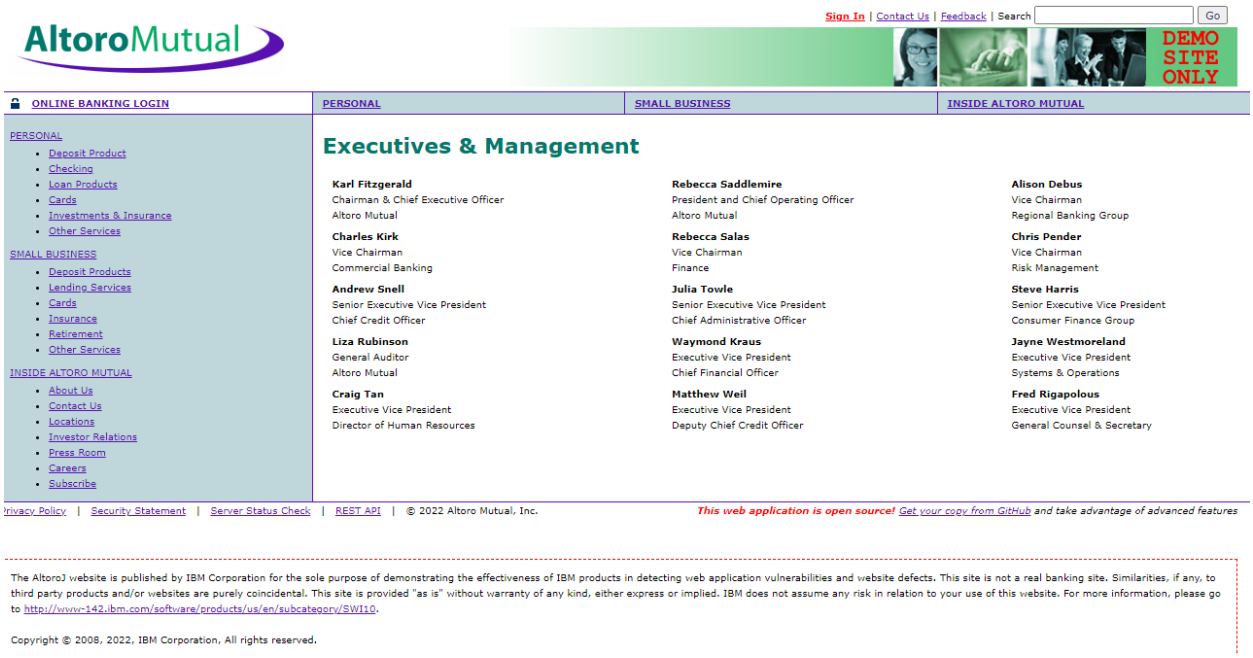
Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:
    - First navigate to demo.testfire.net
    - Once there, on the left hand side locate “Inside Altoro Mutual” and below that select “About Us” > Executives and Management Team >



Karl Fitzgerald, **Chairman & Chief Executive Officer of Altoro Mutual**

- How can this information be helpful to an attacker:

  An Attacker would look for this information for email phishing attacks against the CEO or employees working below them as an email from the CEO is very convincing.

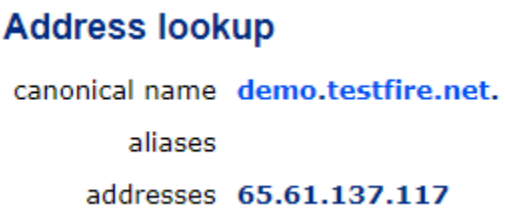
Step 2: DNS and Domain Discovery

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 94085 - USA
2. What is the NetRange IP address:
   `NetRange:  65.61.137.64 - 65.61.137.127`
3. What is the company they use to store their infrastructure:
    a. `CustName:  Rackspace Backbone Engineering`
    b. `Address:  9725 Datapoint Drive, Suite 100`

