Challenge Title: Recon 1

Challenge Category: Reconnaissance

Methodology:

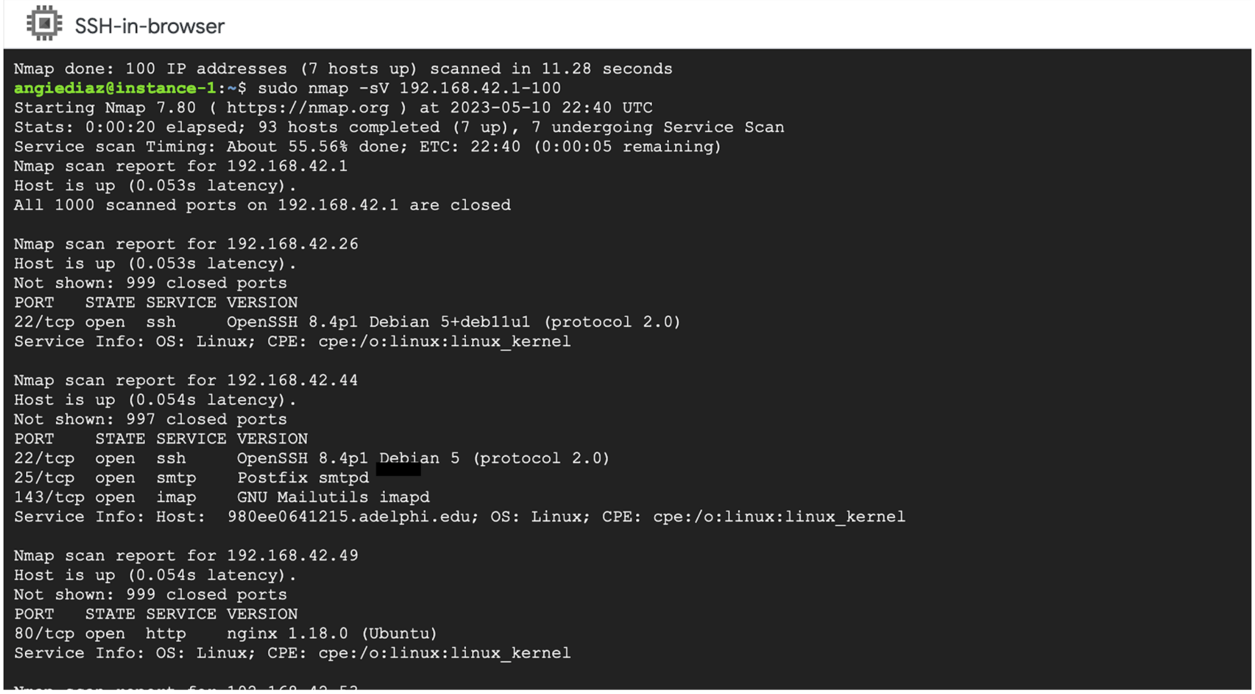
1. Used command sudo nmap -sV 192.168.42.1-100 on Linux terminal.

Flag Capture:

1. Flag: csc380ctf{192.168.42.44}
2. IP address associated with the open email server

Documentation:

1. Command sudo nmap -sV was used to scan between the IP address range 1-100. The purpose of using nmap -sV is to probe open ports to determine service/version info.
2. Port 25 is associated with mail servers, therefore an open port. On the linux terminal it will be displayed as “25/tcp open smtp   Postfix smtpd”.

