2021 年全国职业院校技能大赛（中职组）

网络安全竞赛试题

（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，企业服务器可能被黑客攻击，进行了未知操作，为了确保服务器正常运行，请按照网络安全岗位实施规范，进行相关操作。通过综合运用登录和密码策略、数据库安全策略、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。本模块要求对具体任务的操作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,以赛位号作为文件名。

二、服务器环境说明

Windows 用户名：administrator，密码：P@ssw0rd

Windows Server 2008

Linux 用户名：root，密码：123456

CentOS 7

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，Linux）

请对服务器 Windows、Linux 按要求进行相应的设置，提高服务器的安全性。Windows Server 2008 R2 SP1 Standard

1.密码策略（Windows，Linux）

a.密码策略必须同时满足大小写字母、数字、特殊字符；

b.最小密码长度不少于 8 个字符。

2.登录策略

a.设置账户锁定阈值为 6 次错误锁定账户，锁定时间为 1 分钟，复位账户锁定计数器为 1 分钟之后；（Windows）

b.一分钟内仅允许 5 次登录失败，超过 5 次，登录帐号锁定 1 分钟。（Linux）

3.用户安全管理(Windows)

a.禁止发送未加密的密码到第三方 SMB 服务器；

b.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。

A-2 任务二 本地安全策略设置（Windows）

4.关闭系统时清除虚拟内存页面文件；

5.禁止系统在未登录的情况下关闭；

6.禁止软盘复制并访问所有驱动器和所有文件夹；

7.禁止显示上次登录的用户名。

A-3 任务三 流量完整性保护（Windows，Linux）

8.创建 www.chinaskills.com 站点，在 C:\web 文件夹内中创建名称为 chinaskills.html 的主页，主页显示内容“热烈庆祝 2021 年全国职业技能大赛开幕”，同时只允许使用 SSL 且只能采用域名（域名为 www.test.com）方式进行访问；

9.为了防止密码在登录或者传输信息中被窃取，仅使用证书登录 SSH（Linux）。

A-4 任务四 事件监控（Windows）

10.应用程序日志文件最大大小达到 65M 时将其存档，不覆盖事件。

A-5 任务五 服务加固 SSH\VSFTPD\IIS（Windows，Linux）

11.SSH 服务加固（Linux）

a.SSH 禁止 root 用户远程登录；

b.设置 root 用户的计划任务。每天早上 7:50 自动开启 SSH 服务，22:50 关闭；每周六的 7:30 重新启动 SSH 服务；

c.修改 SSH 服务端口为 2222。

12.VSFTPD 服务加固（Linux）

a.设置数据连接的超时时间为 2 分钟；

b.设置站点本地用户访问的最大传输速率为 1M。

13.IIS 加固（Windows）

a.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；

b.关闭 IIS 的 WebDAV 功能增强网站的安全性。

A-6 任务六 防火墙策略（Linux）

14.只允许转发来自 172.16.0.0/24 局域网段的 DNS 解析请求数据包；

15.禁止任何机器 ping 本机；

16.禁止本机 ping 任何机器；

17.禁用 23 端口；

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

19.为防御 IP 碎片攻击，设置 iptables 防火墙策略限制 IP 碎片的数量，仅允许每秒处理 1000 个；

20.为防止 SSH 服务被暴力枚举，设置 iptables 防火墙策略仅允许 172.16.10.0/24 网段内的主机通过 SSH 连接本机。

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）

一、项目和任务描述：

假定你是某网络安全技术支持团队成员，某企业的服务器系统被黑客攻击，你的团队前来帮助企业进行调查并追踪本次网络攻击的源头，分析黑客的攻击方式，发现系统漏洞，提交网络安全事件响应报告，修复系统漏洞，删除黑客在系统中创建的后门，并帮助系统恢复正常运行。

二、服务器环境参考（以实际赛题为准）

操作系统：Windows/Linux

三、PC机环境参考（以实际赛题为准）

物理机：Windows7或Windows10；

虚拟机1：Ubuntu Linux（用户名：root；密码：toor），安装工具集：Backtrack5,安装开发环境：Python3；

虚拟机2：Kali1.0（用户名：root；密码：toor）；

虚拟机3：Kali2.0（用户名：root；密码：toor）；

虚拟机4：WindowsXP（用户名：administrator；密码：123456）。

四、具体任务

任务说明：Flag格式：Flag{Xxxx123}，括号中的内容作为Flag值，提交Xxxx123即可

B-1 任务一：内存取证

*任务说明：Server1 用户名：administrator，密码：123456

1.从内存文件中获取到用户 admin 的密码并且破解密码，将破解后的密码作为 Flag 值提交；

2.获取当前系统的主机名，将主机名作为 Flag 值提交；

3.获取当前系统浏览器搜索过的关键词，作为 Flag 提交；

4.当前系统中存在的挖矿进程，请获取指向的矿池地址，将矿池的 IP 地址作为 Flag 值提交；

5.恶意进程在系统中注册了服务，请将服务名作为 Flag 值提交。

6.从内存文件中获取黑客进入系统后下载的图片，将图片中的内容作为 Flag 值提交。

B-2 任务二：流量分析

*任务说明：Server1 用户名：administrator，密码：123456

1.使用 Wireshark 查看并分析 Server1 桌面下的 capture.pcapng 数据包文件，找到黑客的 IP 地址，并将黑客的 IP 地址作为 Flag 值（如：172.16.1.1）提交；

