**上海市“星光计划”职业院校技能大赛**

**网络安全竞赛试题**

**（总分1000分）**

|  |
| --- |
|  |

赛题说明

一、竞赛项目简介

“网络安全”竞赛共分A.基础设施设置与安全加固；B.网络安全事件响应、数字取证调查和应用安全；C.CTF夺旗-攻击；D. CTF夺旗-防御等四个模块。竞赛时间安排和分值权重见表1。

表1 竞赛时间安排与分值权重

|  |  |  |  |
| --- | --- | --- | --- |
| 模块编号 | 模块名称 | 竞赛时间（小时） | 合计 |
| A | 基础设施设置与安全加固 | 1.5 | 20% |
| B | 网络安全事件响应、数字取证调查和应用安全 | 40% |
| C | CTF夺旗-攻击 | 1.5 | 20% |
| D | CTF夺旗-防御 | 20% |
| 总计 | 3 | 100% |

二、竞赛注意事项

1.竞赛期间禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

2.请根据大赛所提供的竞赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3.在进行任何操作之前，请阅读每个部分的所有任务。各任务之间可能存在一定关联。

4.操作过程中需要及时按照答题要求保存相关结果。竞赛结束后，所有设备保持运行状态，评判以最后提交的成果为最终依据。

5.竞赛完成后，竞赛设备、软件和赛题请保留在座位上，禁止将竞赛所用的所有物品（包括试卷等）带离赛场。

6.禁止在提交资料上填写与竞赛无关的标记，如违反规定，可视为0分。

**竞赛内容**

**一、竞赛时间**

总计：180分钟

**二、竞赛阶段**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| A模块 | A-1 | 登录安全加固 | 90分钟 | 200分 |
| A-2 | Web安全加固（Web） |
| A-3 | 流量完整性保护与事件监控（Web,Log） |
| A-4 | 防火墙策略 |
| A-5 | Linux操作系统安全配置 |
| B模块 | B-1 | SSH弱口令渗透测试 | 400分 |
| B-2 | Windows操作系统安全配置 |
| B-3 | Wireshark数据包分析 |
| B-4 | 网页渗透 |
| C、D模块 | C模块 | CTF夺旗-攻击 | 90分钟 | 200分 |
| D模块 | CTF夺旗-防御 | 200分 |

**三、竞赛任务书内容**

**（一）拓扑图**



**（二）A模块基础设施设置/安全加固（200分）**

一、项目和任务描述：

假定你是某企业的网络安全工程师，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。

二、说明：

1.所有截图要求截图界面、字体清晰，并粘贴于相应题目要求的位置；

2.文件名命名及保存：网络安全模块A-XX（XX为工位号），PDF格式保存；

3.文件保存到U盘提交。

### A-1：登录安全加固

**任务环境说明：**

* 服务器场景：LOG:（开放链接）
* 用户名:root密码：root
* 服务器场景：Web:（开放链接）
* 用户名：administrator密码：P@ssw0rd

请对服务器Web按要求进行相应的设置，提高服务器的安全性。

1.密码策略（Web）

a.最小密码长度不少于8个字符，将密码长度最小值的属性配置界面截图；

b.密码策略必须同时满足大小写字母、数字、特殊字符，将密码必须符合复杂性要求的属性配置界面截图。

2.登录策略（Web）

a.在用户登录系统时，应该有“For authorized users only”提示信息，将登录系统时系统弹出警告信息窗口截图；

b.一分钟内仅允许5次登录失败的尝试，超过5次，登录帐号锁定1分钟，将账户锁定策略配置界面截图；

c.远程用户非活动会话连接超时应小于等于5分钟，将RDP-Tcp属性对应的配置界面截图。

3.用户安全管理(Web)

a.对服务器进行远程管理安全性SSL加固，防止敏感信息泄露被监听，将RDP-Tcp属性对应的配置界面截图；

b.仅允许超级管理员账号关闭系统，将关闭系统属性的配置界面截图。

### A-2：Web安全加固(Web)

**任务环境说明：**

* 服务器场景：LOG:（开放链接）
* 用户名:root密码：root
* 服务器场景：Web:（开放链接）
* 用户名：administrator密码：P@ssw0rd

1.为了防止web中.mdb数据库文件非法下载，请对Web配置文件进行安全加固，将C:\Windows\System32\inetsrv\config\applicationHost配置文件中对应的部分截图；

