

**Step 1: Google Dorking**

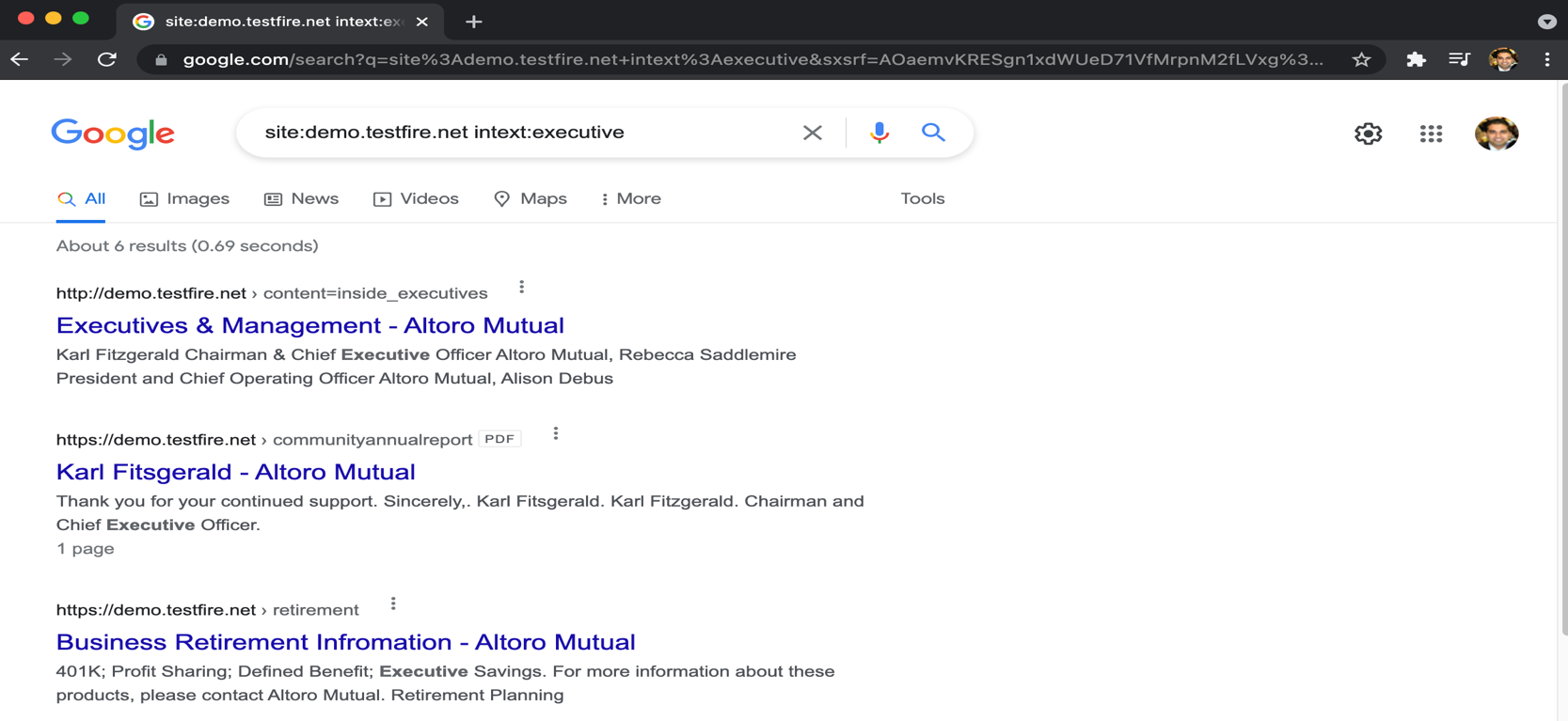
1. Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:

**Answer: -** Karl Fitzgerald Chairman & Chief Executive Officer Altoro Mutual, Rebecca Saddlemire President and Chief Operating Officer Altoro Mutual, Alison Debus

**Note: -** To find on google.com - **site:demo.testfire.net intext:executive.**

1. How can this information be helpful to an attacker:

**Answer: -** Well, Chief executive officer is the import part of the company and hold all of the company access and information. It will be easy for attacker to send phishing email directly to the chief executive officer.



