运维安全审计系统测试报告

[文档信息]

文档名称	运维安全审计系统测试方案		
文档管理编号			
保密级别		文档版本号	
制作人		制作日期	
复审人		复审日期	
扩散范围			
扩散批准人			

[版本变更记录]

时间	版本	说明	修改人

[文档送呈]

单位	目的

目 录

1 概述 ..... 错误!未定义书签。

1.1 文档目的 ..... 错误!未定义书签。

1.2 测试对象 ..... 错误!未定义书签。

2 测试内容..... 错误!未定义书签。

2.1 系统基本配置与测试 ..... 错误!未定义书签。

2.1.1 审计平台安装与监控功能 ..... 错误!未定义书签。

2.1.2 系统管理配置 ..... 错误!未定义书签。

2.2 运维管理配置与测试..... 错误!未定义书签。

2.2.1 运维用户管理..... 错误!未定义书签。

2.2.2 资源管理..... 错误!未定义书签。

2.2.3 授权与访问控制 ..... 错误!未定义书签。

2.2.4 应用发布管理..... 错误!未定义书签。

2.3 设备口令管理配置与测试 ..... 错误!未定义书签。

2.3.1 统一帐户管理 ..... 错误!未定义书签。

2.3.2 设备帐户管理 ..... 错误!未定义书签。

2.4 运维操作审计测试 ..... 错误!未定义书签。

2.4.1 Telnet 协议运维操作测试 ..... 错误!未定义书签。

2.4.2 SSH 协议运维操作测试 ..... 错误!未定义书签。

2.4.3 FTP 协议运维操作测试 ..... 错误!未定义书签。

2.4.4 SFTP 协议运维操作测试 ..... 错误!未定义书签。

2.4.5 RDP 协议运维操作测试 ..... 错误!未定义书签。

2.4.6 VDH 测试 ..... 错误!未定义书签。

2.4.7 Xwindows 协议运维操作测试..... 错误!未定义书签。

2.4.8 VNC 协议运维操作测试 ..... 错误!未定义书签。

2.5 事中违规告警与阻断测试 ..... 错误!未定义书签。

2.6 审计功能测试..... 错误!未定义书签。

2.7 统计报表功能测试 ..... 错误!未定义书签。

2.8 审计日志管理测试 ..... 错误!未定义书签。

1 概述

1.1 文档目的

本文档制定了运维安全审计系统的测试项目和内容，用于运维安全审计系统的测试。

1.2 测试对象

测试对象：运维安全审计系统

2 测试内容

2.1 系统基本配置与测试

2.1.1 审计平台安装与监控功能

2.1.1.1 审计平台安装

测试项目	操作方法	预期结果	实际结果
审计平台安装	将软件安装到 Windows(xp, 2000, vista)各个版本	安装顺利	

2.1.1.2 连接

测试项目	操作方法	预期结果	实际结果
审计平台连接	启动审计平台，设置连接的 IP 地址及端口，输入审计员口令 和密码	能正常连接	

2.1.1.3 系统监控

测试项目	操作方法	预期结果	实际结果
查看信息	登录审计平台，打开设备信息 窗口	能正确显示设备信息	
查看活动用户	打开活动用户窗口	能正确显示活动用户，并能对任意列进行排序	
查看活动会话	打开活动会话窗口，选择其中 一条会话进行实时监控	能显示目前存在运维会话	
查看资源状态	打开资源状态窗口	能正确显示每个资源的连接并发 数量，并能对任意列进行排序	

2.1.2 系统管理配置

测试项目	操作方法	预期结果	实际结果

系统信息	通过浏览器进入，可以看到系统运 行时间、版本、网口、内存区使用 率、日志区使用率等信息；	静态信息显示正确	日志区界面错乱
管理员管理	1、 角色管理：根据管理需求，建立 新角色 2、 添加管理员，并分配其拥有的角 色 3、 访问白名单 4、 管理员证书认证：新增管理员的 认证方式为证书认证并配置证 书，下载证书并采用证书登录管 理页面	1、 建立成功 2、 添加成功，登录后 其角色正确 3、 访同控制有效，其 他地址无法访问 4、 证书能下载。证书 正确时，成功登录， 证书错误时不能登 录。非证书用户采 用证书不能登录	创建用户时，如果 用户名过长没有提 示 为什么不是允许访 同地址，白名单有 何意义。 选择，令牌认证是 什么意思？ 证书无法使用，下 载使用，再次登录 提示证书错误 登录界面没有提示 使用那种方式登录
网络配置	配置外网口、内网口、热备网口地 址，配置网关、首选 DNS、备选 DNS、 虚拟网卡、静态路由表	配置正确	Ping 命令无效 添加静态路由后设备无法访问
外部认证	配置 LDAP、AD 域、Radius 认证服务器	配置正确	未测试
全局配置	1、 NTP 配置 2、 口令复杂度 3、 母页最大记录数 4、 邮件服务器	可以进行时间同步，确 保审计的准确性。 可设置密码的复杂度 可设置数据信息每页 最大行数 可设置发送邮件服务 器	网络不正确，正确 的 ntp 地址报错。 口令复杂度，不完善，没有数子、大 小写等要求 网络配置失效，导 致邮件服务器无法 使用