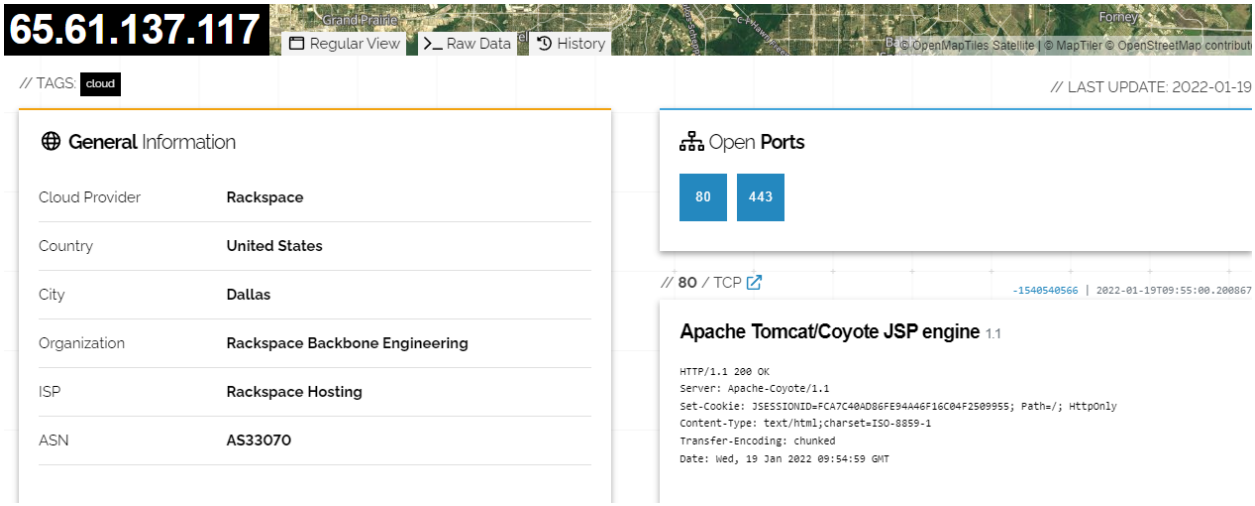
c. City: San Antonio
d. StateProv: TX
e. PostalCode: 78229
f. Country: US
g. RegDate: 2015-06-08
h. Updated: 2015-06-08
i. Ref: https://rdap.arin.net/registry/entity/C05762718

4. What is the IP address of the DNS server:



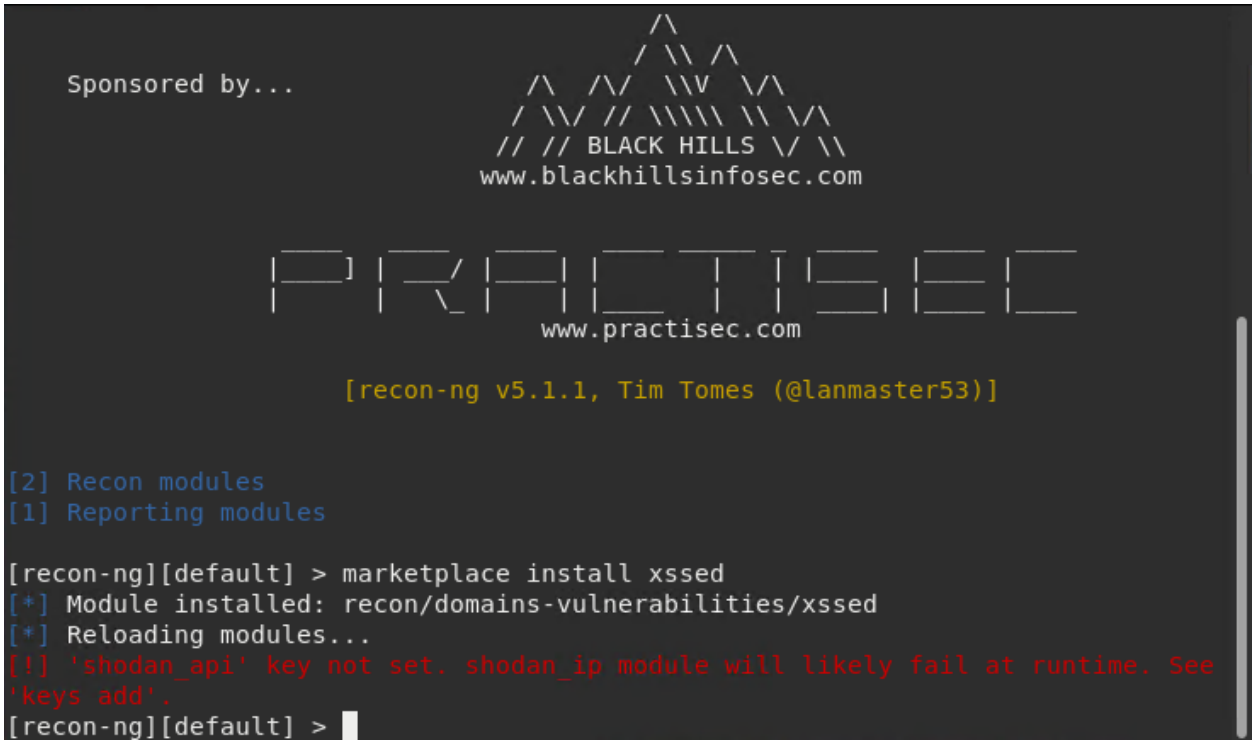
Step 3: Shodan

- What open ports and running services did Shodan find:

