

Penetration Testing 1

Scenario

In this assignment, you will work as a recently hired security analyst at Altoro Mutual, a banking service.

- Concerned about their online presence and the security of their website demo.testfire.net, they have hired you to evaluate the security posture of their operations.
- As a holder of very sensitive customer and financial data, Altoro Mutual is worried about malicious actors compromising their website and gaining this information.

You are tasked with performing website enumeration, discovery, and vulnerability detection. Because this engagement is non-invasive, you will **not** try to hack into their system. Rather, you will discover any potential vulnerabilities or leaks that the company should be worried about.

Please note throughout this assignment, you will target a website named "Altoro Mutual" located at demo.testfire.net. Altoro Mutual was designed by IBM, a company that designs both hardware and software for computers. Their website demo.testfire.net was specifically designed to detect web application vulnerabilities.

Topics Covered in This Assignment

- Website enumeration
- Google Dorking
- OSINT Recon
- Shodan
- Recon-NG
- Installing modules
- Zenmap
- nmap's scripting engine

Lab Environment

You will use Azure online VMs to complete the homework.

To start the labs, log into Azure and launch the Penetration Security machine.

Once you are connected to that machine, launch the Pen Testing Hyper-V machine and start it to boot up Kali Linux.

- Kali credentials:

- Username: root
- Password: toor
- Metasploitable credentials:

- Username: msfadmin
- Password: msfadmin

Note: Your Kali machine will act as the attacker machine, and the Metasploitable machine will act as the victim's machine.

Please note throughout this assignment, you will target a website named "Altoro Mutual" located at demo.testfire.net. Altoro Mutual was designed by IBM, a company that designs both hardware and software for computers. Their website demo.testfire.net was specifically designed to detect web application vulnerabilities.

Instructions:

As you complete the steps below, please record your answers in the Submission.md file. You will submit this file as your homework deliverable.

Step 1: Google Dorking

Altoro Mutual wants to ensure that private information that is unavailable on their public website cannot be found by searching the web.

- For example, Altoro Mutual does not mention their executive members on the website. Using Google, can you identify who the Chief Executive Officer is?

[Karl Fitzgerald Chairman & Chief Executive Officer Altoro Mutual](#)

- How can this information be helpful to an attacker?

[Attackers can use information such as email addresses of employees and management, \(especially those in higher up position\), and exploit that by sending phishing emails.](#)

Step 2: DNS and Domain Discovery

The reconnaissance phase of a penetration test is possibly the most important phase of the engagement. Without a clear understanding of your client's assets, vulnerabilities can go unnoticed and later exploited.

- Navigate to centralops.net.
- Enter the IP address for demo.testfire.net into Domain Dossier and answer the following questions based on the results:
-

