# 攻防世界misc——就在其中

原创

Captain杰派罗 于 2021-10-03 19:09:06 发布 2014 收藏 1

分类专栏： 攻防世界WP 文章标签： 网络安全



本文链接：https://blog.csdn.net/weixin_45770420/article/details/120597331

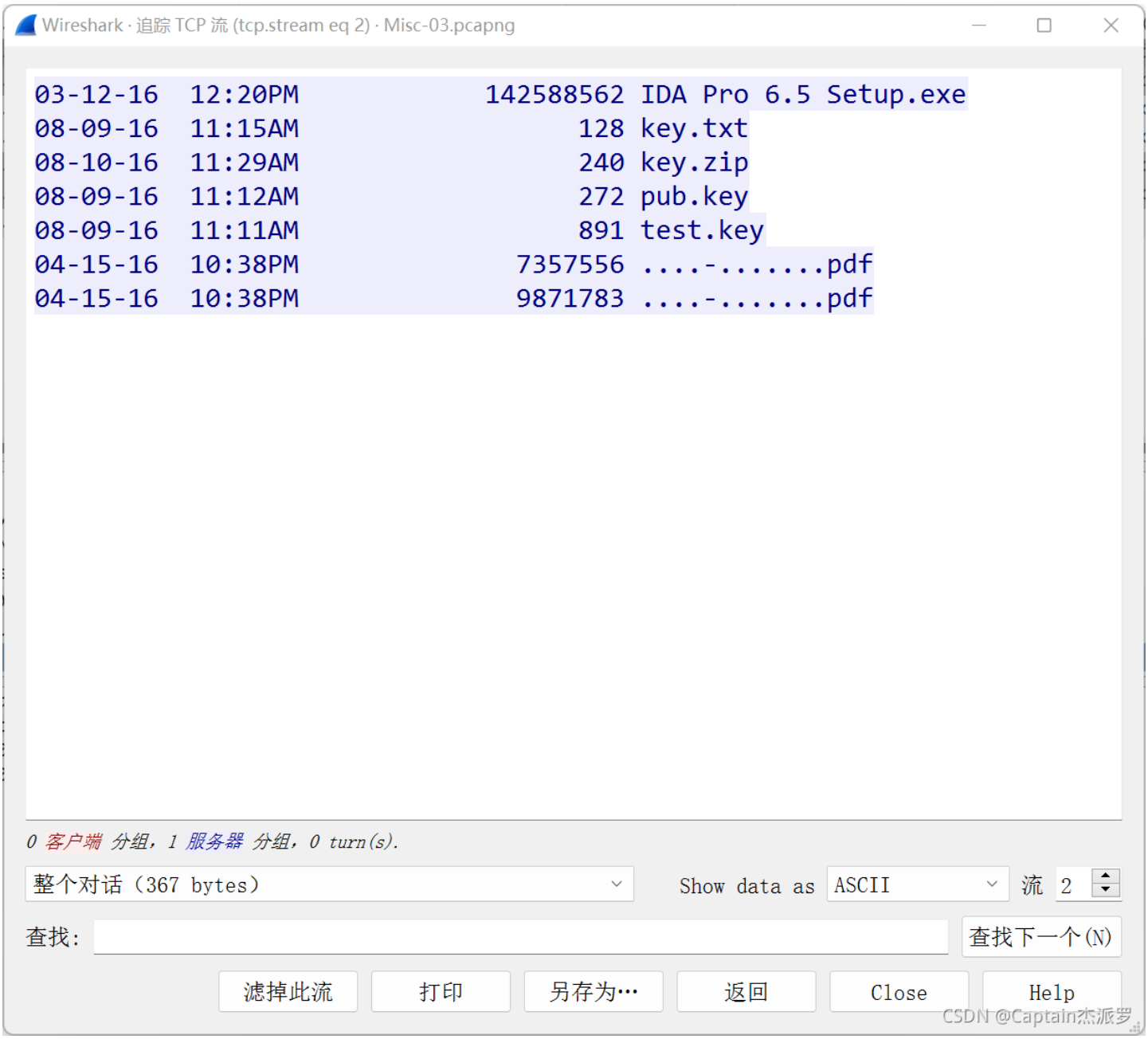


攻防世界WP 专栏收录该内容

32 篇文章 0 订阅

订阅专栏

解压文件，得到wireshark工程文件，打开，发现传输协议以TCP和FTP为主，直接从tcp.stream eq 0 开始追踪TCP流，寻找有效信息，在tcp.stream eq 2发现线索