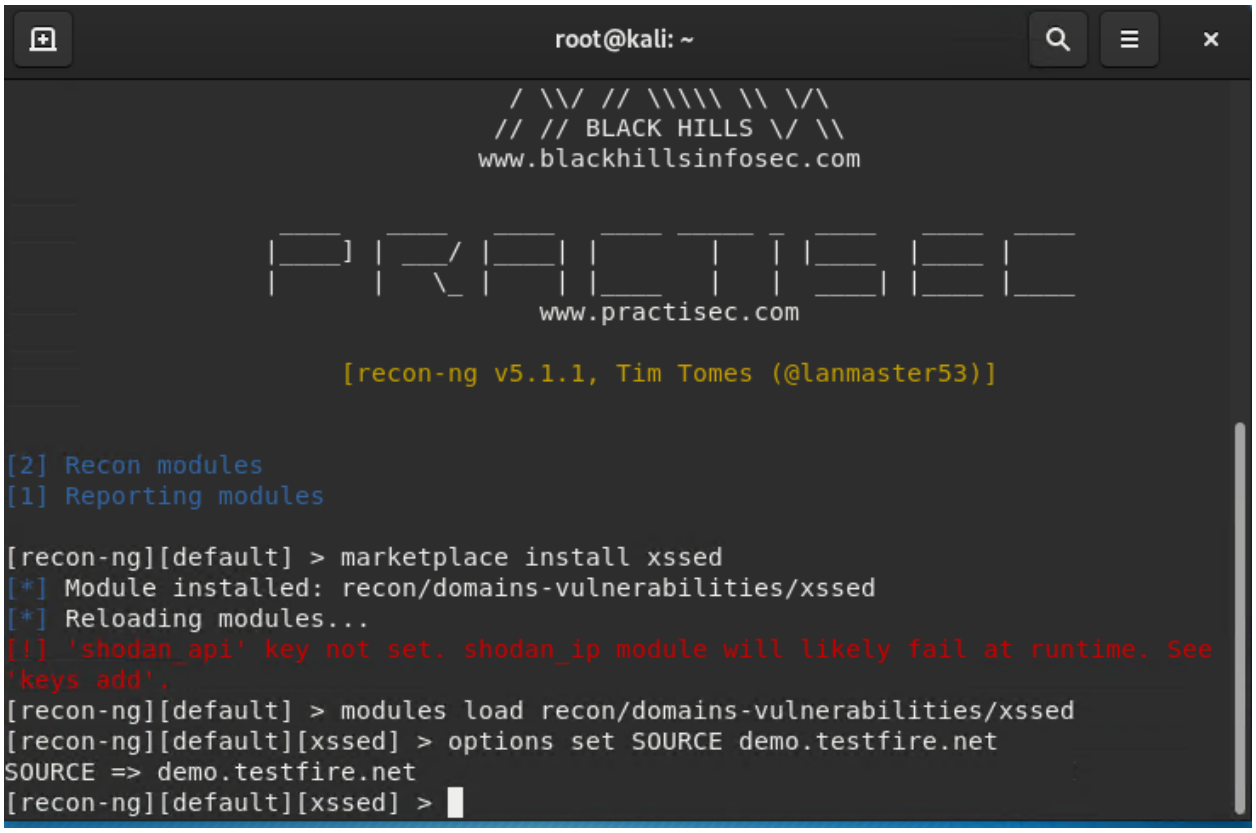


Step 4: Recon-ng

- Install the Recon module xssed.

