**2019年全国职业院校技能大赛中职组**

**“网络空间安全”正式赛卷**

**一、竞赛阶段**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| 第一阶段单兵模式系统渗透测试 | 任务1 | Wireshark数据包分析 | 100分钟 | 100 |
| 任务2 | 文件上传渗透测试 | 100 |
| 任务3 | Web渗透测试 | 100 |
| 任务4 | Windows操作系统渗透测试 | 100 |
| 任务5 | Linux操作系统渗透测试 | 100 |
| 任务6 | 网络协议栈渗透测试 | 100 |
| 任务7 | 系统综合渗透测试及安全加固 | 100 |
| 备战阶段 | 攻防对抗准备工作 | 20分钟 | 0 |
| 第二阶段分组对抗 | 系统加固：15分钟 | 60分钟 | 300 |
| 渗透测试：45分钟 |

**二、拓扑图**



PC机环境：

物理机：Windows7；

虚拟机1：Ubuntu Linux 32bit（用户名：root；密码：toor）,安装工具集：Backtrack5,安装开发环境：Python3；

虚拟机2：Kali1.0（用户名：root；密码：toor）；

虚拟机3：Kali2.0（用户名：root；密码：toor）；

虚拟机4：WindowsXP（用户名：administrator；密码：123456）。

**三、竞赛任务书**

**（一）第一阶段任务书**（700分）

任务1. Wireshark数据包分析（100分）

**任务环境说明：**

* 服务器场景：PYsystem20191
* 服务器场景操作系统：Windows（版本不详）

1.使用Wireshark查看并分析PYsystem20191桌面下的capture4.pcap数据包文件，找出黑客获取到的可成功登录目标服务器FTP的账号密码，并将黑客获取到的账号密码作为Flag值（用户名与密码之间以英文逗号分隔，例如：root,toor）提交；（9分）

2.继续分析数据包capture4.pcap，找出黑客使用获取到的账号密码登录FTP的时间，并将黑客登录FTP的时间作为Flag值（例如：14:22:08）提交；（13分）

3.继续分析数据包capture4.pcap，找出黑客连接FTP服务器时获取到的FTP服务版本号，并将获取到的FTP服务版本号作为Flag值提交；（15分）

4.继续分析数据包capture4.pcap，找出黑客成功登录FTP服务器后执行的第一条命令，并将执行的命令作为Flag值提交;（11分）

5.继续分析数据包capture4.pcap，找出黑客成功登录FTP服务器后下载的关键文件，并将下载的文件名称作为Flag值提交；（13分）

6.继续分析数据包capture4.pcap，找出黑客暴力破解目标服务器Telnet服务并成功获取到的用户名与密码，并将获取到的用户名与密码作为Flag值（用户名与密码之间以英文逗号分隔，例如：root,toor）提交；（9分）

7.继续分析数据包capture4.pcap，找出黑客在服务器网站根目录下添加的文件，并将该文件的文件名称作为Flag值提交；（13分）

8.继续分析数据包capture4.pcap，找出黑客在服务器系统中添加的用户，并将添加的用户名与密码作为Flag值（用户名与密码之间以英文逗号分隔，例如：root,toor）提交。（17分）

任务2. 文件上传渗透测试（100分）

**任务环境说明：**

* 服务器场景：PYsystem20191
* 服务器场景操作系统：Windows（版本不详）

1.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20191进行网站目录暴力枚举测试（使用工具DirBuster，扫描服务器80端口），选择使用字典（使用默认字典directory-list-2.3-medium.txt）方式破解，并设置模糊测试的变量为“{dir}”，将回显信息中从上往下数第六行的数字作为Flag值提交；（11分）

2.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20191进行网站目录暴力枚举测试（使用工具DirBuster，扫描服务器80端口），通过分析扫描结果，找到上传点并使用火狐浏览器访问包含上传点的页面，并将访问成功后的页面第一行的第一个单词作为Flag值提交；（13分）

3.访问成功后上传名为backdoor.php的php一句话木马至服务器，打开控制台使用网站安全狗检测本地是否存在木马，若检测出存在木马，则将木马所在的绝对路径作为Flag值提交，若未检测出木马则提交false；（15分）

4.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20191进行文件上传渗透测试，使用工具weevely在/目录下生成一个木马，木马名称为backdoor.php，密码为pass，该操作使用命令中固定不变的字符串作为Flag值提交；（17分）

