安全计算环境-操作系统-Redhat（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	Linux系统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，这样用户就具备一个私有口令。etc/password文件中记录用户的属性信息，包括用户名、密码、用户标识、组标识等信息。现在Linux系统中不再直接保存在/etc/password文件中,通常将password文件中的口令字段使用一个“x”来代替，将/etc/shadow作为真正的口令文件，用于保存包括个人口令在内的数据。当然，shadow文件是不能被普通用户读取的，只有超级用户才有权读取。 Linux中的/etc/login.defs是登录程序的配置文件，在这里我们可配置密码的最大过期天数，密码的最大长度约束等内容。如果/etc/pam.d/system-auth文件里有相同的选项，则以/etc/pam.d/system-auth里的设置为准，也就是说/etc/pam.d/system-aut的配置优先级高于/etc/login.defs。 Linux系统具有调用PAM的应用程度认证用户。登示服务、屏保等功能，其中一个重要的文件使是etc/pam.d/system-auth 。/etc/pam.d/system-auth或/etc/login.defs中的配置优先级高于其他地方的配置	1)访谈系统管理员系统用户是否已设置密码，并查看登录过程中系统账户是否使用了密码进行验证登录。 2)以有权限的账户身份登录操作系统后，使用命令more查看/etc/shadow文件，核查系统是否存在空口令账户 3)使用命令more查看/etc/login. defs文件，查看是否设置密码长度和定期更换要求 #more /etc/login. defs 使用命令more查看/etc/pam.d/system-auth文件。查看密码长度和复杂度要求 4)检查是否存在旁路或身份鉴别措施可绕过的安全风险	1)登录需要密码 2)不存在空口令账户 3)得出类似反馈信息，如下: PASS MAX_DAYS 90 #登录密码有效期90天 PASS MIN_DAYS 0 #登录密码最短修改时间，增加可以防止非法用户短期更改多次 PASS MIN_LEN 7 #登录密码最小长度7位 PASS WARN_AGE 7 #登录密码过期提前7天提示修改 4)不存在绕过的安全风险	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	Linux系统具有调用PAM的应用程度认证用户、登录服务、屏保等功能，其中一个重要的文件便/etc/pam.d/system-auth，Redhat5以后版本使用pam_tally2.so模块控制用户密码认证失败的次数上限，可以实现登录次数、超时时间，解锁时间等。 着只是针对某个程序的认证规则，在PAM目录(/etc/pam d)下形如sshd、login 等等的对应各程序的认证规则文件中进行修改。若所有密码认证均应用规则，可直接修改system auth文件	1)系统配置并启用了登录失败处理功能 2)以root身份登录进入Linux，查看文件内容: # cat /ete/pam.d/system -auth或根据linux版本不同在common文件中 3)查看/etc/profile中的TIMEOUT环境变量，是否配置超时锁定参数	得出类似反馈信息，如下: 1) 和 2) 查看登录失败处理功能相关参数，/etc/pam.d/system — auth 文件中存在"account required /lib/security/pam_tally.so deny=3 no_ magic root reset"； 3)记录在文件/etc/profile中设置了超时锁定参数，在profile下设置TMOUT= 300s	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	Linux提供了远程访问与管理的接口，以方便管理员进行管理操作，网络登录的方式也是多样的，例如可以使用Telnet登录，也可以使用SSH登录。但是，Telnet不安全。I因为其在数据传输过程中，账户与密码均明文传输，这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码，因此不建议通过Telnet协议对服务器进行远程管理。针对Telnet协议不安全这种情况，可以在远程登录时使用SSH协议。其原理跟Telnet类似，只是其具有更高的安全性。SSH是一个运行在传输控制层上的应用程序，与Telnet相比，它提供了强大的认证与加密功能，可以保证在远程连接过程中，其传输的数据是加密处理过的。因此保障了账户与口令的安全	访谈系统管理员，进行远程管理的方式。 1)以root身份登录进入Linux查看是否运行了sshd服务，service - status-all	grep sshd 查看相关的端口是否打开，netstat -an|grep 22 若未使用SSH方式进行远程管理，则查看是否使用了Telnet 方式进行远程管理 service - -status-all|grep running, 查看是否存在Telnet服务 2)可使用wireshark等抓包工具，查看协议是否为加密 3)本地化管理，N/A	1)使用SSH方式进行远程管理，防止鉴别信息在传输过程中被窃听,Telnet默认不符合 2)通过抓包工具，截获信息为密文，无法读取，协议为加密 3) N/A本地管理	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH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
