**实验五、Window日志文件取证分析**

**一、实验目的**

了解Windows日志系统的作用

能够使用Windows自带工具软件获取相关日志信息

**二、实验内容**

查看Windows日志

理解日志事件类型

了解事件ID

根据安全日志所记录信息分析系统是否存在安全风险

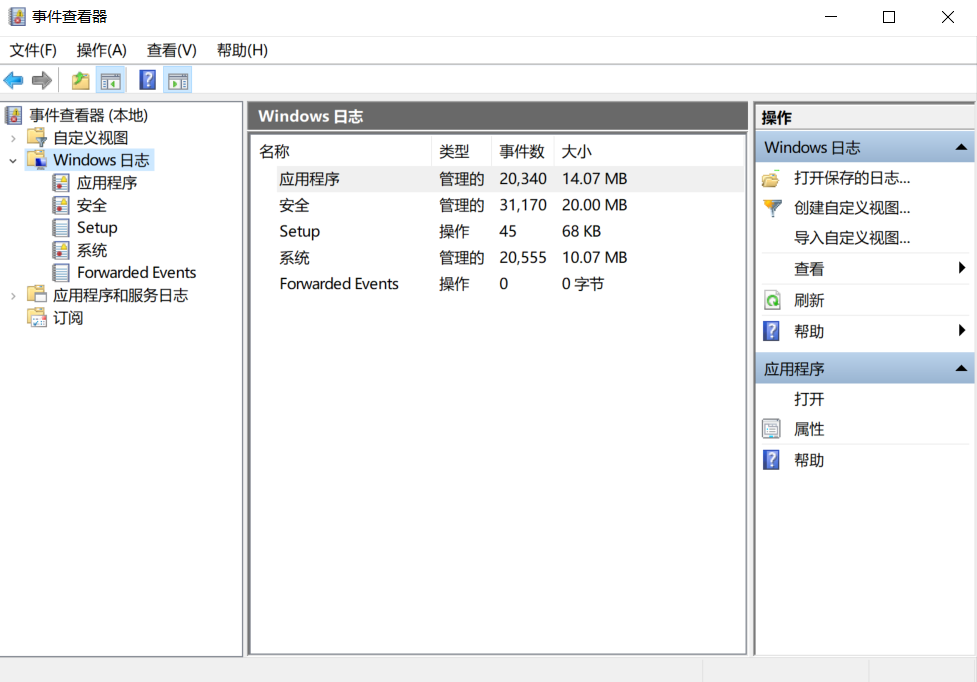
**三、实验步骤**

**1. 查看Windows日志**

(1).按“ win+R”，输入“eventvwr.msc”并回车，打开“事件查看器”。



(2).点击 “windows日志” 查看。



**2.理解五种日志事件类型**

****（1）信息（Information） ：信息事件指应用程序、 驱动程序或服务的成功操作的事件。

（2）警告（Warning）：警告事件指不是直接的、主要的，但是会导致将来问题发生的问题。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。

（3）错误（Error）：错误事件指用户应该知道的重要的问题。错误事件通常指功能和数据的丢失。例如,如果一个服务不能作为系统引导被加载，那么它会产生一个错误事件。

