

Unit 16 Assignment: 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. demo

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 members on the website. Using Google, can you identify who the Chief Executive Officer is?

The CEO is Karl Fitzgerald

How can this information be helpful to an attacker?

This information can be used in a social engineering campaign

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:

Where is the company located? Registrant Street: 330 Potrero Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94085 Registrant Country: US

What is the NetRange IP address? 65.61.137.64 - 65.61.137.127

What is the company they use to store their infrastructure?

What is the IP address of the DNS server? 117.137.61.65

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? 80, 44, 8080

The screenshot shows the Shodan search results for the IP address 65.61.137.117. The page features a satellite map at the top, followed by a table of metadata and sections for open ports and running services.

SHODAN [Search Bar] [Explore] [Downloads] [Reports] [Pricing] [Enterprise Access] [My Account]

65.61.137.117 View Raw Data

cloud

Country	United States
Organization	Rackspace Hosting
ISP	Rackspace Hosting
Last Update	2020-09-19T16:16:58.138444
ASN	AS333070

Ports

- 80
- 443
- 8080

Services

- 80
- tcp
- http

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.

Is Altoro Mutual vulnerable to XSS? Yes, we get the result 1 (new) vulnerabilities found.

```
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] > 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%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.
```

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:

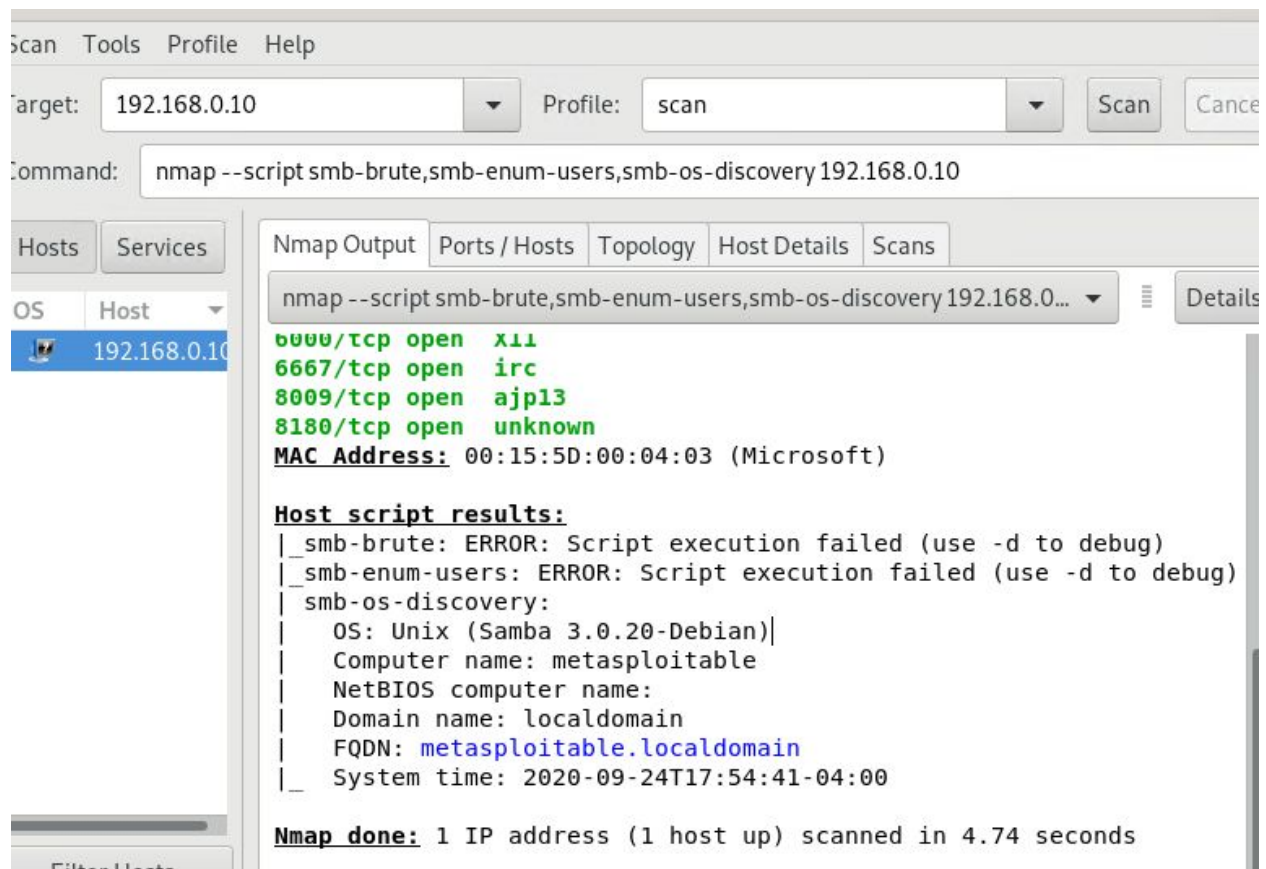
Use Zenmap to run a service scan against the Metasploitable machine.

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

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

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

What is the vulnerability? port 139 is open which is vulnerable to a smb exploitation.



Why is it dangerous? SMB exploitation can reveal info about operating systems, other enumerations etc.

What are your recommendations for the client to protect their server? close port 139, have a waf in place.