Linux主机基线检查表

|  |  |
| --- | --- |
| **检查对象信息** |  |
| **测 试 类** | **主机安全** |
| **测 试 项** | **身份鉴别** |
| 测试内容：   1. 空口令账户查看：   #awk -F: '($2 == ""){print $1}' /etc/passwd /etc/shadow   1. 密码策略：   #cat /etc/login.defs |grep PASS\_MIN\_LEN  #cat /etc/login.defs |grep PASS\_MAX\_DAYS  #cat /etc/login.defs |grep PASS\_MIN\_DAYS  #cat /etc/login.defs |grep PASS\_WARN\_AGE  #cat /etc/login.defs |grep FAIL\_DELAY  #cat /etc/login.defs |grep FAILLOG\_ENAB   1. 登录失败断开连接的设置：   #cat /etc/pam.d/system-auth |grep 'account required /lib/security/pam\_tally.so deny=5 no\_magic\_root reset'   1. 用户登陆超时自动注销设置：   #cat /etc/profile |grep TMOUT   1. 是否安装运行SSH：   #rpm –aq |grep ssh  # service --status-all |grep sshd  #netstat -an |grep 22   1. #service --status-all |grep running | |
| **测试记录：**   1. 操作系统是否存在空口令账户？   □ 否 □ 是，密码栏为空的用户名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 密码策略：   登录密码最小长度限制： □ 8个字符 □ \_\_\_个字符  登录密码有效期： □ 90天 □ \_\_\_天  登录密码最短修改时间： □ 0天 □ \_\_\_天  登录密码过期提前多少天提示修改： □ 7天 □ \_\_\_天  登录错误时等待时间： □ 10秒 □ \_\_\_秒  登录错误记录是否记录到日志： □ 是 □ 否   1. 当前系统管理员帐户口令：   ○ 长度：\_\_\_\_\_\_位  ○ 组成： □数字 □字母 □特殊字符  ○ 更换周期：\_\_\_\_\_\_\_\_\_   1. 是否启用登录失败处理，当出现多次以错误口令尝试登录情况时锁定该帐户？   □ 否 □ 是，登录失败断开连接的次数：  □ 3～5次 □ \_\_\_次  锁定时长：\_\_\_\_\_\_\_\_\_\_\_\_   1. 系统/etc/profile中是否设置TIMEOUT环境变量，设置登录终端操作超时锁定？   □ 否 □ 是 ，TIMEOUT=\_\_\_\_\_\_\_\_\_\_\_   1. 操作系统名称版本号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. 服务器是否接受远程管理？   □ 否 □ 是，远程登录方式为：  ○ 使用SSH远程登录方式  ○ 使用Telnet  ○ 其他\_\_\_\_\_\_\_\_\_\_\_   1. 是否存在除root之外UID为0的用户？   □ 唯一的一个用户。操作系统的身份标示具有唯一性。  □ 二个或者二个以上的用户。操作系统身份标示不具有唯一性。   1. /etc/passwd中是否有相同用户名的账户？   □ 否 □ 是，重复用户名：\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别？   □ 否，只使用用户名/口令 □ 有，包括：  ○ 令牌  ○ 挑战应答  ○ 动态口令  ○ 物理设备  ○ 生物识别技术  ○ 数字证书 | |
| 备注： | |
| **测 试 项** | **访问控制** |
| **测试内容：**   1. 重要文件和目录权限设置是否合理：   #ls –l /etc/passwd   1. 系统是否禁用多余账户：   #cat /etc/shadow |grep ^#   1. 查看多余、过期的账户： 2. #cat /etc/passwd | |
| **测试记录：**   1. 权限设置：   passwd -rw-r-r- root □ 是 □ 否  group -rw-r-r- root □ 是 □ 否  shadow -r------ root □ 是 □ 否   1. 根据业务需求，是否加强对重要文件的访问权限限制？   □ 否 □ 是   1. 是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限？   □ 否 □ 是   1. 系统是否存在多人共用一个账户的情况？   □ 否 □ 是   1. 操作系统管理员和数据库管理员是否为同一自然人？   □ 否 □ 是   1. 系统是否存在多余的、过期的或共享账户名？   □ 否 □ 是，帐户名为\_\_\_\_\_\_\_\_\_\_\_   1. 是否存在无用的默认帐户？  * 否 □ 是，包括：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   (如：mail、news、ftp、uucp、games、gopher等)   1. 操作系统是否具备能对信息资源设置敏感标记功能？   □ 否 □ 是   1. 如何划分敏感标记分类？   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 备注： | |
| **测 试 项** | **安全审计** |
| **测试内容：**   1. 系统日志服务和安全审计服务：   #service syslog status  #service audit status  #service --status-all |grep running  #ps –ef |grep auditd   1. 对ssh、su登录日志进行记录   #cat /etc/syslog.conf |grep ‘authpriv.\* /var/log/secure’   1. 审查规则查看：   Grep “@priv-ops” /etc/audit/filter.conf  Grep “@mount-ops” /etc/audit/filter.conf  Grep “@system-ops”/etc/audit/filter.conf  Grep “@file-ops” /etc/audit/filter.conf  Grep “@open-ops” /etc/audit/filter.conf  Grep “@execute-ops” /etc/audit/filter.conf   1. 审计日志查看工具：   aucat | tail -50 | |
