

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-C

一、竞赛时间

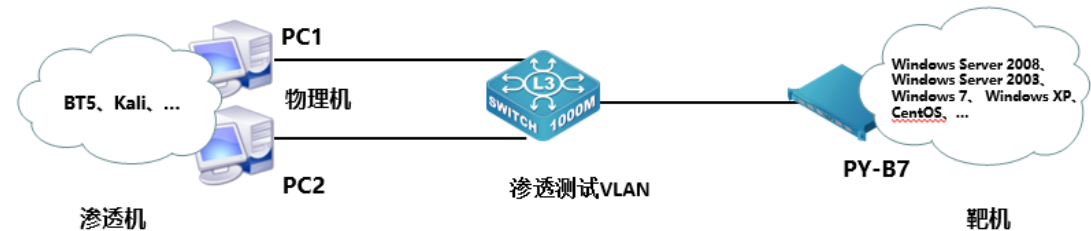
总计：180 分钟

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	页面信息发现		
	B-3	Linux 系统渗透提权		
	B-4	网络安全应急响应		
	B-5	网站渗透		
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，企业服务器可能被黑客攻击，进行了未知操作，为了确保服务器正常运行，请按照网络安全岗位实施规范，进行相关操作。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。

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 A-XX (XX 为工位号)，PDF 格式保存；
3. 文件保存到 U 盘提交。

二、服务器环境说明

AServer08(windows)、 用户名: administrator, 密码: 123456

AServer09(linux) 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. 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: 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: 日志监控 (Windows)

- 8. 安全日志文件最大大小为 128MB,设置当达到最大的日志大小上限时,按需要覆盖事件(旧事件优先);
- 9. 应用日志文件最大大小为 64MB,设置当达到最大的日志大小上限时将其存档,不覆盖事件;
- 10. 系统日志文件最大大小为 32MB,设置当达到最大的日志大小上限时,不覆盖事件(手动清除日志)。

A-4: 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. 限制本地用户登录活动范围限制在 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: 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. 在超过登录后强制注销。

A-6: 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 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;
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。

(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

- ✓ 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: 页面信息发现

✓ 仅能获取 win20230305 的 IP 地址

1. 在渗透机中对服务器信息收集, 将获取到的服务器网站端口作为 Flag 值提交;
2. 访问服务器网站页面, 找到主页面中的 Flag 值信息, 将 Flag 值提交;
3. 访问服务器网站页面, 找到主页面中的脚本信息, 并将 Flag 值提交;
4. 访问服务器网站页面, 找到登录页面信息, 将登录成功后的信息作为 Flag 值提交;
5. 访问服务器网站页面, 找到转化页面信息, 将 Flag 值提交;
6. 访问服务器网站页面, 找到对比页面信息, 将 Flag 值提交。

B-3: Linux 系统渗透提权

✓ 任务环境说明:

✓ 服务器场景: Server2214 (关闭链接)

✓ 用户名: hacker 密码: 123456

1. 使用渗透机对服务器信息收集, 并将服务器中 SSH 服务端口号作为 flag 提交;
2. 使用渗透机对服务器信息收集, 并将服务器中主机名称作为 flag 提交;
3. 使用渗透机对服务器信息收集, 并将服务器中系统内核版本作为 flag 提交;
4. 使用渗透机对服务器管理员提权, 并将服务器中 root 目录下的文本内容作为 flag 提交;
5. 使用渗透机对服务器管理员提权, 并将服务器中 root 的密码作为 flag 提交;
6. 使用渗透机对服务器管理员提权, 并将服务器中 root 目录下的图片内容作为 flag 提交。

B-4: 网络安全应急响应

✓ 服务器场景: Server2228 (开放链接)

✓ 用户名: root, 密码: p@ssw0rd123

1. 找出系统中被植入的后门用户删除掉, 并将后门用户的账号作为 Flag 值提交

（多个用户名之间以英文逗号分割，如：admin,root）；

2. 找出黑客在 admin 用户家目录中添加的 ssh 后门，将后门的写入时间作为 Flag 值（提交的时间格式为：2022-01-12 08:08:18）
3. 找出黑客篡改过环境变量文件并还原，将文件的 md5 值作为 Flag 值提交；
4. 找出黑客修改了 bin 目录下的某个文件，将该文件的格式作为 Flag 值提交；
5. 找出黑客植入系统中的挖矿病毒，将矿池的钱包地址作为 Flag 值（提交格式为：0xa1d1fadd4fa30987b7fe4f8721b022f4b4ffc9f8）提交。

B-5：网站渗透

✓ 仅能获取 lin20230509 的 IP 地址

1. 在渗透机中对服务器主机进行信息收集，服务器开启的端口号作为 Flag 值提交（多个用英文分号隔开）；
2. 在渗透机中对服务器主机进行渗透，获取服务器主机服务信息，将数据库服务版本号作为 Flag 值提交；
3. 在渗透机中对服务器主机进行渗透，将服务器端执行的脚本语言创建时间作为 Flag 值提交；
4. 在渗透机中对服务器主机进行渗透，将用于渗透服务器网站的页面的绝对路径作为 Flag 值提交（路径中 IP 地址用“IP”代替，例如 http://IP/index.php）；
5. 在渗透机中对服务器主机进行渗透，在服务器主机中获取主机信息，将服务器主机的内核版本作为 Flag 值提交；
6. 在渗透机中对服务器主机进行渗透，在服务器主机中获取主机文件信息，将 root 目录下 flag 文件的内容作为 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。