

入侵检测系统分析及其在Linux下的实现（2）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\\_144487.htm](https://www.100test.com/kao_ti2020/144/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c103_144487.htm) 二、Linux下的实现

在对入侵检测技术研究的基础上，我们在Linux系统下设计并实现了一个基于网络的入侵检测系统。2.1 系统的组成结构

该系统的组成结构如图1所示。数据采集模块负责从网络上收集原始的网络数据流，在经过一定的预处理后，这些数据被送到数据分析模块，由数据分析模块进行分析，以便判断是否有违反安全策略的入侵行为发生。并及时将分析结果送到告警模块，由告警模块向控制台产生告警信息。用户可以通过用户界面与控制台交互，通过控制台，一方面可以对各个模块进行配置，另一方面也可以接收告警信息。图1 系统的组成结构

2.2 系统的功能描述 该系统实现了入侵检测的主要功能，包括数据采集、数据预处理、入侵分析以及告警。具体来说，可以完成以下功能：

捕获符合指定条件的网络数据包。 进行IP重组，提供IP包数据。 重组TCP流，提供TCP流数据。 重组应用层数据流，提供HTTP数据流。

实现基于规则的入侵检测方法。 向控制台提交分析结果。

接受控制台的配置和管理。由于该系统功能的实现主要体现在数据采集模块和数据分析模块中，所以下面将对这两个模块加以详细说明。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](http://www.100test.com)