|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | var目录必须挂载为一个独立的文件系统分区 | | |
| **检测编号** | V-38456 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/mtab文件内容需要包含"on /var "字符串的行 | | |
| **配置方法** | 挂载var目录再独立分区 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | home目录必须挂载为一个独立的文件系统分区 | | |
| **检测编号** | V-38473 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/mtab文件内容需要包含"on /home "字符串的行 | | |
| **配置方法** | 挂载home目录再独立分区 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 除了root以外的默认的帐号，必须进行锁定 | | |
| **检测编号** | V-38496 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 用户名不为root，且密码列不为！！或\*的用户必须被锁定 | | |
| **配置方法** | 锁定对应用户 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 禁止帐号的密码配置为空密码 | | |
| **检测编号** | V-38497 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 帐号的密码配置不可以为空 | | |
| **配置方法** | 用户设置密码 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/passwd文件必须不包含密码的哈希值 | | |
| **检测编号** | V-38499 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 密码管理文件必须不展示密码哈希值 | | |
| **配置方法** | 对于有哈希值的密码，需要进行删除 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 登录系统的密码长度配置必须限制至少为14位 | | |
| **检测编号** | V-38475 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统必须限制登录密码长度至少14位 | | |
| **配置方法** | 修改系统配置文件内容，变更为14 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 用户在24小时内不能过再次修改密码 | | |
| **检测编号** | V-38477 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统必须限制登录密码修改最短时长为24小时 | | |
| **配置方法** | 修改系统配置文件内容，变更为24 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 必须在密码无效的7天前对用户进行警告 | | |
| **检测编号** | V-38480 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统须配置密码过期提醒时间为7天 | | |
| **配置方法** | 修改系统配置文件内容，变更为7 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须使用FIPS 140-2标准的加密哈希算法生成的账号密码 | | |
| **检测编号** | V-38577 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 用户密码必须使用FIPS 140-2标准 | | |
| **配置方法** | 系统配置文件增加crypt\_style = sha512配置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 用户密码必须至少每60天进行修改 | | |
| **检测编号** | V-38479 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 用户密码有效期必须为60天 | | |
| **配置方法** | 修改系统配置文件内容，变更为60 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | root密码不能以明文形式通过网络传递 | | |
| **检测编号** | V-1046 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | /etc/syslog.conf 文件中是否存在 authpriv.\* | | |
| **配置方法** | 在系统上启用ssh，并将其用于所有用于获取根访问的远程连接 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统引导加载程序必须要求身份验证 | | |
| **检测编号** | V-4249 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | 对应系统配置文件中必须包含password --md5参数 | | |
| **配置方法** | 使用grub-md5-crypt工具生成md5密码，并将其应用到指定系统配置文件 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统不能有配置空密码的帐户 | | |
| **检测编号** | V-770 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | /etc/pam.d/system-auth文件中必须不包含nullok字符串 | | |
| **配置方法** | 删除/etc/pam.d/system-auth中nullok的设置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | root账号的UID必须且仅为0 | | |
| **检测编号** | V-38500 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | root账号配置必须UID为0 | | |
| **配置方法** | 配置root账号UID为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/shadow文件的所属组必须为root组 | | |
| **检测编号** | V-38503 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/shadow文件属组必须为root | | |
| **配置方法** | 配置/etc/shadow文件属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/gshadow文件的组必须属于root组 | | |
| **检测编号** | V-38448 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/gshadow文件属组必须为root | | |
| **配置方法** | 配置/etc/gshadow文件属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/passwd文件的组必须属于root组 | | |
| **检测编号** | V-38451 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/passwd文件属组必须为root | | |
| **配置方法** | 配置/etc/passwd文件属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/group文件的组必须属于root组 | | |
| **检测编号** | V-38451 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/group文件属组必须为root | | |
| **配置方法** | 配置/etc/group文件属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 匿名FTP帐户不能使用shell功能 | | |
| **检测编号** | V-4387 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | /etc/passwd文件中ftp的配置，必须是如下值之一：  /bin/false /dev/null /usr/bin/false /bin/true /sbin/nologin | | |
| **配置方法** | 配置FTP连接使用非函数shell，编辑/etc/passwd文件删除与ftp帐户关联的任何可运行的shell功能。 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/shadow文件必须所属于root用户 | | |
| **检测编号** | V-38502 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/shadow文件属主必须为root | | |
| **配置方法** | 配置/etc/shadow文件主属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/gshadow文件必须所属于root用户 | | |
| **检测编号** | V-38443 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/gshadow文件属主必须为root | | |
