

Windows排查

万里

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。



中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

- (一) 获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；
- (二) 获取第（一）项以外的身份认证信息五百组以上的；
- (三) 非法控制计算机信息系统二十台以上的；
- (四) 违法所得五千元以上或者造成经济损失一万元以上的；
- (五) 其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

- (一) 数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；
- (二) 其他情节特别严重的情形。

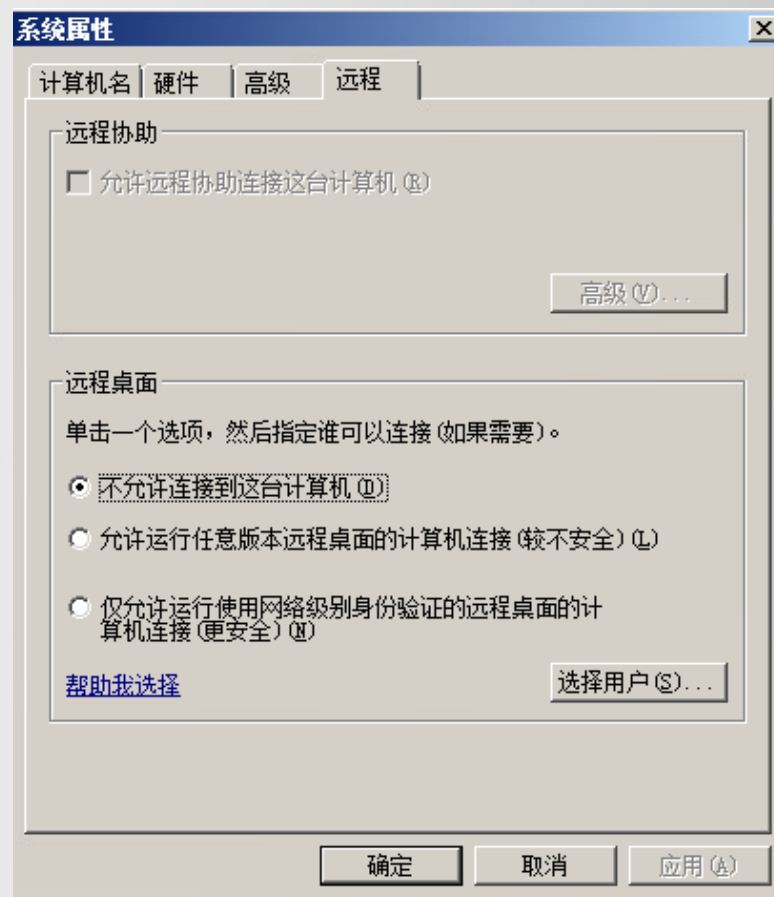
明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

- A. 检查系统账号安全**
- B. 检查异常端口、进程**
- C. 检查启动项、计划任务、服务**
- D. 检查系统相关信息**
- E. 检查系统日志**
- F. 日志分析**

检查系统账号安全

1、查看服务器是否有弱口令，远程管理端口是否对公网开放。

检查方法：根据实际情况咨询相关服务器管理员

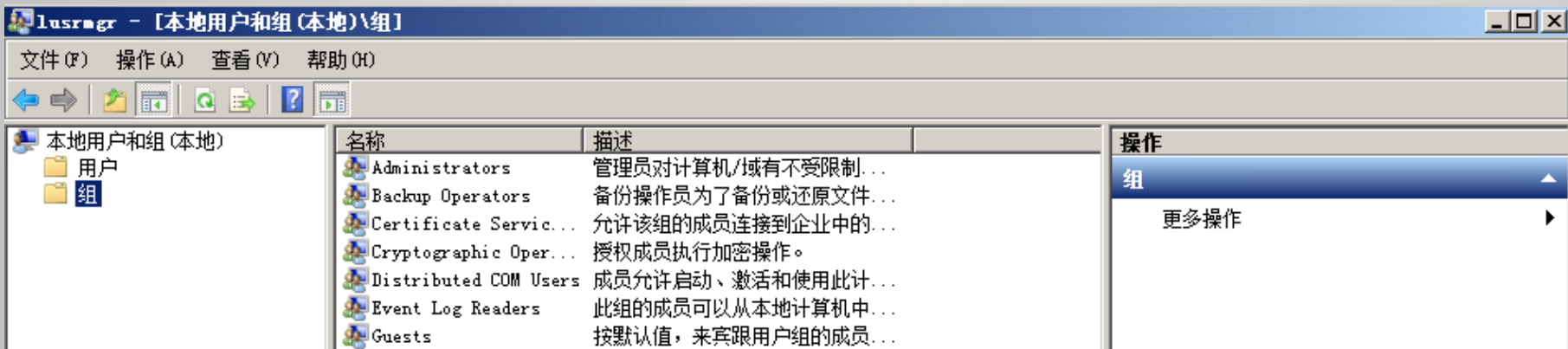
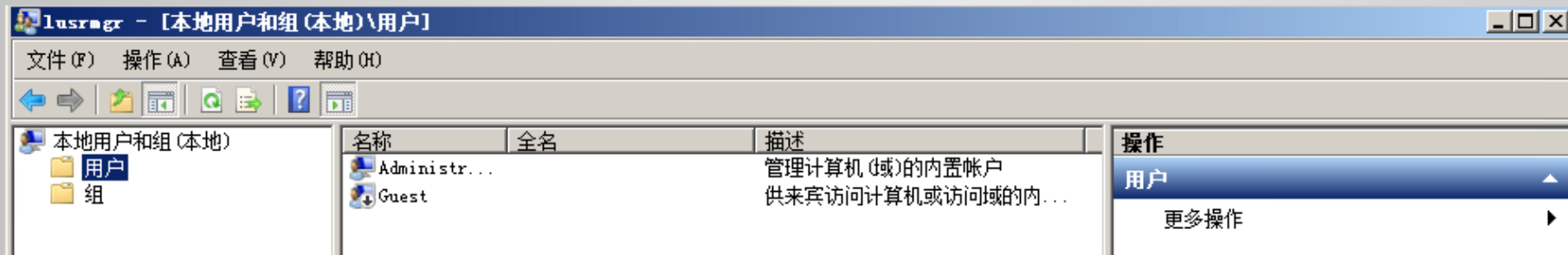


