信息安全管理与评估　第一阶段

网络系统集成与安全防护

（样题）

目 录

第一阶段竞赛项目试题（此为样题，仅作试题形式参考）

本文件为信息安全管理与评估项目竞赛-第一阶段试题，第一阶段内容包括：网络平台搭建、网络安全设备配置与防护。

本次比赛时间为240分钟。

介绍

竞赛阶段	任务阶段	竞赛任务
第一阶段 网络系统集成与安全防护	任务1	网络系统集成
	任务2	网络系统安全加固

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

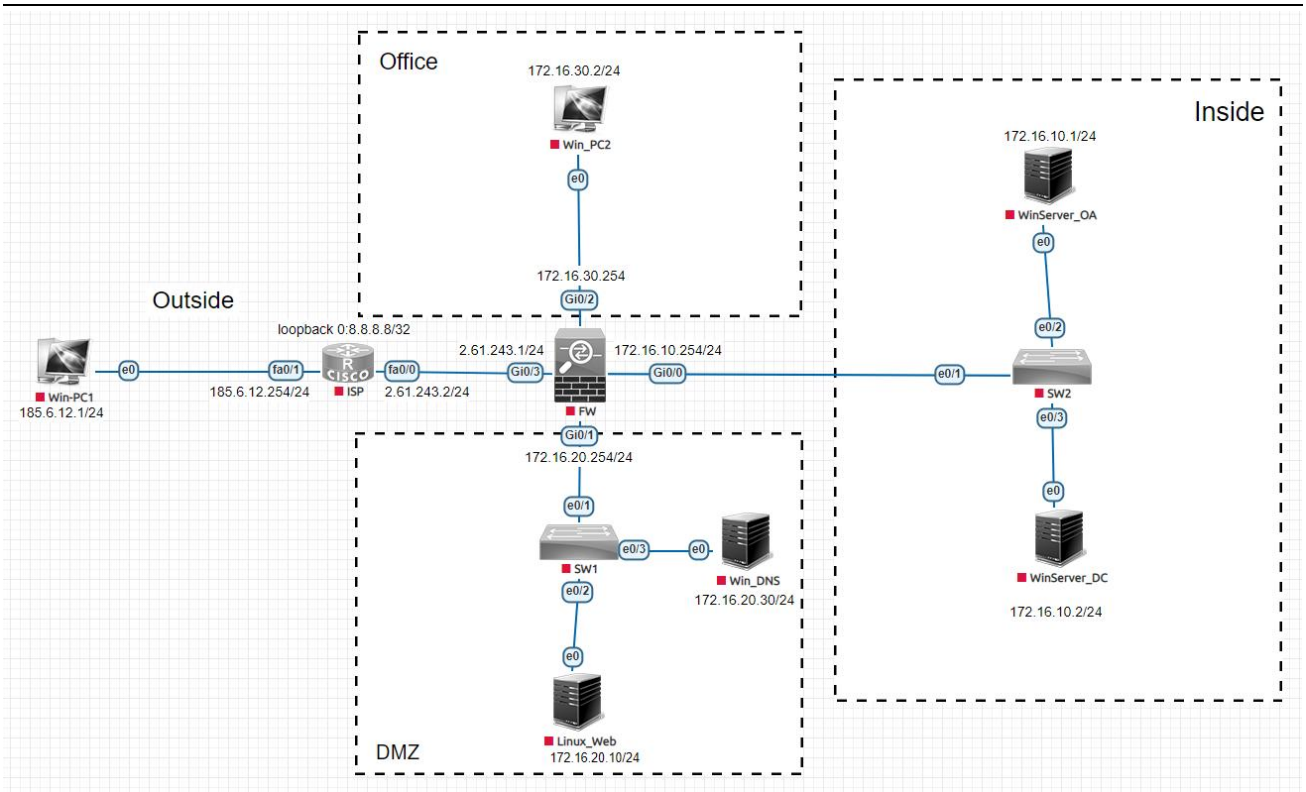
本项目阶段分数为40分。

注意事项

本赛项评分方式为上机检测，参赛选手在答题过程中请勿将用户名及密码修改为非指定密码。如判分员无法登陆系统，且无法验证赛题结果，该赛题无法得分。

项目和任务描述

1. 网络拓扑图



2. IP地址规划表

设备名称	接口	IP地址	说明
ISP	fa0/0	2.61.243.2/24	接Win_PC1
	fa0/1	185.6.12.254/24	接FW Gi0/2
	loopback 0	8.8.8.8/32	管理地址
FW	Gi0/0	172.16.10.254/24	Inside区
	Gi0/1	172.16.20.254/24	DMZ区
	Gi0/2	172.16.30.254/24	Office办公区
	Gi0/3	2.61.243.1/24	Outside区
SW1	e0/1	——	接FW Gi0/1
	e0/2	——	接Linux_web
	e0/3	——	接Win_DNS
SW2	e0/1	——	接FW Gi0/0
	e0/2	——	接WinServer_DC
	e0/3	——	接WinServer_OA