5.上传使用weevely生成的木马backdoor1.php至服务器中，打开控制台使用网站安全狗检测本地是否存在木马，若检测出存在木马，则将木马所在的绝对路径作为Flag值提交，若未检测出木马则提交false；（11分）

6.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20191进行文件上传渗透测试（使用工具weevely，连接目标服务器上的木马文件），连接成功后将目标服务器主机名的字符串作为Flag值提交；（11分）

7.开启网站安全狗的所有防护，再次使用weevely生成一个新的木马文件并将其上传至目标服务器，将上传后页面提示的第二行内容作为Flag值提交；（13分）

8.开启网站安全狗的所有防护，再次使用weevely生成木马文件并将其上传至目标服务器，要求能够上传成功，将生成该木马必须要使用的参数作为Flag值提交。（9分）

任务3. Web渗透测试（100分）

**任务环境说明：**

* 服务器场景：PYsystem20192（用户名：root；密码：123456）
* 服务器场景操作系统：PYsystem20192（版本不详）

1.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行Web渗透测试（使用工具w3af的对目标Web服务器进行审计），在w3af的命令行界面下，使用命令列出所有用于审计的插件，将该操作使用的命令作为Flag值提交；（9分）

2.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行Web渗透测试，使用工具w3af对Web服务器进行审计，在w3af的命令行界面下加载爬行模块来搜集phpinfo信息及蜘蛛爬行数据，将该操作使用的命令作为Flag值提交；（11分）

3.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行Web渗透测试，使用工具w3af对Web服务器进行审计，在w3af的命令行界面下启用审计插件sql盲注、命令注入及sql注入来测试服务器网站安全性，并将该操作使用的命令作为Flag值提交；（13分）

4.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行Web渗透测试，使用工具w3af对Web服务器进行审计，在w3af的命令行界面下设置目标服务器地址启动扫描，将该操作使用命令中固定不变的字符串作为Flag值提交；（11分）

5.在本地PC渗透测试平台Kali1.0中对审计结果进行查看，将审计结果中含有漏洞的URL地址作为Flag值（提交答案时IP用192.168.80.1代替，例如http://192.168.80.1/login.php）提交；（17分）

6.在第5题的基础上，进入exploit模式，加载sqlmap模块对网站进行SQL注入测试，将载入sqlmap模块对网站进行SQL注入测试需要使用的命令作为Flag值提交；（9分）

7.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行SQL注入测试，将数据库最后一个库的库名作为Flag值提交； （19分）

8.通过本地PC中渗透测试平台Kali1.0对服务器场景PYsystem20192进行SQL注入测试，将数据库的root用户密码作为Flag值提交。 （11分）

任务4. Windows操作系统渗透测试（100分）

**任务环境说明：**

* 服务器场景：PYsystem20194
* 服务器场景操作系统：Windows（版本不详）

1.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行系统服务及版本扫描渗透测试，并将该操作显示结果中445端口对应的服务版本信息字符串作为Flag值提交；（7分）

2.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景网络连接信息中的DNS信息作为Flag值 (例如：114.114.114.114) 提交；（9分）

3.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文件名称作为Flag值提交；（11分）

4.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文档内容作为Flag值提交；（15分）

5.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景桌面上222文件夹中唯一一个图片中的英文单词作为Flag值提交；（17分）

6.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景中的当前最高账户管理员的密码作为Flag值提交；（20分）

7.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20194进行渗透测试，将该场景中回收站内文件的文档内容作为Flag值提交。（21分）

任务5. Linux操作系统渗透测试（100分）

**任务环境说明：**

* 服务器场景：PYsystem20195
* 服务器场景操作系统：Linux（版本不详）

1.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行系统服务及版本扫描渗透测试，并将该操作显示结果中21端口对应的服务版本信息字符串作为Flag值提交；（5分）

2.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/home/guest目录中唯一一个后缀为.pdf文件的文件名称作为Flag值提交；（7分）

3.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/home/guest目录中唯一一个后缀为.pdf文件的文件内容作为Flag值提交；（9分）

4.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/var/www目录中唯一一个后缀为.bmp文件的文件名称作为Flag值提交；（7分）

5.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/var/www目录中唯一一个后缀为.bmp的图片文件中的英文单词作为Flag值提交；（9分）

