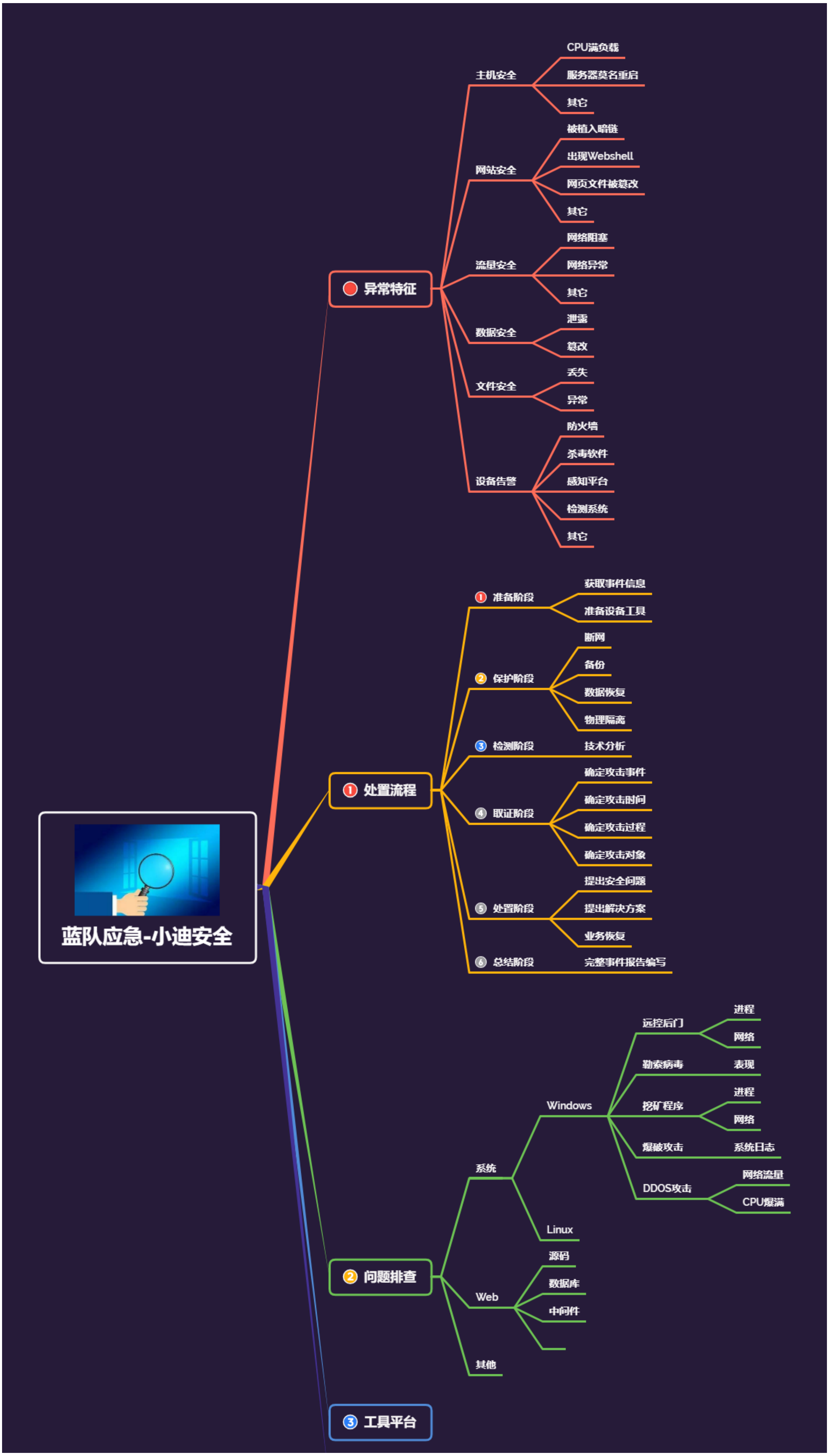
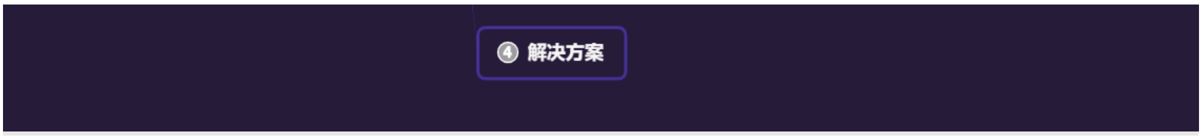
Day166　应急响应-拒绝服务&钓鱼指南&DDOS压力测试&邮件反制分析&应用日志



蓝队应急-小迪安全

- ● 异常特征
  - 主机安全
    - CPU满负载
    - 服务器莫名重启
    - 其它
  - 网站安全
    - 被植入暗链
    - 出现Webshell
    - 网页文件被篡改
    - 其它
  - 流量安全
    - 网络阻塞
    - 网络异常
    - 其它
  - 数据安全
    - 泄露
    - 篡改
  - 文件安全
    - 丢失
    - 异常
  - 设备告警
    - 防火墙
    - 杀毒软件
    - 感知平台
    - 检测系统
    - 其它
- ① 处置流程
  - ① 准备阶段
    - 获取事件信息
    - 准备设备工具
  - ② 保护阶段
    - 断网
    - 备份
    - 数据恢复
    - 物理隔离
  - ③ 检测阶段
    - 技术分析
  - ④ 取证阶段
    - 确定攻击事件
    - 确定攻击时间
    - 确定攻击过程
    - 确定攻击对象
  - ⑤ 处置阶段
    - 提出安全问题
    - 提出解决方案
    - 业务恢复
  - ⑥ 总结阶段
    - 完整事件报告编写
- ② 问题排查
  - 系统
    - Windows
      - 远控后门
        - 进程
        - 网络
      - 勒索病毒
        - 表现
      - 挖矿程序
        - 进程
        - 网络
      - 爆破攻击
        - 系统日志
      - DDOS攻击
        - 网络流量
        - CPU爆满
    - Linux
  - Web
    - 源码
    - 数据库
    - 中间件
  - 其他
- ③ 工具平台



1.知识点

- 1、CC攻击分析
- 2、钓鱼邮件分析
- 3、内网渗透分析

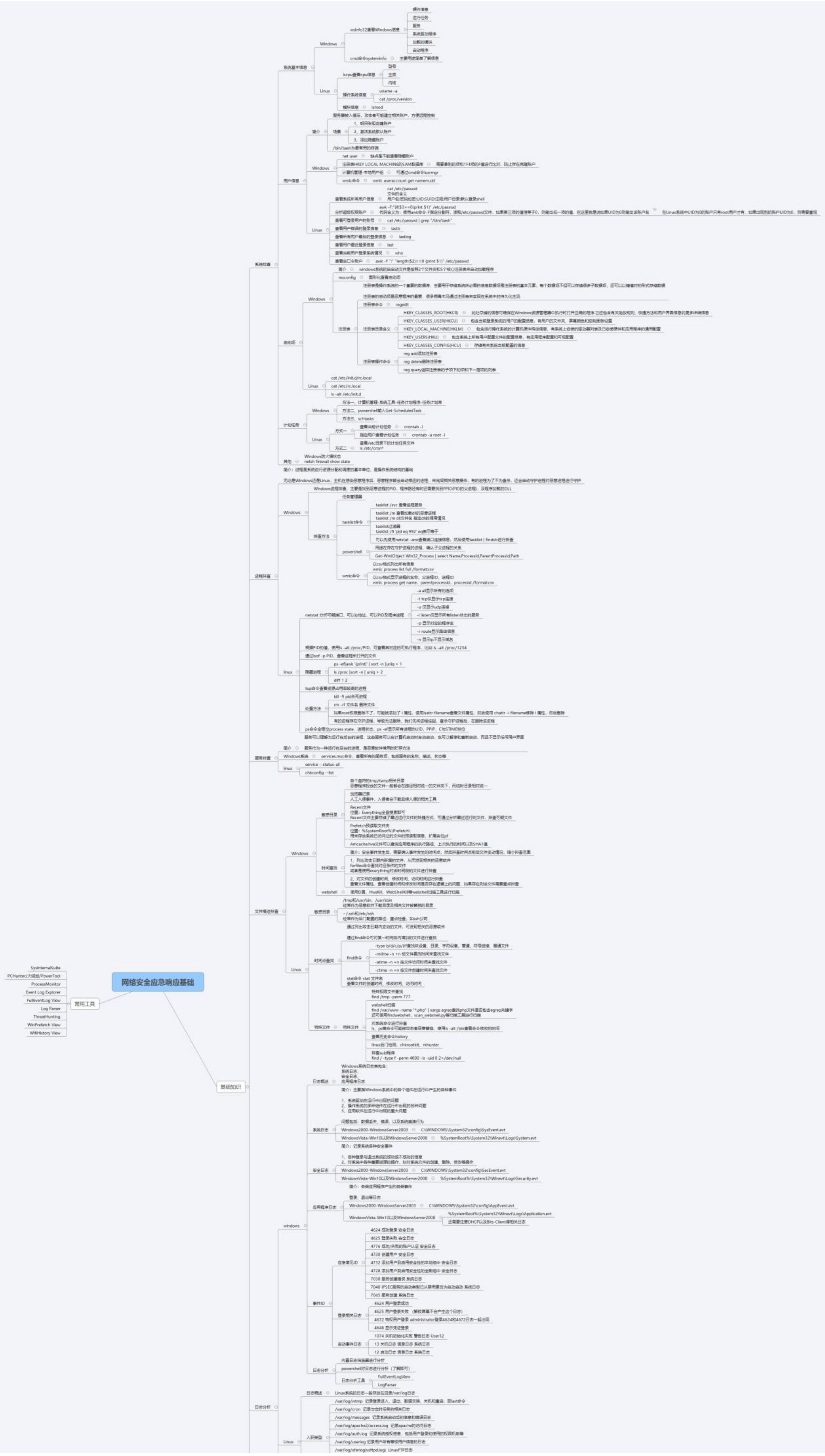
2.内容点

```
应急响应：
1、抗拒绝服务攻击防范应对指南
2、勒索软件防范应对指南
3、钓鱼邮件攻击防范应对指南
4、网页篡改与后门攻击防范应对指南
5、网络安全漏洞防范应对指南
6、大规模数据泄露防范应对指南
7、僵尸网络感染防范应对指南
8、APT攻击入侵防范应对指南
9、各种辅助类分析工具项目使用
```

```
溯源反制：
威胁情报，信息库追踪，设备反制，IDS&IPS等反制，工具漏洞反制，蜜罐钓鱼反制等
```

```
威胁情报相关平台:
Virustotal
深信服威胁情报中心
微步在线
venuseye
安恒威胁情报中心
