




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

原创

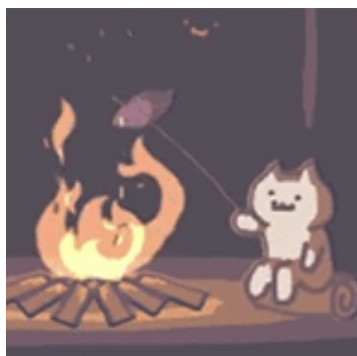
shu天  于 2021-09-02 23:04:34 发布  127  收藏 1

分类专栏: [ctf](#) 文章标签: [ssh tcp/ip ctf misc](#)

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/120071592

版权



[ctf 专栏收录该内容](#)

81 篇文章 4 订阅

订阅专栏

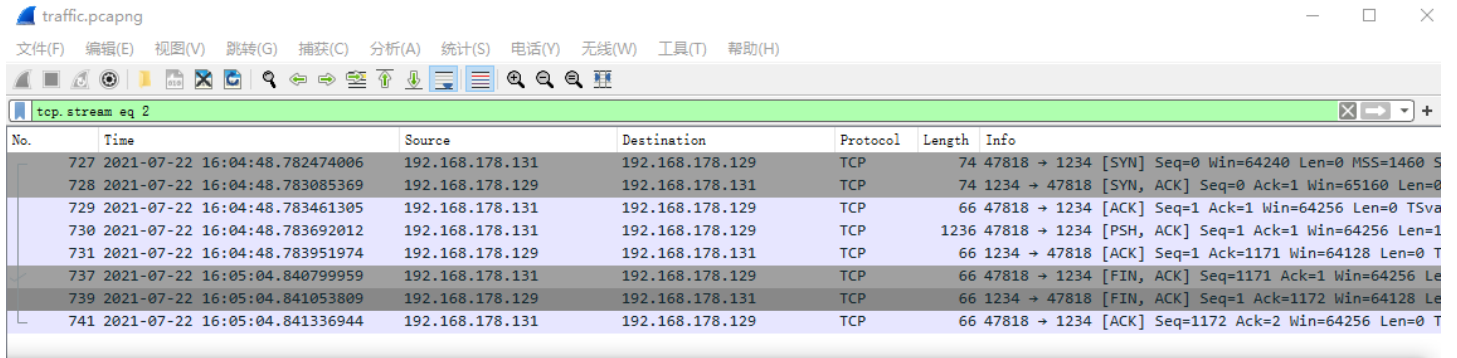
[2021蓝帽杯决赛]ssh_traffic

抓取了一段流量，想知道他们用ssh传输了些什么呢？

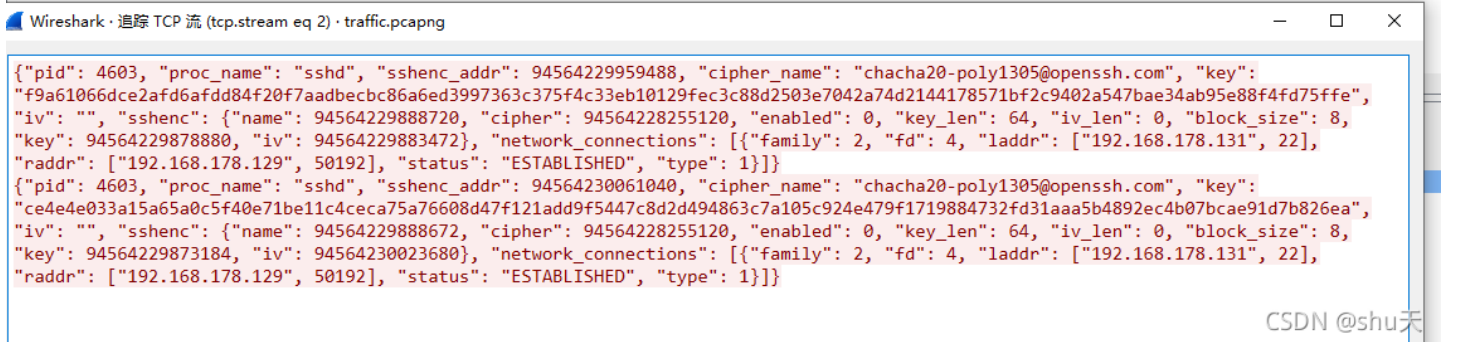
附件: [ssh_traffic_5e202f7c667dfd9b0398d65bfed46b2c.zip](#)

