如何用好wireshark————规则过滤

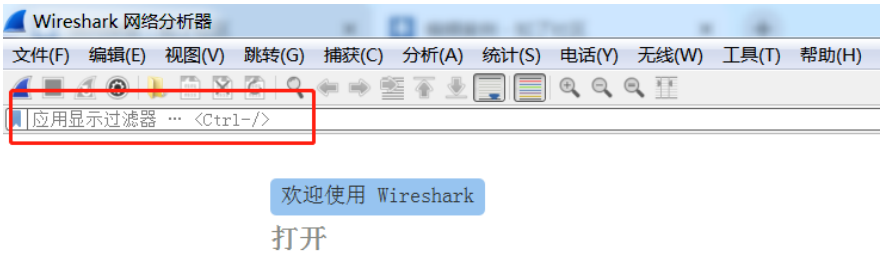
设备管理 朱恺 2020-02-26 发表

问题描述

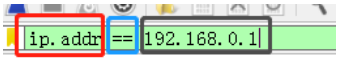
wireshark是我们网络技术工程师常用的分析工具，俗话说：工欲善其事，必先利其器。wireshark这把利器使用的好坏决定了你对问题处理的效率和理解。在我的个人经验来看我的很多技术的理解是建立在这个工具的使用逐渐灵活的基础上的，甚至能帮助你进行举一反三自行突破未知领域的知识。但是软件都是人写的，wireshark也不例外，有一些误导性的提示往往会引导你往错误的方向驱使，谜底就在手边却不得而见。
这里就将写一些自己琢磨的wireshark使用小技巧分享给各位网工同学。
wireshark如何进行规则过滤?

解决方法

一旦打开wireshark主要的显示窗口中就已经体现了过滤器的存在：

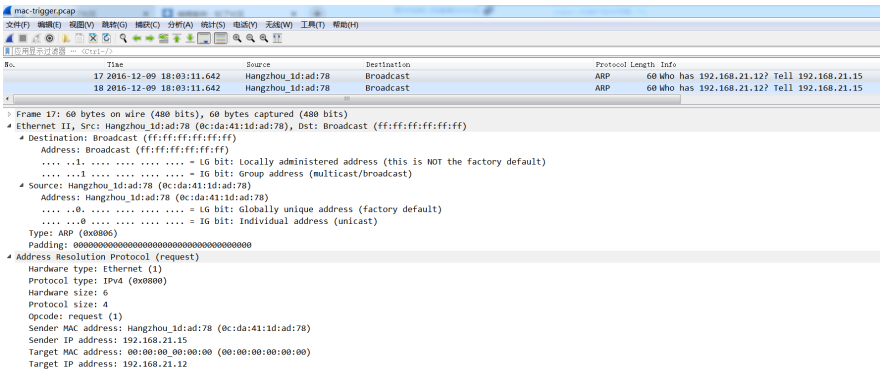


往里输入 过滤规则然后就能在默认网卡上抓取你感兴趣的报文，比如“ip”，“bootp”，在输入的时候随着字符的变化过滤规则会有一些颜色的变化，比如绿色代表输入正确可以过滤，显示红色代表输入错误无法匹配过滤语句，显示黄色我的理解可能是不够完整。
无论抓取还是分析报文我们大部分第一步都是会在过滤器中输入自己第一步想要筛选的感兴趣报文进行解读，过滤语句又分“逻辑判断”、“协议名称”“具体输入值”这三个部分，比如输入ip.addr==192.168.0.1：

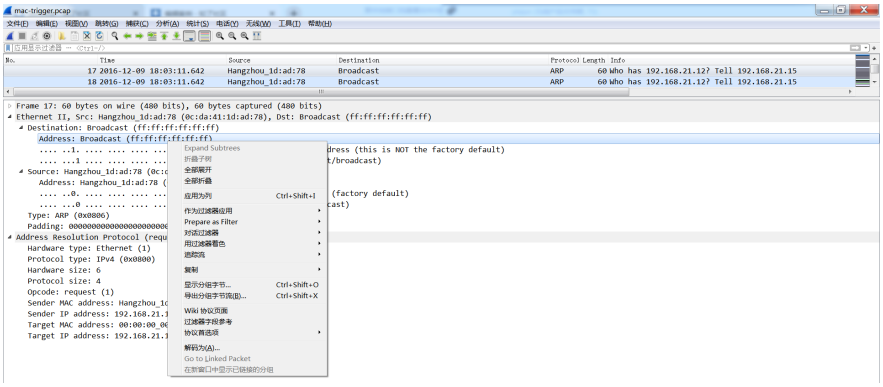


这代表了什么？ 代表一个ip地址（ip.addr）等于（==）192.168.0.1 这样过滤器就会在原始报文中进行查找凡是符合这个条件的就会按照既定顺序进行排列显示。
逻辑判断符号有：==（等于）、&&（与）、||（或）、！（非） 很好理解吧。
有同学就问了：哎呀，那我怎么才能知道协议名称呢？我需不需要熟读协议？
非也，熟读死记显然不适用于当代青年人。学会如何去找到协议名称这个至关重要。

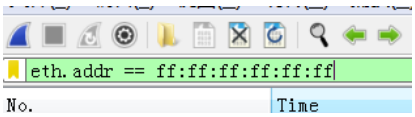
我们可以在报文的详细内容中找到答案：



wireshark本身默认的协议插件就提供了逐层分析知名协议的功能，我们不过滤找到一个报文，发现是个ARP协议的，将报文内容逐层打开，你会发现每行内容都写的满满当当。这个时候协议名称如何选取的条件就展现在我们眼前了。你在任意一行右击鼠标，显示出来的可选择条目中选择作为过滤器应用，或者准备作为过滤器。



这时你会发现过滤器中已经输入了这一行代表的参数含义了，显示为：
eth.addr==ff：ff：ff：ff：ff：ff



代表mac地址为全F的报文：广播报文
按照这种方法我们就能知道如何在wireshark中写mac地址的表达方式：eth.addr。至于后面的赋值，是全F还是固定参数 就看你分析的需要了。

按照这样的方法，即使你不熟悉wireshark中如何拼写过滤语句 你也一样能分析报文，只需要翻看报文的详细内容稍微懂点英文就可以搞定了，简单又有趣。这样的操作多了之后能飞速的提升你的报文结构的理解和举一反三的能力。
怎么样？还不快去试试吗？