360威胁情报中心
绿盟威胁情报中心
AlienVault
RedQueen安全智能服务平台
IBM X-Force Exchange
ThreatMiner
```

3.演示案例



网络安全应急响应基础
常用工具
SysinternalSuite
PCHunter/火绒剑/PowerTool
ProcessMonitor
Event Log Explorer
FullEventLog View
Log Parser
ThreatHunting
WinPrefetch View
WifiHistory View
基础知识
系统排查
系统基本信息
Windows
wsinfo32查看Windows信息
硬件信息
运行任务
服务
系统驱动程序
加载的模块
启动程序
cmd命令systeminfo
主要用途简单了解信息
Linux
lscpu查看cpu信息
型号
主频
内核
操作系统信息
uname -a
cat /proc/version
模块信息
lsmod
用户信息
简介
服务器被入侵后，攻击者可能建立相关账户，方便远程控制
场景
1、明目张胆创建账户
2、激活系统默认账户
3、添加隐藏账户
/bin/bash为最常用的终端
Windows
net user
缺点是不能查看隐藏账户
注册表HKEY LOCAL MACHINE的SAM数据库
需要拿到的项和1F4项的F值进行比对，防止存在克隆账户
计算机管理-本地用户组
可通过cmd命令lusrmgr
wmic命令
wmic useraccount get namem,sid
Linux
查看系统所有用户信息
cat /etc/passwd
文件的含义
用户名:密码加密:UID:SUID:注释:用户目录:默认登录shell
分析超级权限账户
awk -F:'{if($3==0)print $1}' /etc/passwd
代码含义为：使用awk命令-F限定分割符，读取/etc/passwd文件，如果第三项的值等于0，则输出该一项的值，在这里意思是如果UID为0则输出该账户名
在Linux系统中UID为0的账户只有root用户才有，如果出现别的账户UID为0，则需要重视
查看可登录用户的账号
cat /etc/passwd | grep "/bin/bash"
查看用户错误的登录信息
lastb
查看所有用户最后的登录信息
lastlog
查看用户最近登录信息
last
查看当前用户登录系统情况
who
查看空口令账户
awk -F ":" 'length($2)==0 {print $1}' /etc/passwd
启动项
Windows
简介
windows系统的自启动文件是按照2个文件夹和5个核心注册表来自动加载程序
msconfig
图形化查看启动项
注册表
注册表是操作系统的一个重要的数据库，主要用于存储系统所必需的信息数据项是注册表的基本元素，每个数据项不但可以存储很多子数据项，还可以以键值对的形式存储数据
注册表的启动项是恶意程序的最爱，很多病毒木马通过注册表来实现在系统中的持久化驻留
