



OWASP

Open Web Application
Security Project

浅谈溯源取证技术

Id:不许联想



OWASP

Open Web Application
Security Project

目录

- 工作概述
- 应急处理流程
- 安全事件分类
- 常见应急方法技巧
- 实际案例



OWASP

Open Web Application
Security Project

应急工作概述



应急工作概述

应急响应工作是在安全事件发生前做好相对应安全建设，发生时对安全事件相关网络设备进行备份、调查、取证等操作来确保公司信息资产的**机密性、完整性、可用性**

未雨绸缪

发生前

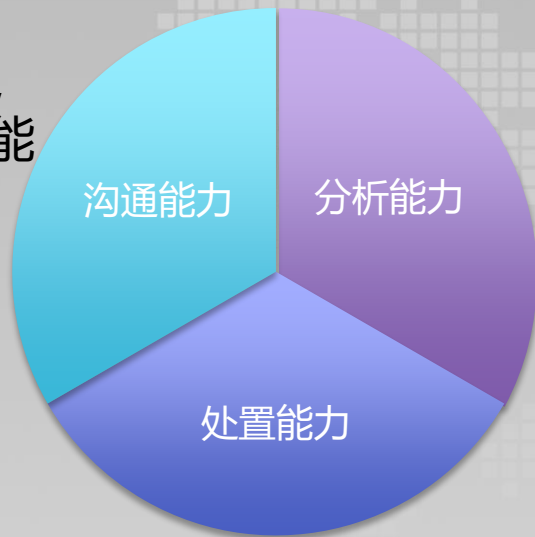
发生后

亡羊补牢



应急人员需要能力

能够适应各种客户现场，
能够利用现有资源尽可能
推动安全事件处理进度



能够深入理解攻击原理，
多维度关联分析多种攻
击方法

能够调动多部门协同处理安全
事件，降低业务恢复时间，缩降低
受害程度



应急能力组成

专业团队 + 基础数据 = 完成一次看似不可能完成的任务



应急工作需要全方位的日志作为基础数据，用于驱动安全活动的稳定运行，但是由于很多项目日志系统建设不完善，部分应用服务默认无日志，造成应急响应人员巧妇难为无米之炊。





OWASP

Open Web Application
Security Project

应急处理流程

应急处理流程

准备

是安全事件响应的第一个阶段，即在事件真正发生前为事件响应做好准备

检测

以适当的方法确认在系统，网络中是否出现了恶意代码、文件和目录是否被篡改等异常活动、现象

抑制

限制攻击、破坏所波及的范围

根除

找出事件的根源并彻底根除，以避免攻击者再次使用相同手段攻击系统，引发安全事件

恢复

目标是把所有被攻破的系统或者网络设备还原到正常的任务状态

跟踪

回顾并整合应急响应事件过程的相关信息



简化应急处理流程

沟通

快速有效收集被恶意攻击业务相关的所有信息资料，并留存证据

分析

能够深入理解攻击原理，多维度关联分析多种攻击方法

消除

通过对有关恶意代码或行为的分析结果，找出事件根源明确相应的补救措施并彻底清除，对攻击源进行准确定位并采取措施将其中断；

整改

清理系统、恢复数据、程序、服务，把所有被攻破的系统和网络设备彻底还原到正常的任务状态，并且输出安全应急报告，对同类安全风险进行排查加固





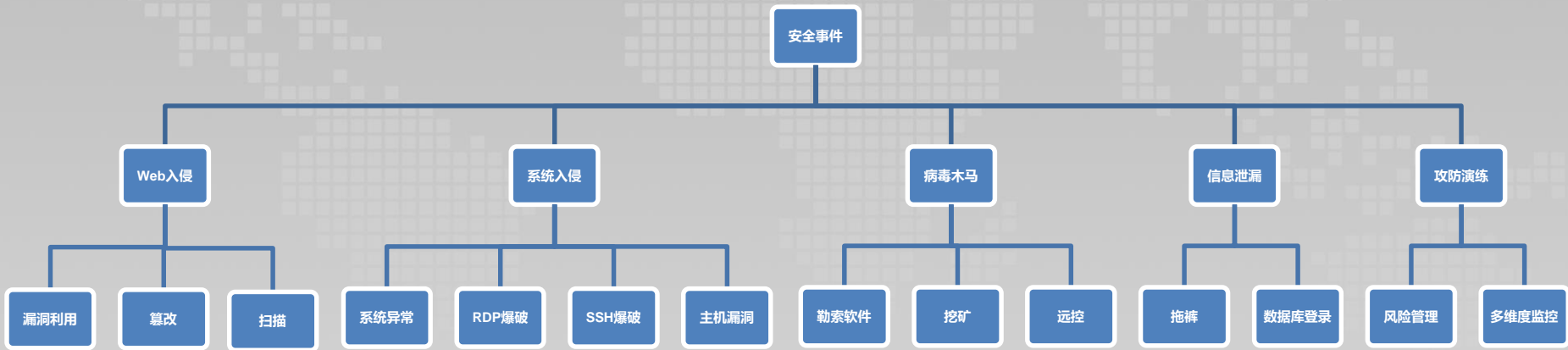
OWASP

Open Web Application
Security Project

安全事件分类



安全事件分类



安全事件分类

APT+挖矿/勒索

挖矿/勒索

名称	压缩前	压缩后	类型	修改日期
DAMP NTDS.txt *	2.6 KB	1.1 KB	文本文档	2021-07-24 22:47
domains.txt *	1.5 KB	1 KB	文本文档	2021-07-24 22:01
enhancement-chain.7z *	52.8 KB	52.8 KB	360压缩 7Z 文件	2021-07-24 22:45
Kerber-ATTACK.rar *	9.4 KB	9.4 KB	360压缩 RAR 文件	2021-07-24 22:33
NetScan.txt *	1.7 KB	1 KB	文本文档	2021-07-24 23:03
p.bat *	1 KB	1 KB	Windows 批处理文件	2021-07-24 22:40
PENTEST SQL.txt *	1 KB	1 KB	文本文档	2021-07-24 22:48
ProxifierPE.zip *	2.9 MB	2.9 MB	360压缩 ZIP 文件	2021-07-22 20:06
RDP_NGROK.txt *	1.5 KB	1 KB	文本文档	2021-07-24 23:07
RMM_Client.exe *	13.6 MB	12.0 MB	应用程序	2021-07-22 18:48
Routerscan.7z *	2.9 MB	2.9 MB	360压缩 7Z 文件	2021-07-24 23:05
RouterScan.txt *	1.7 KB	1 KB	文本文档	2021-07-24 23:05
SQL DAMP.txt *	3.9 KB	1.4 KB	文本文档	2021-07-24 22:46
Алиасы для msf.gar *	1 KB	1 KB	360压缩 RAR 文件	2021-07-24 22:53
Анонимность для параноиков.txt *	1.2 KB	1 KB	文本文档	2021-07-24 23:04
DAMP LSASS.txt *	1 KB	1 KB	文本文档	2021-07-24 22:58
Если необходимо отсканировать всю сетку одним листом...	1 KB	1 KB	文本文档	2021-07-24 22:58
Закреп AnyDesk.txt *	1.5 KB	1 KB	文本文档	2021-07-24 22:50
Заменяем sorted адфайндера.txt *	1 KB	1 KB	文本文档	2021-07-24 22:36
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt *	1.5 KB	1 KB	文本文档	2021-07-24 22:44
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt *	1.2 KB	1 KB	文本文档	2021-07-24 22:39
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt *	3.4 KB	1.5 KB	文本文档	2021-07-24 22:37
КАК ПРЫГАТЬ ПО СЕССИЯМ С ПОМОЩЬЮ ПЕЙЛОА...	1.8 KB	1 KB	文本文档	2021-07-24 22:37
Личная безопасность.txt *	1.3 KB	1 KB	文本文档	2021-07-24 23:01
Мануал робота с AD DC.txt *	8.9 KB	2.5 KB	文本文档	2021-07-22 20:42
МАНУАЛ.txt *	2.5 KB	1.1 KB	文本文档	2021-07-24 22:33
Меняем RDP порт.txt *	1 KB	1 KB	文本文档	2021-07-24 22:51
ОТКЛЮЧЕНИЕ ДЕФЕНДЕРА ВРУЧНУЮ.txt *	1.7 KB	1 KB	文本文档	2021-07-24 22:35
параметр запуска локера на линукс версиях.txt *	1.5 KB	1 KB	文本文档	2021-07-24 22:56
ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ.txt *	4.3 KB	1.6 KB	文本文档	2021-07-24 22:32