似乎是有东西被加密了，继续追踪流，tcp.stream eq 14 处发现公钥

Wireshark · 追踪 TCP 流 (tcp.stream eq 14) · Misc-03.pcapng

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj
0u8yMWH4Qi+xTbjHgbE7wOukOaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBB
d85B/LTc36XZ7JVfX5kGy5tIR3tquuPIVKNdAsHlSqh9S7YSS39RdnSa5rOUyGhr
LzxwzzM9IO4e+QQ+CQIDAQAB
-----END PUBLIC KEY-----
```

0 客户端 分组，1 服务器 分组，0 turn(s).

整个对话（272 bytes） Show data as ASCII 流 14

查找: 查找下一个(N)

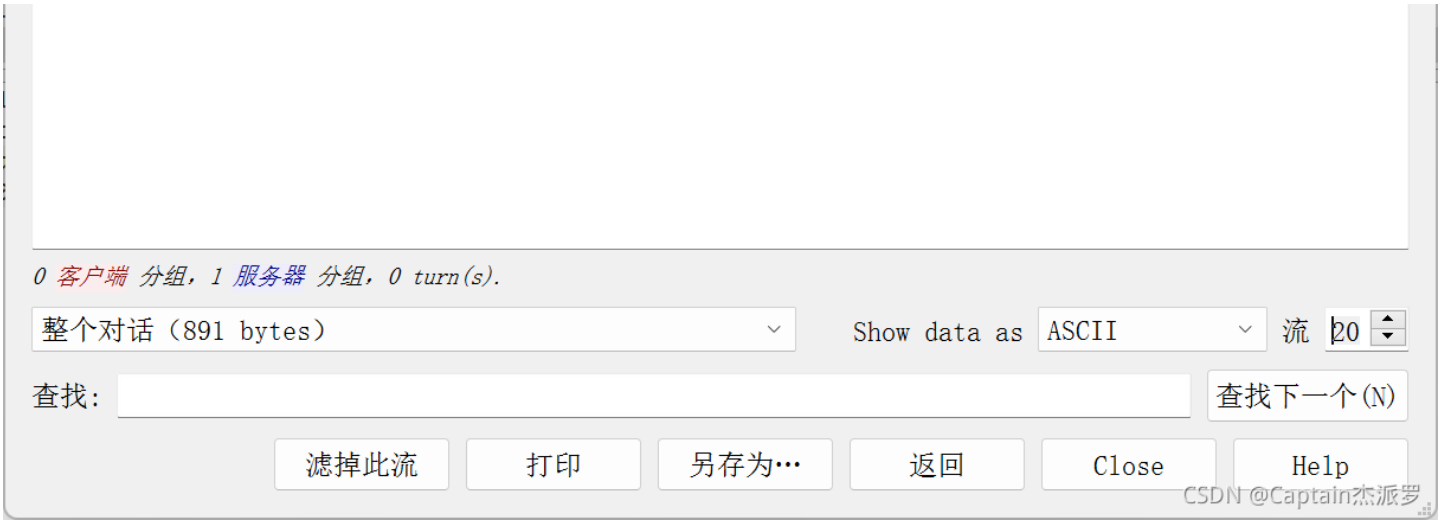
滤掉此流 打印 另存为… 返回 Close Help



继续，tcp.stream eq 20 处发现私钥

Wireshark · 追踪 TCP 流 (tcp.stream eq 20) · Misc-03.pcapng

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj0u8yMWH4Qi+xTbjHgbE7wOuk
OaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBBd85B/LTc36XZ7JVfX5kGy5tI
R3tquuPIVKNdAsHlSqh9S7YSS39RdnSa5rOUyGhrLzxwzzM9IO4e+QQ+CQIDAQAB
AoGADiaw5mGubtCxbkeBOVYf+V/fXnjVSf76QbrzsD1kOooUjfV6sKR2C5Pd7S7H
H+1owENBBgEKvoBtb/cqA2tvU9vQ4l5TMBJcHv6LEcb9WPpnMxPV2GNjO+DTPGPy
Xnu1UZlZjwx+NaF5rESoSSVS2ZaaIixBs4RWRXk+lHEbTFECQQD6Rp6jMweRgPHO
pR3mgIK83zL+kzqYM5isIPv3DIC5JQN2kXqK73IDQCFVlfXnr9lAAVRzLDsAXLqv
le/o6yQLAkEA+edY+GERlLuD1t2k9Js0Dc7EwnLcxoFUE60ivj8Gf9jzLskGHxsv
0IV6J5OHwPh54kAxAnqCjSqNRAWGNzr+uwJBALYEjDUm1LdGrxXZ0jAkgHC6Z0zs
aK3uwHdXGcinqCp+t9EQpq3KzQF+L4AeKxRQONEq5m9I2LQ/vGocwrmD4dcCQQDb
rTyOinWz8upAFPKOe2hUwvA/pkzgyosoCMhDyI9kD0gmVlvlODbd7Jem9o8dWM97
zcXHUf41LbSkmN6U6m1FAkEAqmZbr35bPfkeoiikwNl6OVQytg12TZjw2vIbvfub
f9Rvti8Lh/tbrmhZroiz8/l3aAZmugI1NBcbeZR0gz8ggg==
-----END RSA PRIVATE KEY-----
```




