kali linux渗透测试

第31课 使用TcpDump分析网络流量

TcpDump简介

TcpDump是一款资深网络工作人员必备的工具。

TcpDump是一款小巧的纯命令行工具，正是由于它的体积小巧，所以这款工具可以完美的运行在大多数路由器，防火墙以及Linux系统中。而且TcpDump现在有了Windows版本。

TcpDump使用

抓包命令

```
1 tcpdump -v -i eth0
```

参数解读:

-i 用来指定要监听的网卡

-v 表示以verbose mode显示

CTRL+C 结束监听

将监听到的数据保存下来

```
1 tcpdump -v -i eth0 -w cap-20190907.pcap
```

pcap文件可以用 wireshark 查看

-w 表示要将捕获到的数据保存下来，后面的文件名就是要保存到哪里

谢谢观赏