开封市第一届职业技能大赛

网络安全项目（世赛项目）

样题

开封市第一届职业技能大赛执委会技术指导组

2023 年 2 月

项目说明

项目名称：网络安全项目

一、项目完成时间：

网络安全项目比赛总时间为420分钟，本项目共有四个模块，其中模块A、B，合计240分钟;模块C、D，合计180分钟。

二、项目配分：满分1000 分，其中模块A，200分；模块B，400分；模块C，200分;模块D，200分。

赛程及安排见下表：

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
A模块	A-1	登录安全加固（Windows, Linux）	240分钟	200分
	A-2	本地安全策略设置（Windows）		
	A-3	流量完整性保护（Windows, Linux）		
	A-4	事件监控（Windows）		
	A-5	不公开		
	A-6	不公开		
B模块	B-1	服务远程控制		400分
	B-2	CMS网站渗透		
	B-3	远程代码执行		
	B-4	不公开		
	B-5	不公开		
阶段切换	阶段切换		60分钟	0
C、D模块	C模块	CTF夺旗-攻击	180分钟	200分
	D模块	CTF夺旗-防御		200分

三、竞赛设备

赛场提供计算机及软件。

四、注意事项

1.选手要在抽签的工位上进行比赛，按要求在任务书封面上填写好工位号、市或地区、选手姓名。

2.除组委会规定允许携带的比赛用品外，不得携带任何与竞赛无关的物品和通讯工具等进场。进入竞赛场地后，必须遵守赛场纪律，否则现场裁判人员有权取消该选手参赛资格。

3.竞赛时间结束，所有参赛选手要立刻停止操作，等待裁判人员验收。

4.在比赛过程中，选手若有违规操作，将根据具体情况在专业规范扣除相应的分数。

5.每次任务完成后，应保证桌面、工具清洁，现场工具及其他物品摆放整齐。

竞赛任务书内容

拓扑图

模块 A　基础设施设置与安全加固（试题）

时间：A+B 模块=240 分钟

分值：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。

四、任务要求

模块 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）

序号	描述
1	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：
2	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：
3	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：
4	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

序号	描述
1	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：
2	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	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：
4	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：

模块 A-2：本地安全策略设置（Windows）

序号	描述

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：

模块 A-3：流量完整性保护（Windows，Linux）

序号	描述
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“预祝本次竞赛顺利结束”，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：

模块 A-4：事件监控（Windows）

序号	描述
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：

模块 B　安全事件响应/网络安全数据取证/应用安全（试题）

时间：A+B 模块=240 分钟

分值：400 分

任务要求：

模块 B-1：服务远程控制

（一）任务环境说明：

- ✓ 服务器场景名：Server2008（关闭链接）
- ✓ 服务器场景操作系统：未知
- ✓ 服务器场景用户名：root
- ✓ 服务器场景密码：Admin123

（二）任务要求：

序号	描述
1	通过本地 PC 中渗透测试平台 Kali 对服务器场景进行系统版本扫描渗透测试，并将该操作显示结果中系统信息作为 FLAG 提交；
2	通过本地 PC 中渗透测试平台 windows7 对服务器场景进行终端服务开启，并将该操作显示结果中服务端口号作为 FLAG 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，找到服务器场景中的管理员用户的桌面下中的可执行文件，并将全称作为 FLAG 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，找到服务器场景中的管理员桌面下的文本文档，将文件内容作为 FLAG 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，找到服务器场景中的管理员用户的文档中的文件，将文件内容作为 FLAG 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，找到服务器场景中的后门用户并将用户名作为 FLAG 提交；
7	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，找到服务器场景中的桌面背景，并将的文件全称作为 FLAG 提交；

模块 B-2：CMS 网站渗透

（一）任务环境说明：

- ✓ 服务器场景：Server2206（关闭链接）
- ✓ 服务器场景操作系统：未知

（二）任务要求

序号	描述
1	使用渗透机对服务器信息收集，并将服务器中网站服务端口号作为 flag 提交；
2	使用渗透机对服务器信息收集，将网站的名称作为 flag 提交；
3	使用渗透机对服务器渗透，将可渗透页面的名称作为 flag 提交；
4	使用渗透机对服务器渗透，并将网站中所用的数据库的表名作为 flag 提交；
5	使用渗透机对服务器渗透，将网站管理员的加密密码作为 flag 提交；
6	使用渗透机对服务器渗透，将服务器的本地名称作为 flag 提交。

模块 B-3：远程代码执行

（一）任务环境说明：

- ✓ 服务器场景：Server2207（关闭链接）
- ✓ 服务器场景操作系统：未知

（二）任务要求

序号	描述
1	使用渗透机对服务器信息收集，并将服务器中网站服务端口号作为 flag 提交；
2	使用渗透机对服务器信息收集，并将服务器中网站服务的版本号作为 flag 提交；
3	使用渗透机对服务器信息收集，并将服务器中网站漏洞作为 flag 提交；（如果为多个用;隔开）
4	使用渗透机对服务器渗透，并将服务器的主机名作为 flag 提交；
5	使用渗透机对服务器渗透，并将服务器网站载体程序名称缩写作为 flag 提交；
6	使用渗透机对服务器渗透，并将服务器中网站漏洞的文件名称作为 flag 提交。

模块 C　CTF 夺旗-攻击

时间：C+D 模块=180 分钟

分值：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。

模块 D　CTF 夺旗-防御

时间：C+D 模块=180 分钟

分值：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答题平台。

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。

附表1　评分表

A模块和D模块评分表另附。B模块和C模块评分表现场公布。