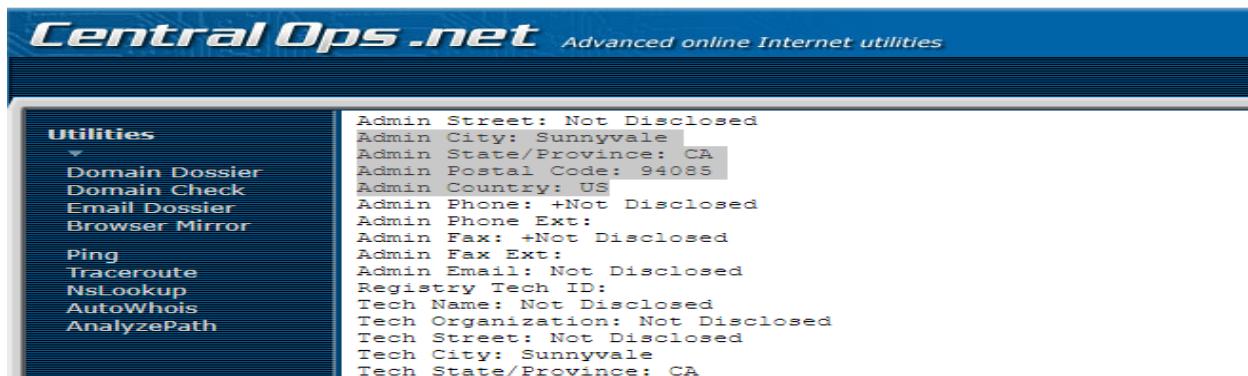
enter: demo.testfire.net



The screenshot shows the Central Ops .net website with a blue header bar. Below it, a sidebar on the left lists various utilities: Utilities, Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath. The main content area is titled "Domain Dossier" with the subtitle "Investigate domains and IP addresses". It displays the domain "demo.testfire.net" in a search field. Below the search field are several checkboxes: "domain whois record" (checked), "DNS records" (checked), "traceroute" (checked), "network whois record" (checked), and "service scan" (checked). A "go" button is next to the checkboxes. At the bottom of the main area, there is a message about missing contact information and a link to reduced Whois data due to GDPR.

1. Where is the company located?

Sunnyvale, Ca 94085 US



This screenshot shows the same Central Ops .net interface as the previous one, but the main content area now displays detailed Whois information for the domain "demo.testfire.net". The information includes: Admin Street: Not Disclosed, Admin City: Sunnyvale, Admin State/Province: CA, Admin Postal Code: 94085, Admin Country: US, Admin Phone: +Not Disclosed, Admin Phone Ext: +Not Disclosed, Admin Fax: +Not Disclosed, Admin Email: Not Disclosed, Registry Tech ID: Not Disclosed, Tech Name: Not Disclosed, Tech Organization: Not Disclosed, Tech Street: Not Disclosed, Tech City: Sunnyvale, and Tech State/Province: CA.

2. What is the NetRange IP address?

NetRange: 65.61.137.64 - 65.61.137.127



This screenshot shows the Central Ops .net interface again, but this time the main content area is titled "Network Whois record". It displays the query "Queried whois.arin.net with \"n ! NET-65-61-137-64-1\"...". Below this, a table shows the NetRange (65.61.137.64 - 65.61.137.127), CIDR (65.61.137.64/26), NetName (RACKS-8-189343775333749), NetHandle (NET-65-61-137-64-1), Parent (RSPC-NET-4 (NET-65-61-128-0-1)), and NetType (Reassigned).

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

Rackspace Backbone engineering, 9725 Datapoint Drive, suite 100, San Antonio,TX 78229 US

Customer: Rackspace Backbone Engineering (C05762718)
RegDate: 2015-06-08
Updated: 2015-06-08
Ref: <https://rdap.arin.net/registry/ip/65.61.137.64>

CustName: Rackspace Backbone Engineering
Address: 9725 Datapoint Drive, Suite 100
City: San Antonio
StateProv: TX
PostalCode: 78229
Country: US
RegDate: 2015-06-08
Updated: 2015-06-08
Ref: <https://rdap.arin.net/registry/entity/C05762718>

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

DNS server ip: 65.61.137.117

Address lookup

canonical name [demo.testfire.net](#).

aliases

addresses [65.61.137.117](#)

Step 3: Shodan

Using Shodan and the information gathered from Google Dorking, find any other useful information that can be used in an attack.

- Navigate to [shodan.io](#).
- Run a scan against the IP address of the DNS server for demo.testfire.net.
 - What open ports and running services did Shodan find?

open ports: 80, 443

Apache Tomcat/Coyote JSP Engine services

General Information

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

Open Ports

- 80
- 443

// 80 /TOP 5

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Fri, 03 Jan 2022 20:38:15 GMT
Content-Type: text/html; charset=ISO-8859-1
Path:/; httpOnly
Transfer-Encoding: chunked
Date: Fri, 03 Jan 2022 20:38:15 GMT
```

// 443 /TOP 5

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=AA9447C44B32B177987511E9512099; Path=/; Secure; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Mon, 03 Jan 2022 08:01:55 GMT
```