3. 服务器和客户端基本配置

Win_PC1

- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：administrator/Worldcolleges2022
- 网络地址/掩码/网关：185.6.12.1/24/无

Win_PC2

- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：administrator/Worldcolleges2022
- 网络地址/掩码/网关：172.16.30.2/24/172.16.30.254

Linux_Web

- 全限定域名：web.Worldcolleges.com
- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：root/Worldcolleges2022
- 网络地址/掩码/网关：172.16.20.10/24/172.16.20.254

Win_DNS

- 全限定域名：dns.Worldcolleges.com
- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：administrator/Worldcolleges2022
- 网络地址/掩码/网关：172.16.20.30/24/172.16.20.254

WinServer_DC

- 全限定域名：dc.Worldcolleges.com
- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：administrator/Worldcolleges2022
- 网络地址/掩码/网关：172.16.10.1/24/172.16.10.254

WinServer_OA

- 全限定域名：oa.Worldcolleges.com
- 普通用户/登录密码：skills/Worldcolleges2022
- 超级管理员/登录密码：administrator/Worldcolleges2022
- 网络地址/掩码/网关：172.16.10.2/24/172.16.10.254

第一阶段任务书

任务1：网络系统集成

1. 根据拓扑图和网络地址规划，完成对各网络设备和操作系统的基本配置。
2. 请对ISP进行配置，使Outside区域PC能够访问DMZ区域。
3. 请对FW进行配置，划分Office、DMZ、Inside区域为trust区域，Outside区域为untrust区域，使trust区域之间可以互相访问，untrust区域不能访问trust区域。
4. 在DCFW上配置SNAT功能，使Office区域区域能够访问Outside区域。
5. 请对FW进行配置，使用2.61.243.220为Web做IP映射，并允许Outside、Inside和Office区域用户访问Web服务。
6. 在WinServer_DC上完成域控的安装与部署，并将WinServer_OA和Win_DNS添加到域控中。

