**2025年河北省职业院校学生技能大赛**

**“网络空间安全技能大赛”赛项样题A**

**模块一：CTF夺旗（竞赛时间 120 分钟，共 100 分）**

**(一) 项目描述**

CTF夺旗阶段考核内容领域涉及Web安全、密码学、逆向工程、PWN、安全杂项共五个方向，主要考察参赛选手对各个专业知识领域的深入理解。每个方向的题目各2道共10个题目。

**(二) 任务书**

请根据赛题要求及现场答题卡任务要求提交正确答案，题目包含访问远程服务器中web等服务的题目，也包含下载附件在本地计算机中使用工具进行分析的题目，需要从各题目中寻找预先放置的正确flag值，然后提交平台进行得分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 类型 | 题目名称 | 题目描述 | 分值 |
| 1 | Web安全 | babyweb | 查看网络请求，看看有什么不一样的地方。 | 12 |
| 2 | Web安全 | 忘记密码 | 阿拉丁忘记了自己的登录密码，你能帮他找回吗？ | 15 |
| 3 | 密码学 | RC4 | 小明使用了流密码对他的关键信息进行了加密，你能够从中解密呢？ | 7 |
| 4 | 密码学 | 仿射密码 | 使用仿射函数y=3x+9加密得到的密文为JYYHWVPIDCOZ，请尝试对其解密。flag为flag{大写明文}。 | 5 |
| 5 | 逆向工程 | haha | haha.exe目前无法直接运行，找到启动haha.exe的方法。flag{}. | 10 |
| 6 | 逆向工程 | explorer\_dmp | explorer.exe进程已经被木马感染了，现已经获取explorer.exe进程的dump文件，尝试从DUMP文件中找到flag，flag{}. | 11 |
| 7 | 安全杂项 | 奇怪的图片 | 给了个压缩包，你能找到正确的flag吗。 | 9 |
| 8 | 安全杂项 | 我不玩了 | 需要从流量中寻找可疑的内容，答案或许就隐藏在其中，flag格式flag{}。 | 11 |
| 9 | PWN | pwn-1 | 下载附件并分析，找到其中的漏洞并编写漏洞利用脚本，使用nc ip port访问题目。 | 10 |
| 10 | PWN | pwn-2 | 下载附件并分析，找到其中的漏洞并编写漏洞利用脚本，使用nc ip port访问题目。 | 10 |
| 合计 | | | | 100 |

**模块二：渗透测试（竞赛时间 120 分钟，共 100 分）**

**(一) 项目描述**

在一个模拟的网络环境中实现网络安全渗透测试工作，要求参赛选手作为攻击方，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。

渗透测试阶段，参赛选手可以利用一系列网络安全攻击渗透工具对所提供的网络安全攻击靶场环境进行综合分析、挖掘和渗透。

**(二) 任务书**

A公司有一个新研发的web服务要上线，需要您的团队对已经部署了这个web服务的服务器整体进行渗透测试，发现其中可能存在的问题，A公司为了验证您的工作成功，已经在服务器中的不同位置放置了不同的字符串作为发现问题的判断依据，现在请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这台主机的渗透测试。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。

本任务素材清单：Kali操作机和待渗透的linux服务器

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务编号** | 任务要求 | **分值** |
| **任务** **1** | 网站cookie返回了不应该返回的内容，请利用技术手段并找到 flag，并将 flag 提交。  flag 格式 flag{flag 值} | 10 |
| **任务** **2** | 网站功能存在文件包含漏洞，请利用漏洞读取网站的源代码，，并将index.php文件中的 flag 提交。  flag 格式 flag{flag 值} | 15 |
| **任务** **3** | 服务器的数据库配置有问题，请利用技术手段读取数据库中Users数据库，并读取fl4g表中的内容，将其中的flag提交。  flag 格式 flag{flag 值} | 20 |
| **任务** **4** | 服务器中存在低权限的用户，使用技术方法得到低权限用户的shell，在某个用户的home中存在一个文件，读取其中的flag并提交。  flag 格式 flag{flag 值} | 25 |
| **任务** **5** | 在服务器的root目录中存在一个隐藏文件，使用提权技术获取root的权限，然后读取这个隐藏文件的内容，并将其中的flag内容提交。  flag 格式 flag{flag 值} | 30 |