| **测试记录：**   1. 系统是否采用有第三方审计工具或系统？   □ 否 □ 是，名称：\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 系统是否运行日志服务和安全审计服务？   □ 否 □ 是   1. 系统是否对ssh、su登录日志进行记录？   □ 否 □ 是   1. 审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件？   □ 否 □ 是   1. 日志记录包括：   □ 日期、时间  □ 事件类型  □ 主体标识  □ 客体标识  □ 结果  □ 其他，\_\_\_\_\_\_\_\_\_   1. 是否能够根据审计记录数据进行分析，并生成审计报表？   □ 否 □ 是   1. 审计进程的访问权限设置是否合理？   □ 否 □ 是   1. 是否有第三方对审计进程监控和保护的措施？   □ 否 □ 是，名称：\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否配置有日志服务器？   □ 否 □ 是   1. 是否严格限制用户访问审计记录的权限？   □ 否 □ 是   1. 是否采取措施保护审计日志？   □ 否 □ 是 ，备份策略：\_\_\_\_\_\_\_\_\_\_\_  备份周期：\_\_\_\_\_\_\_\_\_\_\_ | |
| 备注： | |
| **测 试 项** | **剩余信息保护** |
| **测试内容：**   1. 访谈管理员存放在硬盘上还是在内存中的信息，在被释放或者再分配给其他用户前是否得到完全清除； 2. 访谈管理员系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除。 3. echo $HISTSIZE或grep HISTSIZE /etc/profile | |
| **测试记录：**   1. 存放在硬盘上还是在内存中的信息，在被释放或者再分配给其他用户前是否得到完全清除？   □ 否 □ 是   1. 系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前是否得到完全清除？   □ 否 □ 是  记录历史命令historysize值：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 备注： | |
| **测 试 项** | **入侵防范** |
| **测试内容：**   1. 服务查看：   #service --status-all |grep running  补丁安装情况：   1. Rpm –qa |grep patch | |
| **测试记录：**   1. 是否安装有主机入侵检测软件？   □ 否 □ 是，名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ○ 是否具备报警功能？  □ 否 □ 是   1. 是否有第三方入侵检测系统，如IDS？   □ 否 □ 是，名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否启用主机防火墙、TCP SYN保护机制？   □ 否 □ 是   1. 是否使用一些文件完整性检查工具或脚本定时对重要文件的完整性进行检查，如对比校验值等？   □ 否 □ 是，工具名称：\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否对重要的配置文件进行备份？   □ 否 □ 是，文件名称：\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 系统是否已经关闭危险及非必需的网络服务？   □ 否 □ 是，服务有：○ echo、shell、login、finger、r命令等  ○ talk、ntalk、pop-2、sendmail、imapd、pop3d等  ○ 其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 操作系统及补丁版本：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. 系统补丁升级方式:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 3. 系统补丁安装情况：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 4. 操作系统是否仅安装所必须的系统组件和应用程序？   □ 是 □ 否，\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否定期更新系统补丁？   □ 否 □ 是，更新周期：\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 备注： | |
| **测 试 项** | **恶意代码防范** |
| **测试内容：**   1. 应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署覆盖范围如何； 2. 应检查主要服务器，查看是否安装了实时检测与查杀恶意代码的软件产品并进行及时更新； 3. 应检查防恶意代码产品是否实现了统一管理； 4. 应检查网络防恶意代码产品，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与主机防恶意代码产品有不同的恶意代码库。 | |
| **测试记录：**   1. 主机系统是否安装了防病毒软件？   □ 否 □ 是  防病毒软件名称及版本号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  最新病毒库更新时间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 病毒库的最新版本更新日期距离检查日期是否超过一个星期？   □ 否 □ 是   1. 是否安装有网络防病毒产品？   □ 否 □ 是，型号：\_\_\_\_\_\_\_\_\_\_\_\_  病毒库最新更新日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 防病毒软件是否采用统一的病毒更新策略和查杀策略？   □ 否 □ 是，查杀频率：\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 备注： | |