2.限制目录执行权限,对picture和upload目录设置执行权限为无，将编辑功能权限的配置界面截图；

3.开启IIS的日志审计记录(日志文件保存格式为W3C,只记录日期、时间、客户端IP地址、用户名、方法)，将W3C日志记录字段的配置界面截图；

4.为了减轻网站负载，设置网站最大并发连接数为1000，将编辑网站限制的配置界面截图；

5.防止文件枚举漏洞枚举网络服务器根目录文件，禁止IIS短文件名泄露，将配置命令截图；

6.关闭IIS的WebDAV功能增强网站的安全性，将警报提示信息截图。

### A-3：流量完整性保护与事件监控（Web,Log）

**任务环境说明：**

* 服务器场景：LOG:（开放链接）
* 用户名:root密码：root
* 服务器场景：Web:（开放链接）
* 用户名：administrator密码：P@ssw0rd

1.为了防止密码在登录或者传输信息时被窃取，仅使用证书登录SSH（Log），将/etc/ssh/sshd\_config配置文件中对应的部分截图；

2.将Web服务器开启审核策略

登录事件 成功/失败;

特权使用 成功;

策略更改 成功/失败;

进程跟踪 成功/失败;

将审核策略的配置界面截图；

3.配置Splunk接收Web服务器，安全日志，系统日志，CPU负载，内存，磁盘空间，网络状态。将转发器：部署成功的页面截图。

### A-4：防火墙策略

**任务环境说明：**

* 服务器场景：LOG:（开放链接）
* 用户名:root密码：root
* 服务器场景：Web:（开放链接）
* 用户名：administrator密码：P@ssw0rd

所有服务器开启防火墙,为防止勒索病毒攻击对防火墙进行加固策略：

1.Windows系统禁用445端口，将防火墙入站规则截图；

2.Linux系统禁用23端口，将iptables配置命令截图；

3.Linux系统禁止别人ping通，将iptables配置命令截图；

4.Linux系统为确保安全禁止所有人连接SSH除了172.16.1.1这个ip，将iptables配置命令截图。

### A-5：Linux操作系统安全配置

* 服务器场景：AServer002（开放链接）
* 用户名：root，密码：123456
* 请对服务器Linux按要求进行相应的设置，提高服务器的安全性。

1.设置禁止使用最近用过的6个旧密码，将配置文件中对应的部分截图;

2.设置密码复杂程度，允许重试3次，新密码必须与旧密码有4位不同，最小位数6位，大写字母至少包含2位，小写字母至少包含3位，特殊字母个数至少包含1位，将配置文件中对应的部分截图;

3.禁止匿名用户登录vsftpd服务，将配置文件中对应的部分截图；

4.设置关闭ftp-data端口不使用主动模式，使用ipv4进行监听，将配置文件中对应的部分截图；

5. 将Telnet服务的端口号修改为2323 ,查看Telnet服务端口信息，将回显结果截图；

6.限制Telnet用户连接，单个IP允许的最大连接数为1，总的最大连接数为10，将配置文件中对应的部分截图；

7.允许root用户通过SSH远程登录，将配置文件中对应的部分截图；

8.配置SSH服务，设置RSA证书登录，将配置文件中对应的部分截图；

9.修改网站的httpd服务为root权限，将配置文件中对应的部分截图；

10.设置HTTP服务，修改网站的配置文件，配置滚动日志按天记录网站的访问日志和错误日志，将配置文件中对应的部分截图。

## （三）B模块安全事件响应/网络安全数据取证/应用安全（400分）

### B-1：SSH弱口令渗透测试

**任务环境说明：**

* 服务器场景：Server18-2（关闭链接）
* 服务器场景操作系统：Linux（版本不详）
1. 在本地PC渗透测试平台Kali中使用zenmap工具扫描服务器场景Linux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21、22、23端口。并将该操作使用的命令中必须要添加的字符串作为FLAG提交（忽略ip地址）；
2. 通过本地PC中渗透测试平台Kali对服务器场景Linux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SSH服务对应的服务端口信息作为FLAG提交；
3. 在本地PC渗透测试平台Kali中使用MSF模块对其爆破，使用search命令，并将扫描弱口令模块的名称信息作为FLAG提交；
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，..,..）；
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；
6. 在msf模块中指定密码字典，字典路径为桌面tools文件夹2.txt，用户名为test爆破获取密码并将得到的密码作为FLAG提交；
7. 在上一题的基础上，使用第6题获取到的密码SSH到靶机，将test用户家目录中唯一一个后缀为.bmp图片的文件名的字符串作为FLAG提交。

### B-2：Windows操作系统渗透测试

**任务环境说明：**

* 服务器场景：Server2105（关闭链接）
* 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；
2. 通过本地PC中渗透测试平台Kali对服务器场景进行渗透测试，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；
3. 通过本地PC中渗透测试平台Kali对服务器场景进行渗透测试，将该场景中的当前最高账户管理员的密码作为Flag值提交；
4. 通过本地PC中渗透测试平台Kali对服务器场景进行渗透测试，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；
5. 通过本地PC中渗透测试平台Kali对服务器场景进行渗透测试，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；
6. 通过本地PC中渗透测试平台Kali对服务器场景进行渗透测试，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；

