金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）

网络安全

BRICS-FS-28-RU

技术样题 TP(省级/区域选拔赛)

2024 年 04 月

目录

1 参加比赛的形式

大赛为单人参赛形式，每支队伍 1 名选手。

2 项目阶段简介

项目由四个阶段组成，将按顺序完成。向参与者提供答题说明、靶机信息、IP 地址分配表及信息地址分配表。

项目包括以下阶段：

1. 职业素养与理论技能；

2. 网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用；

3. 网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析；

4. 新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）与安全技能应用；

3 项目阶段和所需时间

序号	竞赛阶段	内容模块	竞赛时长（分钟）
第一阶段	职业素养与理论技能	职业素养与理论技能	60
第二阶段	网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用	网络攻防渗透与漏洞挖掘	90
		数据安全分析与应用	
第三阶段	网络安全运营技能应用，包括安全事件响应、安全	网络安全事件响应	90

	加固与溯源分析；	安全加固与溯源分析	
第四阶段	新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）安全技能应用	智能网联安全靶场挑战	60

表 1. 项目阶段列表

样题

4 第一阶段：职业素养与理论技能

背景：作为信息安全技术人员必须能够掌握操作系统安全基础、网络安全基础、数据库安全基础等相关基础知识，利用这些基础知识进一步学习信息安全技术掌握 WEB 漏洞挖掘、数据安全分析，从而具备成为高水平信息安全人员的基础。

理论阶段题目主要包含职业素养，漏洞挖掘，数据安全，应急响应，安全加固等相关内容，详细内容见下表：

序号	内容模块	说明
第一阶段（理论）	职业素养	网络安全规范意识、安全意识、纪律意识等；
	法律法规	《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》以及其他网络和数据安全相关法律法规和标准规范等。
	漏洞挖掘知识点	Web 漏洞原理知识、服务器漏洞原理知识、SQL 注入漏洞基本利用方法、文件操作漏洞基本利用方法、CSRF 漏洞基本利用方法、SSRF 漏洞基本利用方法、XSS 漏洞基本利用方法、XXE 漏洞基本利用方法、无恶意特征漏洞基本利用方法、信息泄漏漏洞利用方法、目录遍历漏洞利用方法、反序列化漏洞基本利用方法、未授权漏洞基本利用方法、命令/代码执行类漏洞利用方法；
	数据安全知识点	数据安全法规政策、数据安全基础理论、数据安全技术理论、数据安全管理流 程、数据安全评估、个人数据安全意识
	应急响应知识点	应急响应原理流程与排查、LINUX/windows 应急响应过程中所涉及的排查点,包括账户排查（特权账户、影子账户）、网络通信与端口排查、进程分析、 启动项分析、定时任务排查、服务分析、Webshell 排查、系统后门排查、常见 web 漏洞攻击特征判断、敏感信息漏洞利用特征、sql 注入漏洞利用特征；
	安全加固知识点	Windows 账户与密码的安全策略设置，用户和用户组的权限管理、审核，日志的启用使用安全模版来分析配置计算机。、Linux 系统中的账号和组、弱口令密码带来的风险、检查空口令的方法、检查系统中是否存在其它 id 为 0 的用户的方法、Linux 文件系统的文件格式分类；