3. 

```
Nmap done: 100 IP addresses (7 hosts up) scanned in 11.28 seconds
angiediaz@instance-1:~$ sudo nmap -sV 192.168.42.1-100
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-10 22:40 UTC
Stats: 0:00:20 elapsed; 93 hosts completed (7 up), 7 undergoing Service Scan
Service scan Timing: About 55.56% done; ETC: 22:40 (0:00:05 remaining)
Nmap scan report for 192.168.42.1
Host is up (0.053s latency).
All 1000 scanned ports on 192.168.42.1 are closed

Nmap scan report for 192.168.42.26
Host is up (0.053s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.42.44
Host is up (0.054s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd [redacted]
143/tcp open  imap    GNU Mailutils imapd
Service Info: Host:  980ee0641215.adelphi.edu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.42.49
Host is up (0.054s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.42.53
```

Challenge Title: Recon 2

Challenge Category: Reconnaissance

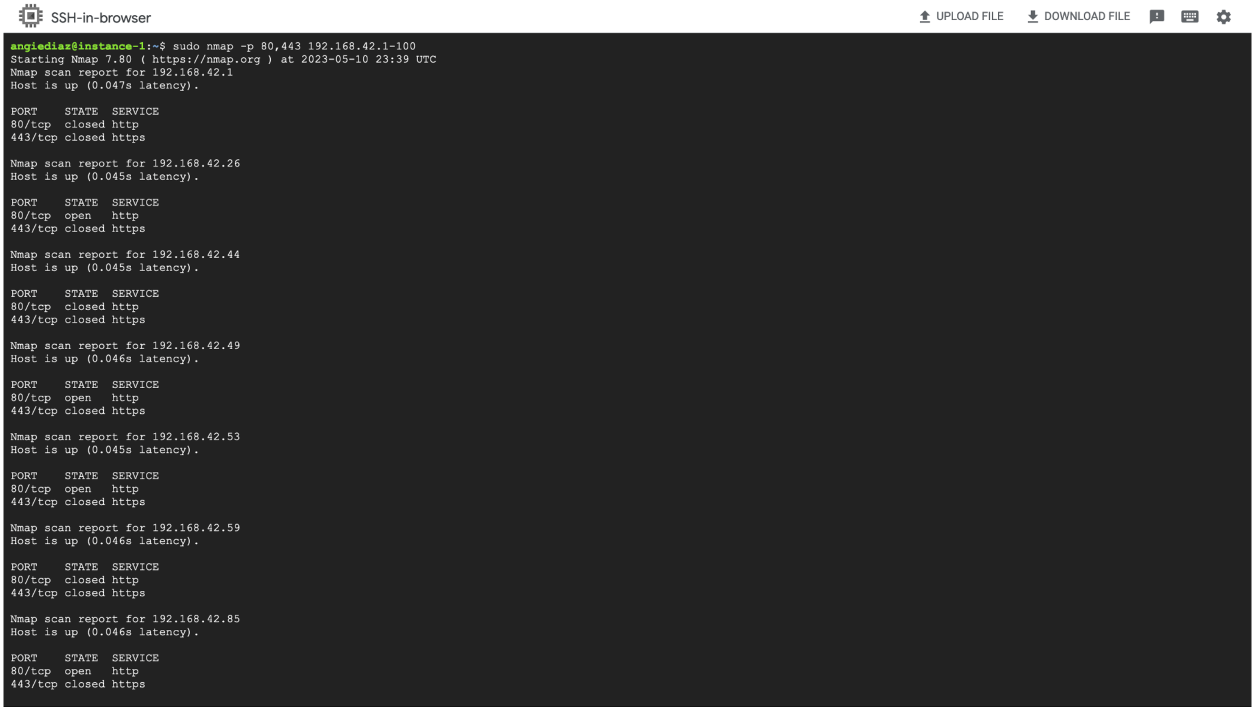
Methodology:

1. The command sudo nmap -p 80,443 192.168.42.1-100 is used to scan for these specific ports that will find the IP address for the Ubuntu web server.

