安全应用：应用IDS保卫数据库 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/166/2021_2022__E5_AE_89_E5_85_A8_E5_BA_94_E7_c101_166587.htm 目前，针对应用及其后台数据库的应用级入侵已经变得越来越猖獗，如SQL注入、跨站点脚本攻击和未经授权的用户访问等。所有这些入侵都有可能绕过前台安全系统并对数据来源发起攻击。 为了对付这类威胁，新一级别的安全脱颖而出，这就是应用安全。这种安全技术将传统的网络和操作系统级入侵探测系统(IDS)概念应用于数据库(即应用)。与通常的网络或操作系统解决方案不同的是，应用IDS提供主动的、针对SQL的保护和监视，可以保护数以千计的预先包装或自行开发的Web应用。例如，应用IDS可以监视和防护关键的数据，使那些针对数据库的攻击，如缓冲区溢出和Web应用攻击等无法对数据库造成真正的损害，而且应用IDS还可以对这些事件进行审查。 应用安全与网络和主机安全之间存在很大的区别。应用是千差万别的，但攻击的目标总是相同的，也就是入侵数据库。由于应用使用SQL与数据库进行通信，因此好的应用IDS应当能够解析SQL，并且提供一种能够理解流量的内容，且又能与应用划清界线的客观保护层。 多数应用IDS都有三个组件。第一个是基于网络或主机的传感器。网络传感器连接到交换机上的一个端口上，该端口的配置决定它可以查看到数据库内的所有流量。相比之下，主机传感器直接驻留在应用上。传感器可以收集SQL交易并对其进行解析，然后决定是否应当针对该流量发出警报。如果有必要发出警告，警告会被传递给下一个组件，即控制台服务器。这台服务器存储事

件信息，并且是策略配置和升级等传感器维护活动的中心点。应用IDS中的第三个组件是Web浏览器，管理员可以利用它来修改IDS设置、实时监视事件并生成报告。 以SQL注入攻击为例，攻击者会试图绕过Web服务器定义的SQL语句，目的就是要注入自己的语句。假设要输入的用户名为Bob，口令为Hardtoguess。 当看到这些输入的内容后，数据库就会找到WebUsers 行中与之匹配的内容，然后该应用会对用户进行验证。为了入侵数据库，SQL注入攻击会欺骗应用，并使之相信自己已经提交了正确的证书。例如，攻击使用的口令是‘ blah ’或‘ A ’= ‘ A ’，因此攻击时创建的SQL语句可能会是:SELECT * FROM WebUsers WHERE Username= ‘ Bob ’ AND Password= ‘ blah ’ OR ‘ A ’= ‘ A ’。 从逻辑上来分析‘ A ’= ‘ A ’永远都是TRUE，而WHERE子句也可以匹配所有的行，就这样，攻击者在根本没有正确用户名或口令的情况下也能蒙混过关，得到验证。应用服务器会接受输入的信息并且允许攻击者通过。接下来，应用服务器会通过SQL命令从数据库中请求数据。 如果有了应用IDS，传感器会收集SQL命令并对其进行解密，然后查看这些命令到底要访问数据库中的哪些表和列。利用这种方法，传感器就可以判断出到底是正常情况还是一次攻击行为。如果发现的行为是IDS策略不允许的，传感器会判断攻击的威胁水平并采取适当的措施，通常是向管理员的控制台和/或通过电子邮件发出警告。 这只是应用层攻击的一个简单例子，而且今天的许多公司都在面临这样的威胁。通过实施应用级IDS，企业就可以有效地保护易受攻击的数据，并且将最新的攻击和威胁拒之门外。 100Test 下载频道开通，各类考试题目直接下载。详细请访