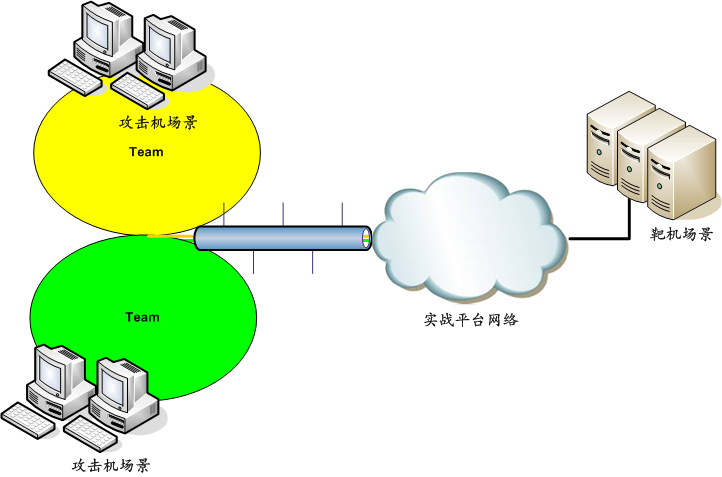
**2018年全国职业院校技能大赛中职组**

**“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 | MSSQL数据库渗透测试 | 100分钟 | 100 |
| 任务2 | 主机发现与信息收集 | 100 |
| 任务3 | SNMP信息收集与利用 | 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 | 网络协议堆栈渗透测试 | 100 |
| 任务7 | Web应用程序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：Kali（用户名：root；密码：toor）；

虚拟机3：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. MSSQL数据库渗透测试（100分）

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用zenmap工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机IP地址和指定开放的1433、3306、80端口。并将该操作使用的命令中必须要使用的字符串作为FLAG提交；（10分）

2.通过本地PC中渗透测试平台BT5对服务器场景server2003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数据库服务对应的服务端口信息作为FLAG提交；（10分）

3.在本地PC渗透测试平台BT5中使用MSF中模块对其爆破，使用search命令，并将扫描弱口令模块的名称作为FLAG提交；（10分）

4.在上一题的基础上使用命令调用该模块，并查看需要配置的信息（使用show options命令），将回显中需要配置的目标地址,密码使用的猜解字典,线程,账户配置参数的字段作为FLAG提交（之间以英文逗号分隔，例hello,test，..,..）；（10分）

5.在msf模块中配置目标靶机IP地址，将配置命令中的前两个单词作为FLAG提交；（10分）

6.在msf模块中指定密码字典，字典路径为/root/2.txt爆破获取密码并将得到的密码作为FLAG提交；（14分）

7.在msf模块中切换新的渗透模块，对服务器场景server2003进行数据库服务扩展存储过程进行利用，将调用该模块的命令作为FLAG提交；（14分）

8.在上一题的基础上，使用第6题获取到的密码并进行提权，同时使用show options命令查看需要的配置，并配置CMD参数来查看系统用户，将配置的命令作为FLAG提交；（14分）

9.在利用msf模块获取系统权限并查看目标系统的异常（黑客）用户，并将该用户作为FLAG提交。（8分）

### 任务2. 主机发现与信息收集（100分）

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段(例如：172.16.101.0/24)进行主机发现扫描,并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

2.通过本地PC中渗透测试平台BT5使用genlist对服务器场景server2003所在网段进行扫描进行主机存活发现, 并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

3.在通过本地PC中渗透测试平台BT5使用nbtscan对服务器场景server2003所在网段进搜索扫描，获取目标的MAC地址等信息，并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

4.假设服务器场景server2003设置了防火墙无法进行ping检测，通过PC中渗透测试平台BT5使用arping检测主机连通性扫描（发送请求数据包数量为4个），并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

5.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段进行存活性扫描，且要把最终扫描的存活主机输出到文件ip.txt中，并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文逗号分割，例a,b）；（12分）

6.通过本地PC中渗透测试平台BT5使用nbtscan从第5题的ip.txt文件中读取IP扫描主机信息MAC地址等信息，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

