windows 系统安全

1. Windows 安全子系统，安全子系统包括以下部分，winlogon，图形化标识和验证 GINA，本地安全认证，安全认证者提供的接口，认证包，安全支持提供者，网络登录服务，安全账号管理者，下面详细说说这些东西都是干嘛的

a) Winlogon 和 GINA ,winlogon 调用 GINA DLL 并监视安全序列 ,而 GINADLL 通过提供一个交互式的界面为用户登录提供认证请求，GINA DLL 被设计为一个独立的模块，也可以用一个更好的方式比如指纹识别来代替内置的 GINA DLL 模块。在启动的过程中先加载 winlogon，然后 winlogon 加载 GINA DLL，GINA 负责提供一个登录接口，在开始的过程中，winlogon 会首先加载注册表，查看 HKLM/Software/Microsoft/Windows NT/CurrectVersion/Winlogon 然后在里面查看是不是存在 GinaDLL 键，如果不存在的话，那么系统调用自带的 msgina.dll

b) 本地安全认证，本地安全认证 LSA 是安全子系统的核心，它的作用就是加载认证包，管理域间的信任关系，GINA DLL 在提供登录接口之后，调用的就是 LSA 用于加载认证包，

c) 安全支持者提供的接口，微软的安全支持提供者提供的接口 SSPI 用于提供一些安全服务 API，为应用程序和服务提供请求安全的认证连接和

d) 认证包为真实用户提供认证 ,在通过 GINA DLL 的可信认证之后认证包返回用户的 SIDs 给 LSA，然后将其放在用户的访问令牌中

e) 安全支持提供者 ,安全支持提供者用于实现一些附加的安全机制 ,安装时以驱动程序的形式安装 ,默认会有 Msnsspc.dll（微软网络挑战反应认证模块），Msapsspc.dll 分布式密码认证挑战反应模块和 Schannel.dll 证书模块等

f) 网络登录服务，这个服务用于在通过认证之后建立一个安全的通道，要实现这个目标必需通过安全通道与域中的域控制器来建立连接，然后通过安全的通道传递用户口令，在域的域控制器上的响应请求之后，重新取回用户的 SIDs 和用户权限

g) 安全账号管理器 SAM，这个是一个用来保护用户用户名和密码的数据库，不同的域有不同的 SAM，在域复制的过程中，Sam 包将会被拷贝

2. Windows 对用户账号的安全管理使用了安全账号管理器机制，安全账号管理器对账号的管理通过安全标志进行，安全标志是唯一的，即便用户名相同。SAM 保存在%systemroot%\system32\config\sam 里面，该文件是 windows 的用户账户数据库，在 windows 域控制器中，账户和口令被保存在活动的目录里面，对应的文件是%systemroot%\ntds\ntds.dit

3. 还有一个机制就是 syskey，在运行里面输入就可以对系统进行二重加密，而且这个加密一旦启用就无法关闭，这个加密就是对 windows 账户数据库的加密

4. 登录验证，在用户尝试登录 windows 时，系统会首先使用默认的 kerberos 作为基本的验证机制，如果找不到密钥分发中心的 KDC 服务，那么就会使用 NT 的 NTLM 安全机制来验证本地的 SAM 用户，验证过程如下：

a) 输入用户名密码之后 GINA 会收集这些信息

b) 然后 GINA 把信息传送给 LSA，LSA 再传递给 SSPI（安全支持者提供的接口）

c) SSPI 将用户名密码传递给 KerberosSSP，然后检查目的及其是本机还是域名，如果是本机，那么返回错误消息给 SSPI，如果找不到 KDC，则机器生成

一个用户不可见的内部错误，这个内部错误促发 SSPI 通知 GINA，然后 GINA 再次传送这些信息给 SSPI，SSPI 传送用户名密码给 NTML，然后 NTML 使用 Netlogon 服务和本地 SAM 来验证用户

5. 用户权限与权力，网络的安全取决于给用户或组的授权能力，包括权限、权力和共享。权限是可以授予用户或做的文件系统能力，分为登录权限和操作权限，权力是在系统上完成指定动作的授权

a) 用户权力，权力适用于对整个系统范围内的对象和任务，通常是授权用户执行某些系统任务，比如允许用户关闭系统等

b) 用户权限，权限适用于特定的对象，比如目录和文件（只适用于 NTFS 的卷）的操作，允许那个用户可以使用这些对象和如何使用这些对象，权限分为 RXWDPO，R 读，X 执行，W 可写，D 删除，P 更改权限，O 获取目录的所有权，

c) 共享权限，共享权限适用于文件夹，如果文件夹不是共享的，那么在网络上就不会有人看到它，也就无法访问

6. 日志与审计，windows 有 3 种类型的事件日志

a) 系统日志，用于跟踪系统时间，跟踪系统的启动过程中的事件或控制器的故障

b) 应用程序日志，跟踪用户程序关联的事件，比如应用程序加载的 dll，或失败的信息

c) 安全日志，安全日志的默认状态是关闭的，用于记录登录上网和下网，改变访问权限以及系统的启动和关闭，日志的默认存储路径在 %systemroot%\system32\config 中，位于注册表的

HKLM\System\CurrentControlSet\Services\Eventlog 后，下面的 Application，Security，System 三个子文件分别对应了应用程序，安全，系统三个日志

d) 设置文件的访问权限，首先应用为 NTFS 格式的磁盘，可以在文件属性的安全选项卡中进行设置，进入安全标签之后应首先取消允许将父系的可继承权限传播给该对象选项，然后在下面的用户中选择该文件的权限。

e) 日志审计的基本规则

i. FTP 日志分析，在#DATE 后面显示的为日期，然后在下面显示的信息依次是：

时间，IP 地址，USER，用户名， 331（试图登录）

时间，IP 地址，PASS – 530（登录失败）

时间，IP 地址，PASS – 230（登录成功）

时间，IP 地址，PASS – 530（登录失败）

ii. HTTP 日志分析，基本顺序为： 日期，时间，访客 IP，访问的 IP，端口，后面可能是 GET 然后一个文件（或网页），后面的信息是浏览器和操作系统

7. 安全策略：

a) 密码策略，这个可以在控制面板本地安全策略里面找到，设置的密码必需符合安全性要求，并且有效期默认为 42 天，其中所有的选择的都是可以自己设置的，包括密码的安全性要求的开关等

b) 锁定策略，可以在本地安全策略里面设置账户锁定策略，就是输入多少次密码输入错误之后执行的操作

c) 审核策略，审核策略是网络安全的核心之一，这个也是在本地安全策略 secpol.msc 里面的，审核报告会被写入安全日志，可以使用事件查看器来查看，

d) 用户权力指派，安全组定义了从建立页面文件到登录服务器控制台的各种权力。用户和组通过被添加到相应的安全组页面而得到的这些系统权限

e) 安全选项 :安全选项包括了一些与安全有关的注册表项 ,这些表项与用户无关，只影响到常规的系统操作，可以使用 secedit 命令来更改，可以使用 Refresh-policyMachine_policy 在不重启计算机的情况下刷新策略

f) 装载自定义的安全模板 :安全模板是对整个系统安全属性的一个配置文件，系统管理员可以生产一个安全模板 ,并把它应用于本地计算机或输出到一个活动目录的组策略对象，当一个新的模板加入到一个新的组策略之后，所有受它所影响的计算机都会接收到模板的设置，

g) Windows 加密文件系统，用于提供一种核心文件的加密技术，用于 NTFS 的卷上