# 模板 XXX_XX 系统配置检查报告

| | | | |
|---|---|---|---|
| ■文档编号 | | ■密级 | 商业机密 |
| ■版本编号 | V1.0 | ■日期 | 2011-05-23 |

■**版本变更记录**

| 时间 | 版本 | 说明 | 修改人 |
| --- | --- | --- | --- |
| 2011-05-23 | V1.0 | 文档创建 | 李贵鹏 |
| | | | |
| | | | |
| | | | |

■**适用性声明**

本文档是绿盟科技在 XXXX 股份有限公司（以下简称“XXXX”）XXXX 系统安全服务中，对整体网络服务器进行安全手工检查后提交的手工检查报告，供相关人员参考。

# 目录

# 表格索引

# 插图索引

未找到目录项。

# 一. 概述

手工检查主要是通过人工以远程登陆的方式对检查范围内的服务器和网络、安全设备进行安全检查，通过远程的方式对被检查对象进行一系列的安全探测，以发现目标可能存在的安全隐患，是安全服务工作中发现信息系统脆弱性的主要技术手段之一。

通过手工检查工作，可以详细的了解当前网络和服务器中可能存在的潜在安全隐患，有效发现网络设备、操作系统和应用软件在补丁安装情况，帐号、口令策略，网络与服务，文件系统，日志审核增强，安全性增强等几个方面存在的安全风险、漏洞和威胁，为进一步通过技术手段降低或解决发现的问题提供了参考依据和方法。

在 XXXXX 系统安全服务中，绿盟科技使用手工检查对 XXXXX 系统服务器进行了安全检查，通过对检查结果的分析，对发现的问题提供了建议解决方案，供系统管理员参考。

接下来将对手工检查结果进行详细描述。

## 1.1 检查时间

| 安全检查时间 | |
|---|---|
| 起始时间 | 2011 年 05 月 20 日 |
| 结束时间 | 2011 年 05 月 20 日 |

## 1.2 检查范围

此次检查的范围为 XXXXX 系统。

表 1.1 手工抽样检查列表

| 区域划分描述 | IP 地址段 | 列表地址数量 | 抽样比例 | 手工检查地址数量 |
|---|---|---|---|---|
| ***** | 172.*.*.*/24 | 19 | 20% | 6 |
| ***** | 172.*.*.*/24 | 46 | 20% | 9 |
| ***** | 172.*.*.*/24 | 27 | 20% | 5 |
| ***** | 172.*.*.*/24 | 4 | 20% | 1 |
| ***** | 172.*.*.*/24 | 4 | 20% | 1 |
| ***** | 172.*.*.*/24 | 13 | 20% | 3 |

| | | | | |
|---|---|---|---|---|
| ***** | 172.*.*.*/24 | 16 | 20% | 3 |
| ***** | 172.*.*.*/24 | 29 | 20% | 6 |
| ***** | 172.*.*.*/24 | 18 | 20% | 4 |
| ***** | 172.*.*.*/24 | 9 | 20% | 2 |

选取原则为地址列表中的 20%作为手工检查主机：

- 首先，考虑表中“区域分组”
- 其次，考虑相同区域分组中选“应用说明”>“操作系统”
- 最后，在相同类型相同配置的主机中，我们一般选用 1 号主机和末号主机，为保证系统安全我们建议选用末号主机进行检查

选取网络设备列表如下：

表 1.2 手工检查服务器列表

| 设备名 | IP 地址 | 备注 |
|---|---|---|
| | 172.*.*.*/32 | 交换 |
| | 172.*.*.*/32 | 交换 |
| | 172.*.*.*/32 | 交换 |
| | 172.*.*.*/32 | 交换 |
| | 172.*.*.*/32 | 路由 |
| | 172.*.*.*/32 | 路由 |
| | 172.*.*.*/32 | 防火墙 |
| | 172.*.*.*/32 | 防火墙 |

选取服务器列表如下：

表 1.3 手工检查服务器列表

| IP 地址 | 主机名 | 操作系统版本 | 应用说明 |
|---|---|---|---|
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2003 R2 企业版 32 位 | |

| | | | |
|---|---|---|---|
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2003 R2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | Windows 2008 SP2 企业版 32 位 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |

| | | | |
|---|---|---|---|
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | RedHat Enterprise Linux 5.5 X86_64 | |
| 172.*.*.* | XXXXXXX | | |