7. 在Linux_Web上完成Apache的安装与部署。

8. 在Win_DNS上完成DNS的安装与部署。

9. 在WinServer_OA上完成IIS Web服务器的安装与部署。

任务2：网络系统安全加固

1. 在WinServer_DC上，检查Kerberos策略，将“服务票证最长寿命”时间值设置为342,并应用于域成员。

2. 在WinServer_DC上，检查 “配置Kerberos允许的加密类型”，将加密类型设为aes256_hmac_sha1,并应用于域成员。

3. 在WinServer_DC上，检查密码策略，启用“密码必须符合复杂性要求”将“强制密码历史”值设为18，并应用于域成员。

4. 在WinServer_DC上，检查密码策略，将“密码长度最小值”的值设为12，并应用于域成员。

5. 在WinServer_DC上，检查密码策略，密将“密码最长使用期限”的值设为26，并应用于域成员。

6. 在WinServer_DC上，检查可以从网络访问此计算机的对象，仅保留管理员组，删除其余不必要的对象,并应用于域成员。

7. 在WinServer_DC上，为系统开启SYN洪水保护，设置处于SYN_RCVD状态至少已经进行一次重传的 TCP连接请求阈值为400,并应用于域成员。

8. 在WinServer_DC上，检查“账户锁定阈值”，将阈值设置为10,并应用于域成员。

9. 在 Linux_web上，检查密码策略，将配置的当前密码的有效期限的配置命令转换为md5值。

10. 在 Linux _Web上，设置密码安全策略，将连续输错3次密码，帐号锁定5分钟，root账户锁定10分钟。

11. 在 Linux _Web上，配置SSH 安全策略，将SSH默认端口的修改为5000。

12. 在 Linux _Web上，配置SSH安全策略，仅允许172.16.30.0/24网段的用户进行sshd远程连接。

13. 在Linux_Web上，配置Apache安全策略，禁止网段172.16.10.0/24网段访问。

14. 在Linux_Web上，配置Apache安全策略，将远程连接的超时时间配置为10。

15. 在WinServer_OA上，配置并启用CA证书，并为Win_PC2颁发客户端证书。

分值分布表

表1 第一阶段分值表

序号	描述	分值
A	网络系统集成与安全防护	
A1	网络系统集成	
A2	网络系统安全加固	

信息安全管理与评估　第二阶段

网络安全事件响应

数字取证调查

应用程序安全

（样题）

第二阶段竞赛项目试题（此为样题，仅作试题形式参考）

本文件为信息安全管理与评估项目竞赛-第二阶段试题，第二阶段内容包括：网络安全事件响应、数字取证调查和应用程序安全。

本次比赛时间为180分钟。

介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引！

（1）当竞赛结束，离开时请不要关机；

（2）所有配置应当在重启后有效；

（3）除了CD-ROM/HDD/NET驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

本项目模块分数为30分。

项目和任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络安全防护的重要部分。现在，A集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助A集团追踪此网络攻击来源，分析恶意攻击攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码，帮助其巩固网络安全防线。

本模块主要分为以下几个部分：

- 网络安全事件响应
- 数字取证调查
- 应用程序安全

本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。选手的电脑中已经安装好

Office 软件并提供必要的软件工具 （Tools 工具包）。

工作任务

第一部分 网络安全事件响应

任务1：应急响应

A集团的WebServer服务器被黑客入侵，该服务器的Web应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

本任务素材清单：Server服务器虚拟机。

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

任务 1：应急响应		
序号	**任务内容**	**答案**
1	提交攻击者的两个内网 IP 地址	
2	提交网站管理员用户的用户名与密码	
3	提交黑客得到 mysql 服务的 root 账号密码的时间（格式：dd/MM/yyyy:hh:mm:ss）	
4	查找黑客在 WEB 应用文件中写入的恶意代码，提交文件绝对路径	
5	查找黑客在 WEB 应用文件中写入的恶意代码，提交代码的最简形式（格式：<?php xxxx?>）	
6	分析攻击者的提权手法，提交攻击者通过哪一个指令成功提权	
7	服务器内与动态恶意程序相关的三个文件绝对路径	
8	恶意程序对外连接的目的 ip 地址	

第二部分 数字取证调查

任务2 ：操作系统恶意程序检测

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析A集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：操作系统镜像、内存镜像。

请按要求完成该部分的工作任务。

任务 2：操作系统恶意文件检测		
序号	**任务内容**	**答案**
1	提交恶意进程名称（两个）	
2	被破坏的文件位置	
3	加密数据的内存地址	
4	原文件内容	
5	分析恶意程序行为	

任务3： 网络数据包分析

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

本任务素材清单：捕获的网络数据包文件。

请按要求完成该部分的工作任务。

任务 3： 网络数据包分析		
序号	**任务内容**	**答案**
1	提交恶意程序传输协议（只提交一个协议，两个以上视为无效）	
2	恶意程序对外连接目标 IP	

3	恶意程序加载的 dll 文件名称	
4	解密恶意程序传输内容	
5	分析恶意程序行为	

任务4： 计算机单机取证

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

本任务素材清单：取证镜像文件。

请按要求完成该部分的工作任务。

任务 4： 计算机单机取证		
证据编号	**在取证镜像中的文件名**	**镜像中原文件 Hash 码（MD5，不区分大小写）**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		
evidence 7		
evidence 8		
evidence 9		
evidence 10		

第三部分 应用程序安全

任务5：Android恶意程序分析

A集团发现其发布的Android移动应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：android的apk文件。

请按要求完成该部分的工作任务。

任务 5：Android 恶意程序分析		
序号	**任务内容**	**答案**
1	提交素材中的恶意应用回传数据的 url 地址	
2	提交素材中的恶意代码保存数据文件名称（含路径）	
3	提交素材中的恶意行为发起的 dex 的 SHA1 签名值	
4	描述素材中恶意代码的行为	

任务6：Windows系统恶意程序分析

A集团发现其网络中蔓延了一种恶意程序，现在已采集到恶意程序的样本，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：恶意程序文件。