по отключению дефендера.txt *	1 KB	1 KB	文本文档	2021-07-24 23:06
ПОВИШЕНИЯ ПРИВИЛЕГИЙ.txt *	1 KB	1 KB	文本文档	2021-07-24 22:45
поднятие прав (дефолт).txt *	1 KB	1 KB	文本文档	2021-07-24 22:57
Получение доступа к серверу с бекапами Shadow P...	4.8 KB	2.0 KB	文本文档	2021-07-24 22:51
ПРОСТАВЛЕНИЕ.txt *	1 KB	1 KB	文本文档	2021-07-24 22:34
Рабочая станция на работу через Tor сеть.txt *	1 KB	1 KB	文本文档	2021-07-24 23:08
Рабочий скрипт создания VPS сервера для тестиро...	1 KB	1 KB	文本文档	2021-07-24 22:59
рклон.zip *	11.9 MB	11.9 MB	360压缩 ZIP 文件	2021-07-24 22:37
Сайт создание батников.txt *	1 KB	1 KB	文本文档	2021-07-24 22:52
Скрипт для sorted .rar *	1 KB	1 KB	360压缩 RAR 文件	2021-07-24 22:53
СМБ АВТОБРУТ.txt *	7.1 KB	2.6 KB	文本文档	2021-07-24 22:47
СНЯТИЕ-AD.rar *	350.7 KB	350.1 KB	360压缩 RAR 文件	2021-07-24 22:32
Список ТГ форумов, много интересного.txt *	1 KB	1 KB	文本文档	2021-07-24 22:49
Установка метаслойт на влс.txt *	1 KB	1 KB	文本文档	2021-07-24 22:52
хантинг админов, прошу ознакомиться, очень пол...	20.5 KB	7.2 KB	文本文档	2021-07-24 22:49
Эксплуатация CVE-2020-1472 Zerologon in Cobalt Stri...	1.2 KB	1 KB	文本文档	2021-07-24 22:55
это установка армитажа. ставится поверх Metasploit...	1 KB	1 KB	文件	2021-07-24 22:54

大小: 83.8 MB 共 55 个文件和 5 个文件夹 压缩率 73.7% 已经选择 1 个文件夹





OWASP

Open Web Application
Security Project

常见应急方法技巧


```
127.0.0.1 - - [11/Jun/2018:12:47:22 +0800] "GET /login.html HTTP/1.1" 200 786 "-"  
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36"
```

来源IP、访问日期、请求方法、请求地址、状态码、浏览器指纹

通过日志查看当天ip连接数, 过滤重复:`cat access_log | grep "20/Oct/2008" | awk '{print $2}' | sort | uniq -c | sort -nr`

当天ip连接数最高的ip都在干些什么:`cat access_log | grep "20/Oct/2008:00" | grep "122.102.7.212" | awk '{print $8}' | sort | uniq -c | sort -nr | head -n 10`

当天访问页面排前10的url:`cat access_log | grep "20/Oct/2008:00" | awk '{print $8}' | sort | uniq -c | sort -nr | head -n 10`

接着从日志里查看该ip在干嘛:`cat access_log | grep 122.102.7.212 | awk '{print $1"\t"$8}' | sort | uniq -c | sort -nr | less`

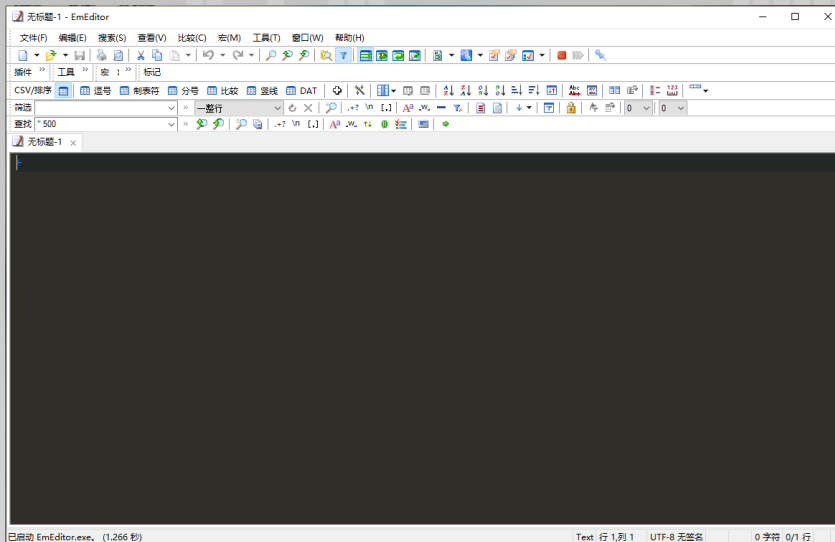
查看某一时间段的ip连接数:`grep "2006:0[7-8]" www20060723.log | awk '{print $2}' | sort | uniq -c | sort -nr | wc -l`



Web日志工具



Emurasoft
EmEditor



新搜索

GET

811,790 个事件 (21/11/30 10:11:45.000 之前) 无事件采样

事件 (811,790) 模式 统计信息 可视化

设置时间线的格式 缩小 缩放到所选区域 取消选择 每列 1 天

日期	事件数
2021年 周三 9月 15日	~10,000
2021年 周三 9月 29日	~10,000
2021年 周二 10月 13日	~110,000
2021年 周三 10月 27日	~10,000
2021年 周三 11月 10日	~10,000

隐藏字段	所有字段	i	_time	主机	数据来源	sourcetype	uri_path	uri
选定字段		>	21/11/18 22:50:09.000	WinDev2108Eval	access.log	access_combined	/mobileweb/buss/PatientByOneself.aspx	/mobileweb/buss/PatientByOneself.aspx
			a host 1					studyid=XJRMYY202111030013
			a root 100+					



分析分类

文件分析

- 文件日期、新增文件、可疑/异常文件、最近使用文件、浏览器下载文件
- Webshell 排查与分析，核心应用关联目录文件分析

进程分析

- 当前活动进程 & 远程连接，启动进程&计划任务，服务

服务系统信息

- 环境变量/账号信息/History/系统配置文件

日志分析

- 安全设备日志/操作系统日志/网站应用日志/其他日志

查看系统信息

- 查看账户信息 `net user` `cat /etc/passwd`
- 检查补丁情况 `systeminfo` `uname -a`
- 查看系统日志 `eventvwr`
- 查看注册表/服务 (Win) `regedit`
- 查看用户连接状况 `netstat` `netstat`
- 查看账户登录状况 `quser` `who / last`
- 搜索近期修改文件 `用眼睛/工具` `find / -ctime -1 -print`
- 查看网站日志 `应用服务log目录` `应用服务log目录`
- 检查数据库修改情况 `数据库日志`
- 查看进程 `任务管理器` `ps -aux`
- 检查防护设备日志 `杀毒软件/IPS/IDS/WAF/日志服务器`