## 1.3 检查内容

本次安全检查工作进行以下内容：

- 对检查范围内的系统、服务进行信息获取。
- 对检查范围内的系统、服务的漏洞进行检查；
- 提供安全漏洞修补建议；
- 提供手工检查列表

# 二. 检查结果摘要

**本次手工检查服务的工作内容包括：**

1、对网络设备、核心数据及中间件、总部接入、营业部接入、网上交易接入、三方存管、生产验证和灾备区等服务服务器系统进行了手工抽样检查；

2、对网络设备状态，风险状态，主要安全问题；服务器主机状态，风险状态，主要安全问题；数据库应用状态，风险状态，主要安全问题进行分析；

3、通过发掘网络设备和服务器中存在的安全隐患（系统隐患、应用配置缺陷），以便能根据这些检测信息修补漏洞缺陷，为维护服务器的健康稳定，提供相应的安全建议；

**本次手工检查服务结果：**

1、本次检查交换和路由设备，没有未发现严重问题；

2、本次检查防火墙设备，发现配置策略未生效、存在日志审计、设备管理、攻击防护和部分配置漏洞等问题；

3、本次检查 Windows 主机发现系统，存在日志审计、文件系统、windows 服务配置、登录管理、安全配置和部分配置漏洞等问题；

4、本次检查 Linux 主机发现系统，存在账号管理、口令管理、登陆管理、服务安全和部分配置漏洞等问题；

5、本次检查 AIX 主机发现系统，存在口令管理、日志审计、登录管理、服务安全和部分配置漏洞等问题；

6、本次检查数据库发现，存在登录管理、ORACLE 账号权限、服务安全等问题；

# 三. 检查结果分析

本次检查中共 40 台有效设备，其中对网络设备 8 台和服务器 32 台进行了检查，下面将手工检查结果进行详细分析。

## 3.1 风险分布

绿盟科技的工程师分析了当前网络、系统、数据库风险状况，发现 Windows 系统、Linux 系统、AIX 系统和数据库大都存在共性漏洞，所以会从漏洞列表层面进行细致的罗列分析。

## 3.2 网络设备检查列表

在本次检查中交换机，路由器存在口令管理、设备配置漏洞等问题；

在本次检查中发现防火墙主要存在以下问题未启用策略，在业务允许的情况下，强烈建议修补。

### 3.2.1 交换机

在本次检查中针对交换机设备，分别对系统管理、账号管理、口令要求、日志审计、设备管理、服务安全、安全防护、增强要求要求这 8 个方面进行了检查。

发现交换机设备主要存在以下问题口令管理、设备配置漏洞等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补

#### 3.2.1.1 RC07-JY-AS35-12

表 3.1 RC07-JY-AS35-12 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 设备名称 | |
| 应用说明 | 交换 | 版本号 | |
| **设备当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |

| | | | |
|---|---|---|---|
| 系统管理 | 系统版本 | 12.2 | 建议系统版本升级为 12.2 及以上版本并定期进行配置备份。 |
| 账号管理 | 共享账户检查 | 无 | 建议记录要求账号和用户为一对一的关系 |
| 口令要求 | 口令复杂度要求 | 长度满足且复杂度满足 | 建议采用静态口令认证技术的设备，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。 |
| | 口令加密功能 | 已启用 | 建议口令采用 enable secret 设置方式 |
| 日志审计 | 远程日志服务器存储 | 已启用 | 建议设备日志均能通过远程日志功能传输到日志服务器 |
| 设备管理 | SSH 登陆维护 | transport input telnet ssh 存在 telnet 维护模式 | 建议使用 SSH 方式访问 |
| | 登陆账户超时退出 | 已设置 exec-timeout 5 | 建议设置 exec-timeout 为 30 秒以内 |
| | SNMP 安全强化 | SNMP 开启,为业务需要 | 建议关闭 SNMP 服务，防止管理漏洞 |
| | 关闭未使用接口 | shutdown 命令为业务需要 | 建议禁用交换机 shutdown 命令或路由器的 AUX 端口 |
| 服务安全 | 禁用非必要网络服务 | 未见多于服务 | 建议禁用 Finger 服务、CDP 服务、DNS 服务、TCP small 服务、UDP small 服务、bootp 服务、从网络启动、从网络下载初始配置文件 |
| | 关闭非必要网络路由功能 | IP Classless 为业务需要 | 建议禁用 IP 源路由服务、ARP-Proxy 服务、IP Classless、Directed Broadcast |
| 安全防护 | 端口安全防范 | 已启用 port-security | 建议启用端口安全防范 MAC Spoofing 和 |