Flag Capture:

1. Flag: csc380ctf{192.168.42.49}
2. This represents the IP address associated with the Ubuntu web server.

Documentation:

1. Command sudo nmap -p is used for <port ranges>: Only scan specified ports.
2. Port 80 is associated with a http connection and port 443 is associated with https connection.
3. Therefore, once the command is used it displays the IP addresses with the ports 80 and 443.
4. To conclude the IP address associated with the Ubuntu web server is 192.168.42.49.
5. 

```
angiediaz@instance-1:~$ sudo nmap -p 80,443 192.168.42.1-100
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-10 23:39 UTC
Nmap scan report for 192.168.42.1
Host is up (0.047s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap scan report for 192.168.42.26
Host is up (0.045s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 192.168.42.44
Host is up (0.045s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap scan report for 192.168.42.49
Host is up (0.046s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 192.168.42.53
Host is up (0.045s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 192.168.42.59
Host is up (0.046s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap scan report for 192.168.42.85
Host is up (0.046s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
```

Challenge Title: Recon 3

Challenge Category: Reconnaissance

Methodology:

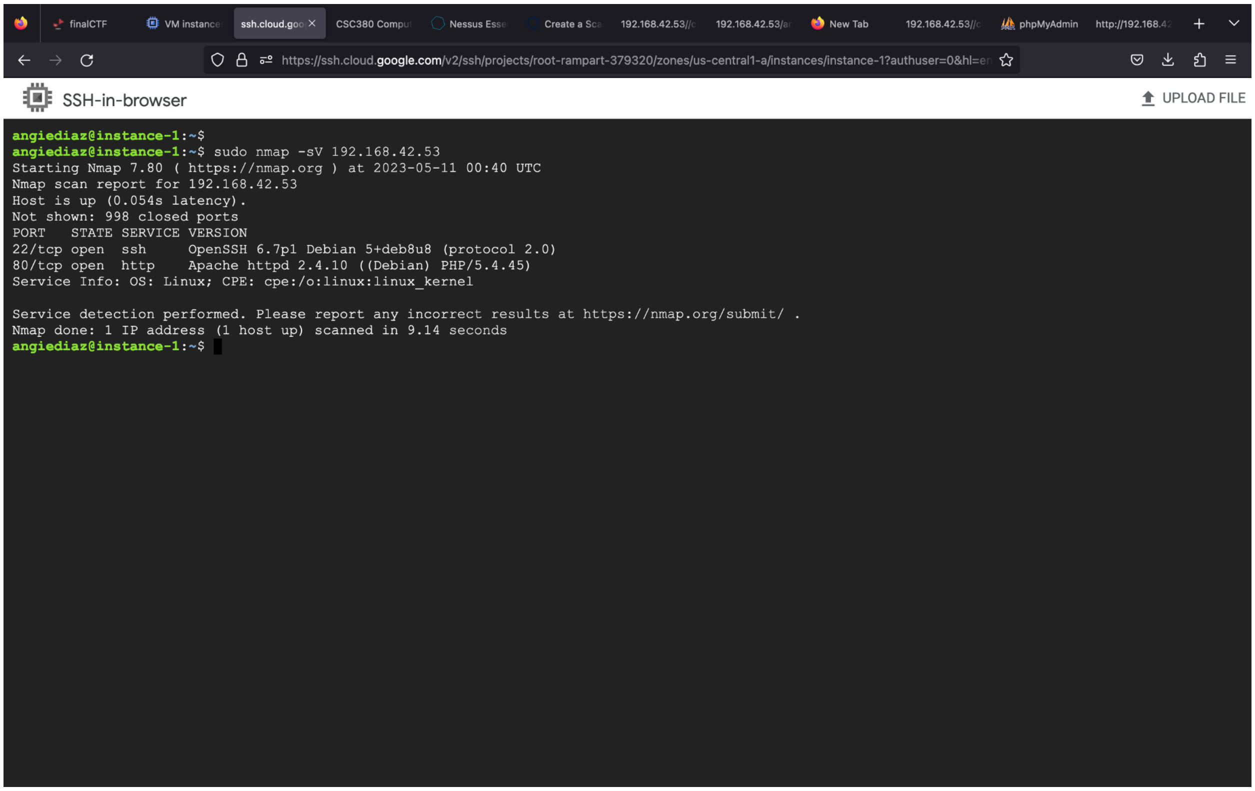
1. The command sudo nmap -sV 192.168.42.53 is used

