**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（9）**

**（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与密码策略、Nginx安全策略、日志监控策略、中间件服务安全策略、本地安全策略、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 事件监控

3.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-3任务三 中间件服务加固SSHD\VSFTPD\IIS（Windows, Linux）

4.SSH服务加固（Linux）

a.修改ssh服务端口为2222；

b.ssh禁止root用户远程登录；

c.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；

d.修改SSHD的PID档案存放地。

5.VSFTPD服务加固（Linux）

a.设置运行vsftpd的非特权系统用户为pyftp；

b.限制客户端连接的端口范围在50000-60000；

c.限制本地用户登陆活动范围限制在home目录。

6.IIS加固（Windows）

a.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)；

b.关闭IIS的WebDAV功能增强网站的安全性。

### A-4任务四 服务安全配置（Windows）

7.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；

8.在本地策略里配置禁用未登陆前关机；

9.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；

10.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-5任务五 防火墙策略（Linux）

11.为防止Nmap扫描软件探测到关键信息，设置iptables防火墙策略对3306号端口进行流量处理；

12.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；

13.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。

### A-6任务六 本地安全策略设置（Windows）

14.关闭系统时清除虚拟内存页面文件；

15.禁止系统在未登录的情况下关闭；

16.禁止软盘复制并访问所有驱动器和所有文件夹；

17.禁止自动管理登录；

18.禁止显示上次登录的用户名。

# 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.在Kali中使用Nmap工具查看本地路由与接口,并将该操作使用的全部命令作为Flag值提交；

2.通过Kali对靶机场景进行VNC服务扫描渗透测试，并将使用的脚本名称作为Flag值（如：MySQL-brute.nse）提交；

3.通过Kali对靶机场景进行VNC服务扫描渗透测试，并将该操作显示结果中VNC版本号作为Flag值提交；

4.在Kali中使用Nmap发送空的UDP数据对类DNS服务avahi进行拒绝服务攻击，并将使用的脚本名称作为Flag值（如：MySQL-brute.nse）提交；

5.通过Kali对靶机场景进行模糊测试，来发送异常的包到靶机服务器，探测出隐藏在服务器中的漏洞，并将使用的脚本名称作为Flag值（如：MySQL-brute.nse）提交；

6.在Kali中使用Zenmap工具扫描服务器场景可能存在存在远程任意代码执行漏洞，并将使用的脚本名称的字符串作为Flag值（如：MySQL-brute.nse）提交；

7.在Kali中使用Zenmap工具扫描服务器场景可能存在远程任意代码执行漏洞（提示：检测路径为/cgi-bin/bin，需添加--script-args uri=/cgi-bin/bin参数），并将该操作显示结果中漏洞编号和发布时间作为Flag值（漏洞编号和发布时间的字符串之间以分号隔开）提交。

### B-2任务二：Web渗透测试

\*任务说明：仅能获取Server2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-3任务三：数据分析数字取证

\*任务说明：仅能获取Server3的IP地址

1.使用Wireshark查看并分析Server3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-4任务四：漏洞扫描与利用

\*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对靶机场景Server4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-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Flag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安全应用

\*任务说明：仅能获取Server6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-7任务七：数据库渗透测试

\*任务说明：仅能获取Server7的IP地址

1.在渗透机Kali2.0中使用zenmap工具扫描服务器场景Server7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Server7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Server7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-8任务八：Linux系统安全

\*任务说明：仅能获取Server8的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server8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-9任务九：操作系统应急响应

\*任务说明：仅能获取Server9的IP地址

1.将黑客成功登录系统所使用的IP地址作为Flag值提交；

2.黑客成功登录系统后修改了登录用户的用户名，将修改后的用户名作为Flag值提交；

3.黑客成功登录系统后成功访问了一个关键位置的文件，将该文件名作为Flag值提交；

4.黑客对数据库进行了暴力破解，将最后一次暴力破解的时间作为Flag值提交；

5.黑客在系统中隐藏了某个批处理文件，将该文件内容作为Flag值提交。

### B-10任务十：Web渗透测试

\*任务说明：仅能获取Server10的IP地址

1.通过渗透机访问靶机HTTP服务，尝试上传或获取Web服务应用程序对应的木马类型，将木马应在位置（绝对目录）不变的部分作为Flag值提交；

2.通过渗透机渗透靶机HTTP服务，将漏洞利用过程中对文件名修改的最关键部分字符串作为Flag提交；

3.通过渗透机渗透靶机HTTP服务，将靶机的完整OS版本作为Flag值提交；

4.通过渗透机渗透靶机HTTP服务，下载靶机Web根目录下无后缀名的文件，并将文件名作为Flag值提交；

5.分析并找到文件中的密码值，并将密码值作为Flag值提交；

6.将密码值解密后的明文作为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。