**Week 16 Homework: Penetration Testing 1**

**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?

Graphical user interface, text, application, email

Description automatically generated

* How can this information be helpful to an attacker?

Google Dorking is a search technique that enables hackers to gain access to information that corporations and individuals did not intend to make publicly available. Using this technique, hackers are able to identify vulnerable systems and can recover usernames, passwords, email addresses, and even credit card details.

<https://www.mcafee.com/blogs/enterprise/google-dorking/#:~:text=Google%20Dorking%20is%20a%20search,and%20even%20credit%20card%20details>.

**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:
  1. Where is the company located?

Graphical user interface, text, application, email

Description automatically generated

* 1. What is the NetRange IP address?

Graphical user interface, text, application, email

Description automatically generated

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

Text

Description automatically generated

Underlying infrastructure in IT

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

Graphical user interface, text, application, email

Description automatically generated

DNS is where it will query and DNS servers will change so wasn’t sure if this is not right

**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](https://www.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?

Graphical user interface, website

Description automatically generated

Looking for version # for published exploits <https://www.exploit-db.com/exploits/43008>

**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.

Text

Description automatically generated

* Set the source to demo.testfire.net.

Text

Description automatically generated

* Run the module.

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* Is Altoro Mutual vulnerable to XSS?

Yes!!

**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.

Text

Description automatically generated

**Graphical user interface, text

Description automatically generated**

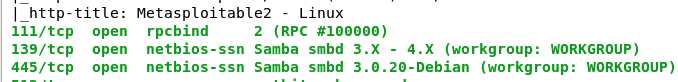
Text, letter

Description automatically generated

* + **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?

Samba smbd 3.X -4.X

<https://www.exploit-db.com/exploits/16320>

<https://www.cvedetails.com/vulnerability-list/vendor_id-102/product_id-171/version_id-41384/Samba-Samba-3.0.20.html>

* + Why is it dangerous?

This exploit triggers a heap overflow in the Samba dameon, specifically in the SMB which is the Server Message Block which is a protocol for sharing files, printers, serial ports and data on a network. In essence the way computers talk to one another. These ports need to remain secure, however, it is ok to leave them open because they are necessary for communication across the internet so they need remain secure including making sure they are configured correctly, patched when necessary, strict security rules in place and monitored frequently to avoid exploits.

<https://www.upguard.com/blog/smb-port>

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

These ports need to remain secure and open as they are necessary for communication across the internet. Therefore, my recommendations for the client is to keep them secure by making sure they are configured correctly, patched when necessary, strict security rules put into place and monitored frequently to avoid exploits.