**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（6）**

**（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、日志安全审计、数据库安全策略、Web安全加固、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.密码策略必须同时满足大小写字母、数字、特殊字符；

b.强制密码历史为5个密码；

c.密码最长存留期为45天；

d.最小密码长度不少于8个字符。

2.用户安全管理

a.禁止普通用户使用注册表编辑工具以及Ctrl+Alt+Del；

b.交互式登录时不显示用户名；

c.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；

d.禁止普通用户使用命令提示符;

e.设置不显示上次登录的用户名。

**A-2任务二：日志安全配置（Windows）**

3.配置审核登陆，记录内容包括用户登录使用的账户、登录是否成功、登录时间、以及远程登录时间、及用户使用的IP地址；

4.启用本地安全策略中对Windows系统的审核策略更改，成功和失败操作都需要审核；

5.启用本地安全策略中对Windows系统的审核对象访问，成功和失败操作都需要审核。

**A-3任务三：中间件服务安全加固VSFTPD/HTTPD/BIND（Linux）**

6.VSFTPD

a.vsftpd禁止匿名用户上传；

b.设置无任何操作的超时时间为5分钟；

c.匿名用户访问的最大传输速率为512KB/S；

d.用户访问的最大传输速率为1M。

7.HTTPD

a.更改默认监听端口为6666；

b.设置禁止目录浏览；

c.隐藏Apache版本号；

d.将Apache服务降权，用户为apache，用户组为www。

8.BIND

a.隐藏bind版本号；

b.设置不提供递归服务。

### A-4任务四：IP协议安全配置

9.指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为5；

10.指定处于SYN\_RCVD状态的TCP连接数的阈值为500；

11.指定处于至少已发送一次重传的SYN\_RVCD状态中的TCP连接数的阈值为400。

### A-5任务五：防火墙策略（Windows）

12.禁止任何机器ping本机；

13.禁止本机ping任何机器；

14.拒绝 TCP 标志位全部为 1 及全部为 0 的报文访问本机；

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

**A-6任务六：本地安全策略（Windows）**

16.禁止匿名枚举SAM帐户；

17.禁止系统在未登录的情况下关闭；

18.禁止存储网络身份验证的密码和凭据；

19.禁止将Everyone权限应用于匿名用户；

20.在超过登录时间后强制注销。

# 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.通过渗透机渗透机BT5使用fping对服务器场景Server1所在网段(例如：172.16.101.0/24)进行主机发现扫描,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；

2.通过渗透机渗透机Kali2.0使用genlist对服务器场景Server1所在网段进行扫描进行主机存活发现, 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；

3.通过渗透机渗透机Kali2.0使用nbtscan对服务器场景Server1所在网段进搜索扫描，获取目标的MAC地址等信息，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；

4.假设服务器场景Server1设置了防火墙无法进行ping检测，通过渗透机渗透机Kali2.0使用arping检测主机连通性扫描（发送请求数据包数量为4个），并将该操作使用的命令中固定不变的字符串作为Flag值提交；

5.通过渗透机渗透机Kali2.0使用fping对服务器场景Server1所在网段进行存活性扫描，且要把最终扫描的存活主机输出到文件ip.txt中，并将该操作使用的命令中必须要使用的参数作为Flag值（各参数之间用英文逗号分割，例a,b）提交；

6.通过渗透机渗透机Kali2.0使用nbtscan从第5题的ip.txt文件中读取IP扫描主机信息MAC地址等信息，并将该操作使用的命令中固定不变的字符串作为Flag值提交；

7.通过渗透机渗透机Kali2.0使用xprobe2对服务器场景Server1进行TCP扫描，仅扫描靶机80,3306端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为Flag值提交；

8.通过渗透机渗透机Kali2.0使用xprobe2对服务器场景Server1进行UDP扫描，仅扫描靶机161,162端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为Flag值提交。