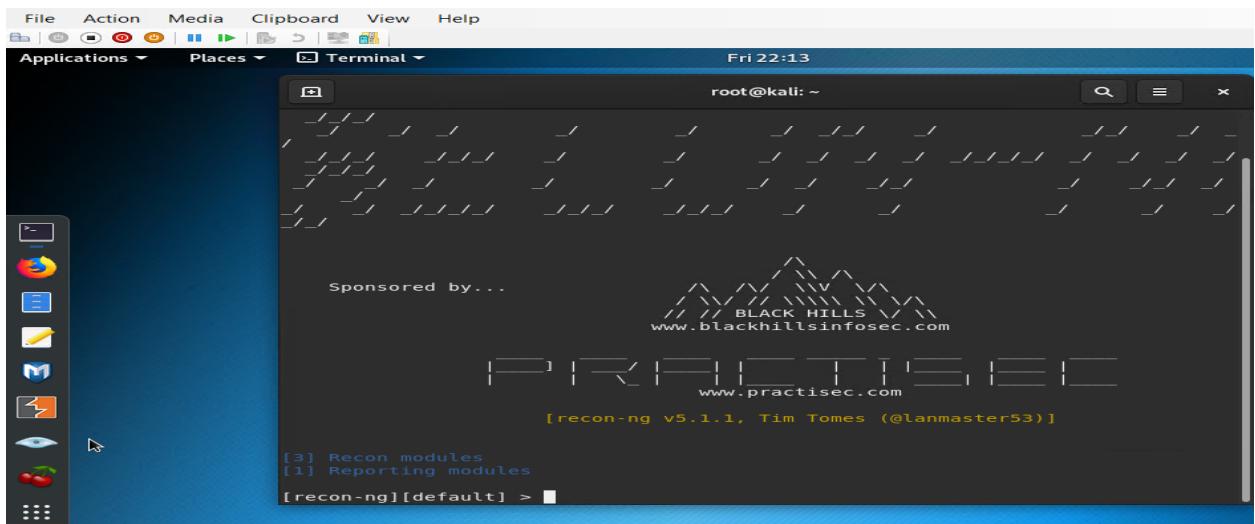
SSL Certificate

Step 4: Recon-ng

Altoro Mutual is also concerned about cross-site scripting attacks, which can cause havoc on their website. Verify whether or not Altoro Mutual is vulnerable to XSS by completing the following:

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

enter: recon-ng



enter: marketplace load xssted

A screenshot of a Kali Linux desktop environment. The terminal window shows the command [recon-ng] > marketplace load xssted being run, which installs the 'domains-vulnerabilities/xssed' module. The terminal window title is 'Terminal'. The desktop interface includes a dock with icons for various applications like Firefox, Nautilus, and a text editor.

```
File Action Media Clipboard View Help
Applications Places Terminal Fri 22:14
root@kali: ~
[recon-ng] > marketplace load xssted
Interfaces with the module marketplace
Usage: marketplace <info|install|refresh|remove|search> [...]
[recon-ng][default] >
```

enter: marketplace install xssted

A screenshot of a Kali Linux desktop environment. The terminal window shows the command [recon-ng] > marketplace install xssted being run, which installs the 'domains-vulnerabilities/xssed' module. The terminal window title is 'Text Editor'. The desktop interface includes a dock with icons for various applications like Firefox, Nautilus, and a text editor.

```
File Action Media Clipboard View Help
Applications Places Terminal Fri 22:15
root@kali: ~
[recon-ng] > marketplace install xssted
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[recon-ng][default] >
```

