数据安全综合场景赛场景说明文档

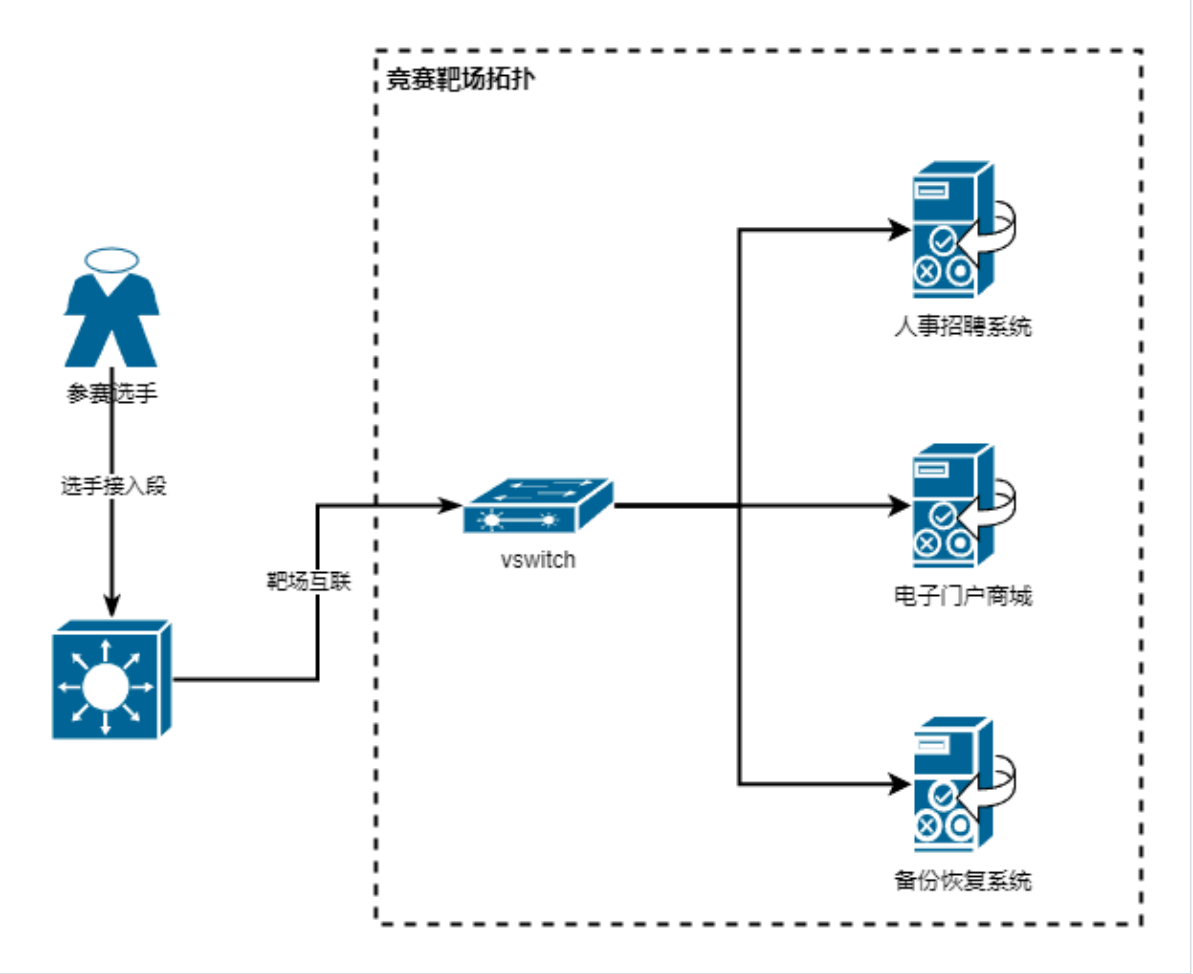
场景说明

在这个场景中，某公司需要对三个系统进行全面的数据安全评估。参赛团队应从数据安全的角度出发，系统性地分析数据在整个生命周期中的各个环节，包括采集、传输、存储、利用、共享和销毁等。团队可以运用以下能力进行深入评估：

1. 日志分析：通过分析系统日志和网络日志，识别攻击痕迹和异常行为，以确定黑客入侵的方式和时间点。
2. 流量溯源：跟踪黑客的攻击路径，识别攻击者的入侵来源及其在系统内的活动，帮助了解攻击的途径和范围。
3. 泄露数据识别：检测数据包中的敏感信息或异常流量，以识别黑客是否泄露了敏感数据，进而确定被盗信息的类型和数量。
4. 数据加解密算法：评估所使用的数据加密算法及密钥管理机制的安全性，查找可能存在的漏洞或弱点。
5. 敏感数据识别：运用机器学习或正则表达式等技术，识别和标记敏感数据（如身份证号码、银行账户信息等），以确认黑客可能盗取的敏感数据。
6. 数据生命周期管理：全面管理数据从采集到处理、分析、共享、保护直至销毁的全过程，确保各环节的安全性。
7. 分类分级：根据数据的重要性和安全级别对数据进行分类分级，以确定相应的保护措施优先级和范围。
8. 安全评估与漏洞修复：识别和修复系统中的安全漏洞，以提升整体安全性。