（4）成功审核（Success audit）：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。

（5）失败审核（Failure audit） ：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。

**3. 了解日志事件ID**

事件ID代表发生了什么事件，来源代表哪个程序或者服务干了这件事

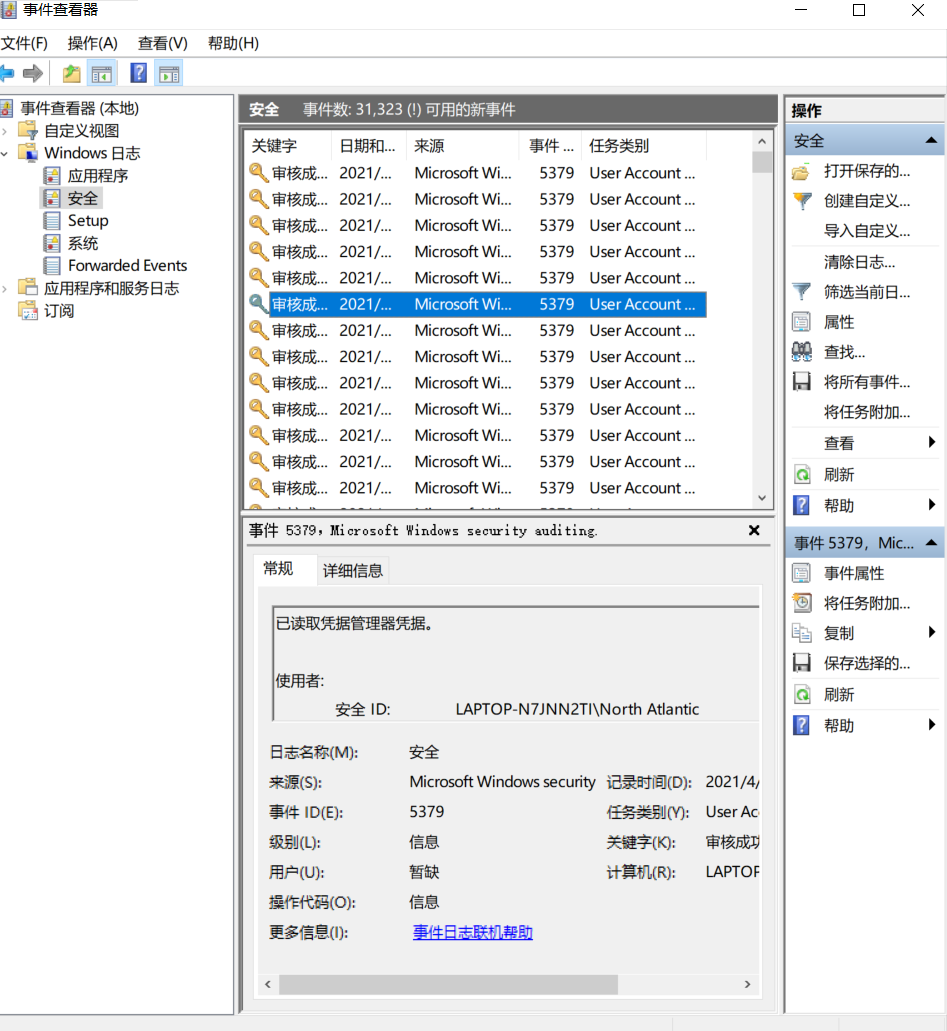
常见事件ID解释:

|  |  |  |  |
| --- | --- | --- | --- |
| 1001 | 信息 | Save Dump | 计算机已经从检测错误后重新启动。检测错误: 0x4a4b4d53 (0xc000000e, 0x01d04bf0, 0x00000010, 0x0000029a)。 已将转储的数据保存在: C:\WINDOWS\Minidump\Mini052809-01.dmp。 |
| 1005 | 警告 | Dhcp | 您的计算机检测到网络地址为 00A21C2EFEC4 的网卡的 IP 地址  192.168.1.2 已在网络上使用。 计算机会自动获取另一个地址。 |
| 4202 | 信息 | Tcpip | 系统检测到网卡 Realtek...Family PCI Fast Ethernet NIC –  数据包计划程序微型端口 与网络断开， 而且网卡的网络配置已经释放。  如果 网卡没有断开，这可能意味着它出现故障。  请与您的供应商联系以获得更新的驱动程序。 |
| 4226 | 警告 | Tcpip | TCP/IP 已经达到并发 TCP 连接尝试次数的安全限制。 |
| **6005** | 信息 | EventLog | 事件日志服务已启动。(开机) |
| **6006** | 信息 | EventLog | 事件日志服务已停止。(关机) |
| **6009** | 信息 | EventLog | 按ctrl、alt、delete键(非正常)关机 |
| 6011 | 信息 | EventLog | 此机器的 NetBIOS 名称和 DNS 主机名从 MACHINENAME 更改为 AA。 |
| **7036** | 信息 | Service Control Manager | xxx服务处于运行或停止等状态。 |

**4.根据安全日志所记录信息分析系统是否存在安全风险**

安全日志:

记录系统的审计事件, 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,系统事件等。安全日志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。



经筛查,该windows系统不存在安全风险

**四、实验结果**

1. 成功在事件查看器中查看Windows日志并理解windows 信息,警告,错误,成功审核,失败审核五种日志类型。

2. 了解了事件ID以及常见事件ID解释。

3. 成功根据安全日志所记录信息分析Windows系统是否存在安全风险,结果为不存在安全风险。

**五、写出本次实验的实验心得**

1. 通过本次实验了解Windows日志系统的作用并能够使用Windows自带工具软件获取相关日志信息;

2. 体会到进行实际实验操作对于计算机学习的重要性;

3. 在计算机专业学习过程中要扎实基础,深刻了解背后原理提高对计算机攻击的防御能力。