**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（8）**

**（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和密码策略、日志安全策略、中间件服务安全策略、流量完整性策略、防火墙策略、WEB安全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）

1.密码策略（Windows，linux）

a.最小密码长度不少于8个字符;

b.密码策略必须同时满足大小写字母、数字、特殊字符。

2.登录策略（Windows，linux）

a.在用户登录系统时，应该有“For authorized users only”提示信息;

b.一分钟内仅允许5次登录失败的尝试，超过5次，登录帐号锁定1分钟；

c.远程用户非活动会话连接超时应小于等于5分钟。

3.用户安全管理(Windows)

a.对服务器进行远程管理安全性SSL加固，防止敏感信息泄露被监听;

b.查找并删除服务器中可能存在的帐号hacker;

c.普通用户进行最小权限管理，对关闭系统仅限管理员帐号。

### A-3任务三 流量完整性

4.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-3任务三 日志安全审计（Windows）

5.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；

6.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；

7.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-4任务四 流量完整性保护（Windows）**

8.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-5任务五 防火墙策略

9.Windows系统禁用445端口；

10.Windows系统禁用23端口；

11.Linux系统使用iptables禁用23端口；

12.Linux系统使用iptables禁止别人ping通。

### A-2任务二 Nginx安全策略（Linux）

13.禁止目录浏览和隐藏服务器版本和信息显示；

14.限制HTTP请求方式，只允许GET、HEAD、POST；

15.设置客户端请求主体读取超时时间为10；

16.设置客户端请求头读取超时时间为10；

17.将Nginx服务降权，使用www用户启动服务。

# 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TCP同步扫描 (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；sS

2.通过渗透机Kali2.0对靶机场景进行TCP同步扫描 (使用Nmap工具)，并将该操作显示结果中从下往上数第4行的服务器信息作为Flag值提交；ms-sql-s

3.通过渗透机Kali2.0对靶机场景不ping主机进行扫描（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；sP

4.通过渗透机Kali2.0对靶机场景不ping主机进行扫描（使用Nmap工具），并将该操作显示结果中从下往上数第10行的“：”后的数字作为Flag值提交；977

5.通过渗透机Kali2.0对靶机场景进行UDP扫描渗透测试只扫描53，111端口（使用Nmap工具），并将该操作显示结果中111端口的状态信息作为Flag值提交；open

6.通过渗透机Kali2.0对靶机场景进行滑动窗口扫描渗透测试（使用Nmap工具），并将该操作使用的命令中必须要使用的参数作为Flag值提交；sW

7.通过渗透机Kali2.0对靶机场景进行RPC扫描扫描渗透测试（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；sR

8.通过渗透机Kali2.0对靶机场景进行RPC扫描扫描渗透测试（使用Nmap工具）,并将该操作显示结果中从下往上数第7行的服务信息作为Flag值提交。

### B-2任务二：FTP弱口令渗透测试

\*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值提交（忽略ip地址）；-p 21,22,23

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FTP服务对应的服务端口信息作为Flag值提交；21/tcp

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信息作为Flag值提交；auxiliary/scanner/ftp/ftp\_login

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值提交（之间以英文逗号分隔，例hello,test，..,..）；RHOSTS,PASS\_FILE,THREADS,USERNAME

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；set RHOSTS

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题获取到的密码登陆ftp服务，将该目录中Flag值2.bmp的图片文件中的英文单词作为Flag值提交。

### B-3任务三：PE Reverse

\*任务说明：仅能获取Server3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-4任务四：MYSQL安全测试

\*任务说明：仅能获取Server4的IP地址

1.利用渗透机场景kali中的工具确定MySQL的端口，将MySQL端口作为Flag值提交；3306/tcp

2.管理者曾在web界面登陆数据库，并执行了select '<?php echo \'<pre>\';system($\_GET[\'cmd\']); echo \'</pre>\'; ?>' INTO OUTFILE 'C:/phpstudy/test1.php'语句，结合本执行语句使用dos命令查看服务器的详细配置信息，并将服务器的系统型号作为Flag值提交；