| | | | |
|---|---|---|---|
| | | | MAC Address Flooding |
| | 过滤常见已知攻击 | 未配置 | 建议在网络边界，设置安全访问控制列表，过滤掉已知安全攻击数据包，例如 TCP 1434 端口（防止 SQL slammer 蠕虫）tcp445,5800,5900（防止 Della 蠕虫） |
| | ACL 控制业务服务访问 | 已配置 | 建议 ACL 的配置必须精确到协议，IP 或端口 |
| | 日志时间 NTP | ntp server 已启用，业务需要 | 建议关闭 NTP 服务 |
| 增强要求 | 更改设备缺省 Banner | ACCESS IS RESTRICTED TO AUTHORISED PERSONNEL ONLY | 修改路由交换设备的缺省 Banner 信息，Banner 最好不要有系统平台或地址等有碍安全的信息 |
| | SNMP 服务主机限制 | 已配置 | 建议只与特定主机进行 SNMP 协议交互 |
| | 禁用 SNMP 写功能 | 已启动 | 未使用 SNMP 的 WRITE 功能时，禁用 SNMP 的写（WRITE）功能。启用 SNMP 写功能，建议设置复杂度足够的 Community 字符串 |

### 3.2.2 路由器

在本次检查中针对路由器设备，分别对系统管理、账号管理、口令要求、日志审计、设备管理、服务安全、安全防护、增强要求要求这 8 个方面进行了检查。

发现路由器设备主要存在以下问题口令管理、设备管理配置漏洞等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补

### 3.2.2.1 RC07-JY-AR28-4

表 3.2 RC07-JY-AR28-4 检查列表

| 基本信息 | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 设备名称 | |
| 应用说明 | 交换 | 版本号 | |
| **设备当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 系统管理 | 系统版本 | 12.2 | 建议系统版本升级为 12.2 及以上版本并定期进行配置备份。 |
| 账号管理 | 共享账户检查 | 无 | 建议记录要求账号和用户为一对一的关系 |
| 口令要求 | 口令复杂度要求 | 长度满足且复杂度满足 | 建议采用静态口令认证技术的设备，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。 |
| | 口令加密功能 | 已启用 | 建议口令采用 enable secret 设置方式 |
| 日志审计 | 远程日志服务器存储 | 已启用 | 建议设备日志均能通过远程日志功能传输到日志服务器 |
| 设备管理 | SSH 登陆维护 | transport input telnet ssh 存在 telnet 维护模式 | 建议使用 SSH 方式访问 |
| | 登陆账户超时退出 | 已设置 exec-timeout 5 | 建议设置 exec-timeout 为 30 秒以内 |
| | SNMP 安全强化 | SNMP 开启，业务需要 | 建议关闭 SNMP 服务，防止管理漏洞 |
| | 关闭未使用接口 | 已关闭 line aux 0 | 建议禁用交换机 shutdown 命令或路由器的 AUX 端口 |

| | | | |
|---|---|---|---|
| 服务安全 | 禁用非必要网络服务 | 未见多于服务 | 建议禁用 Finger 服务、CDP 服务、DNS 服务、TCP small 服务、UDP small 服务、bootp 服务、从网络启动、从网络下载初始配置文件 |
| | 关闭非必要网络路由功能 | IP Classless 为业务需要 | 建议禁用 IP 源路由服务、ARP-Proxy 服务、IP Classless、Directed Broadcast |
| 安全防护 | 过滤常见已知攻击 | 未配置 | 建议在网络边界，设置安全访问控制列表，过滤掉已知安全攻击数据包，例如 TCP 1434 端口（防止 SQL slammer 蠕虫）tcp445,5800,5900（防止 Della 蠕虫） |
| | ACL 控制业务服务访问 | 已配置 | 建议 ACL 的配置必须精确到协议，IP 或端口 |
| | 日志时间 NTP | ntp server 已启用，业务需要 | 建议关闭 NTP 服务 |
| 增强要求 | 更改设备缺省 Banner | ACCESS IS RESTRICTED TO AUTHORISED PERSONNEL ONLY This system is equipped with a security system | 修改路由交换设备的缺省 Banner 信息，Banner 最好不要有系统平台或地址等有碍安全的信息 |
| | SNMP 服务主机限制 | 已配置 | 建议只与特定主机进行 SNMP 协议交互 |

| | | | |
|---|---|---|---|
| | 禁用 SNMP 写功能 | 已启动 | 未使用 SNMP 的 WRITE 功能时，禁用 SNMP 的写（WRITE）功能。启用 SNMP 写功能，建议设置复杂度足够的 Community 字符串 |