检查系统账号安全

2、查看服务器是否存在可疑账号、新增账号。

检查方法：打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增可疑的账号，如有管理员组（Administrators）里的新增账户如有请立即禁用或删除掉。

。

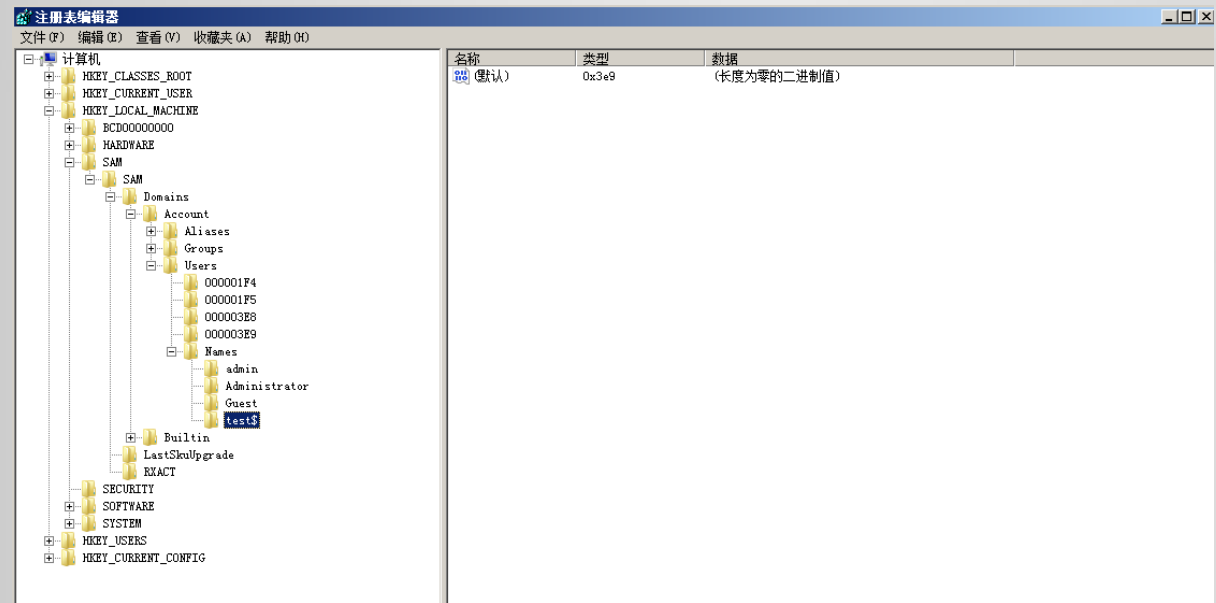


检查系统账号安全

3、查看服务器是否存在隐藏账号、克隆账号。

检查方法： a、打开注册表，查看管理员对应键值。（regedit）

b、使用D盾_web查杀工具，集成了对克隆账号检测的功能



注册表编辑器

名称: 名称 (默认) 类型: 0x3e9 数据: (长度为零的二进制值)

计算机

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
 - BCD00000000
 - HARDWARE
 - SAM
 - Domains
 - Account
 - Aliases
 - Groups
 - Users
 - 000001F4
 - 000001F5
 - 000003E8
 - 000003E9
 - Names
 - admin
 - Administrator
 - Guest
 - test\$
 - Builtin
 - LastShutUpgrade
 - RYACT
 - SECURITY
 - SOFTWARE
 - SYSTEM
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG

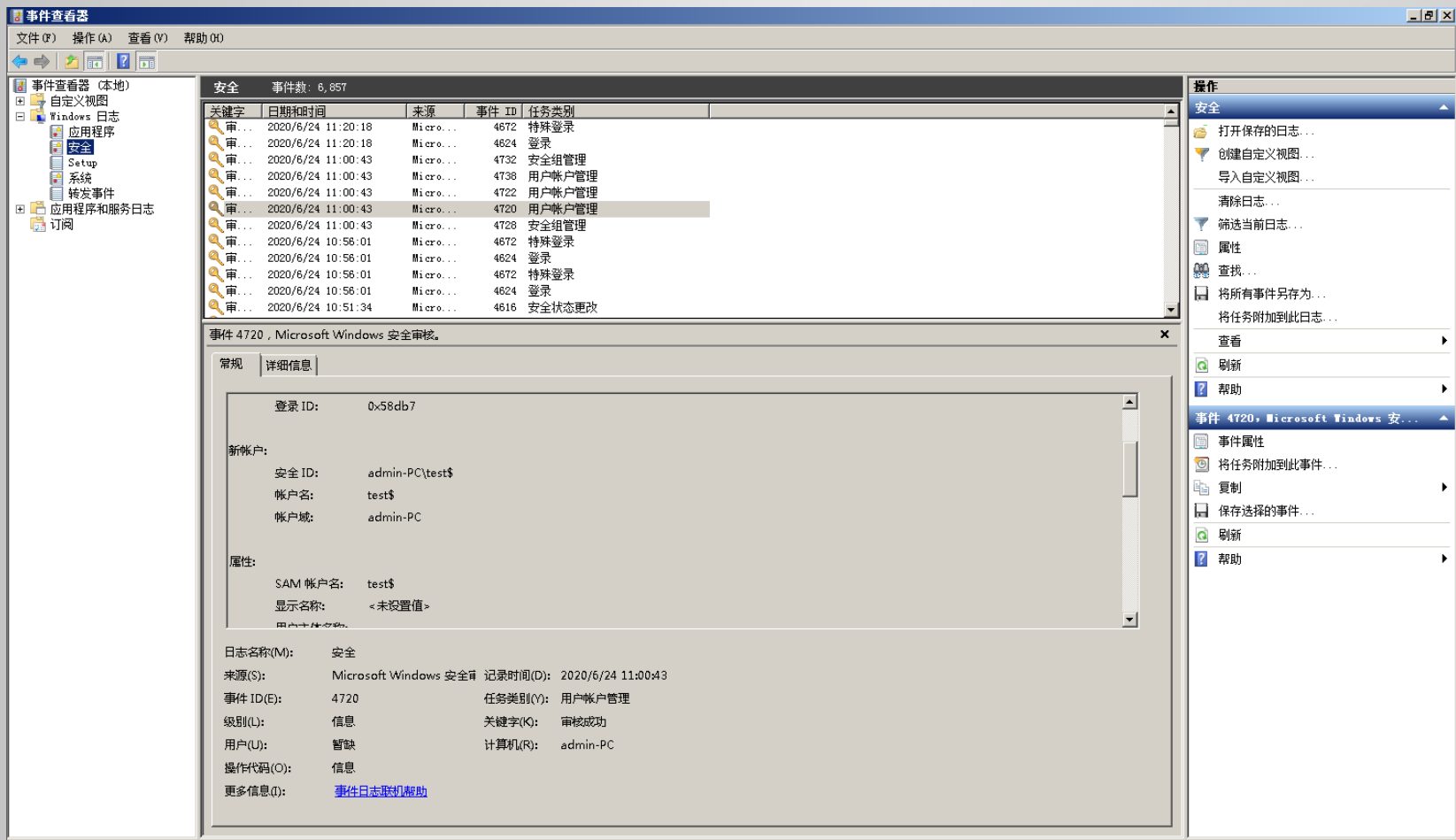
数据库后门追查 | 数据库降权 | 克隆帐号检测 | 流量监控 | IIS池监控 | 端口查看 | 进程查看 | 样本解码 | 文件监