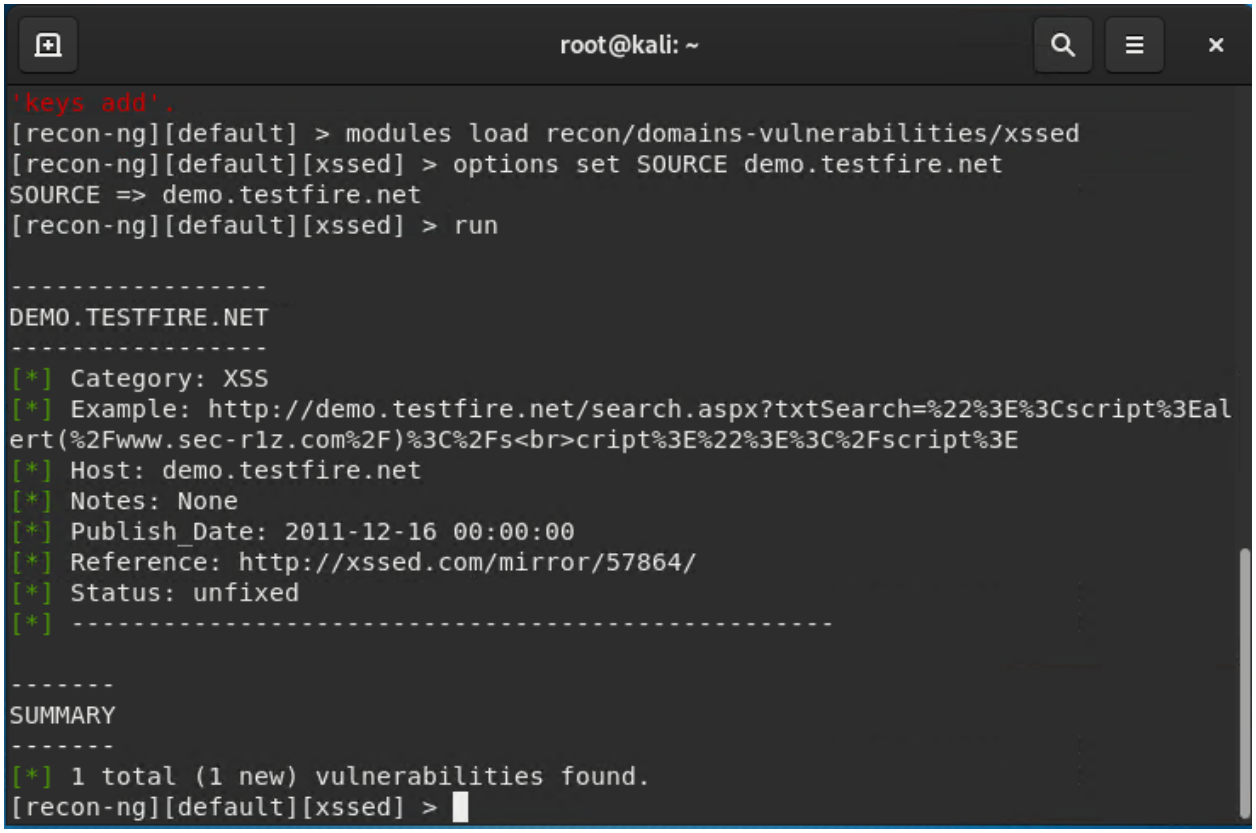


- Set the source to demo.testfire.net // The command for this is “options set SOURCE demo.testfire.net”



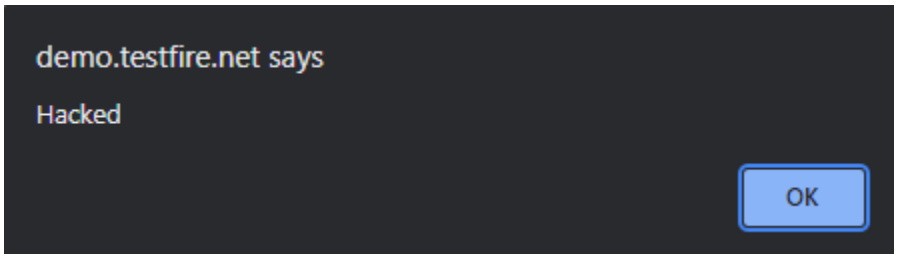
- Run the module.

We're going to now do this with the "run" command



Is Altoro Mutual vulnerable to XSS: **Yes, it also appears to be the only vulnerability found. To test this, we're going to do the following.**

Here's a script: *<script>alert("Hacked")</script>* We're going to load this script into the search bar of demo.testfire.net

