

2024 年甘肃省职业院校技能大赛中职组

电子与信息类“网络安全”赛项竞赛样题-B

一、竞赛时间

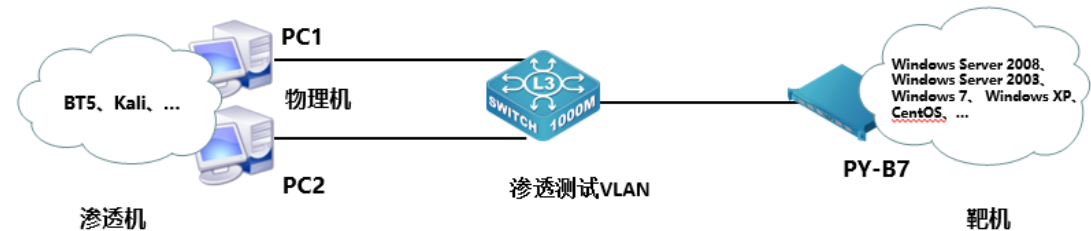
总计：180 分钟

二、竞赛阶段

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
A、B 模块	A-1	登录安全加固	90 分钟	200 分
	A-2	本地安全策略设置		
	A-3	流量完整性保护		
	A-4	事件监控		
	A-5	服务加固		
	A-6	防火墙策略		400 分
	B-1	Windows 操作系统渗透测试		
	B-2	数字取证调查		
	B-3	Web 安全之综合渗透测试		
	B-4	跨站脚本渗透		
	B-5	网络安全事件响应		
C、D 模块	C 模块	CTF 夺旗-攻击	90 分钟	200 分
	D 模块	CTF 夺旗-防御		200 分

三、竞赛任务书内容

（一）拓扑图



（二）A 模块基础设施设置/安全加固（200 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、流量完整性保护策略、事件监控策略、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。

二、服务器环境说明

AServer06(Windows)系统：用户名 administrator 密码 123456

AServer07(Linux)系统：用户名 root 密码 123456

三、说明：

1. 所有截图要求截图界面、字体清晰，并粘贴于相应题目要求的位置；
2. 文件名命名及保存：网络安全模块 A-XX（XX 为工位号），PDF 格式保存；
3. 文件保存到 U 盘提交。

A-1：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) 密码策略必须同时满足大小写字母、数字、特殊字符（Windows），将密码必须符合复杂性要求的属性配置界面截图：

- b) 密码策略必须同时满足大小写字母、数字、特殊字符 (Linux)，将
/etc/pam.d/system-auth 配置文件中对应的部分截图：
- c) 最小密码长度不少于 8 个字符 (Windows)，将密码长度最小值的属性配置界面截图：
- d) 最小密码长度不少于 8 个字符 (Linux)，将/etc/login.defs 配置文件中对应的部分截图：

2. 登录策略

- a) 设置账户锁定阈值为 6 次错误锁定账户，锁定时间为 1 分钟，复位账户锁定计数器为 1 分钟之后 (Windows)，将账户锁定策略配置界面截图：
- b) 一分钟内仅允许 5 次登录失败，超过 5 次，登录帐号锁定 1 分钟 (Linux)，将/etc/pam.d/login 配置文件中对应的部分截图：

3. 用户安全管理 (Windows)

- a) 禁止发送未加密的密码到第三方 SMB 服务器，将 Microsoft 网络客户端：将未加密的密码发送到第三方 SMB 服务器的属性配置界面截图：
- b) 禁用来宾账户，禁止来宾用户访问计算机或访问域的内置账户，将账户：来宾账户状态的属性配置界面截图：

A-2：本地安全策略设置 (Windows)

- 1. 关闭系统时清除虚拟内存页面文件，将关机：清除虚拟内存页面文件的属性配置界面截图：
- 2. 禁止系统在未登录的情况下关闭，将关机：允许系统在未登录的情况下关闭的属性配置界面截图：
- 3. 禁止软盘复制并访问所有驱动器和所有文件夹，将恢复控制台：允许软盘复制并访问所有驱动器和所有文件夹的属性配置界面截图：
- 4. 禁止显示上次登录的用户名，将交互式登录：不显示最后的用户名的属性配置界面截图：

