**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（1）**

**（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，并通过综合运用登录安全加固、数据库安全策略、流量完整性策略、事件监控策略、防火墙策略、IP协议安全配置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

1.密码策略（Windows，Linux）

a.设置最短密码长度为15；

b.一分钟内仅允许4次登录失败，超过4次，登录帐号锁定1分钟。

2.用户安全管理

a.设置user1用户只能在上班时间（周一至周五的9:00~18:00可以登录，将user1的登录时间配置界面截图；

b.在组策略中只允许管理员账号从网络访问本机；

c.设置操作系统中的关键目录（system32、hosts、Program Files、Perflogs）的权限为最优状态，即仅允许管理员用户进行读取及运行。

### A-2任务二 数据库安全策略

3.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；

4.删除默认数据库(test)；

5.改变默认mysql管理员用户为:SuperRoot；

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

### A-3任务三 流量完整性

7.对Web网站进行HTTP重定向HTTPS设置，仅使用HTTPS协议访问网站（Windows）(注：证书颁发给test.com 并通过https://www.test.com访问Web网站)。

### A-4任务四 事件监控

8.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。

### A-5任务五 防火墙策略

9.Windows系统禁用445端口；

10.Windows系统禁用23端口；

11.Linux系统使用iptables禁用23端口；

12.Linux系统使用iptables禁止别人ping通。

### A-6任务六 IP协议安全配置

13.指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为5；

14.指定处于SYN\_RCVD状态的TCP连接数的阈值为500；

15.指定处于至少已发送一次重传的SYN\_RVCD状态中的TCP连接数的阈值为400。

# 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：主机发现与信息收集

\*任务说明：仅能获取Server1的IP地址

1.通过渗透机Kali2.0对靶机场景进行TCP同步扫描 (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TCP同步扫描 (使用Nmap工具)，并将该操作显示结果中从下往上数第4行的服务器信息作为Flag值提交；

3.通过渗透机Kali2.0对靶机场景不ping主机进行扫描（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对靶机场景不ping主机进行扫描（使用Nmap工具），并将该操作显示结果中从下往上数第10行的“：”后的数字作为Flag值提交；

5.通过渗透机Kali2.0对靶机场景进行UDP扫描渗透测试只扫描53，111端口（使用Nmap工具），并将该操作显示结果中111端口的状态信息作为Flag值提交；

6.通过渗透机Kali2.0对靶机场景进行滑动窗口扫描渗透测试（使用Nmap工具），并将该操作使用的命令中必须要使用的参数作为Flag值提交；

7.通过渗透机Kali2.0对靶机场景进行RPC扫描扫描渗透测试（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RPC扫描扫描渗透测试（使用Nmap工具）,并将该操作显示结果中从下往上数第7行的服务信息作为Flag值提交。

### B-2任务二：数据分析数字取证

\*任务说明：仅能获取Server2的IP地址

1.使用Wireshark查看并分析Server2桌面下的attack.pcapng数据包文件，通过分析数据包attack.pcapng找出恶意用户的IP地址，并将恶意用户的IP地址作为Flag值（形式：[IP地址]）提交；

2.继续查看数据包文件attack.pacapng，分析出恶意用户扫描了哪些端口，并将全部的端口号从低到高作为Flag值（形式：[端口名1，端口名2，端口名3…，端口名n]）提交；

3.继续查看数据包文件attack.pacapng分析出恶意用户最终获得的用户名是什么，并将用户名作为Flag值（形式：[用户名]）提交；

4.继续查看数据包文件attack.pacapng分析出恶意用户最终获得的密码是什么，并将密码作为Flag值（形式：[密码]）提交；

5.继续查看数据包文件attack.pacapng分析出恶意用户连接一句话木马的密码是什么，并将一句话密码作为Flag值（形式：[一句话密码]）提交；

6.继续查看数据包文件attack.pacapng分析出恶意用户下载了什么文件，并将文件名及后缀作为Flag值（形式：[文件名.后缀名]）提交；

7.继续查看数据包文件attack.pacapng将恶意用户下载的文件里面的内容作为Flag值（形式：[文件内容]）提交。

### B-3任务三：SSH弱口令渗透测试

\*任务说明：仅能获取Server3的IP地址

1.在渗透机Kali2.0中使用Zenmap工具扫描靶机场景所在网段(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对靶机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SSH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（之间以英文逗号分隔，例hello,test，..,..）提交；

