Jeff King ## 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:

? I can send malicious email for phishing attack. I can create combination of his email,ka.fitzgerald@altoromutual.com

**#### 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: US 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:117.137.61.65

**#### Step 3: Shodan**

**-**What open ports and running services did Shodan find:80/ TCP

 443/ TCP 8080/ TCP

**#### 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: nmap -sS 192.168.0.10

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

**-**Zenmap vulnerability script command: nmap -sC -p 139,145 --script smb-os-discovery 192.168.0.10

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

**1.**What is the vulnerability:The script determined the target machine is running Samba-3.0.20-Debian, which

is vulnerable to the following CVEs (all with CVE Score > 9.0):

**\***CVE-2007-2446

**\***CVE-2012-1182

**\***CVE-2007-4572

**\***CVE-2007-5398

**\***CVE-2007-6015

**2.**Why is it dangerous:Both CVE-2007-2446 and CVE-2012-1182 allow a remote attacker to execute arbitrary code on the target machine. This is dangerous

because an attacker can gain access to the underlying system. Arbitrary code

execution is basically game-over for an attacker.

**3.**What mitigation strategies can you recommendations for the client to protect their server: The client should upgrade the version of samba they are running to the most

recent version, which has patched the vulnerabilities described by

CVE-2007-2446 and CVE-2012-1182.

**---**