2025

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

样题(国际总决赛)

2025 年 11 月

目录

1. 参赛形式

2025 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）网络安全赛项参赛形式为双人赛。

2. 竞赛内容

大赛由四个阶段组成，信息如下表所示：

序号	考核内容
第一阶段	职业素养与理论技能
第二阶段	网络与数据安全技能应用
第三阶段	网络安全运营技能应用
第四阶段	新技术、新应用领域产生的网络安全挑战 （可信数据空间安全）

只有竞赛现场无法完工且经首席专家批准的情况下，才能更改竞赛任务和评分标准。如果参赛选手不遵守职业健康安全环境要求，或使自己和其他选手面临危险，可能会被取消比赛资格。参赛者完成所有阶段后，将对结果进行评分。

3. 大赛阶段和时间要求

网络安全赛项共 4 个阶段，要求选手在每个阶段规定时间内完成。具体阶段名称和时间要求参照如下：

序号	阶段考核内容	比赛时长（分钟）
第一阶段	职业素养与理论技能	30
第二阶段	网络与数据安全技能应用	70
第三阶段	网络安全运营技能应用	90
第四阶段	新技术、新应用领域产生的网络安全挑战（可信数据空间安全）	50

4. 任务内容

4.1. 第一阶段样题

1. 以下哪项不属于参赛选手应具备的职业素养范畴？（ ）

A. 网络安全规范意识

B. 严格遵守工作和竞赛纪律

C. 主动预防安全风险

D. 忽略任务时间节点

2. 《中华人民共和国数据安全法》的实施时间是（ ）。

A. 2016 年 6 月 1 日

B. 2017 年 6 月 1 日

C. 2021 年 9 月 1 日

D. 2020 年 12 月 1 日

3. 以下哪项不属于常见的 Web 漏洞？（ ）

A. SQL 注入

B. 跨站脚本（XSS）

C. 跨站请求伪造（CSRF）

D. 端口扫描

4. 数据安全的三大基本属性是（）。

A. 机密性、完整性和可用性

B. 机密性、及时性和可用性

C. 可靠性、完整性和可用性

D. 机密性、完整性和可扩展性

5. 在应急响应流程中，以下哪项不是常见的排查内容？（）

A. 账户排查

B. 网络通信与端口排查

C. 系统后门排查

D. 系统硬件规格排查

6. Windows 系统中，以下哪项是强密码策略的设置要求？（）

A. 密码长度最少为 3 位

B. 密码可以包含用户名

C. 密码必须包含大写字母、小写字母、数字和特殊字符中的三类

D. 密码可以长期不更换

7. Linux 系统中，用于检查空口令用户的命令是（）。

A. cat /etc/shadow | awk -F: '$2 == "" {print $1}'

B. ls -l /etc/passwd

C. net user

D. chkconfig --list

8. 以下哪项不是数据生命周期管理的环节？（）

A. 数据创建

B. 数据存储

C. 数据销毁

D. 数据克隆

9. 在应急响应中，识别 Webshell 文件常用的方法是（ ）。

A. 检查文件创建时间

B. 分析文件内容特征（如可疑代码）

C. 查看文件大小

D. 根据文件扩展名判断

10. 以下哪项是《关键信息基础设施安全保护条例》的主要监管对象？（ ）

A. 普通企业网站

B. 个人博客

C. 关键信息基础设施运营者

D. 社交媒体账号

4.2. 第二阶段样题

4.2.1. 任务描述一

你是一名网络安全研究员，在调查一个名为“知识之海”的在线书店时，发现其用户登录功能可能存在 SQL 注入漏洞。该书店的用户数据（包括用户名和密码）存储在一个名为 users 的数据库表中。你的任务是利用这个漏洞获取管理员账户的用户名和密码。

4.2.2. 解答示例

- 首先，尝试向登录页面的用户名和密码输入框中分别输入' OR '1'='1 和任意

值，观察页面是否返回异常或错误信息，以验证是否存在 SQL 注入漏洞。

- 如果存在漏洞，通过构造查询语句' UNION SELECT username, password FROM users WHERE username='admin，获取管理员账户的用户名和密码。
- 在获取到管理员的用户名和密码后，使用这些凭据登录后台管理系统，找到包含敏感信息的文件或页面，提取隐藏的 flag（例如：flag{admin_password_is_123456}）。

4.2.3. 任务描述二

在对某公司邮件服务器进行安全评估时，你截获了一段网络通信数据，其中包含一份加密的附件文件。据推测，该附件可能包含敏感信息，如员工工资单或公司机密合同。你的任务是分析数据包，提取附件并解密其中的内容。

4.2.4. 解答示例

- 使用 Wireshark 或其他网络分析工具打开提供的.pcap 文件，查找与邮件传输相关的流量（如 SMTP 或 IMAP 协议的数据包）。
- 在邮件附件的数据包中，提取出加密的附件内容。注意附件可能使用 Base64 或十六进制编码。
- 分析附件的文件头信息，确定加密算法（如 AES 或 RSA）。
- 根据题目提示，尝试使用常见的加密密钥（如 password123 或 flag{}）进行解密。例如，如果附件使用 AES 加密，可以尝试使用 AES 工具或 Python 脚本进行解密。
- 解密后，找到隐藏的 flag，如 flag{sensitive_data_leakage_detected}。