### 注意事项

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。

**模块三：攻防对抗（竞赛时间 120 分钟，最终折算为百分制）**

**(一) 项目描述**

攻防对抗阶段考察选手在安全攻击与安全防守方面的技能。要求选手在比赛开始后对各自的靶机进行安全加固，各战队也可对其他战队靶机开展自由攻击并获取对应分值。

需要针对预设的环境进行黑盒及白盒渗透测试，包含的知识有SQL 注入、文件上传、命令执行、缓冲区溢出、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、密码学分析等。

计分规则

（1）动态flag时间设置

平台设定每轮为15分钟，一共8轮，每次获取到的flag有效时间为30秒，过期后需重新获取，每支队伍每道题目的flag在15分钟内仅计算一次得分。请各队伍注意，在规定时间内重复提交相同题目的flag将不会获得额外分数。

（2）计分模式

分数不设上限，每个队伍拿到flag并提交成功即可获得10分，被攻击成功则会丢10分，服务判down视情况扣分。

（3）服务状态检测

比赛过程中每轮都要检测所有选手服务的状态，防止选手暴力删除服务，恶意修改程序逻辑。

（4）恶意行为检测

平台会检测恶意对他方服务器进行破坏的行为，如删除他方服务器文件，使用通防程序等行为，发现后会公示并扣除50分进行处罚。

**(二) 任务书**

攻击成功后，执行命令"curl -k https://平台地址/Getkey/index/index"获取flag，并提交flag到平台得分，每次获取flag后有提交时间限制，请尽快提交

|  |  |  |
| --- | --- | --- |
| 序号 | 题目名称 | 题目描述 |
| 1 | Web题目一 | ssh端口：22，使用用户名/密码：ctf/3EifHk8l，登录服务器进行维护，服务端口：80。 |
| 2 | Web题目二 | ssh端口：22，使用用户名/密码：ctf/kld8ghhs，登录服务器进行维护，服务端口：80。 |
| 3 | 二进制题目 | ssh端口：22，使用用户名/密码：ctf/5kskhHls，登录服务器进行维护，服务端口：9999。 |

**注：百分制换算**

假设本次攻防对抗赛最高分6665，某队伍得分5000，最终成绩计算公式如下：5000/6665\*100=75.01分。

**2024年河北省职业院校学生技能大赛**

**“网络空间安全技能大赛”赛项样题B**

**模块一：CTF夺旗（竞赛时间 120 分钟，共 100 分）**

**(一) 项目描述**

CTF夺旗阶段考核内容领域涉及Web安全、密码学、逆向工程、PWN、安全杂项共五个方向，主要考察参赛选手对各个专业知识领域的深入理解。每个方向的题目各2道共10个题目。

**(二) 任务书**

请根据赛题要求及现场答题卡任务要求提交正确答案，题目包含访问远程服务器中web等服务的题目，也包含下载附件在本地计算机中使用工具进行分析的题目，需要从各题目中寻找预先放置的正确flag值，然后提交平台进行得分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 类型 | 题目名称 | 题目描述 |  |
| 1 | Web安全 | 科学计数 | 咦?少于4位数的数字会大于999?欺负我书读的少咯? | 12 |
| 2 | Web安全 | missing\_php | 小明用vim编辑php代码，可是电脑突然关机了，你能帮他找回php代码么？ | 15 |
| 3 | 密码学 | 轮环异或加密 | 轮环异或加密，你能解开么？格式：flag{} | 7 |
| 4 | 密码学 | RSA300 | 这里e1=2333，e2=23333，flag格式flag{xxx} | 5 |
| 5 | 逆向工程 | 业务风险 | app中各种应用和业务存在安全风险,通过分析app，发现存在漏洞的点，通过漏洞找出可以攻击的切口进行攻击，并获取到由于漏洞而泄漏的密钥,找出存在的漏洞,通过漏洞获取存在的Flag信息. | 10 |
| 6 | 逆向工程 | 异常版本 | 云端系统发现一款app的版本号有异常行为，通过分析app，发现版本号产生的相关信息,通过分析app逻辑，根据版本信息获取正确的Flag字串，flag{}. | 11 |
| 7 | 安全杂项 | misc-1 | 斑马斑马 你不要睡着啦,再给我看看你受伤的尾巴…flag格式flag{xxxx} | 9 |
| 8 | 安全杂项 | misc-2 | 你爆破的开么？flag格式flag{xxxx} | 11 |
| 9 | PWN | pwn-3 | 下载附件并分析，找到其中的漏洞并编写漏洞利用脚本，使用nc ip port访问题目。 | 10 |
| 10 | PWN | pwn-4 | 下载附件并分析，找到其中的漏洞并编写漏洞利用脚本，使用nc ip port访问题目。 | 10 |
| 合计 | | | | 100 |