### B-3：Wireshark数据包分析

**任务环境说明：**

* 服务器场景：FTPServer220509（关闭链接）
* 服务器场景操作系统：未知
* FTP用户名：wireshark0051密码：wireshark0051
1. 从靶机服务器的FTP上下载wireshark0051.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；
2. 继续分析数据包wireshark0051.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；
3. 继续分析数据包wireshark0051.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；
4. 继续分析数据包wireshark0051.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;
5. 继续分析数据包wireshark0051.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；
6. 继续分析数据包wireshark0051.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；
7. 继续分析数据包wireshark0051.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；
8. 继续分析数据包wireshark0051.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。

### B-4：网页渗透

**任务环境说明：**

* 服务器场景：Server2120（关闭链接）
* 服务器场景操作系统：未知
1. 访问服务器的网站主页，猜测后台数据库中本网页中应用的库名称长度，将长度作为flag提交；
2. 访问服务器的网站主页，猜测后台数据库中本网页中应用的库名称，将名称作为flag提交；
3. 访问服务器的网站主页，猜测后台数据库中本页面中应用的表名称长度，将表名称长度作为flag提交；
4. 访问服务器的网站主页，猜测后台数据库中本网页中应用的表名称，将名称作为flag提交
5. 访问服务器的网站主页，猜测后台数据库中本页面中第二个应用的字段名称，将名作为flag提交。
6. 访问服务器的网站主页，猜测后台数据库中本页面中ID为1的用户名，将用户名作为flag提交。

### B-5：服务渗透测试

**任务环境说明：**

* 服务器场景：Server2209（关闭链接）
* 服务器场景操作系统：未知
1. 使用渗透机对服务器信息收集，并将服务器中网站服务端口号作为flag提交；（若为多个用;隔开）
2. 使用渗透机对服务器信息收集，在服务器网站中找到爬虫文件，并将名称作为flag提交；
3. 使用渗透机对服务器信息收集，在服务器网页中找到flag并将内容提交；
4. 使用渗透机对服务器渗透，并将服务器的主机名作为flag提交；
5. 使用渗透机对服务器渗透，在服务器中找到具有执行权限的文件，在权限的文件中找到flag内容信息并提交；
6. 使用渗透机对服务器渗透，并将服务器中root目录下的flag文件作为flag提交。

### B-6：隐藏信息探索

**任务环境说明：**

* 服务器场景：FTPServer220509
* 服务器场景操作系统： Linux（关闭链接）
* FTP用户名：qdbgts密码：qdbgts
1. 访问服务器的FTP服务，下载图片QR，从图片中获取flag，并将flag提交；
2. 访问服务器的FTP服务，下载文件document，从文件中获取flag，并将flag提交；
3. 访问服务器的FTP服务，下载图片beach，从图片中获取flag，并将flag提交；
4. 访问服务器的FTP服务，下载图片grass，从图片中获取flag，并将flag提交；
5. 访问服务器的FTP服务，下载图片tree，从图片中获取flag，并将flag提交；
6. 访问服务器的FTP服务，下载压缩文件style，从压缩文件中获取flag，并将flag提交。

## （四）模块C CTF夺旗-攻击（本模块200分）

一、项目和任务描述：

假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，以便了解最新的攻击手段和技术，了解网络黑客的心态，从而改善您的防御策略。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

靶机服务器操作系统：Linux/Windows

三、漏洞情况说明：

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。

四、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.选手攻入靶机后不得对靶机进行关闭端口、修改密码、重启或者关闭靶机、删除或者修改flag、建立不必要的文件等操作；

4.在登录自动评分系统后，提交靶机服务器的flag值，同时需要指定靶机服务器的IP地址；

5.赛场根据难度不同设有不同基础分值的靶机，对于每个靶机服务器，前三个获得flag值的参赛队在基础分上进行加分，本阶段每个队伍的总分均计入阶段得分，具体加分规则参照赛场评分标准；

6.本环节不予补时。

## （五）模块D CTF夺旗-防御（本模块200分）

一、项目和任务描述：

假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，其他队不能访问。参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

堡垒服务器操作系统：Linux/Windows

三、漏洞情况说明：

1.堡垒服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.堡垒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.堡垒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.堡垒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。

四、注意事项：

1.每位选手需要对加固点和加固过程截图，并自行制作系统防御实施报告，最终评分以实施报告为准;

2.系统加固时需要保证堡垒服务器对外提供服务的可用性；

3.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；

4.本环节不予补时。

二、说明：

1.所有截图要求截图界面、字体清晰；

2.文件名命名及保存：网络安全模块D-XX（XX为工位号），PDF格式保存；

3.文件保存到U盘提交。