查看linux系统日志

- **/var/log/boot.log**: 录了系统在引导过程中发生的事件, 就是Linux系统开机自检过程显示的信息
- **/var/log/lastlog** : 记录最后一次用户成功登陆的时间、登陆IP等信息
- **/var/log/messages** : 记录Linux操作系统常见的系统和系统服务错误信息
- **/var/log/secure** : Linux系统安全日志, 记录用户和工作组变坏情况、用户登陆认证情况
- **/var/log/btmp** : 记录Linux登陆失败的用户、时间以及远程IP地址
- **/var/log/syslog**: 只记录警告信息, 常常是系统出问题的信息, 使用lastlog查看
- **/var/log/wtmp**: 该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件, 使用last命令查看
- **/var/run/utmp**: 该日志文件记录有关当前登录的每个用户的信息。如 who、w、users、finger等就需要访问这个文件



查看windows系统日志

- **系统：**包含系统进程，设备磁盘活动等。事件记录了设备驱动无法正常启动或停止，硬件失败，重复IP地址，系统进程的启动，停止及暂停等行为。
- **安全：**包含安全性相关的事件，如用户权限变更，登录及注销，文件及文件夹访问，打印等信息。
- **应用程序：**包含操作系统安装的应用程序软件相关的事件。事件包括了错误、警告及任何应用程序需要报告的信息，应用程序开发人员可以决定记录哪些信息。
- **Microsoft：**Microsoft文件夹下包含了200多个微软内置的事件日志分类，只有部分类型默认启用记录功能，如远程桌面客户端连接、无线网络、有线网路、设备安装等相关日志。
- **Microsoft Office Alerts：**微软Office应用程序（包括Word/Excel/PowerPoint等）的各种警告信息，其中包含用户对文档操作过程中出现的各种行为，记录有文件名、路径等信息。
- **Windows PowerShell：**Windows自带的PowerShell应用的日志信息。
- **Internet Explorer：**IE浏览器应用程序的日志信息，默认未启用，需要通过组策略进行配置。



安全设备日志

主机详情

主机资产 安全风险 入侵事件 安全日志

主机信息

系统账号	主机名: [redacted] 16310	主机状态: 在线
端口服务	内网IP: 1 [redacted]	安装时间: 2020-11-18 16:12:02
运行进程	外网IP: 1 [redacted] (拨)	最后上线时间: 2021-11-09 09:18:09
软件应用	操作系统: [redacted] ase 6.5 (Final),64-bit	最后下线时间: 2021-11-09 09:18:05
Web服务	内核版本: 2 [redacted] 6.x86_64	AgentID: [redacted]
Web站点	系统启动时间: [redacted] 06-27 08:02:57	Agent版本: 3 [redacted] 2021-07-12_09-58-20-128
Web应用	代理服务器: --	Bash插件: [redacted]
Web框架	管理信息	负责人邮箱: --
数据库	负责人: --	固定资产编号: --
系统安装包	机房位置: --	
Jar包	备注: --	
启动服务	硬件配置	
计划任务	生产商: O [redacted]	
环境变量	设备型号: C [redacted]	
内核模块	序列号: 7dbf9 [redacted] 3d [redacted] 4-0 [redacted]	
	设备UUID: D30 [redacted] 35 [redacted] 03	
	内存: 32GB, [redacted]	
	CPU: GenuineIn [redacted] [redacted] 系统负载: 低	
	网卡信息	
	网卡名称: eth1	网卡名称: lo
	MAC地址: fa:16 [redacted] 7	MAC地址: [redacted] :00:00:00:00
	IPv4: [redacted]	IPv4: [redacted]



常用工具

- **啊D Webshell检测**：用来检测大量网页源代码中是否包含恶意代码，业内评价较高，适用于win环境下面支持较多种脚本语言。
- **牧云 (CloudWalker)**：长亭推出的一款开源服务器安全管理平台，目前仅包含 Webshell 检测引擎部分，重点调优 Webshell 检测效果，适用于linux环境下面支持较多种脚本语言。
- **ProcessExplorer_v16.21.Chs**：进程管理神器，免费专业增强型任务管理器，系统和应用程序监视工具。它能管理隐藏在后台运行的进程，可以监视/挂起/重启/强行终止任何程序，包括系统级的不允许随便终止的关键进程等。
- **PCHunter**：PC Hunter是一个Windows系统信息查看软件，同时也是一个手工杀毒辅助软件。目前软件支持xp~win10的所有32位操作系统，还支持64位的Win7、Win8、Win8.1和Win10系统。
- **IDA**：交互式反汇编器专业版 (Interactive Disassembler Professional)，人们常称其为IDA Pro，或简称为IDA。是目前最棒的一个静态反编译软件，为众多0day世界的成员和ShellCode安全分析人士不可缺少的利器
- **EmEditor**：一款文本编辑器，特点是可以编辑超大文本极大的方便了应急响应工作。



应急处理流程

- **X情报社区** **网址：** <https://x.threatbook.cn/>。
- **virustotal威胁情报** **网址：** <https://www.virustotal.com/>
- **360勒索解密** **网址：** <http://lesuobingdu.360.cn/>
- **nomoreransom** **网址：** <https://www.nomoreransom.org/>



日志提取



- 浏览器
- Mstsc远程桌面
- Navicat 客户端
- Xshell客户端
- 等等...

- 日志服务器
- 负载
- 堡垒机
- 代理服务器
- IPS
- IDS
- 态势感知
- HIDS

- 系统安全日志
- Web应用日志
- 被删日志
- 等....

- 微步
- 暗网
- 等....



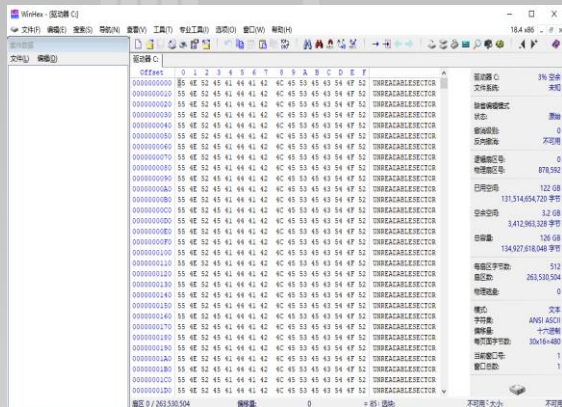
链路日志>应用服务器日志

安全设备日志>常规日志

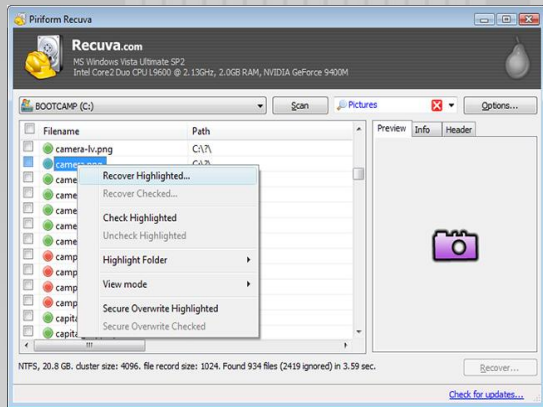
链路日志的真实性优先于应用服务器日志，相同事件也可以通过多个设备日志来辅助判断，安全设备记录的攻击日志通常会比常规日志详细



