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 be used for phishing attacks and gathering credentials or other information to access the system.

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, California
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

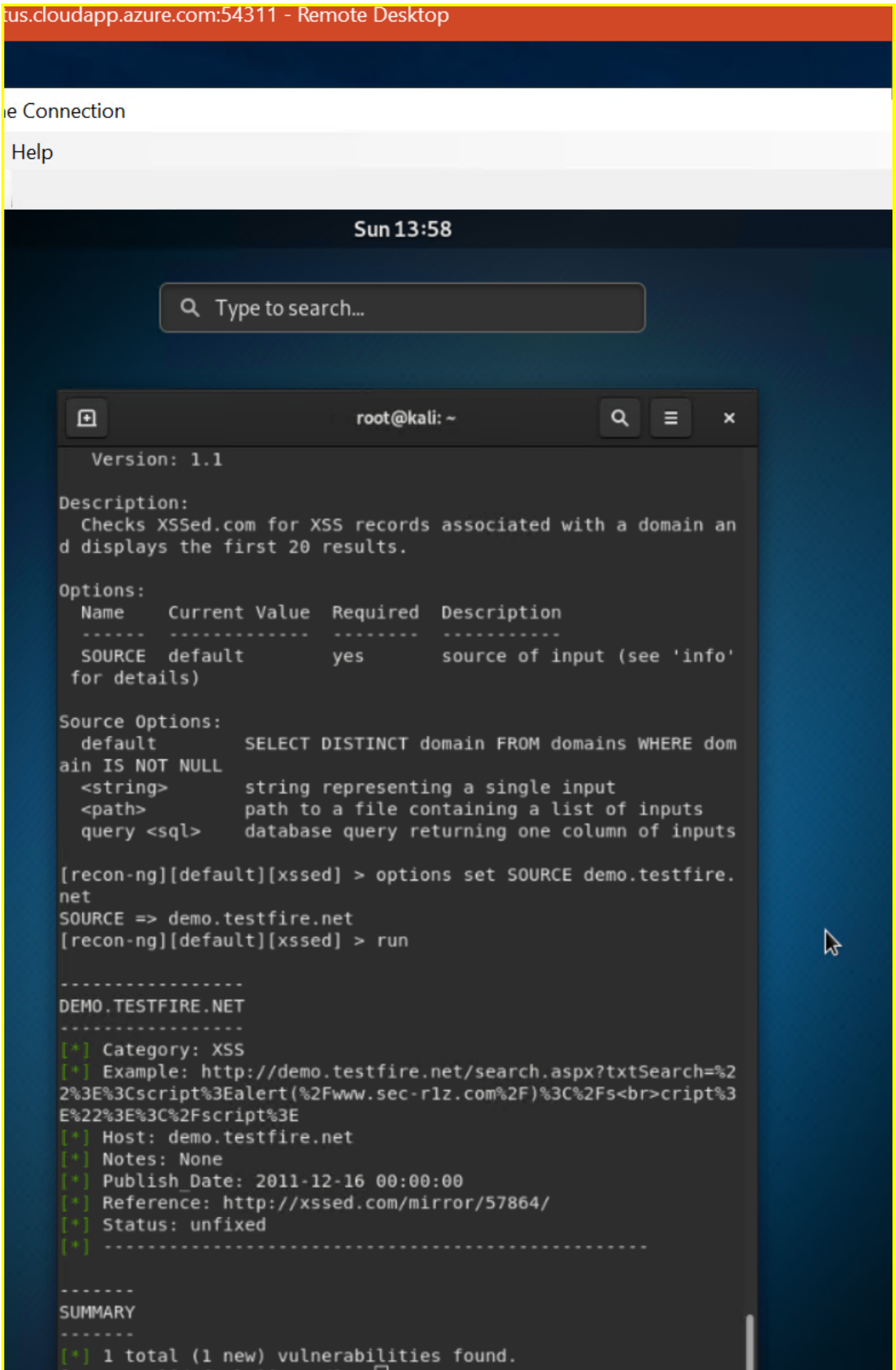
Step 3: Shodan

- What open ports and running services did Shodan find:Port 80 and 443 are open

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


us.cloudapp.azure.com:54311 - Remote Desktop
e Connection
Help
Sun 13:58
Type to search...
root@kali: ~
Version: 1.1
Description:
Checks XSSed.com for XSS records associated with a domain and displays the first 20 results.
Options:
Name Current Value Required Description
SOURCE default yes source of input (see 'info' for details)
Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][default][xssed] > options set SOURCE demo.testfire.net
SOURCE => demo.testfire.net
[recon-ng][default][xssed] > run
DEMO.TESTFIRE.NET
[*] Category: XSS
[*] Example: http://demo.testfire.net/search.aspx?txtSearch=%22%3E%3Cscript%3Ealert(%2Fwww.sec-r1z.com%2F)%3C%2Fs
cript%3E%22%3E%3C%2Fscript%3E
[*] Host: demo.testfire.net
[*] Notes: None
[*] Publish_Date: 2011-12-16 00:00:00
[*] Reference: http://xssed.com/mirror/57864/
[*] Status: unfixed
SUMMARY
[*] 1 total (1 new) vulnerabilities found.

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 –script nmap-vulners -p 139,445 192.168.0.10
- Once you have identified this vulnerability, answer the following questions for your client:

    1. What is the vulnerability: ports 139 and 445 where open which is a vulnerability for Samba or SMB exploits.

    2. Why is it dangerous: This is dangerous because these are file sharing ports allowing computers to communication with themselves. Samba allows Linux machines to communicate with Windows machines. If these are open another device can communicate with your device and alter or affect it.

    3. What mitigation strategies can you recommendations for the client to protect their server: in order to mitigate the effects this could have, it is recommended to update Samba to make sure it is running on the most recent version to reduce the chances of older exploits of SMB being used on the device.