4.1 项目 1.职业素养

1.在处理安全事件时，你应该首先做什么？

A. 尽快通知领导

B. 立即断开网络连接

C. 分析事件并采取适当的响应措施

D. 等待其他团队成员的指示

2.当你发现一个潜在的安全漏洞时，你应该怎么做？

A. 立即修复漏洞

B. 尝试利用漏洞来测试系统安全性

C. 报告漏洞给安全团队或管理层

D. 忽略漏洞，因为它可能并不重要

3.在处理敏感数据时，你应该遵循什么原则？

A. 尽可能分享数据

B. 只在必要时处理数据

C. 忽略数据安全性

D. 将数据存储在不安全的位置

4.在工作中，你发现一位同事正在未经授权的情况下尝试访问敏感数据。你应该怎么做？

A. 立即报告主管

B. 不予理睬，因为这可能只是一个误解

C. 私下询问同事原因

D. 自己处理，不告诉任何人

5.在处理安全问题时，保持沟通的重要性是什么？

A. 不重要，因为安全问题应该由专家解决

B. 很重要，因为团队合作可以加快问题解决速度

C. 有时重要，取决于问题的复杂性

D. 不确定，因为沟通可能会泄露敏感信息

6. 下面哪项是提高网络安全素养的有效途径？

A. 定期更改密码

B. 在公共网络上使用相同密码

C. 将敏感信息公开分享

D. 不使用防病毒软件

7. 哪种类型的培训对于提升网络安全职业素养最为重要？

A. 编程和软件开发课程

B. 社交技巧和演讲训练

C. 安全认证培训和实践经验

D. 体育锻炼和健康生活指导

4.2 项目 2.法律法规

1. 根据《中华人民共和国网络安全法》，网络运营者在保护网络安全方面，下列哪项不是其应当采取的措施？

A. 加密用户数据传输

B. 随意共享用户资料

C. 监控网络安全事件

D. 定期更新安全系统

2. 根据《关键信息基础设施安全保护条例》，下列哪项不是关键信息基础设施运营者的安全保护义务？

A. 建立健全安全管理制度

B. 定期培训从业人员

C. 随意公开运行状况

D. 制定应急预案

3. 依据《数据安全法》，开展数据处理活动应当依照法律、法规的规定，建立健全哪项管理制度？

A.谁处理谁负责

B.全流程数据安全

C.风险评估

D.应急处置

4. 根据《中华人民共和国个人信息保护法》，下列哪项行为不属于个人信息处理者的合规操作？

A. 合法收集个人信息

B. 未经同意公开个人信息

C. 加密存储个人信息

D. 告知信息处理的目的

5.根据《中华人民共和国密码法》规定，国家对密码实行

A 分级管理

B 集中管理

C 统一管理

D 分类管理

4.3 项目 3.安全漏洞挖掘

1. 漏洞挖掘的主要目标是什么?

A. 攻击网络系统

B. 发现系统中的漏洞并提供修复建议

C. 利用漏洞获取个人信息

D. 提高系统性能

2. 下列哪个步骤通常包含在漏洞挖掘的过程中?

A. 数据备份

B. 集中网络流量

C. 漏洞分析和验证

D. 制定市场策略

3. 哪种类型的漏洞挖掘是通过评估软件源代码进行的?

