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 victims 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 remembers 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.

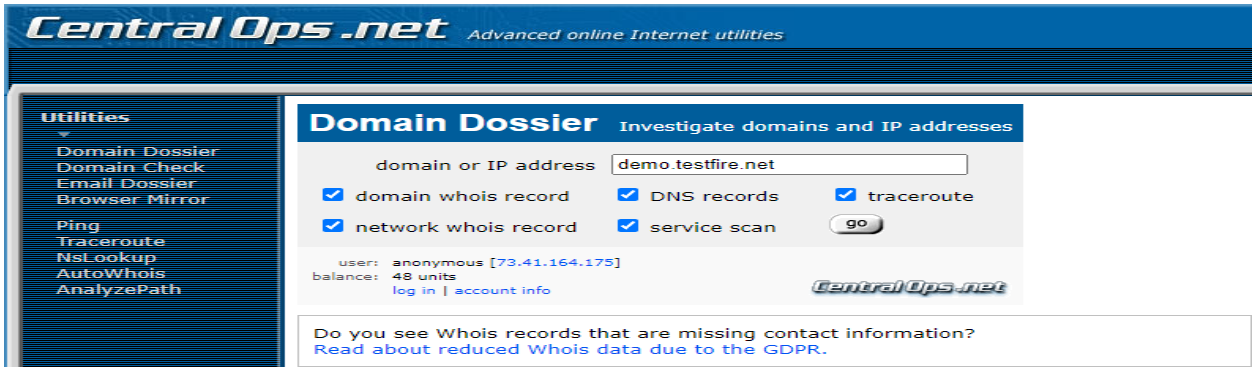
Step 2: DNS and Domain Discovery

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.

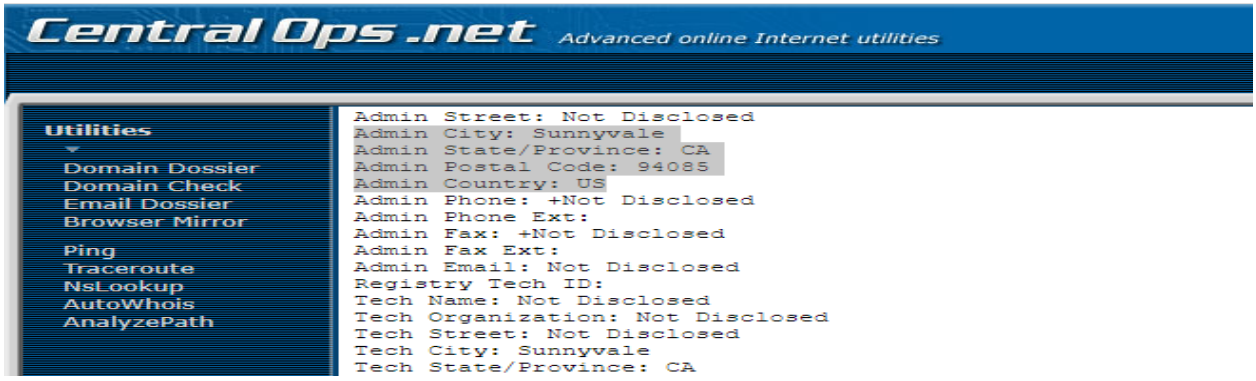
- Enter the IP address for demo.testfire.net into Domain Dossier and answer the following questions based on the results:
-

enter: demo.testfire.net



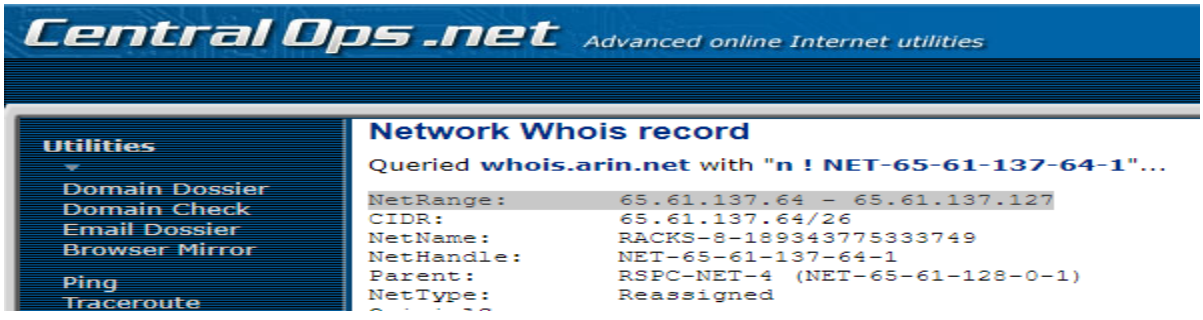
1. Where is the company located?

