

一、windows日志

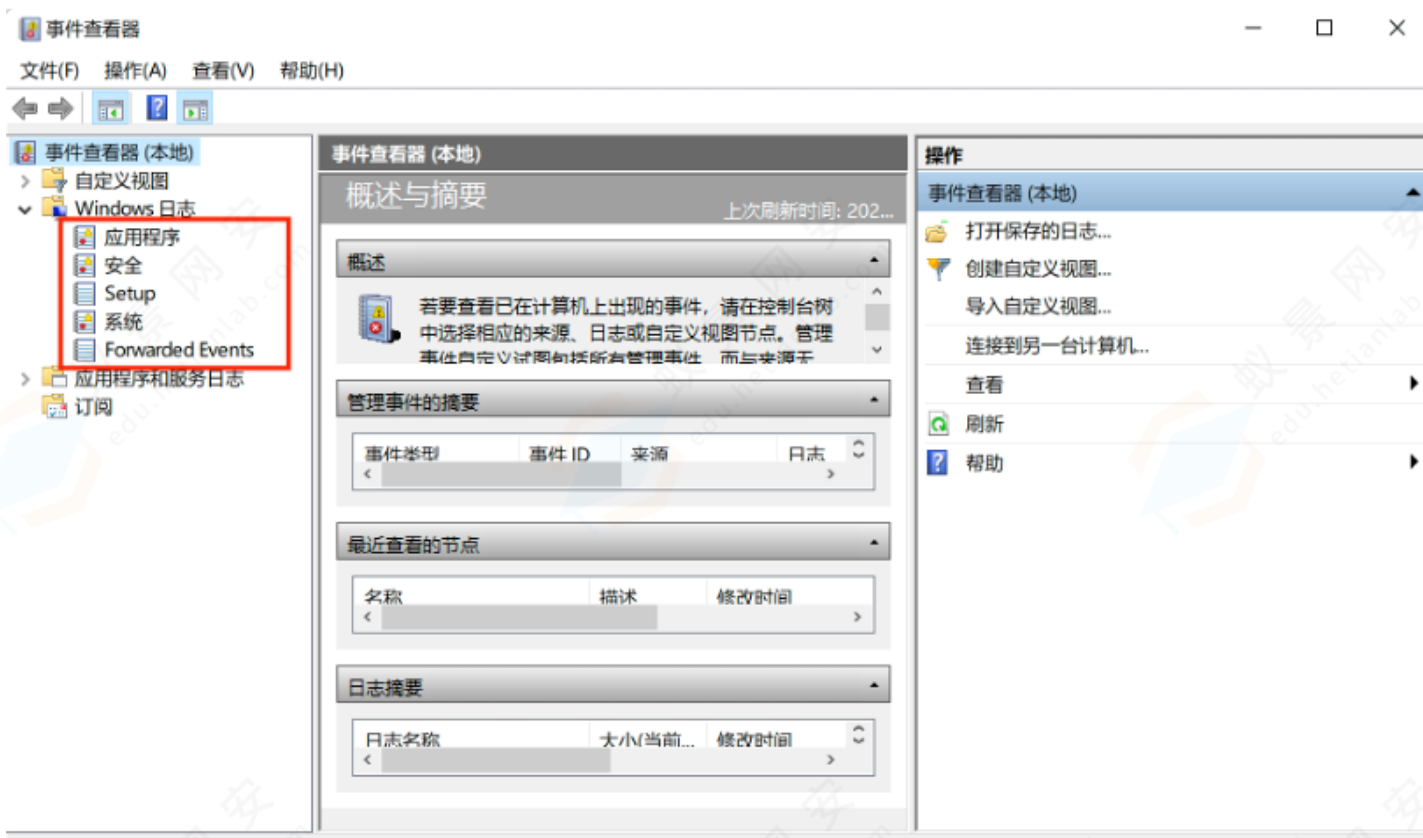
- 如果windows服务器被入侵，往往需要检索和分析相应的安全日志
- 除了安全设备，系统自带的日志就是取证的关键材料，但是此类日志数量庞大，需要高效分析 windows安全日志

1. Windows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
- 查看日志的方法：Win+R，输入 eventvwr.msc 打开事件查看器

2.

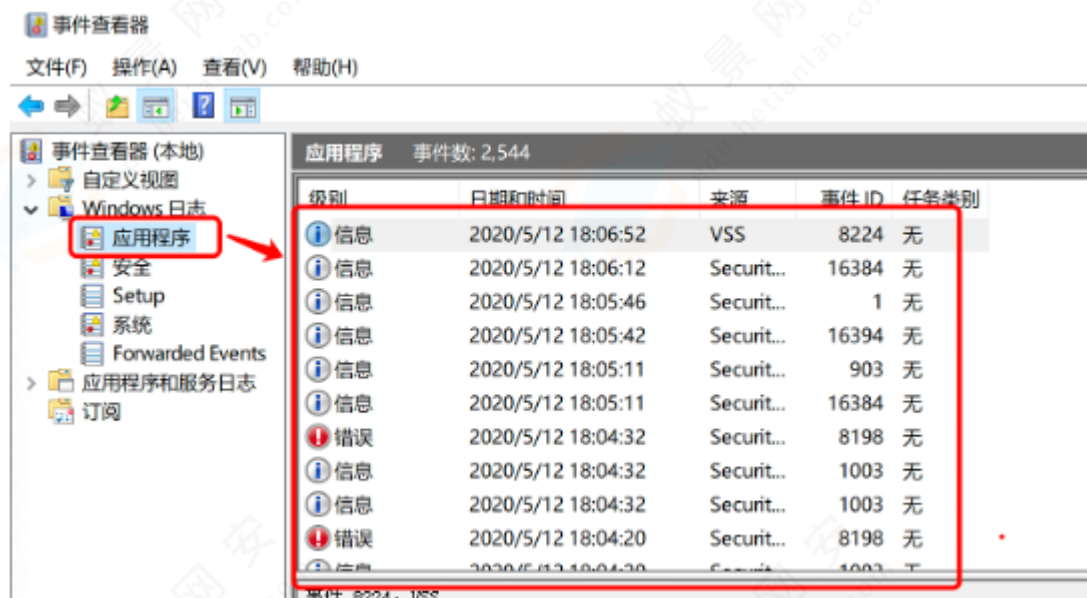
- 事件查看器
 - 可以看到，事件查看器将日志分成了两大类，windows日志、应用程序日志和服务日志
 - windows日志中又有应用程序、安全、setup、系统和 forwarded event这几种事件类型