### 3.2.3 防火墙

在本次检查中针对防火墙设备，分别对系统管理、账号管理、口令要求、日志审计、设备管理、攻击防护、安全管理这 7 个方面进行了检查。

发现防火墙设备主要存在以下问题日志审计、设备管理、攻击防护配置等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补

#### 3.2.3.1 RC07-JY-AF55-1

表 3.3 RC07-JY-AF55-1 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 设备名称 | |
| 应用说明 | 防火墙 | 版本号 | |
| **设备当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 系统管理 | 系统以及配置 | 未查找到版本信息 | 建议系统版本升级为较新版本并定期进行配置备份。 |
| 账号管理 | 账户检查 | 仅存在 admin | 建议删除或锁定与设备运行、维护等工作无关的账号 |
| 口令要求 | 更改初始账号和密码 | 未见初始账号 | 防火墙出厂时缺省配置了初始登陆名，建议进行修改 |
| | 口令长度功能 | 已启用 | 防火墙只能限制口令的长度策略，建议采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母 |

| | | | |
|---|---|---|---|
| | | | 和特殊符号 4 类中至少 2 类。 |
| 日志审计 | 远程日志服务器存储 | 已配置 | 建议设备日志均能通过远程日志功能传输到日志服务器 |
| | 警告配置要求 | 未配置，已启用第三方 | 建议配置告警功能，报告对防火墙本身的攻击或者防火墙的系统内部错误。 |
| 设备管理 | SSH 登陆维护 | set ssh version v2 | 建议使用 HTTPS/SSH 方式访问 |
| | 管理地址限制 | 未配置 | 建议对防火墙的管理地址做源地址限制 |
| | 访问控制列表规范 | 已配置 | 建议在配置访问规则时，源地址，目的地址，服务或端口的范围必须以实际访问需求为前提，尽可能的缩小范围。 |
| 攻击防护 | 常见漏洞防范 | 已配置 | 建议配置访问控制规则 |
| | 防地址欺骗攻击 | 未配置 | 建议开启防源地址欺骗功能 |
| 安全管理 | SNMP 安全控制 | SNMP 开启 | 建议使用 SNMP V3 以上的版本对防火墙做远程管理。 |
| | 设备 Banner 信息检查 | 未找到 banner 信息 | 修改防火墙的缺省 Banner 信息，Banner 最好不要有系统平台或地址等有碍安全的信息 |

## 3.3 系统检查列表

根据手工检查结果和漏洞的风险等级，以及操作的难易程度和对系统的影响，绿盟科技给出修补漏洞的优先级，在充分测试的前提下修复应用程序的漏洞。

检查列表描述了安全检查中发现的各主机相关安全问题，并给出了绿盟科技的专家意见供参考。

### 3.3.1 Windows 服务器

在本次检查中针对 WINDOWS 操作系统，分别对账号管理、口令配置、认证授权、日志审计、登录管理、共享安全、安全防护、服务安全这 8 个方面进行了检查。

发现 Windows 系统主要存在以下问题日志审计、文件系统、windows 服务配置、登录管理、安全配置和部分配置漏洞等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补。

#### 3.3.1.1 172.22.98.102 服务器

表 3.4 172.22.98.102 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 域名/主机名 | |
| 外部 IP 地址 | | 内部 IP 地址 | |
| 应用说明 | | | |
| 操作系统 | Windows Server 2008 | 版本号 | Product version: 6.0.6002 |
| | | | Service pack: 2 |
| | | | Kernel build number: |
| **应用服务信息** | | | |
| 名称 | 应用服务及版本情况 | | |
| 杀毒软件 | 无 | | |
| **主机当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 帐号检查 | 管理员账号更名 | administrator | 建议更改缺省帐户名称 administrator |
| | Guest 用户是否禁用 | 已禁用 guest | 禁用 guest（来宾）账户 |