Sunnyvale, Ca 94085 US



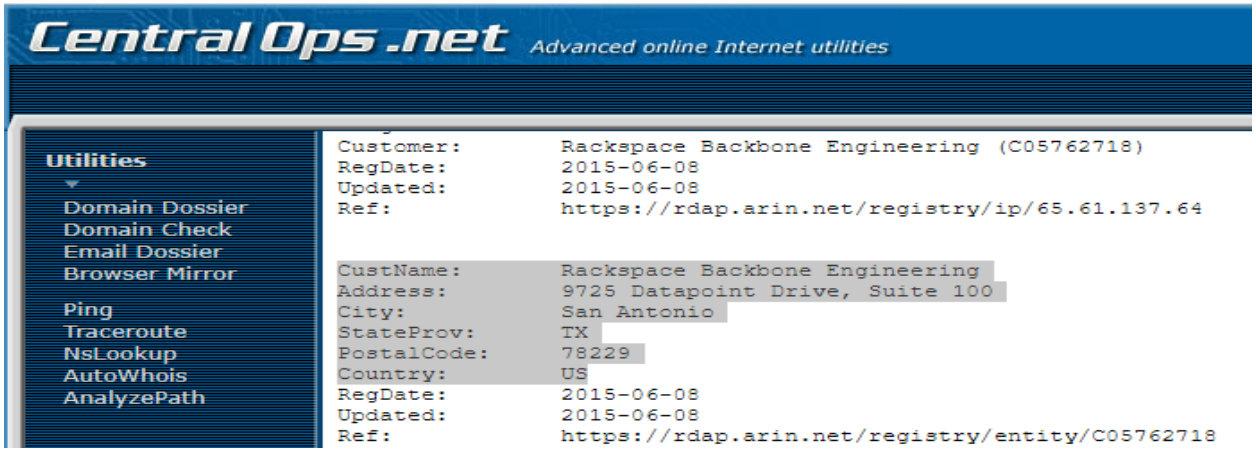
2. What is the NetRange IP address?