7.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行TCP扫描，仅扫描靶机80,3306端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

8.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行UDP扫描，仅扫描靶机161,162端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交。（16分）

### 任务3. SNMP信息收集与利用（100分）

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用autoscan工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机地址。判断存活主机是否开放网络管理服务，若开启则以扫描出开启SNMP服务的主机名作为FLAG提交；（11分）

2.在本地PC渗透测试平台BT5中使用nmap工具进行UDP扫描服务器场景server2003所在网段范围内存活的主机地址，判断网络管理服务的开放情况，若开启，则以扫描出SNMP开放的端口号作为FLAG（各端口之间用英文分号分割，例21;23），若未开放则提交none作为FLAG；（11分）

3.在本地PC渗透测试平台BT5中调用snmpwalk工具测试服务器场景server2003是否开启Windows SNMP服务（共同体为默认字符串为public，通过对目标靶机的.1.3.6.1.2.1.25.1.6分支进行snmpwalk来测试服务的开放情况（SNMP 版本为v2c），并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文分号分割，例a;b）；（11分）

4.在本地PC渗透测试平台BT5中使用ADMsnmp工具尝试猜解团体字符串，并将使用的全部命令作为FLAG提交（提交答案时IP以192.168.100.10代替,使用默认字典snmp.passwd）；（11分）

5.更换使用onesixtyone工具执行命令查看帮助选项，并将输入的命令作为FLAG提交；（11分）

6.在本地PC渗透测试平台BT5中使用onesixtyone对靶机SNMP进行团体字符串猜解，并将使用的全部命令作为FLAG提交（提交的命令为忽略IP后必须使用的命令，字典名字为dict.txt）；（11分）

7.在本地PC渗透测试平台BT5中对猜解结果进行查看，将回显中猜解的团体字符串作为FLAG提交；（11分）

8.在本地PC渗透测试平台BT5中选择新的SNMP攻击模块snmpcheck，根据得到的public团体字符串并利用snmpcheck进行对靶机的信息收集，并将该操作使用的命令中必须使用的参数作为FLAG提交；（11分）

9.查看获取的系统信息，将系统管理员用户和异常（黑客）用户作为FLAG提交，（各用户之间用英文分号分割，例root;user）。（12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：PYsystem4
* 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Kali对服务器场景PYsystem4进行操作系统扫描渗透测试，并将该操作显示结果“Running：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景网络连接信息中的DNS信息作为FLAG提交;(例如114.114.114.114)（13分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交；（14分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交；（16分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交；（15分）

7.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交；（10分）

8.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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提交。（20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：PYsystem5
* 服务器场景操作系统：未知

1.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行操作系统扫描渗透测试，并将该操作显示结果“OS Details：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5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MySQL数据库对应的服务版本信息字符串作为FLAG提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件名称作为FLAG提交；（12分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件内容作为FLAG提交；（16分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root目录中唯一一个后缀为.bmp文件的文件名称作为FLAG提交；（27分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root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提交。（33分）

### 任务6. 网络协议堆栈渗透测试（100分）

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：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.通过物理机的ping程序访问靶机，成功访问后，在攻击机中使用arpspoof程序对物理机进行ARP渗透测试，对物理机进行ARP缓存毒化为：靶机IP地址映射攻击机MAC地址；从靶机服务器场景的FTP服务器中下载文件arpspoof.py，编辑该Python3程序文件，使该程序实现同本任务中arpspoof程序一致的功能，填写该文件当中空缺的F1字符串，将该字符串作为Flag值提交；（9分）

2.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F2字符串，将该字符串作为Flag值提交；（9分）

3.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F3字符串，将该字符串作为Flag值提交；（9分）

4.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F4字符串，将该字符串作为Flag值提交；（9分）

5.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F5字符串，将该字符串作为Flag值提交；（9分）

6.继续从靶机服务器场景FTP服务器中下载文件icmpflood.py，编辑该Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F6字符串，将该字符串作为Flag值提交；（9分）