| **配置方法** | 配置/etc/gshadow文件主属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/passwd文件必须所属于root用户 | | |
| **检测编号** | V-38450 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/passwd文件属主必须为root | | |
| **配置方法** | 配置/etc/passwd文件主属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/group文件必须所属于root用户 | | |
| **检测编号** | V-38458 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/group文件属主必须为root | | |
| **配置方法** | 配置/etc/group文件主属组为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 所有系统命令文件的属主必须为root用户 | | |
| **检测编号** | V-38472 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 检查如下目录所有文件：  /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin  所有文件必须属主都为root | | |
| **配置方法** | 配置如下目录中文件的属主为root：  /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 所有系统文件、程序和目录都必须由系统帐户拥有 | | |
| **检测编号** | V-795 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | 如下目录中的文件必须属主为root：  /etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin | | |
| **配置方法** | 修改如下目录中的文件属主为root：  /etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 通过邮件别名文件执行的文件属主必须为root，必须驻留在仅由root拥有和可写的目录中 | | |
| **检测编号** | V-833 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | /etc/aliases文件属主是否为root | | |
| **配置方法** | 配置/etc/aliases文件属主为root | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/shadow文件的权限必须为不可读写、不可执行 | | |
| **检测编号** | V-38504 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/shadow文件的权限必须为不可读写、不可执行 | | |
| **配置方法** | 配置/etc/shadow文件的权限为不可读写、不可执行 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/gshadow文件的权限必须为不可读写、不可执行 | | |
| **检测编号** | V-38449 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/gshadow文件的权限必须为不可读写、不可执行 | | |
| **配置方法** | 配置/etc/gshadow文件的权限为不可读写、不可执行 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/passwd文件的权限必须为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **检测编号** | V-38457 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/passwd文件的权限必须为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **配置方法** | 配置/etc/passwd文件的权限为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | /etc/group文件的权限必须为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **检测编号** | V-38461 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/group文件的权限必须为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **配置方法** | 配置/etc/group文件的权限为root用户可读写、root组可读、其它用户可读的权限或更小的权限 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 所有的系统命令文件的权限必须为root用户可读写可执行、root组可读与执行、其它用户可读可执行的权限或更小的权限 | | |
| **检测编号** | V-38469 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 如下目录中的文件必须权限为755：  /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin | | |
| **配置方法** | 配置如下目录中所有文件权限为755：  /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须默认接口不支持ICMPv4消息重定向 | | |
| **检测编号** | V-38600 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/default/send\_redirects 文件内数值必须等于 0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/default/send\_redirects 文件内数值为 0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须所有接口都不支持ICMPv4消息重定向 | | |
| **检测编号** | V-38601 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/send\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/send\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | IPv4的IP转发功能必须不开启，除非此系统本身是作为路由器进行使用 | | |
| **检测编号** | V-38511 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/ip\_forward文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/ip\_forward文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统不能接受任何接口上的IPv4源路由包 | | |
| **检测编号** | V-38523 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/accept\_source\_route文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/accept\_source\_route文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须不接受任意接口的ICMPv4重定向包 | | |
| **检测编号** | V-38524 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/accept\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/accept\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须不接受任意接口的ICMPv4安全重定向包 | | |
| **检测编号** | V-38526 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/secure\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/secure\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须记录具有不可能地址的包 | | |
| **检测编号** | V-38528 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/log\_martians文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/log\_martians文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须不接受默认的IPv4的源路由包 | | |
| **检测编号** | V-38529 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/default/accept\_source\_route文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/default/accept\_source\_route文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须不接受ICMPv4默认的安全重定向包 | | |