场景拓扑

当前数据安全综合场景的模拟拓扑如下：



场景简述

人事招聘系统：公司人事招聘业务网站是一个专为招聘和求职者设计的平台，旨在促进企业与求职者之间的连接。它提供职位发布、简历搜索、在线申请和筛选工具，帮助企业高效找到合适人才，同时为求职者提供丰富的职位信息和职业发展资源。通过该网站，双方可以轻松沟通和互动，从而提升招聘效率和求职成功率。

电子门户商城：电子门户商城是一个集中展示和销售商品的在线平台，用户可以通过浏览、搜索和筛选功能轻松找到所需产品。它支持多种支付方式和配送服务，提供便捷的购物体验。同时，商城通常还包含用户评价、促销活动和客服支持，以提升消费者的满意度和忠诚度。通过数据分析，商家可以优化产品供应和市场策略，从而推动销售增长。

备份恢复系统：用于保障系统中数据的安全，防止被数据勒索，建立了数据备份与恢复制度。数据安全管理人员按照数据备份与恢复制度使用数据备份恢复工具`myback`将文件备份到`backserver`服务器中。备份工具`myback`为数据安全管理人员从互联网上下载的非可信备份工具 ，该工具的保存目录为`/root/backup`， 备份文件为工具目录下的`202410311935.bak`文件。备份恢复系统用户名密码为：`root/KKERPKThkPP9AYeY`

场景题干

场景一：数安评估

考题1：请选手通过数据安全评估手段分析人事招聘系统，接管因未授权所造成的功能或接口隐患，并将其企业会员拉美科技有限公司手机号作为答案提交。

【答案标准】例：若获取的手机号为13812345678，则最终答案为：13812345678。

考题2：请选手通过数据安全评估手段分析人事招聘系统，获取该系统的shell权限，并将系统用户uid为1000的用户名作为答案提交。

【答案标准】例：若系统uid为1000的用户名为admin，则最终答案为admin。

场景二：数据恢复

考题1：请选手通过数据安全评估手段分析人事招聘系统，找到被加密的核心配置文件，并根据网站环境配置，恢复其源码并将源码中存在的flag作为答案提交。

【答案标准】例：若获取的flag内容为：flag{ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c}。则提交最终答案为：ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c。

考题2：请选手通过数据安全评估手段分析人事招聘系统,人事招聘系统同时向四位领导发送了同一批员工的联系方式。为了保护这些敏感数据，系统使用RSA算法对信息进行了加密。然而，在传输过程中，数据遭到了截获。现在，请根据给定的流量包(user.pcapng)和数据库qs_boss表信息还原这些联系方式的明文并将侯秀华的手机号作为答案提交。

【答案标准】例：若侯秀华的手机号为13812345678，则最终答案为：13812345678。

场景三：数据识别

考题1：请选手通过数据安全评估手段分析人事招聘系统，现有一批职业数据遭受了内部员工泄漏，好在人事招聘系统使用了数字水印技术，请你根据水印统计内部各个员工泄漏的图片数量，并从大到小进行排序。（访问人事招聘系统的/upload/watermark/水印.zip下载附件）

【答案标准】例：若最终统计结果张三100张，李四200张，则最终提交答案为：李四-200,张三-100。

考题2：请选手通过数据采集手段，根据附件的《会员信息.xlsx》逐个登录"电子门户商城"系统，获取每个会员的电子邮箱信息，并统计使用Gmail邮箱的会员人数，作为答案提交。

【答案标准】例：若最终统计使用Gmail邮箱的会员人数为5。则提交最终答案为：5。

考题3：请选手找到"电子门户商城"系统发布的“加密发票数据”，通过技术手段和线索获取的方式。解密获取发票数据内容，并从发票中提取订单号，根据订单信息统计100张发票中，使用”微信H5支付“的人数，作为答案提交。

【答案标准】例：若最终统计使用”微信H5支付“的人数为5。则提交最终答案为：5。

场景四：数据治理

考题1：现发现"电子门户商城"系统的某些用户存在订单数据高频访问，当前系统策略为“单个会员用户1分钟内订单提交次数大于等于5次属于数据高频访问行为”。请统计出当前系统中存在高频访问行为的订单数量，作为答案提交。
例如：
在时间区间：2024-01-01 17:46:00 - 2024-01-01 17:47:00，发现用户13900000001 有6次订单提交记录，则该6次订单均属于高频访问行为订单。
注意：时间区间计算均从某一分钟的0秒到下一分钟的0秒计算。