NetRange: **65.61.137.64 - 65.61.137.127**



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

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



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

DNS server ip: 65.61.137.117

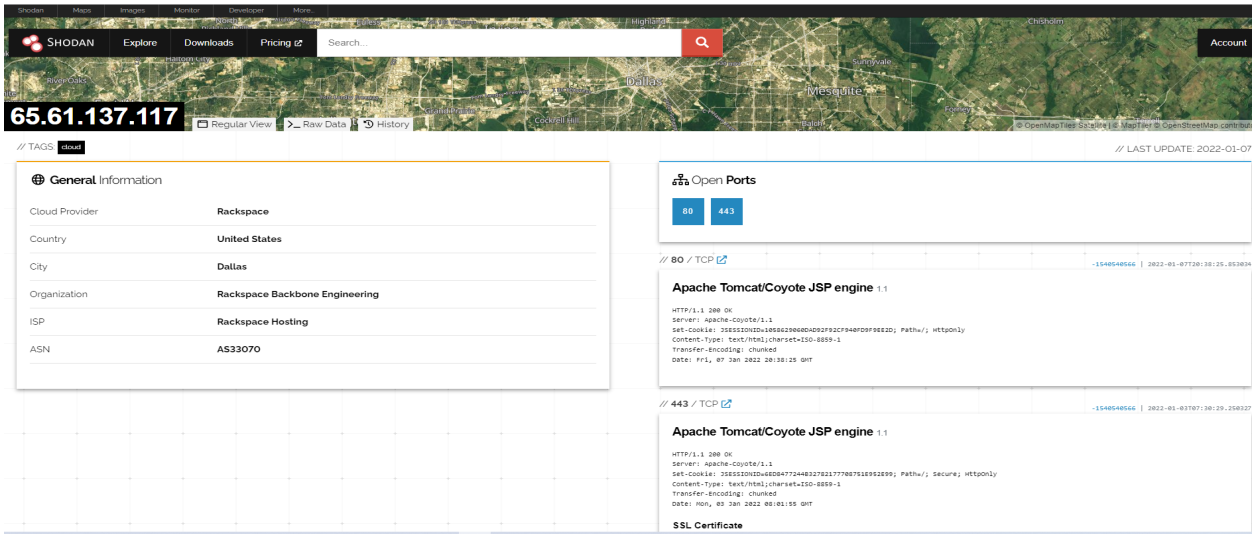
Step 3: Shodan

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

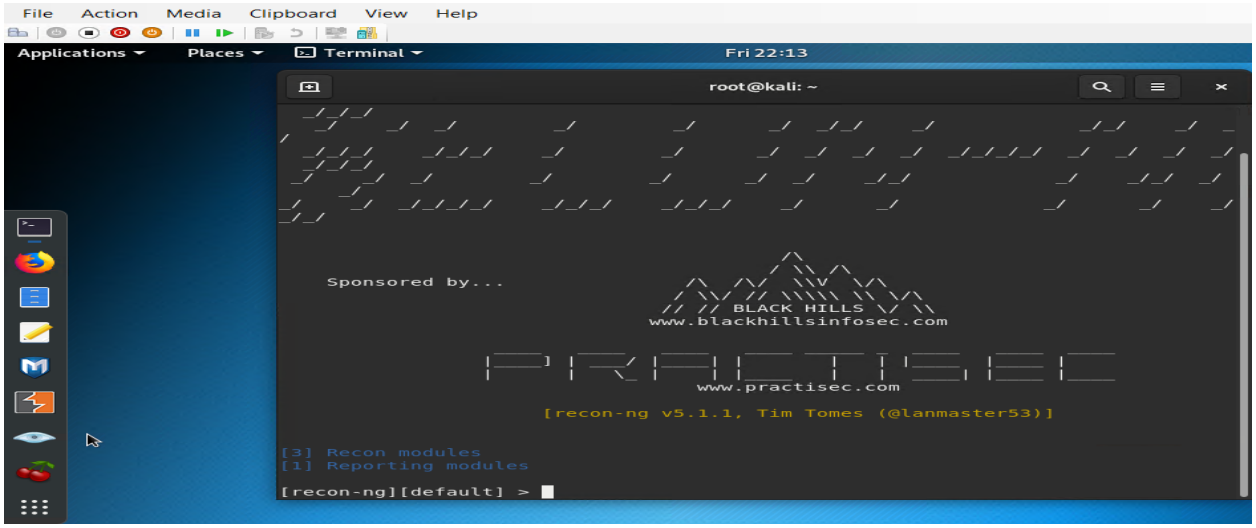


Step 4: Recon-ng

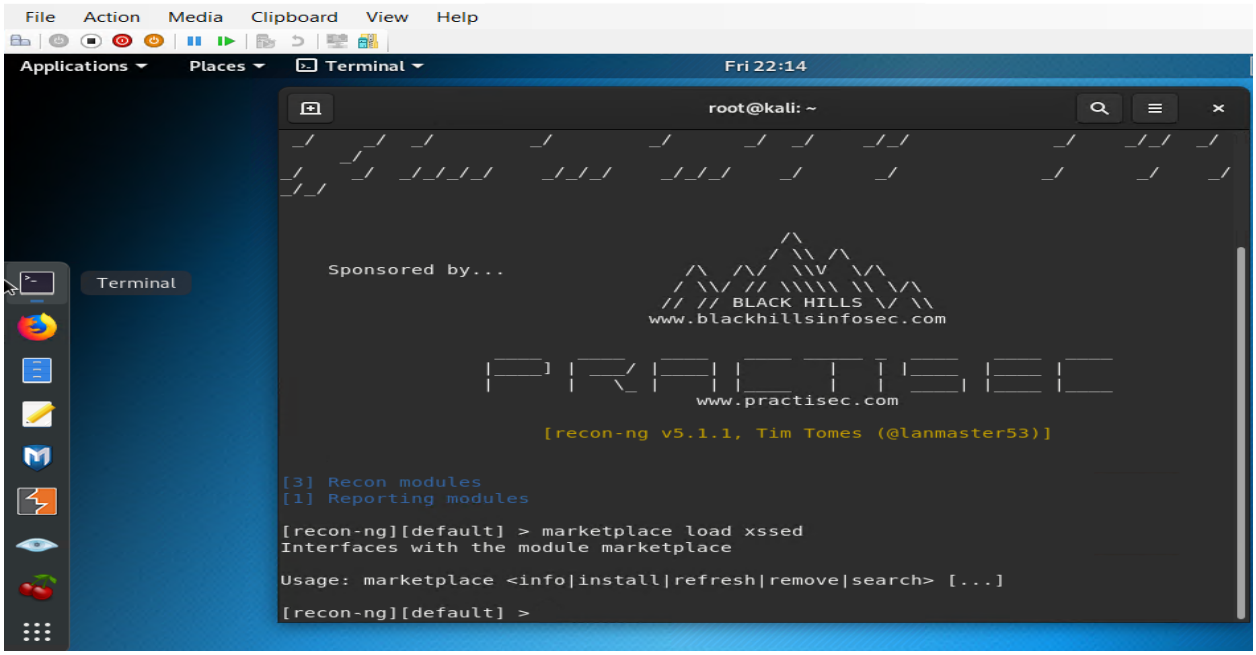
Altoro Mutual is also concerned about cross-site scripting attacks, which can cause havoc on their website. Verify whether or not Altoro Mutual is vulnerable to XSS by completing the following:

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

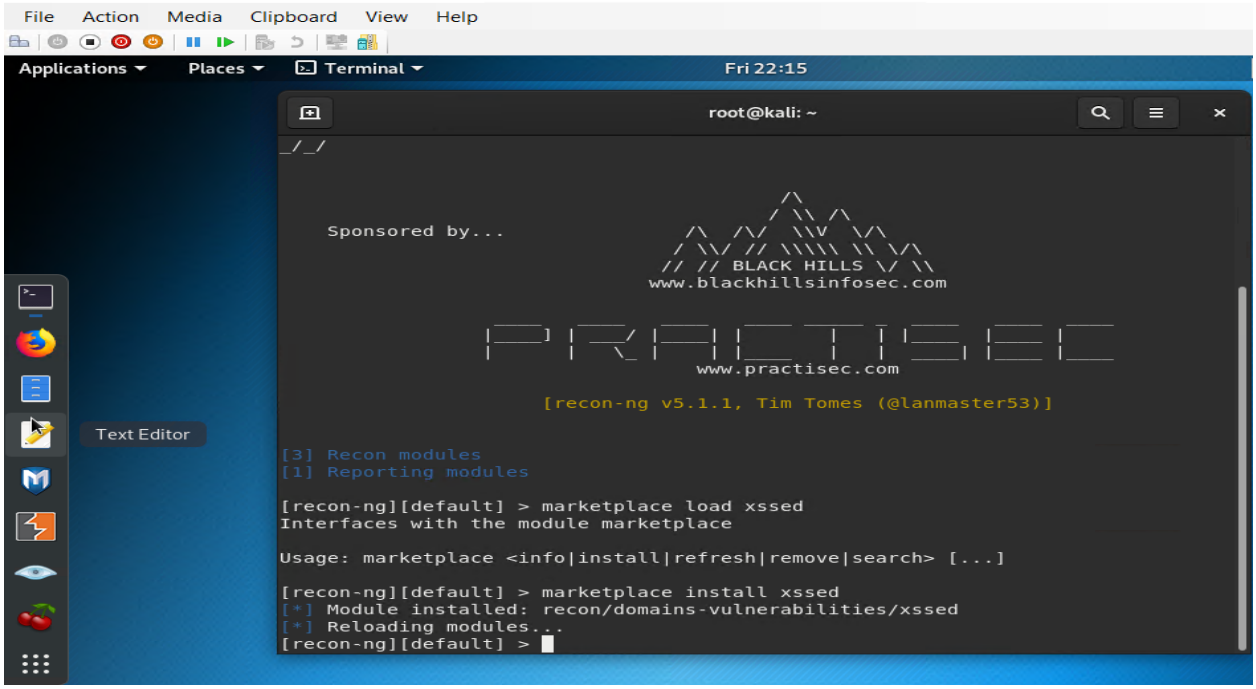
enter: recon-ng



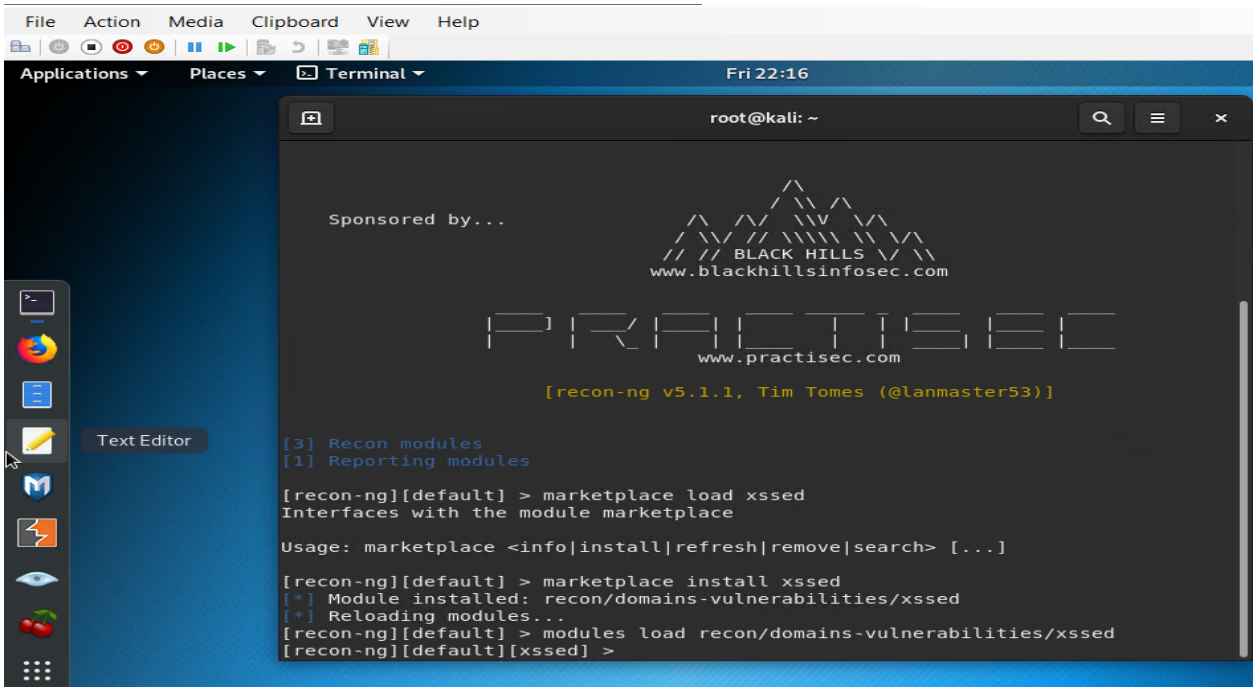
enter: marketplace load xssed