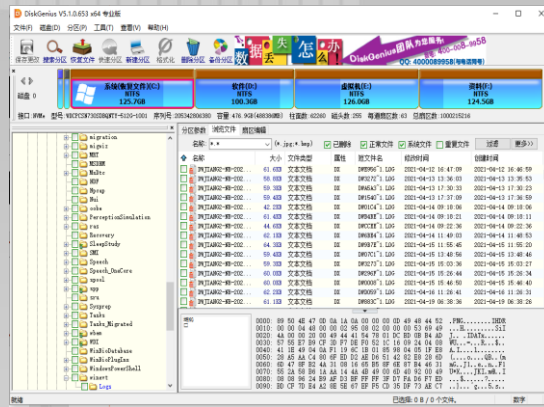
日志恢复



winhex



recuva



DiskGenius
专业版



日志恢复

工作中经常遇到恶意文件会把日志清空，我们推测系统是通过弱口令攻击成功的，但是我们最好能给出排查的依据确保万无一失。

通过调研为了适应多环境我们最终采用了volatility取证软件，windows内存镜像采用DumpIt，他们分别长这样：

```
C:\Users\Administrator>
DumpIt - v1.3.2.20110
Copyright (c) 2007 -
Copyright (c) 2010 -

Address space size:
Free space size:

* Destination = \??
--> Are you sure yo
```

```
C:\Users\Administrator\Desktop\volatility_2.6_win64_standalone>volatility.exe -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help                list all available options and their default values.
                             Default values may be set in the configuration file
                             (/etc/volatilityrc)

  --conf-file=.volatilityrc User based configuration file

  -d, --debug                Debug volatility

  --plugins=PLUGINS         Additional plugin directories to use (semi-colon
                             separated)

  --info                     Print information about all registered objects

  --cache-directory=C:\Users\Administrator\.cache\volatility
                             Directory where cache files are stored

  --cache                    Use caching

  --tz=TZ                    Sets the (Olson) timezone for displaying timestamps
                             using pytz (if installed) or tzset

  -f FILENAME, --filename=FILENAME
                             Filename to use when opening an image

  --profile=WinXPSP2x86     Name of the profile to load (use --info to see a list
```



日志恢复

```
>>volatility -f 镜像 imageinfo
>>volatility -f 镜像 --profile=系统版本 filescan
>>volatility -f 镜像 --profile=系统版本 dumpfiles -Q 内存地址 -D 输出地址
```

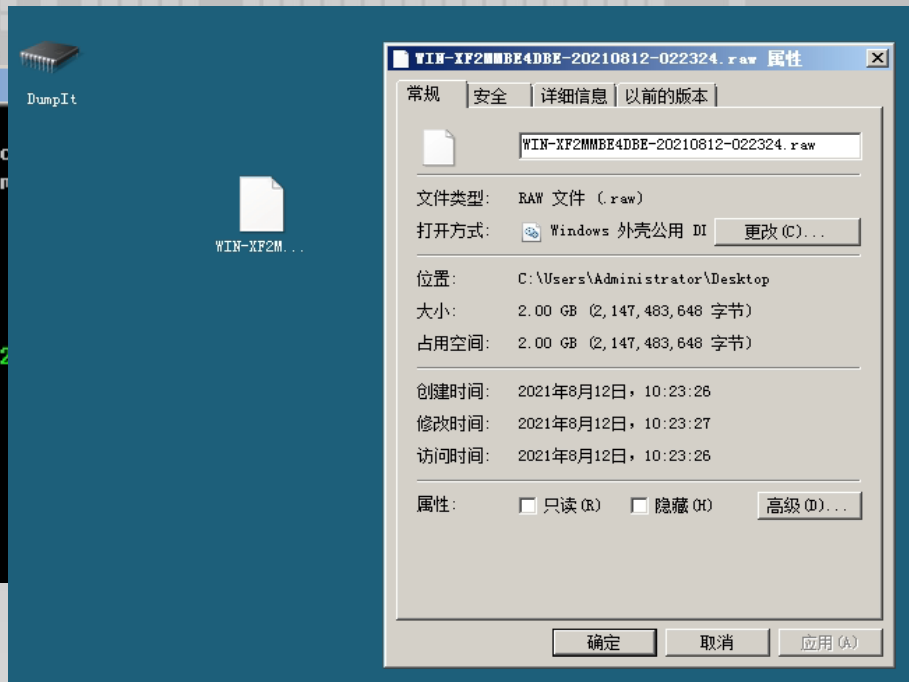
```
C:\Users\Administrator\Desktop>DumpIt.exe

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.com>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      2147483648 bytes <  2048 Mb>
Free space size:        38223355904 bytes < 36452 Mb>

* Destination = \\?\C:\Users\Administrator\Desktop\WIN-XF2
022324.raw

--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```



日志恢复

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator\Desktop>volatility.exe
.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining pr
          Suggested Profile(s) : Win2008SP2x64
aSP2x64
          AS Layer1 : WindowsAMD64P
          AS Layer2 : FileAddressSp
p\WIN-XF2MMBE4DBE-20210812-022324.raw>
          PAE type : No PAE
          DTB      : 0x124000L
          KDBG     : 0xf800019d1f0
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0       : 0xfffff800019
KPCR for CPU 1       : 0xfffffa60005
KUSER_SHARED_DATA    : 0xfffff780000
Image date and time  : 2021-08-12 02
Image local date and time : 2021-08-12 10

管理员: C:\Windows\system32\cmd.exe
0x000000007fb68390 16 0 R--r-- \Device\HarddiskVolume1\Windows\System32
\CodeIntegrity\driver.stl
0x000000007fb6d390 3 0 RW-rwd \Device\HarddiskVolume1\Directory
0x000000007fb77390 33 0 RW-rwd \Device\HarddiskVolume1\Directory
0x000000007fba4580 3 0 RW-rwd \Device\HarddiskVolume1\MftMirr
0x000000007fba54e0 22 0 RW-rwd \Device\HarddiskVolume1\Mft
0x000000007fbb0300 7 0 R--r-- \Device\HarddiskVolume1\Windows\System32
\CodeIntegrity\bootcat.cache
0x000000007fbb0570 3 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\CertEnroll.dll
0x000000007fbb0b20 33 0 RW-rwd \Device\HarddiskVolume1\Mft
0x000000007fbd5730 1 1 RW---- \Device\HarddiskVolume1\Windows\System32
\config\SOFTWARE
0x000000007fbd7730 32 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\drivers\khdc.class.sys
0x000000007fbd86e0 32 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\drivers\nouclass.sys
0x000000007fbd9700 32 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\drivers\lsi_sas.sys
C:\Users\Administrator\Desktop>volatility.exe -f WIN-XF2MMBE4DBE-20210812-022324
.raw --profile=Win2008SP2x64 filescan > filescan.txt
Volatility Foundation Volatility Framework 2.6
C:\Users\Administrator\Desktop>
```

日志恢复

filescan - 记事本

文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)
0x000000007e6e3c80			20	
0x000000007e6e5930			1	
0x000000007e6e61b0			9	
0x000000007e6e64d0			16	
0x000000007e6e6ce0			10	
0x000000007e6e7050			12	
0x000000007e6e7be0			20	
0x000000007e6e7d10			3	
0x000000007e6e82b0			3	
0x000000007e6e8460			8	
0x000000007e6e9690			1	
0x000000007e6e9980			6	
0x000000007e6e9ab0			15	
0x000000007e6eac30			3	
0x000000007e6eb330			15	
0x000000007e6eb460			12	
0x000000007e6ecb90			1	
0x000000007e6ed410			11	
0x000000007e6ee750			12	
0x000000007e6eeb10			13	
0x000000007e6ef270			3	
0x000000007e6ef4e0			15	
0x000000007e6f0050			1	

