深入浅出分析Linux系统内核漏洞的问题（4） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E6_B7_B1_E5_85_A5_E6_B5_85_E5_c103_144389.htm 通常主机A与主机B的TCP连接是通过主机A向主机B提出请求建立起来的，而其间A和B的确认仅仅根据由主机A产生并经主机B验证的初始序列号ISN。具体分三个步骤。 主机A产生它的ISN，传送给主机B，请求建立连接；B接收到来自A的带有SYN标志的ISN后，将自己本身的ISN连同应答信息ACK一同返回给A；A再将B传送来的ISN及应答信息ACK返回给B。至此，正常情况下，主机A与B的TCP连接就建立起来了。 B ---- SYN -- A B B ---- ACK -- A 假设C企图攻击A，因为A和B是相互信任的，如果C已经知道了被A信任的B，那么就要想办法使得B的网络功能瘫痪，防止别的东西干扰自己的攻击。在这里普遍使用的是SYN flood。攻击者向被攻击主机发送许多TCP- SYN包。这些TCP-SYN包的源地址并不是攻击者所在主机的IP地址，而是攻击者自己填入的IP地址。当被攻击主机接收到攻击者发送来的TCP-SYN包后，会为一个TCP连接分配一定的资源，并且会以接收到的数据包中的源地址（即攻击者自己伪造的IP地址）为目的地址向目的主机发送TCP-（SYN ACK）应答包。由于攻击者自己伪造的IP地址一定是精心选择的不存在的地址，所以被攻击主机永远也不可能收到它发送出去的TCP-（SYN ACK）包的应答包，因而被攻击主机的TCP状态机处于等待状态。如果被攻击主机的TCP状态机有超时控制的话，直到超时，为该连接分配的资源才会被回收。因此如果攻击者向被攻击主机发送足够多的TCP-SYN包，并且足

够快，被攻击主机的TCP模块肯定会因为无法为新的TCP连接分配到系统资源而处于服务拒绝状态。即使被攻击主机所在网络的管理员监听到了攻击者的数据包也无法依据IP头的源地址信息判定攻击者是谁。 当B的网络功能暂时瘫痪时，C必须想方设法确定A当前的ISN。首先连向25端口，因为SMTP是没有安全校验机制的，与前面类似，不过这次需要记录A的ISN，以及C到A的大致的RTT(round trip time)。这个步骤要重复多次以便求出RTT的平均值。一旦C知道了A的ISN基值和增加规律，就可以计算出从C到A需要RTT/2 的时间。然后立即进入攻击，否则在这之间有其他主机与A连接，ISN将比预料的多。 C向A发送带有SYN标志的数据段请求连接，只是信源IP改成了B。A向B回送SYN ACK数据段，B已经无法响应，B的TCP层只是简单地丢弃A的回送数据段。这个时候C需要暂停一小会儿，让A有足够时间发送SYN ACK，因为C看不到这个包。然后C再次伪装成B向A发送ACK，此时发送的数据段带有C预测的A的ISN 1。如果预测准确，连接建立，数据传送开始。问题在于即使连接建立，A仍然会向B发送数据，而不是C，C仍然无法看到A发往B的数据段，C必须蒙着头按照协议标准假冒B向A发送命令，于是攻击完成。如果预测不准确，A将发送一个带有RST标志的数据段异常终止连接，C只有从头再来。随着不断地纠正预测的ISN，攻击者最终会与目标主机建立一个会晤。通过这种方式，攻击者以合法用户的身份登录到目标主机而不需进一步的确认。如果反复试验使得目标主机能够接收对网络的ROOT登录，那么就可以完全控制整个网络。 