| | | | |
|---|---|---|---|
| | 是否存在多余帐号 | 未见多余账号 | 避免共用账号,禁用多余账号 |
| 日志配置操作 | 登录日志审核 | 未配置 | 建议审核账户登录的成功和失败事件 |
| | 审核策略更改 | 未配置 | 建议审核策略更改日志的成功和失败事件 |
| | 审核对象访问 | 未配置 | 建议审核对象访问日志的成功和失败事件 |
| | 目录服务访问 | 未配置 | 建议审核目录服务访问日志的成功和失败事件 |
| | 审核特权使用 | 未配置 | 建议审核特权使用日志的成功和失败事件 |
| | 审核系统事件 | 未配置 | 建议审核系统事件日志的成功和失败事件 |
| | 进程跟踪 | 未配置 | 建议进程跟踪日志的成功和失败事件 |
| | 审核账户管理 | 未配置 | 建议账户管理日志的成功和失败事件 |
| | 应用日志大小配置 | 满足要求 | 建议应用日志的大小为32M 并按需要改写事件 |
| | 系统日志大小配置 | 满足要求 | 建议系统日志的大小为32M 并按需要改写事件 |
| | 安全日志大小配置 | 满足要求 | 建议安全日志的大小为32M 并按需要改写事件 |
| 文件系统 | 默认共享检查 | 存在默认共享 | 建议在非域环境中，关闭Windows 硬盘默认共享 |
| | 共享权限检查 | 未配置 | 禁止使用共享权限为”everyone” |
| windows 服务配置 | 屏保密码保护 | 未设置 | 建议设置带密码的屏幕保护，并将时间设定为不大于 15 分钟 |
| | 自动播放关闭 | 未关闭 Windows 自动播放功能 | 建议关闭 Windows 自动播放功能 |
| | SNMP 默认口令修改 | 采用默认的 public | 建议修改 SNMP Community String 默认设置 |
| | 启动项检查 | 未见可疑启动项 | 建议关闭可疑启动项 |

| | | | |
|---|---|---|---|
| | 服务检查 | Task Scheduler、Routing and Remote Access、Remote Registry、Print Spooler | 建议关闭非必需服务 |
| 帐户策略 | 口令复杂度策略 | 未启用 | 1、密码长度不少于 12 位<br>2、至少包括特殊字符、数字、英文大写、英文小写中的三种 |
| | 口令最长生存期策略 | 已启用 | 建议操作系统的账户口令的最长生存期不长于 90 天 |
| | 登录失败账户锁定策略 | 未配置 | 建议配置超过 8 次登录失败锁定账号策略 |
| 登录管理 | 远程登录超时配置 | 未启用 | 建议远程登录超时为 15 分钟 |
| 认证授权 | 远程关机授权 | 仅属于 Administrators 组 | 建议远端系统强制关机只指派给 Administrators 组 |
| | 系统关闭授权 | 还存在其他组 | 关闭系统仅指派给 Administrators 组 |
| | 文件权限指派 | 仅属于 Administrators 组 | 文件或其它对象的所有权仅指派给 Administrators |
| | 匿名权限限制 | 未限制匿名用户连接权限 | 只允许授权帐号从网络访问此计算机 |
| 安全配置 | DEP 功能启用 | 未启用数据执行保护 | 建议启用 DEP 功能 |
| | 启用 SYN 攻击保护设置 | 未启用 | 建议在提供对外访问的服务器上设置 |
| | Windows 是否启用自带防火墙 | 未启用 | 建议启用 Windows 自带防火墙 |
| 防病毒管理 | 是否安装防病毒软件 | 未安装 | 建议安装防病毒软件 |
| | 是否正常升级 | 不适用 | 建议安装后及时更新 |
| 系统管理 | 系统补丁 | 已启用自动更新 | 建议及时更新系统补丁 |