注册表命令
regedit
注册表目录含义
HKEY_CLASSES_ROOT(HKCR)
此处存储的信息可确保在Windows资源管理器中执行时打开正确的程序.它还包含有关拖放规则、快捷方法和用户界面信息的更多详细信息
HKEY_CLASSES_USER(HKCU)
包含当前登录系统的用户的配置信息，有用户的文件夹、屏幕颜色和控制面板设置
HKEY_LOCAL_MACHINE(HKLM)
包含运行操作系统的计算机硬件特定信息，有系统上安装的驱动器列表及已安装硬件和应用程序的通用配置
HKEY_USERS(HKU)
包含系统上所有用户配置文件的配置信息，有应用程序配置和可视配置
HKEY_CLASSES_CONFIG(HCU)
存储有关系统当前配置的信息
注册表操作命令
reg add添加注册表
reg delete删除注册表
reg query返回注册表的子项下的项和下一层项的列表
Linux
cat /etc/init.d/rc.local
cat /etc/rc.local
ls -alt /etc/init.d
计划任务
Windows
方法一、计算机管理-系统工具-任务计划程序-任务计划库
方法二、powershell输入Get-ScheduledTask
方法三、schtasks
Linux
方式一
查看当前计划任务
crontab -l
指定用户查看计划任务
crontab -u root -l
方式二
查看/etc目录下的计划任务文件
ls /etc/cron*
其他
Windows防火墙状态
netsh firewall show state
进程排查
简介：进程是系统进行资源分配和调度的基本单位，是操作系统结构的基础
无论是Windows还是Linux，主机在感染恶意程序后，恶意程序都会启动相应的进程，来完成相关恶意操作，有的进程为了不为查杀，还会启动守护进程对恶意进程进行守护
Windows
Windows进程排查，主要是找到恶意进程的PID，程序路径有时还需要找到PPID(PID的父进程)，及程序加载的DLL
排查方法
任务管理器
tasklist命令
tasklist /svc 查看进程服务
tasklist /m 查看加载dll的恶意进程
tasklist /m dll文件名 指定dll的调用情况
tasklist过滤器
tasklist /fi 'pid eq 992' eq表示等于
可以先使用netstat -ano查看端口连接信息，然后使用tasklist | findstr进行排查
powershell
用途在存在守护进程的进程，确认子父进程的关系
Get-WmiObject Win32_Process | select Name,ProcessId,ParentProcessId,Path
wmic命令
以csv格式列出所有信息
wmic process list full /format:csv
以csv格式显示进程的名称、父进程ID、进程ID
wmic process get name，parentprocessid，processid /format:csv
