黑客画像报告



* 攻击者身份： 自然人
* 备注：
* 攻击者ID： H-0001
* 攻击源IP：
* 192.168.131.80 局域网
* 内网IP： 未知
* 公网IP： 未知
* 网络身份：
* 操作系统：
* Linux x86\_64
* 浏览器信息：
* Safari:Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/86.0.4240.111 Safari/537.36

## 设备指纹

设备

设备1

设备指纹：6403d407aa08ae408b06287ac5a80910

* 操作系统：Linux x86\_64
* CPU核心数：24
* 显卡设备：Google SwiftShader
* 浏览器：Safari浏览器(Safari)
* 设备类型：PC
* 语言：英文
* 音频设备：44100\_2\_1\_0\_2\_explicit\_speakers
* 浏览器UA：Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/86.0.4240.111 Safari/537.36

## 黑客轨迹

* 2022-05-27 00:57:51   攻击了 liweishiMySQLCheat（172.16.23.17），攻击源为 192.168.131.80
* 2022-05-26 00:58:35   攻击了 Linux-test（192.168.180.59） ，攻击源为 192.168.131.80
* 2022-05-26 00:57:32   攻击了 ssssssssssh（172.16.23.14），攻击源为 192.168.131.80
* 2022-05-26 00:44:02   攻击了 Linux-test（192.168.180.57） ，攻击源为 192.168.131.80   Linux-test（192.168.180.59） ，攻击源为 192.168.131.80
* 2022-05-26 00:43:43   攻击了 Linux-test（192.168.180.57） ，攻击源为 192.168.131.80   Linux-test（192.168.180.59） ，攻击源为 192.168.131.80   Linux-test（192.168.180.56） ，攻击源为 192.168.131.80
* 2022-05-26 00:43:33   攻击了 Linux-test（192.168.180.57） ，攻击源为 192.168.131.80   Linux-test（192.168.180.56） ，攻击源为 192.168.131.80
* 2022-05-26 00:43:13   攻击了 Linux-test（192.168.180.57） ，攻击源为 192.168.131.80
* 2022-05-26 00:40:20   攻击了 Linux-test（192.168.180.56） ，攻击源为 192.168.131.80

## 攻击源探测

* 攻击者IP：
* 192.168.131.80（局域网）
* 端口和服务指纹：
  + 23 telnet
  + 443 https
  + 445 microsoft-ds
  + 7000 afs3-fileserver
  + 7100 font-service
  + 7777 cbt
  + 8000 http-alt
* 探测时间：
* 2022-05-27 03:29:06