### 3.3.1.2 172.22.100.18 服务器

表 3.5 172.22.100.18 检查列表

| 基本信息 | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 域名/主机名 | p1j18rzrqbp02 |
| 外部 IP 地址 | | 内部 IP 地址 | 172.22.100.18 |
| 应用说明 | 融资融券全报盘深圳接口-02 | | |
| 操作系统 | Windows Server 2003 | 版本号 | Product version: 5.2 |
| | | | Service pack: 2 |
| | | | Kernel build number: 3790 |
| **主机当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 帐号检查 | 管理员账号更名 | administrator | 建议更改缺省帐户名称 administrator |
| | Guest 用户是否禁用 | 已禁用 guest | 禁用 guest（来宾）账户 |
| | 是否存在多余帐号 | 未见多余账号 | 避免共用账号,禁用多余账号 |
| 日志配置操作 | 登录日志审核 | 未配置 | 建议审核账户登录的成功和失败事件 |
| | 审核策略更改 | 未配置 | 建议审核策略更改日志的成功和失败事件 |
| | 审核对象访问 | 未配置 | 建议审核对象访问日志的成功和失败事件 |
| | 目录服务访问 | 未配置 | 建议审核目录服务访问日志的成功和失败事件 |
| | 审核特权使用 | 未配置 | 建议审核特权使用日志的成功和失败事件 |
| | 审核系统事件 | 未配置 | 建议审核系统事件日志的成功和失败事件 |
| | 进程跟踪 | 未配置 | 建议进程跟踪日志的成功和失败事件 |
| | 审核账户管理 | 未配置 | 建议账户管理日志的成功和失败事件 |
| | 应用日志大小配置 | 满足要求 | 建议应用日志的大小为 32M 并按需要改写事件 |
| | 系统日志大小配置 | 满足要求 | 建议系统日志的大小为 32M 并按需要改写事件 |
| | 安全日志大小配置 | 满足要求 | 建议安全日志的大小为 32M 并按需要改写事件 |

| | | | |
|---|---|---|---|
| 文件系统 | 默认共享检查 | 存在默认共享 | 建议在非域环境中，关闭 Windows 硬盘默认共享 |
| | 共享权限检查 | 未配置 | 禁止使用共享权限为”everyone” |
| windows 服务配置 | 屏保密码保护 | 未设置 | 建议设置带密码的屏幕保护，并将时间设定为不大于 15 分钟 |
| | 自动播放关闭 | 未关闭 Windows 自动播放功能 | 建议关闭 Windows 自动播放功能 |
| | SNMP 默认口令修改 | 采用默认的 public | 建议修改 SNMP Community String 默认设置 |
| | 启动项检查 | 未见可疑启动项 | 建议关闭可疑启动项 |
| | 服务检查 | Task Scheduler、Routing and Remote Access、Remote Registry、Print Spooler | 建议关闭非必需服务 |
| 帐户策略 | 口令复杂度策略 | 未启用 | 1、密码长度不少于 12 位 2、至少包括特殊字符、数字、英文大写、英文小写中的三种 |
| | 口令最长生存期策略 | 已启用 | 建议操作系统的账户口令的最长生存期不长于 90 天 |
| | 登录失败账户锁定策略 | 未配置 | 建议配置超过 8 次登录失败锁定账号策略 |
| 登录管理 | 远程登录超时配置 | 未启用 | 建议远程登录超时为 15 分钟 |
| 认证授权 | 远程关机授权 | 仅属于 Administrators 组 | 建议远端系统强制关机只指派给 Administrators 组 |
| | 系统关闭授权 | 还存在其他组 | 关闭系统仅指派给 Administrators 组 |
| | 文件权限指派 | 仅属于 Administrators 组 | 文件或其它对象的所有权仅指派给 Administrators |
| | 匿名权限限制 | 未限制匿名用户连接权限 | 只允许授权帐号从网络访问此计算机 |
| 安全配置 | DEP 功能启用 | 未启用数据执行 | 建议启用 DEP 功能 |

| | | | |
|---|---|---|---|
| | | 保护 | |
| | 启用 SYN 攻击保护设置 | 未启用 | 建议在提供对外访问的服务器上设置 |
| | Windows 是否启用自带防火墙 | 未启用 | 建议启用 Windows 自带防火墙 |
| 防病毒管理 | 是否安装防病毒软件 | 未安装 | 建议安装防病毒软件 |
| | 是否正常升级 | 不适用 | 建议安装后及时更新 |
| 系统管理 | 系统补丁 | 已启用自动更新 | 建议及时更新系统补丁 |

## 3.3.2 Linux 服务器

在本次检查中针对 Linux 操作系统，分别对账号管理、口令配置、认证授权、日志审计、协议安全、服务安全这 6 个方面进行了检查。

发现 Linux 系统主要存在以下问题系统账号管理、口令管理、登陆管理、服务安全和部分配置漏洞等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补。