1. 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
- 日志默认位置： %SystemRoot%\System32\Winevt\Logs\Application.evtx



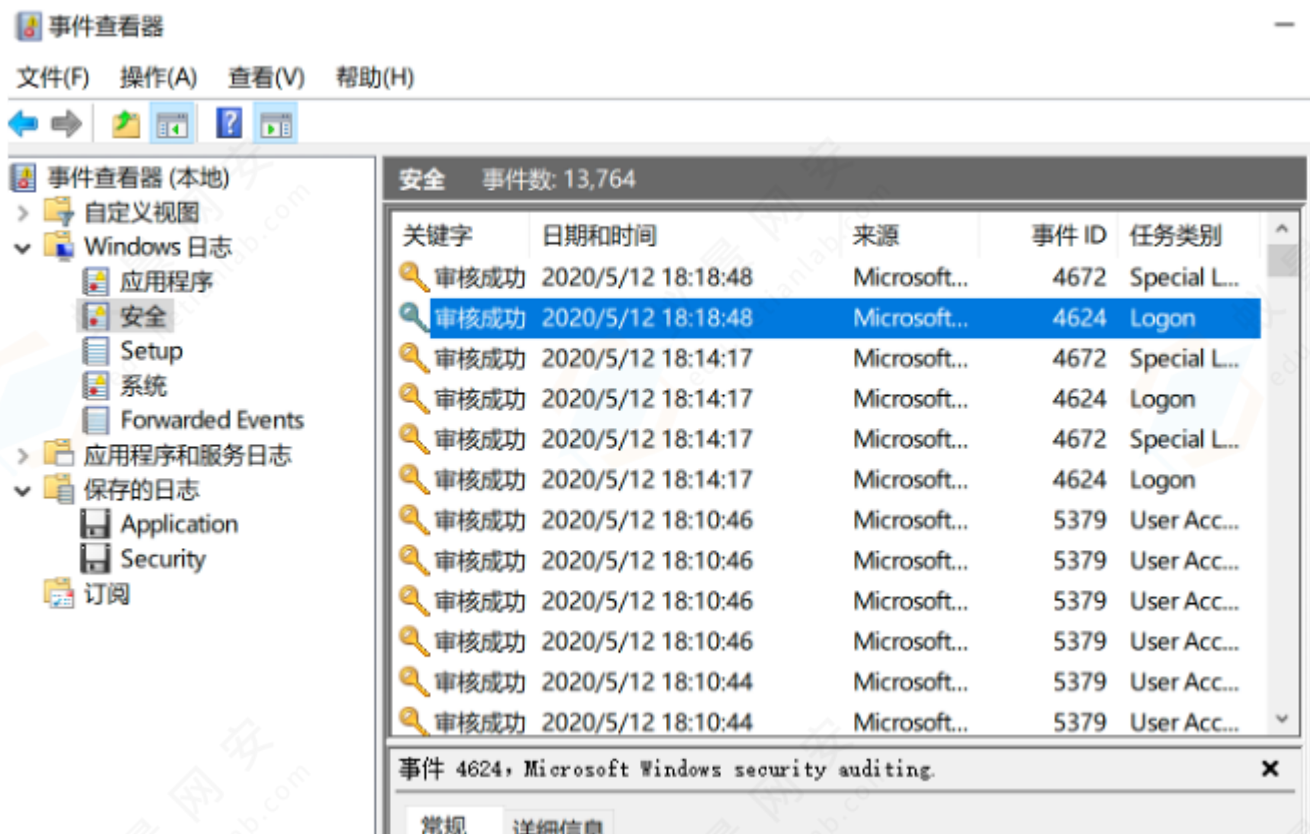
2.系统日志

- 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
- 日志默认位置： %SystemRoot%\System32\Winevt\Logs\System.evtx



3.安全日志

- 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
- 日志默认位置： %SystemRoot%\System32\Winevt\Logs\Security.evtx



• 事件级别

事件级别	说明
信息	信息事件指应用程序、驱动程序或服务成功操作的事件
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
失败审核	失败的审核安全访问尝试
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	

级别	日期和时间			
警告	2020/5/12 18:45:50	审核成功	2020/5/12 18:55:42	Microsoft... 4624
警告	2020/5/12 18:35:43	审核成功	2020/5/12 18:55:42	Microsoft... 4648
警告	2020/5/12 18:15:29	审核失败	2020/5/12 18:55:39	Microsoft... 4625
信息	2020/5/12 18:14:18	审核失败	2020/5/12 18:55:37	Microsoft... 4625
信息	2020/5/12 18:08:10	审核成功	2020/5/12 18:55:35	Microsoft... 4798
错误	2020/5/12 18:05:46	审核成功	2020/5/12 18:41:03	Microsoft... 4672
错误	2020/5/12 18:05:46	审核成功	2020/5/12 18:41:03	Microsoft... 4624

• 事件ID介绍:

- 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/> 搜索 event+ 相应事件的事件 ID
- 常见事件ID

事件ID	说明
4634	注销成功
4624	账号成功登录
4625	账号登录失败
4720	创建用户
4726	删除用户
4672	使用超级用户 (如管理员) 进行登录
4647	用户启动的注销

(1) Windows事件日志分析

- 本地交互式登录
 - 4648-4624-登录成功

<https://learn.microsoft.com/zh-cn/windows/security/threat-protection/auditing/event-4624>

首先是成功的登录, 从日志分析来看至少会有2个事件发生, ID分别为 4648、4624, 以下从上至下分别是各自的截图。

常规

详细信息

试图使用显式凭据登录。

主题:

安全 ID: SYSTEM
帐户名: PC\$
帐户域: WORKGRUOP
登录 ID: 0x3e7
登录 GUID: {00000000-0000-0000-0000-000000000000}

使用了哪个帐户的凭据:

帐户名: Administrator
帐户域: PC
登录 GUID: {00000000-0000-0000-0000-000000000000}

目标服务器:

目标服务器名: localhost
附加信息: localhost

进程信息:

进程 ID: 0x98c
进程名: C:\Windows\System32\winlogon.exe

网络信息:

日志名称(M): 安全
来源(S): Microsoft Windows 安全# 记录时间(D): 2022/9/29 11:31:01
事件 ID(E): 4648 任务类别(Y): 登录
级别(L): 信息 关键字(K): 审核成功
用户(U): 暂缺 计算机(R): PC
操作代码(O): 信息
更多信息(I): [事件日志联机帮助](#)

复制(P)

关闭(C)



首先是 ID 4648 事件，该事件说明有人使用身份凭据在尝试登录，并且头字段中的用户名为 SYSTEM，看看描述信息中有什么：

试图使用显式凭据登录。

主题：

安全 ID: SYSTEM

帐户名: PC\$
帐户域: WORKGRUOP
登录 ID: 0x3e7
登录 GUID: {00000000-0000-0000-0000-000000000000}

使用了哪个帐户的凭据:

帐户名: Administrator
帐户域: PC
登录 GUID: {00000000-0000-0000-0000-000000000000}

目标服务器:

目标服务器名: localhost
附加信息: localhost

进程信息:

进程 ID: 0x630
进程名: C:\Windows\System32\winlogon.exe

网络信息:

网络地址: 127.0.0.1
端口: 0

在进程尝试通过显式指定帐户的凭据来登录该帐户时生成此事件。这通常发生在批量类型的配置中(例如计划任务) 或者使用 RUNAS 命令时。

日志名称: Security
来源: Microsoft-Windows-Security-Auditing
日期: 2022/9/29 14:43:18
事件 ID: 4648
任务类别: 登录
级别: 信息
关键字: 审核成功
用户: 暂缺
计算机: PC (目标机器名)

然后是 ID 4624 事件, 看看描述信息:

已成功登录帐户。

主题:

安全 ID: SYSTEM
帐户名: PC\$
帐户域: WORKGRUOP
登录 ID: 0x3e7

登录类型: 2

新登录:

安全 ID: PC\Administrator
帐户名: Administrator
帐户域: PC
登录 ID: 0x252938
登录 GUID: {00000000-0000-0000-0000-000000000000}

进程信息:

进程 ID: 0x630
进程名: C:\Windows\System32\winlogon.exe

网络信息:

工作站名: PC
源网络地址: 127.0.0.1
源端口: 0

详细身份验证信息:

登录进程: User32
身份验证数据包: Negotiate
传递服务: -
数据包名(仅限 NTLM): -
密钥长度: 0

在创建登录会话后在被访问的计算机上生成此事件。

“主题”字段指明本地系统上请求登录的帐户。这通常是一个服务(例如 Server 服务)或本地进程(例如 Winlogon.exe 或 Services.exe)。

“登录类型”字段指明发生的登录种类。最常见的类型是 2 (交互式)和 3 (网络)。

“新登录”字段会指明新登录是为哪个帐户创建的, 即登录的帐户。

“网络”字段指明远程登录请求来自哪里。“工作站名”并非总是可用, 而且在某些情况下可能会留为空白。

“身份验证信息”字段提供关于此特定登录请求的详细信息。

- “登录 GUID”是可以用于将此事件与一个 KDC 事件关联起来的唯一标识符。
- “传递服务”指明哪些直接服务参与了此登录请求。
- “数据包名”指明在 NTLM 协议之间使用了哪些子协议。
- “密钥长度”指明生成的会话密钥的长度。如果没有请求会话密钥则此字段为 0。

日志名称: Security
来源: Microsoft-Windows-Security-Auditing
日期: 2022/9/29 14:43:18
事件 ID: 4624
任务类别: 登录
级别: 信息
关键字: 审核成功

用户: 暂缺
计算机: PC

• 4625-登录失败

<https://learn.microsoft.com/zh-cn/windows/security/threat-protection/auditing/event-4625>

失败的本地登录, 会产生ID 4625的事件日志

帐户登录失败。

主题:

安全 ID: SYSTEM
帐户名: PC\$
帐户域: WORKGRUOP
登录 ID: 0x3e7

登录类型: 2

登录失败的帐户:

安全 ID: NULL SID
帐户名: Administrator
帐户域: PC

失败信息:

失败原因: 未知用户名或密码错误。
状态: 0xc000006d
子状态: 0xc000006a

进程信息:

调用方进程 ID: 0x630
调用方进程名: C:\Windows\System32\winlogon.exe

网络信息:

工作站名: PC
源网络地址: 127.0.0.1
源端口: 0

详细身份验证信息:

登录进程: User32
身份验证数据包: Negotiate
传递服务: -
数据包名(仅限 NTLM): -
密钥长度: 0

登录请求失败时在尝试访问的计算机上生成此事件。

日志名称: Security
来源: Microsoft-Windows-Security-Auditing

日期: 2022/9/29 14:43:15
事件 ID: 4625
任务类别: 登录
级别: 信息
关键字: 审核失败
用户: 暂缺
计算机: PC

- RDP协议远程登录

- 4648-4624-4672-登录成功
- 使用mstsc远程登录某个主机时，使用的帐户是管理员帐户的话，成功的情况下会有ID为4648、4624、4672的事件产生。

审核成功	2022/9/29 15:11:23	Microsoft Windows 安全审核。	4672 特殊登录
审核成功	2022/9/29 15:11:23	Microsoft Windows 安全审核。	4624 登录
审核成功	2022/9/29 15:11:23	Microsoft Windows 安全审核。	4648 登录

事件 4624 , Microsoft Windows 安全审核。

常规 详细信息

已成功登录帐户。

主题:

安全 ID: SYSTEM
帐户名: PC\$
帐户域: WORKGRUOP
登录 ID: 0x3e7

登录类型: 10

新登录:

安全 ID: PC\Administrator
帐户名: Administrator
帐户域: PC

日志名称(M): 安全

来源(S): Microsoft Windows 安全审核 记录时间(D): 2022/9/29 15:11:23

事件 ID(E): 4624 任务类别(Y): 登录

级别(L): 信息 关键字(K): 审核成功

用户(U): 暂缺 计算机(R): PC

- 4625-登录失败

登录事件 ID为 4625

登录类型为 10 (远程交互)