管理员: C:\Windows\system32\cmd.exe

```
\drivers\kbdclass.sys
0x000000007fbd86e0 32 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\drivers\mouclass.sys
0x000000007fbd700 32 0 R--r-d \Device\HarddiskVolume1\Windows\System32
\drivers\lsi_sas.sys

C:\Users\Administrator\Desktop>volatility.exe -f WIN-XF2MMBE4DBE-20210812-022324
.raw --profile=Win2008SP2x64 filescan > filescan.txt
Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator\Desktop>volatility.exe -f WIN-XF2MMBE4DBE-20210812-022324
.raw --profile=Win2008SP2x64 dumpfiles -Q 0x000000007e6e7be0 -D C:\Users\Adminis
trator\Desktop>
命令语法不正确。

C:\Users\Administrator\Desktop>volatility.exe -f WIN-XF2MMBE4DBE-20210812-022324
.raw --profile=Win2008SP2x64 dumpfiles -Q 0x000000007e6e7be0 -D C:\Users\Adminis
trator\Desktop
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e6e7be0 None \Device\HarddiskVolume1\Windows\System32\w
inevt\Logs\Security.evtx
SharedCacheMap 0x7e6e7be0 None \Device\HarddiskVolume1\Windows\System32\wine
vt\Logs\Security.evtx

C:\Users\Administrator\Desktop>
```

日志恢复

```
选择toor@dwjiang2-nb: /tmp
-rw-r--r-- 1 toor toor 262144 Aug 12 14:38 file.None.0xfffffa80030e8010.vacb
toor@dwjiang2-nb:/tmp$ chmod 777 evtextract
toor@dwjiang2-nb:/tmp$ ./evtextract file.None.0xfffffa80030e8010.vacb output.xml
usage: evtextract [-h] [-v] [-q] input
evtextract: error: unrecognized arguments: output.xml
toor@dwjiang2-nb:/tmp$ ./evtextract file.None.0xfffffa80030e8010.vacb > output.xml
INFO:root:recovered 114 complete records
INFO:root:recovered 0 incomplete records
toor@dwjiang2-nb:/tmp$ ll
total 4388324
drwxrwxrwt 1 root root 4096 Aug 12 14:47 /
drwxr-xr-x 1 root root 4096 Jul 7 10:27 ../
-rw-r--r-- 1 toor toor 2241210811 Jul 8 14:06 20210630-705.log
-rw-r--r-- 1 toor toor 5156666370 Jul 7 10:25 2021063000.log
-rw-r--r-- 1 toor toor 523517262 Jul 7 13:09 2021070100.log
-rw-r--r-- 1 toor toor 461182195 Jul 7 13:11 2021070200.log
-rw-r--r-- 1 toor toor 90241180 Jul 7 13:12 2021070300.log
-rw-r--r-- 1 toor toor 92410536 Jul 7 13:13 2021070400.log
-rw-r--r-- 1 toor toor 558193268 Jul 7 13:15 2021070500.log
-rwxrwxrwx 1 toor toor 10684960 Aug 12 14:24 evtextract*
-rw-r--r-- 1 toor toor 262144 Aug 12 14:38 file.None.0xfffffa80030e8010.vacb
-rw-r--r-- 1 toor toor 141338 Aug 12 14:47 output.xml
toor@dwjiang2-nb:/tmp$ cat output.xml
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4
994-a5ba-3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4608</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12288</Task>
<Opcode>0</Opcode>
<Keywords>0x802000000000000</Keywords>
<TimeCreated SystemTime="2021-08-12 01:49:33.988970"></TimeCreated>
<EventRecordID>1</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="576" ThreadID="580"></Execution>
```



巧用监控小工具

Auditctl有什么用

- 查看文件访问
- 监控系统调用
- 记录用户指令的cmd指令
- 记录系统安全事件 (如入侵行为)
- 监控网络访问

Auditctl优势

- 多个系统自带
- 操作简单
- 功能丰富

安装过程

- yum -y install auditd
- sudo apt-get install auditd

```
[root@iZ2zebpef08x6a2h5quoxvZ ~]# auditctl
usage: auditctl [options]
-a <l,a>          Append rule to end of <l>ist with <a>ction
-A <l,a>          Add rule at beginning of <l>ist with <a>ction
-b <backlog>     Set max number of outstanding audit buffers
                  allowed Default=64
-c              Continue through errors in rules
-C f=f          Compare collected fields if available:
                  Field name, operator(=,!=), field name
-d <l,a>        Delete rule from <l>ist with <a>ction
                  l=task,exit,user,exclude
                  a=never,always
-D              Delete all rules and watches
-e [0..2]       Set enabled flag
-f [0..2]       Set failure flag
                  0=silent 1=printk 2=panic
-F f=v          Build rule: field name, operator(=,!=,<,>,<=,
                  >=,&,&=) value
-h              Help
-i              Ignore errors when reading rules from file
-k <key>        Set filter key on audit rule
-l              List rules
-m text         Send a user-space message
-p [r|w|x|a]    Set permissions filter on watch
                  r=read, w=write, x=execute, a=attribute
-q <mount,subtree> make subtree part of mount point's dir watches
-r <rate>       Set limit in messages/sec (0=none)
-R <file>       read rules from file
-s              Report status
-S syscall      Build rule: syscall name or number
-t              Trim directory watches
-v              Version
-w <path>       Insert watch at <path>
-W <path>       Remove watch at <path>
--loginuid-immutable Make loginuids unchangeable once set
--reset-lost    Reset the lost record counter

[root@iZ2zebpef08x6a2h5quoxvZ ~]#
```



巧用监控小工具

Auditctl常用命令

service auditd status

auditctl -l

auditctl -w 文件-p rwx -k “标记名”

auditctl -w /etc/ -p wa

service auditd start

service auditd restart

ausearch -k “标记名”

#查看服务状态

#查看监控规则

#建立文件监控

#建立文件夹监控

#服务启动

#服务重启

#查看记录

```
[root@iZ2zebpef08x6a2h5quoxvZ /]# service auditd status
Redirecting to /bin/systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; disabled; vendor preset: enabled)
   Active: inactive (dead) since Wed 2021-08-11 19:15:12 CST; 48s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 1136 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Process: 1131 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Main PID: 1132 (code=exited, status=0/SUCCESS)

Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: lost 0
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: backlog 1
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: enabled 1
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: failure 1
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: pid 1132
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: rate_limit 0
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: backlog_limit 8192
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: lost 0
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ augenrules[1136]: backlog 1
Aug 11 14:00:13 iZ2zebpef08x6a2h5quoxvZ systemd[1]: Started Security Auditing Service.
[root@iZ2zebpef08x6a2h5quoxvZ /]# auditctl -l
No rules
```



