干货|windows日志检索和分析

江苏智慧安全可信 乌雲安全 今天

收录于话题
#应急响应
1个 >

前言

在运维工作过程中，如若windows服务器被入侵，往往需要检索和分析相应的安全日志。除了安全设备，系统自带的日志就是取证的关键材料，但是此类日志数量庞大，需要高效分析windows安全日志，提取出我们想要的有用信息，就显得尤为关键。

本文将介绍windows的日志类型、存放位置、检索方案以及方便检索的工具使用方法。

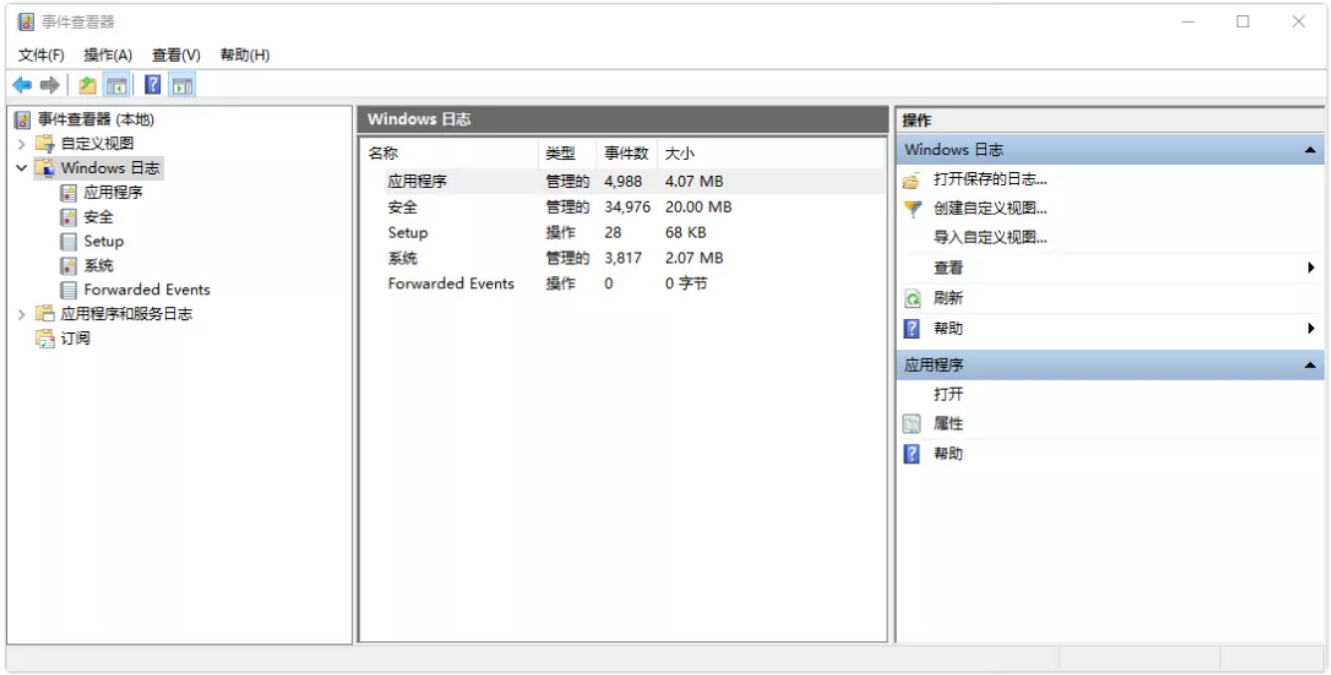
Windows日志

在windows系统的运行过程中会不断记录日志信息，根据种类可以分为事件日志、IIS日志、FTP日志，数据库日志，邮件服务日志等。

事件日志

Windows事件日志文件实际上是以特定的数据结构的方式存储内容，其中包括有关系统，安全，应用程序的记录。每个记录事件的数据结构中包含了9个元素（可以理解成数据库中的字段）：日期/时间、事件类型、用户、计算机、事件ID、来源、类别、描述、数据等信息。运维人员可以根据日志取证，了解计算机所发生的具体行为。

开始-运行，输入 eventvwr.msc 打开事件查看器，查看日志



可以看到，事件查看器将日志分成了2大类，windows日志、应用程序和服务日志，windows日志中又有应用程序、安全、setup、系统、forwarded event这几种事件类型。以下将分别介绍：

