[Hack The Box] HTB—Challenges—forensics—USB Ripper writeup

原创

shu天 于 2022-02-24 09:38:37 发布 585 收藏

分类专栏： 取证 文章标签： linux 服务器 运维 usb 日志

本文链接：https://blog.csdn.net/weixin_46081055/article/details/123104159

[Hack The Box] HTB—Challenges—forensics—USB Ripper writeup

> 附件：auth.json syslog
> **DESCRIPTION:**
> There is a sysadmin, who has been dumping all the USB events on his Linux host all the year… Recently, some bad guys managed to steal some data from his machine when they broke into the office. Can you help him to put a tail on the intruders? Note: once you find it, “crack” it.

auth.json的这种格式和一个Linux中的Usbrip工具一样，该工具记录USB设备事件历史。
在Linux中使用Usbrip显示USB设备事件历史记录

auth.json存储授权或受信任的USB设备列表，该文件可用于调查连接了哪些USB设备以及它们是否为授权设备。 这样，可以找出是否某些用户未经许可从系统复制了某些内容。

1.安装Usbrip

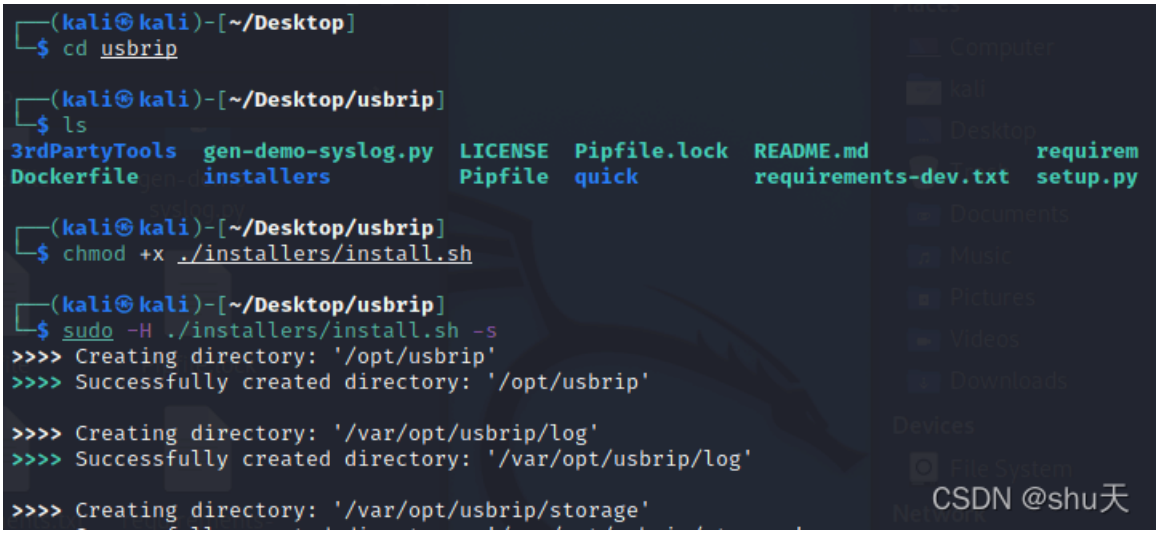
安装依赖：

> python3-venv
> p7zip

```
sudo apt install python3-venv p7zip-full
```

安装Usbrip

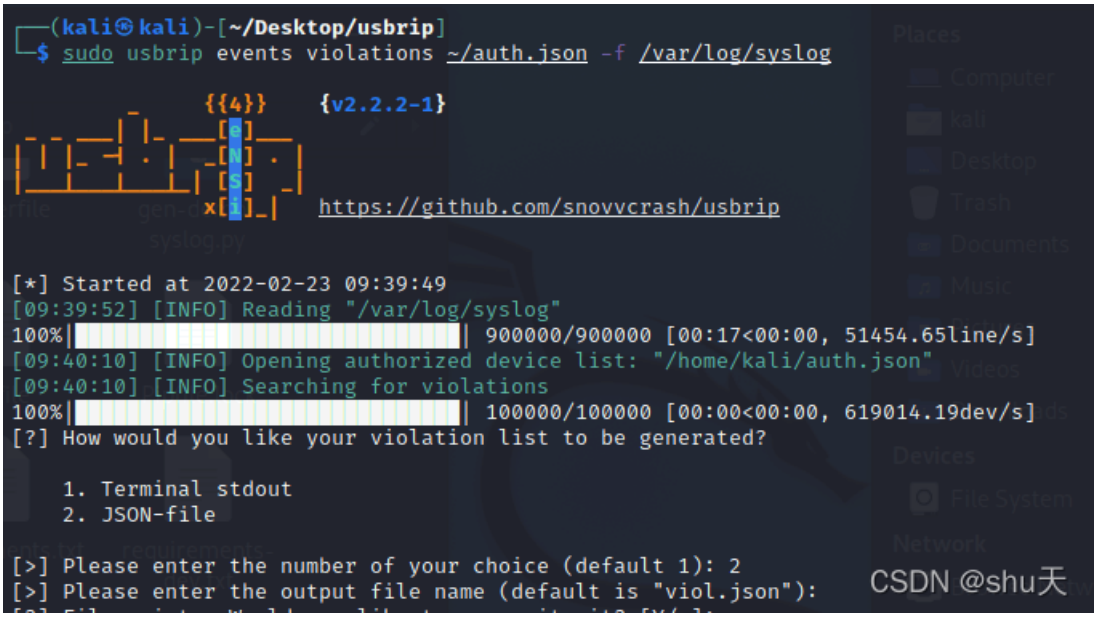