ID	帐号	全名	描述	D盾_检测说明
3ED	test\$			危险! 克隆了[管理帐号]
3EE	test1\$			带\$帐号(一般用于隐藏帐号)
1F4	Administrator		管理计算机(域)的内置...	[管理帐号]
1F5	Guest		供来宾访问计算机或访...	
3E8	IUSR_WIN2008-NE...	Internet 来宾帐户	用于匿名访问 Interne...	

检查系统账号安全

4、结合日志，查看管理员登录时间、用户名是否存在异常。

检查方法： a、Win+R打开运行，输入“eventvwr.msc”，回车运行，打开“事件查看器”。



检查异常端口、进程

1、检查端口连接情况，是否有远程连接、可疑连接。

检查方法：a、netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED

b、根据netstat 定位出的pid，再通过tasklist命令进行进程定位 tasklist | findstr "PID"

```
PS C:\Users\qianxin> netstat -ano
```

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2516
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	580
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	2556
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:7777	0.0.0.0:0	LISTENING	2128
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	372
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	660

```
PS C:\Users\qianxin> tasklist | findstr "2128"
```

```
ew_for_win.exe 2128 Console 1 4,824 K
```

检查异常端口、进程

2、检查进程

1. 开始--运行--输入msinfo32，依次点击“软件环境→正在运行 任务”就可以查看到进程的详细信息，比如进程路径、进程ID、文件创建日期、启动时间等。
2. 打开D盾_web查杀工具，进程查看，关注没有签名信息的进程。
3. 通过微软官方提供的 **Process Explorer** 等工具进行排查。
4. 查看可疑的进程及其子进程。可以通过观察以下内容：
 - 没有签名验证信息的进程
 - 没有描述信息的进程
 - 进程的属主
 - 进程的路径是否合法
 - CPU或内存资源占用长时间过高的进程

检查异常端口、进程

2、检查进程

名称	路径	进程 ID	优先顺序	最小工作集	最大工作集	开始时间	版本
blnsrv.exe	没有资料	564	8	没有资料	没有资料	2020/6/23 2:21	没有
chrome.exe	没有资料	2256	8	没有资料	没有资料	2020/6/23 2:36	没有
chrome.exe	没有资料	2276	8	没有资料	没有资料	2020/6/23 2:36	没有
chrome.exe	没有资料	2344	8	没有资料	没有资料	2020/6/23 2:36	没有
chrome.exe	c:\users\qianxin\appdata\local...	2392	8	200	1380	2020/6/23 2:36	66.
chrome.exe	c:\users\qianxin\appdata\local...	2500	4	200	1380	2020/6/23 2:36	66.
chsim.exe	c:\windows\system32\inputmet...	1348	8	200	1380	2020/6/23 2:34	6.3
cmd.exe	没有资料	2116	8	没有资料	没有资料	2020/6/23 2:37	没有
cmd.exe	没有资料	1588	8	没有资料	没有资料	2020/6/23 2:37	没有
conhost.exe	没有资料	2548	8	没有资料	没有资料	2020/6/23 2:35	没有
conhost.exe	没有资料	2132	8	没有资料	没有资料	2020/6/23 2:37	没有

文件(F) 选项(O) 查看(V)						
进程 性能 用户 详细信息 服务						
名称	PID	状态	用户名	CPU	内存(专用...	描述
blnsrv.exe	564	正在运行	SYSTEM	00	1,088 K	blnsrv
ChsIME.exe	1348	正在运行	qianxin	00	3,884 K	Microsoft IME
cmd.exe	2116	正在运行	qianxin	00	480 K	Windows 命令处理...
cmd.exe	1588	正在运行	qianxin	00	504 K	Windows 命令处理...
conhost.exe	2548	正在运行	qianxin	00	768 K	控制台窗口主进程
conhost.exe	2132	正在运行	qianxin	00	656 K	控制台窗口主进程
csrss.exe	316	正在运行	SYSTEM	00	1,108 K	Client Server Runti...
csrss.exe	300	正在运行	SYSTEM	00	1,226 K	Client Server Runti...

