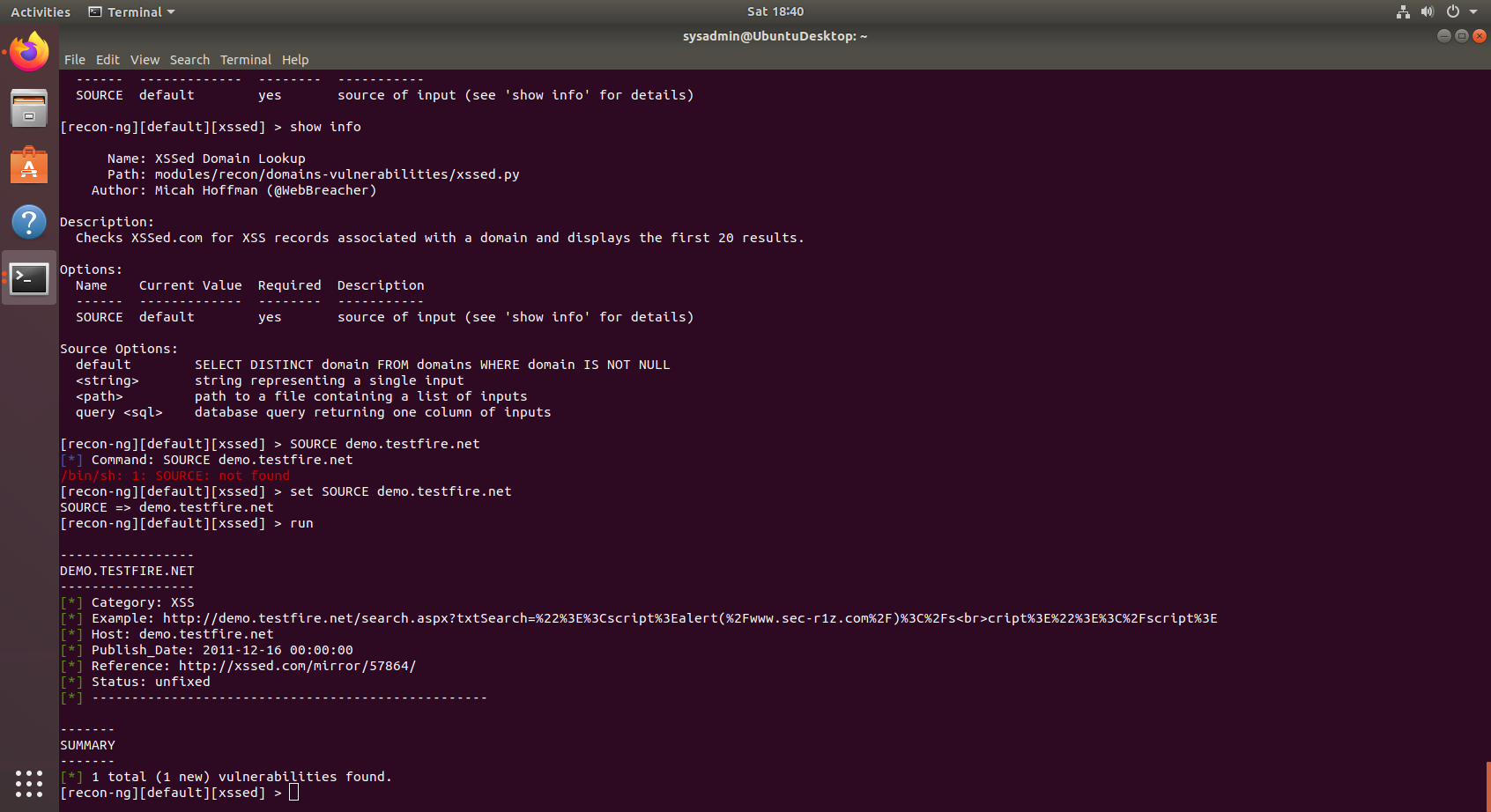
* What open ports and running services did Shodan find: *Ports; 80, 443, 8080 / Services; Apache Tomcat/Coyote JSP engine1.1 – cookies and SSL*