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



No.	Time	Source	Destination	Protocol	Length	Info
727	2021-07-22 16:04:48.782474006	192.168.178.131	192.168.178.129	TCP	74	47818 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
728	2021-07-22 16:04:48.783085369	192.168.178.129	192.168.178.131	TCP	74	1234 → 47818 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
729	2021-07-22 16:04:48.783461305	192.168.178.131	192.168.178.129	TCP	66	47818 → 1234 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
730	2021-07-22 16:04:48.783692012	192.168.178.131	192.168.178.129	TCP	1236	47818 → 1234 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=1
731	2021-07-22 16:04:48.783951974	192.168.178.129	192.168.178.131	TCP	66	1234 → 47818 [ACK] Seq=1 Ack=1171 Win=64128 Len=0 T
737	2021-07-22 16:05:04.840799959	192.168.178.131	192.168.178.129	TCP	66	47818 → 1234 [FIN, ACK] Seq=1171 Ack=1 Win=64256 Le
739	2021-07-22 16:05:04.841053809	192.168.178.129	192.168.178.131	TCP	66	1234 → 47818 [FIN, ACK] Seq=1 Ack=1172 Win=64128 Le
741	2021-07-22 16:05:04.841336944	192.168.178.131	192.168.178.129	TCP	66	47818 → 1234 [ACK] Seq=1172 Ack=2 Win=64256 Len=0 T

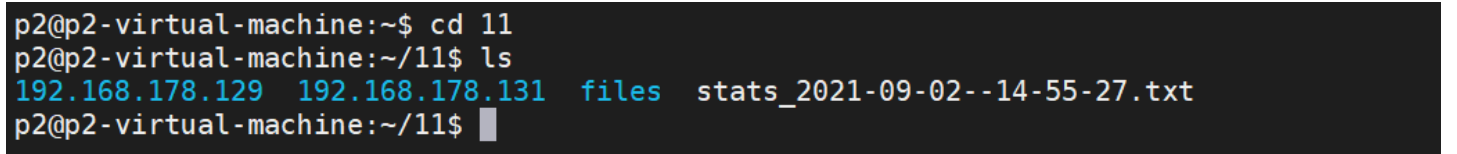


```
{ "pid": 4603, "proc_name": "ssh", "sshenc_addr": "94564229959488", "cipher_name": "chacha20-poly1305@openssh.com", "key": "f9a61066dce2afd6afdd84f20f7aadbecbc86a6ed3997363c375f4c33eb10129fec3c88d2503e7042a74d2144178571bf2c9402a547bae34ab95e88f4fd75ffe", "iv": "", "sshenc": { "name": "94564229888720", "cipher": "94564228255120", "enabled": 0, "key_len": 64, "iv_len": 0, "block_size": 8, "key": "94564229878880", "iv": "94564229883472", "network_connections": [ { "family": 2, "fd": 4, "laddr": ["192.168.178.131", 22], "raddr": ["192.168.178.129", 50192], "status": "ESTABLISHED", "type": 1 } ] } } { "pid": 4603, "proc_name": "ssh", "sshenc_addr": "94564230061040", "cipher_name": "chacha20-poly1305@openssh.com", "key": "ce4e4e033a15a65a0c5f40e71be11c4ceca75a76608d47f121add9f5447c8d2d494863c7a105c924e79f1719884732fd31aaa5b4892ec4b07bcae91d7b826ea", "iv": "", "sshenc": { "name": "94564229888672", "cipher": "94564228255120", "enabled": 0, "key_len": 64, "iv_len": 0, "block_size": 8, "key": "94564229873184", "iv": "94564230023680", "network_connections": [ { "family": 2, "fd": 4, "laddr": ["192.168.178.131", 22], "raddr": ["192.168.178.129", 50192], "status": "ESTABLISHED", "type": 1 } ] } }
```

CSDN @shu天

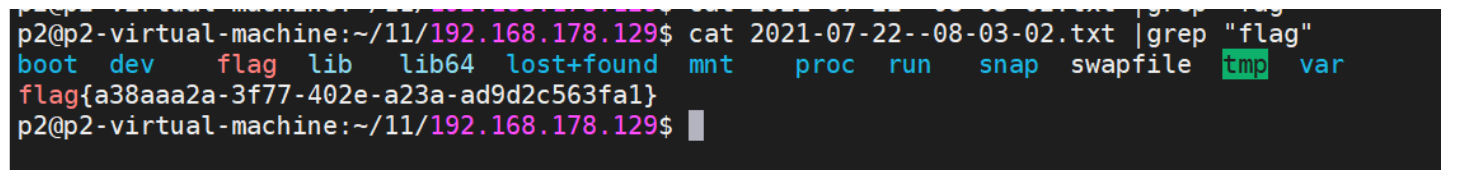
利用工具network-parser解密ssh流量

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



```
p2@p2-virtual-machine:~$ cd 11
p2@p2-virtual-machine:~/11$ ls
192.168.178.129 192.168.178.131 files stats_2021-09-02--14-55-27.txt
p2@p2-virtual-machine:~/11$
```

得到flag



```
p2@p2-virtual-machine:~/11/192.168.178.129$ cat 2021-07-22--08-03-02.txt |grep "flag"
boot dev flag lib lib64 lost+found mnt proc run snap swapfile tmp var
flag{a38aaa2a-3f77-402e-a23a-ad9d2c563fa1}
p2@p2-virtual-machine:~/11/192.168.178.129$
```

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>



[创作打卡挑战赛](#)

赢取流量/现金/CSDN周边激励大奖