**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:

**Answer: -** Registrant City: **Sunnyvale**

Registrant State/Province: **CA**

Registrant Postal Code: **94085**

Registrant Country: **US**

1. What is the NetRange IP address:

**Answer: -** NetRange: 65.61.137.64 - 65.61.137.127

3. What is the company they use to store their infrastructure:

**Answer: -** CustName: Rackspace Backbone Engineering (C05762718)

Address: 9725 Datapoint Drive, Suite 100

City: San Antonio

StateProv: TX

PostalCode: 78229

Country: US

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

**Answer: -** 65.61.137.117

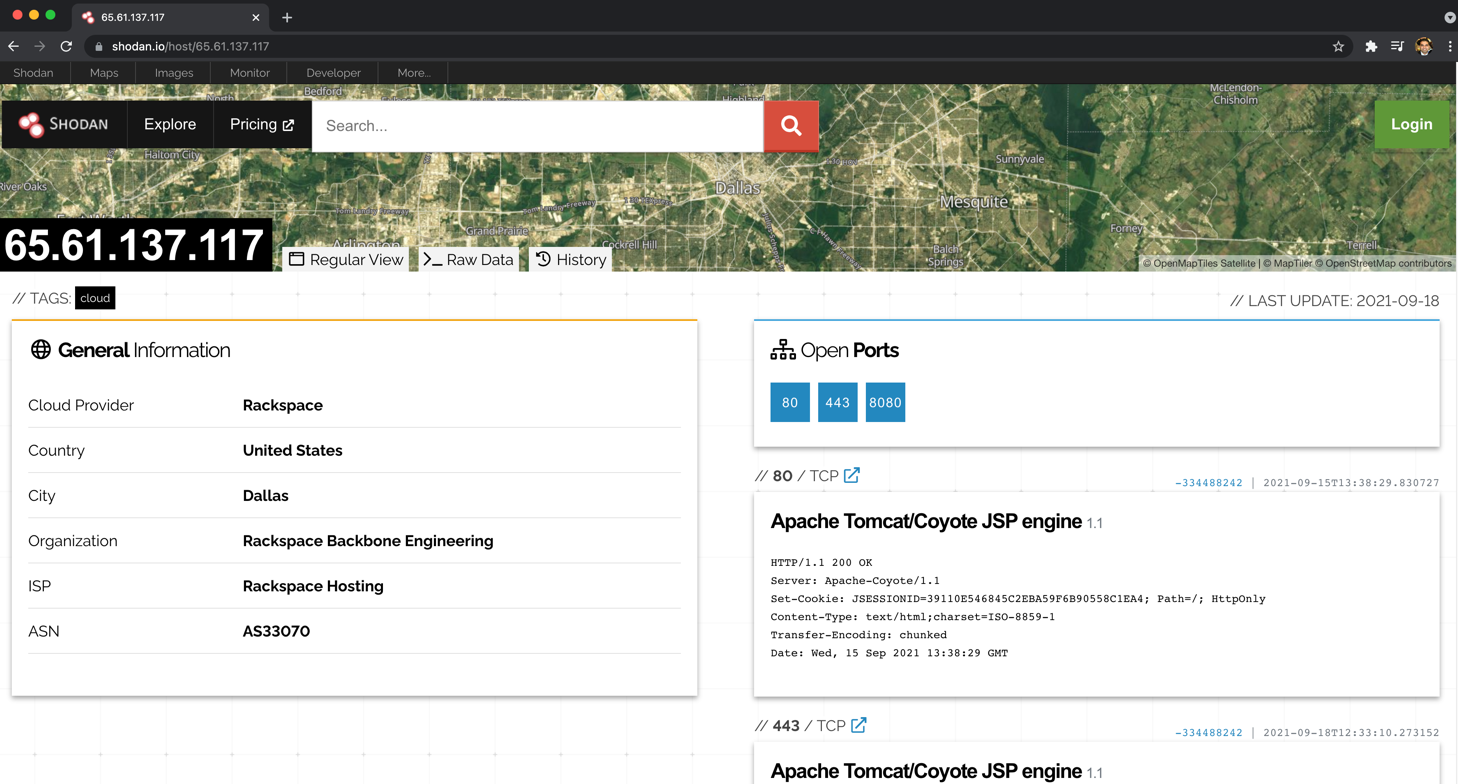


**Step 3: Shodan**

1. What open ports and running services did Shodan find:

**Answer: -** https://www.shodan.io/host/65.61.137.117

Open Ports: 80, 443, 8080 - Services: Apache Tomcat/Coyote JSP Engine (version 1.1)



**Step 4: Recon-ng**

- Install the Recon module `xssed`.