4.3. 第三阶段样题

4.3.1. 任务描述一

公司办公室网络中有多台员工电脑，某天网络管理员发现网络流量异常，部分员工电脑出现蓝屏现象。怀疑有恶意软件在内网中传播，需要你进行调查和处理。

4.3.2. 解答示例

- 入侵检测：分析内存转存文件，查找可疑的进程和服务，例如未知的网络连接或恶意软件特征。查看网络流量统计图表，识别出流量异常的 IP 地址，这些可能是受感染的电脑或攻击源。
- 抑制处置：在网络中隔离受感染的电脑，防止恶意软件进一步传播。
- 终止内存中发现的可疑进程，阻止恶意软件继续运行。
- 系统恢复：对受感染的电脑进行病毒扫描和清除，使用安全软件查杀恶意软件。
- 恢复受影响的系统文件和服务，确保电脑正常运行。
- 证据收集：提取内存文件中的恶意软件样本和相关网络信息，作为调查的证据。
- 记录受感染电脑的 IP 地址、感染时间和症状等信息。

4.3.3. 任务描述二

公司的云平台服务器遭受了攻击，部分数据被窃取。需要你对云平台的日志和网络流量进行分析，找出攻击来源和攻击路径，并提出安全加固方案。

4.3.4. 解答示例

- 溯源分析：分析云平台服务器的访问日志，查找异常的登录记录、API 调用记录等，确定攻击者是如何进入系统的。
- 检查网络流量数据,找出与攻击相关的入站流量源 IP 和出站流量的目标 IP，追踪数据泄露的路径。
- 安全加固：根据溯源分析的结果，加强云平台的访问控制，例如限制 IP 访问白名单、加强身份验证等。
- 更新云平台的安全策略，关闭不必要的端口和服务，减少攻击面。
- 对云平台服务器进行补丁更新，修复已知的安全漏洞。
- 追踪攻击路径：通过日志和网络流量的关联分析，还原攻击者从入侵到数据窃取的完整过程，包括使用的攻击工具和方法。

4.4. 第四阶段样题

4.4.1. 任务描述

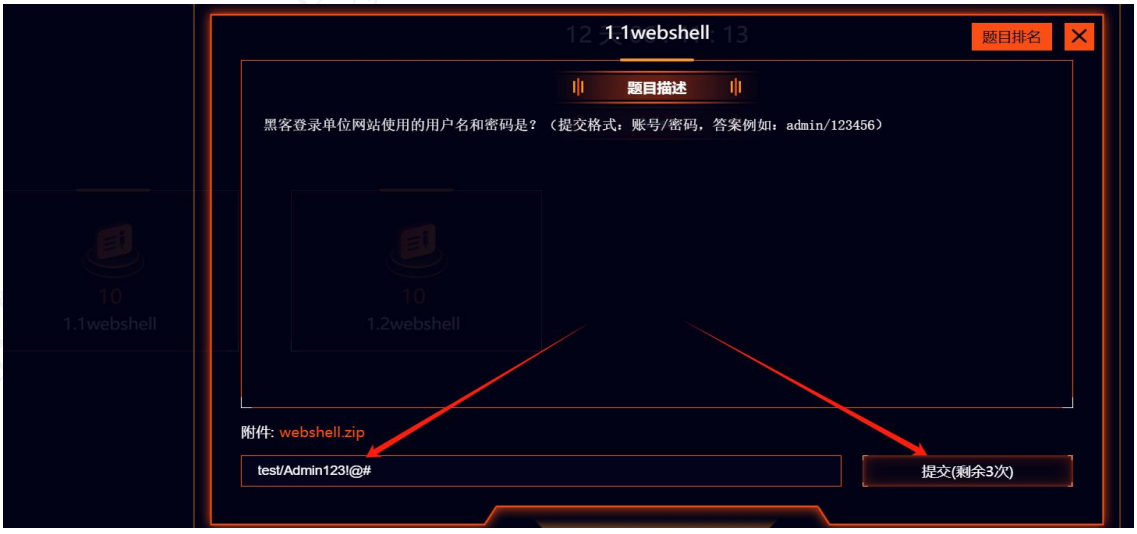
昨日，A 公司入侵检测设备检测到单位网站被黑客挂马，公司为了溯源黑客入侵痕迹，从入侵检测设备中导出相关数据包。作为单位数据防护人员，协助 A 公司对数据包(数据包名为 hack.pcap)进行分析，并寻找如下相关问题答案：

- 第一问：黑客登录单位网站使用的用户名和密码是？（提交格式：账号/密码，答案例如：admin/123456）
- 第二问：黑客入侵单位网站后，往服务器内写入的 webshell 的文件名是？（输入时请包含文件的扩展名，答案例如：webshell.txt）

4.4.2. 解答示例

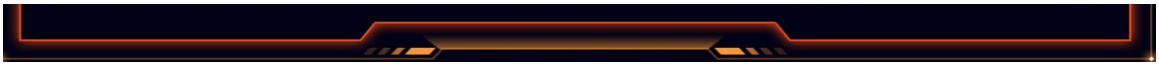
使用 wireshark 打开 hack.pcap，在 tcp.stream eq 6 中找到黑客登录的用户名和密码，并且服务器回显为 200

可以发现用户名为 test，对密码进行 url 解密得到 Admin123!@#，所以第一问最终答案为 test/Admin123!@#，将该答案提交至平台题目名为：1-1webshell 的输入框中，并点击提交



回答正确平台会告知并获得该问得分（正确的情况）

回答错误平台会告知并扣除答题机会（错误的情况）



注意：如图所示命令返还结果信息为错误的结果。则表示并没有完成本题目。则本题目没有成绩！