A. 静态漏洞挖掘

B. 动态漏洞挖掘

C. 社会工程学攻击

D. 网络钓鱼

4. 漏洞挖掘者通常会将发现的漏洞报告给谁？

A. 政府机构

B. 竞争对手

C. 软件供应商或维护团队

D. 公众媒体

5. 漏洞挖掘过程中使用的自动化工具通常用于做什么？

A. 发送钓鱼邮件

B. 分析社交网络数据

C. 加密文件

D. 扫描和识别潜在的漏洞

4.4 项目 4.数据安全

1. 数据加密的主要目的是什么？

A. 提高数据传输速度

B. 降低数据存储成本

C. 保护数据的机密性和完整性

D. 增加数据的可用性

2. 下列哪种方法不是保护数据安全的有效手段？

A. 使用强密码

B. 定期备份数据

C. 将敏感数据存储在公共服务器上

D. 实施访问控制策略

3. 在数据安全管理中，"DRM"一词通常指什么？

A. 数字资源管理

B. 数据恢复模式

C. 数据资源监测

D. 数据风险管理

4. 以下哪种情况不属于数据泄露的可能原因？

A. 网络攻击

B. 误操作

C. 加密数据

D. 内部泄密

5. 数据安全意识培训的目的是什么？

A. 限制员工的访问权限

B. 增强员工对数据保护的认识和技能

C. 加密所有数据

D. 降低网络带宽消耗

4.5 项目 5.应急响应

1. 应急响应计划的主要目的是什么？

A. 防止所有网络攻击

B. 降低网络流量

C. 快速有效地应对安全事件

D. 增加系统的复杂性

2. 下列哪个步骤不是应急响应过程中的关键步骤？

A. 识别和确认安全事件

B. 部署防火墙

C. 评估安全事件的影响

D. 通知相关利益相关者

3. 在应急响应中，"CSIRT"一词通常指什么？

A. 安全策略

B. 通信服务

C. 计算机安全事件响应团队

D. 安全训练课程

4. 下列哪种类型的安全事件不属于应急响应的范畴？

A. 数据泄露

B. 网络攻击

C. 用户密码遗忘

D. 恶意软件感染

5. 应急响应团队的主要职责是什么？

A. 增加系统性能

B. 修复所有安全漏洞

C. 协调应对安全事件

D. 制定安全政策

4.6 项目 6.安全加固

1. 安全加固的主要目的是什么？

A. 降低系统性能

B. 增加系统的复杂性

C. 提高系统的安全性

D. 扩大系统的功能

2. 下列哪种方法不是安全加固的常见手段？

A. 更新补丁和漏洞修复

B. 实施访问控制策略

C. 公开系统所有信息

D. 使用安全加密技术

3. 在安全加固中，"ACL"一词通常指什么？

A. 访问控制列表

B. 账户密码

C. 数据加密层

D. 网络协议

4. 下列哪种做法不符合安全加固的原则？

A. 定期审计系统安全性

B. 禁用不必要的服务和端口

C. 将所有用户设置为管理员权限

D. 加强身份验证机制

5. 安全加固过程中，"DMZ"一词通常指什么？

A. 数据管理区域

B. 防火墙区域

C. 反病毒软件

D. 系统备份区域

4.7 项目 7.新技术、新应用领域产生的网络安全挑战

1.工业互联网中的安全威胁主要包括哪些方面？

A. 网络攻击

B. 物理破坏

C. 数据篡改

D. 设备故障

2.人工智能在工业互联网中的应用有哪些安全挑战？

A. 数据隐私保护

B. 智能算法的安全性

C. 自动化设备的安全性

D. 数据分析的安全性

3.工业互联网中的安全加固措施包括哪些方面？

A. 设备密码管理

B. 数据加密传输

C. 安全漏洞修复

D. 网络监控和入侵检测

4.人工智能安全的主要挑战是什么？

A. 对抗性攻击

B. 数据隐私保护

C. 算法安全性

D. 自动化攻击

5 人工智能安全加固措施包括哪些方面？

A. 对抗性训练

B. 数据加密

C. 算法逻辑验证

D. 安全漏洞修复

6.人工智能在安全领域的应用有哪些？

A. 恶意代码检测

B. 安全事件响应

C. 威胁情报分析

D. 认证和授权管理

7. 智能网联汽车的主要特点是什么？

A. 仅提供基本的驾驶辅助功能

B. 完全不依赖传感器和网络连接

C. 能够与其他车辆和基础设施进行通信

D. 不具备自动驾驶能力

8. 下列哪种技术是智能网联汽车实现自动驾驶的关键？

A. 人工智能

B. 云计算

C. 深度学习

D. GPS 导航

9. 智能网联汽车的主要安全挑战是什么？

A. 电池寿命

B. 车身颜色

C. 网络安全和隐私保护

D. 引擎功率

10. 下列哪个是智能网联汽车所使用的关键技术之一？

A. 蒸汽动力

B. 液压制动系统

C. 人工智能

D. 涡轮增压器

11. 智能网联汽车的主要优势之一是什么？

A. 仅适用于城市道路

B. 增加交通拥堵

C. 提高交通安全性和效率

D. 降低汽车成本

5 第二阶段：网络与数据安全技能应用

背景：在当今数字化时代，数据安全和网络攻防渗透与漏洞挖掘成为信息安全领域的重要焦点。作为信息安全专业人士，我们的任务是确保企业网络和敏感数据的安全，同时主动发现并修补潜在的安全漏洞。数据安全涉及到保护数据的机密性、完整性和可用性，通过加密技术、访问控制和监控手段来防止未经授权的访问和数据泄露。而网络攻防渗透与漏洞挖掘则是针对系统和网络的主动测试和审查，以发现系统中的漏洞和潜在安全隐患。通过模拟攻击、渗透测试和漏洞挖掘，我们能够评估系统的安全性，并及时采取措施修补漏洞，从而提高系统的整体安全水平。综合运用数据安全和网络攻防渗透与漏洞挖掘技能，可以有效地保护企业的重要业务数据，提升网络安全防御能力，为企业的稳健运行和持续发展提供有力支撑。