linux
netstat 分析可疑端口、可以ip地址、可以PID及程序进程
-a all显示所有的选项
-t tcp仅显示tcp连接
-u 仅显示udp连接
-l listen仅显示所有listen状态的服务
-p 显示对应的程序名
-r route显示路由信息
-n 显示ip不显示域名
根据PID的值，使用ls -alt /proc/PID，可查看其对应的可执行程序，比如 ls -alt /proc/1234
通过lsof -p PID，查看进程所打开的文件
隐藏进程
ps -ef|awk '{print}' | sort -n |uniq > 1
ls /proc |sort -n | uniq > 2
diff 1 2
top命令查看资源占用率较高的进程
处置方法
kill -9 pid杀死进程
rm -rf 文件名 删除文件
如果root权限删除不了，可能被添加了 i 属性，使用lsattr filename查看文件属性，然后使用 chattr -i filename移除 i 属性，然后删除
有的进程存在守护进程，导致无法删除，我们先将进程挂起，查杀守护进程后，在删除该进程
ps命令全程位process state，进程状态，ps -ef显示所有进程的UID，PPIP，C与STIME栏位
服务排查
服务可以理解为运行在后台的进程，这些服务可以在计算机启动时自动启动，也可以暂停和重新启动，而且不显示任何用户界面
简介
服务作为一种运行在后台的进程，是恶意软件常用的驻存方法
Windows系统
services.msc命令，查看所有的服务项，包括服务的名称、描述、状态等
linux
service --status-all
chkconfig --list
文件痕迹排查
Windows
敏感目录
各个盘符的tmp/temp相关目录
恶意程序投放的文件一般都会在路径相对统一的文件夹下，而临时目录相对统一
浏览器记录
人工入侵事件，入侵者会下载后续入侵的相关工具
Recent文件
位置：Everything全盘搜索即可
Recent文件主要存储了最近运行文件的快捷方式，可通过分析最近运行的文件，排查可疑文件
Prefetch预读取文件夹
位置：%SystemRoot%\Prefetch\
用来存放系统已访问过的文件的预读取信息，扩展名位pf
Amcache.hve文件可以查询应用程序的执行路径、上次执行的时间以及SHA1值
时间查找
简介：安全事件发生后，需要确认事件发生的时间点，然后排查时间点前后文件变动情况，缩小排查范围
1、列出攻击日期内新增的文件，从而发现相关的恶意软件
forfiles命令查找对应条件的文件
或者是使用everything对该时间段的文件进行排查
2、对文件的创建时间、修改时间、访问时间进行排查
查看文件属性，查看创建时间和修改时间是否存在逻辑上的问题，如果存在则该文件需要重点排查
webshell
使用D盾、HwsKill、WebShellKill等webshell扫描工具进行扫描