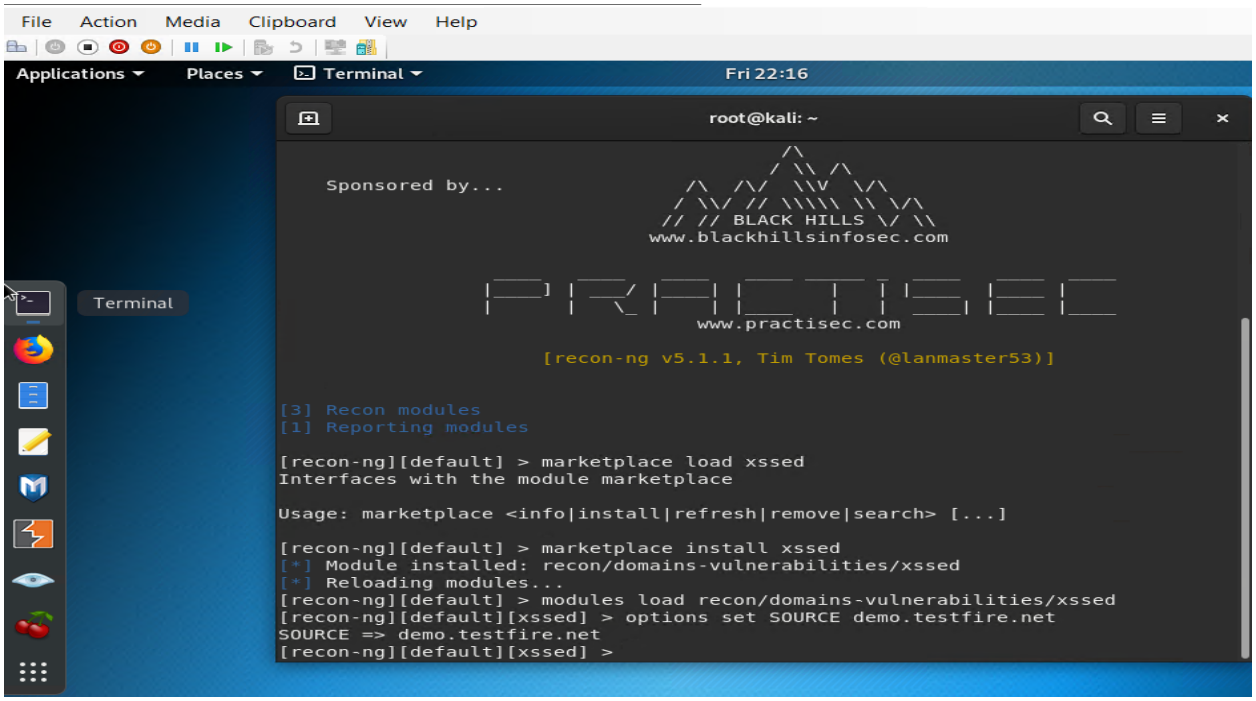
enter: marketplace install xssed



enter: modules load recon/domain-vulnerabilities/xssed

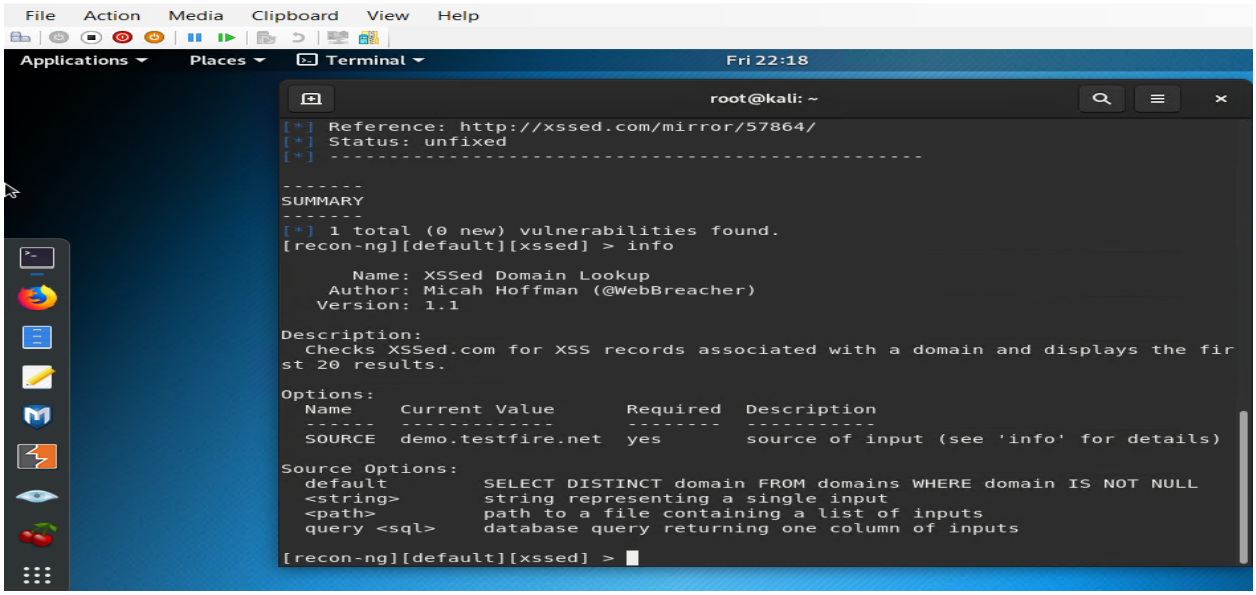


enetr: options set source demo.testfire.net