请按要求完成该部分的工作任务。

任务 6：Windows 系统恶意程序分析		
序号	**任务内容**	**答案**
1	提交恶意程序中的实施系统攻击的函数名	
2	提交恶意程序攻击的系统文件名	
3	提交恶意程序的解密秘钥	
4	描述素材中恶意代码的行为	

分值分配表：

表2 第二阶段分值表

序号	描述	分值
B	网络安全事件响应、数字取证调查、应用程序安全	
B1	应急响应	
B2	操作系统恶意程序检测	
B3	网络数据包分析	
B4	计算机单机取证	
B5	Android 恶意程序分析	
B6	Windows 系统恶意程序分析	

信息安全管理与评估 第三阶段

网络安全渗透（夺旗挑战CTF）

（样题）

第三阶段竞赛项目试题（此为样题，仅作试题形式参考）

根据信息安全管理与评估技术文件要求，第三阶段为网络安全渗透（夺旗挑战CTF）。本文件为信息安全管理与评估竞赛-第三阶段试题。

本次比赛时间为180分钟。

介绍

夺旗挑战CTF（网络安全渗透）的目标是作为一名网络安全专业人员在一个模拟的网络环境中实现网络安全渗透测试工作。

本模块要求参赛者作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试；并且能够通过各种信息安全相关技术分析获取存在的Flag值。

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

本测试项目模块分数为30分。

项目和任务描述

在A集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用你所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取flag值。网络环境参考样例请查看附录A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

- 信息收集
- 逆向文件分析
- 二进制漏洞利用
- 应用服务漏洞利用
- 操作系统漏洞利用
- 杂项与密码学分析
- 系统文件分析

所有设备和服务器的IP地址请查看现场提供的设备列表。

特别提醒

通过找到正确的flag值来获取得分，它的格式如下所示：

flag{<flag值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏感信息并利用工具把它找出来。

工作任务

一、门户网站

一、门户网站			
任务编号	**任务描述**	**答案**	**分值**
任务一	企业门户网站存在隐藏信息，请找出隐藏信息，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务二	企业门户网站存在漏洞，请渗透该系统并找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务三	请获取根目录下的数据包文件进行分析，并将 flag 提交。flag 格式 flag{<flag 值>}		

二、FTP服务器

二、FTP 服务器			
任务编号	**任务描述**	**答案**	**分值**
任务四	FTP 服务器存在漏洞， 找到 FTP 服务器中的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务五	请获取 FTP 服务器中的数据包文件，分析并将 flag 提交。flag 格式 flag{<flag 值>}		
任务六	请获取 FTP 服务器中的附件，分析其中加密信息，将内容解密并将 flag 提交。flag 格式 flag{<flag 值>}		

任务七	请获取 FTP 服务器中的恶意文件，分析并将 flag 提交。flag 格式 flag{<flag 值>}		

三、企业邮件服务器

三、企业邮件服务器			
任务编号	**任务描述**	**答案**	**分值**
任务八	企业邮件服务器存在漏洞，请渗透该系统，并将系统后台存放的 flag 提交。flag 格式 flag{<flag 值>}		
任务九	请查看企业邮件服务器中的邮件，分析附件中的恶意文件，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务十	请查看企业邮件服务器中的邮件，分析邮件中的加密内容，解密后将 flag 提交。flag 格式 flag{<flag 值>}		

四、协同办公服务器

四、协同办公服务器			
任务编号	**任务描述**	**答案**	**分值**
任务十一	渗透该备份服务器，找到根目录下的 flag 文件，将内容作为 flag 提交。flag 格式 flag{<flag 值>}		
任务十二	获取 root 用户的密码明文，将明文作为 flag 提交。flag 格式 flag{<flag 值>}		

五、单点登录服务器

五、单点登录服务器			
任务编号	**任务描述**	**答案**	**分值**
任务十三	单点登录服务器中存在隐藏信息，请找出隐藏信息并将提交 flag。flag 格式 flag{<flag 值>}		

任务十四	单点登录服务器存在漏洞，请渗透该服务器，并将数据库中的 flag 提交。flag 格式 flag{<flag 值>}		
任务十五	单点登录服务器后台存在漏洞，请渗透该服务器，并将根目录下的 flag 文件内容作为 flag 提交。flag 格式 flag{<flag 值>}		