7.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F7字符串，将该字符串作为Flag值提交；（9分）

8.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F8字符串，将该字符串作为Flag值提交；（9分）

9.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F9字符串，将该字符串作为Flag值提交；（9分）

10.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F10字符串，将该字符串作为Flag值提交；（9分）

11. 在本地PC渗透测试平台BT5中通过Python3程序解释器执行程序文件icmpflood.py，并打开WireShark监听网络流量，分析通过程序文件icmpflood.py产生的ICMP流量，并将该ICMP数据对象中的Code属性值通过MD5运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（10分）

### 任务7. Web应用程序渗透测试及安全加固（100分）

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：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

服务器场景FTP上传服务用户名：anonymous，密码：123456

服务器场景FTP上传服务端口：21

1.在攻击机端通过浏览器访问主页http://靶机IP地址，通过Web应用程序渗透测试方法登陆磐石公司模拟产品网站，成功登陆后，将Web页面弹出的字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（7分）

2.从靶机服务器场景FTP服务器中下载文件loginauthentic.php，编辑该PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F11字符串，将该字符串作为Flag值提交；（7分）

3.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F12字符串，将该字符串作为Flag值提交；（7分）

4.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F13字符串，将该字符串作为Flag值提交；（7分）

5.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F14字符串，将该字符串作为Flag值提交；（7分）

6.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F15字符串，将该字符串作为Flag值提交；（7分）

7.将编辑好后的loginauthentic.php程序文件上传至靶机FTP服务，在攻击机端通过浏览器访问主页http://靶机IP地址，通过本任务第1题所使用的Web应用程序渗透测试方法登陆磐石公司模拟产品网站，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交；（7分）

8.成功登陆磐石公司模拟产品网站后，继续点击超链接进入磐石公司产品信息页面，通过Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，并将该字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（8分）

9.从靶机服务器场景FTP服务器中下载文件product.php，编辑该PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F16字符串，将该字符串作为Flag值提交；（7分）

10.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F17字符串，将该字符串作为Flag值提交；（7分）

11.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F18字符串，将该字符串作为Flag值提交；（7分）

12.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F19字符串，将该字符串作为Flag值提交；（7分）

13.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F20字符串，将该字符串作为Flag值提交；（7分）

14.将编辑好后的product.php程序文件上传至靶机FTP服务，并在攻击机端通过本任务第8题中使用的Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（8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：CentOS2018065（用户名：root；密码：123456），服务器操作系统：CentOS（版本不详）；

场景2：Windows2018065（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. CentOS2018065靶机服务器如下服务及端口不允许关闭：21、22、23、80、555、3306、7000-7999；Windows2018065靶机服务器如下服务及端口不允许关闭：HTTP 80、FTP 21、Telnet 23、7000-7999；

