



willingtolove

一念成了佛，一念成了魔~

博客园

首页

新随笔

联系

订阅

管理

随笔 - 147 文章 - 0 评论 - 90 阅读 - 207万

昵称： willingtolove  
园龄： 7年9个月  
粉丝： 78  
关注： 32  
+加关注

搜索

找找看

积分与排名

积分 - 332860

排名 - 2287

随笔分类

【 C# 相关】 (27)

【 Java 相关】 (1)

【 JS 相关】 (20)

【 SQL 相关】 (13)

【 SqlServer 相关】 (18)

【 开发工具 相关】 (14)

【 .Net Core 相关】 (7)

【 .NET 相关】 (40)

【 Bootstrap 相关】 (1)

【 Git 相关】 (6)

【 Html 相关】 (2)

【 IDE工具 相关】 (4)

【 jQuery 相关】 (4)

【 JS插件】 (1)

【 Linux】 (2)

更多

随笔档案

2020年10月(1)

Wireshark过滤器写法总结

目录

- #Wireshark提供了两种过滤器：
  - 1、捕获过滤器
  - 2、显示过滤器
- #过滤器具体写法
  - #显示过滤器写法
    - 1、过滤值比较符号及表达式之间的组合
    - 2、针对ip的过滤
    - 3、针对协议的过滤
    - 4、针对端口的过滤（视传输协议而定）
    - 5、针对长度和内容的过滤
    - 5、针对http请求的一些过滤实例。
  - #捕捉过滤器写法
    - 1、比较符号
    - 2、常用表达式实例

#Wireshark提供了两种过滤器：

[回到顶部](#)

1、捕获过滤器

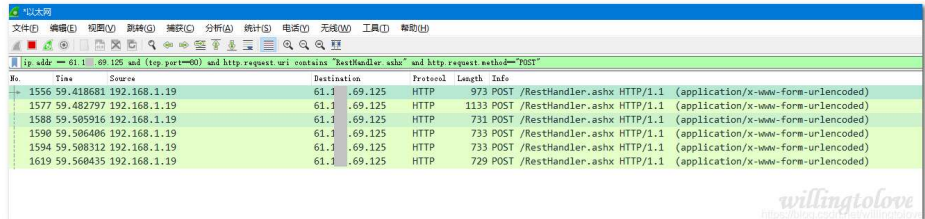
捕获过滤器：在抓包之前就设定好过滤条件，然后只抓取符合条件的数据包。



[回到顶部](#)

2、显示过滤器

显示过滤器：在已捕获的数据包集合中设置过滤条件，隐藏不想显示的数据包，只显示符合条件的数据包。



注意：这两种过滤器所使用的语法是完全不同的，想想也知道，捕捉网卡数据的其实并不是Wireshark,而是WinPcap,当然要按WinPcap的规则来，显示过滤器就是Wireshark对已捕捉的数据进行筛选。

使用捕获过滤器的主要原因就是性能。如果你知道并不需要分析某个类型的流量，那么可以简单地使用捕获过滤器过滤掉它，从而节省那些会被用来捕获这些数据包的处理器的资源。当处理大量数据的时候，使用捕获过滤器是相当好用的。

Wireshark拦截通过网卡访问的所有数据，前提是没有设置任何代理。  
Wireshark不能拦截本地回环访问的请求，即127.0.0.1或者localhost。

#过滤器具体写法

[回到顶部](#)

#显示过滤器写法

1、过滤值比较符号及表达式之间的组合

过滤值比较符号

英文	符号	描述及示例
eq	==	等于. ip.src==10.0.0.5
ne	!=	不等于. ip.src!=10.0.0.5
gt	>	大于. frame.len > 10
lt	<	小于. frame.len < 128
ge	>=	大于等于. frame.len ge 0x100
le	<=	小于等于. frame.len le 0x20
contains		包含. sip.To contains "a1762"
matches	~	正则匹配.host matches "acme\.(org com net)"
bitwise_and	&	位与操作. tcp.flags & 0x02

willingtolove  
<https://blog.csdn.net/willingtolove>

多个表达式间的组合

英文	符号	意义及示例
and	&&	AND 逻辑与. ip.src==10.0.0.5 and tcp.flags.fin
or		OR 逻辑或. ip.src==10.0.0.5 or ip.src==192.1.1.1
xor	^^	XOR 逻辑异或. tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29
not	!	NOT 逻辑非. not llc
[...]		见 Slice 切片操作符.
in		见集合操作符.