**Step 4: Recon-ng**

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

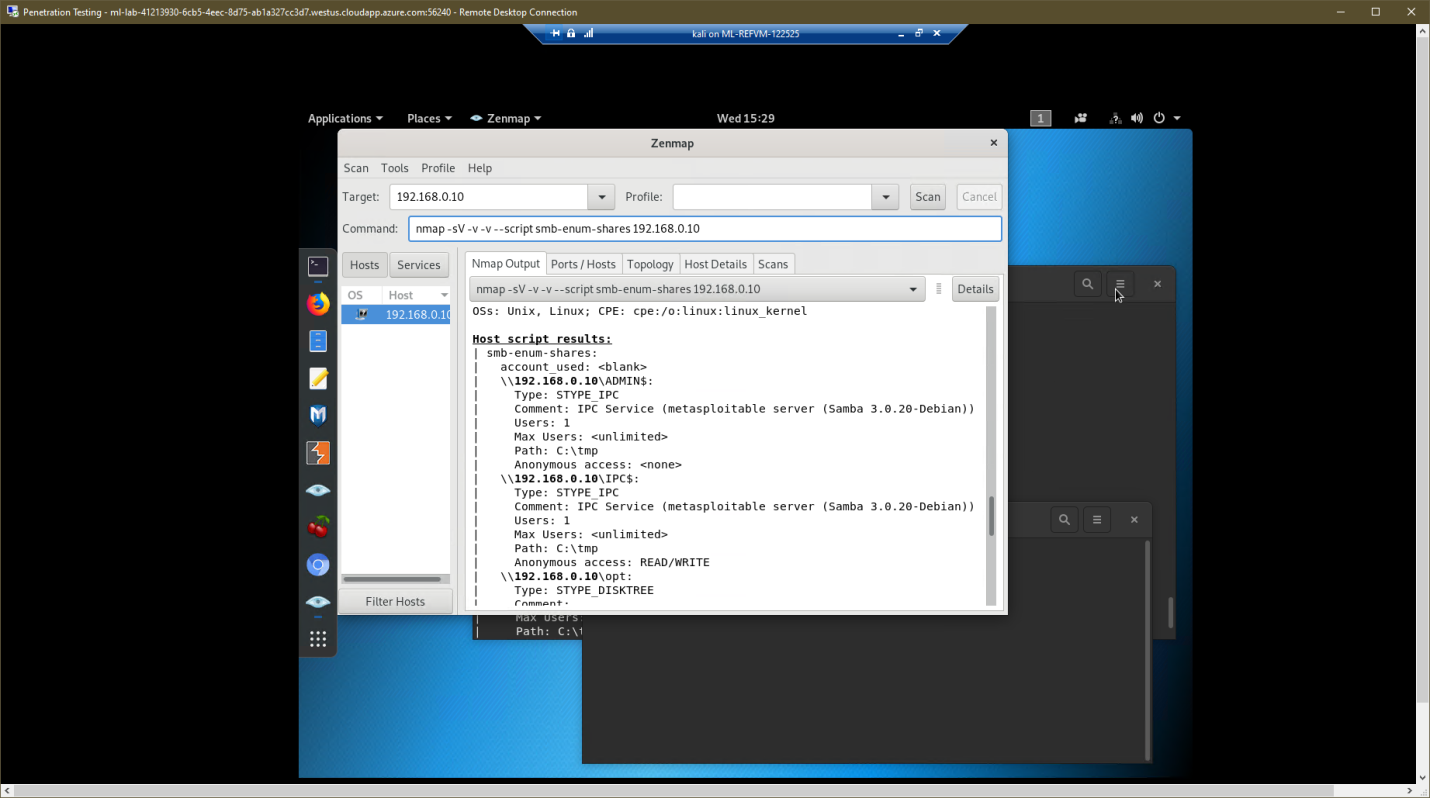
Is Altoro Mutual vulnerable to XSS: *According to the xssed reference:* [*http://xssed.com/mirror/57864/*](http://xssed.com/mirror/57864/) *the demo.testfire.net XSS vulnerability is not fixed.*