Linux
敏感目录
/tmp和/usr/bin、/usr/sbin
经常作为恶意软件下载目录及相关文件被替换的目录
~/.ssh和/etc/ssh
经常作为后门配置的路径，重点检查，如ssh公钥
时间点查找
通过列出攻击日期内变动的文件，可发现相关的恶意软件
通过find命令可对某一时间段内增加的文件进行查找
find命令
-type b/d/c/p/l/f查找块设备、目录、字符设备、管道、符号链接、普通文件
-mtime -n +n 按文件更改时间来查找文件
-atime -n +n 按文件访问时间来查找文件
-ctime -n +n 按文件创建时间来查找文件
stat命令 stat 文件名
查看文件的创建时间、修改时间、访问时间
特殊文件
特殊文件
特殊权限文件查找
find /tmp -perm 777
webshell扫描
find /var/www -name "*.php" | xargs egrep查找php文件是否包含egrep关键字
还可使用findwebshell、scan_webshell.py等扫描工具进行扫描
对系统命令进行排查
ls、ps等命令可能被攻击者恶意替换，使用ls -alt /bin查看命令修改的时间
查看历史命令history
linux后门检测，chkrootkit、rkhunter
排查suid程序
find / -type f -perm 4000 -ls -uid 0 2>/dev/null
日志分析
windows
日志概述
Windows系统日志包含：
系统日志、
安全日志、
应用程序日志
系统日志
简介：主要指Windows系统中的各个组件在运行中产生的各种事件
1、系统驱动在运行中出现的问题
2、操作系统的多种组件在运行中出现的各种问题
3、应用软件在运行中出现的重大问题
问题包括：数据丢失、错误，以及系统崩溃行为
Windows2000-WindowsServer2003
C:\WINDOWS\System32\config\SysEvent.evt
WindowsVista-Win10以及WindowsServer2008
%SystemRoot%\System32\Winevt\Logs\System.evt
安全日志
简介：记录系统各种安全事件
1、各种登录与退出系统的成功或不成功的信息
2、对系统中各种重要资源的操作，如对系统文件的创建、删除、修改等操作
Windows2000-WindowsServer2003
C:\WINDOWS\System32\config\SecEvent.evt
WindowsVista-Win10以及WindowsServer2008
%SystemRoot%\System32\Winevt\Logs\Security.evt
应用程序日志
简介：各类应用程序产生的各类事件
登录、退出等日志
Windows2000-WindowsServer2003
C:\WINDOWS\System32\config\AppEvent.evt
