入侵检测系统的理论和实践 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c101_251024.htm 自从计算机以网络方式被连接开始，网络安全就成为一个重大问题，随着INTERNET的发展，安全系统的要求也与日俱增，其要求之一就是入侵检测系统。 本文旨在介绍几种常见的入侵检测系统及其理论和实践，需要指出的是，本文仅仅是一篇介绍性的文章,即使我推荐了许多可能的系统，在你相信其可靠性前，最好还是深入的研究一下他们。(NND,烦死我了,要敲4个字，以后我就简称ID得了。入侵检测系统就是IDS ：-) ) 一、什么是入侵检测。 入侵检测是指监视或者在可能的情况下，阻止入侵或者试图控制你的系统或者网络资源的那种努力。简而言之，它的工作方式是这样的：你有台机器，被连接到网络上，也许就是被连到了INTERNET上，出于可以理解的原因,你也愿意为被授权者设置从网络上访问你的系统的许可。比如，你有以台连接到INTERNET上的WEB服务器，愿意让客户、职员和潜在客户可以访问存储在WEB服务器上的页面。 然而，你并不愿意那些未经授权的职员、顾客或者其他未经授权的第三方访问系统。比如，你不愿意除了公司雇佣的网页设计人员以外的人员可以修改储存在机器上的页面。典型的做法之一就是使用防火墙或者某种认证系统来防止未经授权的访问。 但是，在一些情况下，简单的使用防火墙或者认证系统也可以被攻破。入侵检测就是这样以种技术，它会对未经授权的连接企图作出反应，甚至可以抵御以部分可能的入侵。 二、为什么要使用ID呢？ 以下给出了使用ID的理

由：（1）你需要保护自己的数据安全和系统，而事实是在现在的INTERNET环境下，如果你仅仅使用普通的密码和文件保护方式，你不可能永远保证你数据和系统的安全性。（2）对于保护数据来说，没有什么比系统的安全更重要了，想就这么把你的机器连上INTETNET而不作任何防护，甚至连管理员密码都不设，就指望这台机器会太平无事，那简直是近乎于痴心妄想。同样，系统对核心文件或者授权数据库（比如NT的SAM和UNIX的/ETC/PASSWORD或者/ETC/SHADOW）的保护也是非常重要的。（3）在通过局域网连接到INTERNET的环境下，经常会采用防火墙或者其他保护措施，如果在NT环境下，如果开放了文件共享，或者允许TELNET，这台机器就需要更好的保护，比如在防火墙中对137－139端口（属于TCP/UDP），SMB协议下的NT文件共享加以限制、使用SSH取代UNIX环境下的TELNET连接。（4）ID还有进一步的作用，由于被放置在防火墙和被保护的系统之间，ID等于是在系统之上增加了以层保护。比如，通过ID对敏感端口的监测就可以判断防火墙是否已经被攻破，或者防护措施已经被灭了。 三、ID有哪些种类呢？ ID可以分为两大类，（1）基于网络的系统：这种ID放置于网络之上，靠近被检测的系统，它们监测网络流量并判断是否正常。（2）基于主机的系统：这种系统经常运行在被监测的系统之上，用以监测系统上正在运行的进程是否合法。我还想补充最近出现的一种ID：位于操作系统的内核之中并监测系统的最底层行为。所有这些系统最近已经可以被用于多种平台。基于网络的ID 简介 基于网络的IDS是指监测整个网络流量的系统，一块网卡就可能会有两种用途： 普通模式： 受数据包

里面所包含的MAC地址决定，数据被发送到目的主机。 任意模式（Promiscuous mode）：所有可以被监测到的信息均被主机接收。 网卡可以在普通模式和任意模式之间进行切换，同样，使用操作系统的低级功能就可以完成这种变换。基于网络的IDS一般是需要把网卡设置成后以种模式。 包嗅探和网络监测 包嗅探和网络监测最初是为了监测以太网的流量而设计的，最初的代表性产品就是NOVEL的LANALYSER和MS的NETWORK MONITOR。 这些产品一般会拦截它们在网络上可疑拦截的一切数据包，当一个数据包被拦截后，可能会有以下几种情况： 对包进行累加，在截取的时间段内对数据包进行累加，用以确定该时间段内网络的负载，LANALYSER和MS的NM都在网络负载的表示界面方面有很好的表现。 对数据包进行分析：比如，当你想对抵达一个WEB服务器的数据进行分析时，你往往会先捕获一些数据，然后进行分析。包嗅探工具在近年有了长足的发展，象ETHEREAL和新版的MSNM都可以对数据包进行详尽的分析。 最后罗嗦以句（NND，洋人就是P多）：工具本身无善恶，全在人心，通过对连接到UNIX的TELNET连接进行包嗅探，就可能可以截取用户的密码，任何一个入侵者一旦得手，首先的事情就是会安装包嗅探器（NND，那是说高手，象俺最多在自己的机器上装个嗅探器，嘿嘿） 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