**西安电子科技大学**

**计算机与网络安全综合实验 课程实验报告**

**实验名称 入侵检测系统实验**

网络与信息安全 学院 2118021 班

成 绩

姓名 盖乐 学号 21009200991

同作者

实验日期 2024 年 6 月 6 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# 实验1. 入侵检测系统实验一

## 一、实验目的

## 验证入侵检测系统配置过程。

## 验证入侵检测系统控制信息流传输过程的机制。

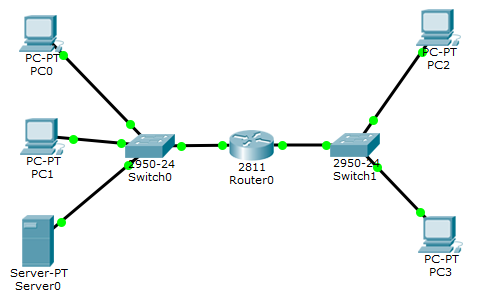
## 验证基于特征库的入侵检测机制的工作过程。

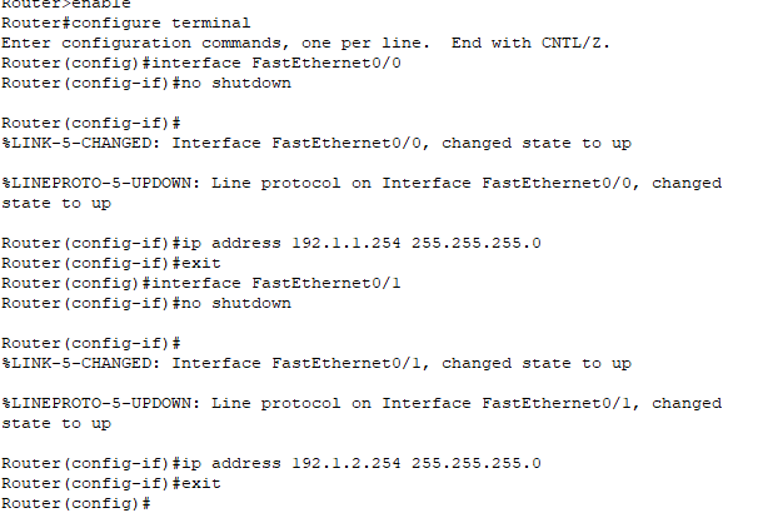
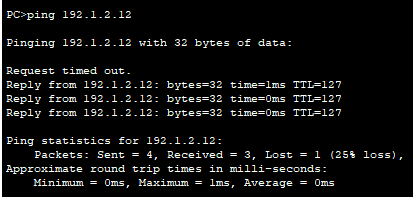
## 二、实验任务

1. 使用自己的语言简述基于特征库的入侵检测机制的工作过程。

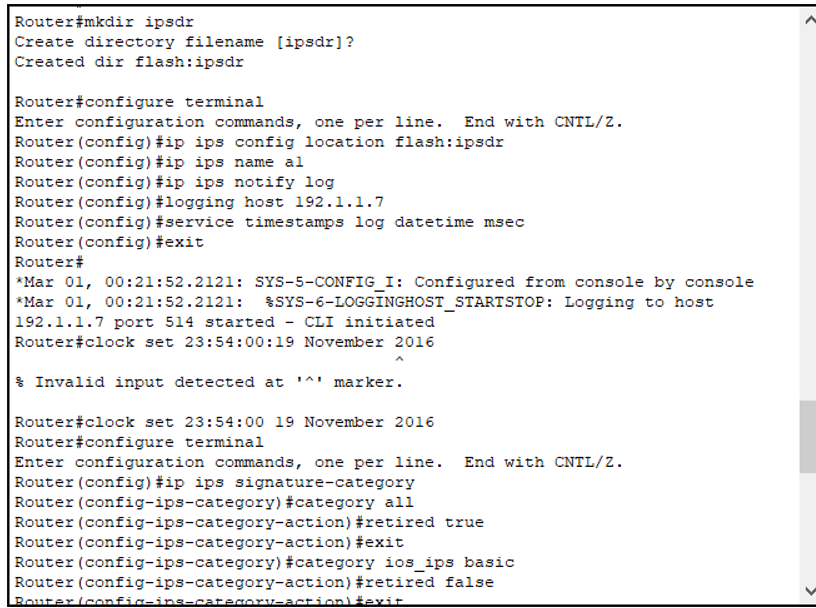
首先需要加载特征库，并且打开路由器端口的特征检测机制，这样当路由器发现符合特征的数据流时，就会采取相关动作。