审核失败	2022/9/29 15:11:19	Microsoft Windows 安全审核。	4625 登录
审核失败	2022/9/29 15:11:19	Microsoft Windows 安全审核。	4776 凭据验证

事件 4625, Microsoft Windows 安全审核。

常规

详细信息

帐户登录失败。

主题:

安全 ID:	SYSTEM
帐户名:	PC\$
帐户域:	WORKGRUOP
登录 ID:	0x3e7

登录类型: 10

登录失败的帐户:

安全 ID:	NULL SID
帐户名:	administrator
帐户域:	PC

日志名称(M):	安全		
来源(S):	Microsoft Windows 安全审核	记录时间(D):	2022/9/29 15:11:19
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):	PC

(2) 登录爆破实例

- 4624 –登录成功
- 4625 –登录失败
- 4634 – 注销成功
- 4647 – 用户启动的注销
- 4672 – 使用超级用户（如管理员）进行登录

1. Win+R 输入 eventvwr.msc, 打开事件管理器
2. Windows日志 -> 安全 -> 筛选当前日志
3. 输入事件ID: 4625, 进行日志筛选

筛选器 XML

记录时间(G): 任何时间

事件级别:
☐ 关键(L) ☐ 警告(W) ☐ 详细(B)
☐ 错误(R) ☐ 信息(I)

☒ 按日志(O) 事件日志(E): 安全

☐ 按源(S) 事件来源(V):

包括/排除事件 ID: 输入 ID 号和/或 ID 范围, 使用逗号分隔。若要排除条件, 请先键入减号。例如 1,3,5-99,-76(N)

4625

任务类别(T):

关键字(K):

用户(U): <所有用户>

计算机(P): <所有计算机>

清除(A)

确定 取消

4. 发现事件ID: 4625, 事件数8153, 即用户登录失败了8153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: 18,906 (1) 可用的新事件

已筛选: 日志: Security; 来源: ; 事件 ID: 4625。事件数: 8,153

关键字	日期和时间	来源	事件 ID	任务类别
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:22:55	Microsoft Windows 安全审核。	4625	登录

事件 4625, Microsoft Windows 安全审核。

常规 详细信息

安全 ID: NULL SID
帐户名: -
帐户域: -
登录 ID: 0x0

登录类型: 3

登录失败的帐户:
安全 ID: NULL SID
帐户名: administrator
帐户域:

日志名称(M): 安全
来源(S): Microsoft Windows 安全审核 记录时间(D): 2022/9/30 11:22:55
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): PC
操作代码(O): 信息

5、查看网络信息，可得知爆破来源IP为 192.168.81.134

安全 事件数: 33,439

已筛选: 日志: Security; 计算机: PC; 来源: ; 事件 ID: 4625。事件数: 15,539

关键字	日期和时间	来源	事件 ID	任务类别
审核失败	2022/9/30 11:24:15	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:24:15	Microsoft Windows 安全审核。	4625	登录
审核失败	2022/9/30 11:24:15	Microsoft Windows 安全审核。	4625	登录

事件 4625, Microsoft Windows 安全审核。

常规 详细信息

失败信息:

失败原因: 未知用户名或密码错误。

状态: 0xc000006d

子状态: 0xc000006a

进程信息:

调用方进程 ID: 0x0

调用方进程名: -

网络信息:

工作站名: \\192.168.81.134

源网络地址: 192.168.81.134

源端口: 49132

6、筛选来自此IP的登录成功日志 4624，判断是否爆破登录成功
筛选当前日志，XML，手动编辑查询，输入如下XML过滤语句：

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System/EventID=4624] and *[EventData[Data[@Name='IpAddress' s]='192.168.81.134']]</Select>
  </Query>
</QueryList>
```


筛选器 XML

若要以 XPath 格式提供事件筛选器，请单击下面的“手动编辑查询”复选框。

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System/EventID=4624] and *[EventData[Data
[@Name='IpAddress']='192.168.80.129']]</Select>
  </Query>
</QueryList>
```

☒ 手动编辑查询(Q)

确定

取消

发现存在以下登录成功日志

已筛选:高级筛选器, 单击“筛选器”命令以查看筛选器配置。。事件数: 1

关键字	日期和时间	来源	事件 ID	任务类别
审核成功	2022/9/30 11:24:36	Microsoft Windows 安全审核。	4624	登录

事件 4624, Microsoft Windows 安全审核。

常规

详细信息

新登录:

安全 ID: PC\Administrator
帐户名: Administrator
帐户域: PC
登录 ID: 0x78a856
登录 GUID: {00000000-0000-0000-0000-000000000000}

进程信息:

进程 ID: 0x0
进程名: -

网络信息:

工作站名: [\\192.168.81.134](#)
源网络地址: 192.168.81.134

日志名称(M): 安全

来源(S): Microsoft Windows 安全审核 记录时间(D): 2022/9/30 11:24:36

事件 ID(E): 4624 任务类别(V): 登录

级别(L): 信息 关键字(K): 审核成功

用户(U): 暂缺 计算机(R): PC

爆破事件日志怎么获取? 如何爆破windows?