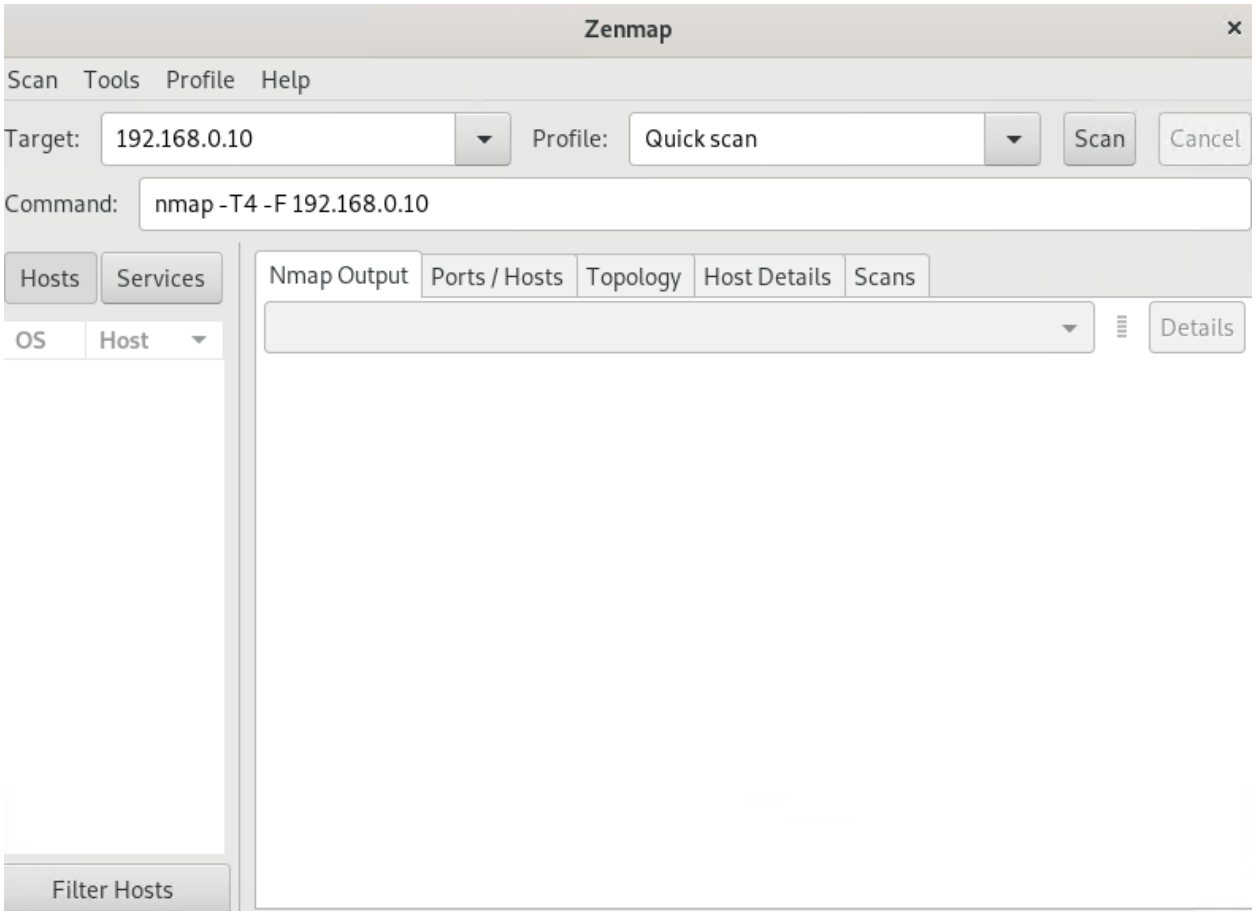


Tada!

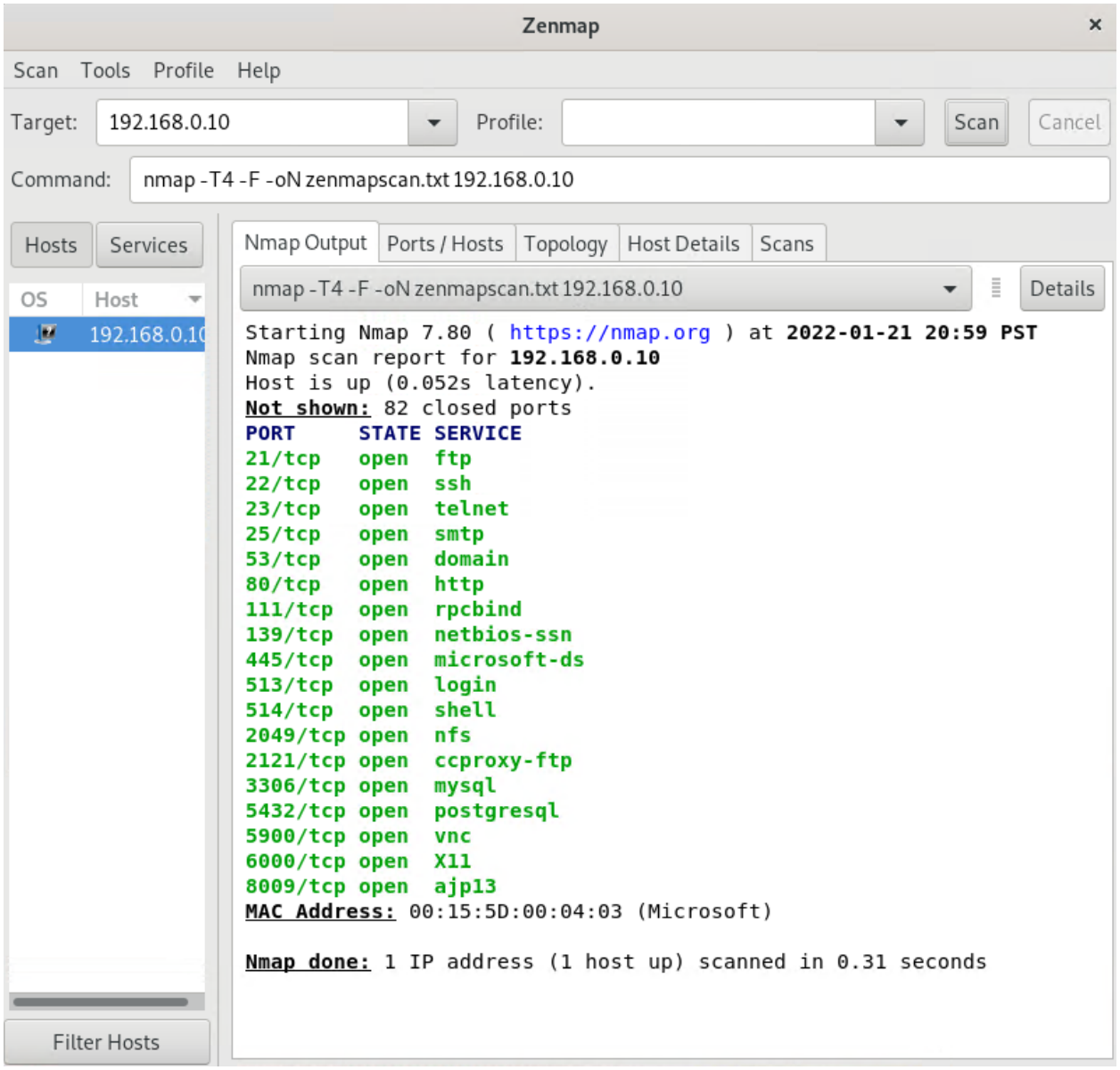
Step 5: Zenmap

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:

