Linux应急：<https://blog.csdn.net/qq_41874930/article/details/109079044>

 https://blog.csdn.net/weixin\_43526443/article/details/122744731

Window应急: <https://baijiahao.baidu.com/s?id=1710337028628832865&wfr=spider&for=pc>

 https://baijiahao.baidu.com/s?id=1710337028628832865&wfr=spider&for=pc

首先收集客户机器信息以及样本，做好文件备份

然后判断安全事件的类型，是系统层面的，如挖矿病毒、后门木马，还是网络应用层面的，如webshell，或者是网络层面，如断网、DDOS等，之后隔离机器(火绒剑，D盾)

日志、用户、进程、启动项、样本，看到可疑的就杀掉，删文件，打补丁，溯源

最后产出一份安全事件报告，**查看定时任务，日志，用户，进程，端口\_通信，启动项等**

**Linux常用命令**

netstat -anpl #检查当前存在的连接与监听端口

netstat -anplt #只检查tcp相关

ps -ef #查看当前系统上运行的所有进程与其使用的命令

ps aux #查看当前系统运行的所有进程与其占用的cpu与内存情况

top #动态查询当前系统运行中的所有进程与其占用的cpu情况

last或者last -f /var/log/wtmp #显示用户的最近登陆信息

who或者who /var/run/utmp #显示当前谁还登陆在服务器上

lastb或者last -f /var/log/btmp #显示登录失败的用户的信息

cat ~/.bash\_history或者history #查看历史命令

cat /etc/passwd #查看用户异常的gid

lsof -i（查看正在进行的网络连接）

lsof -g gid #查看相关文件

crontab -l #查看定时任务 -r是删除

service --status-all（枚举主机的所有服务）

ll ~/.ssh #查看攻击者是否添加私钥

chkconfig --list 列出所有开机启动项

日志在/var/log目录下

**Windows常用命令**

1. 多看临时目录(tmp/temp),浏览器相关文件,文件修改时间
2. 最近打开的文件(C:\Users\[用户名]\Recent or C:\Documents and Settings\[用户名]\Recent)
3. 网络连接排查：netstat -ano
4. 进程 tasklist 杀进程:taskkill /pid 272 -f
5. 漏洞和补丁信息:Systeminfo
6. 可疑进程：火绒剑等工具 webshell就D盾等工具
7. 启动项和计划任务 Autoruns工具（官网[www.sysinternals.com](http://www.sysinternals.com)）

**Java内存马查杀 注入servlet filter**

<https://github.com/su18/MemoryShell>

web日志依靠安全厂商设备或者看数据包用winshark看，主要通过态势感知设备发现入侵行为

##### 系统日志就LogonTracer 我自己用的比较多

##### 看不懂的请求包直接干掉或者去客户测试环境测试

## Webshell工具流量特征:

1. **蚁剑：**

**ini\_set**

**ini\_set\_time**

**ini\_set\_limit**

**@ini\_set("display\_errors","0")**

**部分代码明文传输，较好辨认**

**菜刀：**

**老版本采用明文传输，非常好辨认**

**新版本采用base64加密，检测思路就是分析流量包，发现大量的base64加密密文就需要注意**

**冰蝎：**

**冰蝎1：冰蝎1有一个密钥协商过程，这个过程是明文传输，并且有两次流量，用来校验**

**冰蝎2：因为内置了很多的UA头，所以当某一个相同IP重复请求，但是UA头不一样的时候就需要注意了**

**冰蝎3：因为省去了协商过程，所以流量上可以绕过很多，但是其他特征依旧保留，比如ua头**

**冰蝎数据包总是伴随着大量的content-type：application什么什么，无论GET还是POST，请求的http中，content-type为application/octet-stream**

**还有他们的accept之类的长度总是等长，正常的根据应用场景和不同文件，长度是不同的**

**哥斯拉：**

**cookie这个值的地方有一个小纰漏，就是正常请求cookie最后结尾是没有分号的，可能后续作者会进行调整修改**

**还有响应，哥斯拉会响应三次，而且我认为还有一个地方需要注意的就是webshell连接，所以一般会设置长时间连接，所以connection这里会是keep-alive**

##### Win：重新开启Windows Event Log 服务(复原日志) github上有完整