检查启动项、计划任务、服务

1、检查服务器是否有异常的启动项。

a、登录服务器，单击【开始】>【所有程序】>【启动】，默认情况下此目录在是一个空目录，确认是 否有非业务程序在该目录下。

b、单击开始菜单 >【运行】，输入 msconfig，查看是否存在命名异常的 启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

c、单击【开始】>【运行】，输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

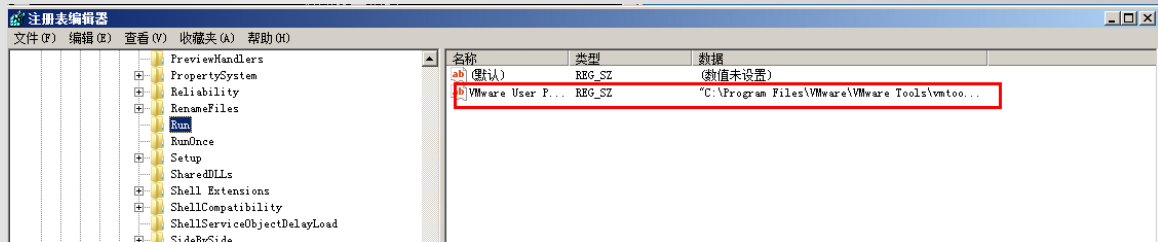
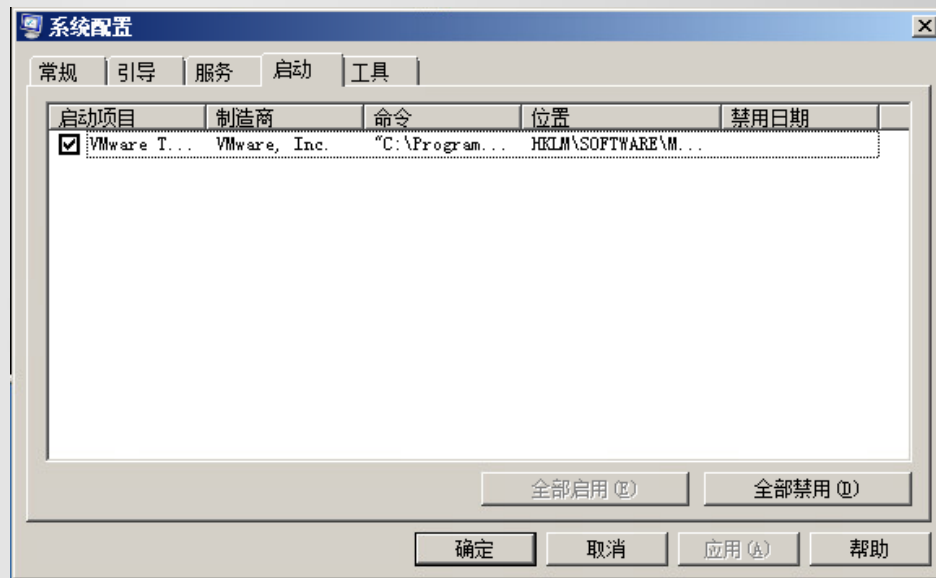
检查右侧是否有启 动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