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值提交。

### B-4任务四：Web安全应用

\*任务说明：仅能获取Server4的IP地址

1.通过渗透机访问靶机的HTTP服务，扫描获取HTTP服务中的任务入口地址（使用字典directories.txt），并将任务入口的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

2.通过渗透机访问靶机的HTTP服务，并访问任务入口地址，分析页面内容并获得密码，将密码作为Flag值提交；

3.通过渗透机访问靶机的HTTP服务，将题目2中获得的密码进行解密，由此访问新的任务入口，分析页面内容并获得密码，将密码作为Flag值提交；

4.通过渗透机访问靶机的HTTP服务，将题目3中获得的密码进行解密，将解密后的密码作为Flag值提交；

5.通过渗透机的火狐浏览器访问地址http://靶机IP/aredil/taherice.php，分析页面内容并获得密码，将密码作为Flag值提交；

6.通过渗透机的火狐浏览器访问地址http://靶机IP/secam/erahegi.php，分析页面内容并获得密码，将密码作为Flag值提交。

### B-5任务五：文件MD5校验

\*任务说明：仅能获取Server5的IP地址

1.进入虚拟机操作系统：Server5中的/root目录，找到test.txt文件，并使用md5sum工具来计算出该文件的md5值，并将计算该文件md5的命令的字符串作为Flag值提交；

2.进入虚拟机操作系统：Server5中的/root目录，找到test.txt文件，并使用md5sum校验工具来计算出该文件的md5值，并将计算该文件得到的md5值的字符串中前6位作为Flag值提交；

3.进入虚拟机操作系统：Server5中的/root目录，将test.txt文件的文件名称改为txt.txt，然后再使用md5sum工具计算txt.txt文件的md5值，并将计算该文件得到的md5值的字符串中前5位数字和之前test.txt文件md5值的字符串中前5位数字相减的结果作为Flag值提交；

4.进入虚拟机操作系统：Server5，使用md5sum工具来计算/etc/passwd文件的md5值，并将改md5值导入到passwd.md5文件中，并将该命令的字符串作为Flag值提交；

5.进入虚拟机操作系统：Server5，创建一个新的用户，用户名为user6，密码为123456。再次计算/etc/passwd的md5值，并将该值与passwd.md5文件中的值进行对比，并将添加用户后/etc/passwd文件的md5值的字符串中前三位数字和之前/etc/passwd文件md5值的字符串中前三位数字相减的结果作为Flag值提交。

### B-6任务六：Windows系统安全

\*任务说明：仅能获取Server6的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server6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端口对应的服务状态信息字符串作为Flag值提交；

2.将首选DNS服务器地址作为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.将系统最高权限管理员账户的密码作为Flag值提交。

### B-7任务七：渗透测试

\*任务说明：仅能获取Server7的IP地址

1.通过本地PC中渗透测试平台Kali对靶机场景Server7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MS17010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MS17010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-8任务八：JS文件上传绕过

\*任务说明：仅能获取Server8的IP地址

1.访问靶机网站http://靶机IP/scrg/，将文件上传页面完整URL作为Flag值（形式：http://172.16.1.1/页面路径）提交；

2.分析文件上传页面，将验证文件格式的函数名称作为Flag值提交；

3.获取靶机FTP服务下php文件，上传php文件，将修改后的Content-Type信息作为Flag值提交；

4.分析文件上传时的数据包，将文件上传后的路径作为Flag值（形式：http://172.16.1.1/文件路径）提交；

5.将靶机网站服务所使用的ServerAPI值作为Flag值提交；

6.将靶机网站服务所使用的版本号作为Flag值提交。

### B-9任务九：内存取证

\*任务说明：仅能获取Server9的IP地址

1.从内存文件中找到异常程序的进程，将进程的名称作为Flag值提交；

2.从内存文件中找到黑客将异常程序迁移后的进程编号，将迁移后的进程编号作为Flag值提交；

3.从内存文件中找到受害者访问的网站恶意链接，将网站的恶意链接作为Flag值提交；

4.从内存文件中找到异常程序植入到系统的开机自启痕迹，使用Volatility工具分析出异常程序在注册表中植入的开机自启项的Virtual地址，将Virtual地址作为Flag值提交；

5.从内存文件中找到异常程序植入到系统的开机自启痕迹，将启动项最后一次更新的时间作为Flag值（只提交年月日，例如：20210314）提交。

### B-10任务十：Linux系统安全

\*任务说明：仅能获取Server10的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server10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。

# 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

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

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。