网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用，详细内容见下表：

序号	竞赛阶段	内容模块	说明
第二阶段	网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用	网络攻防渗透与漏洞挖掘	使用漏洞探测工具成功探测到 Web 漏洞、使用漏洞探测工具成功探测到网络服务脆弱性、使用漏洞探测工具成功探测到服务器漏洞；利用弱口令进行爆破、利用文件类漏洞获取敏感文件、利用文件类漏洞上传恶意代码、利用命令执行漏洞运行恶意命令、利用 SQL 注入漏洞获取数据库信息、利用 XSS 漏洞实现恶意代码注入和执行、利用目录遍历漏洞访问任意文件、利用 XXE 漏洞执行探测和攻击、利用 CSRF 漏洞伪造请求、利用 SSRF 漏洞伪造请求、通过信息泄露漏洞访问敏感信息、
		数据安全分析与应用	主要考察选手数据包分析、数据取证等能力；敏感信息泄露、数据分类、数字水印技术、常见加解密算法等内容

5.1 项目 1.网络攻防渗透与漏洞挖掘

任务一、网站漏洞挖掘

某公司的网站近期遭受了多次未知攻击，安全团队怀疑网站存在漏洞，需要你进行渗透测试。你获得了该网站的访问权限，并发现网站使用了一种新型的漏洞防护技术，使得常规的攻击方法无效。你需要深入分析网站结构和代码，找到漏洞并获取网站的 webshell 权限，以获取 flag 值。

1.点击平台中的，获取题目场景按钮，获取题目下发环境，然后对下发的网站进行渗透，获取网站 webshell 权限之后即可获取 flag 值，并对该 flag 进行提交。

任务二、web 攻防渗透

一家电子商务公司的网站遭受了一系列黑客攻击，导致用户数据泄露和系统瘫痪。作为安全专家，你被委派对网站进行渗透测试，发现网站存在多个漏洞，包括 SQL 注入漏洞、权限提升漏洞等。你需要利用这些漏洞获取网站的 flag 并

提交，以揭示网站的安全隐患，帮助公司加强安全防护。

1.利用题目环境中存在的 sql 注入漏洞，flag 在数据库中，尝试获取数据库数据中的 flag,并提交该 flag.

2.利用题目环境中存在的漏洞，对靶机服务器进行 getshell，在服务器根目录下获得 Flag 进行提交；

3.利用题目环境中存在的漏洞，对靶机服务器进行权限提升，在服务器/root/目录下获得 Flag 进行提交。

5.2 项目 2.数据安全分析与应用

任务一、敏感数据泄漏分析

某 PHPCMS 部署于企业 DMZ 区，但近期针对该 CMS 爆出了 RCE-0day，使得攻击者通过 0day 上传了 webshell，并通过该 webshell 上传了某热门 C&C 工具。最终在安全网关处发现有数据外泄行为。通过应急响应小组排查分析以及全流量回溯设备，发现泄密事件 2 起，C&C 通道 1 个，落地 webshell 文件 1 个。可惜的是，攻击者隐藏了部分流量，因此 0day 攻击与上传过程流量未成功抓取。根据上述背景，回答以下问题，并将答案提交到平台，平台会自动进行判分：

1.攻击者上传的 webshell 文件名是什么？例如 1.php

2.攻击者获取到的秘密值 1 是什么？格式：小写 UUID 例如 e7e4dd79-9505-3863-be33-5af0352ce7b6

3.C&C stager client 请求下载的 dll 的相对地址是什么？例如：对于 URLhttp://1.1.1.1/SI0 那么答案为/SI0

4.C&C 经攻击者修改后的心跳间隔是多少秒？例如：1

5.攻击者获取的 secret2.txt 文件的 MD5 值是什么？注意：是下载下来的文

件(secret2.txt)的 MD5 值，不是下载文件命令/下载参数的 MD5 值。格式：小写 md5 例如 84f0feb07beae896d471f45527d781b0