2. This command is used to probe open ports to determine service/version info

Flag Capture:

1. Flag: csc380ctf{2.4.10}
2. This represents the version number of the web server software on 192.168.42.53

Documentation:

1. The command nmap -sV probes open ports and determines service/version info.
2. 

```
angiediaz@instance-1:~$
angiediaz@instance-1:~$ sudo nmap -sV 192.168.42.53
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-11 00:40 UTC
Nmap scan report for 192.168.42.53
Host is up (0.054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.10 ((Debian) PHP/5.4.45)
Service Info: OS: 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 9.14 seconds
angiediaz@instance-1:~$
```

3. Therefore, the command mentioned above displays the following information: version apache httpd 2.4.10(Debian) php/5.4.45).

Challenge Title: Recon 4

Challenge Category: Reconnaissance

Methodology:

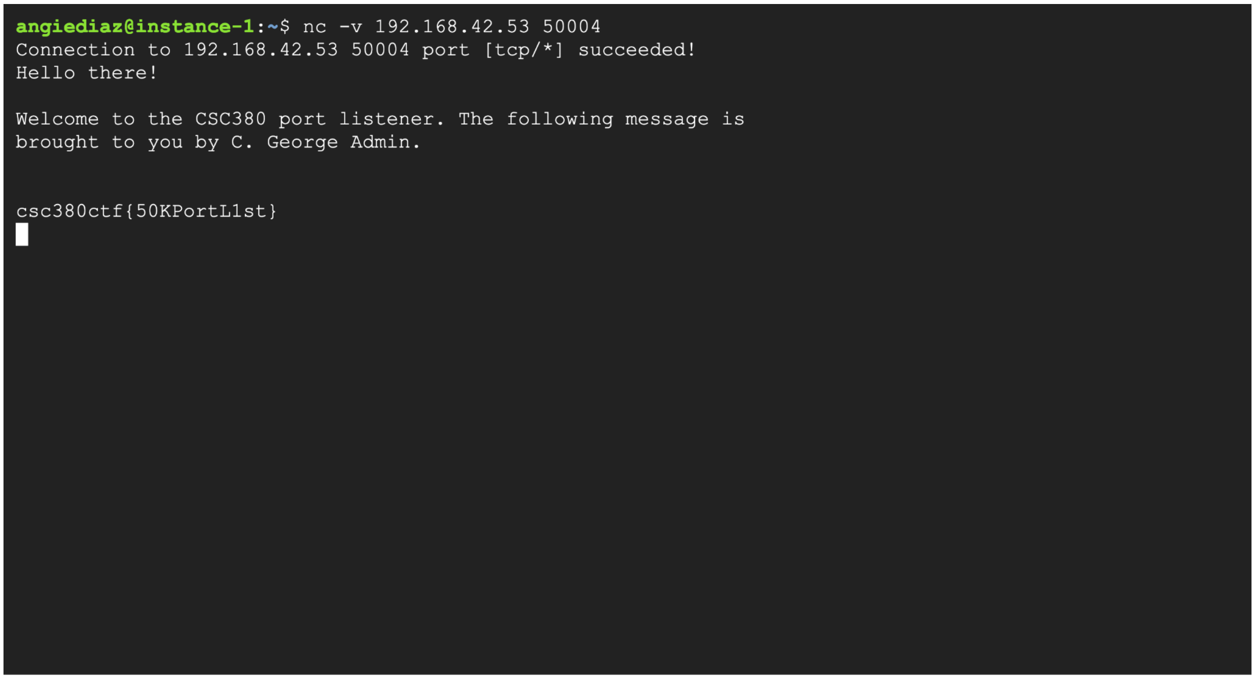
1. The command netcat was used to get the message sent back to you when you connect to the highest listening port on the web server that is also accessible via OpenSSH version 6.7p1.
2. The command netcat -v is used to get the message displayed on the terminal window.