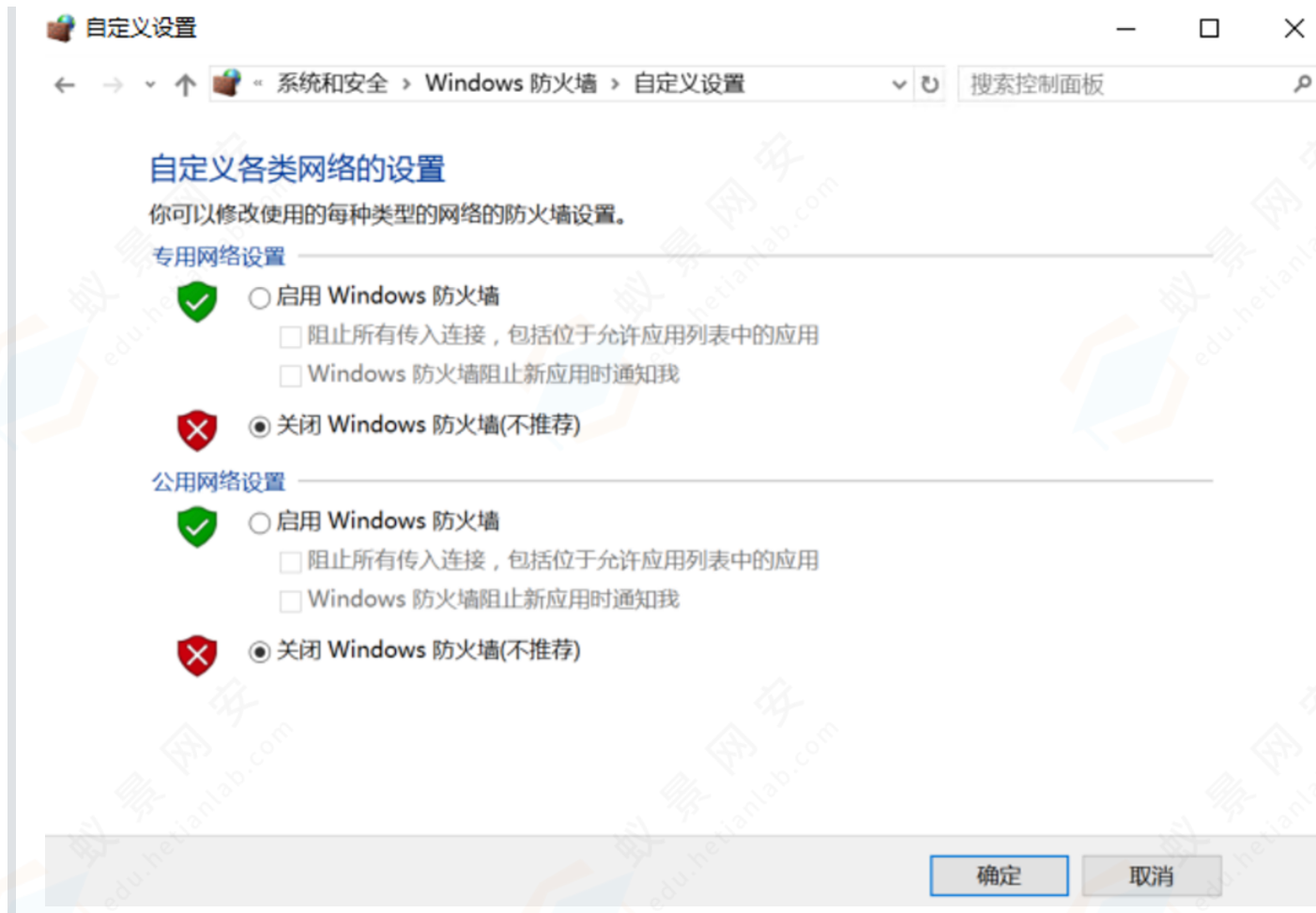
- windows爆破一般是445 (文件共享服务)、3389 (远程桌面连接) 服务
- hydra 登录爆破

hydra -l administrator -P /usr/share/wordlists/fasttrack.txt smb://192.168.80.128 -vV

```
(kali㉿kali)-[~]  
$ hydra -l administrator -P /usr/share/wordlists/fasttrack.txt smb://192.168.80.128  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret  
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and  
ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-26 21:22:21  
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)  
[DATA] max 1 task per 1 server, overall 1 task, 222 login tries (l:1/p:222), ~222 tries per task  
[DATA] attacking smb://192.168.80.128:445/
```

- 注意: 想要正确爆破445端口, 必须关闭靶机 (我这里是windows server 2016) 的系统防火墙



3. Linux日志

- Linux系统拥有非常灵活和强大的日志功能，可以保存几乎所有的操作记录，并可以从中检索出我们需要的信息。
- 内核及系统日志
 - 由系统服务rsyslog统一进行管理，日志格式基本相似
 - 用户日志
 - 记录系统用户登录及退出系统的相关信息
 - 程序日志
 - 由相应的应用程序进行独立管理。如：web服务，ftp服务
 - 常见日志文件

一台Linux不是所有的日志文件都有

日志文件	文件说明
/var/log/cron	每当 cron
进程开始一个工作时，就会将相关信息记录在这个文件中。	
/var/log/secure	记录验证和授权方面的信息，只要涉及账号和密码的程序都会记录，比如 SSH
登录， su	文件说明

切换用户， sudo	
授权，甚至添加用户和修改用户密码都会记录在这个日志文件中	
/var/log/wtmp	永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接编辑查看，而需要使用 last
命令来查看	
/var/run/utmp	记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变化，只记录当前登录用户的信息。同样这个文件不能直接编辑查看，而要使用 w, who, users
等命令来查询	
/var/log/btmp	记录所有失败登录日志信息。这个文件是二进制文件，不能直接编辑查看，使用 lastb
命令或 last -f /var/log/btmp	
命令可以查看 btmp 文件。	
/var/log/cups	涉及所有打印信息的日志。
/var/log/faillog	包含用户登录失败信息。此外，错误登录命令也会记录在本文件中。
/var/log/messages	记录系统重要信息的日志。这个日志文件中会记录 Linux 系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就应该是这个日志文件。此外， mail, cron, daemon, kern 和 auth
等内容也记录在 var/log/messages	
日志中。	
/var/log/dmesg	包含内核缓冲信息（kernel ring buffer
）。在系统启动时，会在屏幕上显示许多与硬件有关的信息。可以用 dmesg	
查看它们。记录了系统在开机时内核自检的信息，也可以使用 dmesg	
命令直接查看内核自检信息	
/var/log/auth.log	包含系统授权信息，包括用户登录和使用的权限机制等。
/var/log/boot.log	包1含系统启动时的日志。
日志文件	文件说明

/var/log/daemon.log	包含各种系统后台守护进程日志信息。
/var/log/dpkg.log	包括安装或 dpkg
命令清除软件包的日志。	
/var/log/kern.log	包含内核产生的日志，有助于在定制内核时解决问题。
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接编辑查看，而要使用 lastlog
命令查看	
/var/log/user.log	记录所有等级用户信息的日志。
/var/log/alternatives.log	更新替代信息都记录在这个文件中。
/var/log/anaconda.log	在安装Linux时，所有安装信息都储存在这个文件中。
/var/log/yum.log	包含使用 yum
安装的软件包信息。	
/var/log/maillog /var/log/mail.log	包含系统运行电子邮件服务器的日志信息。例如， sendmail
日志信息就全部送到这个文件中。	