enter: modules load recon/domain-vulnerabilities/xssed

enetr: options set source demo.testfire.net

The screenshot shows a Kali Linux desktop environment with a terminal window open as root. The terminal title is "root@kali: ~". The window contains a logo for "BLACK HILLS" with the URL "www.blackhillsinfosec.com". Below the logo, the text "PRACTISE" is partially visible, followed by the URL "www.practisesec.com". The terminal prompt shows "[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]". The user is interacting with the "marketplace" module, specifically the "xssed" module. The terminal output includes:

```
[3] Recon modules
[1] Reporting modules

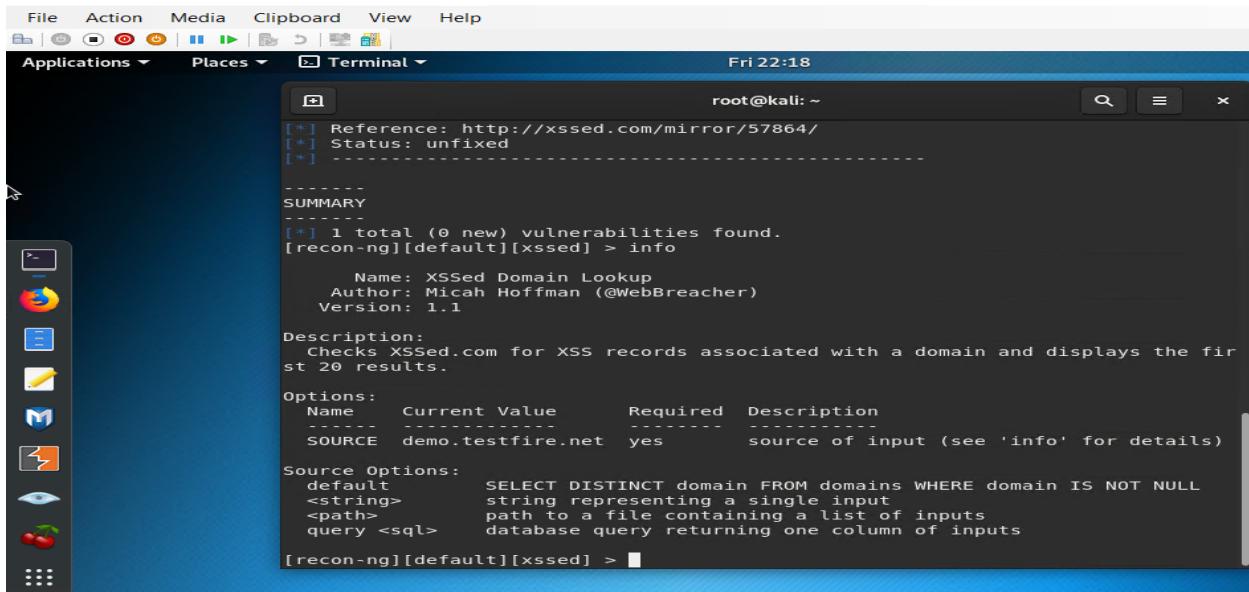
[recon-ng][default] > marketplace load xssed
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] > marketplace install xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[recon-ng][default] > modules load recon/domains-vulnerabilities/xssed
[recon-ng][xssed] > options set SOURCE demo.testfire.net
SOURCE => demo.testfire.net
[recon-ng][xssed] >
```