- Set the source to `demo.testfire.net`.

- Run the module.

1. Is Altoro Mutual vulnerable to XSS:

**Answer: -** Yes, only one vulnerability found. I have mentioned script below how to search for the vulnerability.

**Commands: -** marketplace install xssed

modules load recon/hosts-ports/shodan\_ip

keys add shodan\_api yKC1OHMTFyjP80nl0E7ObMQB6HS1KSMP

modules load recon/domains-vulnerablilities/xssed

options set SOURCE demo.testfire.net

run

modules load reporting/html

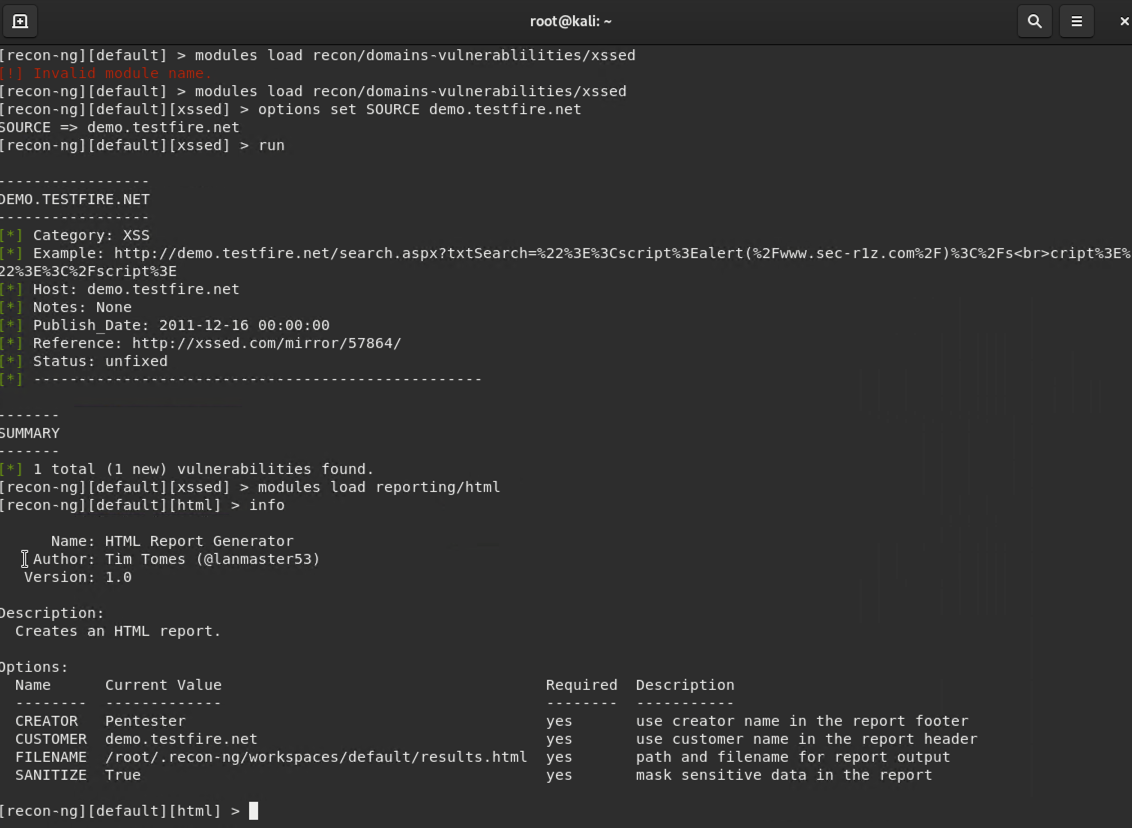
info

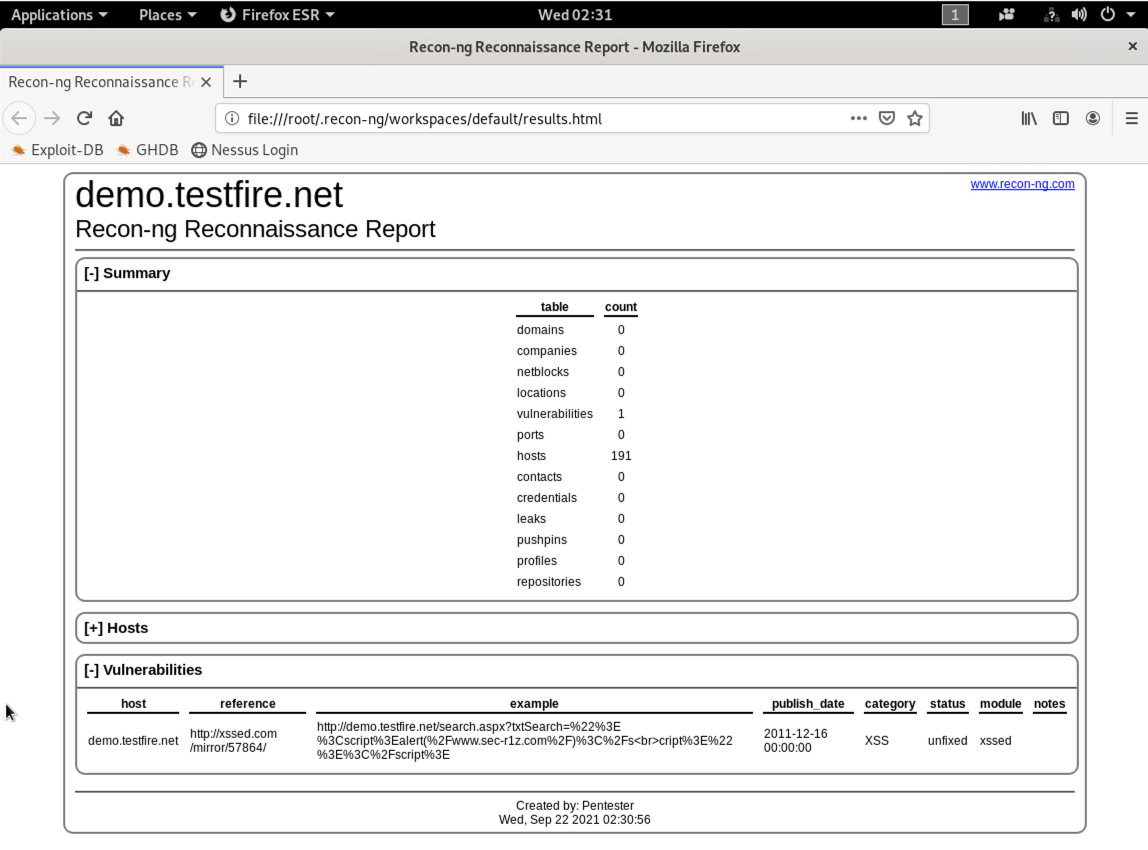
options set CREATOR Pentester

options set CUSTOMER demo.testfire.net

xdg-open /root/.recon-ng/workspaces/default/results.html









**Step 5: Zenmap**

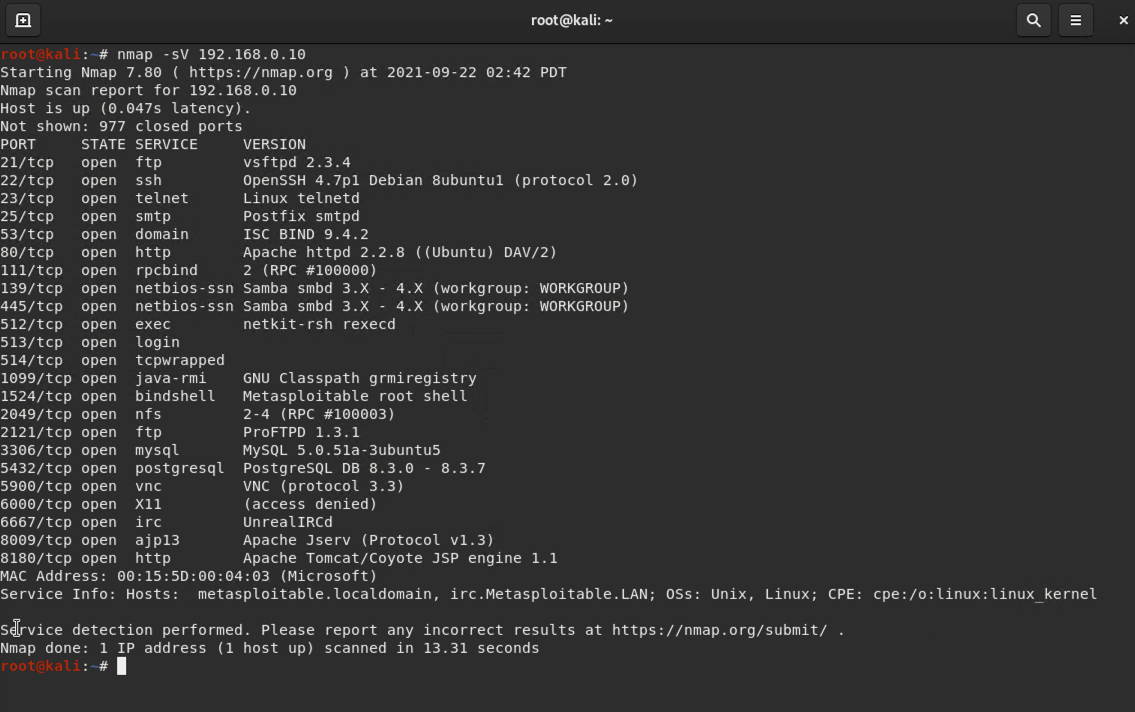
Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

