**2022年全国职业院校技能大赛（中职组）**

**网络安全竞赛试题**

**（2）**

**（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-2任务二 日志安全配置（Windows）

4.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；

5.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；

6.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）

7.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。

8.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。

9.BIND

a.隐藏bind版本号；

b.设置不提供递归服务。

### A-4任务四 流量完整性保护（Windows）

10.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（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 WEB安全加固（Windows）

14.为了防止web中.mdb数据库文件非法下载，请对Web配置文件进行安全加固;

15.限制目录执行权限,对picture和upload目录设置执行权限为无；

16.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)。

# 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值提交（各参数之间用英文逗号分割，例a,b）；

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：Windows系统安全

\*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-3任务三：Web信息收集

\*任务说明：仅能获取Server3的IP地址

1.通过Kali对靶机场景进行Web扫描渗透测试（使用工具nikto，查看该命令的完整帮助文件），并将该操作使用命令中固定不变的字符串作为Flag值提交；

2.通过Kali对靶机场景进行Web扫描渗透测试（使用工具nikto，扫描目标服务器8080端口，检测其开放状态），并将该操作使用命令中固定不变的字符串作为Flag值（目标地址以http://10.10.10.1来表示）提交；

3.通过Kali对靶机场景进行Web扫描渗透测试（使用工具nikto，扫描目标服务器80端口），将回显信息中apache服务的版本参数作为Flag值提交；

4.通过Kali对靶机场景进行Web扫描渗透测试（使用工具nikto，扫描目标服务器80端口），将回显信息中php的版本参数作为Flag值提交；

5.通过Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，扫描CGI-BIN目录的文件），将该操作使用的命令中固定不变的字符串作为Flag值（目标地址以：http://10.10.10.1来表示）提交；

6.通过Kali对靶机场景进行Web扫描渗透测试，使用工具nikto并结合Nmap的扫描结果进行扫描，首先使用Nmap工具对靶机所在网段的80端口进行扫描，并将扫描结果以输出至所有格式的方式输出到指定文件target中，将输出至所有格式需要用到的参数作为Flag值提交；

7.通过Kali对靶机场景进行Web扫描渗透测试，使用工具nikto扫描第六题生成的target文件中的网站，并将该操作使用的所有命令作为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.使用Wireshark查看并分析Windows 7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-5任务五：本地文件包含

\*任务说明：仅能获取Server5的IP地址

1.扫描靶机服务器，将靶机网站服务的服务版本作为Flag值提交；

2.在靶机FTP服务中，存在密码文件，使用密码文件暴力破解网站密码，将破解后的密码作为Flag值提交；

3.使用base64加密，将加密后的字符串作为Flag值提交；

4.使用cat命令制作图片木马，新图片名称为backdoor.png，将制作图片木马的完整命令作为Flag值提交；

5.进入靶机网站http://靶机IP/lfi/，在靶机网站中上传backdoor.png文件，在页面上运行上传的图片文件，将完整URL作为Flag值（形式：http://172.16.1.1/页面路径）提交；

6.获取靶机C:\flag.txt文件内容作为Flag值提交。

### B-6任务六：数据库安全加固

\*任务说明：仅能获取Server6的IP地址

1.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库版本号，将查看数据库版本号的命令作为Flag值提交；

2.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库版本号，将查询到的数据库版本号作为Flag值提交；

3.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库列表，将查看数据库列表的命令作为Flag值提交；

4.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，查看所有用户及权限，找到可以从任意 IP 地址访问的用户，将该用户的用户名作为Flag值提交；（如有多个可以从任意 IP 地址访问的用户，提交形式为用户名|用户名|用户名|用户名）

5.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，查看所有用户及权限，找到可以从任意 IP 地址访问的用户，使用drop命令将该用户删除，将操作命令作为Flag值提交；

6.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，改变默认 MySQL 管理员的名称，将系统的默认管理员root 改为 admin，防止被列举，将操作命令作为Flag值提交。

### B-7任务七：操作系统应急响应

\*任务说明：仅能获取Server7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-8任务八：MS15034漏洞扫描与利用

\*任务说明：仅能获取Server8的IP地址

1.在MSF工具中用search命令搜索MS15034HTTP.SYS漏洞拒绝服务攻击模块，将回显结果中的漏洞披露时间作为Flag值（如：2015-10-16）提交；

2.在MSF工具中调用MS15034HTTP.SYS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，并检测漏洞是否存在，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MS15034HTTP.SYS漏洞的拒绝服务攻击模块，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.进入靶机在IIS网站下的编辑输出缓存设置中禁止启用内核缓存，再次运行MS15034HTTP.SYS漏洞的拒绝服务攻击模块，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-9任务九：Web渗透测试

\*任务说明：仅能获取Server9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。

### B-10任务十：PE Reverse

\*任务说明：仅能获取Server10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；

# 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。