Flag Capture:

1. Flag: csc380ctf{5oKPortL1st}
2. Message that is displayed on the terminal window is “Hello there!”

Documentation:

1. Before we start, I had to install netcat onto my terminal. This was done by first putting the command ‘sudo apt-get update’. Then after using the command ‘sudo apt-get install netcat’.
2. Then I used this command line “nc -v 192.168.42.53 50004” to get the message when you connect to the highest listening port.
3. The command nc(netcat) is used for arbitrary TCP and UDP connections and listen. The variable attached to it nc **-v** is used to produce more verbose output.

4. 

```
angiediaz@instance-1:~$ nc -v 192.168.42.53 50004
Connection to 192.168.42.53 50004 port [tcp/*] succeeded!
Hello there!

Welcome to the CSC380 port listener. The following message is
brought to you by C. George Admin.


csc380ctf{50KPortL1st}
```

Challenge Title: Recon 5

Challenge Category: Reconnaissance

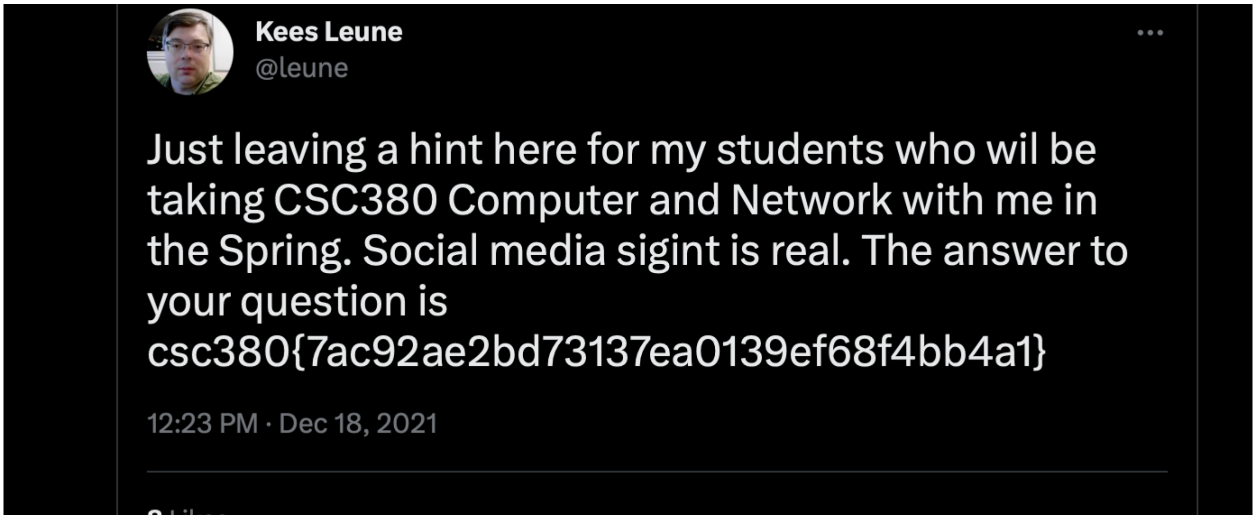
Methodology:

1. Google was used to search for Dr. Leune's social presence online
2. The information that was collected from his main source from the Adelphi.edu directory page.
3. On the directory page, it lists Dr. Leune's twitter, github, linkdin. From these, we start to search through each socia media presence.