1、系统维护	2、 执行重启、配置备份与恢复 3、 执行升级管理 4、 执行重新激活	1、 执行正确 2、 能升级 3、 激活成功	
事件通知	添加邮件事件通知（前提是先配好 邮件服务器）	可收到通知邮件	无法使用，网络不 通

2.2 运维管理配置与测试

221 运维用户管理

测试项目	操作方法	预期结果	实际结果
创建运维用户	创建运维用户，设置口令及认证方式 等	在用户列表中能看到此用户	创建用户时，如果 用户名过长没有提 示 令牌认证？ 证书认证无效 自动密码发送邮箱 无效
口令复杂度设置	在全局配置设置口令复杂度 （高、中、低），在创建运维用户或修改口令验 证	只有复杂度符合的操作才能完成	当密码强度不足时没有提示
口令认证失败死锁	在运维配置中设置死锁次数	口令错超过此次数，运维用户无法登录，只有运维管理员能重新激 活该用户	
密码有效期	设置该运维用户的密码有效期	当密码有效期超过后，运维用户无法登录	最短 15 天，无法测试
用户激活	设置某运维用户是否激活	激活用户方能使用	
创建用户组	选择已建用户分配到此组或建用户 组，新建用户时选择该用户组	在用户组列表中看到 此用户组及包含的用 户	
授权管理	针对选定用户的资源/组的授权	在授权列表可看到此 授权	访问规则模糊不清

运维配置	1、磁盘映射 2、RDP 剪贴板 3、RDP 登录 Console 4、自助登录 5、运维工单状态	1、RDP 运维时，能映射本地磁盘 2、RDP 运维时，能提供剪贴板服务 3、RDP 运维时，能登录至资源的管理控制台 4、SSO 运维时，运维用户能手动输入帐户登录资源 5、运维时需输入工单（要求安装运维工单系统）	没有自动登录方 式，全是手动登录 运维工单管理，没有

222 资源管理

测试项目	操作方法	预期结果	实际结果
创建保护主机及服 务	创建一个 Linux、Unix 保护主机、设 置 IP 地址，并创建 SSH、sftp、Xwindows、VNC 服务	在资源列表中能看到 此资源。	没有 Linux、unix、xwindows、vnc 选项选项
	创建 Windows 保护主机，设置主机 IP 地址，创建 tel net、RDP、ftp 服务	在资源列表中能看到此资源	没有 tln et 选项
创建资源组	可以根据管理需要将一组资源分配到一个资源组	在资源组列表中能看到此资源组	
编辑资源组	可针对协议编辑资源组	能编辑资源组中某一 个协议所包含的所有 资源	不可以
授权管理	针对选定资源的用户/组的授权	在授权列表可看到此 授权	

223 授权与访问控制

2.2.3.1 授权规则管理

测试项目	操作方法	预期结果	实际结果

创建授权规则	在授权规则管理中添加相应规则	在授权规则列表可看到此规则	有授权规则，但是作用不大，仅仅是时间的限制 在规则中存在冲突，时间和周的冲突 规则仅仅是通话 时间生效
授权规则验证	在满足/不满足授权规则的条件下， 访问资源	在满足的条件下可访问资源，否则，不能访问	简单的通过

223.2 授权管理

测试项目	操作方法	预期结果	实际结果
创建授权	创建“用户/组——资源/组”的四种 组合方式的授权	在授权列表可看到此 授权	
查看授权	点击 用户/组”和 资源/组”按钮，查看四种方式的授权	在授权表中能查看到四种方式的授权	通过
资源过滤	在创建 用户/组——资源”时，可对 资源进行过滤	能够准确过滤资源	通过

223.3 访问控制

测试项目	操作方法	预期结果	实际结果
访问日期区间控制	通过设置授权规则中设置访问日期 区间，并在授权时选中此规则	只能在规定的日期区 间中进行访问。	通过，但是有冲突
会话时长控制	通过设置授权规则中设置会话时长 （如 2 分钟），并在授权时选中此规 则	所有经过此规则授权 的用户或者协议均两 分钟后退出。	通过
访问 IP 控制	通过设置授权规则中设置允许访问 的 IP 地址，并在授权时选中此规则	只有允许的地址能够 访问	通过

