**2017年全国职业院校技能大赛**

**中职组“网络空间安全”赛项国赛赛卷**

# 一、竞赛阶段简介

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Linux操作系统服务渗透测试及安全加固 | 两小时 | 25 |
| 任务2 | Windows操作系统服务渗透测试及安全加固 | 25 |
| 任务3 | Windows操作系统服务端口扫描渗透测试 | 20 |
| 第二阶段分组对抗 | 系统加固 | 一小时 | 30 |
| 渗透测试 |

# 二、拓扑图



# 三、竞赛任务书

## （一）第一阶段任务书（70分）

根据《赛场参数表》提供的信息，请使用PC1的谷歌浏览器登录考试平台，登录后点击“闯关关卡”，左侧有本阶段的三个任务列表。

点击右侧的“网络靶机”，进入虚机完成任务，找到FLAG值，填入空框内，点击“提交任务”按钮。

提示： FLAG中包含的字符是英文字符，注意英文字符大小写区分。

虚拟机1：Ubuntu Linux 32bit（用户名：root；密码：toor）；

虚拟机1安装工具集：Backtrack5；

虚拟机1安装开发环境：Python；

虚拟机2：WindowsXP（用户名：administrator；密码：123456）。

任务1. Linux操作系统服务渗透测试及安全加固（25分）

**任务环境说明：**

* 服务器场景：CentOS5.5（用户名：root；密码：123456）
* 服务器场景操作系统：CentOS5.5
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：FTP
* 服务器场景操作系统安装服务：SSH
* 服务器场景操作系统安装开发环境：GCC
* 服务器场景操作系统安装开发环境：Python

1.在服务器场景CentOS5.5上通过Linux命令行开启HTTP服务，并将开启该服务命令字符串作为FLAG值提交；（3分）

2.通过PC2中渗透测试平台对服务器场景CentOS5.5进行操作系统扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作使用命令中必须要使用的参数作为FLAG提交；（3分）

3.通过PC2中渗透测试平台对服务器场景CentOS5.5进行操作系统扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果“OS Details：”之后的字符串作为FLAG提交；（3分）

4.通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作使用命令中必须要使用的参数作为FLAG提交；（4分）

5.通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果的HTTP服务版本信息字符串作为FLAG提交；（4分）

6.在服务器场景CentOS5.5上通过Linux命令行关闭HTTP服务，并将关闭该服务命令字符串作为FLAG值提交；（4分）

7.再次通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果的第2项服务的PORT信息字符串作为FLAG提交。（4分）

任务2. Windows操作系统服务渗透测试及安全加固（25分）

**任务环境说明：**

* 服务器场景：WinServ2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Microsoft Windows2003 Server
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：CA
* 服务器场景操作系统安装服务：SQL

1.PC2虚拟机操作系统WindowsXP打开Ethereal，验证监听到PC2虚拟机操作系统WindowsXP通过Internet Explorer访问IISServ2003服务器场景的Test.html页面内容，并将Ethereal监听到的Test.html页面内容在Ethereal程序当中的显示结果倒数第2行内容作为FLAG值提交；（7分）

2.在PC2虚拟机操作系统WindowsXP和WinServ2003服务器场景之间建立SSL VPN，须通过CA服务颁发证书；IISServ2003服务器的域名为www.test.com，并将WinServ2003服务器个人证书信息中的“颁发给：”内容作为FLAG值提交；（8分）

3.在PC2虚拟机操作系统WindowsXP和WinServ2003服务器场景之间建立SSL VPN，再次打开Ethereal，监听Internet Explorer访问WinServ2003服务器场景流量，验证此时Ethereal无法明文监听到Internet Explorer访问WinServ2003服务器场景的HTTP流量，并将WinServ2003服务器场景通过SSL Record Layer对Internet Explorer请求响应的加密应用层数据长度（Length）值作为FLAG值提交。（10分）

任务3. Windows操作系统服务端口扫描渗透测试（20分）

**任务环境说明：**

* 服务器场景：WinServ2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Microsoft Windows2003 Server
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：CA
* 服务器场景操作系统安装服务：SQL

1.进入PC2虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG1字符串，将该字符串作为FLAG值（形式：FLAG1字符串）提交； （2分）

2.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG2字符串，将该字符串作为FLAG值（形式：FLAG2字符串）提交； （2分）

3.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG3字符串，将该字符串作为FLAG值（形式：FLAG3字符串）提交； （2分）

4.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG4字符串，将该字符串作为FLAG值（形式：FLAG4字符串）提交； （2分）

5.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG5字符串，将该字符串作为FLAG值（形式：FLAG5字符串）提交；（3分）

6.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG6字符串，将该字符串作为FLAG值（形式：FLAG6字符串）提交；（3分）

7.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG7字符串，将该字符串作为FLAG值（形式：FLAG7字符串）提交；（3分）

8.在虚拟机操作系统：Ubuntu Linux 32bit下执行tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，将该文件执行后的显示结果中，包含TCP 80端口行的全部字符作为FLAG值提交。（3分）

## （二）第二阶段任务书（30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台服务器进行渗透。

根据《赛场参数表》提供的第二阶段的信息，请使用PC1的谷歌浏览器登录考试平台。

提示1：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示2：加固全部漏洞；

提示3：对其它参赛队服务器进行渗透，取得FLAG值并提交到自动评分系统；

提示4：十五分钟之后，各位选手才可以进入渗透测试环节。渗透测试环节中，各位选手可以继续加固服务器，也可以选择攻击其他选手的服务器。

**靶机环境说明：**

* 服务器场景：CentOS5.5（用户名：root；密码：123456）
* 服务器场景操作系统：CentOS5.5
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：FTP
* 服务器场景操作系统安装服务：SSH
* 服务器场景操作系统安装服务：SQL
* 服务器场景操作系统安装开发环境：GCC
* 服务器场景操作系统安装开发环境：Python
* 服务器场景操作系统安装开发环境：PHP

**可能的漏洞列表如下：**

1.靶机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;

2.靶机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;

3.靶机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;

4.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;

5.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;

6.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。

**注意事项：**

注意1：任何时候不能人为关闭服务器服务端口，否则将判令停止比赛，第二阶段分数为0分；

注意2：不能对裁判服务器进行攻击，否则将判令停止比赛，第二阶段分数为0分；

注意3：在加固阶段（前十五分钟，具体听现场裁判指令）不得对任何服务器进行攻击，否则将判令攻击者停止比赛，第二阶段分数为0分；

注意4：FLAG值为每台受保护服务器的唯一性标识，每台受保护服务器仅有1个；

注意5：靶机的FLAG值存放在./root/Flaginfoxxxx.xxx.txt文件内容当中（xxxx.xxx是随机产生的字符）；

注意6：在登录自动评分系统后，提交对手靶机的FLAG值，同时需要指定对手靶机的IP地址；

注意7：不得人为恶意破坏自己服务器的FLAG值，一经发现将判令犯规，第三阶段分数为0分；

注意8：本环节是对抗环节，不予补时。

**第二阶段评分说明：**

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

规则2：第二阶段总分为30分，初始分为10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30分；凡是负分的，本阶段评判成绩一律为0分；凡是超过30分的，本阶段评判成绩一律为30分。