巧用监控小工具

```
root@x:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
time->Wed Aug 11 14:06:21 2021
type=PROCTITLE msg=audit(1628661981.191:51): proctitle=766900706173737764
type=PATH msg=audit(1628661981.191:51): item=0 name="passwd" inode=1189189 dev=fe:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1628661981.191:51): cwd="/tmp"
type=SYSCALL msg=audit(1628661981.191:51): arch=c000003e syscall=2 success=yes exit=3 a0=7ac710 a1=0 a2=0 a3=7ffe6218bda0 items=1 ppid=1198 pid=1227 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=15 comm="vi" exe="/usr/bin/vi" key="sec"
----
time->Wed Aug 11 14:06:21 2021
type=PROCTITLE msg=audit(1628661981.192:52): proctitle=766900706173737764
type=PATH msg=audit(1628661981.192:52): item=0 name="passwd" inode=1189189 dev=fe:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1628661981.192:52): cwd="/tmp"
type=SYSCALL msg=audit(1628661981.192:52): arch=c000003e syscall=89 success=no exit=-22 a0=7ffe6218a3f0 a1=7ffe6218b430 a2=fff a3=7ffe621897e0 items=1 ppid=1198 pid=1227 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=15 comm="vi" exe="/usr/bin/vi" key="sec"
----
time->Wed Aug 11 14:06:47 2021
type=PROCTITLE msg=audit(1628662007.594:53): proctitle=766900706173737764
type=PATH msg=audit(1628662007.594:53): item=0 name="passwd" inode=1189189 dev=fe:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1628662007.594:53): cwd="/tmp"
type=SYSCALL msg=audit(1628662007.594:53): arch=c000003e syscall=191 success=no exit=-61 a0=7ac710 a1=7efd013dde2f a2=7ffe6218c380 a3=84 items=1 ppid=1198 pid=1227 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=15 comm="vi" exe="/usr/bin/vi" key="sec"
----
time->Wed Aug 11 14:06:47 2021
type=PROCTITLE msg=audit(1628662007.594:54): proctitle=766900706173737764
type=PATH msg=audit(1628662007.594:54): item=1 name="passwd" inode=1189189 dev=fe:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1628662007.594:54): item=0 name="/tmp" inode=1179649 dev=fe:01 mode=041777 ouid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1628662007.594:54): cwd="/tmp"
type=SYSCALL msg=audit(1628662007.594:54): arch=c000003e syscall=2 success=yes exit=3 a0=7ac710 a1=241 a2=1a4 a3=0 items=2 ppid=1198 pid=1227 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=15 comm="vi" exe="/usr/bin/vi" key="sec"
----
time->Wed Aug 11 14:06:47 2021
type=PROCTITLE msg=audit(1628662007.599:55): proctitle=766900706173737764
type=PATH msg=audit(1628662007.599:55): item=0 name="passwd" inode=1189189 dev=fe:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1628662007.599:55): cwd="/tmp"
type=SYSCALL msg=audit(1628662007.599:55): arch=c000003e syscall=90 success=yes exit=0 a0=7ac710 a1=81a4 a2=0 a3=81f5a0 items=1 ppid=1198 pid=1227 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=15 comm="vi" exe="/usr/bin/vi" key="sec"
sec
```



内容篡改

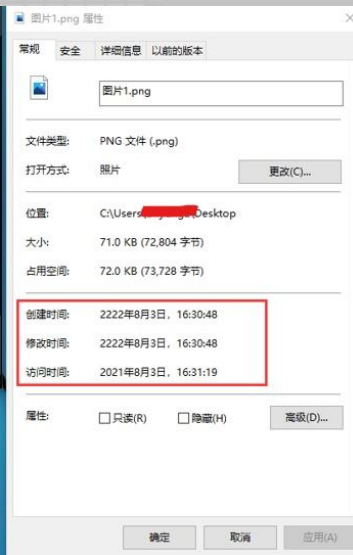
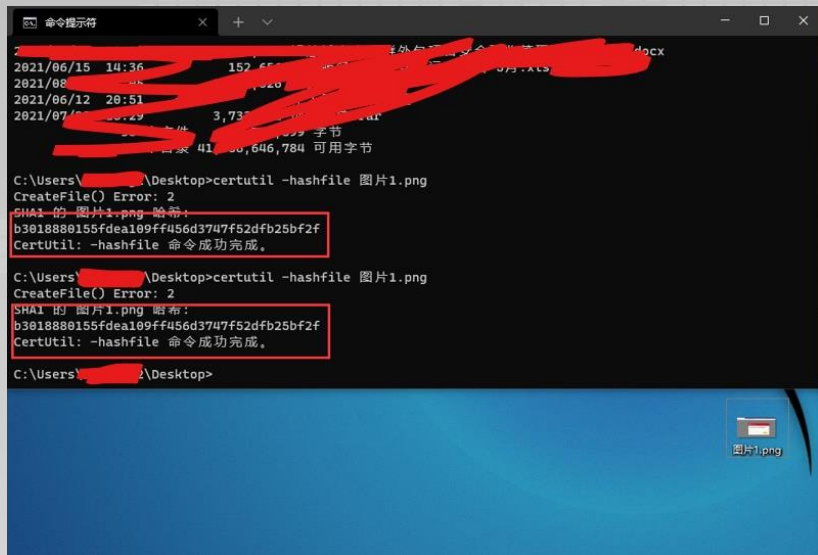
众多应用像nginx tomcat liunx安全日志都是常规的txt log
模式很容易被篡改，你只需要打开日志文件就可以随意进行增删改除

```
1 192.168.1.240 - - [16/Nov/2021:21:44:37 +0800] "GET /e HTTP/1.1" 500 177 "-" "Mozilla/5.0"
2 192.168.1.240 - - [16/Nov/2021:21:52:22 +0800] "GET /ext HTTP/1.1" 500 177 "-" "Mozilla/5.0"
3 192.168.1.240 - - [16/Nov/2021:22:11:00 +0800] "POST /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "kSOAP/2.0"
4 192.168.1.240 - - [16/Nov/2021:22:11:00 +0800] "POST /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "kSOAP/2.0"
5 192.168.1.240 - - [16/Nov/2021:22:11:00 +0800] "POST /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "kSOAP/2.0"
6 192.168.31.103 - - [16/Nov/2021:22:27:19 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
7 192.168.31.103 - - [16/Nov/2021:22:27:22 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
8 192.168.31.103 - - [16/Nov/2021:22:27:24 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
9 192.168.31.103 - - [16/Nov/2021:22:27:38 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
10 192.168.31.103 - - [16/Nov/2021:22:27:43 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
11 192.168.31.103 - - [16/Nov/2021:22:27:45 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
12 192.168.31.103 - - [16/Nov/2021:22:27:46 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
13 192.168.31.103 - - [16/Nov/2021:22:27:59 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
14 192.168.31.103 - - [16/Nov/2021:22:29:08 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
15 192.168.31.103 - - [16/Nov/2021:22:30:15 +0800] "GET /services/SearchInterface? HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
16 192.168.31.103 - - [16/Nov/2021:22:30:19 +0800] "GET /services/SearchInterf HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
17 192.168.31.103 - - [16/Nov/2021:22:30:25 +0800] "GET /services/SearchInterf HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
18 192.168.31.103 - - [16/Nov/2021:22:30:26 +0800] "GET /services/SearchInterf HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
19 192.168.31.103 - - [16/Nov/2021:22:30:33 +0800] "GET /services.SearchInterf HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
20 192.168.31.103 - - [16/Nov/2021:22:30:36 +0800] "GET /services.SearchInter HTTP/1.1" 404 555 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
21 192.168.31.103 - - [16/Nov/2021:22:30:49 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
22 192.168.31.103 - - [16/Nov/2021:22:30:53 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
23 192.168.31.103 - - [16/Nov/2021:22:30:54 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
24 192.168.31.103 - - [16/Nov/2021:22:30:55 +0800] "GET /services/SearchInterface?wsdl HTTP/1.1" 500 494 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36"
```



文件属性

文件更改时间不会改变hash



Windows系统日志

DanderSpritz是NSA的一款界面化的远控工具

常用命令如下:

(1) 统计日志列表, 查询所有日志信息, 包含时间, 数目

`eventlogquery -log Application`

(2) 查看指定类别的日志内容

`eventlogfilter -log Application -num 10`

(3) 删除该类日志所有内容

`eventlogclear -log Application`

(4) 删除单条内容

`eventlogedit -log Application -record 1`

The image displays two screenshots of the Windows Event Viewer application. The top screenshot shows the 'System' log with 4 events. The bottom screenshot shows the 'System2' log with 3 events.

