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:
  You can use the name of the CEO to find them on social media websites and launch Social Engineering attacks to attempt to recover his website login credentials, if an attack of this sort is successful, you would have access to the entire company's network due to him being a high level executive.

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

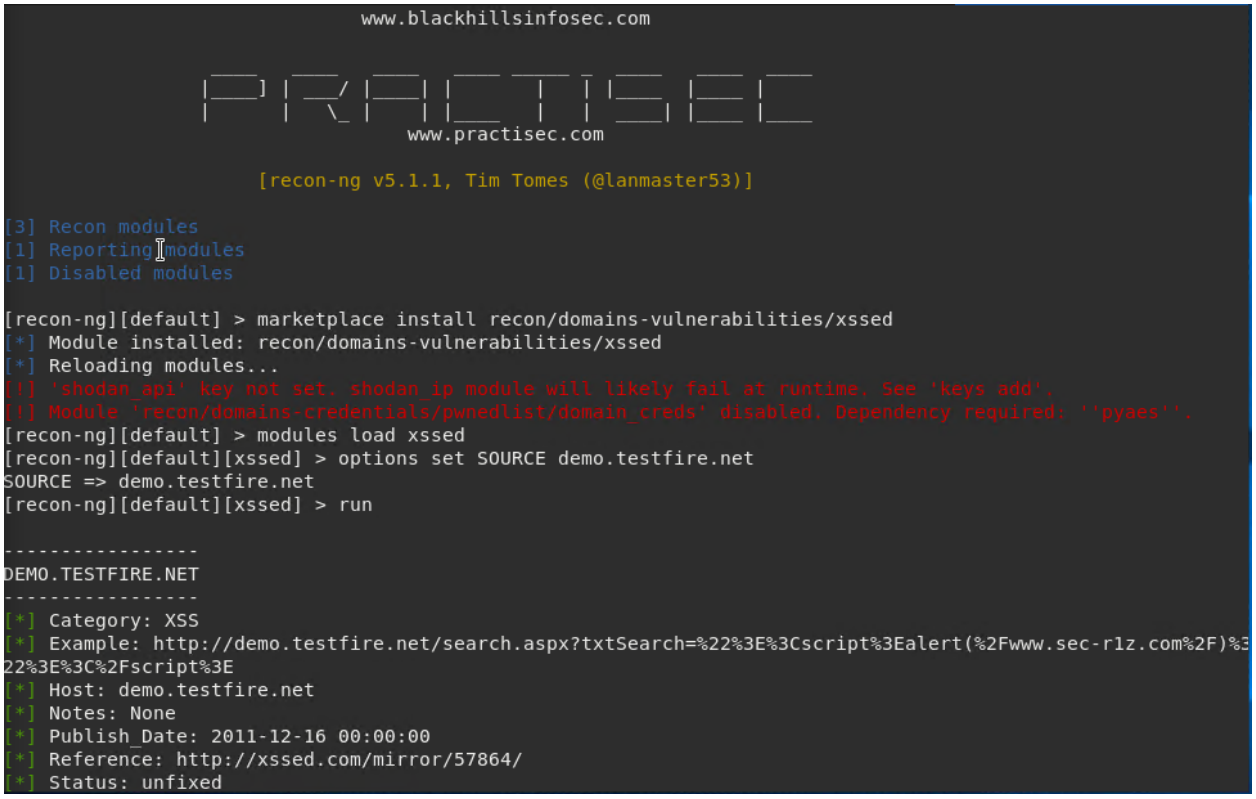
- What open ports and running services did Shodan find: 80 and 443, both running

  Apache Tomcat/Coyote JSP engine

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:



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:
  Zenmap -A -sV 192.168.0.10
- Bonus command to output results into a new text file named zenmapscan.txt:
  Zenmap -A -sV 192.168.0.10 -oN zenmapscan.txt
- Zenmap vulnerability script command:
  zenmap –script vuln 192.168.0.10
- Once you have identified this vulnerability, answer the following questions for your client:

    1. What is the vulnerability:
       SSL/TLS MITM vulnerability (CCS injection)
    2. Why is it dangerous:
       OpenSSL vulnerability that allows an attacker to hijack sessions or obtain sensitive information through a crafted TLS handshake.
    3. What mitigation strategies can you recommendations for the client to protect their server:

- Upgrading to a current, secure version of TLS that is implemented securely and configured to not accept fallback to SSL or early TLS.

- Encrypting data with strong cryptography before sending over SSL/early TLS (for example, using field-level or application-level encryption to encrypt the data prior to transmission).