2.继续分析 capture.pcapng 数据包文件，找出黑客通过工具对目标服务器的哪些服务进行了密码暴力枚举渗透测试，将服务对应的

端口依照从小到大的顺序依次排列作为 Flag 值（如：77/88/99/166/1888）提交；

3.继续分析 capture.pcapng 数据包文件，找出黑客已经获取到目标服务器的基本信息，请将黑客获取到的目标服务器主机名作为 Flag 值提交；

4.继续分析 capture.pcapng 数据包文件，找出黑客成功破解了哪个服务的密码，并将该服务的版本号作为 Flag 值(如：5.1.10)提交；

5.继续分析 capture.pcapng 数据包文件，黑客通过数据库写入了木马,将写入的木马名称作为 Flag 值提交（名称不包含后缀）；

6.继续分析 capture.pcapng 数据包文件，黑客通过数据库写入了木马,将黑客写入的一句话木马的连接密码作为 Flag 值提交；

7.继续分析 capture.pcapng 数据包文件，找出黑客连接一句话木马后查看了什么文件，将黑客查看的文件名称作为 Flag 值提交；

8.继续分析 capture.pcapng 数据包文件，黑客可能找到异常用户后再次对目标服务器的某个服务进行了密码暴力枚举渗透,成功破解出服务的密码后登录到服务器中下载了一张图片,将图片文件中的英文单词作为 Flag 值提交。

B-3 任务三：渗透测试

*任务说明：Server1 用户名：administrator，密码：123456

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MS17010漏洞利用模块，将回显结果中的漏洞公开时间作为Flag值提交；（如：2017-10-16）

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-4 任务四：Python代码分析

*任务说明：Server1 用户名：administrator，密码：123456

1.完善Server1桌面上的Flag.py文件，填写该文件当中空缺的Flag1字符串，并将该字符串作为Flag值提交；

2.继续完善Flag.py文件，填写该文件当中空缺的Flag2字符串，并将该字符串作为Flag值提交；

3.继续完善Flag.py文件，填写该文件当中空缺的Flag3字符串，

并将该字符串作为 Flag 值提交；

4.继续完善Flag.py 文件,填写该文件当中空缺的Flag4 字符串，并将该字符串作为 Flag 值提交；

5.将完善好的脚本文件在 Kali2.0 上执行,将执行成功后的回显内容作为 Flag 值提交。

B-5 任务五：隐写术应用

*任务说明：Server2 用户名：administrator，密码：123456

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-6 任务六：Web 安全应用

*任务说明：仅能获取 Server3 的 IP 地址

1.获取 PHP 的版本号作为 Flag 值提交；（例如：5.2.14）

2.获取 MySQL 数据库的版本号作为 Flag 值提交;（例如:5.0.22）

3.获取系统的内核版本号作为 Flag 值提交；（例如：2.6.18）

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：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.找到 Flag3 作为 Flag 值提交；

6.将系统最高权限管理员账户的密码作为 Flag 值提交。

B-8 任务八：Linux 系统安全

*任务说明：仅能获取 Server5 的 IP 地址

1.通过本地 PC 中渗透测试平台 Kali 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 22 端口对应的服务状态信息字符串作为 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；

6.找到 Flag4 作为 Flag 值提交。

B-9 任务九：缓冲区溢出

*任务说明：仅能获取 Server6 的 IP 地址，Server6 FTP 服务用户名：admin，密码：123456

1.从靶机服务器场景 FTP 服务器中下载文件 B0.py，编辑该 Python 程序文件，使该程序实现对 Server6 进行缓冲区溢出渗透测试的功能，填写该文件当中空缺的 F1 字符串，将该字符串作为 Flag 值提交；

2.继续编辑命名为 B0.py 的 Python 程序文件，使该程序实现对 Server6 进行缓冲区溢出渗透测试的功能，填写该文件当中空缺的 F2

字符串，将该字符串作为 Flag 值提交；

3.继续编辑命名为 B0.py 的 Python 程序文件，使该程序实现对 Server6 进行缓冲区溢出渗透测试的功能，填写该文件当中空缺的 F3 字符串，将该字符串作为 Flag 值提交；

4.继续编辑命名为 B0.py 的 Python 程序文件，使该程序实现对 Server6 进行缓冲区溢出渗透测试的功能，填写该文件当中空缺的 F4 字符串，将该字符串作为 Flag 值提交；

5.继续编辑命名为 B0.py 的 Python 程序文件，使该程序实现对 Server6 进行缓冲区溢出渗透测试的功能，成功渗透后找到 Server6 回收站内的文档，将文档内容作为 Flag 值提交。

B-10 任务十：远程代码执行

*任务说明：仅能获取 Server7 的 IP 地址，Server7 FTP 服务用户名：admin，密码：123456

1.从靶机服务器场景 FTP 服务器中下载文件 RCE.py，编辑该 Python 程序文件，使该程序实现对 Server7 进行远程代码执行渗透测试的功能，填写该文件当中空缺的 F1 字符串，将该字符串作为 Flag 值提交；

2.继续编辑命名为 RCE.py 的 Python 程序文件，使该程序实现对 Server7 进行远程代码执行渗透测试的功能，填写该文件当中空缺的 F2 字符串，将该字符串作为 Flag 值提交；

3.继续编辑命名为 RCE.py 的 Python 程序文件，使该程序实现对 Server7 进行远程代码执行渗透测试的功能，填写该文件当中空缺的 F3 字符串，将该字符串作为 Flag 值提交；

4.继续编辑命名为 RCE.py 的 Python 程序文件，使该程序实现对 Server7 进行远程代码执行渗透测试的功能，填写该文件当中空缺的 F4 字符串，将该字符串作为 Flag 值提交；

5.继续编辑命名为 RCE.py 的 Python 程序文件，使该程序实现对 Server7 进行远程代码执行测试的功能，成功渗透后找到 Server7 桌面上的文档，将文档内容作为 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。

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；

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。

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.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。