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	对于第三级及以上的操作系统要求采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	访谈和核查系统管理员在登录操作系统的过程中使用了哪些身份鉴别方法，是否采用了两种或两种以上组合的鉴别技术，如口令教字证书Ukey、令牌、指纹等，是否有一种鉴别方法在鉴别过程中使用了密码技术	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术，如调用了密码机或采取SM1-SM4等算法	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技
访问控制	a)应对登录的用户分配账户和权限	对于Linux中一些重要的文件，应检查Linux系统主要目录的权限设置情况，Linux系统对文件的操作权限，包括4种:读(r,4)；写(w,2)；执行(x,1)；空(一，0)，文件的权限分为属主(拥有者)、属组、其它用户和用户组的权限	以有相应权限的身份登录进入Linux,使用“1s-1文件名”命令，查看重要文件和目录权限设置是否合理，如: # 1s -1 /etc/passwd #744。	重点查看以下文件和目录权限是否设置合理。 —rwx- - - - -:数字表示为700 -rwxr--r- -:数字表示为744 -rw-rw-r-x:数字表示为665 drwx-x—x:数字表示为711 drwr- - - - -:数字表示为700 配置文件权限值不能大于644，对于可执行文件不能大于755	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	Linux操作系统本身安装后提供各种账号，如adm lp sync shutdown halt mail uucp operator games gopher ftp等，但这些账户使用时并不需要，有的帐号越多，就越容易受到攻击，应禁用或者删除这些用户。 root作为重要的默认账户，一般要求禁止远程登录	1)以有相应权限的身份登录进入Linux,使用more查看/etc/shadow文件，查看文件中的用户，是否存在adm、lp. sync、 shutdown、 halt.、mail、 uucp、 operator,、games.、gopher ftp等默认的、无用的用户。 2)查看root账户是否能够进行远程登录	1)不存在默认无用的账户 2)使用more查看/etc/ssh/sshd_config文件中的“PermitRootLogin”参数设置为“no“，即:PermitRootLogin no, 即不许可root远程登录	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 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
	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	通常操作系统在运行一段时间后，因业务应用或管理员岗位的调整，出现一些多余的、过期的账户；另一方面，也会出现多个系统管理员或用户使用同一账户登录操作系统的情况，造成审计追踪时无法定位到自然人。如果存在多余的，过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理系统中的账户，删除或停用多余的、过期的账户，同时避免共享账户的存在	1)应核查是否不存在多余或过期账户，如查看games、news、 ftp、 1p等系统默认账户是否被禁用，特权账号halt、shutdown是否被删除 2)应访谈网络管理员、安全管理员、系统管理员不同用户是否采用不同账户登录系统	1)禁用或删除不需要的系统默认账户，如games、news、 ftp、 1p、halt、shutdown等 2)各类管理员均使用自己分配的特定权限账户登录，不存在多余、过期账户	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
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	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。Linux 系统安装后，root拥有所有权限，使用sudo授予普通用户root级权限，在sudoer.conf中进行配置	1)以有相应权限的身份登录进入Linux, 使用more查看/etc/passwd文件中的非默认用户，询问各账户的权限，是否实现管理用户的权限分离 2)以有相应权限的身份登录进入Linux, 使用more查看/etc/sudo.conf文件，核查root级用户的权限都授予哪些账户	1)各用户均具备最小权限,不与其他用户权限交叉。设备下可支持新建多用户角色功能 2)管理员权限仅分配root用户	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理