willingtolove  
<https://blog.csdn.net/willingtolove>

2、针对ip的过滤

- 对源地址进行过滤

ip.src == 192.168.0.1

- 对目的地址进行过滤

ip.dst == 192.168.0.1

- 对源地址或者目的地址进行过滤

ip.addr == 192.168.0.1

- 如果想排除以上的数据包，只需要将其用括号囊括，然后使用 "!" 即可

!(ip.addr == 192.168.0.1)

3、针对协议的过滤

- 获某种协议的数据包，表达式很简单仅仅需要把协议的名字输入即可

5

0

阅读排行榜

- 【JS】JS数组添加元素的三种方法(271494)
- 【SQL】sql update 多表关联更新方法总结(162054)
- js中Date与timestamp（时间戳）的相互转换(128901)
- 【.net】未在本地计算机上注册“microsoft.ACE.oledb.12.0”提供程序解决办法(124647)
- 【C#】C#获取文件夹下的所有文件(120320)

评论排行榜

- 【C#】判断字符串中是否包含指定字符串,contains与indexof方法效率问题(18)
- .Net防sql注入的方法总结(6)
- C#实现在foreach遍历中删除集合中的元素(方法总结)(5)
- 【SQL】sql update 多表关联更新方法总结(5)
- 【.net】未在本地计算机上注册“microsoft.ACE.oledb.12.0”提供程序解决办法(5)

推荐排行榜

- 1. 【SQL】ROW\_NUMBER() OVER(partition by 分组列 order by 排序列)用法详解+经典实例(16)
- 2. 【C#】C#获取文件夹下的所有文件(15)
- 3. 【SQL】sql update 多表关联更新方法总结(14)
- 4. 【C#】判断字符串中是否包含指定字符串,contains与indexof方法效率问题(13)
- 5. 【JS】JS数组添加元素的三种方法(9)

最新评论

1. Re:img标签的onerror事件

当我把 onerror改成了 onError后,才正常运行。

--ping4
2. Re:img标签的onerror事件

666, 我想提醒一下我复制代码出错了。

--ping4
3. Re:【Sql Server】SQL SERVER 递归查询

感谢

--lanboss
4. Re:【SQL】sql update 多表关联更新方法总结

第四种方法很OK, 简单直观~!

--多来哈米
5. Re:【SQL】sql update 多表关联更新方法总结

感谢!

--熬夜点ICU

http

注意：是否区分大小写？答：区分，只能为小写

- 捕获多种协议的数据包

http or telnet

- 排除某种协议的数据包

not arp 或者 !tcp

4、针对端口的过滤（视传输协议而定）

- 捕获某一端口的数据包（以tcp协议为例）

tcp.port == 80

- 捕获多端口的数据包，可以使用and来连接，下面是捕获高于某端口的表达式（以udp协议为例）

udp.port >= 2048

5、针对长度和内容的过滤

- 针对长度的过滤（这里的长度指定的是数据段的长度）

udp.length < 20  
http.content\_length <=30

- 针对uri 内容的过滤

http.request.uri matches "user" （请求的uri中包含"user"关键字的）

注意： matches 后的关键字是 不区分大小写 的！

http.request.uri contains "User" （请求的uri中包含"user"关键字的）

注意： contains 后的关键字是 区分大小写 的！

5、针对http请求的一些过滤实例。

- 过滤出请求地址中包含 "user" 的请求，不包括域名；

http.request.uri contains "User"

- 精确过滤域名

http.host==baidu.com

- 模糊过滤域名

http.host contains "baidu"

- 过滤请求的content\_type类型

http.content\_type =="text/html"

- 过滤http请求方法

http.request.method=="POST"