**B-2任务二：文件上传渗透测试**

\*任务说明：仅能获取Server2的IP地址

1.通过渗透机Kali2.0对服务器场景Server2进行网站目录暴力枚举测试（使用工具DirBuster，扫描服务器80端口），选择使用字典（使用默认字典directory-list-2.3-medium.txt）方式破解，并设置模糊测试的变量为“{dir}”，将回显信息中从上往下数第六行的数字作为Flag值提交；

2.通过渗透机Kali2.0对服务器场景Server2进行网站目录暴力枚举测试（使用工具DirBuster，扫描服务器80端口），通过分析扫描结果，找到上传点并使用火狐浏览器访问包含上传点的页面，并将访问成功后的页面第一行的第一个单词作为Flag值提交；

3.访问成功后上传名为backdoor.php的php一句话木马至服务器，打开控制台使用网站安全狗检测本地是否存在木马，若检测出存在木马，则将木马所在的绝对路径作为Flag值提交，若未检测出木马则提交false；

4.通过渗透机Kali2.0对服务器场景Server2进行文件上传渗透测试，使用工具weevely在/目录下生成一个木马，木马名称为backdoor.php，密码为pass，该操作使用命令中固定不变的字符串作为Flag值提交；

5.上传使用weevely生成的木马backdoor1.php至服务器中，打开控制台使用网站安全狗检测本地是否存在木马，若检测出存在木马，则将木马所在的绝对路径作为Flag值提交，若未检测出木马则提交false；

6.通过渗透机Kali2.0对服务器场景Server2进行文件上传渗透测试（使用工具weevely，连接目标服务器上的木马文件），连接成功后将目标服务器主机名的字符串作为Flag值提交；

7.开启网站安全狗的所有防护，再次使用weevely生成一个新的木马文件并将其上传至目标服务器，将上传后页面提示的第二行内容作为Flag值提交；

8.开启网站安全狗的所有防护，再次使用weevely生成木马文件并将其上传至目标服务器，要求能够上传成功，将生成该木马必须要使用的参数作为Flag值提交。

**B-3任务三：CVE-2019-0708漏洞利用**

\*任务说明：仅能获取Server3的IP地址

1.通过本地PC中渗透测试平台Kali对靶机场景Server3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CVE-2019-0708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CVE-2019-0708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：数据分析数字取证

\*任务说明：仅能获取Server4的IP地址

1.分析Server4桌面下的Bravo-1.pcapng数据包文件，通过分析数据包Bravo-1.pcapng找出恶意用户目录扫描的第2个目录名，并将该目录名作为Flag值提交;

2.继续查看数据包文件Bravo-1.pcapng，分析出恶意用户通过哪个目录写入的一句话木马，并将该目录名作为Flag值提交;

3.继续查看数据包文件Bravo-1.pcapng分析出恶意用户读取了服务器什么文件，并将该文件名及后缀作为Flag值提交;

4.继续查看数据包文件Bravo-1.pcapng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值提交;

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

6.继续查看数据包文件Bravo-1.pcapng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值提交;

7.继续查看数据包文件Bravo-1.pcapng将Web服务器连接的数据库名作为Flag值提交。

### B-5任务五：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-6任务六：Telnet弱口令渗透测试

\*任务说明：仅能获取Server6的IP地址

1.在渗透机Kali2.0中使用Zenmap工具扫描服务器场景Server6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-7任务七：中间人攻击渗透测试

\*任务说明：仅能获取Server7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Server7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Server7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Server7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Server7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（Server7）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（Server7）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Server7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（Server7）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-8任务八：PE Reverse**

\*任务说明：仅能获取Server8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-9任务九：Web安全应用**

\*任务说明：仅能获取Server9的IP地址

\*任务说明：仅能获取Server12的IP地址

1.通过渗透机扫描靶机Server9，将HTTP服务的端口号作为Flag值提交；

2.通过渗透机渗透靶机Server9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Server12，获取后缀名为pcapng的数据包文件，该数据包为黑客对靶机Server9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-10任务十：Windows系统安全

\*任务说明：仅能获取Server10的IP地址

1.通过本地PC中渗透测试平台Kali对服务器场景Server10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。

# 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。