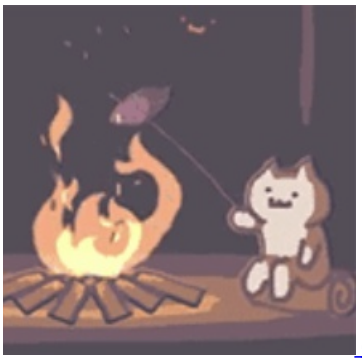
[ctf misc][2021蓝帽杯决赛]ssh_traffic writeup

原创

shu天 于 2021-09-02 23:04:34 发布

分类专栏： ctf 文章标签： ssh tcp/ip ctf misc

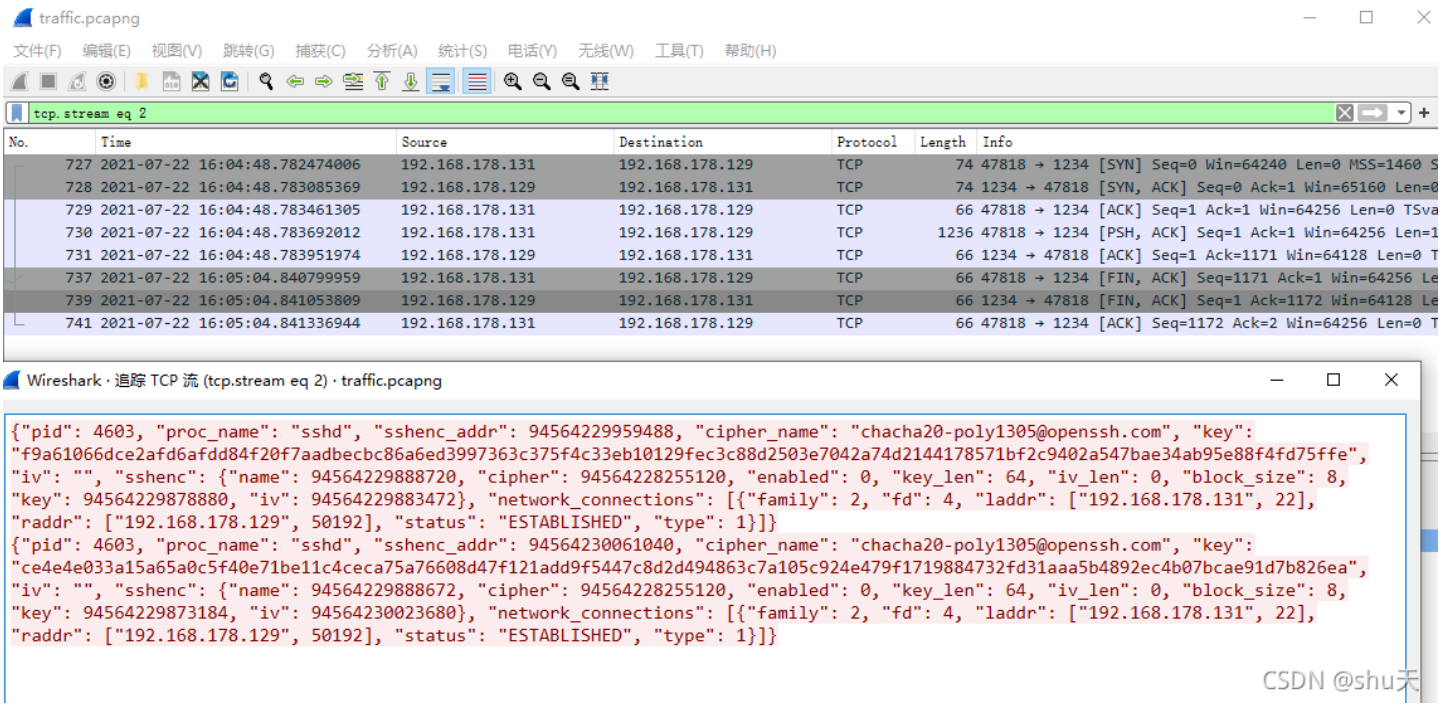


[2021蓝帽杯决赛]ssh_traffic

> 抓取了一段流量， 想知道他们用ssh传输了些什么呢?
> 附件：ssh_traffic_5e202f7c667dfd9b0398d65bfed46b2c.zip

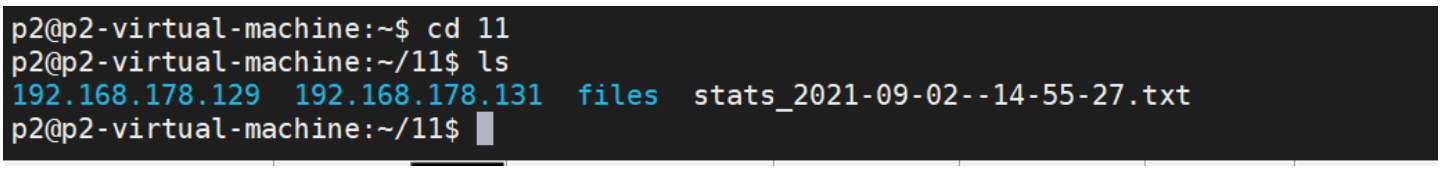
解压得到`traffic.pcapng`，总共三个tcp流

过滤：`tcp.stream eq 2`，得到key，另存为key.json

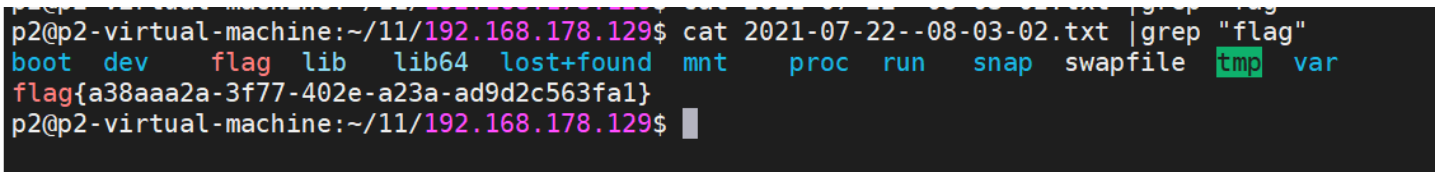


利用工具network-parser解密ssh流量

```
network-parser -p traffic.pcapng --popt keyfile=key.json --proto ssh -o ./11/
```



得到flag



工具安装：https://blog.csdn.net/weixin_46081055/article/details/119888836

> wp参考链接：https://mp.weixin.qq.com/s/e-RZva2y7hpR47FKL0eBpQ