Goal: Gain access to and traverse 4 networked machines in order to get the coupon for a lifetime supply to a mysterious restaurant.

Storyline:
You, the attacker, saw the CEO of Chiptole, Dan, announce that he is the only person in the world to have some 'ultimate free coupon'. You have gained access to a new employee's workplace machine through reconnaissance and weaponization (phishing email). The success of the phishing exploit has given you the username and password of Jayson, and you have infiltrated the machine through SSH.

Starting point:

- Pre-Boot:
  - A virtual Host-Only Adapter is required and must be created if one does not already exist
  - Check to see if any of the 4 machines have conflicting ip's with your machine/network
    - 192.168.56.150
    - 192.168.56.132
    - 192.168.56.115
    - 192.168.56.110
- Make sure all 4 of the virtual machines/boxes are booted up and the network configurations are correct
- Kali box (2020.4) preferred, recommend most updated ssh and nmap on the attacking machine of your choice

A. Traversal from Jayson's machine to Brent's- nmap brute force
   1. On your machine perform an nmap scan with "nmap -sN 192.168.56.0/24" to get a scope of the machines on the network. You should see 4 new ip addresses in total. Notice only one machine has a visible service.
   2. You will need to SSH into this machine with the credentials that you hacked earlier (username:jayson – password:chiptole). Use the following command in terminal:
      a. ssh jayson@192.168.56.150
      b. When prompted for password enter: chiptole
   3. Once ssh is connected look around with "ls" and "cd" until you will find a .txt file on Jayson's Desktop ("Welcome.txt"). The text file is from Jayson's new boss, Brent. Within the text, Brent mentions "nmap", which will indicate that a lot of the machines will have it installed; making it an excellent option for an exploit. Brent also gives a link to the employee handbook on a website he is hosting as he has been practicing HTML. The link will give you Brent's ip address.
   4. You then use Brent's ip to attempt a brute force attack to ascertain Brent's password. Knowing that Jayson's machine only has nmap as a useful hacking tool, you find out that nmap actually has its own brute force function. To set up

the brute force you first need to create a completely blank text file with the username you want to brute force with, which you already know is “brent”. We will name the text file brent.txt and put it on the Desktop

   a. “nmap 192.168.56.132”
      i. to get a look at Brent’s machine initially
   b. “nmap -p 22 --script ssh-brute --script-args userdb=~/Desktop/brent.txt 192.168.56.132
      i. The command to run in terminal to run the brute force attack

5. After a few minutes (should be under 5) of using ssh-brute script against a popular password text file, you will find Brent’s password.
6. Then ssh into Brent’s machine with these credentials
   a. Username:brent – password:blink182
   b. ssh brent@192.168.56.132

B. Traversal from Brent’s machine to Dan’s

1. Go to the Desktop directory in the terminal, “ls” the directory. You will see the to-do.txt and the UFW Update folder.
2. Cat the to-do.txt. It will indicate Dan’s ip address, but no credentials to access his machine. At that point, you will need to go to the FTP server by looking in the UFW Update folder.
3. Once you open the UFWfolder you will see the first README.txt as well as the shell script mentioned in the to-do list. The readme also mentions a previous anonymous attacker which will tell you that there is an anonymous login to get the FTP. It also mentions that the shell script will disable the firewall.
4. Now that you have clues pointing to FTP and the ufw rules, the best route is to disable the machines firewall first (allowing your kali box to ssh), exit ssh, then ssh into Brent’s machine straight from Kali
   a. “sudo ufw disable”
   b. This is recommended purely to avoid multi-layered ssh through multiple machines, which can cause connection/lag issues
5. Connect to Dan’s FTP server
   a. ftp 192.168.56.115 with username:anonymous – password:anonymous
      i. Look around with ‘ls’, ‘cd’, and ‘ls -a’
      ii. Find the hidden .delete.txt file
   b. Use the ‘get’ command to grab the .delete.txt file and place it onto Brent’s machine
      i. get .delete.txt
   c. Back out of the ftp server
   d. Cat the .delete.txt file (remember that it’s hidden), notice that it is encoded
   e. Decode with base64 and xxd -r -p
      i. First line: Copy +Paste line one,
         1. echo NjM2ODY5NzA3NDZmNmM2NTIwNzM2NTcyNzY2NTcyMjAzMTM5MzIyZTMxMzYzODJlMzUzNjJlMzEzMTMwCjBhCg== | base64 -d | xxd -r -p

ii. Second line: Copy + Paste line two,

1. echo 5a4746754f6e527661326c76614739305a57774b0a| xxd -r -p | base64 -d

f. The decoded file contains the important Chiptole server ip and Dan's login credentials

i. Username:dan – password:tokiohotel

g. SSH from Brent's machine into Dan's trying the newfound credentials

i. ssh dan@192.168.56.115

ii. Password: tokiohotel

h. Once inside Dan's machine, disable the firewall, back out of the ssh from Brent's machine, and ssh from your kali box into Dan's machine for a better connection

i. "sudo ufw disable"

ii. ssh dan@192.168.56.115

iii. Password: tokiohotel

C. Traversal from Dan to server & Finding the Coupon

1. SSH into the Chiptole server mentioned in the .delete.txt with Dan's credentials

a. ssh dan@192.168.56.110

b. password: tokiohotel

2. You find the README.txt in the Chiptole server home directory, and start the moon-buggy game so you can unlock secure-coupon.zip

a. To run moon-buggy just type: moon-buggy

3. Get the highscore in moon-buggy and obtain the password for the locked zip file containing the coupon

a. unzip secure-coupon.zip

b. password: i<3abry's

c. cat the coupon.txt to see the Abry's coupon