Windows 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. “开始”|“程序”|“管理工具”|“本地安全策略”|“安全设置”|“帐户策略”;
2. “控制面板”|“管理工具”|“终端服务配置”|连接 RDP-Tcp“属性”|“常规”;
3. “计算机管理”|“本地用户和组”|“用户”。

测试记录：

1. 是否为系统用户设置密码，系统账户登录过程中是否使用了密码进行登录验证？

   □是 □ 否，密码为空的用户名：_____

2. 密码策略：

   密码必须符合复杂性要求： □ 已禁用 □ 已启用

   密码长度最小值： □ 0 个字符 □ ___个字符

   密码最短使用期限： □ 0 天 □ ___天

   密码最长使用期限： □ 42 天 □ ___天

   强制密码历史： □ 0 个记住的密码 □ ___个记住的密码

   用可还原的加密来储存密码：□ 已禁用 □ 已启用

3. 帐户锁定策略：

   帐户锁定时间： □ ____分钟 □ 不适应

   帐户锁定阀值： □ ____次无效登录

   重置帐户锁定计数器： □ ____分钟 □ 不适应

4. 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：_____

5. 操作系统名称及补丁版本：_____

6. 服务器是否接受远程管理？

   □ 否 □ 是，○ 终端服务器是否使用了 SSL 加密？

   □ 否 □ 是

   ○ 加密级别：_____

5、操作系统和数据库系统的不同用户是否分配不同用户名？

□ 否 □ 是，分别是_____

7. Windows 系统用户名是否有重复？

   □ 否 □ 是，重复用户名：_____

8. 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. 计算机管理丨共享文件夹丨共享，查看“共享”下的各个资源设置情况：
2. 防止ipc$空链接枚举:
   HLM\SYSTEM\CurrentControlSet\Control\LSA\restrictanonymous值是否等于1；
3. “管理工具”|“本地安全策略”|“安全设置”|“本地策略”|“用户权限分配”;

测试记录：

1. 访问控制策略：
   %systemdrive\windows\system 目录权限：
   everyone 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   users 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   administrators 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   %systemroot\system32\config 目录权限：
   everyone 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   users 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   administrators 组权限：　☐ 完全控制 ☐ 读取和执行 ☐修改 ☐ 无
   是否开启默认共享：☐ 否　　☐ 是，共享目录：_____
   是否禁止 ipc$空连接进行枚举：☐ 否　　☐ 是, restrictanonymous=1
2. 根据业务需求，是否加强对重要文件的访问权限限制？
   ☐　否　☐ 是
3. 系统用户主要有哪些角色？
   ○ administrators ，用户名包括：_____
   ○ backup operators，用户名包括：_____
   ○ power users，用户名包括：_____
   ○ users，用户名包括：_____
   ○ guests，用户名包括：_____
   ○ 其他：_____
4. 用户权限和特权分配情况：
   ○ 从网络访问此计算机：☐ administrators ☐ backup operators
   ☐ power users　☐ users　☐ everyone
   ☐ 其他_____
   ○ 本地登录：☐ administrators ☐ backup operators
   ☐ power users　☐ users　☐ 其他_____
   ○ 关闭系统:☐ administrators ☐ power users ☐ 其他_____

5. 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

6. 系统是否存在多人共用一个账户的情况？

□ 否 □ 是

7. 操作系统管理员和数据库管理员是否为同一自然人？

□ 否 □ 是

8. 系统是否禁用匿名\默认帐户？

□ 是 □ 否，帐户名为_____

9. 系统是否存在多余的、过期的帐户？

□ 是 □ 否，帐户名为_____

10. 操作系统是否具备能对信息资源设置敏感标记功能？

□ 否 □ 是

如何划分敏感标记分类？_____

备注：

测 试 项	**安全审计**

测试内容：

1. “计算机管理”|“本地安全策略”|“本地策略”|“安全选项”|“审核”；
2. “计算机管理”|“本地安全策略”|“本地策略”|“审核策略”；
3. “事件查看器”|“安全日志”属性。

测试记录：

1. 系统是否开启安全审计功能？

□ 否 □ 是

2. 审核策略：

审核策略更改：	□ 无审核	□ 成功	□ 失败
审核登录事件：	□ 无审核	□ 成功	□ 失败
审核对象访问：	□ 无审核	□ 成功	□ 失败
审核过程跟踪：	□ 无审核	□ 成功	□ 失败
审核目录服务访问：	□ 无审核	□ 成功	□ 失败
审核特权使用：	□ 无审核	□ 成功	□ 失败
审核系统事件：	□ 无审核	□ 成功	□ 失败
审核帐户登录事件：	□ 无审核	□ 成功	□ 失败
审核帐户管理：	□ 无审核	□ 成功	□ 失败

3. 是否采用第三方审计工具或系统？

□ 否 □ 是，名称：_____

4. 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，_____

5. 日志大小上限（KB）：_____

6. 达到事件日志大小上限时：

☐ 按需要覆盖事件

☐ 日志满时将其存档，不覆盖事件

☐ 覆盖时间超过_____天的事件

☐ 不覆盖事件（手动清除日志）

7. 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

8. 是否有第三方对审计进程监控和保护的措施？

☐ 否　　☐ 是，名称：_____

9. 是否配置有日志服务器？

☐ 否　　☐ 是

备注：

测 试 项	**剩余信息保护**

测试内容：

1. “本地安全策略”|“本地策略”|“安全选项”|是否启用“交互式登录：不显示上次的用户名”；
2. “本地安全策略”|“本地策略”|“安全选项”|是否启用“关机：清除虚拟内存页面文件”；
3. “本地安全策略”|“密码策略”|是否禁用“用可还原的加密来存储密码”。

测试记录：

1. 在登录系统时是否显示上次的用户登录名？

☐ 否　　☐ 是

2. 系统是否启用关机前清除虚拟内存页面？

☐ 否　　☐ 是

3. 系统是否禁用用可还原的加密来存储密码？

☐ 否　　☐ 是

备注：

测 试 项	**入侵防范**

测试内容：

1. 运行：services.msc，查看系统服务；

   Netstat －an，查看监听端口；

2. 补丁编号：“控制面板”|“添加删除程序”|记录系统安全补丁编号 KBxxxxxx。

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

2. 是否有第三方入侵检测系统，如 IDS？

☐ 否　　☐ 是，名称：_____

3. 是否启用主机防火墙？

□ 否　　□ 是

4. 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：_____

5. 是否对重要的配置文件进行备份？

□ 否　　□ 是，文件名称：_____

6. 系统是否已经开启服务中一些不必要的服务？

□ 否　　□ 是，服务有：○ Alerter
○ Remote Registry Service
○ Messenger
○ Task Scheduler
○ 其他_____

7. 操作系统及补丁版本：_____

8. 系统补丁升级方式：

□ WSUS 补丁服务器　　□ 其他_____

9. 系统已安装的最新安全补丁名称：

_____

10. 操作系统是否仅安装所必须的系统组件和应用程序？

□ 是　　□ 否，_____

11. 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：_____

2. 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

3. 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：_____

4. 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：	