enter: info

watch for source chngd to: demo.testfire.net



```
[root@kali: ~]
[*] Reference: http://xssed.com/mirror/57864/
[*] Status: unfixed
[*]

SUMMARY
[*] 1 total (0 new) vulnerabilities found.
[recon-ng][default][xssed] > info

    Name: XSSed Domain Lookup
    Author: Micah Hoffman (@WebBreacher)
    Version: 1.1

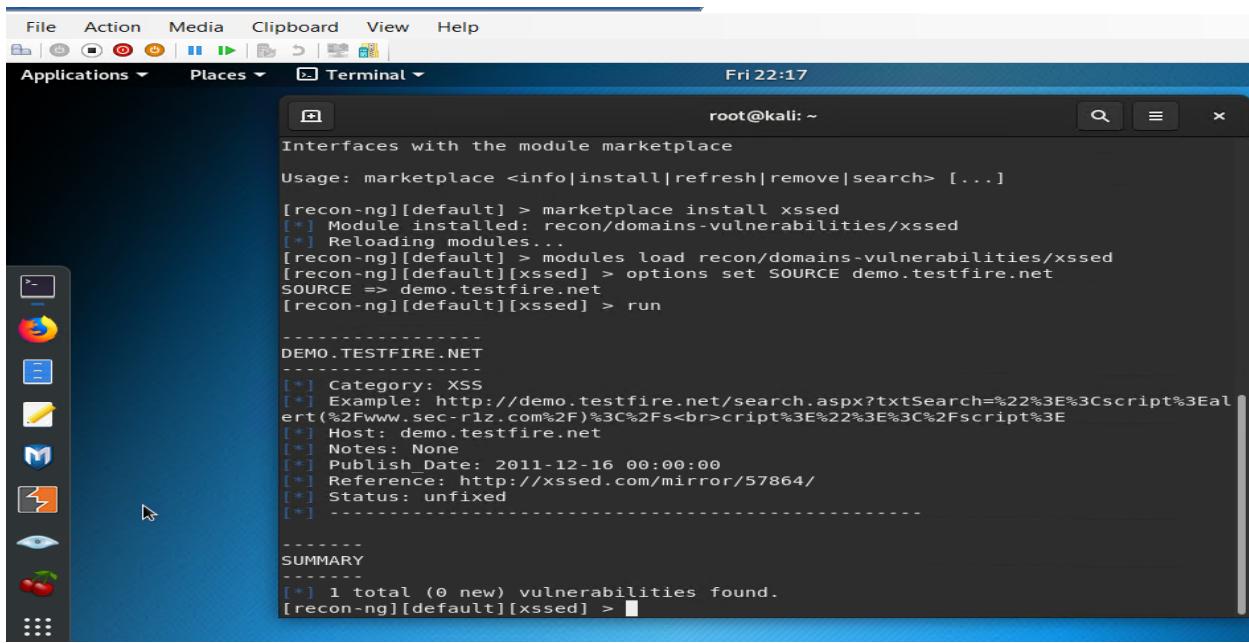
    Description:
        Checks XSSed.com for XSS records associated with a domain and displays the first 20 results.

    Options:
        Name      Current Value      Required      Description
        -----  -----
        SOURCE    demo.testfire.net  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] >
```

enter: run



```
[root@kali: ~]
[*] Interfaces with the module marketplace
Usage: marketplace <info|install|refresh|remove|search> [...]
[recon-ng][default] > marketplace install xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[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-r1z.com%2F)%3C%2Fs<br>cript%3E%22%3C%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 (0 new) vulnerabilities found.
[recon-ng][default][xssed] >
```

Is Altoro Mutual vulnerable to XSS?

Yes. There is one total vulnerability found.