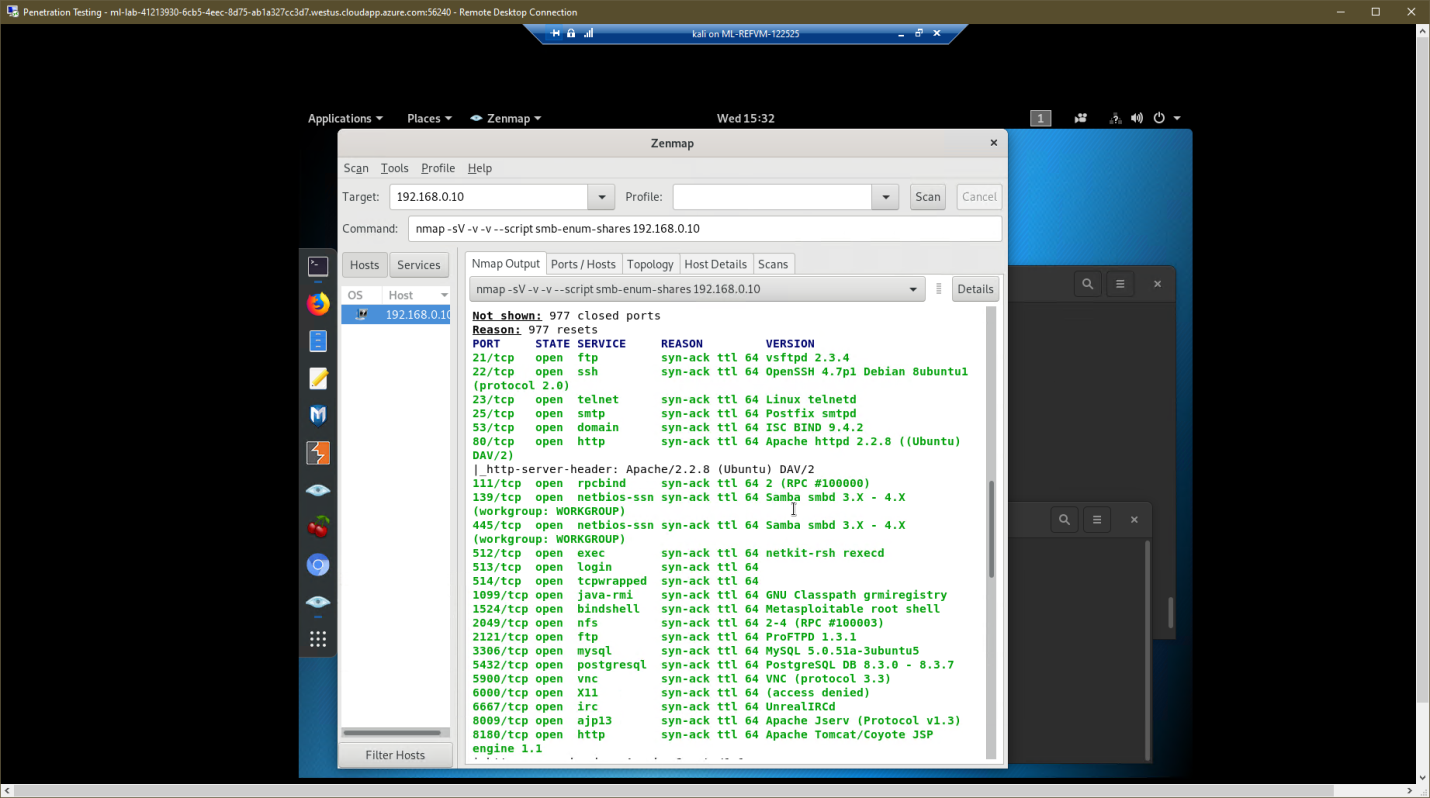
**

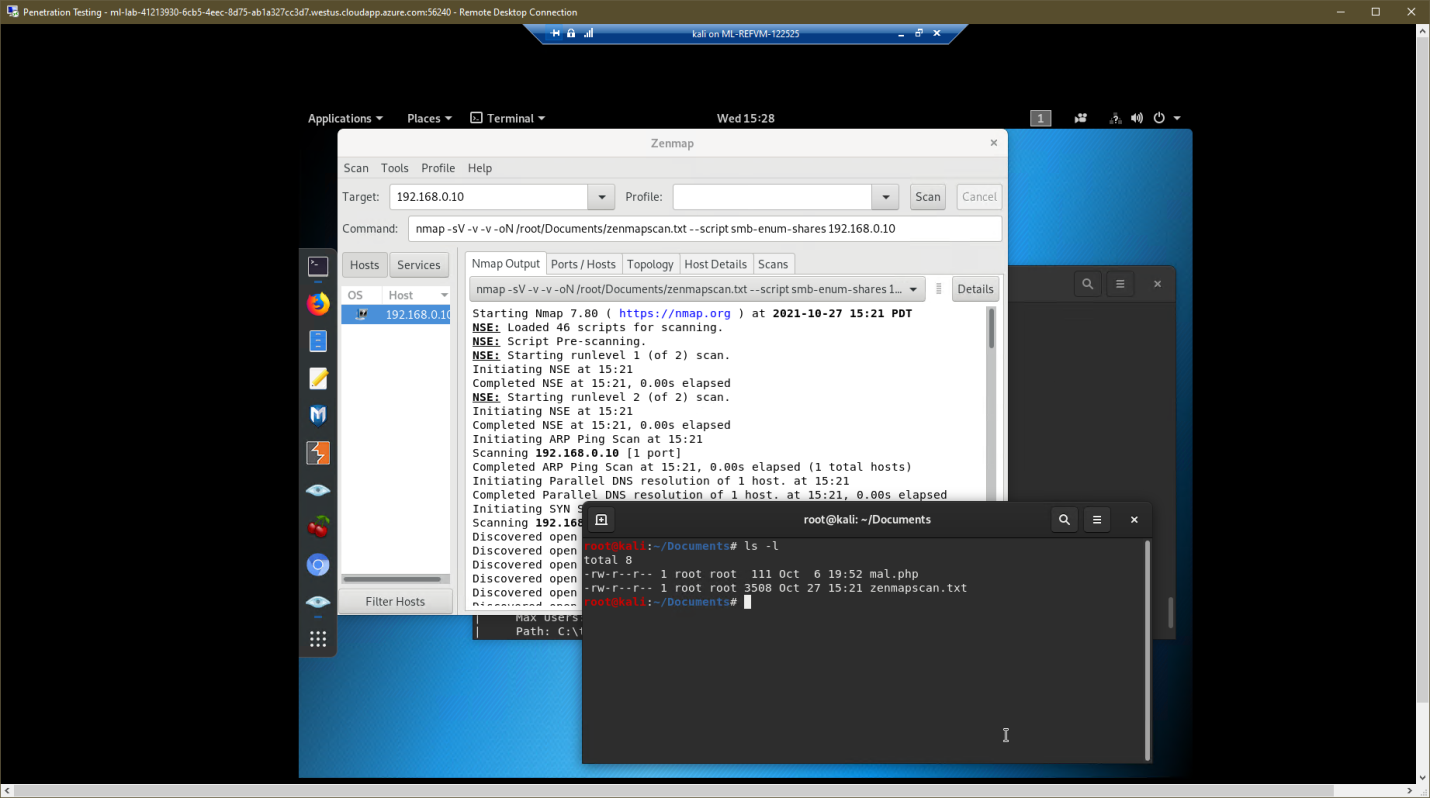
**Step 5: Zenmap**

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 -vv -oN /root/Documents/zenmapscan.txt --script smb-enum-shares 192.168.0.10*
* Zenmap vulnerability script command: *nmap -sV --script smb-enum-shares 192.168.0.10*







* Once you have identified this vulnerability, answer the following questions for your client:
* What is the vulnerability: *smb-enum-shares - We found that an exploitable version of Samba service running on ports139/445. Samba version 3.0.20-debian has a flaw that allows shares to be listed with srvsvc.NetShareGetInfo*

*Also:We found that tcp port 21 is open and vulnerable to a ftp-vsftpd-backdoor attack. The scan also exposed (7) port 80 web page actions that could possibly be vulnerable to CSRF attacks.*

* Why is it dangerous: *. smb-enum-share - Open share information can expose private information. Also if those shares are writable, malware or infected files can be delivered.*

*vsftpd-backdoor attack – vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp. This would allow attackers access to systems. Also, CSRF attacks would trick potential users to execute unwanted commands via their authenticated connection to port 80.*

* What mitigation strategies can you recommend for the client to protect their server:

*Update vsftpd on all servers. Add and enable CSRF token protection and authentication.*

*Update Samba to latest version to mitigate the flaw in version 3.0.20-debian.*