**模块二：渗透测试（竞赛时间 120 分钟，共 100 分）**

**(一) 项目描述**

在一个模拟的网络环境中实现网络安全渗透测试工作，要求参赛选手作为攻击方，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。

渗透测试阶段，参赛选手可以利用一系列网络安全攻击渗透工具对所提供的网络安全攻击靶场环境进行综合分析、挖掘和渗透。

**(二) 任务书**

A公司有一个新研发的web服务要上线，需要您的团队对已经部署了这个web服务的服务器整体进行渗透测试，发现其中可能存在的问题，A公司为了验证您的工作成功，已经在服务器中的不同位置放置了不同的字符串作为发现问题的判断依据，现在请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这台主机的渗透测试。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。

本任务素材清单：Kali操作机和待渗透的linux服务器

请根据赛题环境及任务要求提交正确答案。

|  |  |  |
| --- | --- | --- |
| **任务编号** | 任务要求 | **分值** |
| **任务** **1** | 服务器中除了web服务，还存在一个其他的服务，而且这个服务好像没有验证权限，请登录上这个服务找到其中放置的flag。  flag 格式 flag{flag 值} | 10 |
| **任务** **2** | Web服务存在管理员后台，请找到管理员后台的地址，并利用技术手段登录到网站后台，找到存放在后台的flag并提交。  flag 格式 flag{flag 值} | 15 |
| **任务** **3** | 服务器中的web目录中放置一个flag，请获取webshell并读取web目录中的flag文件内容进行提交。  flag 格式 flag{flag 值} | 20 |
| **任务** **4** | 服务器中存在除root用户外的有权限登录ssh的用户，请使用此用户登录服务器，找到这个用户家目录中的flag进行提交。  flag 格式 flag{flag 值} | 25 |
| **任务** **5** | 在root目录中存在了一个flag，请读取这个flag文件并提交。  flag 格式 flag{flag 值} | 30 |

**注意事项**

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。

**模块三：攻防对抗（竞赛时间 120 分钟，最终折算为百分制）**

**(一) 项目描述**

攻防对抗阶段考察选手在安全攻击与安全防守方面的技能。要求选手在比赛开始后对各自的靶机进行安全加固，各战队也可对其他战队靶机开展自由攻击并获取对应分值。

需要针对预设的环境进行黑盒及白盒渗透测试，包含的知识有SQL 注入、文件上传、命令执行、缓冲区溢出、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、密码学分析等。

计分规则

（1）动态flag时间设置

平台设定每轮为15分钟，一共8轮，每次获取到的flag有效时间为30秒，过期后需重新获取，每支队伍每道题目的flag在15分钟内仅计算一次得分。请各队伍注意，在规定时间内重复提交相同题目的flag将不会获得额外分数。

（2）计分模式

分数不设上限，每个队伍拿到flag并提交成功即可获得10分，被攻击成功则会丢10分，服务判down视情况扣分。

（3）服务状态检测

比赛过程中每轮都要检测所有选手服务的状态，防止选手暴力删除服务，恶意修改程序逻辑。

（4）恶意行为检测

平台会检测恶意对他方服务器进行破坏的行为，如删除他方服务器文件，使用通防程序等行为，发现后会公示并扣除50分进行处罚。

**(二) 任务书**

攻击成功后，执行命令"curl -k https://平台地址/Getkey/index/index"获取flag，并提交flag到平台得分，每次获取flag后有提交时间限制，请尽快提交

|  |  |  |
| --- | --- | --- |
| 序号 | 题目名称 | 题目描述 |
| 1 | Web题目一 | ssh端口：22，使用用户名/密码：ctf/9581d026，登录服务器进行维护，服务端口：80。 |
| 2 | Web题目二 | ssh端口：22，使用用户名/密码：ctf/f89af3a6，登录服务器进行维护，服务端口：80。 |
| 3 | 二进制题目 | ssh端口：22，使用用户名/密码：ctf/e8ce7724，登录服务器进行维护，服务端口：9999。 |

**注：百分制换算**

假设本次攻防对抗赛最高分6665，某队伍得分5000，最终成绩计算公式如下：5000/6665\*100=75.01分。