Flag Capture:

1. Flag: csc380{7ac92ae2bd73137ea0139ef68f4bb4a1}

Documentation:

1. At first I went through his main social media accounts that were listed on his directory. Dr. Leune also has two personal social blogs that he runs. While doing reconnaissance and during this challenge, I had an idea that the flag would be on twitter since where else would he keep a flag. Twitter is where I would upload a flag.
2. While looking at his twitter posts, the flag was posted in 2021. Therefore, while trying to gain more information about a person, it takes a lot of patience.
3. 

Kees Leune
@leune

Just leaving a hint here for my students who wil be taking CSC380 Computer and Network with me in the Spring. Social media sigint is real. The answer to your question is csc380{7ac92ae2bd73137ea0139ef68f4bb4a1}

12:23 PM · Dec 18, 2021

Challenge Title: Attack 0

Challenge Category: Attacks

Methodology:

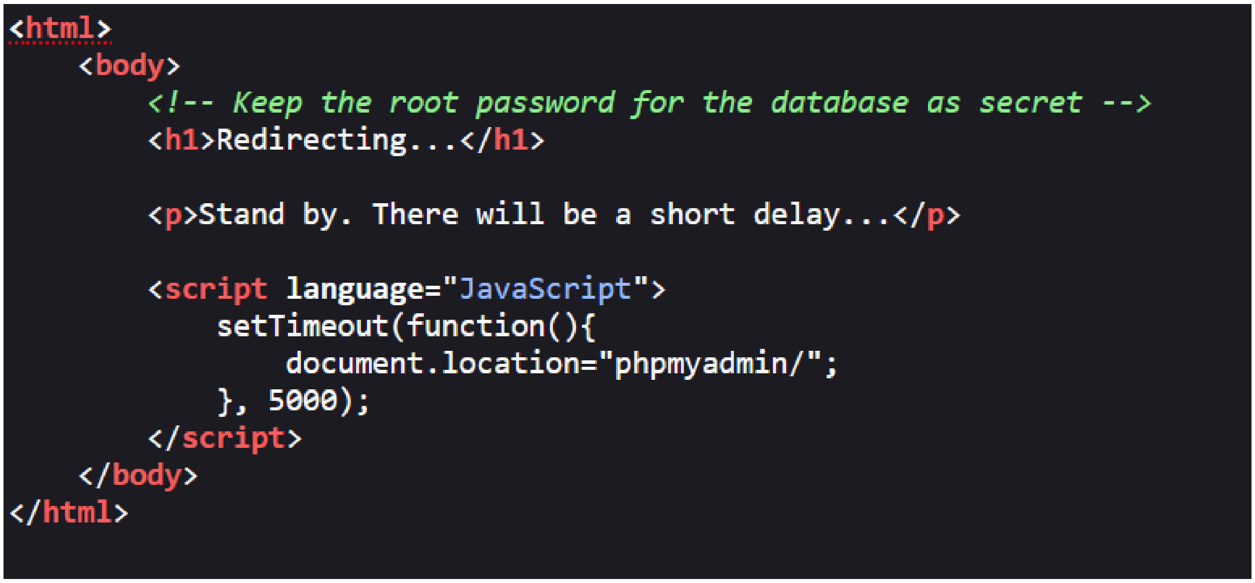
1. I first used a vunerability scanner to scan the IP address 192.168.42.53. After the scan, it listed many vulnerabilities and I filtered it out by searching for ‘phpMyAdmin’.
2. The tool I used was Nessus Essentials.

Flag Capture:

1. Flag: csc380ctf{ReadySetGo!}

Documentation:

1. I typed in the url bar http://192.168.42.26. From here on the source page it says this:



```
<html>
    <body>
        <!-- Keep the root password for the database as secret -->
        <h1>Redirecting...</h1>

        <p>Stand by. There will be a short delay...</p>

        <script language="JavaScript">
            setTimeout(function(){
                document.location="phpmyadmin/";
            }, 5000);
        </script>
    </body>
</html>
```

2. Therefore, on the login page I used the root as the username and secret as password. After the flag ReadySetGo! Will appear.