**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（4）**

**（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、服务安全配置、日志安全审计、中间件安全配置、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.更改或创建密码时执行复杂性要求；

b.密码必须符合复杂性要求；

c.密码最短使用期限为10天。

2.用户安全管理

a.禁用来宾账户，禁止来宾用户访问计算机或访问域的内置账户；

b.查找并删除服务器中可能存在的后门用户；

c.普通用户进行最小权限管理，对关闭系统仅限管理员账号；

d.禁止从远端系统强制关机，将该权限只指派给administrators组。

### A-2任务二 本地安全策略（Windows）

3.要求登录时不显示用户名；

4.在密码过期的前5天开始提示用户在过期之前更改密码；

5.要求任何用户在登录到Windows前都必须按CTRL+ALT+DEL；

6.禁止SAM 帐户和共享的匿名枚举；

7.禁用来宾帐户。

### A-3任务三 服务安全配置（Windows）

8.禁用TCP/IP上的NetBIOS协议，关闭监听的 UDP 137（netbios-ns）、UDP 138（netbios-dgm）以及 TCP 139（netbios-ssn）端口；

9.在本地策略里配置禁用未登陆前关机；

10.设置从屏幕保护恢复时需要输入密码，并将屏幕保护自动开启时间设定为五分钟；

11.对于远程登录的帐户，设置不活动超过时间5分钟自动断开连接。

### A-4任务四 日志安全审计（Windows）

12.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；

13.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；

14.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。

### A-5任务五 中间件安全加固SSHD\VSFTPD\IIS（Windows, Linux）

15．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。

16．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。

17．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 防火墙策略（Windows）

18.禁止任何机器ping本机；

19.禁止本机ping任何机器；

20.拒绝 TCP 标志位全部为 1 及全部为 0 的报文访问本机；

21.禁止转发来自MAC地址为29:0E:29:27:65:EF主机的数据包。

# 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：数据库渗透测试

\*任务说明：仅能获取Server2的IP地址

1.在渗透机Kali2.0中使用zenmap工具扫描服务器场景Server2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1433、3306、80端口。并将该操作使用的命令中必须要使用的字符串作为Flag值提交；

2.通过渗透机Kali2.0对服务器场景Server2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数据库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爆破获取密码并将得到的密码作为Flag值提交；

7.在msf模块中切换新的渗透模块，对服务器场景server2003进行数据库服务扩展存储过程进行利用，将调用该模块的命令作为Flag值提交；

8.在上一题的基础上，使用第6题获取到的密码并进行提权，同时使用show options命令查看需要的配置，并配置CMD参数来查看系统用户，将配置的命令作为Flag值提交；

9.在利用msf模块获取系统权限并查看目标系统的异常（黑客）用户，并将该用户作为Flag值提交。

### B-3任务三：远程文件包含

\*任务说明：仅能获取Server3的IP地址

1.扫描靶机服务器，将靶机FTP服务版本作为Flag值提交；

2.进入靶机网站http://靶机IP/rfi/将靶机文件传输服务下的图片木马文件上传，将文件上传后的URL地址作为Flag值（形式：http://192.168.1.1/文件路径）提交；

3.查看/etc/passwd文件内容，将uid为10003的用户名作为Flag值提交；

4.执行靶机文件传输服务中的php文件，将输出的弹窗信息作为Flag值提交；

5.下载靶机文件传输服务中php文件，填充内容。执行完善的php文件，将完整的URL作为Flag值（形式：http://192.168.1.1/页面路径）提交；

6.查看靶机内核版本，将靶机内核版本作为Flag值提交。

### B-4任务四：Windows系统安全

\*任务说明：仅能获取Server4的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server4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-5任务五：MYSQL信息收集

\*任务说明：仅能获取Server5的IP地址

1.通过渗透机场景Kali中的渗透测试工具对服务器场景MySQL03进行服务信息扫描渗透测试（使用Nmap工具），并将该操作显示结果中数据库版本信息作为Flag值提交；

2.通过渗透机场景Kali中的渗透测试工具对服务器场景MySQL03的数据库进行暴力破解，并将数据库的密码作为Flag值（字典/root/mysql03.txt）提交；

3.通过渗透机场景Kali对服务器场景MySQL03的数据库进行远程连接，并将数据库中库的数量作为Flag值提交；

4.通过渗透机场景Kali对服务器场景MySQL03的数据库进行状态查询，并将数据库状态中的版本作为Flag值提交；

5.通过渗透机场景Kali对服务器场景MySQL03中数据库进行查询当前使用的数据库，并将数据库名称作为Flag值提交；

6.通过渗透机场景Kali对服务器场景MySQL03中数据库进行数据库的所有用户信息查询，并将倒数第二个用户名作为Flag值提交；

7.通过渗透机场景Kali对服务器场景MySQL03中数据库进行数据文件存放路径查询，并将存放路径作为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：Web安全应用

\*任务说明：仅能获取Server7的IP地址

1.通过渗透机扫描靶机的端口（使用Nmap工具），将HTTP服务的服务名称作为Flag值提交；

2.使用渗透机的火狐浏览器访问靶机HTTP服务根目录，根据页面提示寻找注入点，将注入点的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

3.通过靶机Web应用服务的注入点，对其进行渗透测试，将当前Web应用服务使用的数据库名作为Flag值提交；

4.对靶机注入点进行渗透测试，将当前Web应用服务使用的数据库中第2个表（使用字母a-z顺序进行排序）的表名作为Flag值提交；

5.通过渗透机访问靶机HTTP服务，获取该站点后台管理员用户的密码，并将密码作为Flag值提交。

### B-8任务八：数据分析数字取证

\*任务说明：仅能获取Server8的IP地址

1.分析Server8桌面下的Bravo-1.pcapng数据包文件，通过分析数据包Bravo-1.pcapng找出恶意用户目录扫描的第2个目录名，并将该目录名作为Flag值提交;

2.继续查看数据包文件Bravo-1.pcapng，分析出恶意用户通过哪个目录写入的一句话木马，并将该目录名作为Flag值提交;

3.继续查看数据包文件Bravo-1.pcapng分析出恶意用户读取了服务器什么文件，并将该文件名及后缀作为Flag值提交;

4.继续查看数据包文件Bravo-1.pcapng分析出恶意用户写入一句话木马的路径是什么，并将该路径作为Flag值提交;

5.继续查看数据包文件Bravo-1.pcapng分析出恶意用户连接一句话木马的密码是什么，并将一句话木马作为Flag值提交;

6.继续查看数据包文件Bravo-1.pcapng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值提交;

7.继续查看数据包文件Bravo-1.pcapng将Web服务器连接的数据库名作为Flag值提交。

### B-9任务九：CVE-2019-0708漏洞利用

\*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对靶机场景Server1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CVE-2019-0708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CVE-2019-0708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-10任务十：Wireshark数据包分析

\*任务说明：仅能获取Server10的IP地址

1.使用Wireshark查看并分析PYsystem20191桌面下的capture4.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capture4.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capture4.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capture4.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capture4.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capture4.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capture4.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capture4.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。

# 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。