六、应用程序服务器

六、应用程序服务器			
任务编号	**任务描述**	**答案**	**分值**
任务十六	应用程序服务器 5555 端口运行应用存在漏洞，分析并提交 flag。flag 格式 flag{<flag 值>}		
任务十七	应用程序服务器 6666 端口运行应用存在漏洞，分析并提交 flag。flag 格式 flag{<flag 值>}		

分值分布表

表3 第三阶段分值分布

序号	描述	分值
C	夺旗挑战 CTF（网络安全渗透）	
C1	门户网站	
C2	FTP 服务器	
C3	企业邮件服务器	
C4	协同办公服务器	
C5	单点登录服务器	
C6	应用程序服务器	

附录A

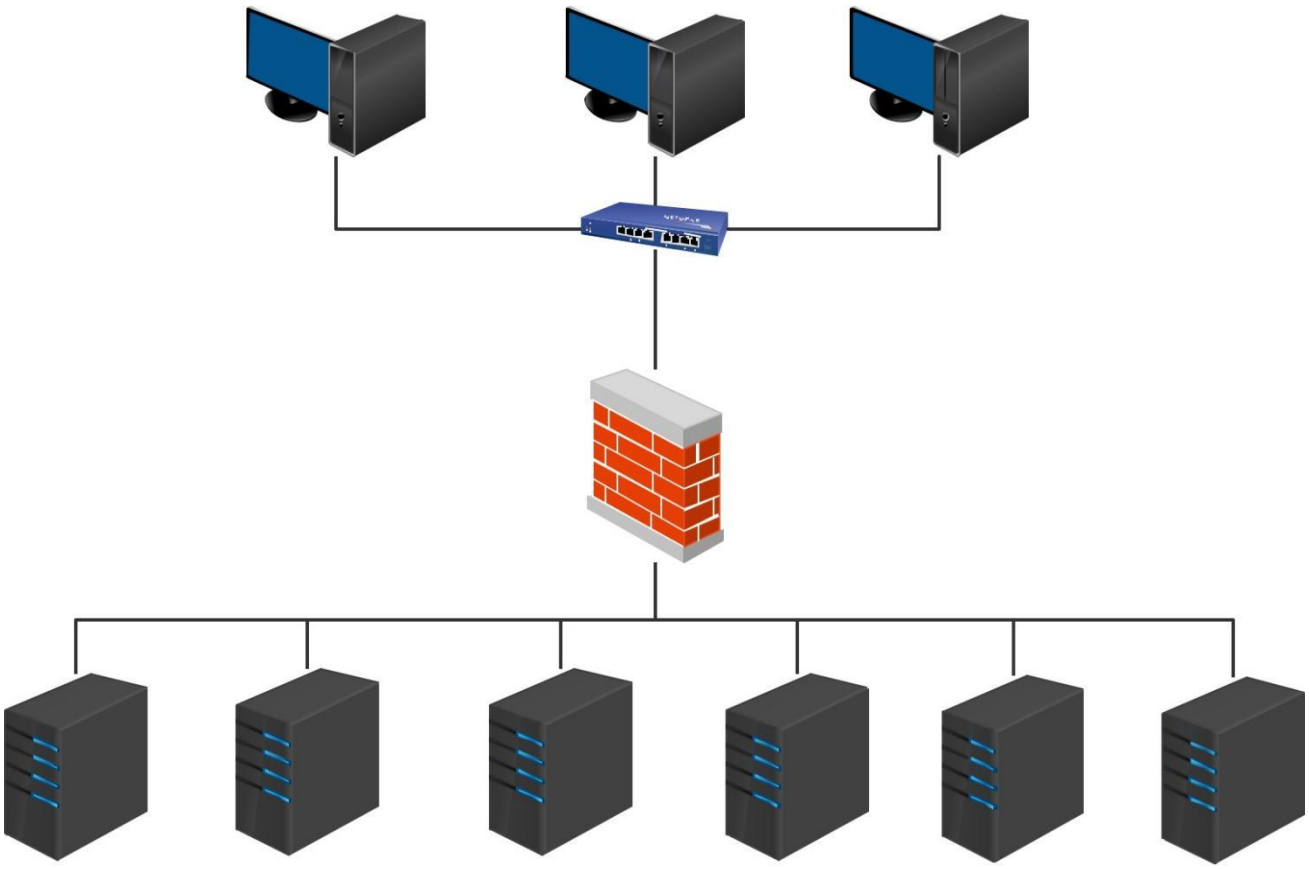


图1 网络拓扑结构图