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 knows who is the main target of the company which he has all information about the company.

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: **Texas, San Antonio (Nortwest Side) 78229**
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 (C05762718)**
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**
  - **http, https, tcp**
  - **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: **Yes**

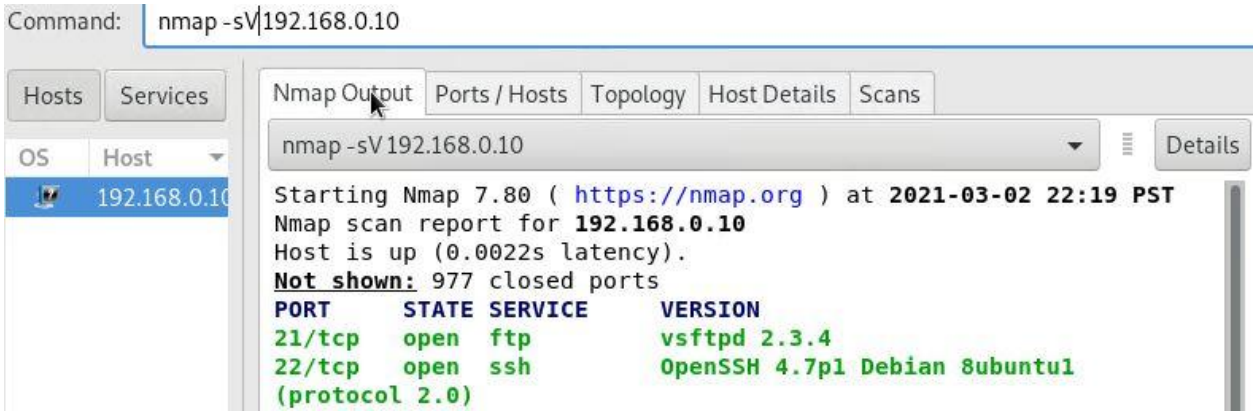
Step 5: Zenmap

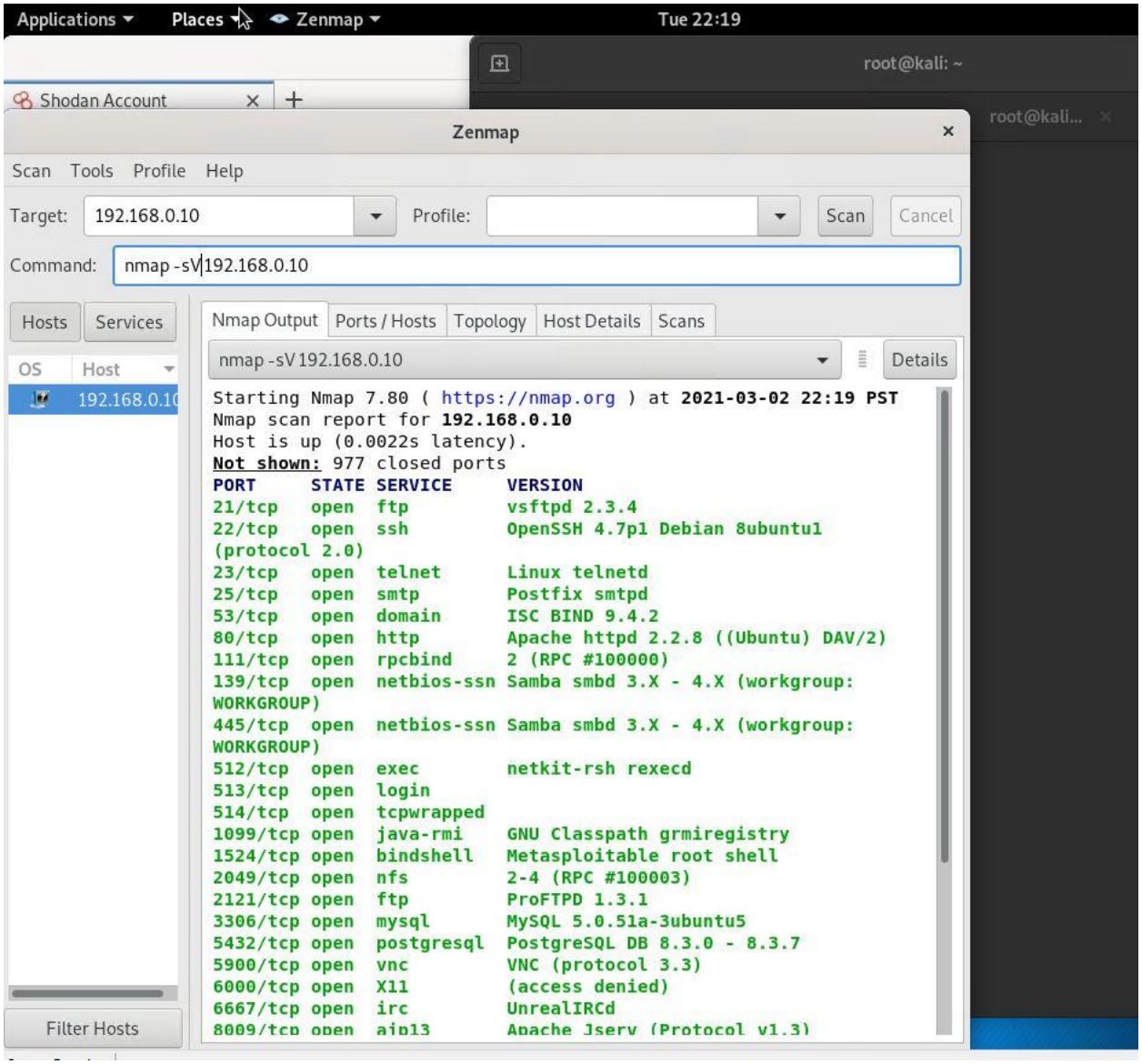
Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

- Command for Zenmap to run a service scan against the Metasploitable machine:

After opened the zenmap from terminal

command is: nmap -sV 192.168.0.10




Applications
Places
Zenmap
Tue 22:19
root@kali: ~
Shodan Account
root@kali...
Zenmap
Scan Tools Profile Help
Target: 192.168.0.10
Profile:
Scan
Cancel
Command: nmap -sV 192.168.0.10
Hosts
Services
OS
Host
192.168.0.10
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV 192.168.0.10
Details
Starting Nmap 7.80 (https://nmap.org) at 2021-03-02 22:19 PST
Nmap scan report for 192.168.0.10
Host is up (0.0022s 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)

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

  nmap -sV -oN ~/Documents/zenmapscan.txt 192.168.0.10

  nmap -sV 192.168.0.10 > ~/Documents/zenmapscan.txt

- Zenmap vulnerability script command:

  Nmap --script ftp-vsftp-backdoor,ftp-vuln-cve2010-4221 192.168.0.10

- Once you have identified this vulnerability, answer the following questions for your client:

  1. What is the vulnerability:

     ftp-vsftp-backdoor, will show on the list a port 5900 is open which is tcp/udp port is used b VNC, a platform for desktop sharing and remote control application.

  2. Why is it dangerous:

     attacker will be granted access to port 5900 and it's a remote desktop protocol that is very dangerous.

  3. What mitigation strategies can your recommendations for the client to protect their server:

     I would recommend closing port 5900 and other ports too. They can use port 22 SSH connection to control their system maybe, also remove anonymous permission. They can follow https://security.appspot.com/vsftpd.html and check for updates/new releases and download to make the system more secure