6.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/var/vsftpd目录中唯一一个后缀为.docx文件的文件名称作为Flag值提交；（8分）

7.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/var/vsftpd目录中唯一一个后缀为.docx文件的文件内容作为Flag值提交；（11分）

8.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/root目录中唯一一个后缀为.txt文件的文件名称作为Flag值提交；（21分）

9.通过本地PC中渗透测试平台Kali2.0对服务器场景PYsystem20195进行渗透测试，将该场景/root目录中唯一一个后缀为.txt文件的文件内容作为Flag值提交。（23分）

任务6. 网络协议栈渗透测试（100分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

* 物理机操作系统：Windows7
* 虚拟机操作系统：Ubuntu Linux 32bit
* 虚拟机操作系统安装工具1：Python3
* 虚拟机操作系统安装工具2：Wireshark
* 虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）
* 用户名：root，密码：123456

靶机：

* 服务器场景：PYsystem20196
* 服务器场景操作系统：Microsoft Windows2003 Server
* 服务器场景FTP下载服务用户名：anonymous，密码：123456
* 服务器场景FTP下载服务端口：2121

1.从靶机服务器场景FTP服务器中下载文件smurf.py，编辑该Python程序文件，使该程序实现通过UDP对靶机服务器场景进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F1字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

2.继续编辑命名为smurf.py的Python程序文件，使该程序实现通过UDP对靶机服务器场景进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F2字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

3.继续编辑命名为smurf.py的Python程序文件，使该程序实现通过UDP对靶机服务器场景进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F3字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（9分）

4.继续编辑命名为smurf.py的Python程序文件，使该程序实现通过UDP对靶机服务器场景进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F4字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（9分）

5.通过Python解释器执行smurf.py，并打开Wireshark监听网络流量，分析通过程序文件smurf.py产生的ICMP流量，并将该ICMP数据对象中的Code属性值通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（11分）

6.继续从靶机服务器场景FTP服务器中下载文件scansion.py，编辑该Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F1字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

7.继续编辑命名为scansion.py的Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F2字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

8.继续编辑命名为scansion.py的Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F3字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

9.继续编辑命名为scansion.py的Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F4字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

10.继续编辑命名为scansion.py的Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F5字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（9分）

11.继续编辑命名为scansion.py的Python程序文件，使该程序实现对靶机服务器场景进行扫描渗透测试的功能，填写该文件当中空缺的F6字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（9分）

12.通过Python解释器执行程序文件scansion.py，将该程序文件执行后的显示结果中，找到关键字Word1和关键字Word2对应的字符串填入以下形式（Word1对应的字符串: Word2对应的字符串），并将该形式字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交。（11分）

任务7. 系统综合渗透测试及安全加固（100分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

* 物理机操作系统：Windows7
* 虚拟机操作系统：Ubuntu Linux 32bit
* 虚拟机操作系统安装工具1：Python3
* 虚拟机操作系统安装工具2：Wireshark
* 虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）
* 用户名：root，密码：123456

靶机：

* 服务器场景：PYsystem20197
* 服务器场景操作系统：Microsoft WindowsXP

1.在攻击机端通过渗透测试方法登录靶机服务器场景，将成功登录后，操作系统桌面显示的字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

2.从靶机服务器场景编辑文件C:\Appserv\www\WebSeep.php，编辑该PHP程序文件，使该程序实现能够同时实现对SQL注入渗透测试和XSS渗透测试的安全防护，填写该文件当中空缺的F1字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

3.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够同时实现对SQL注入渗透测试和XSS渗透测试的安全防护，填写该文件当中空缺的F2字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

4.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够同时实现对SQL注入渗透测试和XSS渗透测试的安全防护，填写该文件当中空缺的F3字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

5.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够同时实现对SQL注入渗透测试和XSS渗透测试的安全防护，填写该文件当中空缺的F4字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（9分）

6.从靶机服务器场景中找到文件C:\PenetrationTest\PenetrationTest.c，编辑该C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F1字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

7.继续编辑本任务第6题中的C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F2字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

8.继续编辑本任务第6题中的C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F3字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

9.继续编辑本任务第6题中的C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F4字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

10.继续编辑本任务第6题中的C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F5字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