事件类型

- 应用程序日志

包含由应用程序或系统程序记录的事件，主要记录程序运行方面的事件，例如数据库程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视哪些事件。如果某个应用程序出现崩溃情况，那么我们可以从程序事件日志中找到相应的记录，也许会有助于问题的解决。

默认位置:

```
%SystemRoot%\System32\Winevt\Logs\Application.evtx
```

- 系统日志

记录操作系统组件产生的事件，主要包括驱动程序、系统组件和应用软件的崩溃以及数据丢失错误等。系统日志中记录的时间类型由Windows NT/2000操作系统预先定义。

默认位置:

```
%SystemRoot%\System32\Winevt\Logs\System.evtx
```

•安全日志

包含由应用程序或系统程序记录的事件，主要记录程序运行方面的事件，例如数据库程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视哪些事件。如果某个应用程序出现崩溃情况，那么我们可以从程序事件日志中找到相应的记录，也许会有助于你解决问题。

默认位置:

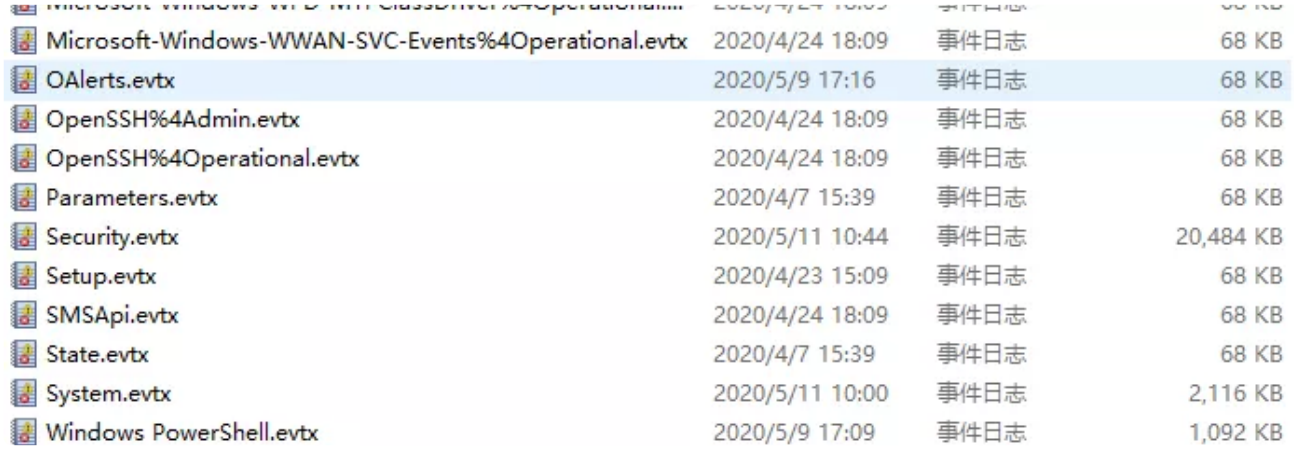
```
%SystemRoot%\System32\Winevt\Logs\Application.evtx
```

•转发事件

日志用于存储从远程计算机收集的事件。若要从远程计算机收集事件，必须创建事件订阅。

默认位置:

```
%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx
```



事件级别

在事件日志中有5个事件级别。

•信息

信息事件指应用程序、驱动程序或服务的成功操作的事件。

•警告

警告事件指不是直接的、主要的，但是会导致将来发生问题的事件。例如，当磁盘空间不足或未找到打印机时，都会记录一个“警告”事件。

•错误

错误事件指用户须知道的重要的问题，通常包括功能和数据的丢失。例如,如果一个服务不能作为系统引导被加载，那么它将会产生一个错误事件。

•成功审核

成功的审核安全访问尝试，主要是指安全性日志，这里记录着用户登录/注销、对象访问、特权使用、账户管理、策略更改、详细跟踪、目录服务访问、账户登录等事件，例如所有的成功登录系统都会被记录为“ 成功审核”事件。

•失败审核

失败的审核安全登录尝试，例如用户试图访问网络驱动器失败，则该尝试会被作为失败审核事件记录下来。

事件ID

Windows 的日志以事件 id 来标识具体发生的动作行为，可通过下列网站查询具体 id 对应的操作

- https://docs.microsoft.com/en-us/windows/security/threat-protection/ 直接搜索 event + 相应的事件id 即可
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j