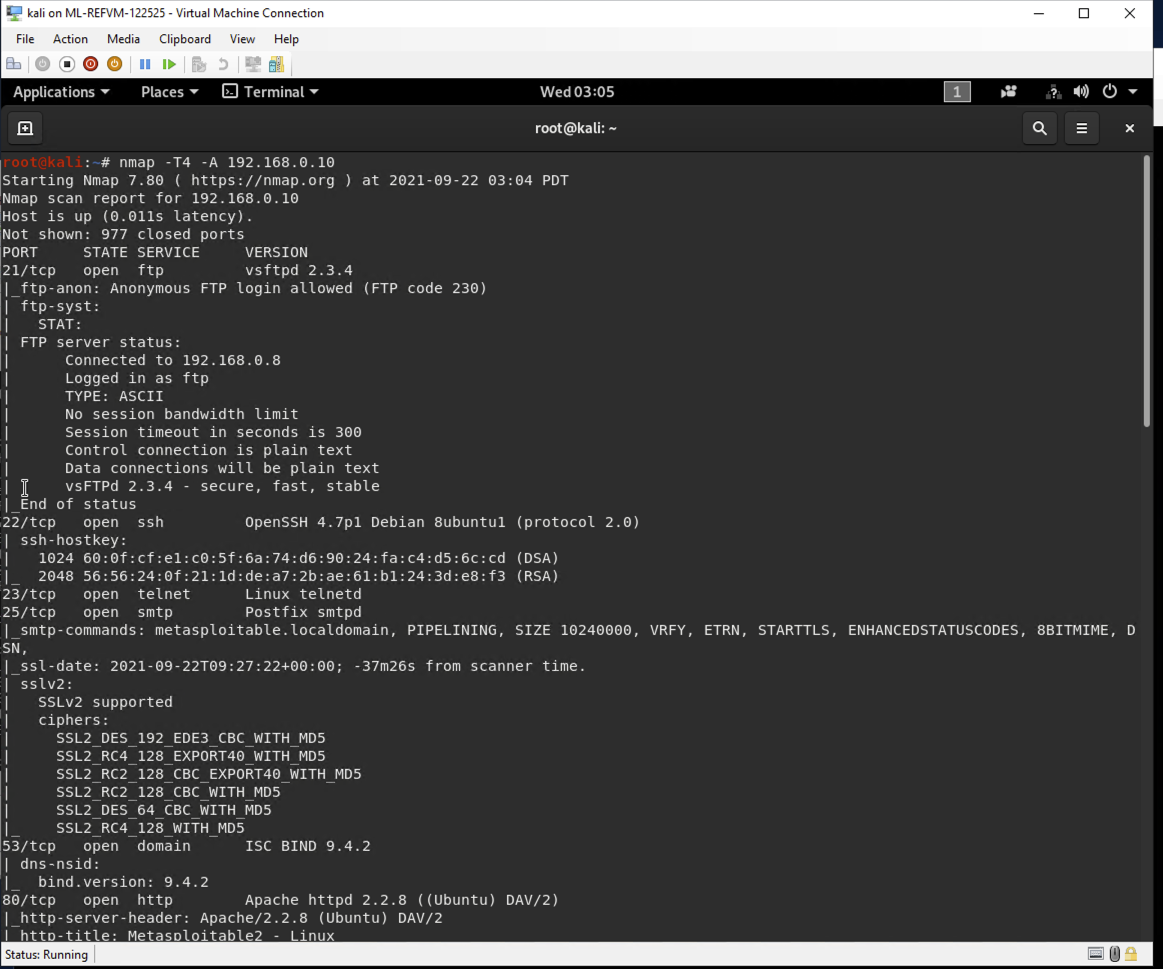
1. Command for Zenmap to run a service scan against the Metasploitable machine:

**Command: -** **nmap -sV 192.168.0.10**

**or**

**nmap -T4 -A 192.168.0.10**







1. Bonus command to output results into a new text file named `zenmapscan.txt`:

**Command: - nmap -sV 192.168.0.10 > zenmapscan.txt**

**or**

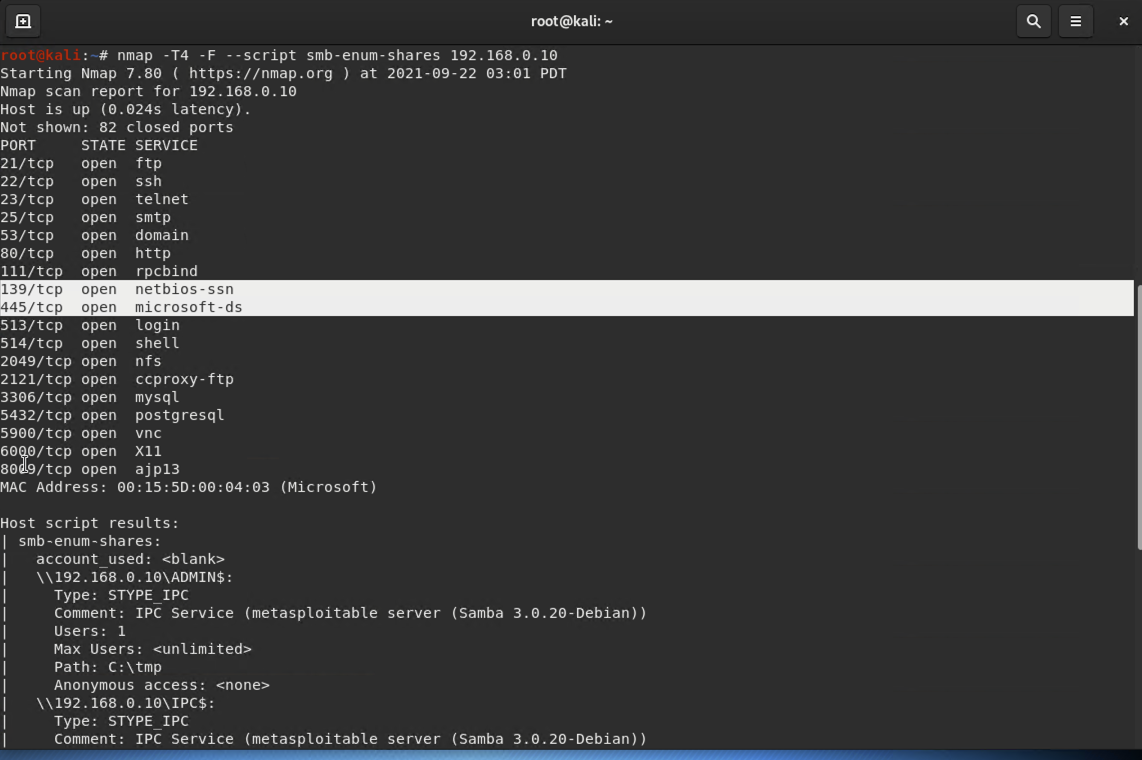
**nmap -T4 -A 192.168.0.10 -oN zenmapscan.txt**