	d)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	操作系统的访问控制策略应由授权主体（如安全管理员）进行配置，非授权主体不得更改访问控制策略。访问控制策略规定操作系统用户对操作系统资源(如文件和目录)具有哪些权限，能进行哪些操作、通过在操作系统中配置访问控制策略，实现对操作系统各用户权限的限制	1)访谈系统管理员，是否指定授权人对操作系统访问控制权限进行配置 2)核查账户权限配置，是否依据安全策略配置各账户的访问规则	1)由专门的安全员负责对访问控制权限的授权工作 2)各账户权限配置，均是基于安全员的安全策略配置进行的访问控制	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	e)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	使用"ls -1文件名"命令，查看重要文件和目录权限设置是否合理,如:#ls -1/etc/passwd #744,应重点查看以下文件和目录权限是否被修改过	由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问。重要文件和目录权限均在合理范围内，用户可根据对文件不同的权限进行操作	符合情况：由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	f)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问安全策略实施所要依据的，是进行重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制。安全增强型Linux (Security Enhanced Linux)简称SELinux,是一个Linux内核模块，也是Linux的一个安全子系统。2.6及以上版本的Linux内被都团经集成了SELinux模块，在使用SELinux的操作系统中，决定一个资源是否能够被访问的因素除了用户的权限(读、写、执行)外，还需要判断每一类进程是否拥有对某一类资源的访问权限，这种权限管理机制的主体是进程，也称为强制访问控制(MAC)。在SELinux中，主体等同于进程，客体是主体访问的资源，可以是文件、目录、端口、设备等	1)明确系统中是否有敏感信息 2)在主体用户或进程划分级别并设置敏感标记，在客体文件设置敏感标记 3)应测试是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略 4)以有相应权限的身份登录进入Linux,使用more查看/etc/selinux/config文件中的SELINUX参数的设定	1) 2) 3)4) linux服务器默认关闭SELinux服务。或采取第三方主机加固系统或对操作系统内核进行二次开发加固，并实际查看系统可视化界面。 SELINUX有三种工作模式，分别是: enforcing:强制模式。违反SELinux规则的行为将阻止并记录到日志中，表示使用SELinux。 permissive:宽容模式。违反SELinux规则的行为只会记录到日志中，一般为调试用，表示使用SELinux disabled:关闭SELinux,使用SELinux	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	Redhat Enterprise Linux-3 update 2以后都开始使用LASU (Linux Aduit Subsystem)来进行审计。且志系统可以记录系统的各种信息,如:安全、调试、运行信息。审计子系统专用来记录安全信息，用于对系统安全事件的追溯。如果审计子系统没有运行，Linux 内核就将安全审计信息传递给日志系统。 Linux 操作系统的auditd进程主要用来记录安全信息。用于对系统安全事件的追溯；而rsyslog进程用来记录系统中的各种信息，如硬件报警和软件日志。Linux操作系统在安全审计配置文件/etc/audit/audit.rules中配置安全事件审计规则	1)以root身份登录进入Linux, 查看服务进程 2)若运行了安全审计服务，则查看安全审计的守护进程是否正常 # ps -ef|grep auditd 3)若未开启系统安全审计功能，则确认是否部署了第三方安全审计工具 4)以root身份登录进入Linux查看安全事件配置: #gerep " @priv-ops" /etc/audit/filter.conf .... more/etc/audit/audit.rules	1)开启审计进程内容如下: [root@localhost april]# service auditd status auditd (pid 1656) is running... [root@localhost april]# service rsyslog statusr syslogd (pid 1681) is running... [root@localhost april]# 2)Linux服务器默认开启守护进程 3)audit.rules中记录对文件和底层调用的相关记录，记录的安全事件较为全面	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	b)审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	详细的审计记录才能实现有效的审计，审计记录应该包括事件的日期、时间、类型、主体标识、客体标识和结果等。