d、利用安全软件查看启动项、开机时间管理等。

e、组策略，运行gpedit.msc

检查启动项、计划任务、服务

1、检查服务器是否有异常的启动项



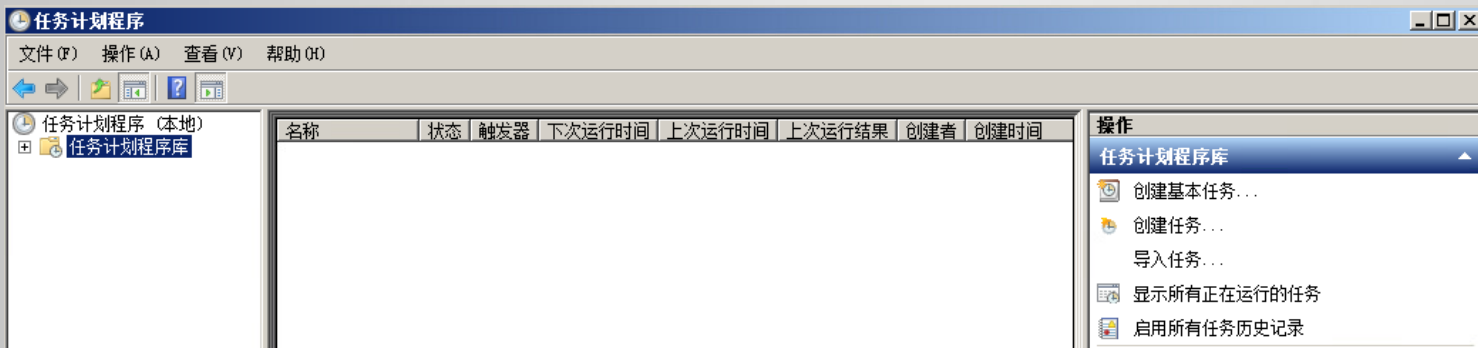
检查启动项、计划任务、服务

2、检查计划任务。

检查方法：

a、单击【开始】>【设置】>【控制面板】>【任务计划】，查看计划任务属性，便可以发现木马文件 的路径。

b、单击【开始】>【运行】；输入 cmd，然后输入at，检查计算机与网络上的其它计算机之间的会话 或计划任务，如有，则确认是否为正常连接。



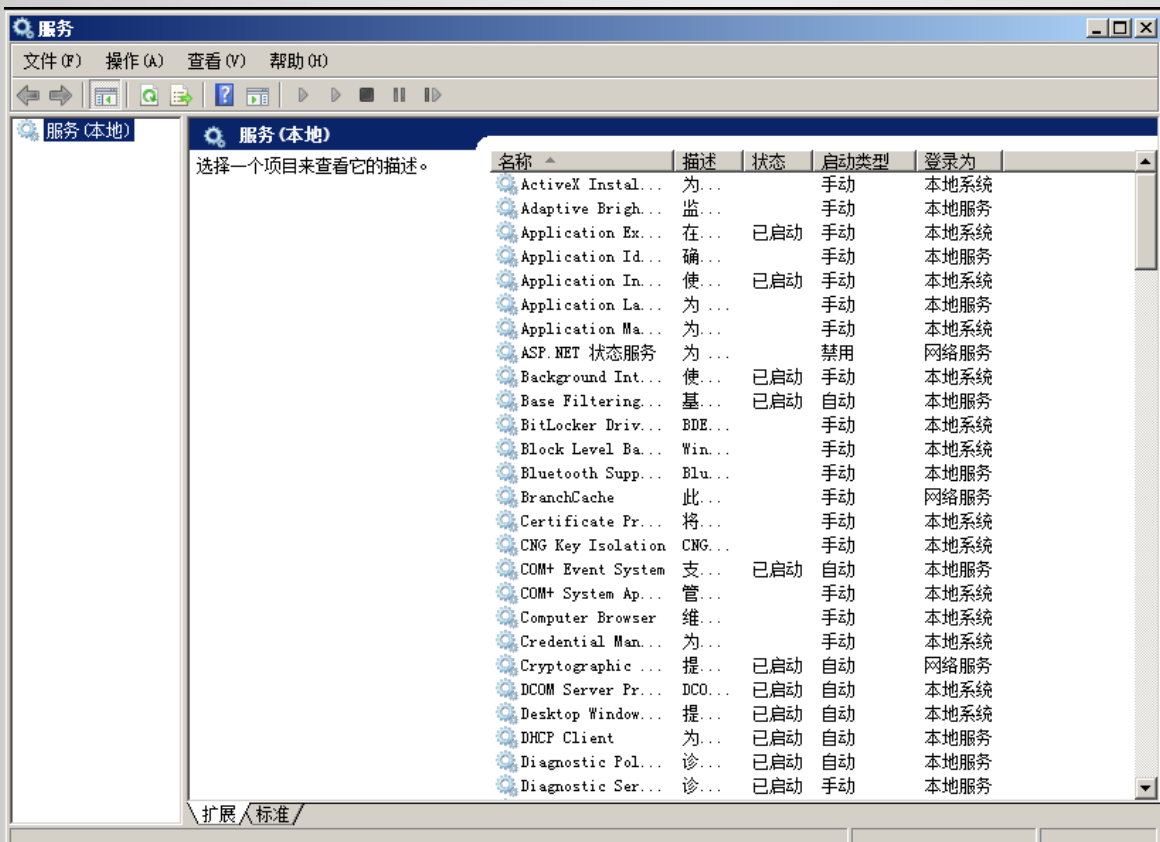
```
文件夹: \
任务名
=====
360ZipUpdater          N/A          就绪
Adobe Acrobat Update Task 2020/6/25 10:00:00 就绪
CCleaner Update        2020/6/24 16:27:57 就绪
CCleanerSkipUAC        N/A          就绪
GoogleUpdateTaskMachineCore 2020/6/25 11:57:09 就绪
GoogleUpdateTaskMachineUA  2020/6/24 12:57:09 就绪
npcapwatchdog          N/A          就绪
RtkAudUService64_BG    N/A          正在运行

文件夹: \Lenovo
任务名
=====
Lenovo ITS PnP Task     N/A          就绪
```

