

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 >

Altoro Mutual

Sign In | Contact Us | Feedback | Search Go

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Executives & Management

Karl Fitzgerald Chairman & Chief Executive Officer Altoro Mutual	Rebecca Saddlemyre President and Chief Operating Officer Altoro Mutual	Alison Debus Vice Chairman Regional Banking Group
Charles Kirk Vice Chairman Commercial Banking	Rebecca Salas Vice Chairman Finance	Chris Pender Vice Chairman Risk Management
Andrew Snell Senior Executive Vice President Chief Credit Officer	Julia Towle Senior Executive Vice President Chief Administrative Officer	Steve Harris Senior Executive Vice President Consumer Finance Group
Liza Robinson General Auditor Altoro Mutual	Waymond Kraus Executive Vice President Chief Financial Officer	Jayne Westmoreland Executive Vice President Systems & Operations
Craig Tan Executive Vice President Director of Human Resources	Matthew Weil Executive Vice President Deputy Chief Credit Officer	Fred Rigapolous Executive Vice President General Counsel & Secretary

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

The Altoro2 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

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:

- Where is the company located:
Sunnyvale, CA 94085 - USA
- What is the NetRange IP address:
NetRange: 65.61.137.64 - 65.61.137.127
- What is the company they use to store their infrastructure:
 - CustName: Rackspace Backbone Engineering
 - 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:

Address lookup

canonical name **demo.testfire.net.**

aliases

addresses **65.61.137.117**

Step 3: Shodan

- What open ports and running services did Shodan find:

65.61.137.117 Regular View Raw Data History

// TAGS: cloud // LAST UPDATE: 2022-01-19

General Information	
Cloud Provider	Rackspace
Country	United States
City	Dallas
Organization	Rackspace Backbone Engineering
ISP	Rackspace Hosting
ASN	AS33070

Open Ports	
80	443

// 80 / TCP [🔗](#) -1540540566 | 2022-01-19T09:55:00.200867

Apache Tomcat/Coyote JSP engine 1.1

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=FCA7C40AD86FE94A46F16C04F2509955; Path=/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2022 09:54:59 GMT
  
```

Step 4: Recon-ng

- Install the Recon module xssed.

```
Sponsored by...

      /\
     /\ \  /\
    /\  /\ \  /\ \
   /\  /\ \  /\ \  /\ \
  /\  /\ \  /\ \  /\ \  /\ \
 // // BLACK HILLS \/\ \
www.blackhillsinfosec.com

PRAC TISEC
www.practisec.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[2] Recon modules
[1] Reporting modules

[recon-ng][default] > marketplace install xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See
'keys add'.
[recon-ng][default] > 
```

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

```
root@kali: ~

      /\
     /\ \  /\
    /\  /\ \  /\ \
   /\  /\ \  /\ \  /\ \
  /\  /\ \  /\ \  /\ \  /\ \
 // // BLACK HILLS \/\ \
www.blackhillsinfosec.com

PRAC TISEC
www.practisec.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[2] Recon modules
[1] Reporting modules

[recon-ng][default] > marketplace install xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See
'keys add'.
[recon-ng][default] > modules load recon/domains-vulnerabilities/xssed
[recon-ng][default][xssed] > options set SOURCE demo.testfire.net
SOURCE => demo.testfire.net
[recon-ng][default][xssed] > 
```

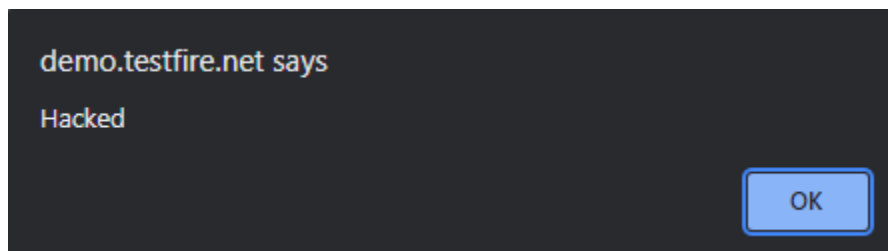
- Run the module.

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