• 比较重要的几个日志

```

登录失败记录：/var/log/btmp    #lastb
最后一次登录：/var/log/lastlog #lastlog
登录成功记录：/var/log/wtmp    #last
登录日志记录：/var/log/secure
目前登录用户信息：/var/run/utmp #w、who、users
历史命令记录：history
仅清理当前用户：history -c

```

- 记录用户的最后一次信息：/var/log/lastlog
 - 查看的某系统用户最后一次登录的记录，一些系统用户从来不登录最后一次就是 **Never logged in**。
 - 不用直接查看该日志文件，通过命令：lastlog
 - 举例：查看 root 用户最后一次登录的信息

```

root@[-] :~# lastlog
Username      Port      From      Latest
root          pts/19    192.168.149.1  五 10月 18 14:34:16 +0800 2019
daemon
bin            **Never  logged in**
sys            **Never  logged in**
sync           **Never  logged in**
games          **Never  logged in**
man            **Never  logged in**
lp             **Never  logged in**

```

- 登录用户的信息: /var/log/utmp
 - 记录有关当前登录用户的信息在文件utmp中, utmp文件可以使用命令查询。如: who、w等
 - who命令: 访问utmp记录, 显示当前正在登录的用户信息。
 - w: 与who命令相似, 但显示的信息更加详细。

```

[root@[-] Desktop]# who
root      tty1          2020-02-09 14:49 (:0)
root      pts/0          2020-02-09 14:58 (:0.0)
[root@[-] Desktop]# w
15:16:10 up 1:28, 2 users, load average: 0.07, 0.02, 0.01
USER      TTY      FROM      LOGIN@    IDLE      JCPU      PCPU      WHAT
root      tty1      :0         14:49     3:59m     3.23s     3.23s     /usr/bin/Xorg :
root      pts/0     :0.0      14:58     0.00s     0.02s     0.00s     w

```

- /var/log/wtmp
 - wtmp日志文件永久记录每个用户登录和退出、数据交换、关机及重启的信息。
 - wtmp文件被命令last和ac使用。
 - last命令: 访问wtmp文件, 显示自从文件第一次创建以来所有登陆过的用户
 - ac命令: 统计登录的总时长, ac root: 显示root用户登陆的总时长
- 登录失败日志: /var/log/btmp
 - 记录Linux登陆失败的用户、时间以及远程IP地址
 - 该文件是一个二进制保存的文件, 直接使用 lastb命令查看。

```

[root@[-] /]# lastb
root      ssh:notty    192.168.37.130  Sun Feb  9 18:36 - 18:36 (00:00)
root      ssh:notty    192.168.37.130  Sun Feb  9 18:36 - 18:36 (00:00)
root      ssh:notty    192.168.37.130  Sun Feb  9 18:36 - 18:36 (00:00)
root      tty1         :0             Sun Feb  9 14:49 - 14:49 (00:00)
[-]      tty8         :2             Sat Feb  8 20:06 - 20:06 (00:00)
[-]      tty1         :0             Fri Feb  7 18:03 - 18:03 (00:00)

```

- 安全日志: /var/log/secure

现在新版的ubuntu、debian、kali已经没有这个文件了, 换成了 /var/log/auth.log

- 一般用来记录安全相关的信息, 记录最多的是哪些用户登录服务器的相关日志。例如: sshd会将所有信息 (其中包括失败登录) 记录在这里
- 如果该文件很大, 说明有人在破解你的root密码

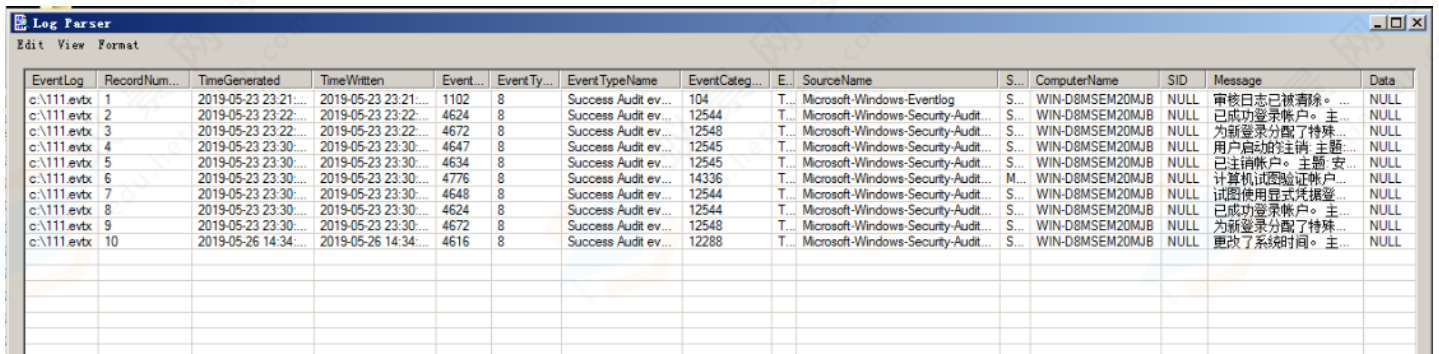

```
Feb 9 17:43:20 pam: gdm-password: pam_unix(gdm-password:auth): auth could not identify password for [haha]
Feb 9 17:43:20 pam: gdm-password: gkr-pam: no password is available for user
Feb 9 17:43:25 pam: gdm-password: pam_unix(gdm-password:session): session opened for user  by (uid=0)
Feb 9 18:36:02 sshd[4176]: Failed password for root from 192.168.37.130 port 40520 ssh2
Feb 9 18:36:08 sshd[4176]: Failed password for root from 192.168.37.130 port 40520 ssh2
Feb 9 18:36:14 sshd[4176]: Failed password for root from 192.168.37.130 port 40520 ssh2
Feb 9 18:36:14 sshd[4177]: Connection closed by 192.168.37.130
Feb 9 18:36:14 sshd[4176]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.37.130 user=root
```