检查启动项、计划任务、服务

3、服务自启动

服务自启动 检查方法：单击【开始】>【运行】，输入services.msc，注意服务状态和启动类型，检查是否有异常服务



检查系统相关信息

1、查看系统版本以及补丁信息

检查方法：单击【开始】>【运行】，输入systeminfo，查看系统信息

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\admin>systeminfo

主机名:                ADMIN-PC
OS 名称:               Microsoft Windows 7 专业版
OS 版本:               6.1.7601 Service Pack 1 Build 7601
OS 制造商:             Microsoft Corporation
OS 配置:               独立工作站
OS 构件类型:           Multiprocessor Free
注册的所有人:          admin
注册的组织:
产品 ID:               00371-177-0000061-85381
初始安装日期:          2020/4/30, 13:22:27
系统启动时间:          2020/6/5, 11:49:52
系统制造商:            VMware, Inc.
系统型号:              VMware Virtual Platform
系统类型:              x64-based PC
处理器:                安装了 1 个处理器。
                       [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~340
                       8 Mhz
BIOS 版本:              Phoenix Technologies LTD 6.00, 2018/4/13
Windows 目录:           C:\Windows
系统目录:               C:\Windows\system32
启动设备:               \Device\HarddiskVolume1
系统区域设置:           zh-cn; 中文(中国)
输入法区域设置:         zh-cn; 中文(中国)
时区:                   (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量:           2.047 MB
可用的物理内存:         1.264 MB
虚拟内存: 最大值:       4.095 MB
虚拟内存: 可用:         3.239 MB
虚拟内存: 使用中:       856 MB
页面文件位置:           C:\pagefile.sys
域:                      WORKGROUP
登录服务器:              \ADMIN-PC
修补程序:                安装了 162 个修补程序。
                       [01]: KB2849697
                       [02]: KB2849696
                       [03]: KB2841134
                       [04]: KB2841134
```

检查系统相关信息

2、查找可疑目录及文件

检查方法：

a、查看用户目录，新建账号会在这个目录生成一个用户目录，查看是否有新建用户目录。

Window 2003 C:\Documents and Settings Window

2008R2 C:\Users\

b、单击【开始】>【运行】，输入%UserProfile%\Recent，分析近打开分析可疑文件。

c、在服务器各个目录，可根据文件夹内文件列表时间进行排序，查找可疑文件。



Windows系统日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。

Windows主要有以下三类日志记录系统事件：