WindowsVista-Win10以及WindowsServer2008
%SystemRoot%\System32\Winevt\Logs\Application.evt
还需要注意DHCP以及Bits-Client等相关日志
事件ID
应急常见ID
4624 成功登录 安全日志
4625 登录失败 安全日志
4776 成功/失败的账户认证 安全日志
4720 创建用户 安全日志
4732 添加用户到启用安全性的本地组中 安全日志
4728 添加用户到启用安全性的全局组中 安全日志
7030 服务创建错误 系统日志
7040 IPSEC服务的启动类型已从禁用更改为自动启动 系统日志
7045 服务创建 系统日志
登录相关日志
4624 用户登录成功
4625 用户登录失败 （解锁屏幕不会产生这个日志）
4672 特权用户登录 administrator登录4624和4672日志一起出现
4648 显示凭证登录
启动事件日志
1074 关机初始化失败 警告日志 User32
13 关机日志 信息日志 系统日志
12 启动日志 信息日志 系统日志
日志分析
内置日志筛选器进行分析
powershell对日志进行分析（了解即可）
日志分析工具
FullEventLogView
LogParser
Linux
日志概述
Linux系统的日志一般存放在目录/var/log日志
入职类型
/var/log/wtmp 记录登录进入、退出、数据交换、关机和重启，即last命令
/var/log/cron 记录与定时任务的相关日志
/var/log/messages 记录系统启动后的信息和错误日志
/var/log/apache2/access.log 记录apache的访问日志
/var/log/auth.log 记录系统授权信息，包括用户登录和使用的权限机制等
/var/log/userlog 记录用户所有等级用户信息的日志
/var/log/xferlog(vsftpd.log) LinuxFTP日志

3.1 内网应急-日志分析-爆破&横向&数据库

```
1、协议口令爆破事件
2、口令传递横向事件
3、数据库安全入侵事件
了解：数据库日志，系统日志，中间件日志，其他应用日志等
```

3.2 红队APT-钓鱼邮件-内容&发信人&附件

```
如何分析邮件安全性：
1、看发信人地址
2、看发信内容信息
3、看发信内容附件
4、查询发信域名反制
    红队APT钓鱼邮件内容分析
    个人邮箱洽谈人发送的内容分析

邮件原文源码：
1、看指纹信息（什么发送工具平台）
2、看发送IP地址（服务器IP或攻击IP）
3、根据域名寻找邮件服务器地址(利用红队手段渗透获取信息)
4、可能存在个人的ID昵称用户名（利用社工的技术手段进行画像）
```

3.3 拒绝攻击-DDOS&CC-代理&防火墙防御

```
*声明：课程只做防范指南，请勿测试真实目标，后果自负!
Web类CC攻击，其他流量攻击（主机流量）
防御手段：CC防火墙，CDN服务，高防服务等
```