A-3：流量完整性保护 (Windows, Linux)

- 1. 创建 www.chinaskills.com 站点，在 C:\web 文件夹内中创建名称为 chinaskills.html 的主页，主页显示内容“热烈庆祝 2024 年甘肃省职业院校

技能大赛开幕”，同时只允许使用 SSL 且只能采用域名(域名为 `www.test.com`) 方式进行访问，将网站绑定的配置界面截图：

2. 为了防止密码在登录或者传输信息中被窃取，仅使用证书登录 SSH (Linux)，将 `/etc/ssh/sshd_config` 配置文件中对应的部分截图：

A-4：事件监控 (Windows)

1. 应用程序日志文件最大大小达到 65M 时将其存档，不覆盖事件，将日志属性-应用程序（类型：管理的）配置界面截图：

A-5：服务加固 SSH\VSFTPD\IIS (Windows, Linux)

1. SSH 服务加固 (Linux)
 - a) SSH 禁止 root 用户远程登录，将 `/etc/ssh/sshd_config` 配置文件中对应的部分截图：
 - b) 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，使用命令 `crontab -l`，将回显结果截图；
 - c) 修改 SSH 服务端口为 2222，使用命令 `netstat -anltp | grep sshd` 查看 SSH 服务端口信息，将回显结果截图；
2. VSFTPD 服务加固 (Linux)
 - a) 设置数据连接的超时时间为 2 分钟，将 `/etc/vsftpd/vsftpd.conf` 配置文件中对应的部分截图：
 - b) 设置站点本地用户访问的最大传输速率为 1M，将 `/etc/vsftpd/vsftpd.conf` 配置文件中对应的部分截图：
3. IIS 加固 (Windows)
 - a) 防止文件枚举漏洞枚举网络服务器根目录文件，禁止 IIS 短文件名泄露，将配置命令截图：
 - b) 关闭 IIS 的 WebDAV 功能增强网站的安全性，将警报提示信息截图：

A-6：防火墙策略 (Linux)

1. 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，将 `iptables`

配置命令截图：

2. 禁止任何机器 ping 本机，将 iptables 配置命令截图：
3. 禁止本机 ping 任何机器，将 iptables 配置命令截图：
4. 禁用 23 端口，将 iptables 配置命令截图：
5. 禁止转发来自 MAC 地址为 29:0E:29:27:65:EF 主机的数据包，将 iptables 配置命令截图：
6. 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，将 iptables 配置命令截图：
7. 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，将 iptables 配置命令截图：

(三)B 模块安全事件响应/网络安全数据取证/应用安全(400 分)

B-1: Windows 操作系统渗透测试

任务环境说明：

- ✓ 服务器场景：Server2105（关闭链接）
- ✓ 服务器场景操作系统：Windows（版本不详）

1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景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 445 端口对应的服务版本信息字符串作为 Flag 值提交；
2. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景网络连接信息中的 DNS 信息作为 Flag 值（例如：114.114.114.114）提交；
3. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景中的当前最高账户管理员的密码作为 Flag 值提交；
4. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景桌面上 111 文件夹中唯一一个后缀为 .docx 文件的文件名称作为 Flag 值提交；
5. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景桌面上 111 文件夹中唯一一个后缀为 .docx 文件的文档内容作为 Flag 值提交；

6. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试,将该场景桌面上 222 文件夹中唯一一个图片中的英文单词作为 Flag 值提交;