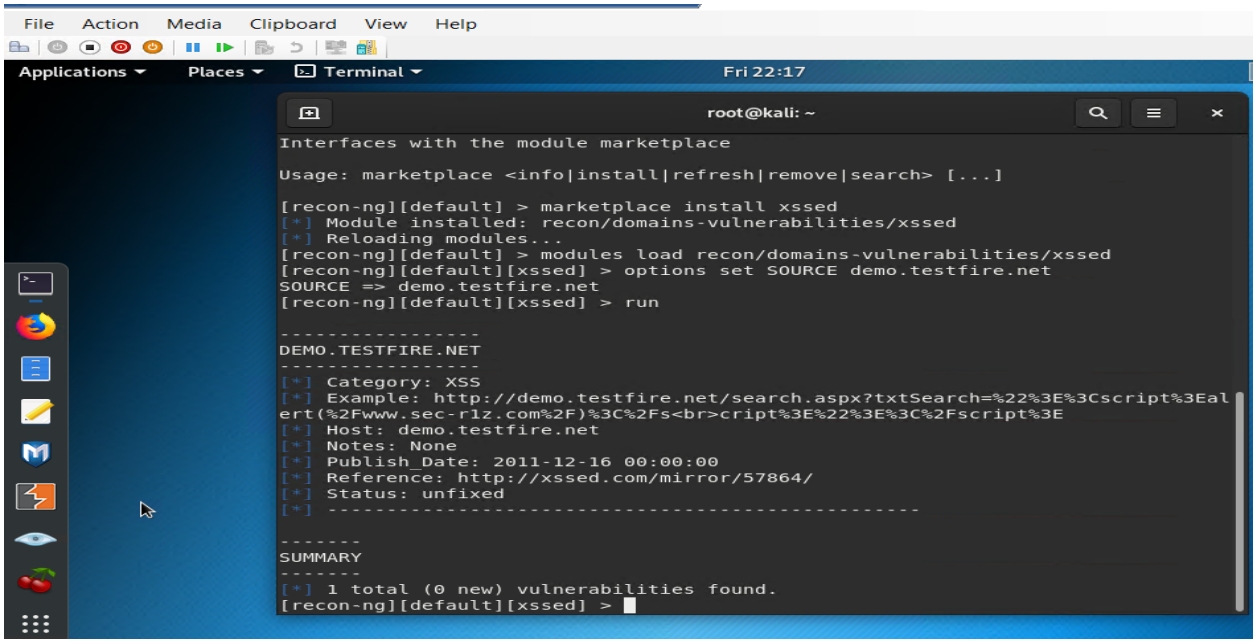


enter: info

watch for source chnged to: **demo.testfire.net**



enter: run



Is Altoro Mutual vulnerable to XSS?

Yes. There is one total vulnerability found.