【答案标准】例：若最终统计存在数据高频访问行为的订单数为50。则提交最终答案为：50。

考题2：为提升企业内部数据安全等级，现需要对"电子门户商城"系统数据库中Classification_DB库进行数据分类分级，请访问并远程连接数据库进行分类分级。已知Classification_DB的用户名为Classification_DB，登录密码与访问端口需自行探测。
Classification_DB里存放了100张表（表名：table1-table100）；每张表都存在10列数据，共计1000列（列名：c1-c1000）；列名与表名对应（表table1的列名为c1-c10，表table2的列名为c11-c20，以此类推）;每列都有5条相同类别的数据，整个数据库共计5000条数据。请根据《数据分类分级规则.xlsx》对c1-c1000列数据进行分类，完成分类后将列名与规则编号对应，拼接为一行字符串，进行一次MD5加密，将加密后的字符作为答案提交。
【答案标准】假设数据库中c1-c5列的数据分别为：
c1：男,女,男,女,男
c2：张三,李四,王五,张三,赵六
c3：192.168.1.1,172.16.1.1,8.8.8.8,223.5.5.5,114.114.114.114
c4：本科,小学,大专,研究生,本科
c5：13900000001,13900000002,13900000003,13900000004,13900000005
则根据《数据分类分级规则.xlsx》识别可得
列名:c1，数据类别：个人一般基本信息，规则编号：1-2
列名:c2，数据类别：个人敏感基本信息，规则编号：1-3
列名:c3，数据类别：个人设备信息，规则编号：2-2
列名:c4，数据类别：个人教育信息，规则编号：4-1
列名:c5，数据类别：重要个人联系及通信信息，规则编号：3-2
则按照列名1:规则编号;列名2:规则编号;列名3：规则编号…… ，拼接列名与规则编号可得字符串
c1:1-2;c2:1-3;c3:2-2;c4:4-1;c5:3-2
对该字符串进行一次小写md5加密获得：77bf2c8e0f67d58615da78d21084b087，则提交最终答案为：77bf2c8e0f67d58615da78d21084b087。
这里给出最终正确答案md5值的部分内容供选手参考：ecaxxxxxxxxxxxxxxxxxxxxxxxxxxxedc。
同时给出前10列与最后10列的分类分级结果供选手参考：
前10列正确答案：c1:2-1;c2:2-2;c3:1-1;c4:1-4;c5:4-2;c6:1-4;c7:2-2;c8:3-2;c9:3-1;c10:1-3
后10列正确答案：c991:3-1;c992:2-2;c993:3-1;c994:1-1;c995:4-2;c996:1-2;c997:1-3;c998:1-1;c999:4-1;c1000:3-1

考题3：为提升企业内部业务的数据安全等级，现需要利用同态加密技术来加密订单系统中的价格信息。请选手访问"电子门户商城"系统的8080端口，使用提供的同态库与开发文档来加密订单数据。完全按要求加密成功后，通过接口获取flag作为答案提交。
【答案标准】例：若获取的flag内容为：flag{ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c}。则提交最终答案为：ddc80d31-ca1d-43b7-b97d-7f6bd6e6b85c。

场景五：数据备份

> 考题1：请选手分析备份恢复系统中的备份工具`myback`程序，获取备份工具的版本信息。版本信息为一串类似 `***.***.***` 的字符串，注意星号不具有占位意义，不代表具体的字符串长度。
>
> 【答案标准】例：若获取的版本信息为：`123.456.789`，则提交的答案为：`123.456.789`。

> 考题2：请选手分析备份恢复系统中的备份恢复工具`myback`中的备份/恢复逻辑，找到用于解密的密钥。
>
> 【答案标准】例：若找到用于解密的密钥为字符串`123456`。则提交最终答案为：`123456`。

> 考题3：请选手分析备份恢复系统中的备份恢复工具`myback`在生成备份文件的逻辑，发现备份工具使用一种常见的方式来校验备份文件的完整性，并且将生成的完整性校验字符串保存在了备份文件中，请选手分析备份恢复工具，找到备份文件`202410311935.cbak`完整性校验值。
>
> 【答案标准】例：完整性的校验值使用字符串的形式提交，如若完整性校验值的16进制为`3A 32 33 34 35 36 37 38 39 30`，则应提交的答案为`3A323334353637383930`，空格仅为显示效果，非答案中字符。答案中所有的英文字符均为大写字符。

> 考题4：攻击者修改了备份文件，导致某些文件无法被成功恢复出来（`202410311935.cbak`已被攻击者修改）。请选手分析备份恢复系统中的备份恢复程序`myback`，结合现有的备份文件`202410311935.cbak`修复备份文件，使之能够成功恢复出所有的文件，其中有个文件包含有商城门户网站部分的源码，将这个文件的Md5作为答案提交。
>
> 【答案标准】例：若某个a.zip文件中包含有商城源码文件，则计算a.zip文件的32位小写Md5字符串。将此md5字符串作为答案提交。

> 考题5：备份文件经过修复后将所有文件成功地恢复了，但是发现有一个未知的文件，经过简单分析后，确认是攻击者留下的后门程序，请选手分析备份恢复系统中的后门程序，确定后门程序连接服务的地址/域名和端口。
>
> 【答案标准】例：若分析得到的后门服务器的IP的为127.0.0.1或者分析得到服务器的域名为mst.com，对应的连接端口为1234，则提交的答案为：IP `127.0.0.1:1234` 或者域名 `mst.com:1234`。