事件ID	说明
1102	清理审计日志
4624	账号成功登录
4625	账号登录失败
4720	创建用户
4726	删除用户
4732	将成员添加到启用安全的本地组中

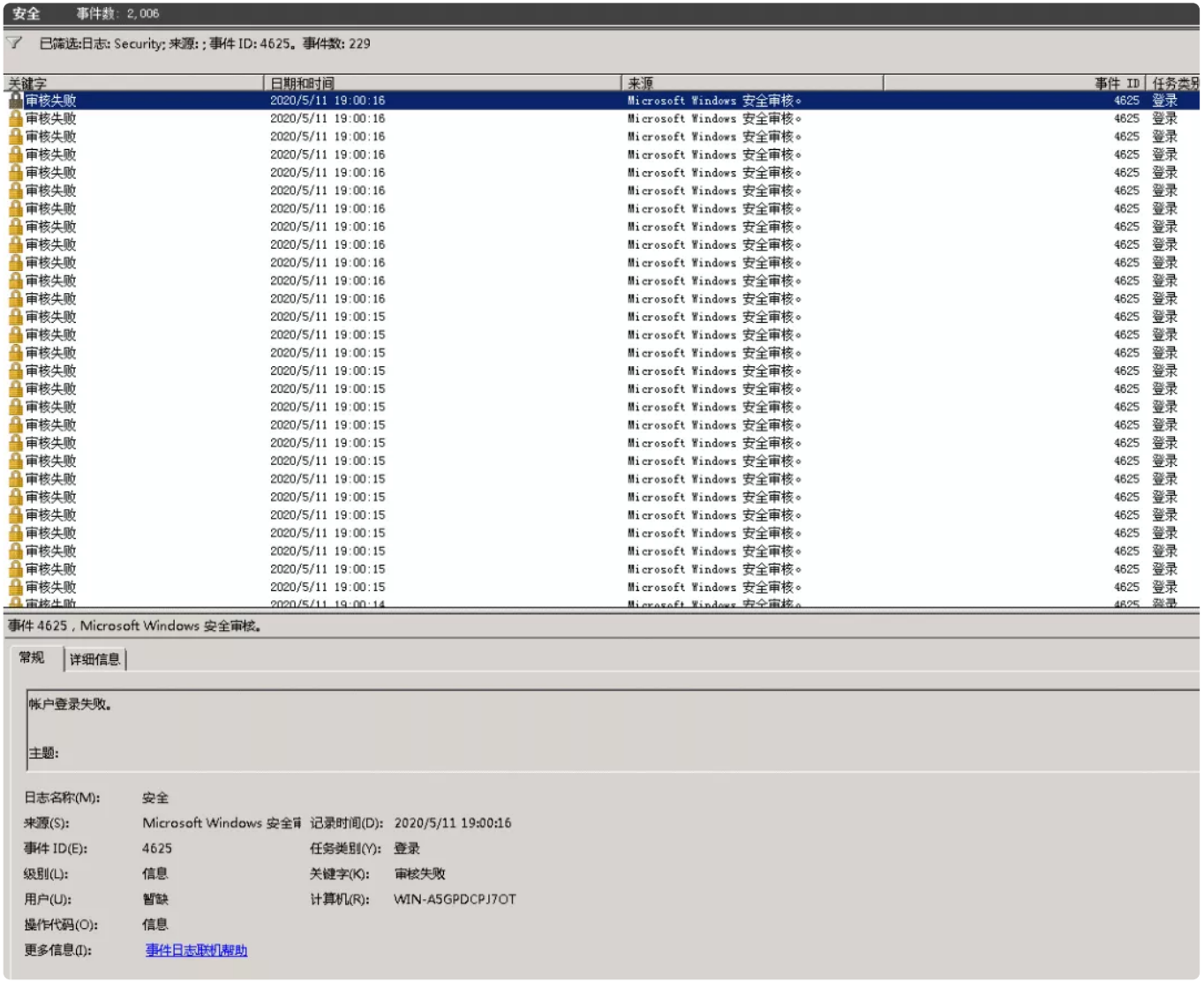
事件ID	说明
4733	将成员从启用安全的本地组中移除

每个成功登录的事件都会标记一个登录类型，不同登录类型代表不同的方式，这里就不一一列举了。

下面配合一个案例查看日志：

在攻击机器上爆破目标靶机的RDP，在靶机上查看日志信息

1.开始-运行，输入 eventvwr.msc2.在事件查看器中，Windows日志 --> 安全，查看系统日志；
3.在系统日志右侧操作中，点击筛选当前日志 ，输入事件 ID 进行筛选。
4.输入事件 ID：4625 进行日志筛选，发现事件 ID：4625，事件数 229，即用户登录失败了 229 次，那么这台服务器管理员账号可能遭遇了暴力猜解。