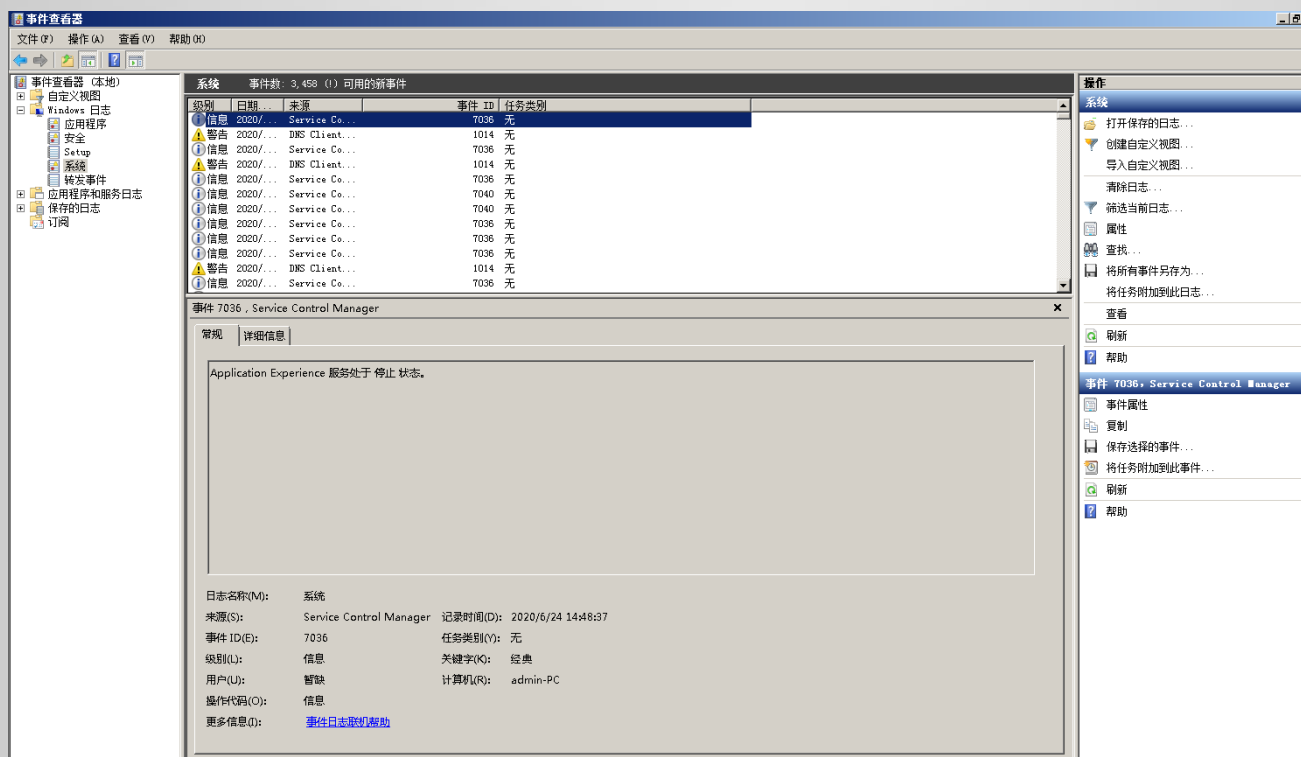
- 应用程序日志
- 系统日志
- 安全日志

Window事件日志简介

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



Window事件日志简介

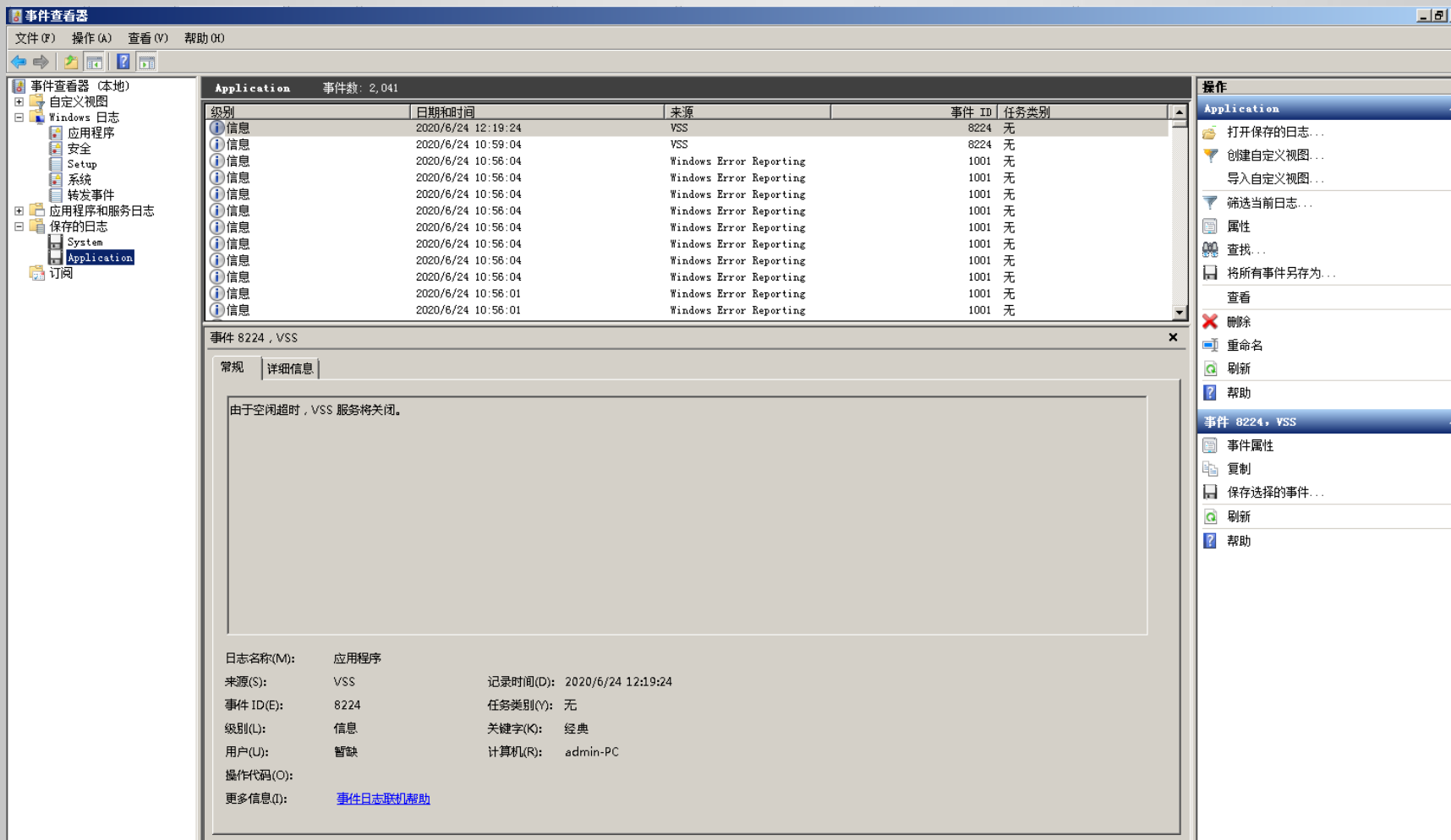
应用程序日志

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，也许会有助于你解决问题。

默认位置： %SystemRoot%\System32\Winevt\Logs\Application.evtx

Window事件日志简介

应用程序日志



The screenshot shows the Windows Event Viewer application. The left pane displays the tree view with 'Application' selected under 'Windows Logs'. The main pane shows a list of events, with event 8224 (VSS) selected. The right pane shows the details for event 8224, VSS, including the message '由于空闲超时, VSS 服务将关闭。' and various properties.

级别	日期和时间	来源	事件 ID	任务类别
信息	2020/6/24 12:19:24	VSS	8224	无
信息	2020/6/24 10:59:04	VSS	8224	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:04	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:01	Windows Error Reporting	1001	无
信息	2020/6/24 10:58:01	Windows Error Reporting	1001	无

事件 8224, VSS

常规 | 详细信息

由于空闲超时, VSS 服务将关闭。

日志名称(M): 应用程序
来源(S): VSS 记录时间(D): 2020/6/24 12:19:24
事件 ID(E): 8224 任务类别(Y): 无
级别(L): 信息 关键字(K): 经典
用户(U): 暂缺 计算机(R): admin-PC
操作代码(O):
更多信息(I): [事件日志联机帮助](#)

Window事件日志简介

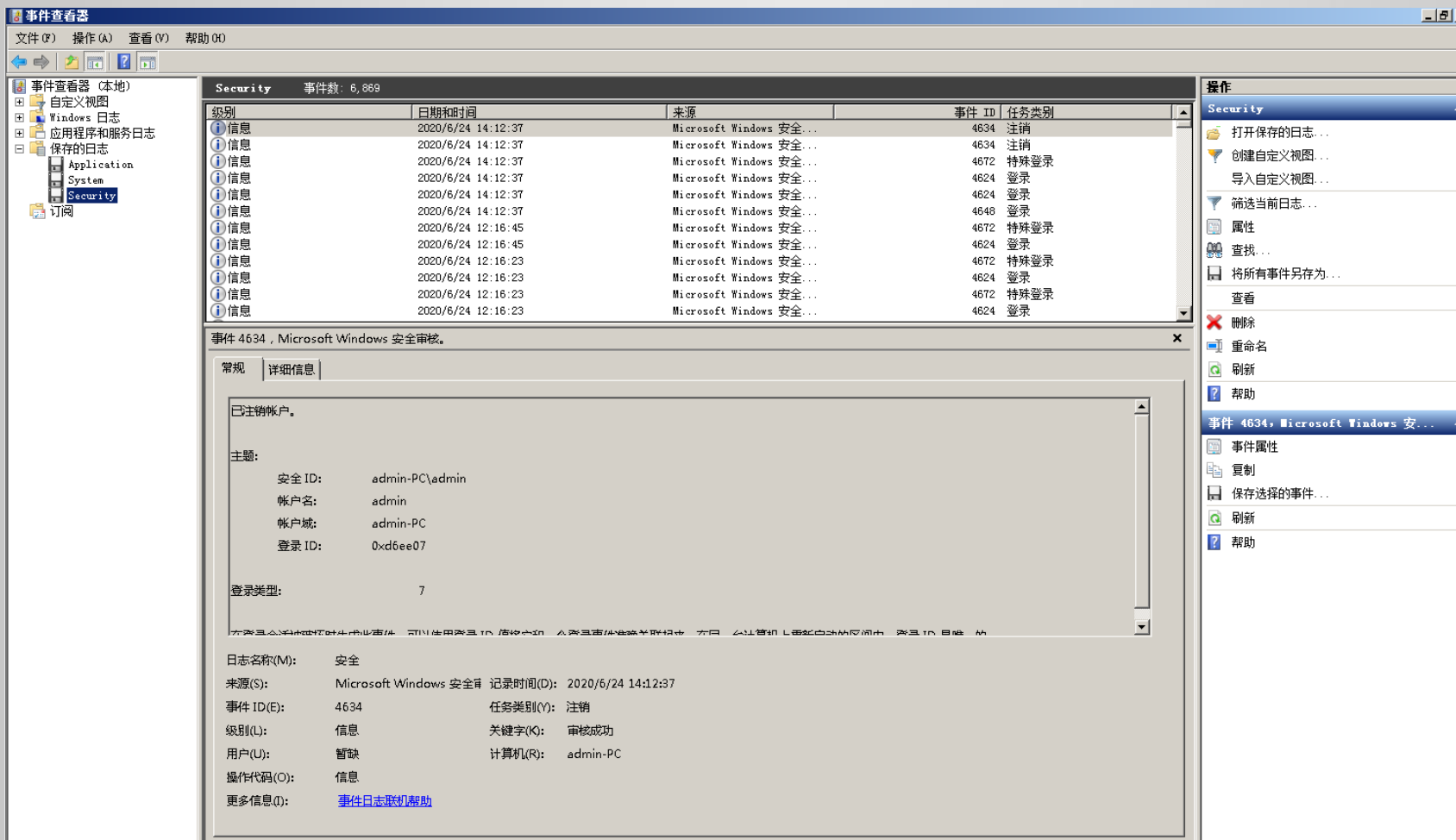
安全日志

记录系统的安全审计事件，包含各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、帐号管理、策略变更、系统事件。安全日志也是调查取证中最常用到的日志。默认设置下，安全性日志是关闭的，管理员可以使用组策略来启动安全性日志，或者在注册表中设置审核策略，以便当安全性日志满后使系统停止响应。

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

Window事件日志简介

安全日志



The screenshot displays the Windows Event Viewer application. The left pane shows the 'Security' log selected under 'Windows Logs'. The main pane shows a list of security events. The right pane shows the 'Operations' menu with options like 'Open saved log...', 'Create custom view...', 'Filter current log...', 'Properties', 'Find...', 'Save all events as...', 'View', 'Delete', 'Rename', 'Refresh', and 'Help'.

级别	日期和时间	来源	事件 ID	任务类别