通过记录中的详细信息，能够帮助管理员或其他相关检查人员准确的分析和定位事件。Linux用户空间审计系统由auditd、ausearch和aureport等应用程序组成，其中ausearch是查找审计事件的工具，可以用来查看系统日志	以有相应权限的身份登录进入Linux,使用命令"ausearch-ts today "，其中，-ts指定时间后的log,或命令"tail -20 /var/log/audit/audit.log"查看审计日志	审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果	符合情况：审计记录包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	非法用户进入系统后的第一件事情就是去清理系统日志和审计日志，而发现入侵的最简单最直接的方法就是去看系统记录和安全审计文件。因此，必须对审计记录进行安全保护，避免受到未预期的删除修改或覆盖等。	访谈审计记录的存储、备份和保护的措施，是否将操作系统日志定时发送到日志服务器上等，并使用sylog方式或smp方式将日志发送到日志服务器。 如果部署了日志服务器,登录日志服务器查看操作系统的日志是否在收集的范围内	操作系统日志定期备份，共定期将本地存储日志转发至日志服务器	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	d)应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容。 在Linux中,Auditd是审计守护进程, syslogd是日志守护进程,保护好审计进程，当事件发生时，能够及时记录事件发生的详细内容。	1)访谈对审计进程监控和保护的措施 2)测试使用非安全审计员中断审计进程，查看审计进程的访问权限是否设置合理。 3)查看是否有第三方系统对被测操作系统的审计进程进行监控和保护	1）2）审计进程不可以非审计人员权限修改 3）部署有第三方审计工具，可实时记录审计日志，管理员不可对日志进行删除	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
	a)应遵循最小安装的原则仅安装需要的组件和应用程序	在安装Linux操作系统时，应试循最小化安装原则，即不需要的包不进行安装。安装的包越多，面临的风险起大，系统瘦身有利于提高系统的安全性。在操作系统使用过程中，为了避免由于多余组件和应用程序带来的安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序	1)访谈安装系统时是否遵循最小化安装原则，查看安装操作手册 2)使用命令"yum list installed" 查看操作系统中已安装的程序包，询问是否有目前不需要的组件和应用程序	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	Linux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，通常可以将其关闭。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)以有相应权限的身份登录进入Linux, 使用命令"service -status-all| grep running" 查看是否已经关闭危险的网络服务 2)以有相应权限的身份登录进入Linux,使用命令"netstat -ntlp"查看并确认是否开放的端口都为业务需要端口，是否已经关闭非必需的端口,Linux不存在共享问题	1)关闭了系统多余服务，危险服务和进程 2)关闭了多余端口	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

入侵防范	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	在Linux系统中存在/etc/hosts.allowr和/etc/hosts.deny两个文件,它们是tcpd服务器的配置文件，tcpd服务器可以控制外部IP对本机服务的访问。其中/etc/hosts.allow控制可以访问本机的IP地址，/ete/hosts.deny控制禁止访问本机的IP,如果两个文件的配置有冲突，以/etc/hosts. deny为准	查看在/etc/hosts.deny中是否有“ALL: ALL”,禁止所有的请求;在/etc/hosts.allow中，是否有如下配置(举例): sshd: 192.168.1.10/255. 255. 255. 0 2)是否采用了从防火墙设置了对接入终端的限制	1)使用more查看/etc/hosts.allow中是否有如下配置限制IP及其访问方式，如(举例): ssbd; 192. 168. 1.10/255.255 255.0 2)对终端接入方式，网络地址范围等条件进行限制。