**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（7）**

**（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：WEB安全加固（Windows）

3.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;

4.限制目录执行权限,对picture和upload目录设置执行权限为无；

5.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)。

### A-3任务三：日志监控（Windows）

6.安全日志文件大小至少为128MB，设置当达到最大的日志大小上限时，覆盖早于30天的日志；

7.应用日志文件大小至少为64MB，设置当达到最大的日志大小上限时，覆盖早于15天的日志；

8.系统日志大小至少为32MB，设置当达到最大的日志大小上限时，按需要覆盖事件。

### A-4任务四：数据库加固（Linux）

9.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；

10.删除默认数据库(test)；

11.改变默认mysql管理员用户为:SuperRoot；

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

13.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：中间件安全加固SSHD\VSFTPD\IIS（Windows, Linux）

14.SSHD服务加固

a.修改SSH连接界面静置时间;

b.修改登录记录的等级为INFO;

c.禁止登陆后显示信息。

15.VSFTPD服务加固

a.同一客户机IP地址允许最大客户端连接数10；

b.最大客户端连接数为100；

c.设置数据连接的超时时间为2分钟；

d.设置本地用户创建文件的权限为022。

16.IIS服务加固

a.关闭FTP匿名访问；

b为了解决IIS短文件名漏洞，设置URL序列为~；

c.设置网站最大并发连接数为10。

**A-6任务六：防火墙安全策略（iptables）**

17.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；

18.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；

19.要求从ftp服务的数据下载请求次数每分钟不得超过 5 个；

20.拒绝 TCP 标志位全部为 1 及全部为 0 的报文访问本机；

21.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：信息收集与利用

\*任务说明：仅能获取Server1的IP地址

1.在渗透机Kali2.0中使用autoscan工具扫描服务器场景Server1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值提交；

2.在渗透机Kali2.0中使用nmap工具进行UDP扫描服务器场景Server1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值（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值；

3.在渗透机Kali2.0中调用snmpwalk工具测试服务器场景Server1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值（各参数之间用英文分号分割，例a;b）提交；

4.在渗透机Kali2.0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值（提交答案时IP以192.168.100.10代替，使用默认字典snmp.passwd）提交；

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值提交；

6.在渗透机Kali2.0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值（提交的命令为忽略IP后必须使用的命令，字典名字为dict.txt）提交；

7.在渗透机Kali2.0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值提交；

8.在渗透机Kali2.0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值提交；

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值（各用户之间用英文分号分割，例root;user）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.分析Server2桌面下的Alpha-1.pcapng数据包文件，通过分析数据包Alpha-1.pcapng找出恶意用户第一次访问服务器的数据包是第几号，并将该号数作为Flag值提交；

2.继续查看数据包文件Alpha-1.pcapng，分析出恶意用户扫描了哪些端口，并将全部的端口号从小到大作为Flag值（形式：端口1,端口2,端口3…,端口n）提交；

3.继续查看数据包文件Alpha-1.pcapng分析出恶意用户登陆后台所用的用户名是什么，并将用户名作为Flag值提交；

4.继续查看数据包文件Alpha-1.pcapng分析出恶意用户在第几个数据包到第几个数据包之间利用了MIME漏洞，并将该数据包之间的号数作为Flag值（格式：1,30）提交；

5.继续查看数据包文件Alpha-1.pcapng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值提交；

6.继续查看数据包文件Alpha-1.pcapng分析出恶意用户第二次写入一句话木马是在哪个路径，并将改路径以及文件名和后缀作为Flag值提交；

7.继续查看数据包文件Alpha-1.pcapng分析出恶意用户下载了什么文件，并将该文件内容作为Flag值提交。

### B-3任务三：Windows系统安全

\*任务说明：仅能获取Server3的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server3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-4任务四：隐写术应用

\*任务说明：仅能获取Server4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-5任务五：PE Reverse**

\*任务说明：仅能获取Server5的IP地址

1.对靶机服务器场景桌面上的PE01.exe二进制文件进行静态调试，将main函数的入口地址作为Flag值提交；

2.对靶机服务器场景桌面上的PE01.exe二进制文件进行静态调试，将该二进制文件中检查许可证的关键函数作为Flag值提交；

3.对靶机服务器场景桌面上的PE01.exe二进制文件进行静态调试，找到Flag1值并提交；

4.对靶机服务器场景桌面上的PE01.exe二进制文件进行静态调试，尝试破解该二进制文件，将注册成功后的回显信息作为Flag值提交；

5.对靶机服务器场景桌面上的PE01.exe二进制文件进行静态调试，将该激活所需的许可证码作为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.获取PHP的版本号作为Flag值（例如：5.2.14）提交；

2.获取MySQL数据库的版本号作为Flag值（例如：5.0.22）提交；

3.获取系统的内核版本号作为Flag值（例如：2.6.18）提交；

4.获取网站后台管理员admin用户的密码作为Flag值提交；

5.找到/root目录中的txt文件，将文件内容作为Flag值提交。

**B-7任务七：MS15034漏洞扫描与利用**

\*任务说明：仅能获取Server7的IP地址

1.在MSF工具中用search命令搜索MS15034HTTP.SYS漏洞拒绝服务攻击模块，将回显结果中的漏洞披露时间作为Flag值（如：2015-10-16）提交；

2.在MSF工具中调用MS15034HTTP.SYS漏洞的辅助扫描模块，将调用此模块的命令作为Flag值提交；

3.使用set命令设置目标IP，并检测漏洞是否存在，运行此模块，将回显结果中倒数第2行的最后一个单词作为Flag值提交；

4.在MSF工具中调用并运行MS15034HTTP.SYS漏洞的拒绝服务攻击模块，将运行此模块后回显结果中倒数第1行的最后一个单词作为Flag值提交；

5.进入靶机在IIS网站下的编辑输出缓存设置中禁止启用内核缓存，再次运行MS15034HTTP.SYS漏洞的拒绝服务攻击模块，运行此模块并将回显结果中倒数第2行的最后一个单词作为Flag值提交。

### B-8任务八：SSH弱口令渗透测试

\*任务说明：仅能获取Server8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（忽略ip地址）提交；

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-9任务九：Linux系统安全

\*任务说明：仅能获取Server9的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server9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-10任务十：JS文件上传绕过**

\*任务说明：仅能获取Server10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。

# 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。