224 应用发布管理

测试项目	操作方法	预期结果	实际结果
创建 VDH 服务器	在应用发布中添加 VDH 服务器	在 VDH 设备管理可看 到此设备	没有设备
监控 VDH 服务器	在 VDH 设备管理中通过监控 VDH 服务器	能 RDP 访问 VDH 服务器	没有设备
添加应用发布	在应用配置中添加应用协议	VDH 应用列表中能看 到此协议	没有设备
测试新应用发布	运维新应用发布	运维过程正常	没有设备

2.3 设备口令管理配置与测试

2.3.1 统一帐户管理

测试项目	操作方法	预期结果	实际结果
添加统一帐户	在统一帐户管理中添加关联某运维 用户的统一帐户	在帐户列表能看到此 统一帐户	
设置统一帐户隶属设备	在新增统帐户的隶属设备列表添 加保护资源	添加成功，被添加资源有此帐户 添加失败，被添加资源没有此帐户	在使用 windowsxp 作为控制资源时添加统一账户失败。
帐户分配	在授权列表中对添加成功的资源进 行帐户分配	帐户分配列表中有此 帐户	失败

2.3.2 设备帐户管理

2.3.2.1 类 Unix 保护资源自动登录配置与测试

测试项目	操作方法	预期结果	实际结果
设备账户管理	选择设备然后添加用户并激活， 注意选择是否密码托管和是否勾选管理账户	在账户资源列表中有此记录	没有测试

设备账户获取	选择添加有管理账户的设备， 获取该 设备上的其他账户	在账户资源列表中有 其他账户信息	没有测试
设备账户托管	可对账户密码进行重置	系统提示密码重置成 功	没有测试
密码变更通知	在口令管理配置编辑要发送邮件的 地址和主题，选择激活状态，需要配 置 DNS	在账户密码变更时，可 以向指定账户发送电 子邮件	没有测试
账户分配	在授权列表中对已经添加资源帐户 的资源对运维用户进行帐户分配， 就是将某一资源账户分配给运维账户	帐户分配列表中有已 添加的资源帐户	没有测试
自动登录验证	验证 SSH、SFTP 的自动登录功能	均能正常登录	没有测试

2.322 Windows 保护资源自动登录配置与测试

测试项目	操作方法	预期结果	实际结果
设备账户管理	选择设备分别采用正确、 错误的密码 添加用户并激活，注意选择是否密码 托管。	错误的密码无法添加 用户。正确的密码添加 用户成功。在账户资源 列表中有此记录。	
账户分配	在授权列表中对已经添加资源帐户 的资源对运维用户进行帐户分配， 就是将某一资源账户分配给运维账户	帐户分配列表中有已 添加的资源帐户	
设备账户托管	选择对用户的密码进行托管。 通过标 准 RDP 客户端验证，原有密码是否 可用。	托管后，原有密码已经 更改，不能登录远程设 备。	
自动登录验证	验证托管前和托管后，telnet 和 RDP 的自动登录功能。	用户托管前和托管后 均能正常登录。	

2.323 Serv-U 保护资源自动登录配置与测试

测试项目	操作方法	预期结果	实际结果

设备账户管理	选择设备分别采用正确、 错误的密码 添加用户，选择 ftp 专用账户并激活， 注意选择是否密码托管。	错误的密码无法添加 用户。正确的密码添加 用户成功。在账户资源 列表中有此记录。	

账户分配	在授权列表中对已经添加资源帐户 的资源对运维用户进行帐户分配， 就是将某一资源账户分配给运维账户	帐户分配列表中有已 添加的资源帐户	
设备账户托管	选择对用户的密码进行托管。 通过标 准 ftp 客户端连接真实服务器验证， 原有密码是否可用。	托管后，原有密码已经 更改，不能登录远程设 备	
自动登录验证	验证托管前和托管后，ftp 的自动登 录功能。	用户托管前和托管后 均能正常登录。	

2.324 未定义的操作系统保护资源自动登录配置与测试

测试项目	操作方法	预期结果	实际结果
添加未定义的操作系统	在资源管理的操作系统配置添加新的操作系统版本。保护资源以此新增的操作系统版本为操作系统类型	操作系统列表有新增的操作系统版本	审计平台安装过 于复杂，应为审 计信息安装到了 本地
SSO 配置	配置新增操作系统版本的参数 （Tel net 登录系统提示信息、Telnet 登录密码输入提示信息、Teln et 登录 成功提示信息等）	配置正常	
设备账户管理	选择设备然后添加用户并激活	若 SSO 配置正确，添 加帐户成功，在账户资 源列表中有此记录。 若 SSO 配置错误，无法添 加帐户，要修改 SSO 配置	
账户分配	在授权列表中对已经添加资源帐户 的资源对运维用户进行帐户分配， 就是将某一资源账户分配给运维账户	帐户分配列表中有已 添加的资源帐户	
自动登录验证	验证 telnet 的自动登录功能。	用能正常登录。	

2.325 密函打印审批

测试项目	操作方法	预期结果	实际结果