主机入侵监测产品IDS应用示例 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__E4_B8_BB_E6_9C_BA_E5_85_A5_E4_c101_251036.htm 海信数码科技有限公司的主机入侵监测产品IDS 作为网络入侵监测工具，因为IDS对网络的流量有一定的限制，在网络安装过多的IDS时，将会对网络速度有较大的影响，所以根据网络的实际 情况及安全性的要求，我们综合考虑了这两种需求，并做出了以下的布署方案。 在每台需要保护的主机（如WWW服务器）上我们都安装IDS的主机监控系统，IDS可以实时监视各种对主机的访问请求，并及时将信息反馈给IDS服务器，这样全网任何一台主机受到攻击时，系统都可以及时发现，并可将反馈信息及时传送给控制台进行处理，并能自动对入侵事件做出反应。 在需要保护的重点的网段，我们也将安装IDS 的网络监控模块，对这一网段的非正常的访问进行监视，对速度的要求及其它原因的综合考虑，我们建议只在极少数十分重要的网段安装IDS 。 IDS具备如下特点： 精确地判断入侵事件 安装在服务器上的IDS有一个完整的黑客攻击信息库，其中存放着各种黑客攻击行为的特征数据。每当用户对服务器上的数据进行操作时，IDS就将用户的操作与信息库中的数据进行匹配，一旦发现吻合，就认为此项操作为黑客攻击行为。由于信息库的内容会不断升级，因此可以保证新的黑客攻击方法也能被及时发现。IDS的攻击识别率可以达到百分之百。 可判断应用层的入侵事件 与防火墙不同，IDS是通过分析数据包的内容来识别黑客入侵行为的。因此，IDS可以判断出应用层的入侵事件。这样就极大的提高了判别黑客攻击行为

的准确程度。 对入侵可以立即进行反应 IDS以进程的方式运行在服务器上，为系统提供实时的黑客攻击侦测保护。一旦发现黑客攻击行为，IDS可以立即做出相应。响应的方法有多种形式，其中包括：报警（如屏幕显示报警、寻呼机报警）、必要时关闭服务直至切断链路，与此同时，IDS会对攻击的过程进行详细记录，为以后的调查工作提供线索。 全方位的监控与保护 防火墙只能隔离来自本网段以外的攻击行为，而IDS监控的是所有针对服务器的操作，因此它可以识别来自本网段内、其他网段以及外部网络的全部攻击行为。这样就有效的解决了来自防火墙后由于用户误操作或内部人员恶意攻击所带来的安全威胁。 由于IDS对用户操作进行详细记录，系统管理人员可以清楚的了解每个用户访问服务器的意图，及时发现恶意攻击的企图，提前采取必要措施。这一切对于有攻击企图的人无疑也起到了强大的震慑作用。 针对不同操作系统特点 网络上运行着各种应用，服务器的操作系统平台也是多种多样。IDS根据系统平台的不同进行有针对性的检验，从而提高了工作效率，同时也提高了侦测的准确性。 网络系统安装了IDS后，可以有效的解决来自网络安全四个层面上的非法攻击问题，既可以避免来自外部网络的恶意攻击，同时也可以加强内部的安全管理，保证主机资源不受来自内部网络的安全威胁，防范住了防火墙后面的安全漏洞。