Sasha Shahidi

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:
  An attacker can target the CEO in a phishing attack

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: 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: Port 80, Port 443, Port 8080, and running services Apache Tomcat/Coyote JSP engine 1.1

Step 4: Recon-ng

- Install the Recon module xssed.
  apt-get update && apt-get install recon-ng
  sudo recon-ng
  marketplace install xssed
  modules load xssed
- Set the source to demo.testfire.net
  options set SOURCE demo.testfire.net
- Run the module.
  run

Is Altoro Mutual vulnerable to XSS:
Yes, the summary says one new vulnerability was 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:

- Command for Zenmap to run a service scan against the Metasploitable machine:
  nmap-T4-F 192.168.0.10

- Bonus command to output results into a new text file named zenmapscan.txt:
  nmap-T4-F -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 21 TCP is vulnerable

  2. Why is it dangerous: Attackers are able to breach the server through Port 21 TCP and have read/write access to the data

  3. What mitigation strategies can you recommendations for the client to protect their server: Close Port 21 TCP until the software is updated