**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（3）**

**（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, 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 Nginx安全策略（Linux）**

3.禁止目录浏览和隐藏服务器版本和信息显示；

4.限制HTTP请求方式，只允许GET、HEAD、POST；

5.设置客户端请求主体读取超时时间为10；

6.设置客户端请求头读取超时时间为10；

7.将Nginx服务降权，使用www用户启动服务。

**A-3任务三 日志监控（Windows）**

8.安全日志文件大小至少为128MB，设置当达到最大的日志大小上限时，覆盖早于30天的日志；

9.应用日志文件大小至少为64MB，设置当达到最大的日志大小上限时，覆盖早于15天的日志；

10.系统日志大小至少为32MB，设置当达到最大的日志大小上限时，按需要覆盖事件。

**A-4任务四 中间件服务加固SSHD\VSFTPD\IIS（Windows, Linux）**

11.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。

12.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。

13.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-5任务五 本地安全策略（Windows）**

14.禁止匿名枚举SAM帐户；

15.禁止系统在未登录的情况下关闭；

16.禁止存储网络身份验证的密码和凭据；

17.禁止将Everyone权限应用于匿名用户；

18.在超过登录时间后强制注销。

**A-6任务六 防火墙策略（Linux）**

19.设置防火墙允许本机转发除ICMP协议以外的所有数据包；

20.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；

21.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）；

22.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.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：渗透测试

\*任务说明：仅能获取Server2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-3任务三：MYSQL安全测试

\*任务说明：仅能获取Server3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；

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;

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；

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-4任务四：Web安全应用

\*任务说明：仅能获取Server4的IP地址

1. 通过渗透机扫描靶机Linux，将HTTP服务的端口号作为Flag值提交；

2. 通过渗透机渗透靶机Linux的HTTP服务，将Web漏洞注入点的URL地址作为Flag值（形式：http://172.16.1.1/页面路径）提交；

3. 通过渗透机访问靶机Windows，获取后缀名为pcapng的数据包文件，该数据包为黑客对靶机Linux的渗透测试过程，并将文件名作为Flag值提交；

4. 通过渗透机分析pcapng数据包文件，将黑客登录管理员用户时使用的密码作为Flag值提交；

5. 通过渗透机分析pcapng数据包文件，将黑客上传的木马文件中的有效代码作为Flag值提交；

6. 通过渗透机分析pcapng数据包文件，将黑客连接数据库时使用的密码作为Flag值提交。

### B-5任务五：网站XSS漏洞

\*任务说明：仅能获取Server5的IP地址

1.进入靶机网站http://靶机IP/kzjb/，使用渗透机场景中的xsser命令检测靶机网站是否存在xss漏洞，将命令输出的Accur关键字的值作为FLAG值提交；

2.使用test用户（密码：123456）登录靶机网站，在输入框中测试页面是否存在xss漏洞，使用JavaScript语句在页面中弹窗“HelloWorld”信息，将弹窗所需要的函数名称作为FLAG值提交；

3.分析输入框所在页面，将页面中出现的JavaScript函数名称作为FLAG值提交；

4.下载靶机FTP中文本文件，将下载的文本文件内容上传至网站输入框中。下载靶机FTP中的.py文件并运行，下载靶机FTP中的.pyc文件并运行。将.py文件输出第一行的第二个单词作为FLAG值提交；

5.下载靶机FTP中php文件，在http://靶机IP/kzjb/upload.php页面下上传php文件,获取C:\flag.txt文件内容作为FLAG值提交。

### B-6任务六：数据分析数字取证

\*任务说明：仅能获取Server6的IP地址

1.分析Server6桌面下的Alpha-1.pcapng数据包文件，通过分析数据包Alpha-1.pcapng找出恶意用户第一次访问服务器的数据包是第几号，并将该号数作为Flag值提交；

2.继续查看数据包文件Alpha-1.pcapng，分析出恶意用户扫描了哪些端口，并将全部的端口号从小到大作为Flag值（形式：端口1,端口2,端口3…,端口n）提交；

3.继续查看数据包文件Alpha-1.pcapng分析出恶意用户登陆后台所用的用户名是什么，并将用户名作为Flag值提交；

4.继续查看数据包文件Alpha-1.pcapng分析出恶意用户在第几个数据包到第几个数据包之间利用了MIME漏洞，并将该数据包之间的号数作为Flag值（格式：1,30）提交；

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

6.继续查看数据包文件Alpha-1.pcapng分析出恶意用户第二次写入一句话木马是在哪个路径，并将改路径以及文件名和后缀作为Flag值提交；

7.继续查看数据包文件Alpha-1.pcapng分析出恶意用户下载了什么文件，并将该文件内容作为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Windows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；

2.通过渗透机Kali2.0对服务器场景Windows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；

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；

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；

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，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：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：Windows操作系统渗透测试

\*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对服务器场景Server9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Server9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-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。

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。