复制私钥（全文，一个字符都不要漏）

把解压的文件送进kali进行foremost分离，分别得到三种文件：png、pdf、zip，其中图片多而杂乱，没有有效信息，pdf文件损坏无法打开，暂且不顾，zip文件可以直接解压得到key.txt

```
┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE]
└─$ foremost -T Misc-03.pcapng
Processing: Misc-03.pcapng
|foundat=key.txtη@
@º@@J@@@@@@T @Gh~M@@d@}@VU@S@@b@@@P@h-@D@@@
                                        @@@~@fC@@    @@3@:@Úm@v4&@7@{rKpVrQl@@@@PK
*|

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE]
└─$ ls
Misc-03.pcapng  out.jpg  output_Sun_Oct__3_18_47_44_2021  test2.png  test.png

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE]
└─$ cd output_Sun_Oct__3_18_47_44_2021

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021]
└─$ ls
audit.txt  jpg  pdf  zip

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021]
└─$ cd zip

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ ls
00000047.zip

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ unzip 00000047.zip
Archive:  00000047.zip
 extracting: key.txt

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ ls
00000047.zip  key.txt
```



读取key.txt，乱码，怀疑内容被加密

```
┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ cat key.txt
η@
@º@@J@@@@@@T @Gh~M@@d@}@VU@S@@b@@@P@h-@D@@@
                                        @@@~@fC@@    @@3@:@Úm@v4&@7@{rKpVrQl@@@@
```

将之前复制的私钥存储为key文件

```
┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ vim pri.key

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ cat pri.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj0u8yMWH4Qi+xTbjHgbE7wOuk
OaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBBd85B/LTc36XZ7JVfX5kGy5tI
R3tquuPIVKNdAsHlSqh9S7YSS39RdnSa5rOUyGhrLzxwzzM9IO4e+QQ+CQIDAQAB
AoGADiaw5mGubtCxbkeBOVYf+V/fXnjVSf76QbrzsD1kOooUjfV6sKR2C5Pd7S7H
H+1owENBBgEKvoBtb/cqA2tvU9vQ4l5TMBJcHv6LEcb9WPpnMxPV2GNjO+DTPGPy
```

```
Xnu1UZlZjwx+NaF5rESoSSVS2ZaaIixBs4RWRXk+lHEbTFECQQD6Rp6jMweRgPHO
pR3mgIK83zL+kzqYM5isIPv3DIC5JQN2kXqK73IDQCFVlfXnr9lAAVRzLDsAXLqv
le/o6yQLAkEA+edY+GERlLuD1t2k9Js0Dc7EwnLcxoFUE60ivj8Gf9jzLskGHxsv
0IV6J5OHwPh54kAxAnqCjSqNRAWGNzr+uwJBALYEjDUm1LdGrxXZ0jAkgHC6Z0zs
aK3uwHdXGcinqCp+t9EQpq3KzQF+L4AeKxRQONEq5m9I2LQ/vGocwrmD4dcCQQDb
rTyOinWz8upAFPKOe2hUwvA/pkzgyosoCMhDyI9kD0gmVlvlODbd7Jem9o8dWM97
zcXHUf41LbSkmN6U6m1FAkEAqmZbr35bPfkeoiikwNl6OVQytg12TZjw2vIbvfub
f9Rvti8Lh/tbrmhZroiz8/l3aAZmugI1NBcbeZR0gz8ggg==
-----END RSA PRIVATE KEY-----
```



利用openssl解密，读取解密后的文件，得到flag

```
┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ openssl rsautl -decrypt -in key.txt -inkey pri.key -out flag.txt

┌──(jack㉿kali)-[/mnt/hgfs/Kali-KDE/output_Sun_Oct__3_18_47_44_2021/zip]
└─$ cat flag.txt
hi, boys and girls! flag is {haPPy_Use_0penSsI}
```

*注意：提交格式为flag{xxxxxx}*

> 总结：
>
> 1. 流量分析问题，就算流量数据再多也要大胆追踪流，多试试
> 2. 如果不直接导出对象，要敢于foremost分离
> 3. misc问题会涉及到加解密问题，相关工具要及时收集整理并学会使用