```
root@kali: ~  
'keys add'.  
[recon-ng][default] > modules load recon/domains-vulnerabilities/xssed  
[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-rlz.com%2F)%3C%2Fs<br>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.  
[recon-ng][default][xssed] > 
```

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

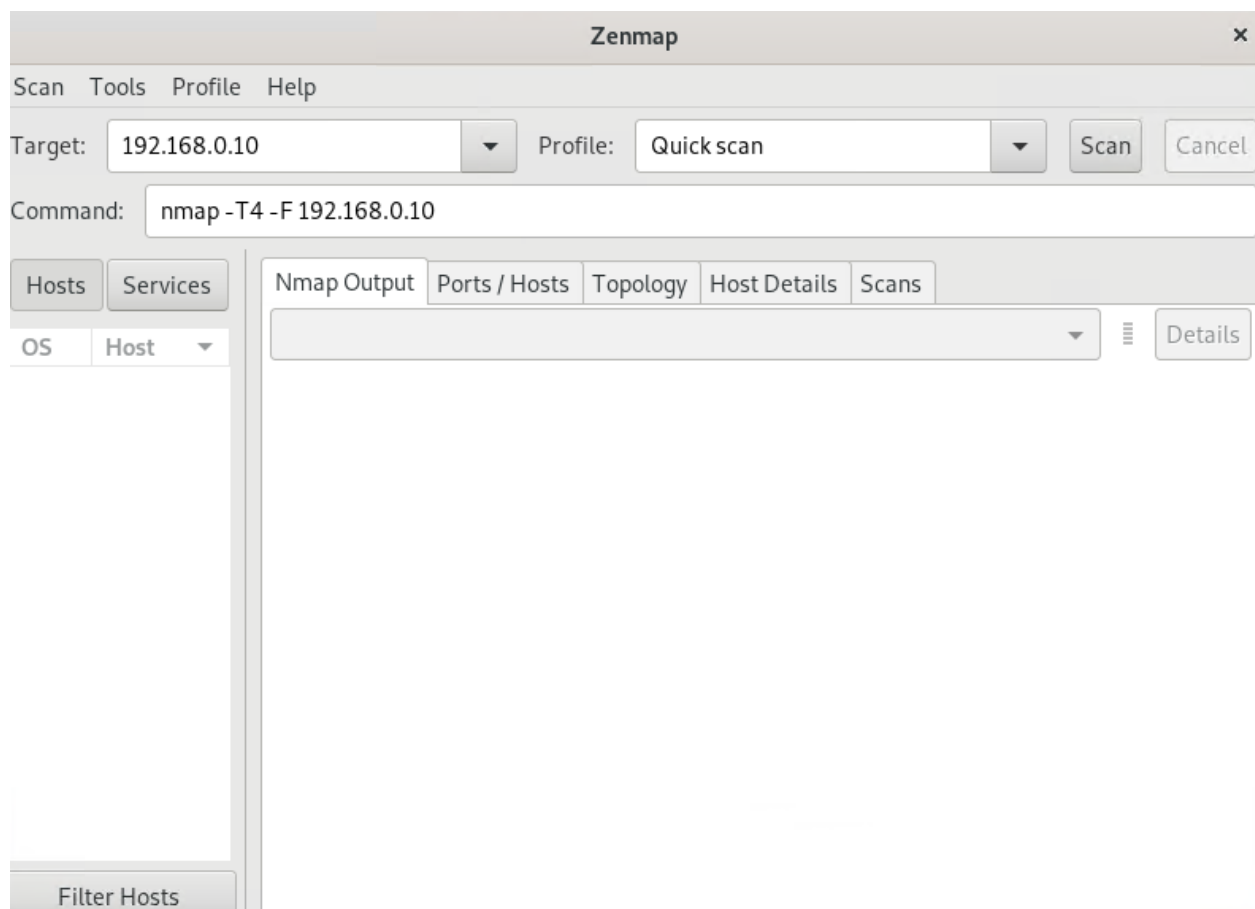


Tada!

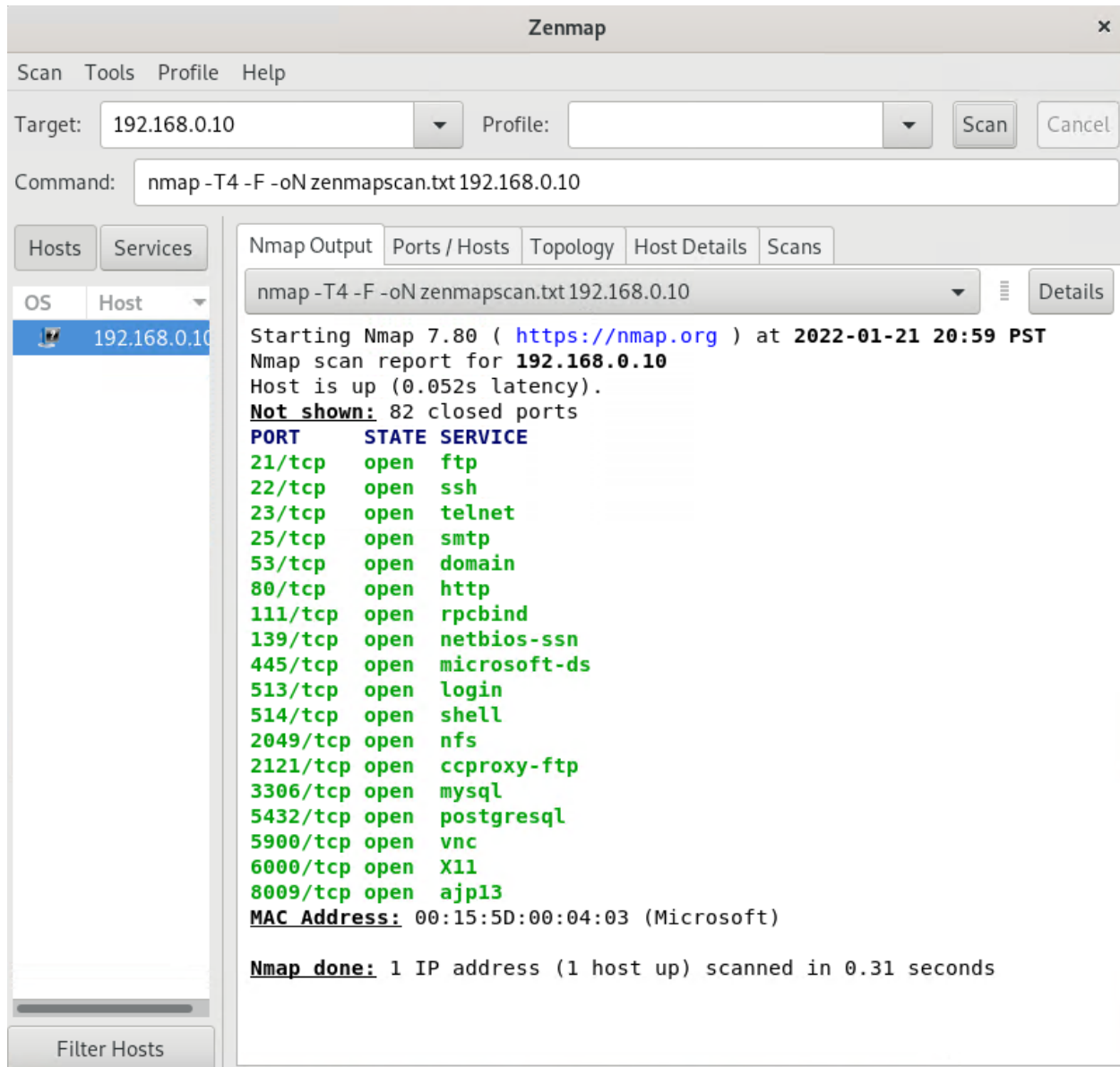
Step 5: Zenmap

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:

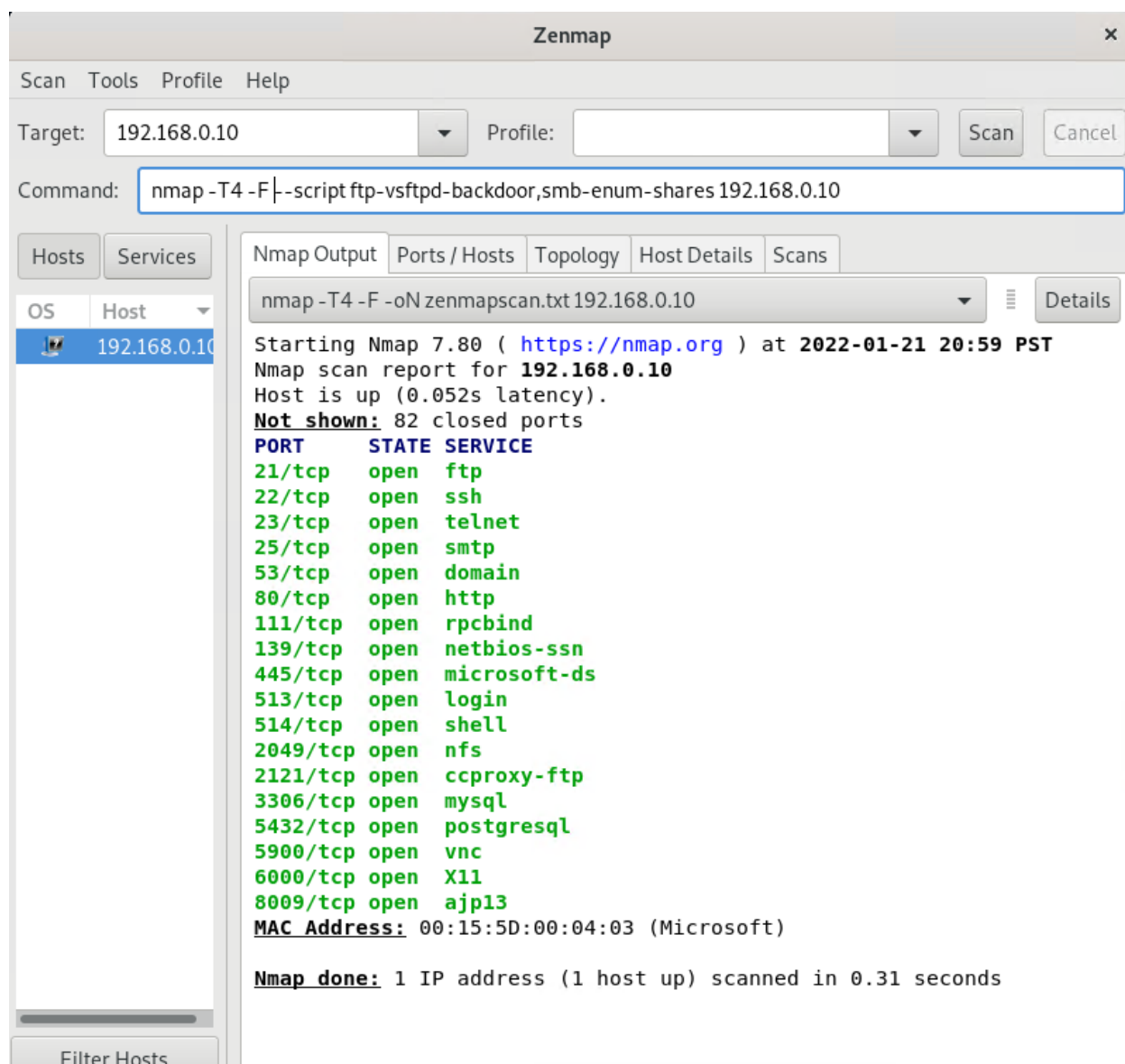
- Command for Zenmap to run a service scan against the Metasploitable machine:
 1. Run the Pentesting Lab from Azure
 2. Open Hyper-V-Manager to view available VM's
