**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（5）**

**（总分100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。根据比赛实际情况，竞赛赛场实际使用赛题参数、表述及环境可能有适当修改，具体情况以实际比赛发放赛题为准。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） | 权值 |
| A | 基础设施设置与安全加固 | 3 | 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 | 3 | 20% |
| D | CTF夺旗-防御 | 20% |
| 总计 | | 6 | 100% |

二、竞赛注意事项

1.比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比赛环境，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。比赛结束后，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.比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（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**

# 模块A 基础设施设置与安全加固

**（本模块20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，并通过综合运用用户安全管理和密码策略、本地安全策略、日志安全审计、数据库安全策略、Web安全加固、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。本模块要求根据竞赛现场提供的A模块答题模板对具体任务的操作进行截图并加以相应的文字说明，以word文档的形式书写,以PDF格式保存，以“赛位号+模块A”作为文件名，PDF格式文档为此模块评分唯一依据。

二、服务器环境说明

Windows 用户名：administrator，密码：123456

Linux 用户名：root，密码：123456

三、具体任务（每个任务得分以电子答题卡为准）

**A-1任务一 登录安全加固（Windows）**

1.密码策略

a.密码策略必须同时满足大小写字母、数字、特殊字符；

b.强制密码历史为5个密码；

c.密码最长存留期为45天；

d.最小密码长度不少于8个字符。

2.用户安全管理

a.禁止普通用户使用注册表编辑工具以及Ctrl+Alt+Del；

b.交互式登录时不显示用户名；

c.设置取得文件或其他对象的所有权，将该权限只指派给administrators组；

d.禁止普通用户使用命令提示符;

e.设置不显示上次登录的用户名。

**A-2任务二 本地安全策略设置（Windows）**

3.关闭系统时清除虚拟内存页面文件；

4.禁止系统在未登录的情况下关闭；

5.禁止软盘复制并访问所有驱动器和所有文件夹；

6.禁止自动管理登录；

7.禁止显示上次登录的用户名。

**A-3任务三 日志安全审计（Windows）**

8.启用本地安全策略中对Windows系统的审核目录服务访问，仅需要审核失败操作；

9.启用本地安全策略中对Windows系统的审核特权使用，成功和失败操作都需要审核；

10.启用本地安全策略中对Windows系统的审核系统事件，成功和失败操作都需要审核；

11.启用本地安全策略中对Windows系统的审核帐户管理，成功和失败操作都要审核；

12.启用本地安全策略中对Windows系统的审核进程追踪，仅失败操作需要审核。

**A-4任务四 数据库加固（Linux）**

13.以普通帐户mysql安全运行mysql服务，禁止mysql以管理员帐号权限运行；

14.删除默认数据库(test)；

15.改变默认mysql管理员用户为:SuperRoot；

16.使用mysql内置MD5加密函数加密用户user1的密码为(P@ssw0rd1!)；

17.赋予user1用户对数据库所有表只有select,insert,delete,update权限。

**A-5任务五 Web安全加固（Linux）**

18.为了减轻网站负载，设置网站最大并发连接数为1000；

19.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；

20.关闭IIS的WebDAV功能增强网站的安全性。

**A-6任务六 防火墙安全策略（iptables）**

21.为确保安全Linux系统禁止所有人通过ssh连接除了172.16.1.1这个ip；

22.在工作时间，即周一到周五的8:30-18:00，开放本机的ftp服务给 192.168.1.0网络中的主机访问；

23.要求从ftp服务的数据下载请求次数每分钟不得超过 5 个；

24.拒绝 TCP 标志位全部为 1 及全部为 0 的报文访问本机；

25.配置iptables防火墙过滤规则，以封堵目标网段（172.16.1.0/24），并在两小时后解除封锁。

# 模块B 网络安全事件响应、数字取证调查和应用安全

**（本模块40分，每个子任务4分）**

### B-1任务一：Linux系统安全

\*任务说明：仅能获取Server1的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server1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22端口对应的服务版本信息字符串作为Flag值提交；

2.找到/var/www目录中的图片文件，将文件名称作为Flag值提交；

3.找到Flag1作为Flag值提交；

4.找到Flag2作为Flag值提交；

5.找到Flag3作为Flag值提交。

### B-2任务二：漏洞扫描与利用

\*任务说明：仅能获取Server2的IP地址

1.通过本地PC中渗透测试平台Kali对靶机场景Server2进行系统服务及版本扫描渗透测试，以xml格式向指定文件输出信息（使用工具Nmap），将以xml格式向指定文件输出信息必须要使用的参数作为Flag值提交；

2.在本地PC的渗透测试平台Kali中，使用命令初始化MSF数据库并将此命令作为Flag值提交；

3.在本地PC的渗透测试平台Kali中，打开MSF，使用db\_import将扫描结果导入到数据库中，并查看导入的数据，将查看该数据要使用的命令作为Flag值提交；

