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:
  -Karl Fitzgerald.
- How can this information be helpful to an attacker:
  -The attacker can either use this information to either spearphish the CEO or they could use it in a phishing attack against the company claiming to be from the CEO.

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:

1. Where is the company located:
   -9750 Datapoint Drive, Suite 100, San Antonio TX USA
2. What is the NetRange IP address:
   -65.61.137.64/26
3. What is the company they use to store their infrastructure:
   -Rackspace Backbone Engineering
4. What is the IP address of the DNS server:
   -65.61.137.117

Step 3: Shodan

- What open ports and running services did Shodan find:
  -80, 443, 8080

Step 4: Recon-ng

- Install the Recon module `xssed`.
  -*`marketplace install recon/domains-vulnerabilities/xssed`*
- Set the source to `demo.testfire.net`.
  `-options set source demo.testfire.net`
- Run the module.

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:

- Command for Zenmap to run a service scan against the Metasploitable machine:
  `nmap -sV 192.168.0.10`
- Bonus command to output results into a new text file named `zenmapscan.txt`:
  `nmap -sV 192.168.0.10 > zenmapscan.txt`
- Zenmap vulnerability script command:
  `nmap -v --script smb-enum-shares 192.168.0.10`
- Once you have identified this vulnerability, answer the following questions for your client:
  1. What is the vulnerability:
     -This vulnerability allows use to access to shares files on their Samba database. This sometimes contains confidential files the attacker can use.

2. Why is it dangerous:
   -This exploits the integrity and confidentiality of user’s data.
3. What mitigation strategies can you recommend for the client to protect their server:
   -I would recommend restricting access to shares files and to not put any confidential information on shares files on the samba database as it is vulnerable.