11.继续编辑本任务第6题中的C程序源文件，使该程序实现对靶机服务器场景是否存在缓冲区溢出漏洞进行安全测试，填写该文件当中空缺的F6字符串，将该字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（7分）

12.使用靶机服务器场景中的Microsoft Visual C++编译器对以上6-11小题中编辑的PenetrationTest.c源文件进行编译、链接，使程序运行转入执行操作系统Shell程序，将操作系统弹出的Shell系统提示符字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交；（10分）

13.对以上靶机服务器场景出现的缓冲区溢出漏洞进行安全加固，找到解决该问题需要修改的操作系统配置文件，将完整的配置文件的文件名字符串通过SHA256运算后返回哈希值的十六进制结果作为Flag值（形式：十六进制字符串）提交。（11分）

**（二）第二阶段任务书（300分）**

假定各位选手是某电子商务企业的信息安全工程师，负责企业某些服务器的安全防护，该服务器可能存在着各种问题和漏洞。你需要尽快对该服务器进行安全加固，15分钟之后将会有其它参赛队选手对这些服务器进行渗透。

根据《赛场参数表》提供的第二阶段的信息，请使用PC的谷歌浏览器登录实战平台。

**靶机服务器环境说明：**

场景1：CentOS2019024（无法打开控制台操作该靶机，只能获取到该靶机的IP，选手需要通过其他方法进入靶机才能进行加固），服务器操作系统：CentOS（版本不详）；

场景2：Windows2019024（无法打开控制台操作该靶机，只能获取到该靶机的IP，选手需要通过其他方法进入靶机才能进行加固），服务器场景操作系统：Windows（版本不详）。

**注意事项：**

1.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

2.Flag值为每台靶机服务器的唯一性标识，每台靶机服务器仅有1个；

3.靶机服务器的Flag值存放在/root/flagvalue.txt文件或C:\flagvalue.txt文件中；

4.在登录自动评分系统后，提交对手靶机服务器的Flag值，同时需要指定对手靶机服务器的IP地址；

5. CentOS2019024靶机服务器如下服务及端口不允许关闭：80、3306、7000-8000双向、8080；Windows2019024靶机服务器如下服务及端口不允许关闭：21、80、7000-8000双向；

6.系统加固时需要保证靶机对外提供服务的可用性，服务只能更改配置，不允许更改内容；

7.本环节是对抗环节，不予补时。

**可能的漏洞列表如下：**

1.服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.靶机服务器上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

3.靶机服务器上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

4.靶机服务器上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

5.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

6.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

7.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

**评分说明：**

规则1：每提交1次对手靶机服务器的Flag值增加2分，每当被对手提交1次自身靶机服务器的Flag值扣除2分，每个对手靶机服务器的Flag值只能提交一次；

规则2：系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分，每检测到一次违规行为扣除一次分数，扣分明细显示在违规记录中，计算在第二阶段总成绩中：

1）攻防阶段启用Flag检测机制，如发现Flag异常（譬如：删除、修改、移动、杀进程），记为一次违规行为，每次扣分3分；

2）攻防阶段启用服务端口检测机制，如发现关闭题目要求开启的端口，记为一次违规行为，每端口每次扣分1分；

3）攻防阶段靶机服务器IP地址为DHCP自动获取，不允许修改，如修改触发上述所有检测机制；

4）在加固时间后，选手自己关闭靶机服务器或被他人关闭，触发上述所有检测机制，且裁判员不予帮助重启。

规则3：第二阶段总分为300分，初始分为100分。在实际得分和大屏显示中，某选手得分可能会显示负分或者超过300分；凡是负分的，本阶段评判成绩一律为0分；凡是超过300分的，本阶段评判成绩一律为300分；0-300分的评判成绩保持不变。