4.在MSF工具中用search命令搜索搜索MS08067漏洞利用模块，将回显结果中的漏洞公开时间作为Flag值（如：2017-10-16）提交；

5.在MSF工具中调用MS08067漏洞攻击模块，并检测靶机是否存在漏洞，将回显结果中最后一个单词作为Flag值提交。

### B-3任务三：Web安全应用

\*任务说明：仅能获取Server3的IP地址

1.通过渗透机扫描靶机中运行的服务，将完整的HTTP服务名称作为Flag值提交；

2.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/rececit/enehevibo.php，通过密码破译得到明文密码，并将明文密码作为Flag值提交；

3.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/irascence/futuresive.php，通过密码破译得到明文密码，并将明文密码作为Flag值提交；

4.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/economyia/tortly.php，通过密码破译进入新的页面，并将新页面的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

5.在新的页面中，通过解密页面内容获得密码，并将密码作为Flag值提交；

6.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/corticory/heseur.php，通过解密页面内容得到密码，并将密码作为Flag值提交。

### B-4任务四：流量分析

\*任务说明：仅能获取Server4的IP地址

1.通过Kali访问目标靶机http://xxx.xxx.xxx.xxx:8081(xxx.xxx.xxx.xxx为靶机IP地址,例如172.16.101.1:8081)下载文件获取流量包。将流量包进行解压，获取流量包中的文件名作为Flag值（形式：文件名.文件类型）提交；

2.通过Kali中利用wireshark从服务器场景Server4中下载的流量包进行流量包分析，使用HTTP模式下的过滤表达式过滤HTTP GET方法的流量包，过滤表达式命令作为Flag值提交；

3.根据第2步回显信息从过滤出的流量包中分析，找到Flag值文件流量的IP地址，并将该HTTP流量包（第1步中下载的流量包）含Flag值信息的请求源ip作为Flag值提交；

4.在渗透测试平台Kali中利用wireshark从包含Flag值信息的流量包中的IP数据包中找到目标信息文件，并将该文件名作为Flag值（形式：文件名.文件类型）提交；

5.在渗透测试平台Kali中使用wireshark分析下载的流量包，并从包含Flag值信息的GET/POST请求流量中找出响应IP及响应内容，并将该Flag值请求的响应IP（流量包中的IP）作为Flag值提交；

6.使用wireshark工具分析响应流量包（第5步Flag值请求对应的response响应流量数据包）中的数据内容，将该响应数据中的文件名，作为Flag值（形式：文件名.文件类型）提交；

7.使用wireshark工具提取流量包中内容（即第6步响应流量包中的文件内容），将该提取操作必须使用的到的wireshark功能的快捷键作为Flag值（xx+xx为Flag值提交格式,例如ctrl+alt+F4）提交；

8.将第7步提取出的文件进行解压，将该文件解压后的文件内容第一行作为Flag值提交。

### B-5任务五：FTP弱口令渗透测试

\*任务说明：仅能获取Server5的IP地址

1.在渗透机Kali2.0中使用Zenmap工具扫描服务器场景Server5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值提交（忽略ip地址）；

2.通过渗透机Kali2.0对服务器场景Server5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FTP服务对应的服务端口信息作为Flag值提交；

3.在渗透机Kali2.0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信息作为Flag值提交；

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值提交（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值提交；

6.在msf模块中指定密码字典，字典路径为/root/2.txt,用户名为test爆破获取密码并将得到的密码作为Flag值提交；

7.在上一题的基础上，使用第6题获取到的密码登陆ftp服务，将该目录中Flag值2.bmp的图片文件中的英文单词作为Flag值提交。

### B-6任务六：Web渗透测试

\*任务说明：仅能获取Server6的IP地址

1. 通过渗透机扫描同网段内网中的NBT服务（使用NBTscan工具），将执行内网扫描必须使用的参数作为Flag值提交；

2. 通过渗透机扫描靶机80  
HTTP服务的目录（使用字典dict.txt，使用工具DirBuster），将后台管理页面的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

3. 通过渗透机的火狐浏览器登入靶机HTTP站点的后台管理系统，找到后台管理系统中的漏洞位置，将漏洞位置的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

4. 通过渗透机对靶机漏洞进行渗透测试，将靶机数据库的库名作为Flag值提交；

5. 通过渗透机对靶机漏洞进行渗透测试，将靶机数据库的用户名作为Flag值提交；

6. 通过渗透机对靶机漏洞进行渗透测试，将靶机数据库的密码作为Flag值提交。

### B-7任务七：中间人攻击渗透测试

\*任务说明：仅能获取Server7的IP地址

\*任务说明：仅能获取Server11的IP地址

1.通过上题渗透后得到控制权限的服务器场景Server7进行查看本地的arp缓存表的操作，并将该操作所使用的命令作为Flag值提交；

2.通过上题渗透后得到控制权限的服务器场景Server7进行清除本地的arp缓存表的操作，并将该操作所使用的命令作为Flag值提交；

3.通过本地PC中渗透测试平台Kali对服务器场景Server7以及服务器场景Server11进行中间人攻击渗透测试，打开渗透测试平台Kali的路由转发功能，并将该配置文件的绝对路径作为Flag值提交；