System 事件数: 4

级别	日期和时间	来源	事件 ID	任务类别
信息	2018/6/4 15:21:19	Service Control Manager	7036	无
信息	2018/6/4 15:21:09	Service Control Manager	7036	无
信息	2018/6/4 15:21:09	Virtual Disk Service	3	无
信息	2018/6/4 15:20:21	Eventlog	104	日志清除

System2 事件数: 3

级别	日期和时间	来源	事件 ID	任务类别
信息	2018/6/4 15:21:09	Service ...	7036	无
信息	2018/6/4 15:21:09	Virtual D...	3	无
信息	2018/6/4 15:20:21	Eventlog	104	日志清除

Windows系统日志

- 1.确定时间范围
- 2.删除时间范围内日志

wevtutil epl Security 1.evtx "/q:*[System [TimeCreated[@SystemTime >'2018-08-10T03:21:00' or @SystemTime <'2018-08-10T03:20:00']]"

- 3.覆盖原有日志

```
选择命令提示符

命令:
e1 | enum-logs          列出日志名称。
gl | get-log           获取日志配置信息。
sl | set-log           修改日志配置信息。
ep | enum-publishers  列出事件发布者。
gp | get-publisher    获取事件发布者信息。
im | install-manifest 从清单中安装事件发布者。
um | uninstall-manifest 从清单中卸载事件发布者。
qe | query-events     从日志文件中查询事件。
gli | get-log-info    获取日志信息。
ep1 | export-log      导出日志。
al | archive-log      存档日志。
cl | clear-log        清除日志。

常用选项:
/r {remote}:VALUE
如果指定,则在远程计算机上运行该命令。VALUE 是远程计算机名称。
/im 和 /um 选项不支持远程操作。

/lu {username}:VALUE
指定一个不同的用户以登录到远程计算机。
VALUE 是 domain/user 或 user 形式的用户名。只有在指定 /r 选项时才适用。

/ps {password}:VALUE
指定的用户密码。如果未指定,
或者 VALUE 为 *, 则会提示用户输入密码。
只有在指定 /lu 选项时才适用。

/fa {authentication}:[Default|Negotiate|Kerberos|NTLM]
用于连接到远程计算机的身份验证类型。默认为 Negotiate。

/uni {unicode}:[true|false]
使用 Unicode 显示输出。如果为 true, 则使用 Unicode 显示输出。

要了解特定命令的详细信息, 请键入以下命令:
```


linux系统日志

- 1.确定时间范围
- 2.删除时间范围内日志

wevtutil epl Security 1.evtx "/q:*[System [TimeCreated[@SystemTime >'2018-08-10T03:21:00' or @SystemTime <'2018-08-10T03:20:00']]"

- 3.覆盖原有日志

```
选择命令提示符

命令:
e1 | enum-logs          列出日志名称。
gl | get-log           获取日志配置信息。
sl | set-log           修改日志配置信息。
ep | enum-publishers  列出发布者。
gp | get-publisher    获取发布者信息。
im | install-manifest 从清单中安装事件发布者。
um | uninstall-manifest 从清单中卸载事件发布者。
qe | query-events     从日志文件中查询事件。
gli | get-log-info    获取日志信息。
ep1 | export-log      导出日志。
al | archive-log      存档日志。
cl | clear-log        清除日志。

常用选项:
/r {r | remote}:VALUE
如果指定,则在远程计算机上运行该命令。VALUE 是远程计算机名称。
/im 和 /um 选项不支持远程操作。

/lu {u | username}:VALUE
指定一个不同的用户以登录到远程计算机。
VALUE 是 domain/user 或 user 形式的用户名。只有在指定 /r 选项时才适用。

/ps {p | password}:VALUE
指定的用户密码。如果未指定,
或者 VALUE 为 *, 则会提示用户输入密码。
只有在指定 /u 选项时才适用。

/fa {a | authentication}:[Default|Negotiate|Kerberos|NTLM]
用于连接到远程计算机的身份验证类型。默认为 Negotiate。

/uni {uni | unicode}:[true|false]
使用 Unicode 显示输出。如果为 true, 则使用 Unicode 显示输出。

要了解特定命令的详细信息, 请键入以下命令:
```

liunx系统更改

master 1 branch 0 tags [Go to file](#) [Code](#)

AV1080p Update README.md 9df7aee on 6 Jun 2017 6 commits

README.md	Update README.md	5 years ago
logtamper.py	Update logtamper.py	5 years ago

README.md

logtamper

python修改linux日志

使用

躲避管理员w查看

```
python logtamper.py -m 1 -u re4lity -i 192.168.0.188
```

清除指定ip的登录日志

```
python logtamper.py -m 2 -u re4lity -i 192.168.0.188
```

修改上次登录时间地点

```
python logtamper.py -m 3 -u re4lity -i 192.168.0.188 -t tty1 -d 2014:05:28:10:11:12
```

About

python修改linux日志

Readme

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%





OWASP

Open Web Application
Security Project

实际案例

案例1

问题背景:

2021年中某客户项目现场域控服务器存在勒索病毒DNS请求, 域控服务器疑似感染勒索病毒

The screenshot displays a security dashboard for a ransomware attack event. The main title is "勒索病毒WannaCry尝试通信" (Ransomware WannaCry Attempt Communication). The event is categorized as "攻击者" (Attacker) using the "勒索病毒WannaCry尝试通信" (Ransomware WannaCry Attempt Communication) attack method, targeting 1 server and launching 3 attacks.

Key details include:

- Source: 英国-Wales-Swansea (United Kingdom - Wales - Swansea)
- Destination: 199.7.83.42/美国-California-Los Angeles (United States - California - Los Angeles)
- Attack Chain Stage: 安装工具 (Installation Tool)
- Disposal Status: 新建 (New)
- Event Category: 威胁类 (Threat Class)
- Start/End Time: 2021-07-11 09:59:52 ~ 2021-07-11 16:24:21
- Analysis Type: 告警分析 (Alert Analysis)
- Threat Level: 较大 (Significant)
- Attack Features: --
- Device Source: UTS_
- Confidence: 高 (High)
- Response Code: --
- Attack Direction: 未知 (Unknown)
- Device Action: 允许 (Allow)

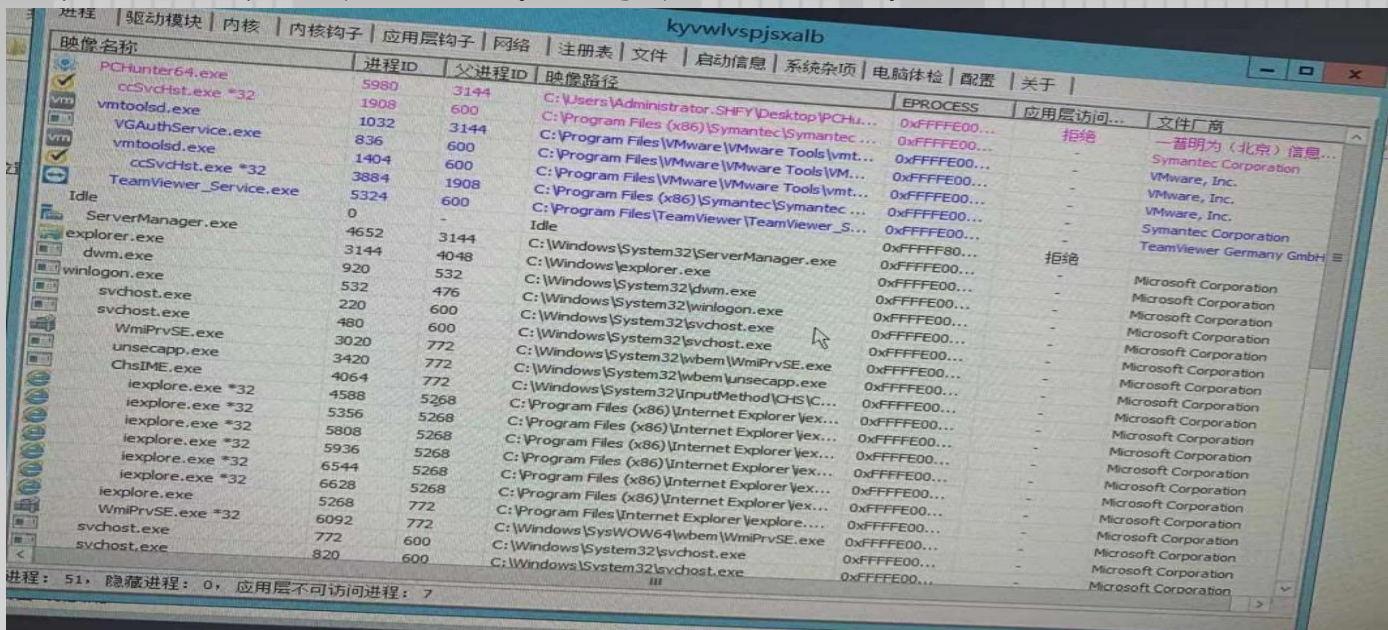
The "攻击过程" (Attack Process) section shows a log entry for "2021-07-11 09:59:52" with the tool "安装工具". The event name is "勒索病毒WannaCry尝试通信". The attack result is "企图" (Attempt) with 3 attack attempts. The "载荷" (Payload) section shows the following data:

```
8lxxYEwc/AZ
P
IE_~,5*5KFMww)iuqerfsodp9ifjaposdfjhgosurijfaewrgweacom
```



