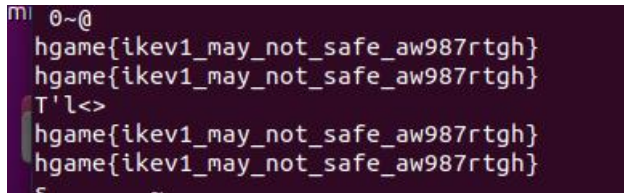


Misc

Tunnel

Pcap 流量文件，拖入虚拟机，string 一下，发现 flag

hgame{ikev1_may_not_safe_aw987rtgh}



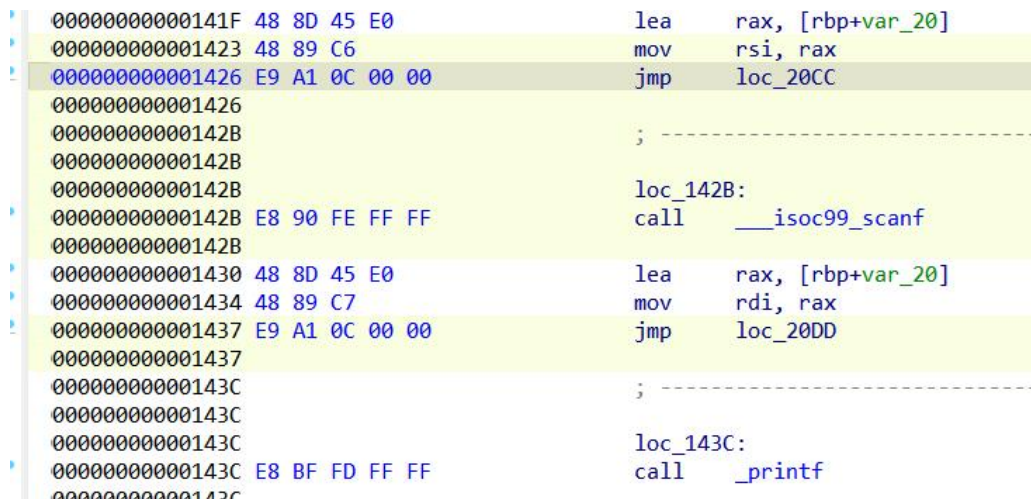
```
m 0~@
hgame{ikev1_may_not_safe_aw987rtgh}
hgame{ikev1_may_not_safe_aw987rtgh}
T'l<>
hgame{ikev1_may_not_safe_aw987rtgh}
hgame{ikev1_may_not_safe_aw987rtgh}
S
```

Re

Patchme

根据题目描述需要修复漏洞，拖入 ida 发现两个漏洞分别是 gets 的栈溢出和 printf 的格式化字符串漏洞，取巧的方法首先写一个没有漏洞的 c 程序，在 linux 环境下用 gcc 编译，将得到的二进制文件拖入 ida，对着 patch

将 gets 函数改为 scanf("%23s")， printf 函数加上输出位数即可，由于 lea 命令占用 7 字节，会覆盖后方命令，所以需要 jmp 到 frame 段来增加 lea 命令



```
00000000000141F 48 8D 45 E0      lea     rax, [rbp+var_20]
000000000001423 48 89 C6         mov     rsi, rax
000000000001426 E9 A1 0C 00 00   jmp     loc_20CC
000000000001426
00000000000142B ; -----
00000000000142B
00000000000142B loc_142B:
00000000000142B E8 90 FE FF FF   call    ___isoc99_scanf
00000000000142B
000000000001430 48 8D 45 E0      lea     rax, [rbp+var_20]
000000000001434 48 89 C7         mov     rdi, rax
000000000001437 E9 A1 0C 00 00   jmp     loc_20DD
000000000001437
00000000000143C ; -----
00000000000143C
00000000000143C loc_143C:
00000000000143C E8 BF FD FF FF   call    _printf
00000000000143C
```

Flag: hgame{You_4re_a_p@tch_master_Or_reverse_ma5ter}