技术文献:Windows登录类型知多少? PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/140/2021_2022__E6_8A_80_E6_9C_AF_E6_96_87_E7_c100_140009.htm 如果你留意Windows系统的安全日志，在那些事件描述中你将会发现里面的“ 登录类型 ”并非全部相同，难道除了在键盘上进行交互式登录之外还有其它类型吗？不错，Windows为了让你从日志中获得更多有价值的信息，它细分了很多种登录类型，以便让你区分登录者到底是从本地登录，还是从网络登录，以及其它更多的登录方式。因为了解了这些登录方式，将有助于你从事件日志中发现可疑的黑客行为，并能够判断其攻击方式。下面我们就来详细地看看Windows的登录类型。登录类型2：交互式登录（Interactive） 这应该是你最先想到的登录方式吧，所谓交互式登录就是指用户在计算机的控制台上进行的登录，也就是在本地键盘上进行的登录，但不要忘记通过KVM登录仍然属于交互式登录，虽然它是基于网络的。 登录类型3：网络（Network） 当你从网络的上访问一台计算机时在大多数情况下Windows记为类型3，最常见的情况就是连接到共享文件夹或者共享打印机时。另外大多数情况下通过网络登录IIS时也被记为这种类型，但基本验证方式的IIS登录是个例外，它将被记为类型8，下面将讲述。 登录类型4：批处理（Batch） 当Windows运行一个计划任务时，“ 计划任务服务 ”将为这个任务首先创建一个新的登录会话以便它能在此计划任务所配置的用户账户下运行，当这种登录出现时，Windows在日志中记为类型4，对于其它类型的工作任务系统，依赖于它的设计，也可以在开始工作时产生类

型4的登录事件，类型4登录通常表明某计划任务启动，但也可能是一个恶意用户通过计划任务来猜测用户密码，这种尝试将产生一个类型4的登录失败事件，但是这种失败登录也可能是由于计划任务的用户密码没能同步更改造成的，比如用户密码更改了，而忘记了在计划任务中进行更改。 登录类型5：服务（Service） 与计划任务类似，每种服务都被配置在某个特定的用户账户下运行，当一个服务开始时，Windows首先为这个特定的用户创建一个登录会话，这将被记为类型5，失败的类型5通常表明用户的密码已变而这里没得到更新，当然这也可能是由恶意用户的密码猜测引起的，但是这种可能性比较小，因为创建一个新的服务或编辑一个已存在的服务默认情况下都要求是管理员或servers operators身份，而这种身份的恶意用户，已经有足够的能力来干他的坏事了，已经用不着费力来猜测服务密码了。 登录类型7：解锁（Unlock） 你可能希望当一个用户离开他的计算机时相应的工作站自动开始一个密码保护的屏保，当一个用户回来解锁时，Windows就把这种解锁操作认为是一个类型7的登录，失败的类型7登录表明有人输入了错误的密码或者有人在尝试解锁计算机。 登录类型8：网络明文（NetworkCleartext） 这种登录表明这是一个像类型3一样的网络登录，但是这种登录的密码在网络上是通过明文传输的，Windows Server服务是不允许通过明文验证连接到共享文件夹或打印机的，据我所知只有当从一个使用Advapi的ASP脚本登录或者一个用户使用基本验证方式登录IIS才会是这种登录类型。“ 登录过程 ”栏都将列出Advapi。 登录类型9：新凭证（NewCredentials） 当你使用带/Netonly参数的RUNAS命令运行一个程序时，RUNAS以本

地当前登录用户运行它，但如果这个程序需要连接到网络上的其它计算机时，这时就将以RUNAS命令中指定的用户进行连接，同时Windows将把这种登录记为类型9，如果RUNAS命令没带/Netonly参数，那么这个程序就将以指定的用户运行，但日志中的登录类型是2。 登录类型10：远程交互（RemoteInteractive） 当你通过终端服务、远程桌面或远程协助访问计算机时，Windows将记为类型10，以便与真正的控制台登录相区别，注意XP之前的版本不支持这种登录类型，比如Windows 2000仍然会把终端服务登录记为类型2。 登录类型11：缓存交互（CachedInteractive） Windows支持一种称为缓存登录的功能，这种功能对移动用户尤其有利，比如你在自己网络之外以域用户登录而无法登录域控制器时就将使用这种功能，默认情况下，Windows缓存了最近10次交互式域登录的凭证HASH，如果以后当你以一个域用户登录而又没有域控制器可用时，Windows将使用这些HASH来验证你的身份。 上面讲了Windows的登录类型，但默认情况下Windows 2000是没有记录安全日志的，你必须先启用组策略“ 计算机配置/Windows设置/安全设置/本地策略/审核策略 ”下的“ 审核登录事件 ”才能看到上面的记录信息。希望这些详细的记录信息有助于大家更好地掌握系统情况，维护网络安定。