4. 日志分析工具

(1) Log Parser

Log Parser (是微软公司出品的日志分析工具, 它功能强大, 使用简单, 可以分析基于文本的日志文件、XML 文件、CSV (逗号分隔符) 文件, 以及操作系统的事件日志、注册表、文件系统、Active Directory。它可以像使用 SQL 语句一样查询分析这些数据, 甚至可以把分析结果以各种图表的形式展现出来。

Log Parser 2.2下载地址: <https://www.microsoft.com/en-us/download/details.aspx?id=24659>



EventLog	RecordNum...	TimeGenerated	TimeWritten	Event...	EventTy...	EventTypeName	EventCateg...	E...	SourceName	S...	ComputerName	SID	Message	Data
c:\11\evtx	1	2019-05-23 23:21...	2019-05-23 23:21...	1102	8	Success Audit ev...	104	T...	Microsoft-Windows-Eventlog	S...	WIN-D8MSEM20MJB	NULL	审核日志已被清除。...	NULL
c:\11\evtx	2	2019-05-23 23:22...	2019-05-23 23:22...	4624	8	Success Audit ev...	12544	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	已成功登录帐户。主...	NULL
c:\11\evtx	3	2019-05-23 23:22...	2019-05-23 23:22...	4672	8	Success Audit ev...	12548	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	为新登录分配了特殊...	NULL
c:\11\evtx	4	2019-05-23 23:30...	2019-05-23 23:30...	4647	8	Success Audit ev...	12545	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	用户自动注销。主题...	NULL
c:\11\evtx	5	2019-05-23 23:30...	2019-05-23 23:30...	4634	8	Success Audit ev...	12545	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	已注销帐户。主题...	NULL
c:\11\evtx	6	2019-05-23 23:30...	2019-05-23 23:30...	4776	8	Success Audit ev...	14336	T...	Microsoft-Windows-Security-Audit...	M...	WIN-D8MSEM20MJB	NULL	计算机试图验证帐户...	NULL
c:\11\evtx	7	2019-05-23 23:30...	2019-05-23 23:30...	4648	8	Success Audit ev...	12544	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	试图使用登录凭据登...	NULL
c:\11\evtx	8	2019-05-23 23:30...	2019-05-23 23:30...	4624	8	Success Audit ev...	12544	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	已成功登录帐户。主...	NULL
c:\11\evtx	9	2019-05-23 23:30...	2019-05-23 23:30...	4672	8	Success Audit ev...	12548	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	为新登录分配了特殊...	NULL
c:\11\evtx	10	2019-05-26 14:34...	2019-05-26 14:34...	4616	8	Success Audit ev...	12288	T...	Microsoft-Windows-Security-Audit...	S...	WIN-D8MSEM20MJB	NULL	更改了系统时间。主...	NULL

基本查询结构

```
Logparser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\xx.evtx"
```

使用Log Parser分析日志

1、查询登录成功的事件

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"
```

2、查询登录失败的事件

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"
```

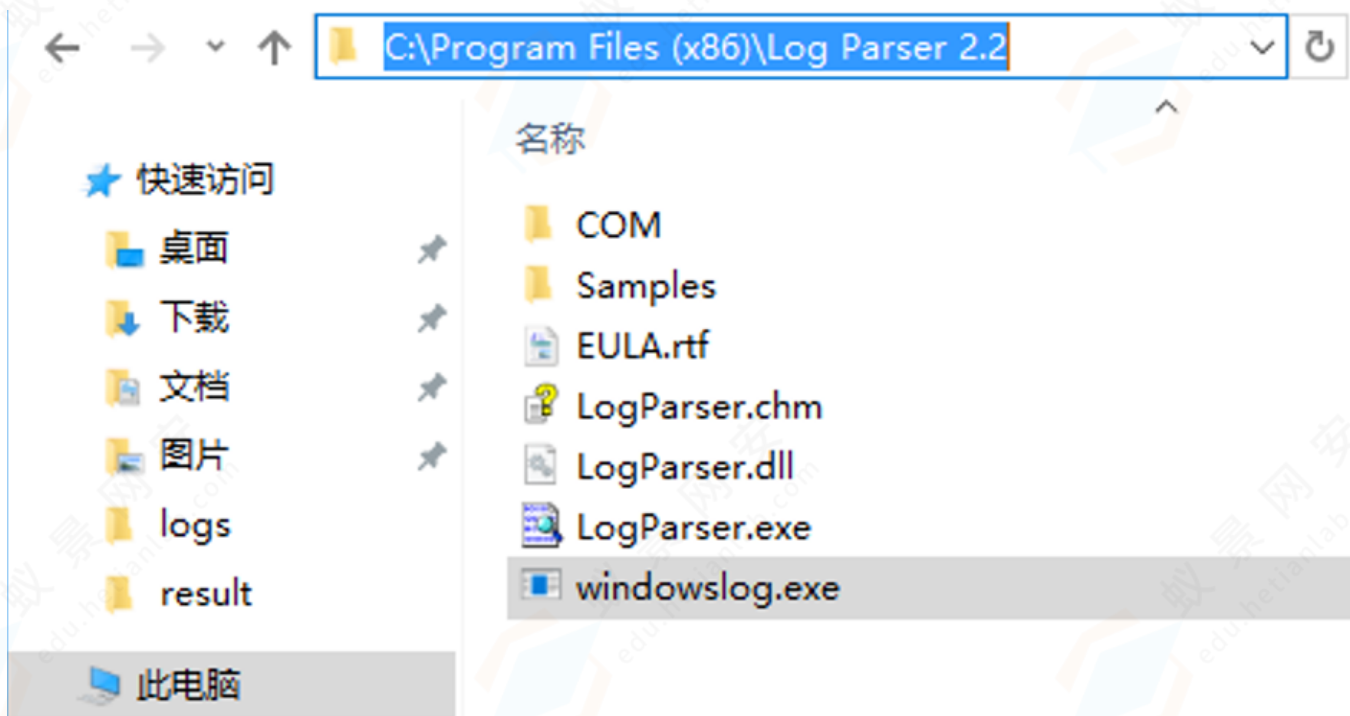
3、系统历史开关机记录:

