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 may be able to send malicious emails now that they know their target's full name.

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:

- Where is the company located: Sunnyvale, CA

- What is the NetRange IP address: 65.61.137.64 - 65.61.137.127

- What is the company they use to store their infrastructure: Rackspace Backbone Engineering

- What is the IP address of the DNS server: 65.61.137.117

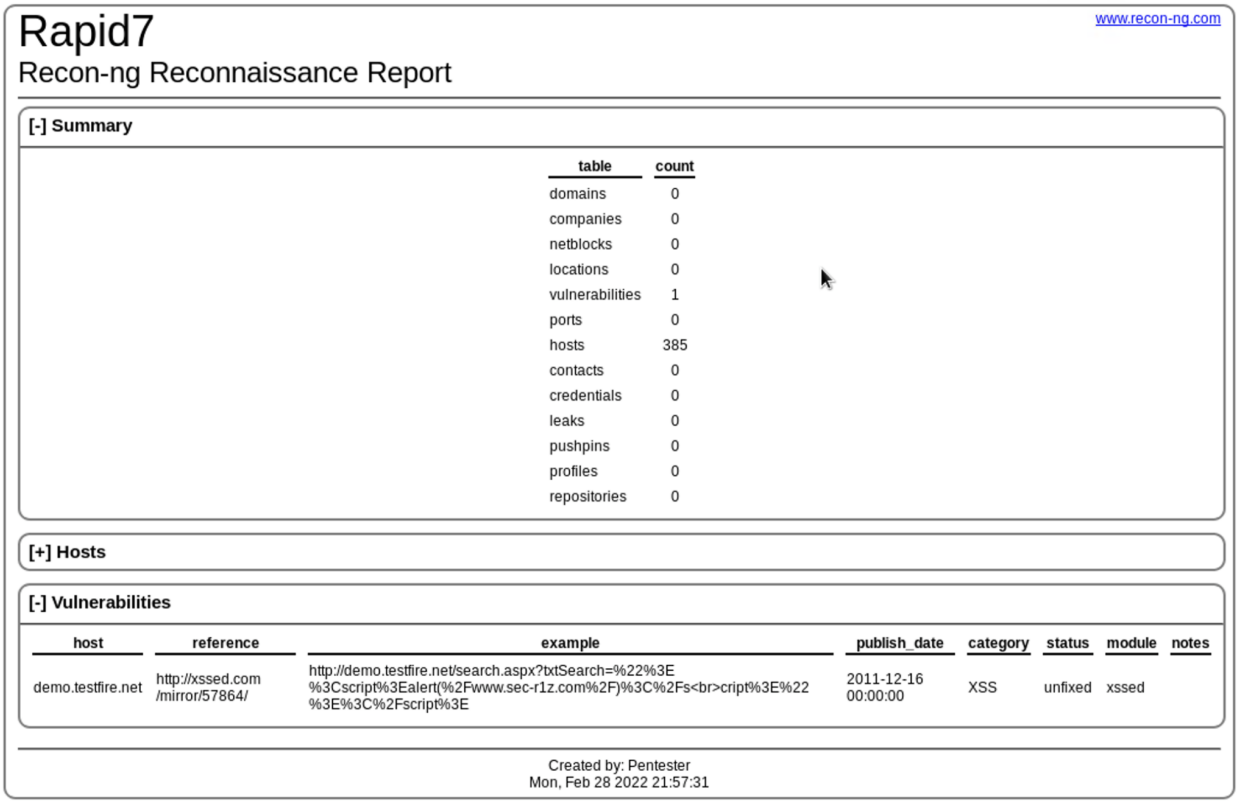
Step 3: Shodan

- What open ports and running services did Shodan find: Port 80 and Port 443 are open. Running services: Apache Tomcat/Coyote JSP engine 1.1

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



Rapid7

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	1
ports	0
hosts	385
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Hosts

[-] Vulnerabilities

host	reference	example	publish_date	category	status	module	notes
demo.testfire.net	http://xssed.com /mirror/57864/	http://demo.testfire.net/search.aspx?txtSearch=%22%3E %3Cscript%3Ealert(%2Fwww.sec-r1z.com%2F)%3C%2Fs cript%3E%22 %3E%3C%2Fscript%3E	2011-12-16 00:00:00	XSS	unfixed	xssed	

Created by: Pentester
Mon, Feb 28 2022 21:57:31

Step 5: Zenmap

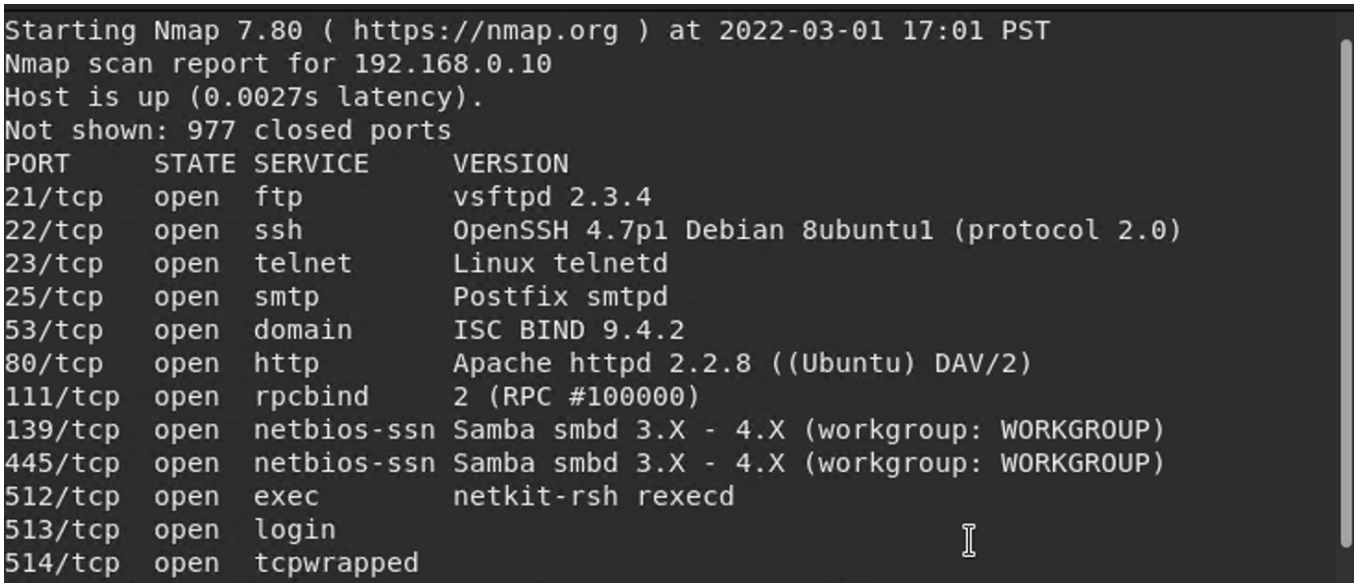
Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

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

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

- Zenmap vulnerability script command:
  - nmap--script ftp-vsftpd-backdoor 192.168.0.10

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



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-01 17:01 PST
Nmap scan report for 192.168.0.10
Host is up (0.0027s 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
```

- What is the vulnerability: The version Samba smbd 3.x - 4.x (workgroup: WORKGROUP) on ports 139.445 is the vulnerability.

- Why is it dangerous: Samba is dangerous as it allows different machines and operating systems to share resources with one another.

- What mitigation strategies can you recommend for the client to protect their server: Making sure the most recent version of Samba is being used.