

YOUR LOGO

网络监听工具使用：

Sniffer技术详解

▶▶▶ 2024 ◀◀◀

主讲人：郑冬贤

时间：2024

目录

C A T A L O G U E

1. Sniffer工具概述

2. Sniffer工具的使用方法

3. Sniffer工具的高级应用

4. Sniffer工具的安全与法律问题

YOUR LOGO

Part 01

Sniffer工具概述

Sniffer定义与功能

Sniffer基本概念

Sniffer（嗅探器）是一种网络分析工具，用于捕获和分析网络上流动的数据包，广泛应用于网络监控、故障排查和安全审计。

Sniffer工具通过捕获网络接口的数据包，为网络工程师提供透明的数据传输内容，帮助识别和修复网络问题。

Sniffer工作原理

网络数据包捕获机制

Sniffer工具通过将网卡设置为混杂模式，监听经过网络接口的所有数据包，读取并存储数据包内容，按协议类型进行解析和展示。

Sniffer使用场景



网络安全与性能监控

Sniffer工具在网络安全中用于流量监控、异常检测、攻击防护以及网络性能评估，确保网络环境的健康和安全。

YOUR LOGO

Part 02

Sniffer工具的使用方法

选择网络适配器



适配器选择的重要性

使用Sniffer前需选择合适的网络适配器，确保捕获的数据包来自正确的网络接口，对于分析网络流量至关重要。

设置捕获过滤器



过滤器的应用

设置过滤器可以减少不必要的数据量，提高分析效率，如使用TCP端口过滤器只捕获HTTP相关的数据包。

开始捕获数据包

数据包捕获过程

点击Sniffer软件界面上的“开始捕获”按钮，Sniffer将监视选定的适配器，并显示捕获到的数据包。



YOUR LOGO

Part 03

Sniffer工具的高级应用

协议分析与数据包解码



数据包结构解析

Sniffer工具可以解析数据包的头部字段和负载内容，提供协议级别的详细信息，如HTTP请求和响应信息。



数据流与会话跟踪

01

会话跟踪功能

Sniffer工具通过跟踪和记录每个会话的数据流，使得用户可以直观地查看数据包在不同时间点的状态。

法律取证中的应用

合法性与有效性

Linux sniffer在法律取证中合法且有效，可以捕获和分析网络流量，帮助取证人员获取关键的网络通信数据。

YOUR LOGO

Part 04

Sniffer工具的安全与法律 问题

遵守法律法规

合法授权的必要性

在使用Sniffer进行网络监听时，必须确保有合法的授权，如法院命令或搜查令，以避免违法行为。



保护用户隐私



数据处理的规范性

破解得到的敏感信息属于隐私数据，需要妥善保管，防止泄露，仅用于合法的安全测试和修复漏洞。

YOUR LOGO

谢谢大家

▶▶▶ 2024 ◀◀◀

主讲人：郑冬贤

时间：2024