# 应急响应与溯源 by 菠萝吹雪

## 日志分析

### Windows

- 安全性日志：C:\Windows\System32\winevt\Logs\Security.evtx
- 系统日志：C:\Windows\System32\winevt\Logs\System.evtx
- 应用程序日志：C:\Windows\System32\Winevt\Logs\Application.evtx
- 敏感事件ID：
  - 4624：登录成功
  - 4625：登录失败
  - 4648：尝试显式凭据登录
  - 4672：授予特殊权限
  - 4720：新建用户
  - 4735：安全组更改
  - 4799：枚举组用户
- 分析工具：
  - LogonTracer(可视化)：https://github.com/JPCERTCC/LogonTracer
  - FullEventLogView(可导出)：https://www.nirsoft.net/utils/full_event_log_view.html

### Linux

- 常用日志：
  - 安全日志：/var/log/secure
  - root邮箱：/var/spool/mail/root
  - 登录成功：/var/log/wtmp
  - 登录失败：/var/log/btmp
  - 计划任务：/var/log/cron
  - 操作命令记录：cat ~/.bash_history
  - web相关：
    - Apache：
      - /var/log/apache/access.log
      - /var/log/apache2/access.log
      - /etc/httpd/logs/access_log
    - Nginx：
      - /var/log/nginx/
      - /usr/local/nginx/logs
    - Tomcat：/TOMCAT_HOME/logs
    - Weblogic：
      - weblogic 8.x版本：$MW_HOME\user_projects\domains\<domain_name>\
      - weblogic 9及以后版本：$MW_HOME\user_projects\domains\<domain_name>\servers\
  - 其他服务：
    - redis：
      - /var/log/redis/redis-server.log
      - /var/log/redis_6379.log
    - mysql：
      - /usr/local/mysql
      - /var/log/mysql
    - oracle：$ORACLE_BASE/diag/rdbms/
- 常用命令：
  - 查看连接失败的IP：lastb
  - 查看root用户启动的进程：lsof -u root
  - 查看7天内修改的文件：find -type f -mtime -7
  - 查看7天内创建的文件：find -type f -ctime -7
  - 查看file中有root关键字的行并标注：grep -nv 'root' file
  - 一键打印access.log中100列、聚合、排序：awk -F " " '{print $100}' access.log| sort|uniq -c|sort -nr

## 流量分析

- wireshark
  - 过滤协议：tcp/udp/arp/icmp/http/ftp/smtp
  - 过滤ip：ip.addr eq xxx.xxx.xxx.xxx
  - 过滤端口：tcp.port == 端口号/udp.port == 端口号
  - 模糊匹配：contains，例如http contains "eval"即可显示包含eval的http包

## 内存分析

- dump内存：
  - ProcessHacker(dump进程)：https://processhacker.sourceforge.io/
  - RamCapturer(dump整机)：https://belkasoft.com/ram-capturer
- Volatility
  - 查看镜像信息：volatility -f 文件 imageinfo
  - 查看进程：volatility -f 文件 --profile=版本号 pslist
  - 提取进程：volatility -f 文件 --profile=版本号 memdump -p 进程id -D ./ D是路径
  - 查看注册表：volatility -f 文件  --profile=版本号 hivelist
  - 扫描文件：volatility -f 文件  --profile=版本号 filescan | grep keywords keywords是扫描关键字
  - 查看用户密码：volatility -f 文件  --profile=版本号 printkey -K "SAM\Domains\Account\Users\Names"

## 进程排查

### Windows

- 网络连接：netstat -ano
- 外部连接：netstat -b
- 查看已建立连接：netstat -ano|findstr "ES"
- 查看进程：tasklist
- 终止进程：taskkill /f /pid [pid]
- 定位程序：tasklist | findstr "pid"
- 查看程序路径：wmic process | findstr "程序.exe"

### Linux

- netstat同windows
- 查看计划任务：crontab -l
- 删除计划任务：rm /etc/cron.d/[file]
- 查看指定端口进程：lsof -i:端口号
- 查看进程：ps aux
- 终止进程：kill pid
- 查看隐藏进程
  - 挂载情况：cat /proc/mount
  - 遍历cmdline：/proc/[pid]/cmdline
  - 一键三连
    - ps -ef | awk '{print $2}'| sort -n | uniq >1
    - ls /proc |sort -n|uniq >2
    - diff 1 2

## 痕迹排查

### Windows

- 敏感目录：
  - 临时目录：C:\TEMP，各种TEMP
  - 应用目录：C:\Users\用户名\AppData\Roaming
  - 近期文件：C:\Users\用户名\Recent
  - 回收站：C:\$Recycle.Bin
  - 各种浏览器的下载文件目录
  - 预读取文件目录：%SystemRoot%\Prefetch\
  - 应用程序执行路径：%SystemRoot%\appcompat\Programs\
- 时间点：
  - 搜索2023年5月20日起新增exe文件的路径、上次修改时间、上次修改日期
  - forfiles /m *.exe /d +2023/5/20 /s /p c:/ /c "cmd /c echo @path @fdate @ftime" 2>null
- Webshell：
  - 只推荐D盾，因为D盾的误报率是有目共睹的，宁可错杀一千绝不放过一个
  - https://www.d99net.net/

### Linux

- 敏感目录：
  - 临时目录：/tmp
  - 命令目录1：/usr/bin
  - 命令目录2：/usr/sbin
  - ssh1：~/.ssh
  - ssh2：/etc/ssh
  - 环境变量：/etc/profile
- 特殊文件：
  - 查看1天内新增sh文件：find / -ctime 0 -name "*.sh"
  - 查看suid权限文件：find / -perm -4000 2>/dev/null
- 后门：
  - chkrootkit(rootkit入侵检测)：https://chkrootkit.org/download/
  - 常用命令
    - 执行：chkrootkit
    - 查看异常：chkrootkit | grep 'INFECTED'

## 域名溯源

- whois查询：https://whois.chinaz.com/
- ICP备案查询：https://beian.miit.gov.cn/
- 网安备案查询：https://www.beian.gov.cn/portal/registerSystemInfo
- 有些域名商是可以通过找回功能找回指定域名所属注册人部分联系方式的，比如前三后二手机号巴拉巴拉，当然了，也可以社工客服。

## EMAIL溯源

- https://epieos.com/
- https://emailrep.io/

## 手机号溯源

- https://www.reg007.com/
- http://www.newx007.com/
- https://fee.icbc.com.cn/index.jsp
- 支付宝转账、钉钉通讯录导入、微信搜索

## ID溯源

- https://whatsmyname.app/
- https://github.com/p1ngul1n0/blackbird
- https://github.com/sherlock-project/sherlock
- 搜索引擎、SRC排名、QQ群、微信群、抖音、快手、微博、知乎、脉脉、牛客网、github、gitee、csdn、cnblogs

## IP溯源

- 定位
  - https://www.chaipip.com/
  - https://www.opengps.cn/
- 情报
  - https://x.threatbook.com/
  - https://ti.360.net/
  - https://tix.qq.com/
  - https://ti.qianxin.com/
  - https://www.virustotal.com/gui/home/search