- 过滤tcp端口

tcp.port==80

5

0

```
http && tcp.port==80 or tcp.port==5566
```

- 过滤http响应状态码

```
http.response.code==302
```

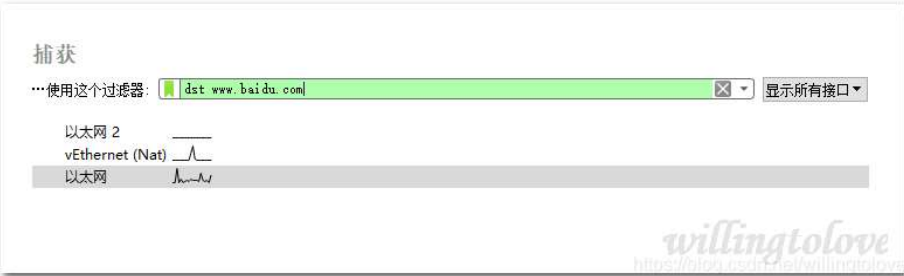
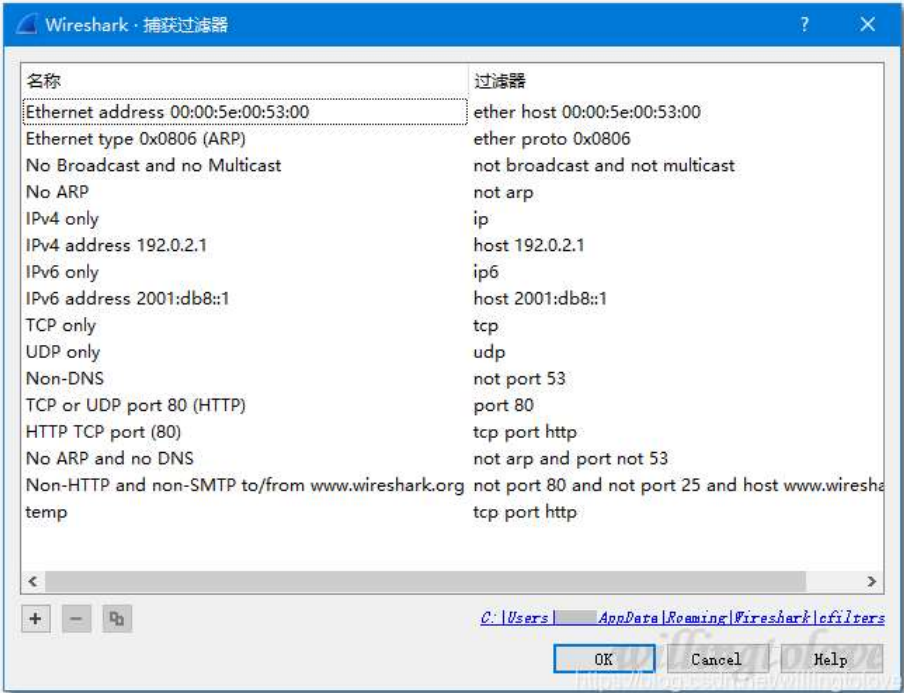
- 过滤含有指定cookie的http数据包

```
http.cookie contains "userid"
```

[回到顶部](#)

#捕捉过滤器写法

在wireshark的工具栏中点击 **捕获** → **捕获过滤器** ，可以看到一些过滤器的写法，如下图：



1、比较符号

与: &&或者and  
或: ||或者or  
非: ! 或者not

实例:

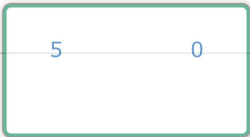
```
src or dst portrange 6000-8000 && tcp or ip6
```

2、常用表达式实例

- 源地址过滤

```
src www.baidu.com
```

- 目的地址过滤



dst www.baidu.com

• 目的地址端口过滤

dst post 80

• 协议过滤

udp

作者: willingtolove

出处: <http://www.cnblogs.com/willingtolove/>

本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。

分类: [【抓包工具 相关】](#)

好文要顶

关注我

收藏该文

willingtolove

粉丝 - 78 关注 - 32

[+加关注](#)

« 上一篇: [ASP.NET Core中添加MIME 类型](#)

» 下一篇: [.net intallutil.exe 安装服务报错: 未能加载文件或程序集 \(异常来自 HRESULT:0x80131515\)](#)

posted @ 2020-03-18 19:13 willingtolove 阅读(13161) 评论(1) 编辑 收藏 举报

[刷新评论](#) [刷新页面](#) [返回顶部](#)

登录后才能查看或发表评论，立即 [登录](#) 或者 [逛逛](#) 博客园首页

【推荐】阿里云金秋云创季，云服务器2核2G低至49.68元/年  
【推荐】腾讯云11.11云上盛惠，云服务器2核2G低至50元/1年

编辑推荐:

- 现代 CSS 指南 -- at-rule 规则扫盲
- 如何在 .NET 程序崩溃时自动创建 Dump?
- .NET 零开销抽象指南
- .Net Core & RabbitMQ 限制循环消费
- .NET API 接口数据传输加密最佳实践

阅读排行:

- 还在用双层for循环吗? 太慢了
- 看了同事这10个IDEA神级插件，我也悄悄安装了
- 来啦来啦 | 开源 \* 安全 \* 赋能 - .NET Conf China 2022
- C# 9.0 添加和增强的功能【基础篇】
- 快速创建软件安装包-ClickOnce

历史上的今天:

2019-03-18 【JS】JavaScript 指定日期增加天数