| **检测编号** | V-38532 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/default/secure\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/default/secure\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须忽略默认的ICMPv4的重定向消息 | | |
| **检测编号** | V-38533 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/default/accept\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/default/accept\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须不响应ICMPv4发送的一个广播地址 | | |
| **检测编号** | V-38535 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须忽略ICMPv4伪造的错误的回应 | | |
| **检测编号** | V-38537 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/icmp\_ignore\_bogus\_error\_responses文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/icmp\_ignore\_bogus\_error\_responses文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须配置synccookies防止TCP SYN洪水攻击 | | |
| **检测编号** | V-38539 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/tcp\_syncookies文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/tcp\_syncookies文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须使用一个反向路径过滤器对IPv4网络流量进行过滤 | | |
| **检测编号** | V-38542 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/all/rp\_filter文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/all/rp\_filter文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统默认情况下必须使用一个反向路径过滤器对IPv4网络传输流量进行过滤 | | |
| **检测编号** | V-38544 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv4/conf/default/rp\_filter文件内数值必须等于1 | | |
| **配置方法** | 配置/proc/sys/net/ipv4/conf/default/rp\_filter文件内数值为1 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须忽略默认的ICMPv6重定向包 | | |
| **检测编号** | V-38548 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/net/ipv6/conf/default/accept\_redirects文件内数值必须等于0 | | |
| **配置方法** | 配置/proc/sys/net/ipv6/conf/default/accept\_redirects文件内数值为0 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | TFTP程序必须运行在"安全模式"，只有在主机文件系统的一个目录提供访问 | | |
| **检测编号** | V-847 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | 系统文件中server\_args属性的值为-s /var/lib/tftpboot | | |
| **配置方法** | 配置系统文件中属性值为-s /var/lib/tftpboot | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | .rhosts文件或hosts.equiv文件在系统必须不存在 | | |
| **检测编号** | V-38491 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/hosts.equiv文件必须不存在，~/.rhosts文件也必须不存在 | | |
| **配置方法** | 删除/etc/hosts.equiv 和 ~/.rhosts 文件 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 必须禁止root帐号从虚拟控制台登录到系统 | | |
| **检测编号** | V-38492 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/securetty文件中必须不包含vc+数字 | | |
| **配置方法** | 删除/etc/securetty文件中vc+数字配置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 必须禁止root帐号从串口控制台登录到系统 | | |
| **检测编号** | V-38494 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/securetty文件中必须不包含ttyS+数字 | | |
| **配置方法** | 删除/etc/securetty文件中ttyS+数字配置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 审计系统必须配置审核所有试图通过/etc/localtime对系统时间进行改变的行为 | | |
| **检测编号** | V-38530 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 审计系统必须审核试图通过/etc/localtime文件修改时间的行为 | | |
| **配置方法** | 增加审计系统配置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须要求系统管理员在多次登录尝试失败时对账号进行锁定 | | |
| **检测编号** | V-38592 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统配置文件中unlock\_time属性必须为604800 | | |
| **配置方法** | 配置系统文件中unlock\_time属性值为604800 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 不可执行(noexec)的选项必须添加到/tmp分区的挂载参数中 | | |
| **检测编号** | V-57569 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | tmp目录分区设置必须存在noexec参数 | | |
| **配置方法** | 配置系统文件tmp分区的参数设置noexec | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 使用sudo命令必须进行验证 | | |
| **检测编号** | V-58901 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统文件中必须不能配置NOPASSWD 或 !authenticate 配置项 | | |
| **配置方法** | 删除系统文件中的NOPASSWD 或 !authenticate 配置项 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须使用SMB客户端签名，用于连接使用smbclient的samba服务器 | | |
| **检测编号** | V-38656 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统配置文件中必须配置client signing = mandatory | | |
| **配置方法** | 增加client signing = mandatory配置到系统文件 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须使用SMB客户端签名使用mount.cifs配置去连接samba服务器 | | |
| **检测编号** | V-38657 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统配置文件必须包含sec=krb5i或sec=ntlmv2i配置项 | | |
| **配置方法** | 增加sec=krb5i或sec=ntlmv2i配置项到对应系统配置文件 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 帐户必须在35天不使用后被锁定 | | |
| **检测编号** | V-38692 | **检测优先级** | 低 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 账号在35天不登录后必须被锁定 | | |
