**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（10）**

**（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, 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。

1.密码策略（Windows, Linux）

a.最小密码长度不少于13个字符；

b.密码必须符合复杂性要求。

2.用户安全管理(Windows)

a.设置取得文件或其他对象的所有权，将该权限只指派给administrators组；

b.禁止普通用户使用命令提示符;

c.设置不显示上次登录的用户名。

### 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 数据库安全策略

8.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；

9.删除默认数据库(test)；

10.改变默认mysql管理员用户为:SuperRoot；

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

**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；

15.启用本地安全策略中对Windows系统的审核帐户管理，成功和失败操作都要审核；

16.启用本地安全策略中对Windows系统的审核进程追踪，仅失败操作需要审核。

### A-4任务四 流量完整性保护（Windows）

17.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-6任务六 防火墙策略（Linux）**

18.设置防火墙允许本机转发除ICMP协议以外的所有数据包；

19.为防止Nmap等扫描软件探测到关键信息，设置iptables防火墙策略对80号端口进行流量处理；

20.为防御拒绝服务攻击，设置iptables防火墙策略对传入的流量进行过滤，限制每分钟允许3个包传入，并将瞬间流量设定为一次最多处理6个数据包（超过上限的网络数据包将丢弃不予处理）；

21.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。

# 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对靶机场景进行秘密FIN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对靶机场景进行秘密FIN扫描 (使用Nmap工具)，并将该操作显示结果中从下往上数第7行的端口信息作为Flag值提交；

3.通过渗透机Kali2.0对靶机场景进行圣诞树（Xmas Tree）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对靶机场景进行圣诞树（Xmas Tree）扫描（使用Nmap工具），并将该操作显示结果中从下往上数第5行的服务名称作为Flag值提交；

5.通过渗透机Kali2.0对靶机场景使用SYN包而不是用ACK包进行扫描渗透测试（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；

6.通过渗透机Kali2.0对靶机场景使用SYN包而不是用ACK包进行扫描渗透测试（使用Nmap工具），并将该操作显示结果中从下往上数第8行的服务状态作为Flag值提交；

7.通过渗透机Kali2.0对靶机场景进行ACK和ICMP两种扫描类型并行的扫描渗透测试（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ACK和ICMP两种扫描类型并行的扫描渗透测试（使用Nmap工具）,并将该操作显示结果中从下往上数第3行的服务名称作为Flag值提交。

### B-2任务二：Windows操作系统渗透测试

\*任务说明：仅能获取Server2的IP地址

1.通过本地PC中渗透测试平台Kali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1433端口对应的服务版本信息作为Flag值（例如3.1.4500）提交；

2.通过本地PC中渗透测试平台Kali对服务器场景Server2进行系统服务及版本扫描渗透测试，将DNS服务器的主机完全合格域名作为Flag值提交；

3.将目标服务器中SQL-Server数据库低权限（无法通过数据库执行指令系统命令）用户的密码作为Flag值提交；

4.将目标服务器中SQL-Server数据库权限较高（可以通过数据库指令执行系统命令）用户的密码作为Flag值提交；

5.找到C:\Windows\system32文件夹中266437文件夹中后缀为.docx的文件，将文档内容作为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logs.pcapng数据包文件，通过分析数据包attack.pcapng找出恶意用户目录扫描的第9个文件，并将该文件名作为Flag值（形式：[robots.txt]）提交；

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

3.继续查看数据包文件logs.pacapng分析出恶意用户读取服务器的文件名是什么，并将该文件名作为Flag值（形式：[robots.txt]）提交；

4.继续查看数据包文件logs.pacapng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（形式：[/root/whoami/]）提交；

5.继续查看数据包文件logs.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logs.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logs.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：中间人攻击渗透测试

