

知 wireshark合并防火墙抓包文件使用技巧















其他 孙兆强 2021-05-29 发表

组网及说明

不涉及

问题描述

我们用防火墙的web界面抓包的时候，因为防火墙对每个抓包文件的大小有限制，所以会抓出来很多的抓包文件，一个个看很浪费时间。利用wireshark将多个抓包文件合并为一个文件可大大节省时间。

名称	修改日期	类型	大小
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	72 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	81 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	63 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	61 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	55 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	73 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	94 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	81 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	85 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	83 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	76 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	60 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	64 KB
 pcap_node8_context1_20210426135...	2021/4/26 13:57	Wireshark captu...	69 KB

过程分析

不涉及

解决方法

将所有的抓包文件放入桌面的名字为“抓包”的文件夹。

Win+R输入cmd打开电脑cmd

```
cd C:\Program Files\Wireshark //根据自己的安装路径来修改
```

```
mergcap.exe -w C:\Users\s11757\Desktop\all.pcap C:\Users\s11757\Desktop\抓包\*
```

*表示文件夹内所有

all.pcap为生成的整合的文件名

C:\Users\s11757\Desktop\抓包* //表示源文件路径

C:\Users\s11757\Desktop\all.pcap //表示目标文件路径及文件名

```
C:\Users\s11757>cd C:\Program Files\Wireshark
C:\Program Files\Wireshark>mergcap.exe -w C:\Users\s11757\Desktop\all.pcap C:\Users\s11757\Desktop\抓包\*
C:\Program Files\Wireshark>
```