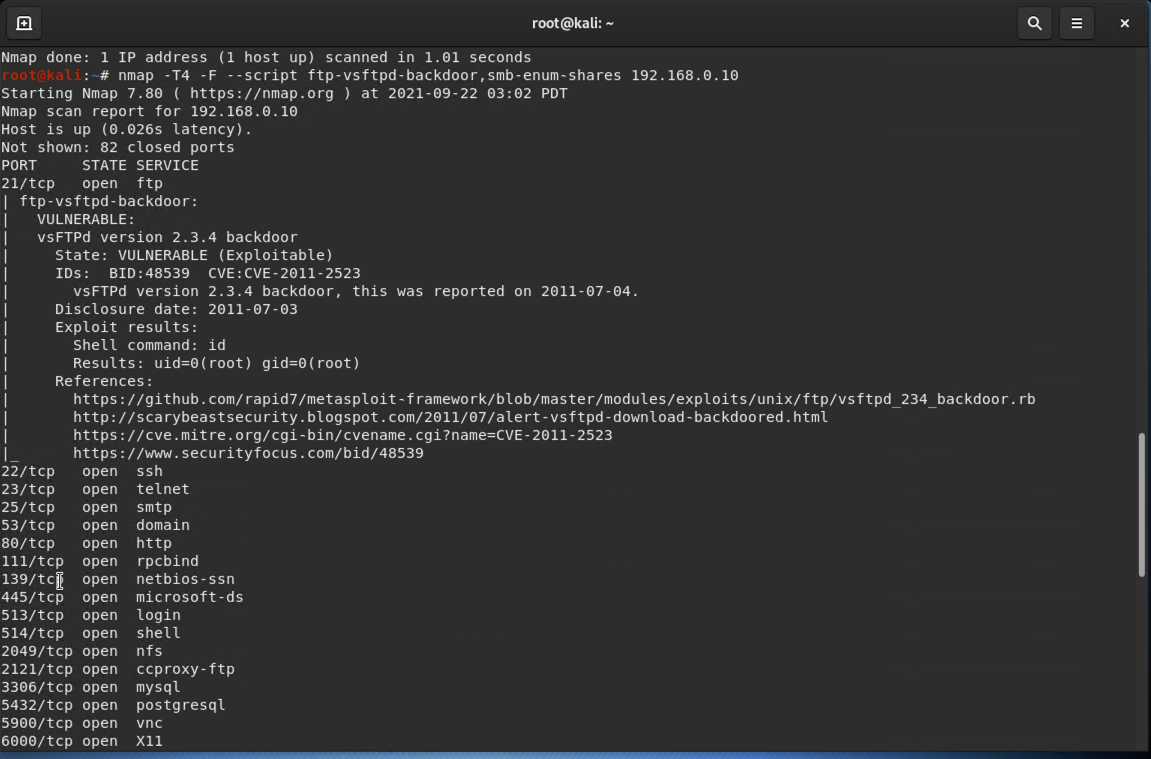
1. Zenmap vulnerability script command:

**Command: - nmap -T4 -F --script smb-enum-shares 192.168.0.10**

**Or**

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





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

1) What is the vulnerability:

**Answer: -** Zenmap did found the vulnerable service, below are the details.

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

Host script results:

smb-enum-shares:

account\_used: <blank>

\\192.168.0.10\ADMIN$:

Type: STYPE\_IPC

Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))

User: 1

Max Users: <unlimited>

Path: C:\tmp

Anonymous access: <none>

\\192.168.0.10\IPC$

Type: STYPE\_IPC

Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))

User:1

Max Users: <unlimited>

Path: C:\tmp

Anonymous access: READ/WRITE

\\192.168.0.10\tmp:

Type: STYPE\_DISKTREE

Comment: oh noes!

User: 1

Max Users: <unlimited>

Path: C:\tmp

Anonymous access: READ/WRITE

2) Why is it dangerous:

**Answer: -** Well, as you can see the hacker attack method on vsFTPD version 2.3.4 backdoor and SMB vulnerabilities, it give attacker permission to upload a shared library or spread payloads through connected systems and attacker can load the server & execute and it’s impacting on the CIA triad for example files shared on system, complete loss of protection, and delete file in the system.

3) What mitigation strategies can you recommendations for the client to protect their server:

**Answer: -** The vsFTPD v2.3.4 service was running as root and unlikely this version wont encounter vulnerability in a live situation because this version of VSFTPD is outdated and was only available for one day. Also from Microsoft a patch was released in march 2017 and there are few solution for it, apply SMB patch for samba, remove anonymous permissions from the server and block port services and most important is the vsFTPD version 2.3.4 contained backdoor and if we update the latest version of the vsFTPD there will be possible way to mitigate this risk.

Thank you,

Aziz Somani