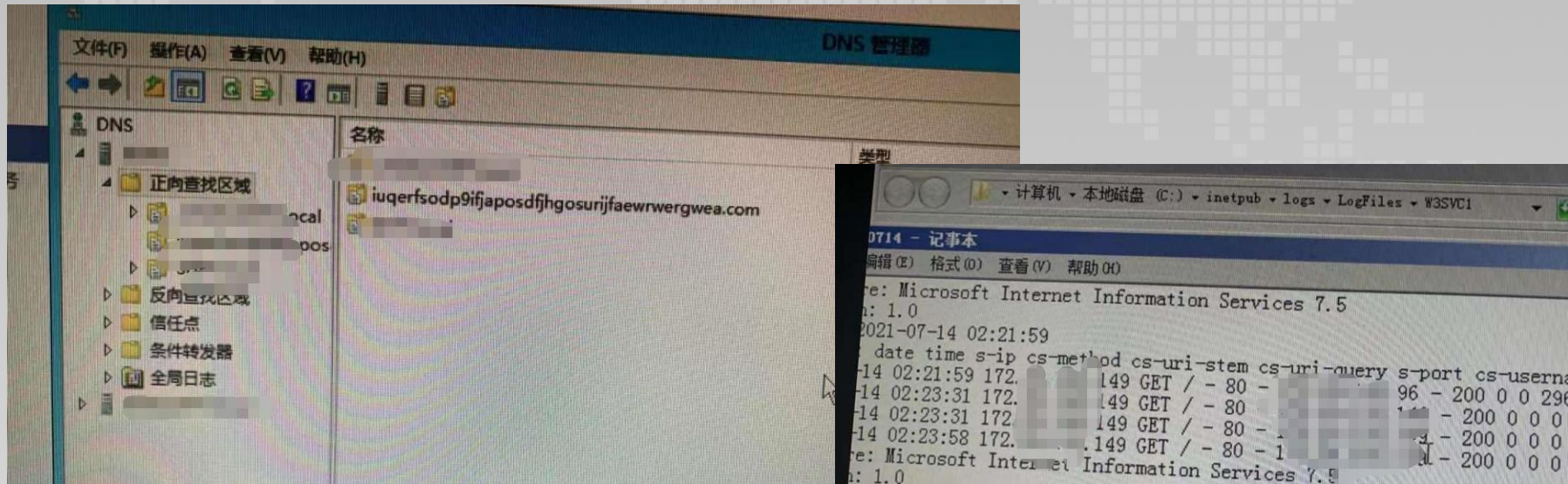
案例1

域控安全排查：对服务器进行进程、网络、启动项、账号等信息进行排查后发现该服务器并未感染病毒或者后门进程。



案例1

经过排查是内网众多个人PC机器感染勒索病毒通过域控转发DNS请求，最后通过在域控自定义转发勒索病毒的域名，通过自建IIS打印访问IP，获取内网感染情况并顺利清理所有客户端病毒



案例2

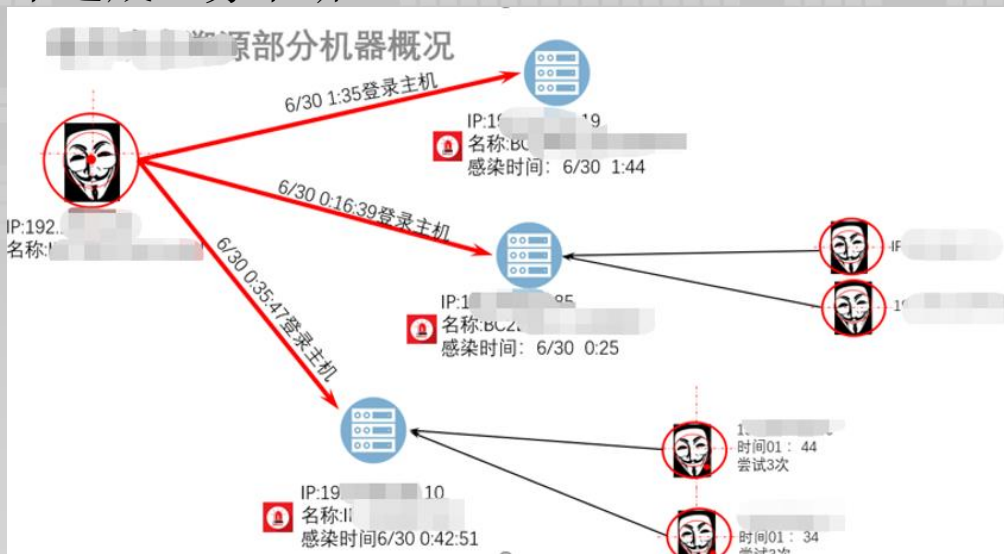
问题背景：运维系统发现多个业务服务器出现异常，经过排查已经感染勒索病毒
希望协助处理

处理过程：现场检查后已经关闭多个高危端口，并且补丁已经通过内网
补丁服务器更新到最新



案例2

最后经过排查服务器是经过运维机器感染Sodinokibi勒索病毒，因为运维服务器已经格式化处理无法继续溯源，因感染服务器为边缘化服务器，且数据备份所以侥幸未造成业务中断



案例3

问题背景：web代理服务器攻击第三方数据库，导致第三方服务器崩溃，无法正常使用

排查经过：检查应用服务器和代理服务器均无后门，web日志未发现CC或者其他异常，但是代理服务器发现卡巴斯基记录半连接攻击，但是第三方数据日志通过一个星期交涉都未拿到



案例3

排查结果，通过Nginx代理报错日志发现Nginx连接数近日一直处于高并发状态，但是客户端请求很低，通过日志比对确认无误不是CC攻击，最后通过Nginx访问状态码确认数据库已经于事发前两天就无法工作，数据库重启后导致我司网站程序Druid处于一直链接状态导致访问数据库连接数较高。

安全活动						
卡巴斯基半连接攻击		发生	发生	发生	发生	
Nginx连接数超1024		发生	发生	发生	发生	
日期	15日	16日	17日	18日	19日	20日





OWASP

Open Web Application
Security Project

Thank you!