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:
    - ***Allows opportunity for reconnaissance, gathering and planning regarding a malicous attack on the company or personally. Most likely Phising or Spearphising.***

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 (HTTP), 443 (HTTPS), 22 (TCP)***
    - ***Apache Tomcat Version 1.1***
    - ***HTTP ONLY***

Step 4: Recon-ng

- Install the Recon module `xssed`.

- ***Marketplace install 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***

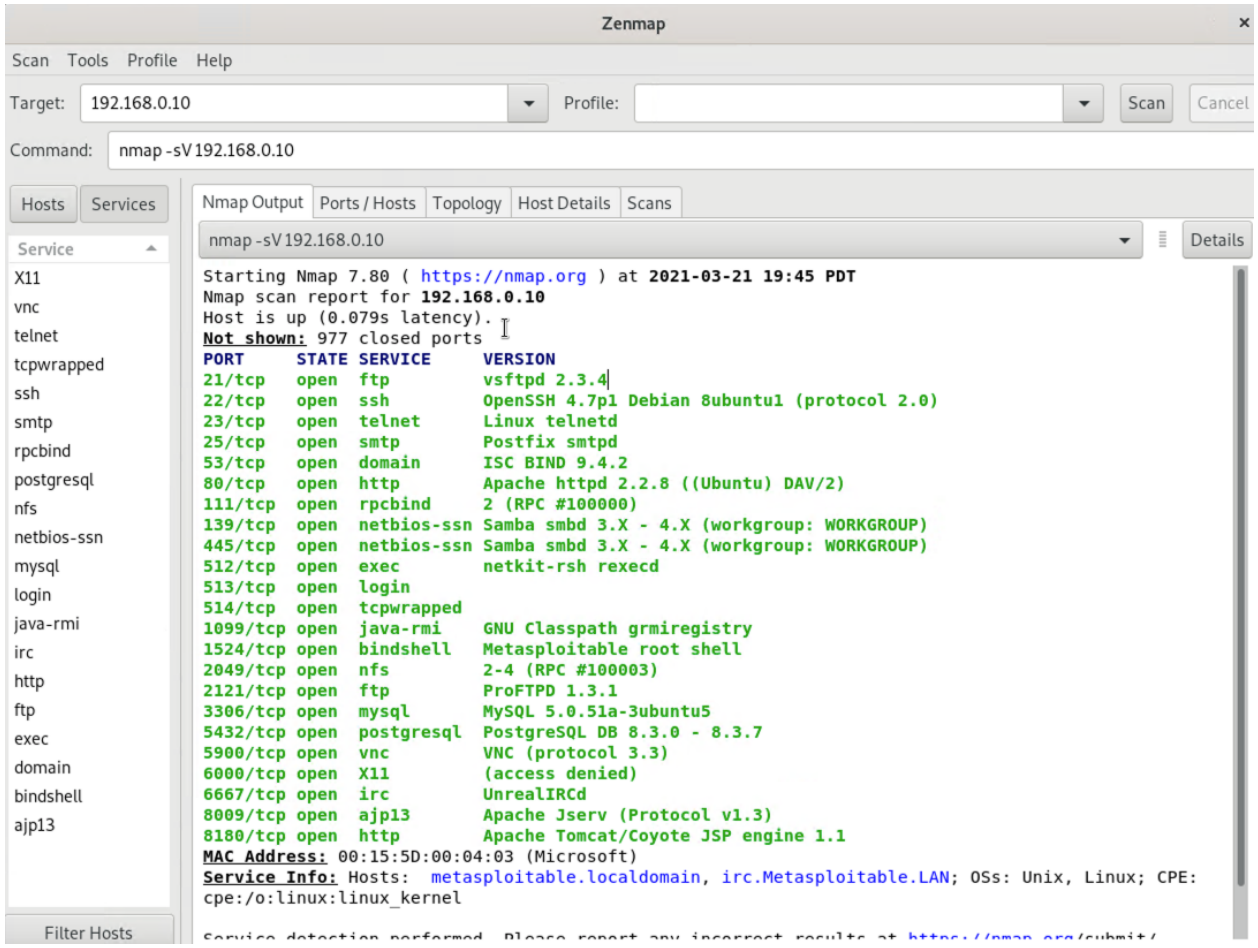
```
[recon-ng][default][xssed] > options set SOURCE demo.testfire.net
SOURCE => demo.testfire.net
[recon-ng][default][xssed] > info

      Name: XSSed Domain Lookup
    Author: Micah Hoffman (@WebBreacher)
   Version: 1.1

Description:
  Checks XSSed.com for XSS records associated with a domain and displays the first 20 results.

Options:
  Name    Current Value      Required  Description
  ------  -------------      --------  -----------
  SOURCE  demo.testfire.net  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][xssed] > run

-----------------
DEMO.TESTFIRE.NET
-----------------
[*] Category: XSS
[*] Example: http://demo.testfire.net/search.aspx?txtSearch=%22%3E%3Cscript%3Ealert(%2Fwww.sec-r1z.com%2F)%3C%2Fs<br>cript%3E%
22%3E%3C%2Fscript%3E
[*] Host: demo.testfire.net
[*] Notes: None
[*] Publish_Date: 2011-12-16 00:00:00
[*] Reference: http://xssed.com/mirror/57864/
[*] Status: unfixed
[*] ------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (1 new) vulnerabilities found.
[recon-ng][default][xssed] >
```

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




```
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds
```

- Bonus command to output results into a new text file named `zenmapscan.txt`:

-
```
4.0K -rw-r--r--  1 root root 1.7K Mar 21 19:54 zenmapscan.txt
root@kali:~#
```

- Zenmap vulnerability script command:

```
root@kali:~# nmap -sV 192.168.0.10 -oN zenmapscan.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-21 19:53 PDT
Nmap scan report for 192.168.0.10
Host is up (0.100s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

- Once you have identified this vulnerability, answer the following questions for your client:
    1. What is the vulnerability:
        - ***BadLock, requires patching***
    2. Why is it dangerous:
        - ***Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mishandle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."***
    3. What mitigation strategies can you recommendations for the client to protect their server:
        - ***Patch Samba to the following versions: 4.2.11, 4.3.8, 4.4.2 or the latest versions.***