 3. Start "Kali" VM
 4. Open a terminal
 5. Enter "zenmap"
 6. We are then going to use the Metasploitable machine that's part of the Hyper-V-Manager 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

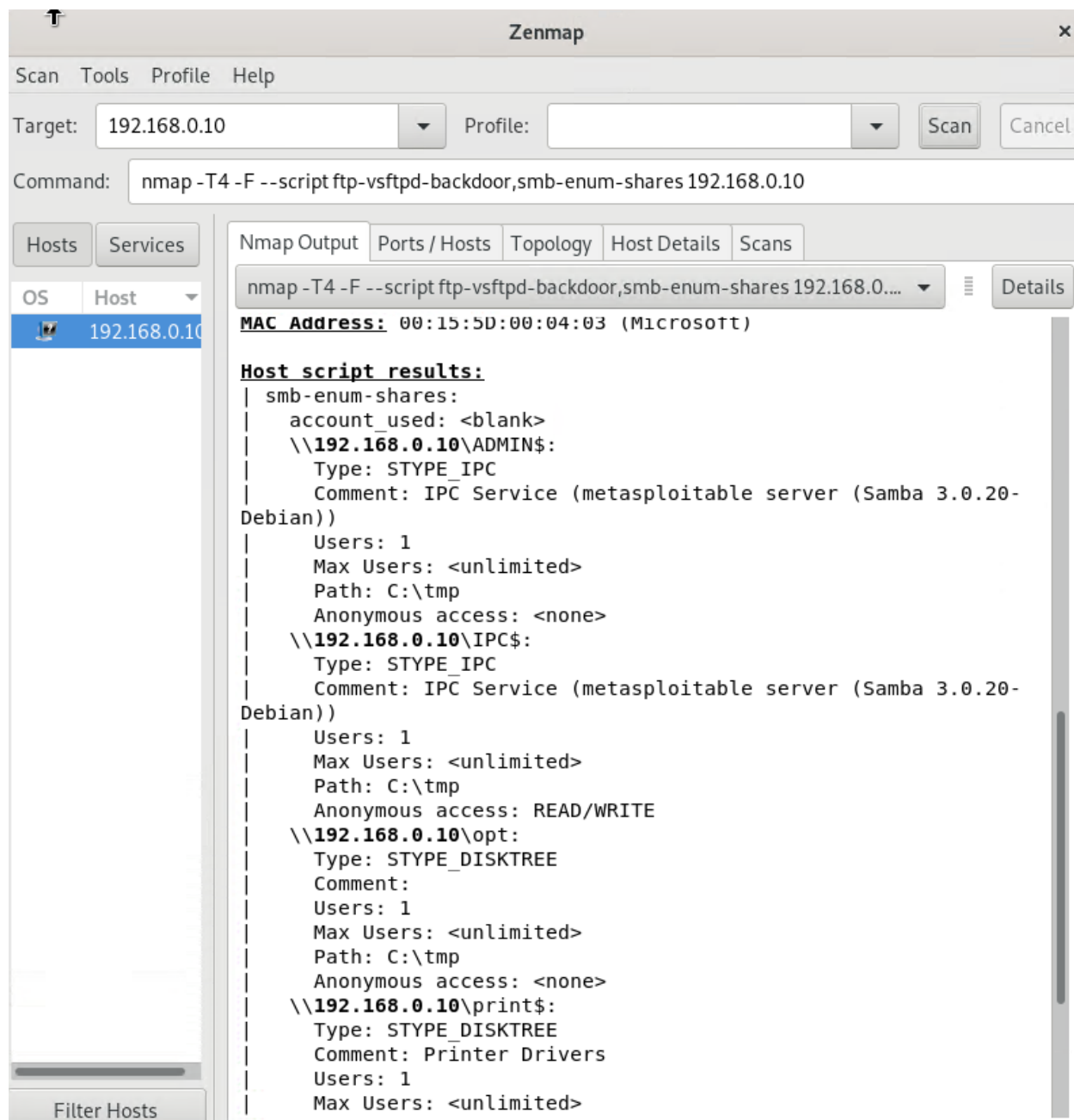
Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -F --script ftp-vsftpd-backdoor,smb-enum-shares 192.168.0.10 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?		
https://www.securityfocus.com/bid/48539		
https://github.com/rapid7/metasploit-framework/blob/		
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 recommend for the client to protect their server:

VSFTPD 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 Linux RHSA-2017:1390