### 3.3.2.1 172.22.98.34 服务器

表 3.6 172.22.98.34 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 域名/主机名 | |
| 外部 IP 地址 | | 内部 IP 地址 | |
| 应用说明 | | | |
| 操作系统 | Linux | 版本号 | Product version: 5.5 |
| | | | Kernel build number: 2.6.18 |
| **主机当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 账号管理 | 共享账号检查 | 无 | 避免共用账号的情况 |
| | 多余账户锁定策略 | **** | 建议锁定与设备运行、维护等工作无关的账号 |
| | root 账户远程登录限制 | PermitRootLogin yes | 建议限制具备超级管理员权限的用户远程 |

| | | | |
|---|---|---|---|
| | | | 登录 |
| 口令配置 | 口令复杂度策略 | password requisite pam_cracklib.so try_first_pass retry=3 | 1、密码长度不少于 12 位<br>2、至少包括特殊字符、数字、英文大写、英文小写中的三种 |
| | 口令最长生存期策略 | PASS_MAX_DAYS 99999<br>PASS_MIN_DAYS 0<br>PASS_MIN_LEN 5<br>PASS_WARN_AGE 7 | 建议操作系统的账户口令的最长生存期不长于 90 天 |
| 认证授权 | 系统关键目录权限控制 | passwd:-rw-r--r--<br>shadow:-r--------<br>group:-rw-r--r-- | 建议配置某些关键目录其所需的最小权限 |
| | 用户缺省权限控制 | umask 002<br>umask 022 | 建议全局默认设置 umask 值为 027 或更小权限 |
| 日志审计 | 系统日志完备性检查 | 已启用 log:/var/log/secure | |
| | 统一远程日志服务器配置 | 未进行配置 | 建议配置远程日志功能，将需要重点关注的日志内容传输到日志服务器进行备份 |
| | 设置 history 时间戳 | no config | 建议配置 history 时间戳 |
| 登录管理 | SSH 登录配置 | 未配置 PermitRootLogin no<br>PermitEmptyPasswords no | 建议配置使用 SSH 等加密协议进行远程登录维护，并安全配置 SSHD 的设置。不使用 TELENT 进行远程登录维护 |
| 服务安全 | 关闭不必要的系统服务 | sendmail 0:off 1:off 2:on 3:on 4:on 5:on 6:off<br>bluetooth 0:off 1:off 2:on 3:on 4:on 5:on 6:off | 建议关闭不必要的系统服务 |
| | 禁止 Cotrol-alt-Delete | 已启用<br>ca::ctrlaltdel:/sbin/shutdown -t3 -r now | |

### 3.3.3 AIX 服务器

在本次检查中针对 AIX 操作系统，分别对账号管理、口令配置、认证授权、日志审计、登录管理、服务安全这 6 个方面进行了检查。

发现 AIX 系统主要存在以下问题系统口令管理、日志审计、登录管理、服务安全和部分配置漏洞等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补。

#### 3.3.3.1 172.22.98.11 服务器

表 3.7 172.22.98.11 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 域名/主机名 | p1dbcx1 |
| 外部 IP 地址 | | 内部 IP 地址 | 172.22.98.11 |
| 应用说明 | 备份-AIX 服务器 | | |
| 操作系统 | AIX | 版本号 | Product version: 6.1<br>Kernel build number: 2.6.18 |
| **主机当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 账号管理 | 共享账号检查 | 无 | 避免共用账号的情况 |
| | 多余账户锁定策略 | 无 | 建议锁定与设备运行、维护等工作无关的账号 |
| | root 账户远程登录限制 | PermitRootLogin yes | 限制具备超级管理员权限的用户远程登录 |
| 口令配置 | 口令复杂度策略 | minlen=0<br>minalpha=0<br>mindiff=0<br>minother=0<br>pwdwarntime=0 | 1、密码长度不少于 12 位<br>2、至少包括特殊字符、数字、英文大写、英文小写中的三种 |
| | 口令最长生存期策略 | histexpire = 0 | 建议操作系统的账户口令的最长生存期不长于 90 天 |
| 认证授权 | 系统关键目录权限控制 | passwd:-rw-r--r--<br>shadow:-r-------- | 建议配置某些关键目录其所需的最小权限 |

