

2024

计算机与网络安全综合实验

时间：2024年

本次实验任务——入侵检测系统实验

- 入侵检测系统实验一

- 入侵检测系统实验二

- ✓ 入侵检测系统(Intrusion Detection System, IDS)的功能是发现针对网络和主机系统的入侵行为并予以反制。
- ✓ 实现这一功能的步骤包括捕获信息、检测信息、确定入侵行为并予以反制。
- ✓ 根据保护对象不同，可分为主机入侵检测系统和网络入侵检测系统。

本次实验任务——入侵检测系统实验

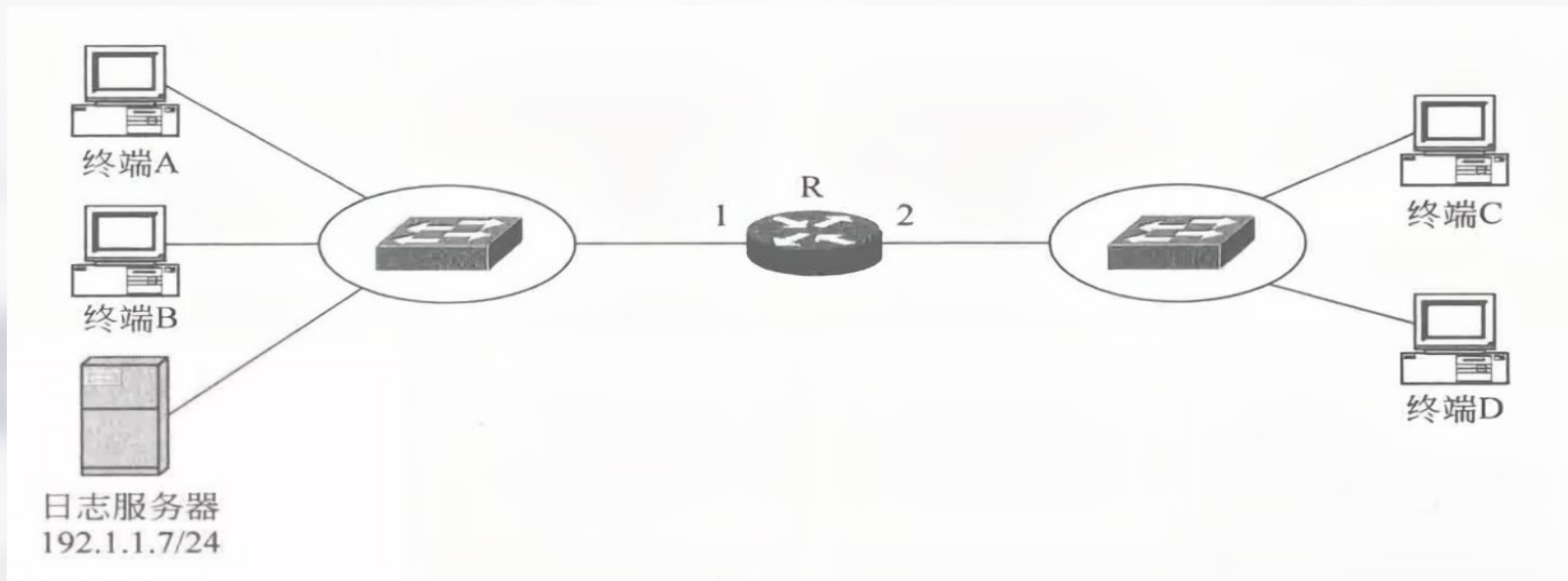
- ✓ 入侵检测系统和防火墙是两种功能不同的安全设备。
 - 防火墙的作用是控制网络间信息传输过程。
 - 入侵检测系统的作用是在网络传输的信息流中，或者输入输出主机系统的信息流中检测出用于实施入侵的异常信息，并对异常信息予以反制。
- ✓ 入侵检测系统可以分为两大类，分别是主机入侵检测系统和网络入侵检测系统。
 - 主机入侵检测系统主要用于检测到达某台主机的信息流、监测对主机资源的访问操作。
 - 网络入侵检测系统主要用于检测流经某段关键链路的信息流。

本次实验任务——入侵检测系统实验

- 路由器通过加载特征库对信息流实施入侵检测。
- 如需对指定信息流实施入侵检测，可以通过建立扩展分组过滤器与入侵检测规则之间的绑定达到这一目的。

入侵检测系统实验一

- 互连网结构如图，完成路由器R的接口和终端的网络信息配置过程后，各终端之间可以相互ping通。

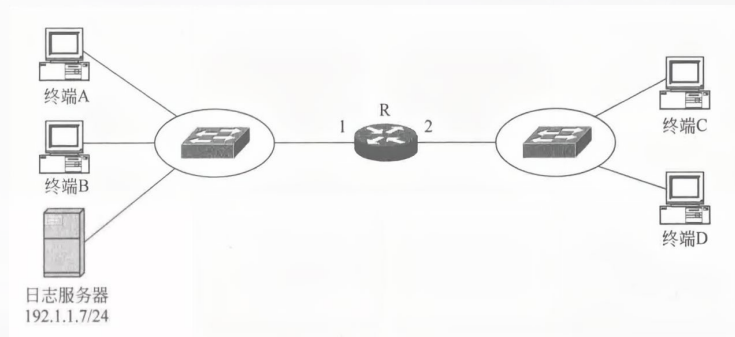


入侵检测系统实验一

- 在路由器R接口1输出方向设置**入侵检测规则**，要求：一旦检测到ICMP

ECHO请求报文，则丢弃该报文，并向日志服务器发送警告信息。

- 启动该入侵检测规则后，如果终端C和D发起ping终端A和B的操作，则ping操作不仅无法完成，而且会在日志服务器中记录警告信息。
- 如果终端A和B发起ping终端C和D的操作，则ping操作依然能够完成。



