入侵检测系统分析及其在Linux下的实现（4） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c103_144484.htm 三、实例分析 下面结合入侵检测的实例来介绍该系统是如何检测入侵的，这里以WEB攻击为例来进行介绍。WEB攻击是入侵的一大类，它是指利用CGI、WEB服务器和浏览器等存在的安全漏洞来损害系统安全或导致系统崩溃的一类入侵方式。由于WEB的广泛使用，关于它的各种安全问题不断地发布出来，这些漏洞中的一些漏洞甚至允许攻击者获得系统管理员的权限而进入站点内部。因此，WEB攻击的危害很大。 虽然WEB攻击种类繁多，但是分析一下，还是具有如下几个特点： ● 都是通过HTTP数据流来进行的，所以可以通过HTTP数据流来进行检测。 ● HTTP是无状态的协议，一般都是通过一次请求来实现，或者包含有一次具有典型的入侵特征的请求，所以利用一次请求信息就可以实现检测。 ● 一般都是通过构造别有用心的请求字符串来实现的，所以可以采用基于规则的方法。 在我们的系统中可以检测出100多种WEB攻击方式。例如规则：alert http $EXTERNALNET any -> $HTTPSERVER 80 (content:/maillist.pl. nocase. msg: WEB-CGI Maillist CGI access attempt .) 。该规则规定了检测从外网的任意端口到内网的WEB服务器的80端口的数据流。检测条件为请求中包含“ /maillist.pl ”字符串，匹配不分大小写，告警名称为“ WEB-CGI Maillist CGI access attempt ”。这里利用了两个自定义的变量$EXTERNALNET和$HTTPSERVER，分别表示外网和WEB服务器。 四、结束语 本文在对入侵检测系统进行分

析的基础上，在Linux系统下实现了一个基于网络的入侵检测系统。实践表明，该系统对于检测一些常见的入侵方式具有很好的效率和性能。同时，该系统提供了完整的框架，可以灵活地应用于各种环境并扩充。当然，本系统还有很多不足的地方：数据源比较单一，还应该加入日志数据源；而且现在对于应用层协议只实现了HTTP协议分析，以后还可以加入其他协议分析，如TELNET、FTP等。这些都需要今后进一步完善。未来的入侵检测系统将会结合其它网络管理软件，形成入侵检测、网络管理、网络监控三位一体的工具。同时，网络安全需要纵深的、多层次的防护。即使拥有当前最强大的入侵检测系统，如果不及时修补网络中的安全漏洞的话，安全也无从谈起。只有将入侵检测系统与其他安全工具结合起来，才能构筑起一道网络安全的立体防御体系，最大程度地确保网络系统的安全。