8 数据包分析

1)应急响应

2)工作中可能有一些问题

3)HTTP TCP ARP ICMP,DOS ARP 断网 木马蠕虫 加密包

8.1 工具

科来中文版、Wireshark、各种 sniffer(cain)

8.2 基本命令

1)基本用法

显示过滤器比较运算符：通过扩展过滤条件可查找某一域值，Wireshark 针对此功能支持数字比较运算符。

1. ==或 eg

例如：ip.src==10.2.2.2

显示所有源地址为 10.2.2.2 的 IPv4 数据流

2.!=或 ne

例如：tcp.srcport!=80

显示源端口除了 80 以外的所有 TCP 数据流

3.>或 gt

例如：frame.time relative>1 显示距前一个报文到达时间相差 1 秒的报文

4. <或 lt

例如：tcp.window size<1460 显示当 TCP 接收窗口小于 1460 字节时的报文

5.>=或 ge

例如：dns:count.answers>=10

显示包含 10 个以上 answer 的 DNS 响应报文

6.<=或 le

例如：ip.地<=10

显示 IP 报文中 Time to Live 字段小于等于 10 的报文

7.contains

例如：http contains “GET”

显示所有 HTTP 客户端发送给 HTTP 服务器的 GET 请求

对于基于 TCP 应用的过滤条件采用比较运算符。例如，如果想看端口 80 上面的 HTTP 数据流，使用 HTTP.port==80。

小贴士：

运算符两边不用留空格。i

p.src =10.2.2.2 与 ip.Src==10.2.2.2 的效果是相同的

8.3 案例分析

详见文档

2.2 技术参考文档

1)小包，数据包小于 64 字节，或者几个字节，如果多，说明可能攻击，或者网络异常

2)整数倍，32 48 96,木马或者蠕虫，病毒

3)网段堵塞，某一协议数据包特别大，不断单击。打开，最终会发现是哪一个 XIP(http ARP【最多】 TCP)