安全 事件数: 2,006
已筛选:日志: Security; 来源: ; 事件 ID: 4625。事件数: 229
关键字 日期和时间 来源 事件 ID 任务类别
审核失败 2020/5/11 19:00:16 Microsoft Windows 安全审核。 4625 登录
审核失败 2020/5/11 19:00:15 Microsoft Windows 安全审核。 4625 登录
事件 4625，Microsoft Windows 安全审核。
常规 详细信息
帐户登录失败。
主题:
日志名称(M): 安全
来源(S): Microsoft Windows 安全审 记录时间(D): 2020/5/11 19:00:16
事件 ID(E): 4625 任务类别(Y): 登录
级别(L): 信息 关键字(K): 审核失败
用户(U): 暂缺 计算机(R): WIN-A5GPDCPJ7OT
操作代码(O): 信息
更多信息(I): 事件日志联机帮助

日志工具

Sysmon 是微软的一款轻量级的系统监控工具，最开始是由 Sysinternals 开发的，后来 Sysinternals 被微软收购，现在属于 Sysinternals 系列工具。它通过系统服务和驱动程序实现记录进程创建、文件访问以及网络信息的记录，并把相关的信息写入并展示在 windows 的日志事件里。

sysmon 特点是用完整的命令行记录子进程和父进程的创建行为。

使用 sha1（默认），MD5，SHA256 或 IMPHASH 记录进程镜像文件的 hash 值。可以同时使用多个 hash，包括进程创建过程中的进程 GUID。

每个事件中包含 session 的 GUID。

下载地址

```
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
```

安装

```
Sysmon.exe -i
```

更新配置文件

```
sysmon.exe -c sysmonconfig-export.xml
```

如果需要卸载

```
sysmon.exe -u
```

查看日志记录

Win+R ,eventvwr.msc，应用程序和服务日志 `/Microsof/Windows/Sysmon/Operational`

Sysmon 日志默认保存在 `%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx`，可在事件查看器的日志属性设置保存在远程服务器，或通过其他工具或脚本保存。

logparser

logparser 是一款 windows 日志分析工具

登录成功的所有事件

```
LogParser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\Security.evtx where EventID=4624"
```

指定登录时间范围的事件

```
LogParser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\Security.evtx where TimeGenerated>'2018-06-19 23:32:11' and TimeGenerated<'2018-06-20 23:34:00' and EventID=4624"
```

提取登录成功的用户名和IP

```
LogParser.exe -i:EVT -o:DATAGRID "SELECT EXTRACT_TOKEN(Message,13,' ') as EventType,TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,5,'|') as Username,EXTRACT_TOKEN(Message,38,' ') as Loginip FROM c:\Security.evtx where EventID=4624"
```

登录失败的所有事件

```
LogParser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\Security.evtx where EventID=4625"
```

提取登录失败用户名进行聚合统计

```
LogParser.exe -i:EVT "SELECT EXTRACT_TOKEN(Message,13,' ') as EventType,EXTRACT_TOKEN(Message,19,' ') as user,count(EXTRACT_TOKEN(Message,19,' ')) as Times,EXTRACT_TOKEN(Message,39,' ') as Loginip FROM c:\Security.evtx where EventID=4625 GROUP BY Message”
```

系统历史开关机记录

```
LogParser.exe -i:EVT -o:DATAGRID "SELECT TimeGenerated,EventID,Message FROM c:\System.evtx where EventID=6005 or EventID=6006"
```

总结

本文介绍了windows的日志类型，事件日志的类型、级别、存放位置和ID，日志的检索方案以及检索工具sysmon和logparser的使用。对于蓝队来说，应急和取证溯源离不开日志，因此定时的日志备份非常重要。

作者：江苏智慧安全可信技术研究院

扫描关注乌雲安全

觉得不错点个“赞”、“在看”哦👇

阅读原文

喜欢此内容的人还喜欢

Chrome灵魂插件，我的十八搬兵器！

乌雲安全

随笔 | 为什么中国没有超级英雄?

一个坏土豆

1700亿头部券商被立案调查！62家公司IPO受牵连?

凤凰网财经