| | | | |
|---|---|---|---|
| | | group:-rw-r--r-- | |
| | 用户缺省权限控制 | umask 022 | 建议全局默认设置 umask 值为 027 或更小权限 |
| 日志审计 | 系统日志完备性检查 | 未进行配置 | 建议系统应配置完备日志记录，记录对与系统相关的安全事件 |
| | 统一远程日志服务器配置 | 未进行配置 | 建议配置远程日志功能，将需要重点关注的日志内容传输到日志服务器进行备份 |
| | 设置 history 时间戳 | no config | 建议配置 history 时间戳 |
| 登录管理 | SSH 登录配置 | 未配置 PermitRootLogin no<br>PermitEmptyPasswords no | 建议配置使用 SSH 等加密协议进行远程登录维护，并安全配置 SSHD 的设置。不使用 TELENT 进行远程登录维护 |
| 服务安全 | 关闭不必要的系统服务 | sendmail 0:off 1:off 2:on 3:on 4:on 5:on 6:off<br>bluetooth 0:off 1:off 2:on 3:on 4:on 5:on 6:off | 建议关闭不必要的系统服务 |
| | 禁止 Cotrol-alt-Delete | 未进行配置 | 建议禁止 Control-Alt-Delete 键盘关闭命令 |

## 3.4 数据库检查列表

在本次检查中针对 Oracle 数据库，分别对账号管理、口令要求、登录管理、ORACLE 账号权限、服务安全这 5 个方面进行了检查。

发现 Oracle 数据库主要存在以下问题登录管理、ORACLE 账号权限、服务安全等问题，在检查项给出手工检查所对应的安全建议。在业务允许的情况下，强烈建议修补

### 3.4.1 Oracle 数据库

表 3.8 Qracle 检查列表

| **基本信息** | | | |
|---|---|---|---|
| 设备所在地 | 北京 | 域名/主机名 | |
| 外部 IP 地址 | | 内部 IP 地址 | |
| 应用说明 | | | |
| 数据库 | Qracle | 版本号 | Product version: 10g |
| **主机当前状态** | | | |
| 检查项目 | 检查类别 | 状态 | 安全建议 |
| 账号管理 | 共享账户检查 | 无 | 避免不同用户间共享账号 |
| | 多余账号锁定 | 无 | 建议删除或锁定与数据库运行、维护等工作无关的账号。 |
| 口令管理 | 登录失败锁定策略 | 未配置 | 建议当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号。建议在设置锁定次数的同时设置一个口令锁定时间值，使得超过此值则自动解除账号锁定。 |

| | | | |
|---|---|---|---|
| | 更改默认账号密码 | 已更改 | 建议更改数据库默认帐号的密码，不能以用户名作为密码或使用默认密码的账户登陆到数据库。 |
| | 启用密码管理策略 | 未配置 | 建议开启密码管理策略，当用户连续认证失败次数超过规定次数时，锁定该用户使用的账号； |
| | 口令最长生存期策略 | 未配置 | 建议账户口令的生存期不长于 90 天。周期性地改变口令是一种很好的安全措施。 |
| 登陆管理 | 限制 SYSDBA 远程登录 | 未配置 | 建议限制具备数据库超级管理员（SYSDBA）权限的用户远程登录。 |
| | 空闲远程连接断开 | 未配置 | 建议 10 分钟以上的无任何操作的空闲数据库连接设置自动断开 |
| 权限管理 | 数据字典保护 | 未配置 | 建议启用数据库字典保护达到保护数据库的目的，从而普通 dba 登陆到数据库，不具备访问 X$开头的表，以此来加强对数据库的保护 |
| 服务安全 | 数据库监听器关闭和启动设置密码 | 未配置 | 使用 lsnrctl start 或 lsnrctl stop 命令起停 listener 需要密码； |

# 四. 安全建议

此次出现的高风险，可以折射出部分管理制度缺失，提供以下建议供中信证券相关人员参考。

- 建议所有 Windows 系统使用“Windows Update”进行更新。
- 对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。
- 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
- 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。
- 对于 Oracle 系统或者应用程序订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。
- 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。

# 五. 本期检查总结

从检查结果中可以看出，XXXXX 系统的服务器和 Oracle 数据库系统都存在较为严重的安全隐患，需要对操作系统及数据库进行加固，具体加固建议在文档中已列出。

在实施加固时需要注意避免正在使用的业务系统，可以先加固备份服务器，经测试能正常使用后再加固其它服务器。