4.通过本地PC中渗透测试平台Kali对服务器场景Server7以及服务器场景Server11进行中间人攻击渗透测试，通过arpspoof命令对客户端Server7以及服务器Server11进行arp污染 ，并将该操作必须要用到的参数作为Flag值提交；

5.中间人渗透攻击成功后，渗透测试平台kali能够监听到客户端Server7向服务器Server11中的login.php页面提交的登陆网站用户名，密码信息，使用服务器场景Server7桌面上的Chrome浏览器，访问Server11服务器场景的Web站点http://Linux靶机ip/login.php，使用已经保存好的用户名，密码直接登录，并在kali上使用抓包软件wireshark进行抓包，设置wireshark过滤规则，过滤所有请求方式为POST的http请求包，将需要使用的过滤器表达式作为Flag值（==符号前后不要加空格）提交；

6.分析抓到的POST请求包，并将POST请求内容中客户端Server7向服务器Server11中的login.php页面提交的登陆网站admin用户的密码作为Flag值提交。

### B-8任务八：隐写术应用

\*任务说明：仅能获取Server8的IP地址

1.找出文件夹1中的文件，将文件中的隐藏信息作为Flag值提交；

2.找出文件夹2中的文件，将文件中的隐藏信息作为Flag值提交；

3.找出文件夹3中的文件，将文件中的隐藏信息作为Flag值提交；

4.找出文件夹4中的文件，将文件中的隐藏信息作为Flag值提交；

5.找出文件夹5中的文件，将文件中的隐藏信息作为Flag值提交。

### B-9任务九：文件上传渗透测试

\*任务说明：仅能获取Server9的IP地址

1.通过渗透机Kali2.0对服务器场景Server9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；

2.通过渗透机Kali2.0对服务器场景Server9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；

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；

4.通过渗透机Kali2.0对服务器场景Server9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；

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；

6.通过渗透机Kali2.0对服务器场景Server9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；

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；

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。

### B-10任务十：主机发现与信息收集

\*任务说明：仅能获取Server10的IP地址

1.通过渗透机Kali2.0对靶机场景进行秘密FIN扫描 (使用Nmap工具)，并将该操作使用命令中必须要使用的参数作为Flag值提交；

2.通过渗透机Kali2.0对靶机场景进行秘密FIN扫描 (使用Nmap工具)，并将该操作显示结果中从下往上数第7行的端口信息作为Flag值提交；

3.通过渗透机Kali2.0对靶机场景进行圣诞树（Xmas Tree）扫描（使用Nmap工具），并将该操作使用命令中必须要使用的参数作为Flag值提交；

4.通过渗透机Kali2.0对靶机场景进行圣诞树（Xmas Tree）扫描（使用Nmap工具），并将该操作显示结果中从下往上数第5行的服务名称作为Flag值提交；

5.通过渗透机Kali2.0对靶机场景使用SYN包而不是用ACK包进行扫描渗透测试（使用Nmap工具），并将该操作使用命令中必须要使用的参数作为Flag值提交；

6.通过渗透机Kali2.0对靶机场景使用SYN包而不是用ACK包进行扫描渗透测试（使用Nmap工具），并将该操作显示结果中从下往上数第8行的服务状态作为Flag值提交；

7.通过渗透机Kali2.0对靶机场景进行ACK和ICMP两种扫描类型并行的扫描渗透测试（使用Nmap工具）,并将该操作使用命令中必须要使用的参数作为Flag值提交；

8.通过渗透机Kali2.0对靶机场景进行ACK和ICMP两种扫描类型并行的扫描渗透测试（使用Nmap工具）,并将该操作显示结果中从下往上数第3行的服务名称作为Flag值提交。

# 模块C CTF夺旗-攻击

**（本模块20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攻击机。

二、操作系统环境说明：

客户机操作系统：Windows 10

攻击机操作系统：Kali Linux 2019版

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。

# 模块D CTF夺旗-防御

**（本模块20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。

每位选手按照发现需要加固点、实施加固和检验加固成效等步骤实施系统防御。完成防护工作后，每队选手需要按照实施步骤必要文字说明配以关键过程或者关键操作结果截图的形式，自行制作系统防御实施报告。实施报告以word文档的形式书写,以PDF格式保存，以“赛位号+模块D”作为文件名，PDF格式文档为此模块评分唯一依据。

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需要加固的堡垒服务器。

二、操作系统环境说明：

客户机操作系统：Windows 10

攻击机操作系统：Kali Linux 2019版

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.系统加固时需要保证堡垒服务器对外提供服务的可用性；

2.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；

3.本环节不予补时。