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。

实验原理

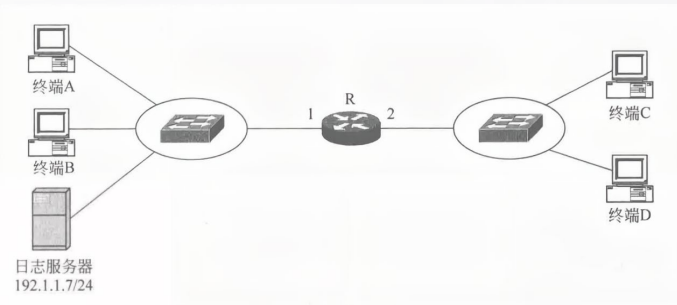
- Cisco集成在路由器中的入侵检测系统采用基于特征的入侵检测机制。
 - 首先需要加载特征库，特征库中包含用于标识各种入侵行为的信息流特征。
 - 一旦在某个路由器接口的输入或输出方向设置入侵监测机制，则需要采集通过该接口输入或输出的信息流，然后与加载的特征库中的特征进行比较。
 - 如果该信息流与标识某种入侵行为相关的信息流特征匹配，则对该信息流采取相关的动作。
- 特征库中与每一种入侵行为相关的信息有两部分
 - 一是标识入侵行为的信息流特征；
 - 二是对具有入侵行为特征的信息流所采取的动作。

入侵检测系统实验二

- 在路由器R接口1输出方向设置**入侵检测规则**。要求：一旦检测到终端C

发送给终端A的ICMP ECHO请求报文，则丢弃该报文并向日志服务器发送警告信息。

- 启动该入侵检测规则后，如果终端C发起ping终端A的操作，则ping操作不仅无法完成，而且会在日志服务器中记录警告信息。
- 其他终端之间的ping操作依然能够完成。

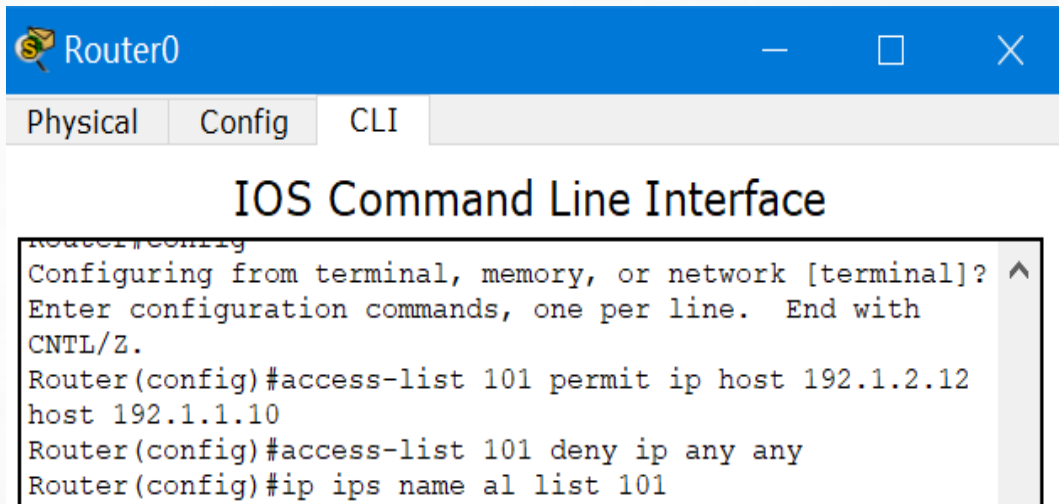


实验目的

- 验证对特定信息流实施入侵检测的过程。
- 验证指定信息流的入侵检测规则配置过程。

实验原理

- 用扩展分组过滤器指定信息流类别，将用于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。



The screenshot shows a window titled "Router0" with three tabs: "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The command prompt is "Router#config". The user enters "Configuring from terminal, memory, or network [terminal]?", followed by "Enter configuration commands, one per line. End with CNTL/Z.". The user then enters "Router(config)#access-list 101 permit ip host 192.1.2.12 host 192.1.1.10", "Router(config)#access-list 101 deny ip any any", and finally "Router(config)#ip ips name a1 list 101".

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#access-list 101 permit ip host 192.1.2.12
host 192.1.1.10
Router(config)#access-list 101 deny ip any any
Router(config)#ip ips name a1 list 101
```

- 编号为101的扩展分组过滤器允许继续传输的IP分组是源IP地址是PC2的IP地址192.1.2.12，目的IP地址是PC0的IP地址192.1.1.10的IP分组。
- 指定名字为a1的入侵检测规则时，绑定编号为101的扩展分组过滤器，这表示只对编号为101的扩展分组过滤器允许继续传输的IP分组实施名为a1的入侵检测规则，则只对PC2发送给PC0的IP分组实施名为a1的入侵检测规则。