Week 16 Homework Submission File: Penetration Testing 1

Step 1: Google Dorking

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

Answer: Chief Executive Officer is Karl Fitzgerald

* + **How can this information be helpful to an attacker:**

Answer: By have the Chief Executive Officers name, Karl Fitzgerald however there are other executives on the header of the company . With this information the use of email address to conduct phishing and burte force attacks

Graphical user interface, website

Description automatically generated with medium confidence

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:**

Answer:

Text, letter

Description automatically generated

* + **What is the NetRange IP address:**

Answer: **65.61.137.64 - 65.61.137.127**

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

Answer:

Text

Description automatically generated

Text, letter

Description automatically generated

* 1. **What is the IP address of the DNS server:**

Answer: 65.61.137.117

**Step 3: Shodan**

* + What open ports and running services did Shodan find:

Answer; Open Ports : Port 80; Port 443 and Port 8080

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Step 4: Recon-ng

* + Install the Recon module xssed.

Commands; recon-ng

* + marketplace install xssed
  + Modules load xssed
  + Info

* + Set the source to demo.testfire.net.

Text

Description automatically generated

 Run the module.

Text

Description automatically generated

 Is Altoro Mutual vulnerable to XSS:

Step 5: ZenmapYour 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:

Graphical user interface, text, application

Description automatically generated

* + Bonus command to output results into a new text file named zenmapscan.txt:

Graphical user interface, text, application

Description automatically generated

* + Zenmap vulnerability script command:

Graphical user interface, text, application, email

Description automatically generated

* + Once you have identified this vulnerability, answer the following questions for your client:
    1. **What is the vulnerability:**

Answer: the vulnerability id the is the STYPE\_DISKTREE which is the servers and is a temp file which is read/write

* + **Why is it dangerous:**

Answer: have access to the servers and then able to change system actions

* 1. **What mitigation strategies can you recommendations for the client to protect their server:**

Answer: Remove the temp file TYPE\_DISKTREE