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4634	注销
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4634	注销
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4672	特殊登录
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4624	登录
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4624	登录
信息	2020/6/24 14:12:37	Microsoft Windows 安全...	4648	登录
信息	2020/6/24 12:16:45	Microsoft Windows 安全...	4672	特殊登录
信息	2020/6/24 12:16:45	Microsoft Windows 安全...	4624	登录
信息	2020/6/24 12:16:23	Microsoft Windows 安全...	4672	特殊登录
信息	2020/6/24 12:16:23	Microsoft Windows 安全...	4624	登录
信息	2020/6/24 12:16:23	Microsoft Windows 安全...	4672	特殊登录
信息	2020/6/24 12:16:23	Microsoft Windows 安全...	4624	登录

事件 4634, Microsoft Windows 安全审核。

常规 | 详细信息

已注销帐户。

主题:

安全 ID: admin-PC\admin
帐户名: admin
帐户域: admin-PC
登录 ID: 0xd6ee07

登录类型: 7

日志名称(M): 安全
来源(S): Microsoft Windows 安全审核 记录时间(D): 2020/6/24 14:12:37
事件 ID(E): 4634 任务类别(Y): 注销
级别(L): 信息 关键字(K): 审核成功
用户(U): 暂缺 计算机(R): admin-PC
操作代码(O): 信息
更多信息(I): [事件日志联机帮助](#)

审核策略

Windows Server 2008 R2 系统的审核功能在默认状态下并没有启用，建议开启审核策略，若日后系统出现故障、安全事故则可以查看系统的日志文件，排除故障，追查入侵者的信息等。

PS：默认状态下，也会记录一些简单的日志，日志默认大小20M

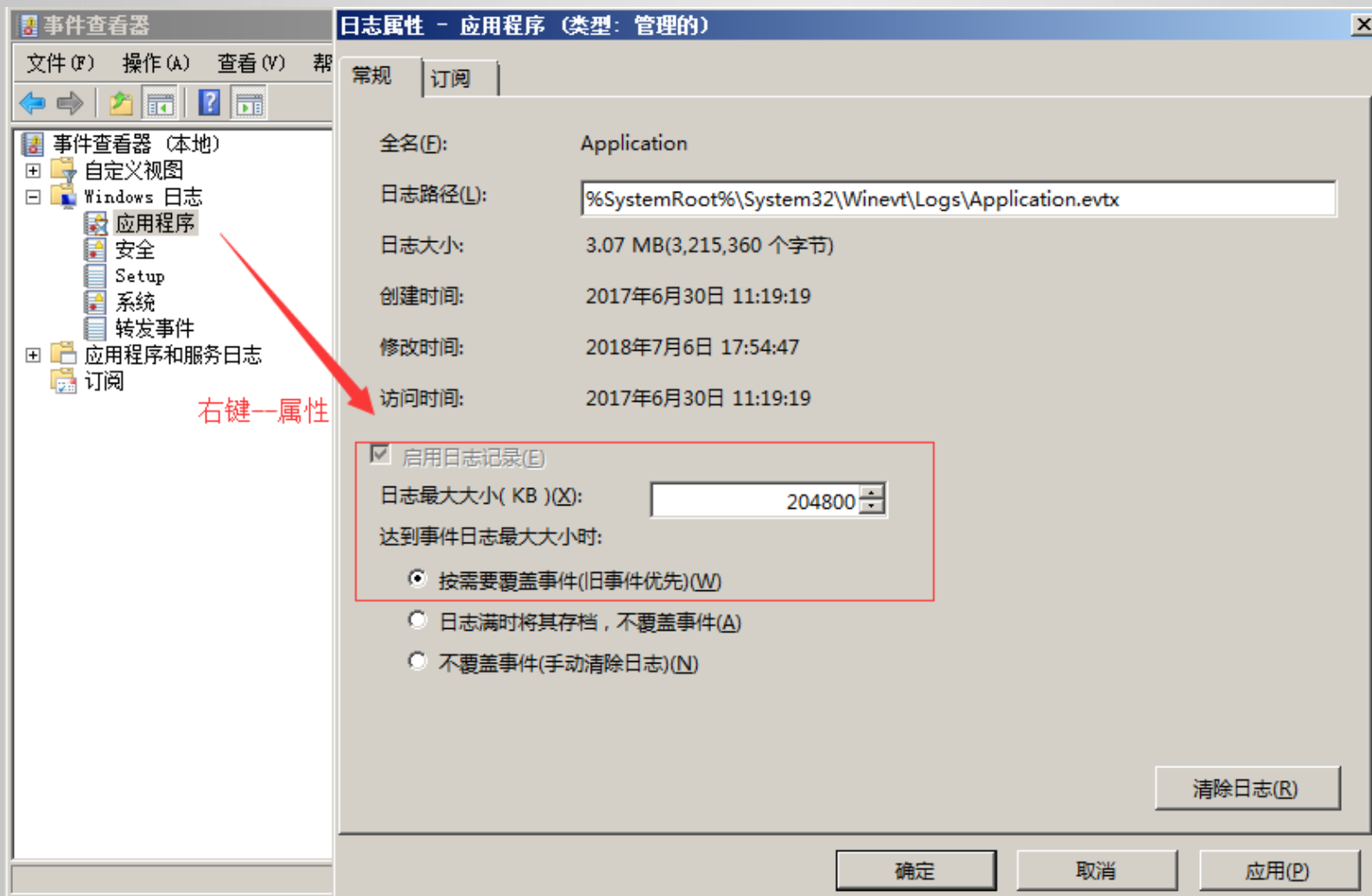
审核策略与事件查看器

设置1：开始 → 管理工具 → 本地安全策略 → 本地策略 → 审核策略，参考配置操作



审核策略与事件查看器

设置2：设置合理的日志属性，即日志最大大小、事件覆盖阈值等



审核策略与事件查看器

查看系统日志方法

在开始菜单上，所有程序->管理工具-> 事件查看器

按 "Window+R"，输入 "eventvwr.msc" 也可以直接进入“事件查看器”



事件日志分析

对于Windows事件日志分析，不同的EVENT ID代表了不同的意义，摘录一些常见的安全事件的说明

事件ID	说明
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
4720	创建用户

审核策略与事件查看器

事件日志分析

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

登录类型	描述	说明
2	交互式登录（Interactive）	用户在本地进行登录。
3	网络（Network）	最常见的情况就是连接到共享文件夹或共享打印机时。
4	批处理（Batch）	通常表明某计划任务启动。
5	服务（Service）	每种服务都被配置在某个特定的用户账号下运行。
7	解锁（Unlock）	屏保解锁。
8	网络明文（NetworkCleartext）	登录的密码在网络上是通过明文传输的，如FTP。
9	新凭证（NewCredentials）	使用带/Netonly参数的RUNAS命令运行一个程序。
10	远程交互，（RemoteInteractive）	通过终端服务、远程桌面或远程协助访问计算机。
11	缓存交互（CachedInteractive）	以一个域用户登录而又没有域控制器可用