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 | MSSQL数据库渗透测试 | -p 1433,3306,80 | 10 |
| 单兵闯关 | MSSQL数据库渗透测试 | 1433/tcp | 10 |
| 单兵闯关 | MSSQL数据库渗透测试 | auxiliary/scanner/mssql/mssql\_login | 10 |
| 单兵闯关 | MSSQL数据库渗透测试 | RHOSTS,PASS\_FILE,THREADS,USERNAME | 10 |
| 单兵闯关 | MSSQL数据库渗透测试 | set RHOSTS | 10 |
| 单兵闯关 | MSSQL数据库渗透测试 | cbc2b1 | 14 |
| 单兵闯关 | MSSQL数据库渗透测试 | use auxiliary/admin/mssql/mssql\_exec | 14 |
| 单兵闯关 | MSSQL数据库渗透测试 | set CMD cmd.exe /c net user | 14 |
| 单兵闯关 | MSSQL数据库渗透测试 | hacker | 8 |
| 单兵闯关 | 主机发现与信息收集 | g | 12 |
| 单兵闯关 | 主机发现与信息收集 | s | 12 |
| 单兵闯关 | 主机发现与信息收集 | r | 12 |
| 单兵闯关 | 主机发现与信息收集 | arping -c 4 | 12 |
| 单兵闯关 | 主机发现与信息收集 | g,a | 12 |
| 单兵闯关 | 主机发现与信息收集 | nbtscan -f ip.txt | 12 |
| 单兵闯关 | 主机发现与信息收集 | xprobe2 -T 80,3306 | 12 |
| 单兵闯关 | 主机发现与信息收集 | xprobe2 -U 161,162 | 16 |
| 单兵闯关 | SNMP信息收集与利用 | ADMIN6291524037 | 11 |
| 单兵闯关 | SNMP信息收集与利用 | 161;162 | 11 |
| 单兵闯关 | SNMP信息收集与利用 | v;c | 11 |
| 单兵闯关 | SNMP信息收集与利用 | ./ADMsnmp 192.168.100.10 -wordfile snmp.passwd | 11 |
| 单兵闯关 | SNMP信息收集与利用 | ./onesixtyone | 11 |
| 单兵闯关 | SNMP信息收集与利用 | ./onesixtyone -c dict.txt | 11 |
| 单兵闯关 | SNMP信息收集与利用 | public | 11 |
| 单兵闯关 | SNMP信息收集与利用 | t | 11 |
| 单兵闯关 | SNMP信息收集与利用 | Administrator;hacker | 12 |
| 单兵闯关 | Windows操作系统渗透测试 | Microsoft Windows XP|2003 | 6 |
| 单兵闯关 | Windows操作系统渗透测试 | Microsoft Windows XP microsoft-ds | 6 |
| 单兵闯关 | Windows操作系统渗透测试 | 8.8.4.4 | 13 |
| 单兵闯关 | Windows操作系统渗透测试 | dctfvg | 14 |
| 单兵闯关 | Windows操作系统渗透测试 | xyfjyhha | 16 |
| 单兵闯关 | Windows操作系统渗透测试 | sunny | 15 |
| 单兵闯关 | Windows操作系统渗透测试 | xybjjfajbgbdbe | 10 |
| 单兵闯关 | Windows操作系统渗透测试 | oajdnfdx | 20 |
| 单兵闯关 | Linux操作系统渗透测试 | Linux 2.6.32 - 3.10 | 6 |
| 单兵闯关 | Linux操作系统渗透测试 | MySQL (unauthorized) | 6 |
| 单兵闯关 | Linux操作系统渗透测试 | bjjhbcag | 12 |
| 单兵闯关 | Linux操作系统渗透测试 | tjekdb | 16 |
| 单兵闯关 | Linux操作系统渗透测试 | bjjfajbg | 27 |
| 单兵闯关 | Linux操作系统渗透测试 | belief | 33 |
| 单兵闯关 | 网络协议堆栈渗透测试 | spoofp = ethernet/arp | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | ype = 0x806 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | wtype = 0x1 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | type = 0x800 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | op = 2 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | floodp = ethernet/ip/udp | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | ype = 0x800 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | ersion = 4 | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | roto = "udp" | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | [UDP].dport | 9 |
| 单兵闯关 | 网络协议堆栈渗透测试 | eccbc87e4b5ce2fe28308fd9f2a7baf3 | 10 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | 8096020fc0359c06c565f173a7085350c0698ea7f8aaf8b94686940e7b327758 | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | select \* from users where username=? and password=? | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $pdo->prepare($sql); | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $statment->execute(array($username,$password)); | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $res=$statment->fetch(); | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | empty( | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | 1cf93d8ad17292474f0afe66df7f7b6c38ae09b750ab7b1d405168b381dddc37 | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | 30a3784e88ea0a9c80f0807a1792353334c2cb71a437ae3c166f5ddaebd2b290 | 8 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | (strstr($keyWord,$str1)) || (strstr($keyWord,$str2)) | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $conn=mssql\_connect("localhost" | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $found=0; | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | $obj=mssql\_fetch\_object($res) | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | if($found= | 7 |
| 单兵闯关 | Web应用程序渗透测试及安全加固 | 29e0c22d73a58b28fc87ecc2e806d7b01b0bda167b5b1230ae54a5d249b4b3c5 | 8 |
| 分组混战 | 分组混战任务1 | 123456 | 2 |
| 分组混战 | 分组混战任务2 | 654321 | 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。