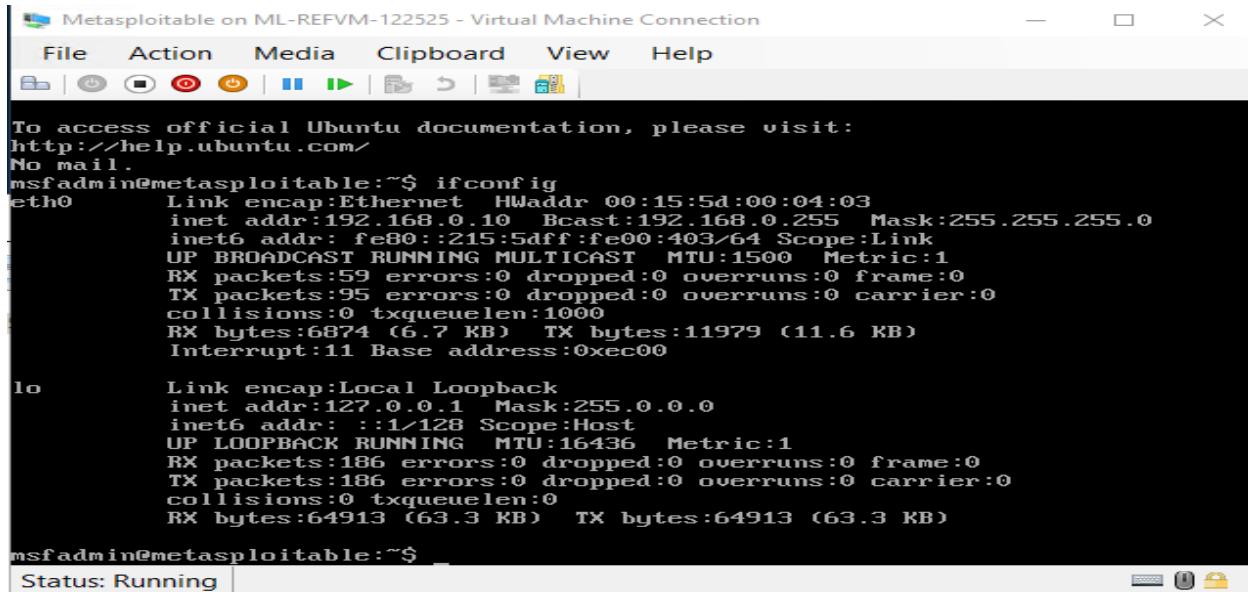
<script>alert("www.sec-r1z.com")</script>

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:

- Use Zenmap to run a service scan against the Metasploitable machine.

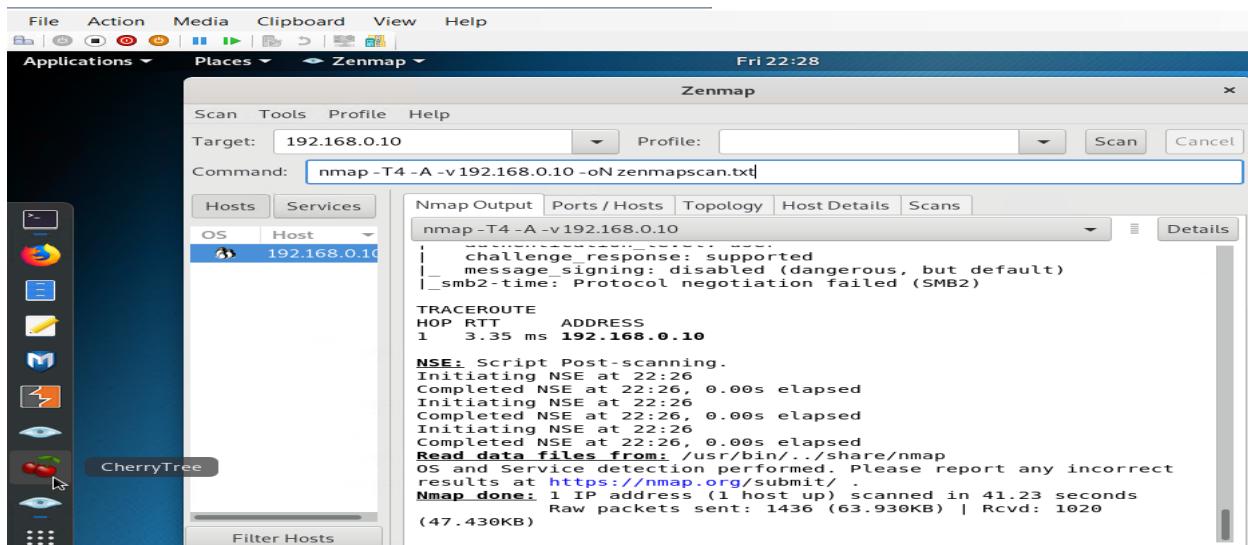
log in to Metasploitable and run **ifconfig** to get their ip address: 192.168.0.10