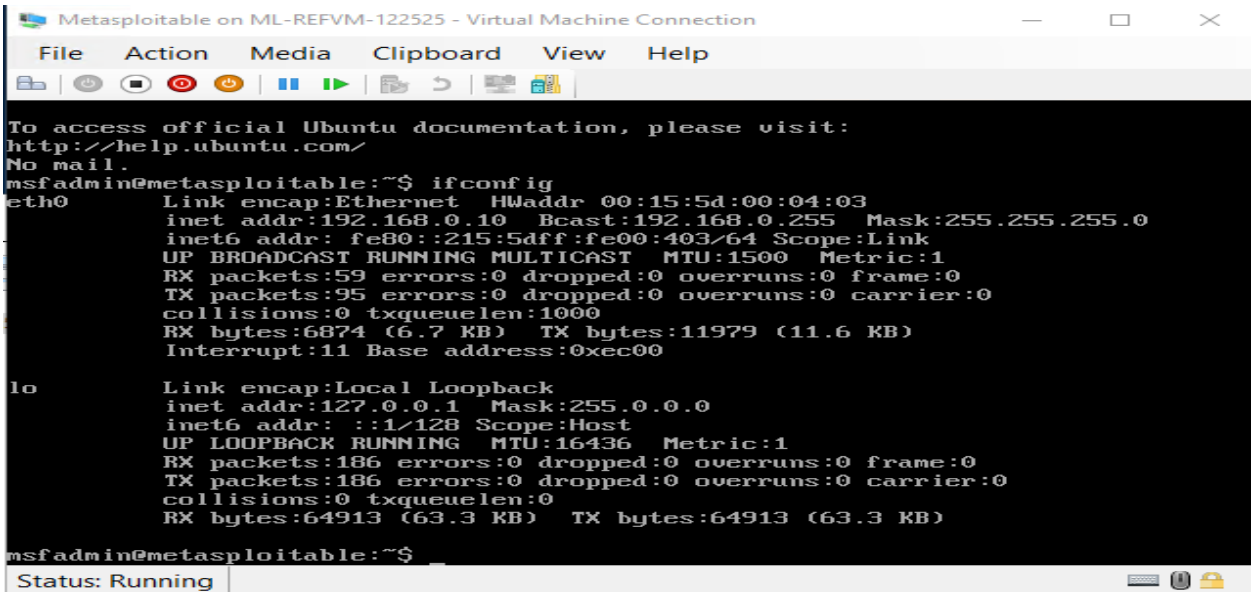
<script>alert("www.sec-r1z.com")</script

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:

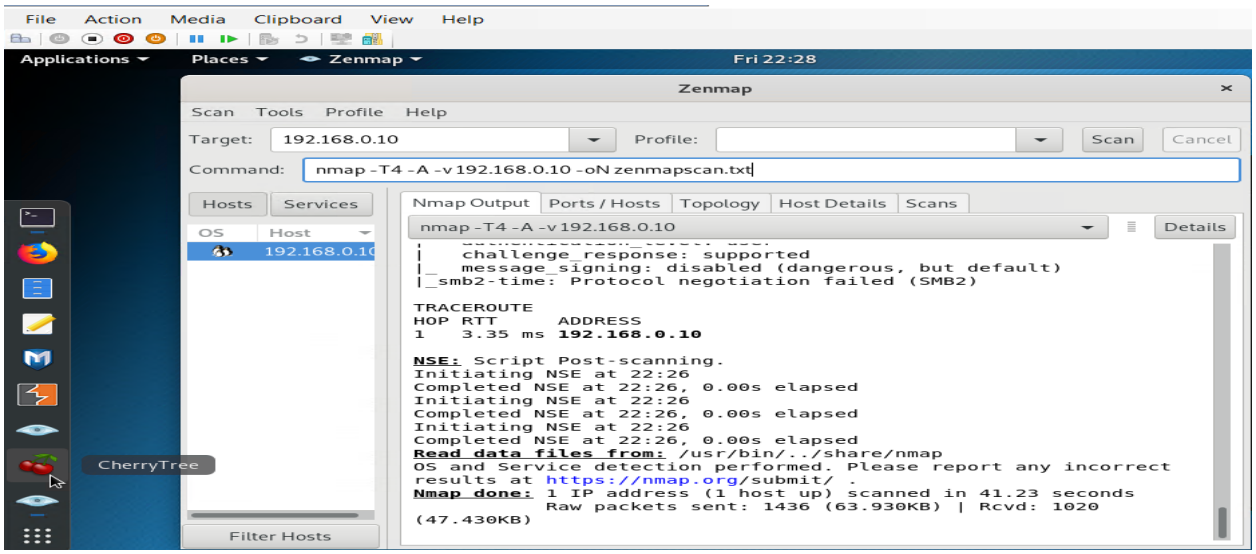
- Use Zenmap to run a service scan against the Metasploitable machine.