| **配置方法** | 系统配置文件中INACTIVE属性配置为35 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统日志必须进行日常的滚动记录 | | |
| **检测编号** | V-38624 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /etc/cron.daily/logrotate文件必须存在 | | |
| **配置方法** | 安装logrotate服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 邮件中继必须加以限制 | | |
| **检测编号** | V-38622 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | 系统配置文件中inet\_interfaces属性必须等于localhost | | |
| **配置方法** | 配置系统文件中inet\_interfaces属性为localhost | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 系统必须使虚拟地址空间随机化功能生效 | | |
| **检测编号** | V-38596 | **检测优先级** | 中 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | /proc/sys/kernel/randomize\_va\_space 文件数值必须为2 | | |
| **配置方法** | 配置/proc/sys/kernel/randomize\_va\_space文件内容为2 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | x86系统必须将“Ctrl-Alt-Delete”组合键响应取消 | | |
| **检测编号** | V-38668 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | 系统必须配置组合键关机记录日志 | | |
| **配置方法** | /etc/init/control-alt-delete.override文件中配置关机日志记录功能 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | TFTP程序必须在安全模式下，只有在主机文件系统的一个目录提供访问操作 | | |
| **检测编号** | V-38701 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | 系统文件中必须配置server\_args = -s /var/lib/tftpboot参数 | | |
| **配置方法** | 增加配置server\_args = -s /var/lib/tftpboot到指定系统文件中 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | NFS服务器不能启用不安全的文件锁定选项 | | |
| **检测编号** | V-38677 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | /etc/exports文件内容必须为空 | | |
| **配置方法** | 删除/etc/exports文件内容 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | SSH守护进程必须配置为只使用sshv2协议 | | |
| **检测编号** | V-38607 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | 系统文件配置Protocol属性必须为2 | | |
| **配置方法** | 配置Protocol属性为2 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rlogind服务必须没有运行 | | |
| **检测编号** | V-38602 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | rlogin服务必须没有运行 | | |
| **配置方法** | 停止rlogin服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | SSH守护进程不能使用空密码允许身份验证 | | |
| **检测编号** | V-38614 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | 系统文件中PermitEmptyPasswords属性必须为no | | |
| **配置方法** | 修改系统文件中PermitEmptyPasswords属性为no | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rshd 服务必须没有运行 | | |
| **检测编号** | V-38594 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | rshd服务必须没有运行 | | |
| **配置方法** | 停止rshd服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rsh-server 必须不安装 | | |
| **检测编号** | V-71967 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 🗹redhat6系列 🗹Debian系统 | | |
| **基线要求** | rsh-server服务必须没有安装 | | |
| **配置方法** | 卸载rsh-server服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rexecd 服务必须没有运行 | | |
| **检测编号** | V-38598 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | rexecd服务必须没有运行 | | |
| **配置方法** | 停止rexecd服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | telnet-server 必须不安装 | | |
| **检测编号** | V-38587 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | telnet-server服务必须没有安装 | | |
| **配置方法** | 卸载telnet-server服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | telnet 服务必须没有运行 | | |
| **检测编号** | V-38589 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | □redhat5系列 🗹redhat6系列 □Debian系统 | | |
| **基线要求** | telnet服务必须没有运行 | | |
| **配置方法** | 停止telnet服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | x86系统 ctrl-alt-delete关键序列必须被禁用 | | |
| **检测编号** | V-4342 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | 关机键序列必须被禁用 | | |
| **配置方法** | /etc/inittab文件中去除关机键序列配置 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | SSH守护进程必须配置为只使用sshv2协议 | | |
| **检测编号** | V-4295 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | 系统配置文件中Protocol属性必须为2 | | |
| **配置方法** | 配置系统文件中Protocol属性值为2 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | telnet守护进程必须没有运行 | | |
| **检测编号** | V-24386 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | telnet服务必须没有运行 | | |
| **配置方法** | 停止telnet服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | 任何有效的TFTP守护进程必须授权系统中的认证方案批准 | | |
| **检测编号** | V-4695 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | tftp服务必须没有运行 | | |
| **配置方法** | 停止tftp服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rexec守护进程必须没有运行 | | |
| **检测编号** | V-4688 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | rexec服务必须没有运行 | | |
| **配置方法** | 停止rexec服务 | | |
| **备注** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **检测名称** | rsh守护进程必须没有运行 | | |
| **检测编号** | V-4687 | **检测优先级** | 高 |
| **适用范围** | 🗹普通终端 □服务器终端 □涉密终端 | | |
| **支持系统** | 🗹redhat5系列 □redhat6系列 □Debian系统 | | |
| **基线要求** | rsh服务必须没有运行 | | |
| **配置方法** | 停止rsh服务 | | |
| **备注** |  | | |