B-2: 数字取证调查

- ✓ 服务器场景: FTPServer20221010 (关闭链接)
 - ✓ 服务器场景操作系统: 未知
 - ✓ FTP 用户名:attack817 密码: attack817
1. 分析 attack.pcapng 数据包文件,通过分析数据包 attack.pcapng 找出恶意用户第一次访问 HTTP 服务的数据包是第几号,将该号数作为 Flag 值提交;
 2. 继续查看数据包文件 attack.pcapng,分析出恶意用户扫描了哪些端口,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 attack.pcapng 分析出恶意用户登录后台所用的密码是什么,将后台密码作为 Flag 值提交;
 4. 继续查看数据包文件 attack.pcapng 分析出恶意用户写入的一句话木马的密码是什么,将一句话密码作为 Flag 值提交;
 5. 继续查看数据包文件 attack.pcapng 分析出恶意用户下载了什么文件,将该文件内容作为 Flag 值提交。

B-3: Web 安全之综合渗透测试

- ✓ 服务器场景名称: Server2010 (关闭链接)
 - ✓ 服务器场景操作系统: 未知
1. 使用渗透机场景 Kali 中的工具扫描服务器,通过扫描服务器得到 web 端口,登陆网站(网站路径为 IP/up),找到网站首页中的 Flag 并提交;
 2. 使用渗透机场景 windows7 访问服务其场景中的网站,通过上题给的信息获取本题,并将本题中的 Flag 提交;
 3. 使用渗透机场景 windows7 根据第二题的入口继续访问服务器本题场景,通过提示得到 Flag 并提交;
 4. 使用渗透机场景 windows7 根据第三题入口继续访问服务器的本题场景,通过

提示联系前两题上传特定文件名得到 Flag 并提交；

5. 使用渗透机场景 windows7 根据第四题入口继续访问服务器的本题场景，通过提示得到 Flag 并提交；
6. 使用渗透机场景 windows7 根据第五题入口继续访问服务器的本题场景，通过提示得到 Flag 并提交；
7. 使用渗透机场景 windows7 访问 http://靶机 IP/7，对该页面进行渗透测试，通过提示得到 Flag 并提交；
8. 使用渗透机场景 windows7 访问 http://靶机 IP/8，对该页面进行渗透测试，通过提示得到 Flag 并提交；
9. 使用渗透机场景 windows7 访问 http://靶机 IP/9，对该页面进行渗透测试，通过提示得到 Flag 并提交；
10. 使用渗透机场景 windows7 访问 http://靶机 IP/10，对该页面进行渗透测试，通过提示得到 Flag 并提交；
11. 使用渗透机场景 windows7 访问 http://靶机 IP/11，对该页面进行渗透测试，通过提示得到 Flag 并提交；
12. 使用渗透机场景 windows7 访问 http://靶机 IP/12，对该页面进行渗透测试，通过提示得到 Flag 并提交；
13. 使用渗透机场景 windows7 访问 http://靶机 IP/13，对该页面进行渗透测试，通过提示得到 Flag 并提交；

B-4：跨站脚本渗透

- ✓ 服务器场景：Server2125（关闭）
- ✓ 服务器场景操作系统：未知

1. 访问服务器网站目录 1，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；
2. 访问服务器网站目录 2，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；
3. 访问服务器网站目录 3，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；

4. 访问服务器网站目录 4，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；
5. 访问服务器网站目录 5，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；
6. 访问服务器网站目录 6，根据页面信息完成条件，将获取到弹框信息作为 flag 提交；

B-5：网络安全事件响应

- ✓ 服务器场景：Server2215（关闭链接）
- ✓ 服务器场景操作系统：未知

1. 黑客通过网络攻入本地服务器（靶机），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。

（四）模块 C CTF 夺旗-攻击

（本模块 200 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答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

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。

（五）模块 D CTF 夺旗-防御

（本模块 200 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。

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/Windows7

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. 每位选手需要对加固点和加固过程截图，并自行制作系统防御实施报告，最终评分以实施报告为准；
2. 系统加固时需要保证堡垒服务器对外提供服务的可用性；
3. 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；
4. 本环节不予补时。

二、说明：

1. 所有截图要求截图界面、字体清晰；
2. 文件名命名及保存：网络安全模块 D-XX（XX 为工位号），PDF 格式保存；
3. 文件保存到 U 盘提交。