**全国职业院校技能大赛**

高等职业教育组

**信息安全管理与评估**

**任务书**

**模块三**

网络安全渗透、理论技能与职业素养

# 比赛时间及注意事项

本阶段比赛时长为180分钟，时间为9:00-12:00。

【注意事项】

（1）通过找到正确的flag值来获取得分，flag统一格式如下所示：

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。

**注：**部分flag可能非统一格式，若存在此情况将会在题目描述中明确指出flag格式，请注意审题。

（2）选手首先需要在U盘的根目录下建立一个名为“BGWxx”的文件夹（xx用具体的工位号替代），请将赛题第三阶段所完成的“信息安全管理与评估竞赛答题卡-模块三”答题文档，放置在“BGWxx”文件夹中。

例如：08工位，则需要在U盘根目录下建立“BGW08”文件夹，请将第三阶段所完成的“信息安全管理与评估竞赛答题卡-模块三”答题文档，放置在“BGW08”文件夹中。

# 竞赛项目赛题

本文件为信息安全管理与评估项目竞赛-第三阶段赛题，内容包括：网络安全渗透和理论技能与职业素养，其中理论技能与职业素养部分在平台在线答题。

# 介绍

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。

# 所需软硬件设备和材料

所有测试项目都可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

本测试项目模块网络安全渗透为300分,理论技能与职业素养100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：

* 数据库攻击
* 枚举攻击
* 权限提升攻击
* 基于应用系统的攻击
* 基于操作系统的攻击
* 逆向分析
* 密码学分析
* 隐写分析

所有设备和服务器的IP地址请查看现场提供的设备列表。

# 工作任务

## 人力资源管理系统（45分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务一 | 请对门户网站进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  | 15 |
| 任务二 | 请对门户网站进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  | 15 |
| 任务三 | 请对门户网站进行黑盒测试，利用漏洞找到flag3，并将flag3提交。flag3格式flag3{<flag值>} |  | 15 |

## 邮件系统（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务四 | 请对办公系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  | 15 |
| 任务五 | 请对办公系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  | 15 |

## FTP服务器（165分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务六 | 请获取FTP服务器上task6目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 15 |
| 任务七 | 请获取FTP服务器上task7目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 15 |
| 任务八 | 请获取FTP服务器上task8目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 20 |
| 任务九 | 请获取FTP服务器上task9目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 25 |
| 任务十 | 请获取FTP服务器上task10目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 20 |
| 任务十一 | 请获取FTP服务器上task11目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 25 |
| 任务十二 | 请获取FTP服务器上task12目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 20 |
| 任务十三 | 请获取FTP服务器上task13目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  | 25 |

## 应用系统服务器（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务十四 | 应用系统服务器10000端口存在漏洞，获取FTP服务器上task14目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  | 30 |

## 运维服务器（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务十五 | 运维服务器10001端口存在漏洞，获取FTP服务器上task15目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  | 30 |

## 附录A



图1 网络拓扑结构图