Penetration Testing 1

Step 1: Google Dorking

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

Karl Fitsgerald

- How can this information be helpful to an attacker:

It can help set up phishing attacks on fellow employees and executives.

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:

Sunnyvale, CA

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

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, and 8080

Step 4: Recon-ng

- Install the Recon module `xssed`.

- Set the source to `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 -T4 -A 192.168.0.10

- Bonus command to output results into a new text file named `zenmapscan.txt`:
nmap -T4 -A -oN zenmapscan.txt 192.168.0.10

- Zenmap vulnerability script command:
nmap -T4 -F --script ftp-vsftpd-backdoor,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:
Port 139 - open netbios-ssn
Port 445 - open microsoft-ds

  2. Why is it dangerous:
The vsftpd-backdoor can be used on FTP, port 21 with malicious code and can open the backdoor on port 6200.

Windows Server Message Block (SMB) allows access to an organization's network, which includes devices on it. You can traverse along the PCs and network as well as remote access.

  3. What mitigation strategies can you recommendations for the client to protect their server:
Keep your systems patched and updated for security flaws that have been already patched.