通过RADUS.、堡垒主机、安全城、防火墙等运维方式实现对终端入方式的限制	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：通过网路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	1)查看甲方自查的洞扫报告或通过第三方检查的漏洞报告，有无高风险漏洞 2)系统有无漏洞测试环境，补丁更新的机制和流程加何? 3)访谈补丁升级机制，查看补丁安装情况：#rpm -qa grep patch	1有运维团队定期进行漏洞扫描，发现安全风险，及时补修 2)3）更断补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	e)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护真正安全的环境，只具备安全系统还远远不够。如果假设自己不会受到攻击，或认为防护措施已足以保护自己的安全，都是非常危险的。要维护系统安全，必须进行主动监视，以检查是否发生了入侵和攻击。 一般意义上，入侵威胁分为外部渗透、内部渗透和不法行为三种，入侵行为分为物理入侵、系统入侵和远程入侵三种。此项中，关注的操作系统所面对的入侵成胁可能包含了三种造成入侵威胁的入侵行为主要是系统入侵和远程入侵两种。系统入侵，指入侵者在拥有系统的一个低级账号权限下进行的破坏活动。通常，如果系统没有及时更新最近的补丁程序，那么拥有低级权限的用户就可能利用系统漏洞获取更高的管理特权。远程入侵，指入侵者通过网络渗透到一个系统中。这种情况下，入侵者通常不具备任何特殊权限，他们通过漏洞扫扫描端口扫描等技术发现攻击目标，再利用相关技术执行破坏活动	1)访谈并查看入侵检测的措施，如经常通过如下命令查看入侵的重要线索(试图Telnet.FTP等),涉及命令“#more /var/log /secure|grep refused” 2)查看是否启用了主机防火墙、TCP SYN保护机制等设置 3)访谈系统管理员是否安装了主机入侵检测软件。查看已安装的主机入侵，检查系统的配置情况，是否具备报警功能。可执行命令: find / -namie <daemonname> -print 检查是否安装了主机入侵检测软件，如Dragon Squire by Enterasys Networks，ITA by Symantec. Hostsentry by Psionic Software.Logcheck by Psiomc Software. RealSecure-agent by ISS 4)查看网络拓扑图，查看网络上是否部署了网络入侵检测系统，如IDS	1）入侵的重要路径均deny 2)开启主机防火墙相关置 3)安装有基于主机的IDS设备 4)若主机未部署主机IDS设备。可在网络链路上查香是否是IDS、IPS. 发生入侵事件时，记录报警措施等	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为
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Linux系统，也面临着木马和蠕虫的破坏，可以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对恶意代码进行检测	1)核查操作系统中安装了什么防病毒软件，访谈管理员病毒库是否经常更新，核查病毒库最新版本，更新日期是否超过一个星期 2)核查操作系统是否实现了可信验证机制，能够对系统程序、应用程序和重要配置文件/参数进行可信执行验途	1)部署有网络版防病毒软件，病毒库最新，支持防恶意代码的统-管理个 2)部署有主动免疫可信验证机制，可对病责入侵进行及时阻断	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	针对服务器设备，需要服务器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)核查服务器的启动，是否实现可信验证的检测过程，查看对那些系统引导程序、系统程序或重要配置参数进行可信验证 2)修改其中的重要系统程序之一和应用程序之一，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	l）服务器具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 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 不符合情况：无可信根芯片或硬件
数据备份恢复	应提供重要数据处理系统的热冗余，保证系统的高可用性	对于可用性要求较高的等级保护对象来说，仅仅进行数据备份是远远不够的，还必须进行系统备份。重要数据处理系统要求采用热冗余,保证系统的高可用性	1)访谈系统管理员哪些是重要数据处理系统，重要数据处理系统是否有备份机制，是否采用本地热备份站点备份或异地活动互援备份。 2)核查设备列表，重要数据处理系统是否采用热备服务器	1)对重要数据，如用户数据，鉴别数据等定期进行备份，通过磁带备份到本地 2)对于重要设备，采取热备、集群、负载均衡等高可用方式	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余