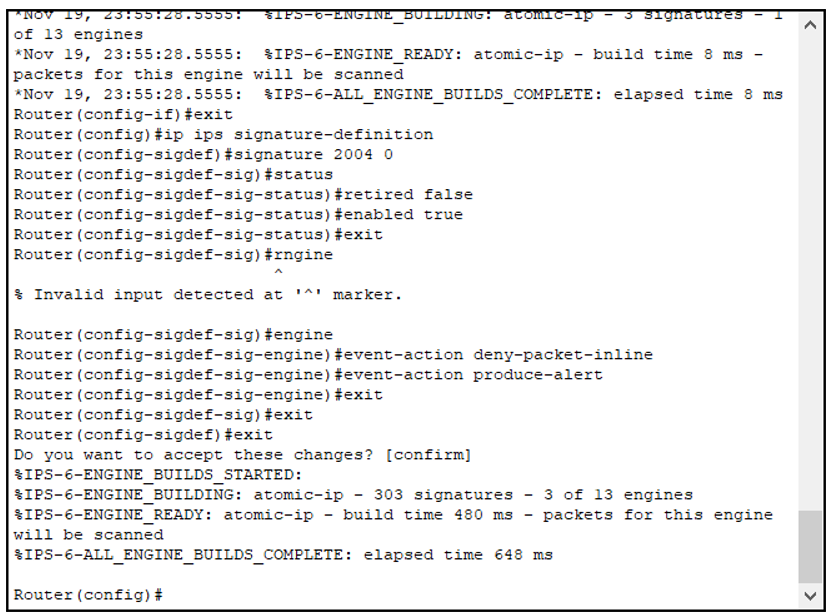
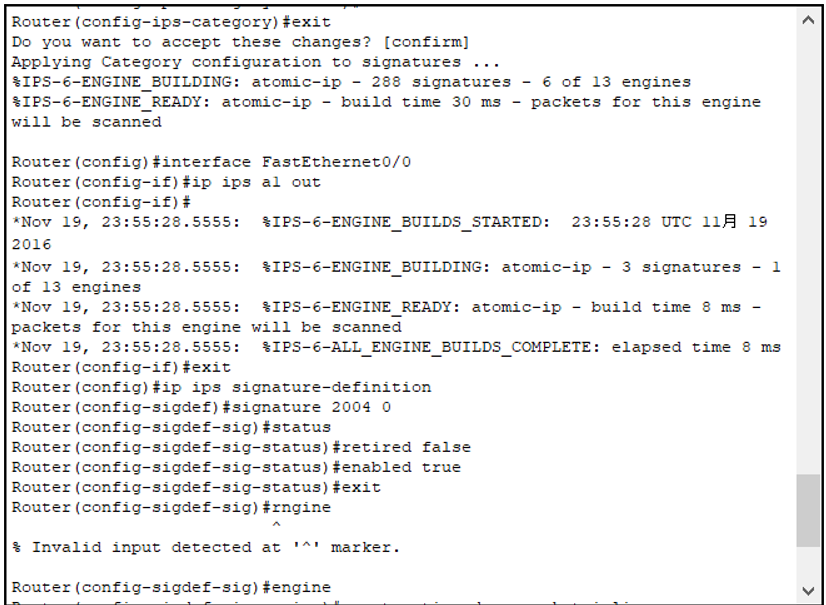
1. 实验步骤
2. 连接网络拓扑并配置路由器，验证终端之间连通性



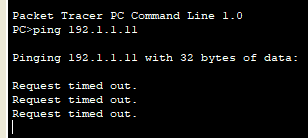


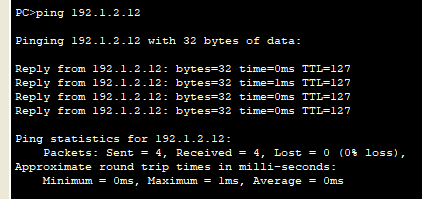
1. 配置路由器的入侵检测功能



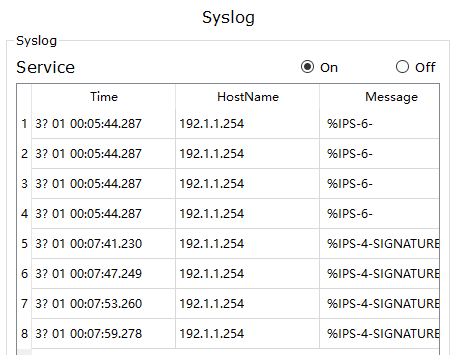


1. 验证PC0和PC2的连通性





PC0能ping通PC2，但PC2不能ping通PC0，并且日志服务器会有记录



## 三、思考与总结

1. 实验过程中你遇到什么问题，如何解决的？通过该实验有何收获？

本次实验学习了配置路由器的入侵检测功能，强化了组网能力，加强了对计算机网络知识的理解。

1. ping是一个双向通信过程，为什么配置入侵检测规则后，PC0可以ping通PC2？

根据IDS的具体机制，通过预设接口的信息流与标识某种入侵行为相关的信息流特征匹配，则对该信息流采取相关的动作，因此PC0可以ping通PC2。

# 实验2. 入侵检测系统实验二

## 一、实验目的

1. 验证对特定信息流实施入侵检测的过程。
2. 验证指定信息流的入侵检测配置过程。

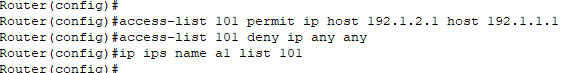
## 二、实验任务

1. 使用自己的语言简述该实验的实验原理。

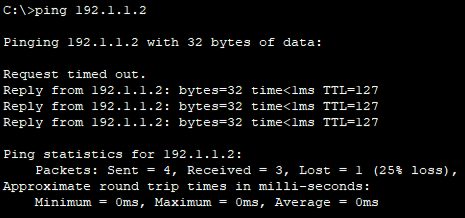
用扩展分组过滤器指定信息流类别，将用户指定信息流类别的扩展分组过滤器与入侵检测规则绑定在一起。

1. 实验步骤

（1）在前一个实验的基础上，相关的命令行接口配置过程如下图。



（2）验证 PC2 不能 ping 通 PC0，但 PC3 可以 ping 通 PC0。进行 PC2 ping PC0 的操作后，日志服务器将记录该事件



## 三、思考与总结

1. 改变命令access-list 101 permit ip host 192.1.2.12 host 192.1.1.10与access-list 101 deny ip any any的顺序会有什么结果？

编号为101的扩展分组过滤器丢弃所有分组，因此不会对任何分组实施入侵检测规则，所以PC2 PC3都可以ping通PC0。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

本次实验学习了设置路由器的入侵检测规则，强化了组网能力，加深了对计算机网络知识的理解。