<<信息安全技术与应用>>

图书基本信息

书名：<<信息安全技术与应用>>

13位ISBN编号：9787115302472

10位ISBN编号：7115302472

出版时间：2013-3

出版时间：人民邮电出版社

<<信息安全技术与应用>>

内容概要

<<信息安全技术与应用>>

书籍目录

章节摘录

版权页： 插图： ②不受加密和交换设备影响。
HIDS只关注主机本身发生的事件，并不关心主机之外的网络事件，所以检测性能不受数据加密、隧道和交换设备影响。
网络入侵检测系统利用网络监听采集网络中传输的数据流，通过网络协议解析还原成传输层或应用层的网络连接记录，然后根据连接记录属性特征识别网络异常行为。
但是当数据采用加密传输或使用加密技术进行攻击时，由于没有密钥解密，自然不能获得协议类型、IP地址和服务类型等基本属性。
此外，网络传感器只采集所在网段的数据，不能采集位于不同网段的数据。
使用交换设备划分多个网段后，将减小网络入侵检测系统监测的范围。
网络传感器造价十分昂贵，安装多台网络传感器将大大增加系统的部署成本。
③不受网络流量影响。
由于网络传感器解析网络数据需要耗费许多计算资源，当网络流量过高时，网络传感器不能及时采集就会丢失数据，在高速网络环境下数据处理和分析能力显著下降是网络入侵检测系统的致命缺陷，因此，随着网络流量的增加，攻击检测率将迅速下降，而且网络流量与检测率之间的矛盾随着吉比特网和10吉比特网的日益普及显得更加突出。
HIDS并不采集网络数据，不会因为网络流量增加而丢失对系统行为的监视，故其检测性能与网络流量无关。
但HIDS也存在许多缺点，HIDS安装在需要保护的主机上，必然会占用主机系统资源，额外负载将降低应用系统的效率。
此外，HIDS完全依赖操作系统固有的审计机制，所以必须与操作系统紧密集成，导致平台的可移植性差。
而且，本身的健壮性也受到主机操作系统安全性的限制。
HIDS只能检测针对本机的攻击，而不能检测基于网络协议的攻击。
（2）网络入侵检测系统 当入侵检测监视的对象为网络关键路径上的网络数据时，称为网络人侵检测系统（network—based intrusion detection system，NIDS）。
局域网通常采用的都是基于广播机制的以太网协议，以太网协议能够使主机接收同一网段内的所有广播数据。
以太网络适配器有正常和混杂两种工作模式，正常模式只接收本机地址和广播地址的数据，混杂模式则接收本网段内的所有数据。
NIDS正是利用了网络适配器的混杂工作模式来实时采集通过网络的所有数据，通过网络协议解析与模式匹配实现入侵行为检测，主要用于发现试图危害网络基础设施的行为。
相对于HIDS而言，NIDS具有下列优点。
①检测与响应速度快。
NIDS能够在成功入侵之前发现攻击和可疑意图，在攻击目标遭受破坏之前即可执行快速响应中止攻击过程。
而HIDS只有当系统Et志记录人侵行为之后才能开始检测，此时，关键应用服务有可能已经遭到破坏。
②入侵监视范围大。
由于每个网络传感器能够采集共享网段内的所有数据，一个网络传感器就可以保护一个网段。
因此，只在网络关键路径上安装网络传感器，就可以监视整个l网络通信。
③入侵取证可靠。
NIDS通过捕获网络流量收集人侵证据，攻击者无法转移证据。
对HIDS而言，如果攻击者破坏了审计记录和系统日志，就很难获得可靠的入侵证据。
④能够检测协议漏洞攻击。
许多攻击程序是基于网络协议漏洞编写的，诸如同步洪流（SYNflood）、Smurf攻击、泪滴攻击（teardrop）等只有通过查看首部或有效载荷才能识别。

NIDS同样也存在一些缺点，网络传感器只监视网段内的通信，所以在交换以太网环境中监测范围受到限制。
在高速网络流量环境下检测精度下降；不能检测加密数据、隧道数据和加密数据攻击；网络传感器向控制台回传数据量大等。

编辑推荐

<<信息安全技术与应用>>

版权说明