详解网络数据截获方法及流程(附图) PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/142/2021_2022__E8_AF_A6_E8_A7_A3_E7_BD_91_E7_c101_142482.htm 网络数据包截获机制是网络入侵检测系统的基础组件。一般指通过截获整个网络的所有信息流量，根据信息源主机，目标主机，服务协议端口等信息简单过滤掉不关心的数据，再将用户感兴趣的数据发送给更高层的应用程序进行分析。流程图如下： 图5.1 网络数据截获流程 一方面要，网络截取模块要能保证截取到所有网络上的数据包，尤其是检测到被分片的数据包(这可能蕴涵着攻击)。 另方面，数据截取模块截取数据包的效率也是很重要的。 它直接影响整个入侵检测系统的运行速度。 5.2各种数据流截获方法 5.2.1 利用广播截取网络数据流 数据包的截取技术是依赖网卡的。而网卡可以通过广播监听到以太网络上的数据包，这就是数据包截取技术的基础。 要想截获不是给自己数据流，就必须绕开系统正常工作的机制，直接通过网卡的混杂模式，使之可以接受目标地址不是自己的MAC地址的数据包，直接访问数据链路层，取数据。 5.2.2各系统截取数据包机制 Linux系统为用户提供一种在理论上是数据链路层的，基于网卡驱动程序的，可以不用操作系统自身协议栈的接口（也称套接字）-SockPacket. 这种套接字可以从数据链路层（就是网线）上直接截取所有链路层数据包。而Unix则是通过Libpcap库直接与内核交互，实现网络截取。如：Libpcap，Tcpdump等。如图： 图5.2 Unix系统监听机制 100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com