安全计算环境-操作系统-终端（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	用户的身份标识和鉴别，就是用户向操作系统以一种安全的方式提交自己的身份证实，然后由操作系统确认用户的身份是否属实的过程，身份标识要求具有唯一性。在用户进入Windows桌面前，如果弹出一个用户登录界面，要求用户输入用户名和密码，Windows 操作系统对用户的用户名和密码进行验证通过后，用户可以登录操作系统。 猜测密码是操作系统最常遇到的攻击方法之-，因此对操作系统的密码策略提出要求，在Windows操作系统中，要求密码历史记录、密码最短长度、密码复杂度等，并要求定期更换	1)用户需要输入用户名和密码才能登录 2)windows默认用户名具有唯一性 3)打开“控制面板”-》“管理工具”-》“计算机管理”一“本地用户机组”检查有哪些用户，并尝试空口令登录 4)打开“控制面板”-》“管理工具”-》 “本地安全策略”一》“账户策略”“密码策略”	1)用户登录需输入用户名和密码 2)用户具备唯一性: 3)尝试使用空口令登录，未成功 4)结果如下: a)复杂性要求:已启用: b)密码长度最小值:长度最小值至少为8位 c)密码长度最长使用期限。不为0 d)密码最短使用期限:不为0 e)强制密码历史:至少记住5个密码以上	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	非法用户能够通过反复输入密码，达到猜测用户密码的目的，因此应该限制用户登录过程中连续输入错误密码的次数。 当用户多次输入错误密码后，操作系统应自动锁定该用户或一段时间内禁止该用户登录，从而增加猜测密码难度的目的。 Windows操作系统具备登录失败处理功能，可以通过适当的配置“账户锁定策略”来对用户的登录进行	1)打开“控制面板”-》 “管理工具”-》“本地安全策略”一》 “账户策略”一》“密码锁定策略” 2)右键点击桌面->“个性化”->“屏幕保护程序”，查看“等待时间”的长短以及“在恢复时显示登录屏幕”选项是否打钩	1)结果如下: a)账户锁定时间:不为不适用 b)账户锁定阈值:不为不适用 2)启用了远程登录连接超时并自动退出功能	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	为方便管理员进行管理操作，众多服务器采用网络登录的方式进行远程管理操作，Windows一般使用“远程桌面 (Remote Desktop)”进行远程管理，《基本要求》中规定了这些传输的数据需要进行加密处理，目的是为了保障账户和口令的安全	1)如果是本地管理成KVM等硬件管理方式，此要求默认满足 2)如果采用远程管理，则需采用带加密管理的远程管理方式。在命令行输入”pgedit.msc“弹出“本地组策略编辑器”窗口，查看“本地计算机策略一》计算机配置一>管理模板一>Windows组件一选程桌面服务>远程桌面会话主机-安全”中的相关	1)本地或VM，默认符合 2)远程运维，采取加密的RDP协议	符合情况：采用RDP远程桌面方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用RDP远程桌面方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
访问控制	a)应对登录的用户分配账户和权限	访问控制是安全防范和保护的主要策略，操作系统访问控制的主要任务是保证操作系统资源不该非法使用和访问，使用访问控制的目的在于通过限制用户对特定资源的访问来保护系统资源。在操作系统中的每一个文件或目录都包含有访问权限，这些访可权限决定了谁能访问和如何访问这些文件和目录。对于操作系统中一些重要的文件，则需要严格控制其访问权限，从而加强系统的安全性。因此，为了确保系统的安全，需要对登录的用户分配账户，并合理配置账户权限。 在Windows系统中，重要目录不能对“everyone”.账户开放，因为这样会带来很大的安全问题，在权限控制方面，尤其要注意当文件权限更改后对于应用系统的影响	访谈系统管理员，操作系统能够登录的账户，以及它们拥有的权限。 选择%systemdrive%\windows\system、%systemroot %\system32\config 等相应的文件夹，右键选择“属性”>“安全”，查看everyone组、users组和administrators组的权限设置	各用户具备最小角色，分别登录；不存在匿名用户，默认用户只许可管理员可以登录	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	对于操作系统的默认账户，由于它们的某些权限与实际系统的要求可能存在差异，从而造成安全隐患，因此这些默认账户应重命名或被删除，并修改默认账户的默认口令。Windows 的系统管理员账户名称就是Administrator,在一定环境下，黑客可以省略猜测用户名这个步骤，直接破解密码。因此，允许默认账访问的危害性是显而易见的	在命令行输入“lusrmgr.msc“弹出“本地用户和组”窗口，查看“本地用户和组->用户”中的相关项目	1查看右侧列表中Window系统的认账Administrato,是否枝被禁用或重命名 2)询问是否已修改默认账户口令 3)查看是否已经禁用guest账户	符合情况：不存在默认的、无用的可登录账户，已禁用guest账户 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改，未禁用guest账户
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	在命令行输入“lusmrgr.msc“,弹出“本地用户和组”窗口，查看“本地用户和组一>用户”中的相关项目，查看右侧用户列表中的用户,询问各账户的用途，确认账户是否属于多余的、过期的账户或共享账户名	不存在多余账户、测试过期账户。不存在多部门、多人共享账户情况	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户