3.利用渗透机场景kali中的msf工具使用root目录下password.txt字典文件破解MySQL的密码，并将破解MySQL的密码所需的模块当作Flag值 (账户为root) 提交;mysql\_login

4.利用渗透机场景kali中的msf工具使用root目录下password.txt字典文件破解MySQL的密码，并将MySQL的密码当作Flag值 (账户为root) 提交;

5.利用上题中的数据库账户密码在登陆数据库，通过select '<?php @eval($\_POST[admin]);?>'\*\*\*\*\*\*\*\*\*\*\*\* 'C:/phpstudy/shell.php'语句向服务器提交名为shell.php的一句话木马，将语句中\*号的明文作为Flag值（\*为大写字母或者空格）提交；INTO OUTFILE

6.使用菜刀连接上题中的shell.php,下载服务器根目录下的压缩包，将压缩包中的Flag值提交。

### B-5任务五：流量分析

\*任务说明：仅能获取Server5的IP地址

1.通过Kali访问目标靶机http://xxx.xxx.xxx.xxx:8081(xxx.xxx.xxx.xxx为靶机IP地址,例如172.16.101.1:8081)下载文件获取流量包。将流量包进行解压，获取流量包中的文件名作为Flag值（形式：文件名.文件类型）提交；

2.通过Kali中利用wireshark从服务器场景Server5中下载的流量包进行流量包分析，使用HTTP模式下的过滤表达式过滤HTTP GET方法的流量包，过滤表达式命令作为Flag值提交；http.request.method==”GET”http.request.method==”GET”

3.根据第2步回显信息从过滤出的流量包中分析，找到Flag值文件流量的IP地址，并将该HTTP流量包（第1步中下载的流量包）含Flag值信息的请求源ip作为Flag值提交；

4.在渗透测试平台Kali中利用wireshark从包含Flag值信息的流量包中的IP数据包中找到目标信息文件，并将该文件名作为Flag值（形式：文件名.文件类型）提交；

5.在渗透测试平台Kali中使用wireshark分析下载的流量包，并从包含Flag值信息的GET/POST请求流量中找出响应IP及响应内容，并将该Flag值请求的响应IP（流量包中的IP）作为Flag值提交；

6.使用wireshark工具分析响应流量包（第5步Flag值请求对应的response响应流量数据包）中的数据内容，将该响应数据中的文件名，作为Flag值（形式：文件名.文件类型）提交；ctrl+H

7.使用wireshark工具提取流量包中内容（即第6步响应流量包中的文件内容），将该提取操作必须使用的到的wireshark功能的快捷键作为Flag值（xx+xx为Flag值提交格式,例如ctrl+alt+F4）提交；

8.将第7步提取出的文件进行解压，将该文件解压后的文件内容第一行作为Flag值提交。

### B-6任务六：Windows系统安全

\*任务说明：仅能获取Server6的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server6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；vsftpd 2.3.4

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-7任务七：Telnet弱口令渗透测试

\*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；-p 21，22，23

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TELNET服务对应的服务端口信息作为Flag值提交；23/tcp

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信息作为Flag值提交；auxiliary/scanner/telnet/telnet\_login

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（字段之间以英文逗号分隔，例hello,test，..,..）提交;RHOSTS,PASS\_FILE,THREADS,PASSWORD

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；set RHOSTS

6.在msf模块中指定密码字典，字典路径为/root/2.txt，用户名为user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telnet到靶机，将桌面上Flag值.bmp的图片文件中的英文单词作为Flag值提交。

### B-8任务八：渗透测试

\*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对靶机场景Server8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；-oX

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；msfdb\_init

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；hosts

4.在MSF工具中用search命令搜索搜索MS17010漏洞利用模块，将回显结果中的漏洞公开时间作为flag值（如：2017-10-16）提交； 2017-03-14

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。completed

### B-9任务九：隐写术应用

\*任务说明：仅能获取Server9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-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Server10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

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。