6 第三阶段：网络安全运营技能应用

背景：在网络安全运营中，安全事件响应、安全加固和溯源分析是至关重要的技能。安全事件响应是指及时有效地应对网络安全事件，迅速减少潜在损失。通过建立完善的安全事件响应团队和流程，可以快速识别、确认和处置安全事件，最大程度地降低安全风险。安全加固则是通过对系统和网络进行加固措施，提升其安全性，减少潜在漏洞和攻击面。这包括加强访问控制、更新补丁、配置防火墙等措施，从而有效地防范各类安全威胁。而溯源分析则是通过对安全事件的溯源追踪，发现事件的源头和传播路径，从而帮助防范未来类似攻击。通过对网络流量和日志的分析，结合数字取证技术，可以有效地追踪攻击者的行为轨迹，为后续的安全防御提供重要参考。综合运用安全事件响应、安全加固和溯源分析等技能，可以有效地提高网络安全的防御能力，保障企业网络和数据的安全。

网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析，详细内容见下表：

序号	竞赛阶段	内容模块	说明
第三阶段	网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析；	网络安全事件响应	主要考查学生对入侵检测、抑制处置、系统恢复、证据收集等知识点的掌握和运用能力。
		安全加固与溯源分析	安全加固考查学生如何增强系统防御能力，而溯源分析则检验学生追踪攻击来源、分析攻击路径的能力。

6.1 项目 1.网络安全事件应急响应

任务一、攻击事件应急

你是某公司的一名安全工程师,有一天,你的同事小李在使用部门一台 linux 终端时发现电脑有些异常卡顿，好像是被大黑客攻击了。小李通过溯源，发现攻击流量源自于网络出口处的一台部署了 web 服务的 windows 终端上,通过软件进行扫描后在该 web 服务器上发现了 sql 注入漏洞。小李将当天下午可能与攻击相关的流量导出后，放置在了 windows 终端的桌面位置，你可以使用公司为你提供的 wireshark 对其进行分析,然后登录 windows 服务器和 linux 终端进行攻击溯源、排查等工作。

本任务素材清单：windows 服务器，linux 服务器

受攻击的服务器已经在竞赛平台中部署完成，可以直接进入系统进行分析取证。windows 用户密码，administrator：com.1234，linux 用户密码，root：com.1234。

请按要求完成该部分工作任务，答案具有唯一值。获取答案后请在平台提交，提交后平台会自动进行判分，回答正确则获取该题分数。

1.攻击者对网页 SQL 漏洞进行利用的 IP 地址是？

2.攻击者注入的一句话木马的密钥是？

3.攻击者一共使用一句话木马进一步向终端上传了文件的数量？（提交阿拉伯数字）

4.攻击者使用一句话木马上传文件访问的 VPS 的 ip 地址是？

5.攻击者创建的用户用户名为？

6.黑客创建了会每隔一段时间自动回连的后门，其连接的恶意服务器的 ip 地址和端口号是？（10.10.10.10:80）

7.木马进程可执行文件的绝对地址是？

8.黑客创建用户密码的 salt 值为？

9.本 linux 终端处于内网环境，黑客的跳板机 IP 地址是（内网 IP）？

10.黑客最后在什么时间成功登录到本终端的？

11.黑客下载、执行挖矿病毒的命令是？

12.黑客连接的恶意域名和端口是？(www.baidu.com:80)

13.从 VPS 下载作为后门的 ssh 公钥的完整地址是（10.10.10.10/folder/file）？

6.2 项目 2.安全加固与溯源分析

任务一、安全加固

作为公司的安全工程师，你负责对公司服务器进行安全加固，以防止未来类似的攻击事件再次发生。

场景： 最近公司的网络系统遭受了一系列的勒索软件攻击，导致公司的业务受到了严重影响。经过初步调查发现，攻击者通过利用某个员工的电脑，成功进入公司内部网络，并在其中一台服务器上植入了恶意软件。为了防止类似事件再次发生，你被委派负责加固公司的服务器安全。