入侵防范	a)应遵循最小安装的原则仅安装需要的组件和应用程序	Windows默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序等。有些操作系统中运行的多余服务和应用程序，如:存在某台终端作为共享打印机使用	1)查看和询问安装的组件情况 在命令行输入"dcomcnfg" ,打开组件服务界面,打开"控制台根节点"->"组件服务"—>"计算机"->"我的电脑".查看右侧组件列表中的组件内容。询问系统管理员，安装的各组件的用途，有无多余的组件 2)查看和询问安装的应用程序情况 在命令行输入"appwiz.cpl,打开程序和功能界面，查看右侧程序列表中的安装的应用程序 询问系统管理员，安装的应用程序的用	1)系统安装遵循最小化安装原则 2)不存在业务所不需要的组件和应用程序	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	b)应关闭不需要的系统服务、默认共享和高危端口	Windows默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其禁用或卸载。Windows 会开启默认共享，例如C$、D$,为了避免默认共享带来的安全风险，应关闭Windows硬盘默认共享。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序，关闭高危端口，是操作系统常用的安全加固方式	1)查看系统服务。 在命令行输入"services. msc"，打开系统服务管理界面，查看右侧的服务详细列表中多余的服务，如Alerter、Remote Registry Servicce Messsenger,Task Scheduler是否已启动。 2)查看监听端口。 在命令行输入"netstat -an"，查看列表中的监听端口，是否包括高危端口，如 TCP 135、139 、45、 593、1025端口，UDP 135、137、 138、445端口，-些流行病毒的后门端口，如TCP 2745、3127、6129端口。 3)查看默认共享。 在命令行输入"net share"，查看本地计算机上所有共享资源的信息，是否打开了默认共享，例如C$、D$ 4)查看主机防火墙策略 在命令行输入"firewal1. cpl"打开Windows防火墙界面，查看Windows防火墙是否启用。点击左侧列表中的"高级设置"，打开"高级安全Windows防火墙"窗口。点击左侧列表中的"入站规则"，右侧显示Windows防火墙的入站规则，查看入站规则中是否	1)不存在多余的服务 2)未启用 不必要的端口 3)未开启默认共享 4）防火墙规则中阻止访问多余的服务，或高危端口	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	通过设定终端接入方式、 网络地址范围等条件限制终端登录，可以极大的节省系统资源，保证了系统的可用性，同时也提高了系统的安全性。对Windows自身来说， 可以通过主机防火墙或TCP/IP筛选来实现以 上功能	1)询问系统管理员管理终端的接入方式。 查看主机防火墙对登录终端的接入地址限制 在命令行输入"firewall.cpl",打开Windows防火墙界面，查看Windowsd防火墙是否启用。点击左侧列表中的"高级设置"，打开"高级安全Windows防火墙"窗口，点击左侧列表中的"入站规则"，双击右侧入站规则中的"远程桌面—用户模式(TCP-In)"，打开"远程桌面用户模式(TCP-In)属性" 窗口，选择"作用城"查看相关项目。 查看IP筛选器对登录终端的接入地址限制 在命令行输入"gpedit.msc"打开本地组策路编辑器界面，点击左侧列表中的"本地计算机策略->计算机配置Windows设置->安全设置->IP安全策略"，在本地计算机双击右侧限制登录终端地址的相关策略"，查看"IP 筛选器列表"和"IP筛选器属性" 2)网络方面对登录终端的接入方式和地址范围的限制 询问并查看是否通过网络设备或硬件防火墙对终端接入方式、网络地址范围等条件	1)通过主机防火墙设置访问控制规则 2)通过网络防火墙、堡垒主机限制、ip段进行接入地址限制	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网络地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制

	d) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，.避免遭受由系统漏洞带的风险	访谈系统管理员是否定期对操作系统进行漏洞扫描，是否对扫描发现的漏洞进行评估和补丁更新测试，是否及时进行补丁更新，更新的方法。 在命令行输入"appwiz.cp1" ,打开程序和功能界面，点击左侧列表中的"查看已安装的更新"，打开"已安装更新"界面，查看右侧列表中的补丁更新情况	对操作系统补丁进行测试和安装，补丁情况为较新稳定版本	
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断	作为Windows系统，木马和蠕虫的泛滥使得防范恶意代码的破坏显得尤为重一要，因此应采取避免恶意代码攻击的技术措施或采取可信验证技术，如在主机上部署防病毒软件或其他可信验证技术。基于网络和基于主机的防病毒软件在系统上应构成立体的防护结构，属于深层防御的一部分。因此基于网络的防病毒软件的病毒库应与基于主机的防病毒软件的病毒库不同。只有当所有主机都及时更新了病毒库才能够做到防止病毒的入侵。因此应有统一的病毒管理策略，统一更新病毒库，定时查杀，及时发现入侵行为有效阻断等	1)查看系统中安装的防病毒软件。询问管理员病毒库更新策略。查看病毒库的最新版本更新日期是否超过一个星期 2)查看系统中采取何种可信验证机制，访谈管理员实现原理等 3)询问系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库 4)询问系统管理员是否果有统一的病毒更新策略和查杀策略 5)当发现病毒入侵行为时，如何发现，如何有效阻断等，报警机制等	)安装有网络版杀毒软件，病毒库最新 2)查看系统中采取何种可信验证机制，实现原理为基于可信根TPM技术等 3)网络版防病毒和主机防病毒均具备不同的病毒库，异构特点4)防病毒为网络版，统一更新病毒库 5)发现病毒入侵，有邮件报警机制	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	针对终端设备，需要终端在启动过程对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)进行完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1）核查终端的启动,是否实现可信验证的过程，查看对那些系统引导程序、系统程序或重要配置参数数进行可信验证 2 修改其中的重要系统程序之-和应用程序之-，核查是否能够检测到并进行报警 3）是否将验证结果形成审计记录送至安全管理中心	1）终端具有可信根芯片或硬件 2） 启动过程基于可信根对引导程序、系统程序、重要配置参数和应用程序等进行可信验证 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录	符合情况：服务器具有可信根芯片或硬件，可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心