# 安徽文达信息工程学院

# 网络应用服务器安全巡检暂行规定

我校各网络应用服务器隶属各业务部门主管使用。日常维护中，各部门无专人负责技术运维，服务器运行不正常的情况时有发生。现按校办公会决定要求，依据《安徽文达信息工程学院网络与信息安全管理办法》和《信息技术中心托管服务器（业务平台）管理办法》等文件精神，决定对各服务器开展月巡检，通过定期检查，提高服务器安全性，确保服务器正常运行。

**一、巡检范围**

所有运行在网络上、对内对外提供网络应用服务的服务器，包括自购的和托管在信息中心机房的，均纳入巡检范围，每月至少需巡检一次。

**二、巡检关注点**

安全巡检的主要关注点是系统的基本运行状况和异常反应，包括反应速度、系统拥塞等重点表现。各使用部门应对服务器做好关键节点的系统状态镜像，保存好系统运行日志和必要的状态参数，为巡检提供基本数据。

**三、巡检内容**

安全巡检应尽可能覆盖服务器运维和安全的全部内容，如系统服务、系统账户和权限、安全策略、防火墙、防病毒系统、操作系统补丁、用户密码安全（重点是密码强度和更改期限）、应用安全、磁盘权限等。

**四、巡检过程**

巡检工作由信息中心人员按月度计划实施，每月至少一次。巡检时，巡检人应根据服务器表现现象和具体情况给予谨慎合理的判断，并做好记录和分析笔记。巡检过程如下：

1、远程服务器至桌面，或SSH登录到远程服务器；也可现场直接进入服务器。

2、查看系统进程，比对异常情况，对可疑进行进程登记并结束进程；

3、查看系统用户账户、密码，发现可疑用户立即登记并禁用，修改其密码，查看其登陆痕迹，用户组中清理其权限；同时督促用户对过期密码进行更改。

4、查看系统服务，比对有无异常，发现可疑服务登记其位置，停止运行并作处理；

5、检查防火墙是否开启，例外列表是否异常；

6、检查防病毒系统更新情况，运行是否正常，有无篡改痕迹；

7、检查系统日志，关注安全日志，可备份后下载至本地进行分析；

8、检查数据库，比对数据库列表；

9、检查备份任务或系统镜像执行情况，及时纠正错误任务，适时做好镜像。

**五、异常管理和跟踪**

如遇异常情况，需要快速特别对待，及时先保护现场并处理，留下证据；切断异常服务器同外部的联系。

以上规定从发布之日起试行，希望全校各业务网络应用服务器主管部门给予巡检支持。

2021年服务器巡检计划表

|  |  |  |
| --- | --- | --- |
| 日期 | 巡检应用服务器 | 主管部门 |
| 4月 | 28 | 网站服务器 | 宣传处 |
| 29 | 教务系统 | 教务处 |
| 30 | 学工系统 | 学生处 |
| 5月 | 26 | 网站服务器 | 宣传处 |
| 27 | 教务系统 | 教务处 |
| 28 | 学工系统 | 学生处 |
| 6月 | 23 | 网站服务器 | 宣传处 |
| 24 | 教务系统 | 教务处 |
| 25 | 学工系统 | 学生处 |
| 7月 | 28 | 网站服务器 | 宣传处 |
| 29 | 教务系统 | 教务处 |
| 30 | 学工系统 | 学生处 |
| 8月 | 25 | 网站服务器 | 宣传处 |
| 26 | 教务系统 | 教务处 |
| 27 | 学工系统 | 学生处 |
| 9月 | 28 | 网站服务器 | 宣传处 |
| 29 | 教务系统 | 教务处 |
| 30 | 学工系统 | 学生处 |
| 10月 | 27 | 网站服务器 | 宣传处 |
| 28 | 教务系统 | 教务处 |
| 29 | 学工系统 | 学生处 |
| 11月 | 24 | 网站服务器 | 宣传处 |
| 25 | 教务系统 | 教务处 |
| 26 | 学工系统 | 学生处 |
| 12月 | 29 | 网站服务器 | 宣传处 |
| 30 | 教务系统 | 教务处 |
| 31 | 学工系统 | 学生处 |

应用服务器巡检表

服务器名称 主管部门

|  |  |  |  |
| --- | --- | --- | --- |
| 巡检时间 |   | 操作人员 |   |
| 巡检项目表 |
| 内容 | 参考标准 | 原纪录 | 检查情况 |
| 1、用户和组 |  用户名和密码是否符合要求 |   |  是[ ]  否[ ]  |
| 2、系统服务 |  系统服务是否正常 |   |  是[ ]  否[ ]  |
| 3、系统进程 |  系统进程是否正常 |   |  是[ ]  否[ ]  |
| 4、系统防火墙 |  防火墙是否开启 |   |  是[ ]  否[ ]  |
| 5、防病毒系统 |  防病毒软件是否开启 |   |  是[ ]  否[ ]  |
| 6、系统日志 |  系统日志是否保留记录 |   |  是[ ]  否[ ]  |
| 7、数据库 |  数据库是否正常 |   |  是[ ]  否[ ]  |
| 8、备份执行情况 |  备份是否正常 |   |  是[ ]  否[ ]  |
| 9、磁盘权限 |  磁盘权限是否更改 |   |  是[ ]  否[ ]  |
| 10、网站上传目录 |  是否正常 |   |  是[ ]  否[ ]  |
| 11、系统补丁升级 |  系统补丁是否正常 |   |  是[ ]  否[ ]  |
| 12、其他情况 |  |  |  |

备注：如遇上述技术问题，我中心积极配合，提供技术保障。

 巡检人员签字：

 服务器单位负责人签字：

 日期： 年 月 日