# 四、答案

|  |  |  |  |
| --- | --- | --- | --- |
| **任务类型** | **任务名称** | **答案** | **分值** |
| 单兵闯关 | 任务1.Wireshark数据包分析 | admin,admin654321 | 9 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | 01:33:08 | 13 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | 3.0.2 | 15 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | dir | 11 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | flag123 | 13 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | root,toor654321 | 9 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | admin654321 | 13 |
| 单兵闯关 | 任务1.Wireshark数据包分析 | user123,123456 | 17 |
| 单兵闯关 | 任务2.文件上传渗透测试 | 200 | 11 |
| 单兵闯关 | 任务2.文件上传渗透测试 | Upload | 13 |
| 单兵闯关 | 任务2.文件上传渗透测试 | c:/appserv/www/uploadfile/uploads/uploads/backdoor.php | 15 |
| 单兵闯关 | 任务2.文件上传渗透测试 | weevely generate pass /backdoor.php | 17 |
| 单兵闯关 | 任务2.文件上传渗透测试 | c:/appserv/www/uploadfile/uploads/uploads/backdoor.php | 11 |
| 单兵闯关 | 任务2.文件上传渗透测试 | PC6249546 | 11 |
| 单兵闯关 | 任务2.文件上传渗透测试 | Upload failed | 13 |
| 单兵闯关 | 任务2.文件上传渗透测试 | generate.img | 9 |
| 单兵闯关 | 任务3.Web渗透测试 | list audit | 9 |
| 单兵闯关 | 任务3.Web渗透测试 | crawl phpinfo web\_spider | 11 |
| 单兵闯关 | 任务3.Web渗透测试 | audit blind\_sqli os\_commanding sqli | 13 |
| 单兵闯关 | 任务3.Web渗透测试 | set target | 11 |
| 单兵闯关 | 任务3.Web渗透测试 | http://192.168.80.1/checklogin.php | 17 |
| 单兵闯关 | 任务3.Web渗透测试 | exploit sqlmap | 9 |
| 单兵闯关 | 任务3.Web渗透测试 | mysql | 19 |
| 单兵闯关 | 任务3.Web渗透测试 | v5a4r8e2w5u9 | 11 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | Microsoft IIS httpd | 7 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | 59.51.78.210 | 9 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | bpemtasxp | 11 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | Vbaernyalsdb | 15 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | encourage | 17 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | xcvfdsrewq4682 | 20 |
| 单兵闯关 | 任务4.Windows操作系统渗透测试 | jhrstbnsrtyu | 21 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | vsftpd 2.3.4 | 5 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | reuwaepl | 7 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | ysdrjsix | 9 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | fasrewth | 7 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | determined | 9 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | yerekwqo | 8 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | pcoehter | 11 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | qadjfwtc | 21 |
| 单兵闯关 | 任务5.Linux操作系统渗透测试 | peryzied | 23 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 00f8b8eca3f611434471e1a2d53e94515dec6e4605d718083181cc91609cb380 | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 215458e5cca7a3d187aef22d998107a4cfb3bc5494785529b0b2a0287efd751f | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | f8f32646c59344968d83a0af87df374eb4926871b43740534b2f5d30fed71844 | 9 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | cf8403c540131933c46bce24dba0d8511efca3c74b1b780023bc842b0d8de206 | 9 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9 | 11 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | beb37b789e6f7fec03cff80ae91911eb913882d5dbc7843f573a90f19a6eb1c3 | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 53f81a436a01c22280fa10fd83fd22f15e201d51197155eed4cf861bdc9d3bf7 | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | ed7f0d0a5fe6e102f4a7085adaf9436d5f6f901798324aa845564003991be86e | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 7dfd17a08827e16aa3437d01445e696026a72b2c32354effa49e7076a23e841b | 7 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 0b9ce1a88cb0d227f8d60c8ea9747ea985d7c961951511a1e6ae296f95551de7 | 9 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 628218ffa16cbf38457cf85c2b67a820819a0915a29df23652cc407aa9af8c45 | 9 |
| 单兵闯关 | 任务6.网络协议栈渗透测试 | 508feb7d8e25fb1793c0ce54f6c80a58d3cc79a8fb45e6b0066d0f9bfdc4e8cc | 11 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | c4e7841bfb5dd083a1bfc302969d12993dea68339e6744fc41681a6c7149c2f5 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 3ebd47a16db21084cde87b984ab71750738d7bfb05d104663951b2eaac14af98 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 41271d7be3eeb63af0307882a7187ba23535f9d4dbda2c907f89baf28f219cd7 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | c854f3d2dda026a3e1ce20ec670bff86fbb5f23350b83f7f9d5cc273dc496773 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 52c01c47b4a6aad7a5d670f70fe7ed7367b44c91f787589c1fc932918e7baa8d | 9 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 714620fc991e71cb230adfc59e00a0476ad519f8712c0789209ded66f515391f | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 70f00d10f2f7b8d54697726b86ba7b88eced6e49537767659afd62ac8804b0c1 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | d5821bc4d42a7df4a4fabb6bc41187d12d919a255fca524f96e2ae0b7392a50e | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 1b1bf6e9e404262bd433c4f5d6419f96b9cc3b12c869584ab733d152a2ac1352 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 1e2fcedea0a416a386176b8c4a83bbb73bfca99576dc0287c8db12a765946f42 | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | 211873ee4872dc13ce24006b16a5fe079f4651e96ee2a8b2fa90dd2de9d185bb | 7 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | dd18967e9219d576416d4a9b6473aa7e6737de350583320c72169e1b844002d3 | 10 |
| 单兵闯关 | 任务7.系统综合渗透测试及安全加固 | d04547565d2a049d793915b59329a5e7dfc26cbbd370f87fbfdec4c68f9e9063 | 11 |
| 分组混战 | 分组混战任务1 | 原始码654321 | 2 |
| 分组混战 | 分组混战任务2 | 原始码123456 | 2 |