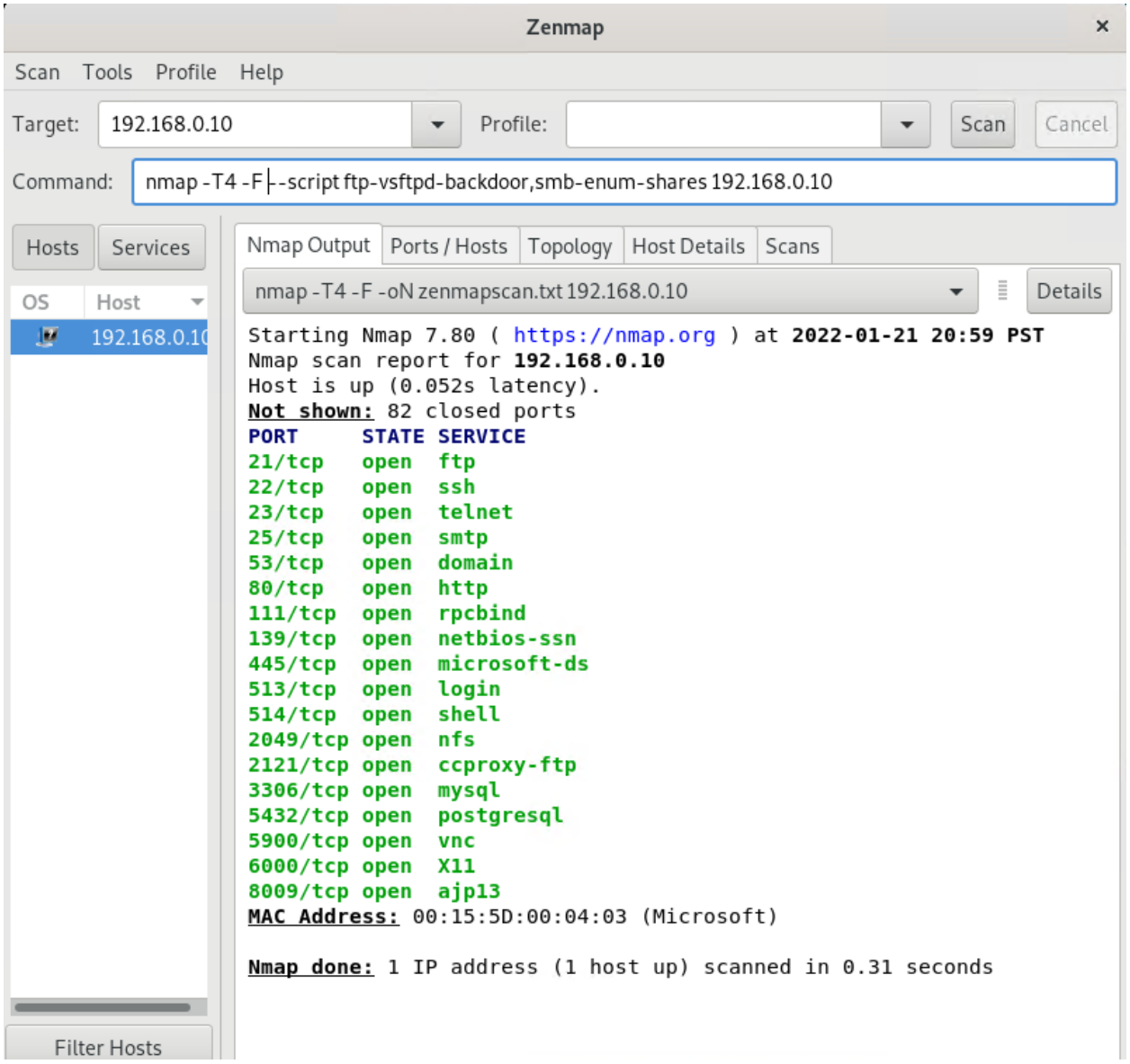
- Command for Zenmap to run a service scan against the Metasploitable machine:
    1. Run the Pentesting Lab from Azure
    2. Open Hyper-V-Manager to view available VM's
    3. Start "Kali" VM
    4. Open a terminal
    5. Enter "zenmap"
    6. We are then going to use the Metasploitable machine that's part of the Hyper-V-Manager with the address 192.168.0.10
    7. On our Zenmap application, input this ip into "Target"
    8. Set your profile scan to "Quick Scan"
    9. Then hit the "SCAN" button



- Bonus command to output results into a new text file named zenmapscan.txt:
    1. To save these results as a text file "zenmapscan.txt" you can add the command: -oN zenmapscan.txt



- Zenmap vulnerability script command:
    1. Two scripts that can be located in Zenmap for vulnerabilities associated with services running on the ports 139/445
        - From the Profile tab and select “Edit Selected Profile”
        - Select the *Scripting* tab and view all the scripts
        - Look for the scripts titled “ftp-vsftpd-backdoor” and “smb-enum-shares”
        - Then select “save changes”

