1. 系统需求分析
   1. 需求分析

对于基础的应用代理防火墙，进行审计功能扩展

1.2总体功能要求

实现审计日志功能，并能对于可能出现的部分不安全状态进行报警

1.3运行环境要求

ubuntu-18.10

1. 系统总体架构

2.1 平台架构

网络拓扑结构为

内网主机A

应用代理防火墙

ens38:192.168.33.1

ens33:192.168.1.122

IP:192.168.33.2

gateway:192.168.33.1

Internet

路由器

桥接模式

物理主机

IP:192.168.1.112

如上图所示，虚拟机中的一台作为应用代理防火墙，与物理主机一起连在路由器上再与Internet相连，另一台作为内网主机，直接与应用代理防火墙相连。

（IP仅作示例）

2.2 总体架构

main函数

dealonereq函数：处理代理请求

checkserver函数：检查访问的服务器

audit函数：日志审计

journel函数：

日志数据采集

connectserver函数：

连接服务器，并进行通信

checkclient函数：检查客户端

getHostname函数：

获取服务器信息

1. 系统功能模块1：日志数据采集模块

通过调用syslog系统日志工具，对日志进行采集。

void openlog(char\*ident,int option,int facility);类似于open，打开日志设备，以供读取和写入

void syslog(int priority,char \*format,……);与write类似，写入日志

void closelog();关闭日志设备

在日志中，共性记录以下几个内容：

·被代理主机以及目的服务器IP

·Protocol：即internet服务标识，如ftp，mail，telnet，http等

·ProcessID：dealonereq的线程id

·LogDateTime：日志数据产生日期和时间

1. 系统功能模块2：日志审计

4.1 模块结构

日志分析程序

原始日志

结果日志

4.2 日志分析程序

根据一些标准，如“出现大量超时会话则可能会被恶意占用带宽”，对原始日志中的数据进行匹配判断并给出报警信息。

1. 运行平台

5.1 软件平台

操作系统：Ubuntu18.10

软件环境：gcc

5.2 硬件平台

a.一台安装Ubuntu系统的PC终端

b.Ubuntu系统c语言编译环境

1. 接口设计

./proxy -p 端口号

1. 系统出错处理设计

（错误产生原因、提示信息、建议处理办法）

a.提示Segmentation Fault，程序内存访问错误，建议重启防火墙并更换端口

b.提示Invalid port number, try again.或Usage: %s -p port\n，输入不合法，建议按照提示进行输入