CTF misc wireshark初步

转载

H4ppyD0g 于 2019-09-12 22:05:26 发布 1006 收藏 5

分类专栏： CTF

原文链接：https://www.cnblogs.com/littlek1d/p/9348502.html

wireshark是网络封包分析软件，可以截取各种网络封包，显示网络封包的详细信息。

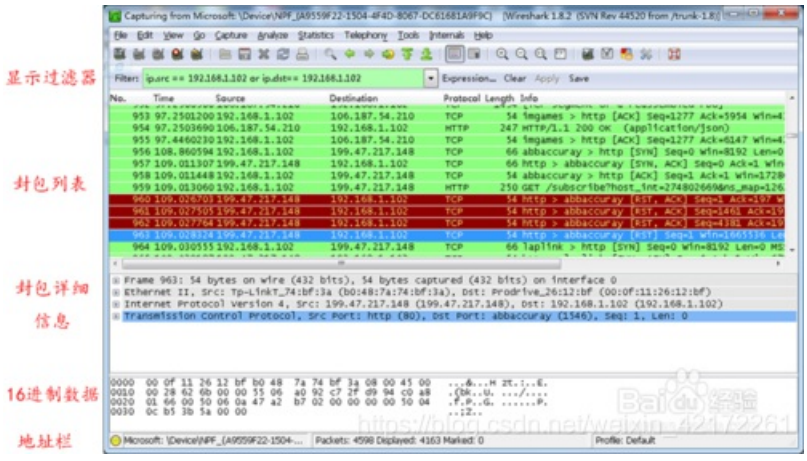
为了安全考虑，wireshark只能查看封包，而**不能修改**封包的内容，**或者发送**封包。

wireshark能获取HTTP，也能获取HTTPS，但是**不能解密HTTPS**，所以wireshark看不懂HTTPS中的内容。

---

wireshark是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你需要选择一个网卡。

Wireshark 窗口介绍



WireShark 主要分为这几个界面

Display Filter(显示过滤器)， 用于过滤

Packet List Pane(封包列表)， 显示捕获到的封包， 有源地址和目标地址，端口号。 颜色不同，代表

Packet Details Pane(封包详细信息), 显示封包中的字段

Dissector Pane(16进制数据)

Miscellanous(地址栏，杂项)

过滤表达式的规则

协议过滤
比如TCP：只显示TCP协议。

IP 过滤
比如 ip.src == 192.168.1.102 ：显示源地址为192.168.1.102，
ip.dst==192.168.1.102,：目标地址为192.168.1.102

端口过滤
tcp.port == 80, ：端口为80的
tcp.srcport == 80：只显示TCP协议的源端口为80的。

http模式过滤
http.request.method==“GET”： 只显示HTTP GET方法的。

逻辑运算符为 AND/ OR

封包详细信息 (Packet Details Pane)

Frame: **物理层**的数据帧概况

Ethernet II: **数据链路层**以太网帧头部信息

Internet Protocol Version 4: **网络层**IP包头部信息

Transmission Control Protocol: **传输层**的数据段头部信息

Hypertext Transfer Protocol: **应用层**的信息

比较重要的信息：源IP， 目的IP， 源端口， 目的端口，协议