\*任务说明：仅能获取Server4的IP地址

\*任务说明：仅能获取Server11的IP地址

1.通过上题渗透后得到控制权限的服务器场景Server4进行查看本地的arp缓存表的操作，并将该操作所使用的命令作为Flag值提交；

2.通过上题渗透后得到控制权限的服务器场景Server4进行清除本地的arp缓存表的操作，并将该操作所使用的命令作为Flag值提交；

3.通过本地PC中渗透测试平台Kali对服务器场景Server4以及服务器场景Server11进行中间人攻击渗透测试，打开渗透测试平台Kali的路由转发功能，并将该配置文件的绝对路径作为Flag值提交；

4.通过本地PC中渗透测试平台Kali对服务器场景Server4以及服务器场景Server11进行中间人攻击渗透测试，通过arpspoof命令对客户端（Server4）以及服务器（Server11）进行arp污染 ，并将该操作必须要用到的参数作为Flag值提交；

5.中间人渗透攻击成功后，渗透测试平台kali能够监听到客户端（Server4）向服务器（Server11）中的login.php页面提交的登陆网站用户名，密码信息，使用服务器场景Server4桌面上的Chrome浏览器，访问Server11服务器场景的Web站点http://Linux靶机ip/login.php，使用已经保存好的用户名，密码直接登录，并在kali上使用抓包软件wireshark进行抓包，设置wireshark过滤规则，过滤所有请求方式为POST的http请求包，将需要使用的过滤器表达式作为Flag值（==符号前后不要加空格）提交；

6.分析抓到的POST请求包，并将POST请求内容中客户端（Server4）向服务器（Server11）中的login.php页面提交的登陆网站admin用户的密码作为Flag值提交。

### B-5任务五：Windows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-6任务六：渗透测试

\*任务说明：仅能获取Server6的IP地址

1.在MSF工具中用search命令搜索MS12020 RDP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：2012-10-16）提交；

2.在MSF工具中调用MS12020 RDP拒绝服务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，并检测靶机是否存在漏洞，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MS12020 RDP拒绝服务漏洞的攻击模块，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.进入靶机关闭远程桌面服务，再次运行MS12020  
RDP拒绝服务漏洞的攻击模块，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-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中运行的服务，将完整的HTTP服务名称作为Flag值提交；

2.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/rececit/enehevibo.php，通过密码破译得到明文密码，并将明文密码作为Flag值提交；

3.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/irascence/futuresive.php，通过密码破译得到明文密码，并将明文密码作为Flag值提交；

4.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/economyia/tortly.php，通过密码破译进入新的页面，并将新页面的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

5.在新的页面中，通过解密页面内容获得密码，并将密码作为Flag值提交；

6.通过渗透机访问靶机的HTTP服务（使用火狐浏览器），URL为http://靶机IP/corticory/heseur.php，通过解密页面内容得到密码，并将密码作为Flag值提交。

### B-8任务八：文件MD5校验

\*任务说明：仅能获取Server8的IP地址

1.进入虚拟机操作系统：Server8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：Server8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：Server8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：Server8，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：Server8，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-9任务九：PE Reverse

\*任务说明：仅能获取Server9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-10任务十：应急响应

\*任务说明：仅能获取Server10的IP地址

1.黑客通过网络攻入本地服务器，在Web服务器的主页上外挂了一个木马连接，请你找到此连接并删除该连接，将对应的标题名称作为Flag值提交;

2.黑客攻入本地的数据库服务器，并添加了除admin以外的具有一个管理员权限的超级用户，将此用户的密码作为Flag值提交;

3.黑客攻入本地服务器，在本地服务器建立了多个超级用户，请你删除除了Administrator用户以外的其他超级管理员用户，然后在命令行窗口输入net user，将Administrator右边第一个单词作为Flag值提交;

4.黑客修改了服务器的启动内容，请你删除不必要的启动项程序，将该启动项程序的名称作为Flag值（如有多个名称之间以英文逗号分隔，如：hello,test）提交;

5.黑客在服务器某处存放了一个木马程序，请你找到此木马程序并清除木马，将木马文件名作为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。

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。