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:15:5d:00:04:03  
          inet addr:192.168.0.10  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::215:5dff:fe00:403/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
             RX packets:59 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:95 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:6874 (6.7 KB)  TX bytes:11979 (11.6 KB)  
             Interrupt:11 Base address:0x0ec00  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING  MTU:16436  Metric:1  
             RX packets:186 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:186 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:64913 (63.3 KB)  TX bytes:64913 (63.3 KB)  
  
msfadmin@metasploitable:~$ _  
Status: Running
```

Bonus: In the same command, output the results into a new text file named zenmapscan.txt.

run a scan on ip 192.168.0.10 and send to file **zenmapscan.txt** (see command bar)



- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.

port 139/445 are running on an outdated samba version.

```

nmap -T4 -A -v -oN zenmapscan.txt 192.168.0.10
Starting Nmap 7.6.1 ( https://nmap.org ) at 2023-09-22 22:32 UTC
Nmap scan report for 192.168.0.10
Host is up.
OS: Linux 3.0.20-Debian (workgroup: WORKGROUP)
Ports: TCP: 139/tcp open rpcbind 2 (RPC #100000)
        445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
        512/tcp open exec netkit-rsh rexecd
        513/tcp open login
        514/tcp open tcpwrapped
        1099/tcp open java-rmi GNU Classpath grmiregistry
        1524/tcp open bindshell Metasploitable root shell
        2049/tcp open nfs 2-4 (RPC #100003)
        2121/tcp open ftp ProFTPD 1.3.1
        3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
MySQL-info:
Protocol: 10
Version: 5.0.51a-3ubuntu5
Thread ID: 10
Capabilities flags: 43564

```

Run the scan with samba –script: **smb-enum-shares**

```

nmap -T4 -A -v -oN zenmapscan.txt --script smb-enum-shares 192.168.0.10
Starting Nmap 7.6.1 ( https://nmap.org ) at 2023-09-22 23:25 UTC
Nmap scan report for 192.168.0.10
Host is up.
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  netbios-ssn
513/tcp    open  login
514/tcp    open  tcpwrapped
1099/tcp   open  java-rmi
1524/tcp   open  bindshell
2049/tcp   open  nfs
2121/tcp   open  ftp
3306/tcp   open  mysql
MySQL-info:
Protocol: 10
Version: 5.0.51a-3ubuntu5
Thread ID: 10
Capabilities flags: 43564

```

```

\\192.168.0.10\print$:
Type: STYPE_DISKTREE
Comment:
Users: 1
Max Users: <unlimited>
Path: C:\tmp
Anonymous access: <none>
\\192.168.0.10\Printer Drivers:
Type: STYPE_DISKTREE
Comment: Printer Drivers
Users: 1
Max Users: <unlimited>
Path: C:\var\lib\samba\printers
Anonymous access: <none>
\\192.168.0.10\tmp:
Type: STYPE_DISKTREE
Comment: oh noes!
Users: 1
Max Users: <unlimited>
Path: C:\tmp
Anonymous access: READ/WRITE

```

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

- What is the vulnerability?

The samba version is outdated.

SAMBA	
Initial release	1992; 30 years ago ^[1]
Stable release	4.15.2 ^[2] / 9 November 2021; 59 days ago
Repository	git.samba.org  
Written in	C, Python
Operating system	Multiplatform
Type	Network file system
License	GPLv3
Website	www.samba.org 

- Why is it dangerous?

Since the system is running on outdated samba version, the system is vulnerable to security exploits that likely would have been prevented had the system been up to date with the proper security patches.

- What are your recommendations for the client to protect their server?

recommending to update the system with the latest version on a regular basis in order to keep with the latest security patches/updates.