1.请检查服务器相关弱口令，并对相关弱口令进行修改，修改成功后，点击平台上的 check 按钮进行检测，检测成功后即可获取对应分数，加固失败则显示失败。

2.请检查服务器上的 redis 服务，限制 redis 服务只可以由本地访问，其他任何地址均无法访问，加固完成后点击平台上的 check 按钮进行检测，检测成功后即可获取对应分数，加固失败则显示失败。

任务二、攻击溯源分析

作为公司的安全工程师,你被委派负责对公司内部网络中的一起安全事件进行溯源分析。以下是该安全事件的场景和要求：

场景： 最近，公司内部网络遭受了一次未经授权的访问事件，导致公司的一些敏感数据受到了泄露。初始调查显示，攻击者通过某个员工的帐户成功登录了公司的服务器，并从其中一台服务器上窃取了数据。为了找出攻击者的身份和攻击路径，你被指示对公司的网络流量和系统日志进行深入分析。

1.网络流量分析： 使用 Wireshark 或类似工具对攻击发生时段的网络流量进行分析，找出攻击者使用的 IP 地址以及他们与公司服务器之间的通信情况，并在平台上进行提交。

2.系统日志审查： 登录公司的服务器，查看系统日志并分析攻击发生时段内的登录记录、命令执行记录等信息，以确定攻击者是如何登录并操作服务器的。

3.恶意软件检测： 对公司服务器上的文件系统进行扫描，查找是否存在恶意软件或后门程序，并确定它们是如何被安装和激活的，找到后在平台提交恶意软件名称。

4.跳板机追踪： 查找攻击者可能使用的跳板机，以确定他们是如何隐藏真实身份并窃取数据的，找到后在平台上提交跳板机的 IP 地址。

7 第四阶段：新技术网络安全技能应用

背景：

智能网联汽车通过连接车辆与互联网，提供丰富的服务和功能，但也带来了安全风险，如远程劫持、数据泄露和恶意攻击等问题。因此，网络安全技能在智能网联汽车领域的应用变得尤为重要，以保障车辆及乘客的安全。

新兴领域网络安全技能应用，包括智能网联汽车安全检测，详细内容见下表：

序号	竞赛阶段	内容模块	说明
第四阶段	新技术、新应用领域产生的网络安全挑战（如智能网联汽车、物联网、人工智能）安全技能应用	智能网联安全靶场挑战	通过虚拟环境中模拟的车辆车机功能，尝试利用多种痛惜协议对车辆实现指令发送并通过指令实现控制车辆要求。

7.1 项目 1.智能网联安全靶场挑战

任务一、车内通信靶场

1、某 OEM 模拟了其生产的某款车型的通信网络，请尝试分析 CAN 通信指令，通过 CAN 指令控制车辆；选手利用成功之后即可在平台中点击 check 按钮进行自动化检测，平台会自动运行检测机制，检测成功之后选手即可自动获得该题分数。

任务二、IVI 风险评估

1、某 OEM 车型 IVI 被黑客入侵，远程窃取了用户敏感信息，请分析某 OEM 提供的 IVI 仿真环境，找到 IVI 存在的脆弱点。通过利用该脆弱点，获取车辆中的敏感信息，并将该敏感信息提交至平台，平台进行自动判分，正确后即可获得对应题目分数。

任务三、车内智能传感器通信测试

1.通过车辆操作平台确认能否正常获取激光雷达点云数据,并确认标定结果是否正确。

1.1 主控单元及左右控制单元网络配置确认。

1.2 激光雷达主机网络配置。

1.3 数据交互配置。

2. 通过车辆操作平台确认能否正常获取毫米波雷达与超声波雷达数据，并确认通道与数据是否正确。

2.1 数据交互的 CAN 通道信息配置。

2.2 数据的获取与分析。