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

(2) windows-logs-analysis

该工具必须和 Log Parser 共同使用

- 将windowslog.exe放到Log Parser的安装路径 (Log Parser的默认安装路径为 C:\Program Files (x86)\Log Parser 2.2)



5. 双击打开 windowslog.exe

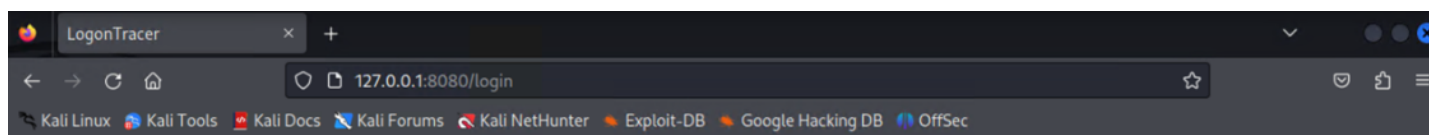
- 选择分析项进行日志分析

Log Parser									
Edit View Format									
Date	Username	Domain	LogonType	AuthPackage	Workstati...	ProcessName	SourceIP	SourceIP2	EventID
2022-10-04 14:38:22	-	-	%%2304	0xc0000073	Advapi	0x3d4	C:\Windows\System32\svchost.exe	-	4625
2022-10-04 14:38:22	-	-	%%2304	0xc0000073	Advapi	0x3d4	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:00:51	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:00:51	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:04:04	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:04:04	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:11:04	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-03-24 09:11:04	-	-	%%2304	0xc0000073	Advapi	0x48	C:\Windows\System32\svchost.exe	-	4625
2023-09-22 19:03:54	-	-	%%2304	0xc0000073	Advapi	0x36c	C:\Windows\System32\svchost.exe	-	4625
2023-09-22 19:03:54	-	-	%%2304	0xc0000073	Advapi	0x36c	C:\Windows\System32\svchost.exe	-	4625

(1) LogonTracer

该工具下载与安装需要一定的科学上网能力，且需要Linux系统内存大于4G

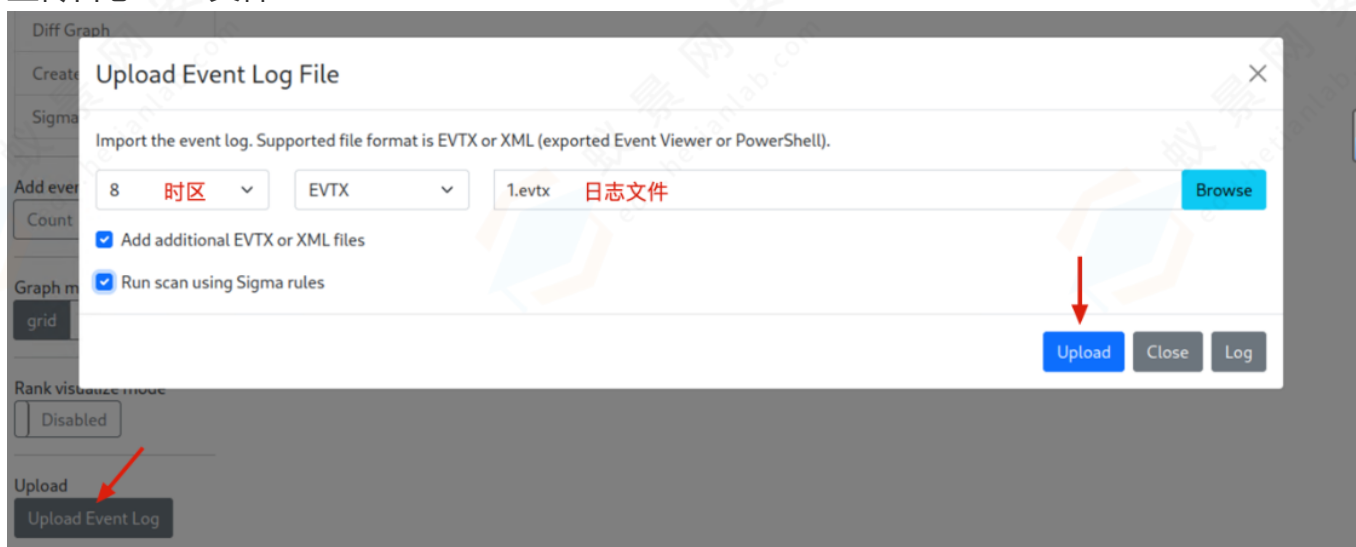
- LogonTracer这款工具是基于Python编写的，并使用Neo4j作为其数据库（Neo4j多用于图形数据库），是一款用于分析Windows安全事件登录日志的可视化工具。它会将登录相关事件中的主机名（或IP地址）和帐户名称关联起来，并将其以图形化的方式展现出来，使得在日志取证时直观清晰。
- github地址：<https://github.com/JPCERTCC/LogonTracer>
- 安装方式：
 - 此安装方式基于 Kali Linux 已安装 docker 和 更新国内阿里apt源 的前提情况下，
 - 1. 安装 docker-compose
 - apt install -y docker-compose (无需科学上网，需要下载1-2分钟)
 - 2. 克隆 LogonTrace 项目
 - git clone <https://ghproxy.com/https://github.com/JPCERTCC/LogonTracer.git> (无需科学上网，需要下载1分钟)
 - 3. 进入LogonTrace项目docker-compose文件夹，并构建镜像
 - cd LogonTracer/docker-compose
 - docker network create neo4j-network
 - docker-compose build （此步骤如果不使用科学上网，会非常慢，大概5-10分钟）
 - docker-compose up -d （此步骤为开启容器，因为该工具使用neo4j数据库，即使该命令执行完成且无报错，也要等待约2分钟才能正常打开）
 - 4. 打开Kali firefox浏览器，访问 <http://127.0.0.1:8080> 并登陆
 - 默认用户名 neo4j
 - 默认密码 password



The login form for LogonTracer features a search icon and the title 'LogonTracer'. It contains two input fields: 'Username' with the value 'neo4j' and 'Password' with masked characters. A 'Remember me' checkbox is present and unchecked. A 'Login' button is located at the bottom right of the form.

- 使用方法

- 上传日志 evtx 文件



- 上传成功后，刷新页面，自动分析