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



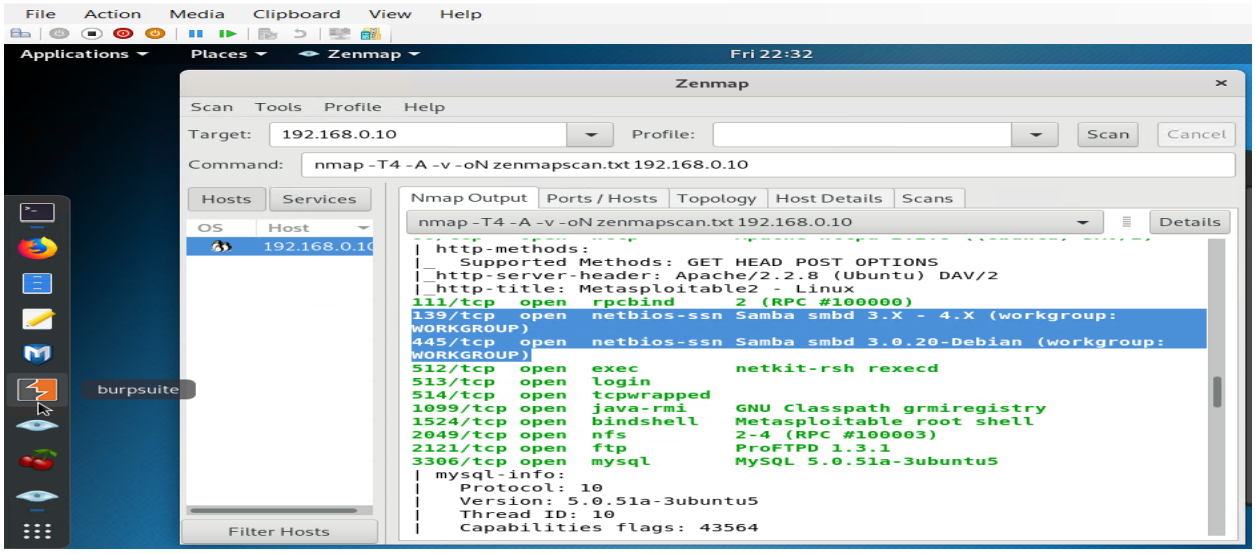
Bonus: In the same command, output the results into a new text file named zenmapscan.txt.

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

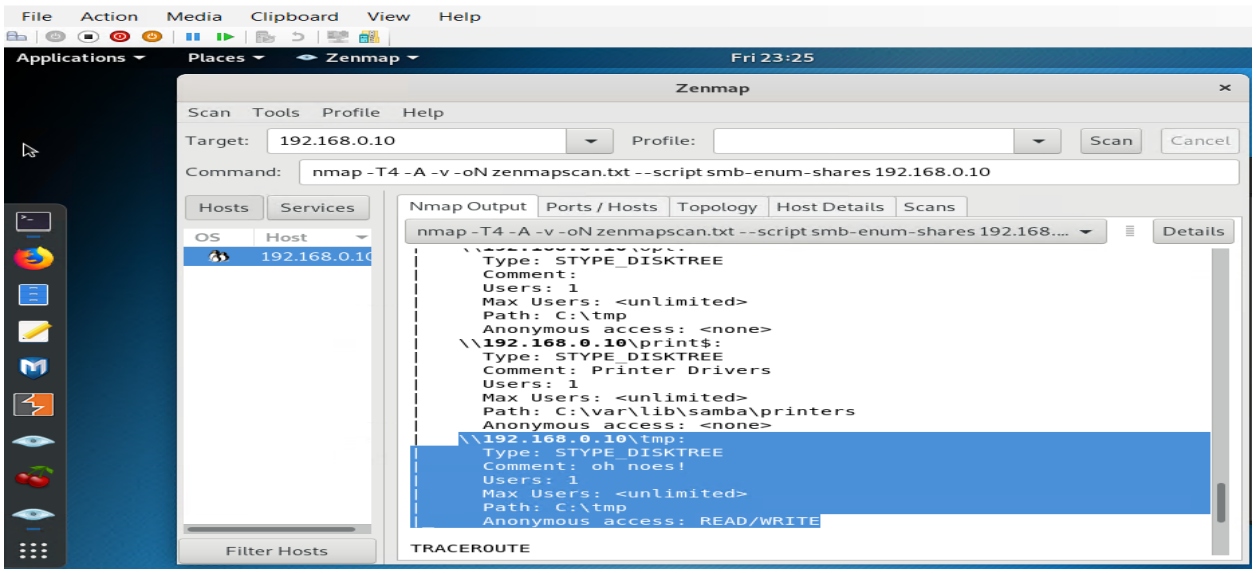


- Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan.

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



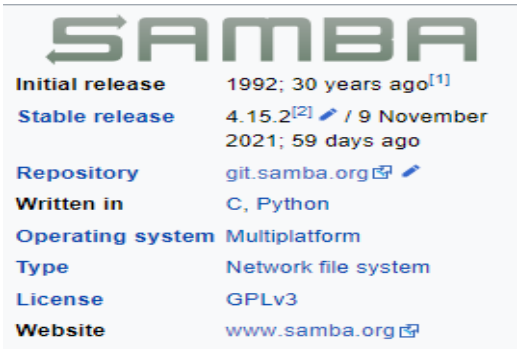
Run the scan with samba –script: **smb-enum-shares**



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

1. What is the vulnerability?'

   The samba version is outdated.



2. 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.

3. 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.