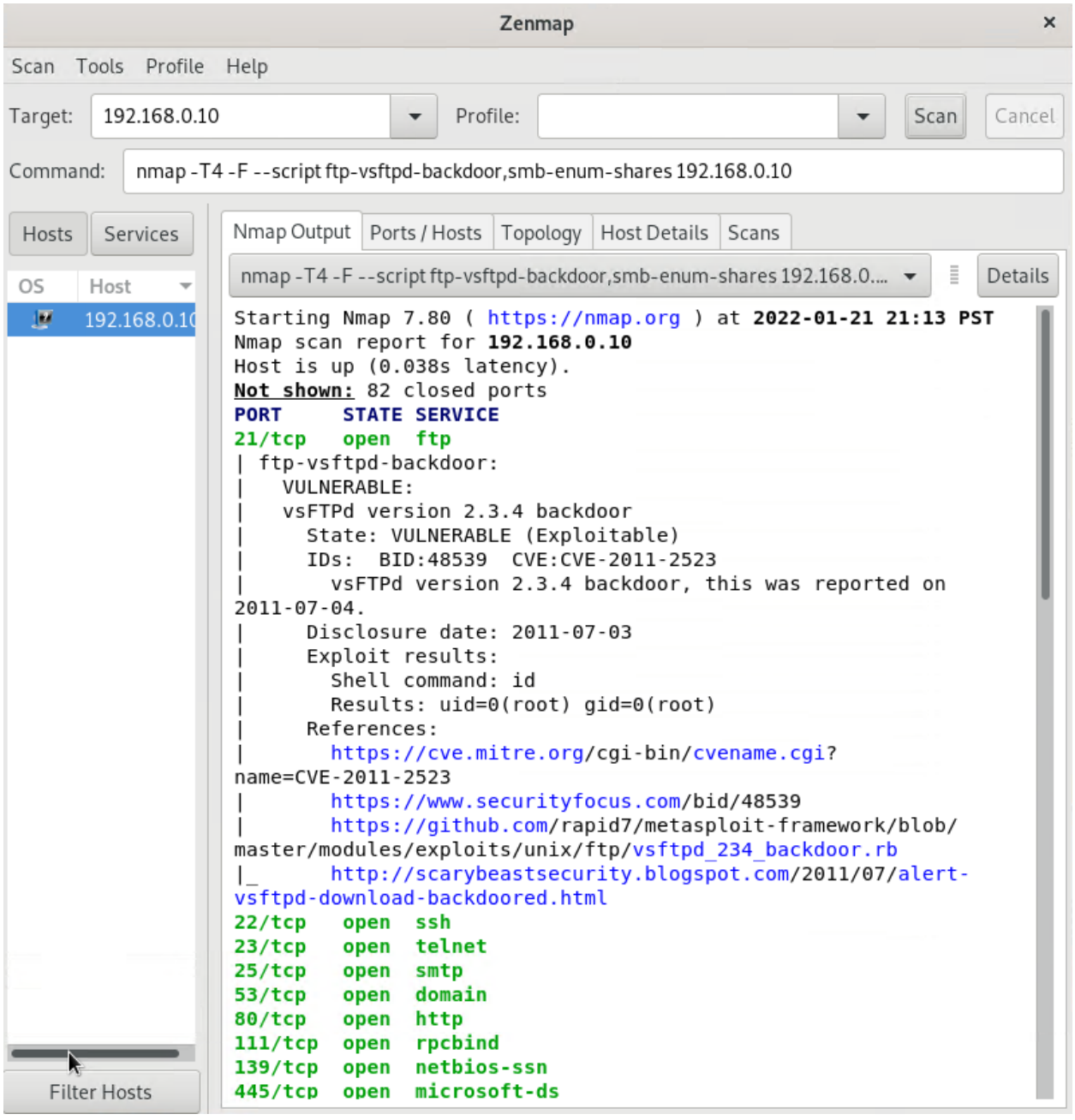


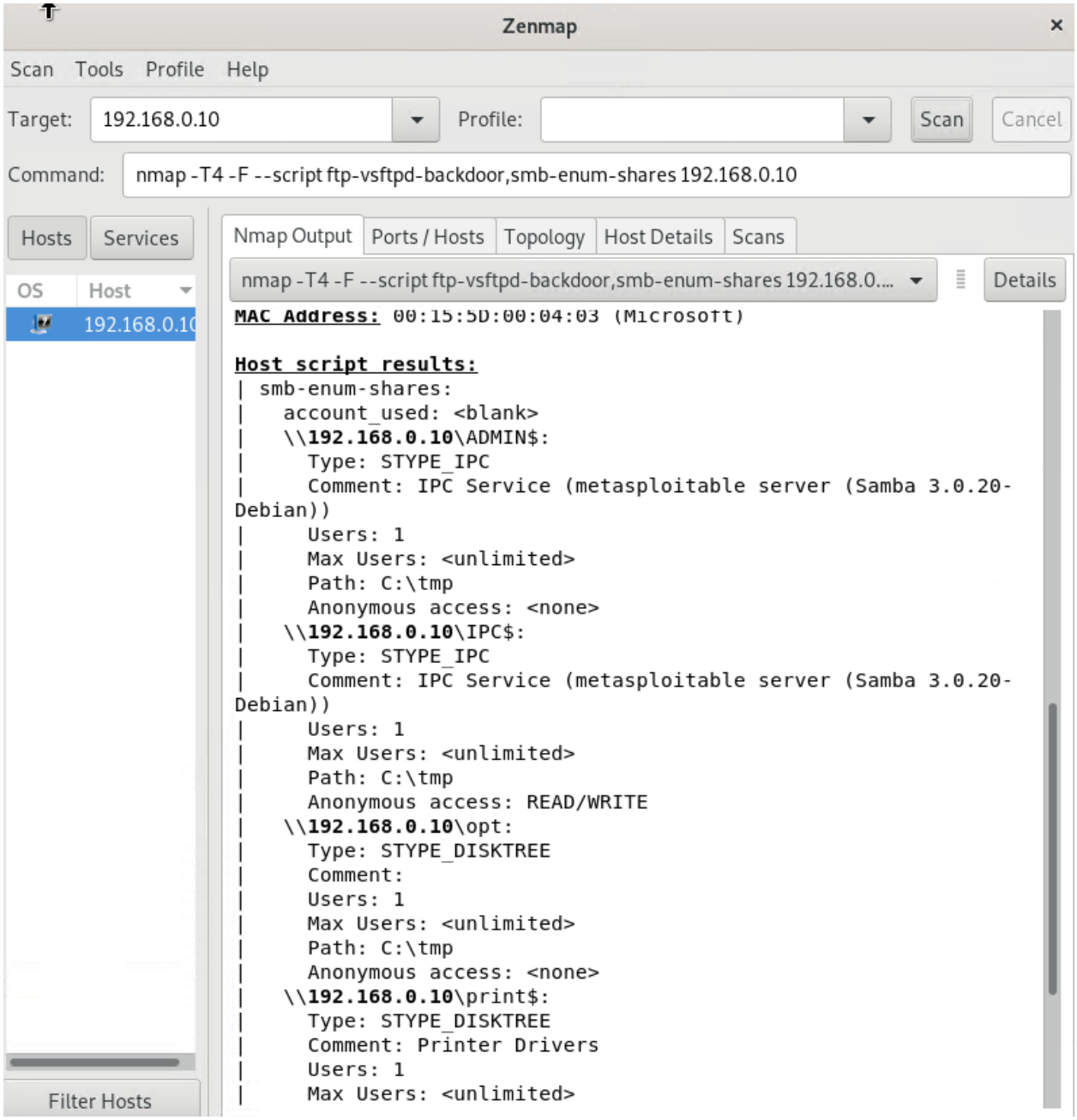
The command nmap -T4 -F --script ftp-vsftpd-backdoor,smb-enum-shares 192.168.0.10

- -T4: T<0-5>: Sets a timing template for how fast the command will run (higher is faster)
- -F: Fast mode - Scan fewer ports than the default scan
- --script: Runs the scripted scan that is followed
- Ftp-vsftpd-backdoor and Smb-enum-share are the exploit scripts that will be run
- 192.168.0.10: The IP address of our Metasploitable platform that will be scanned

Once you have identified this vulnerability, answer the following questions for your client:

1. What is the vulnerability:


Zenmap
Scan Tools Profile Help
Target: 192.168.0.10
Profile:
Scan
Cancel
Command: nmap -T4 -F --script ftp-vsftpd-backdoor,smb-enum-shares 192.168.0.10
Hosts
Services
OS
Host
192.168.0.10
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F --script ftp-vsftpd-backdoor,smb-enum-shares 192.168.0....
Details
Starting Nmap 7.80 (https://nmap.org) at 2022-01-21 21:13 PST
Nmap scan report for 192.168.0.10
Host is up (0.038s latency).
Not shown: 82 closed ports
PORT STATE SERVICE
21/tcp open ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539 CVE:CVE-2011-2523
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.securityfocus.com/bid/48539
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_ http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds



We can see ports 139/445 down at the bottom as vulnerable, along with a few others.

2. Why is it dangerous:
    - The danger of this is due to the VSFTPD 2.3.4 backdoor attack that is applied on port 21 through malicious code. Upon success of the code, port 6200 is opened as a backdoor
    - The Windows Server Message Block (SMB) allows access through an organization's networks through use of SMB protocols. The purpose of these protocols is for file and printer sharing, along with the remote

access services.

3. What mitigation strategies can you recommendations for the client to protect their server:
   VSFPTD 2.3.4 can be fixed with updating to subsequent patches that are constantly being updated
   - SMB (CVE-2017-0145) patch was released by Microsoft MS17-010, and SAMBA (CVE-2017-0145) patches were released by Red Hat for Linus RHSA-2017:1390