```
git clone https://github.com/snovvcrash/usbrip.git
cd usbrip
chmod +x ./installers/install.sh
sudo -H ./installers/install.sh -s
```



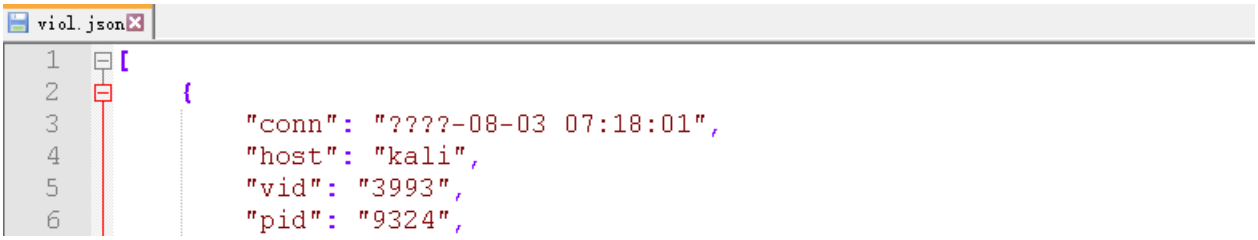
2.分析

检查是否有未经授权的USB访问

```
sudo usbrip events violations ~/auth.json -f syslog
```



viol.json



```
        "prod": "1F8ADAEE73D993944FC7C7783",
        "manufact": "884CCC9A3DF08F49C621373E",
        "serial": "71DF5A33EFFDEA5B1882C9FBDC1240C6",
        "port": "1-1",
        "disconn": "????-08-03 07:18:10"
    },
    {
        "conn": "????-08-08 03:24:02",
        "host": "kali",
        "vid": "1d6b",
        "pid": "0002",
        "prod": "EHCI Host Controller",
        "manufact": "Linux 5.10.0-kali7-amd64 ehci_hcd",
        "serial": "0000:02:03.0",
        "port": "usb1",
```


把序列号MD5解密

71DF5A33EFFDEA5B1882C9FBDC1240C6

flag：`HTB{mychemicalromance}`

> 参考wp：
> https://securitybyexpert.com/usb-ripper-forensics-challenges-hackthebox/