# 五、评分标准

## 1.评分阶段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **阶段名称** | **任务阶段** | **分值** | **评分方式** |
| 第一阶段权重70% | 单兵模式系统渗透测试 | 任务1 | 100 | 机考评分 |
| 任务2 | 100 | 机考评分 |
| 任务3 | 100 | 机考评分 |
| 任务4 | 100 | 机考评分 |
| 任务5 | 100 | 机考评分 |
| 任务6 | 100 | 机考评分 |
| 任务7 | 100 | 机考评分 |
| 第二阶段权重30% | 分组对抗 | 系统攻防演练 | 300 | 机考评分 |

## 2.第一阶段评分规则

规则1：第一阶段总分为700分,分为7个任务，每道题细分在赛题中标明；

规则2：系统自动评分和排名，显示在大屏幕上；

规则3：同分的选手会根据系统提供的答题时间进行排名，答题时间为最后一个正确FLAG值提交的时间，先提交者排名靠前。

## 3.第二阶段评分规则

规则1：第二阶段总分为300分，初始分为100分；

规则2：每提交1次对手靶机的FLAG值得分，每当被对手提交1次自身靶机的FLAG值扣分，每个对手靶机的FLAG值只能提交一次，得分和扣分的具体分值在赛题中标明；

规则3：系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分，每检测到一次违规行为扣除一次分值，扣分明细显示在扣分榜中，记录在第二阶段总成绩中：

1）攻防阶段启用FLAG检测机制，如发现FLAG异常（譬如：删除、修改、杀进程），记为一次违规行为，扣除相应分值；

2）攻防阶段启用服务端口检测机制，如发现关闭题目要求开启的端口，记为一次违规行为，扣除相应分值；

3）攻防阶段靶机IP参数不允许修改，如修改记为一次违规行为，扣除相应分值；

4）在加固时间后，选手自己关闭靶机或被他人关闭，均记为三次违规行为，扣除相应分值，且裁判员不予帮助重启。

规则4：选手的得分显示在大屏，某选手的显示成绩可能会显示负分或者超过300分；凡是负分的，本阶段“复核成绩”一律为0分；凡是超过300分的，本阶段“复核成绩”一律为300分；选手成绩排名次序保持不变，得分相同的选手根据“显示成绩”以及得分时间点不同而排名不同。

【注】

显示成绩：这是系统自动打出的分值，会显示在大屏幕上，分值可能是负值，可能是超过第二阶段满分300分的分值；

复核成绩：分值在0-300分之间，是裁判长根据系统导出的成绩进行修订，保证第二阶段成绩不影响其他阶段成绩。

## 4.整体合分规则

规则1：最终成绩由第一阶段成绩和第二阶段复核成绩相加得来，如果总分相同，以第二阶段复核成绩高低排序，第二阶段复核成绩高者靠前；

规则2：如果第二阶段复核成绩也相同，以第二阶段提交正确FLAG值（显示成绩）高低排序，显示成绩高者排名靠前；

规则3：第二阶段提交正确FLAG值（显示成绩）相同，以第二阶段提交最后一个正确的FALG时间排序，先完成者排名靠前。

## 5.成绩录入规则

规则1：成绩录入系统的分值不能相同；

规则2：同分选手，按照排名顺序，从最后一位选手开始，排名每靠前一位，增加0.01分录入系统。