新型数据安全治理赛参赛手册

参赛选手需登陆新型数据安全治理赛平台，平台会为参赛选手分配操作机及赛题相关服务器，参赛选手需通过远程桌面的方式登陆操机，并根据操作机桌面上的《ZL01新型数据安全治理参赛手册》进行赛题作答。比赛平台操作手册详见第四章。

一、比赛内容

**（一）数据脱敏**

本题主要考察参赛选手按照给定脱敏规则对数据库中指定字段进行脱敏的能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 数据库 | Oracle 库 |

**注：服务器IP地址及用户名密码详见《ZL01新型数据安全治理参赛手册》**

**2.赛题要求**

按照下表要求对数据库中的数据进行脱敏。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **库** | **表** | **字段** | **要求** |
| **1** | orcltt | 个人联系信息 | Mobile | 值为手机号的：  替换最后四位数字 |
| **2** | orcltt | 合同基本信息 | ContractAmount | 全部匿名化为:  \*\*\*\*\*\*\*\*\*\* (10个\*) |
| **3** | orcltt | 交易对手信息 | Account | 替换为：100000 |
| **4** | orcltt | 金额信息 | CTCurrency | 值为“人民币”的替换为：元  其他值替换为：其他 |

**3.推荐工具**

数据脱敏工具。

**（二）敏感数据识别**

本题主要考察参赛选手识别数据库中指定敏感类型的字段能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 数据库 | Oracle 库 |

**注：服务器IP地址及用户名密码详见《ZL01新型数据安全治理参赛手册》**

**2.赛题要求**

对数据库中涉及下表列出的敏感类型的数据进行识别操作，并将每种敏感类型数据的识别规则相关信息记录在操作机桌面上的《ZL02敏感数据识别结果表》中。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **敏感类型** | **数据库名** | **表名** | **字段名** | **识别规则（正则/字典/无规律）** | **正则表达式** | **字典** |
| 用户ID | DB | Table | ID | 正则 | [A-Za-z]{6}\d{6} | / |
| 地址 | DB | Table | Address | 无规律 | / | / |
| 性别 | DB | Table | gender | 字典 | / | 男|man|male|女|woman|female |

**注：上表内容仅为示例，非考试内容，敏感类型、数据库名、表名、字段名已提供，选手仅需填写表格中的识别规则、正则表达式、字典三列内容。**

**3.推荐工具**

敏感数据发现工具、数据分类分级工具。

**（三）数据备份**

本题主要考察参赛选手备份、恢复数据库的能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 数据库A | Oracle A库 |
| **2** | 数据库B | Oracle B库 |
| **3** | 备份管理服务器 | 备份管理 |
| **4** | 备份介质服务器 | 备份介质 |

**2.赛题要求**

（a）分别将1、2号两台主机的数据库备份至4号主机；

（b）将1号主机的备份数据，恢复到2号主机的数据库中；

（c）将2号主机的备份数据，恢复到1号主机的数据库中；

（d）完成比赛。

**3.推荐工具**

数据备份工具。

**（四）数据供给隔离**

本题主要考察参赛选手共享不同网段数据库中数据的能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 数据库A | Oracle A库 |
| **2** | 数据库B | Oracle B库 |
| **3** | 服务器 | 数据管理 |

**2.赛题要求**

（a）1号、2号主机在不同的网段，将1号主机的数据库，共享给2号主机；

（b）启动2号主机的数据库；

（c）完成比赛。

**3.推荐工具**

数据复制工具、数据备份工具。

**（五）勒索病毒灾后有效恢复**

本题主要考察参赛选手在生产环境被勒索病毒感染后，恢复生产数据库的能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 数据库服务器 | Oracle 库 |
| **2** | 数据库验证服务器 | Oracle 库 |
| **3** | 备份服务器 | 数据备份管理 |

**2.赛题要求**

（a）定时备份1号主机的数据库至3号主机数据库（备份频率自行设计）；

（b）开始答题后的40分钟内，平台将自动模拟1号主机的数据库感染毒；

（c）参赛选手需编写SQL脚本验证1号主机数据库是否感染病毒；发现1号主机数据库感染病毒后，参赛选手需对3号主机的备份数据进行恢复、排查病毒感染情况；

（d）参赛选手需选择3号主机中最新的一份安全数据，恢复或挂载到2号主机，并启动数据库；

（e）完成比赛。

**3.推荐工具**

数据备份工具。

**（六）数据安全共享**

本题主要考察参赛选手在保证数据安全的要求下，从生产环境安全共享数据到开发测试环境的能力。

**1.服务器资源列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务器名称** | **用途** |
| **1** | 生产服务器 | Oracle 库 |
| **2** | 数据服务器 | 数据管理 |
| **3** | 数据存储服务器 | 数据存储池 |
| **4** | 脱敏服务器 | 脱敏软件 |
| **5** | 脱敏用数据库 | 脱敏库 |
| **6** | 开发测试用库 | 开发测试库 |

**2.赛题要求**

（a）在2号主机部署数据管理软件，利用3号主机作为存储池；

（b）在4号主机部署脱敏软件；

（c）获取1号主机的数据库数据，挂载或共享到5号主机，并启动数据库。按如下要求对5号主机数据库进行数据脱敏：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **库** | **表** | **字段** | **要求** |
| **1** | orcltt | 个人联系信息 | Mobile | 全部匿名化为:  \*\*\*\*\*\*\*\*\*\*\*(11个\*) |
| **2** | orcltt | 个人基本概况信息 | Name | 全部匿名化为:  \*\*\*\*\*\*\*\*\*\* (10个\*) |
| **3** | orcltt | 交易对手信息 | CustomerName | 全部匿名化为:  \*\*\*\*\*\*\*\*\*\* (10个\*) |
| **4** | orcltt | 金额信息 | CTAccount | 全部匿名化为:  \*\*\*\*\*\*\*\*\*(9个\*) |

（d）将脱敏后的数据，挂载或共享到6号主机，并启动数据库；

（e）完成比赛。

**3.推荐工具**

数据备份工具、数据脱敏工具、数据复制工具。

二、评分细则

|  |  |  |  |
| --- | --- | --- | --- |
| **赛题** | **计分项** | **计分项说明** | **总分** |
| **1** | 数据脱敏准确率 | 正确脱敏的字段数/待脱敏的数据字段总数\*300分  注：一个字段内的所有数据准确脱敏视为答对，否则视为打错不计入得分 | 300分 |
| **2** | 敏感字段识别率 | 正确识别的敏感字段数/待识别的敏感字段总段\*300分 | 300分 |
| **3** | 1号主机数据库成功恢复数据到2号主机 | 恢复成功，且与1号主机数据库数据相同得250分，  未恢复或数据恢复不准确得0分 | 250分 |
| 2号主机数据库成功恢复数据到1号主机 | 恢复成功，且与2号主机数据库数据相同得250分，  未恢复或数据恢复不准确得0分 | 250分 |
| **4** | 完成数据供给 | 供给数据库可用，且与1号主机数据库数据相同得500分；  供给数据库不可用，或与1号主机数据库数据不相同得0分 | 500分 |
| **5** | 成功恢复安全数据 | 验证数据库可用，且与生产数据库数据相同，得200分；  验证数据库不可用，或与生产数据库数据不同，得0分 | 200分 |
| 安全数据与中毒操作的时间间隔 | 时间间隔：小于5分钟，得500分；  时间间隔：5~10分钟，得300分；  时间间隔：10~20分钟，得100分；  时间间隔：大于20分钟，得0分 | 500分 |
| **6** | 成功共享数据到  开发测试库 | 开发测试库可用，且数据库完整，得500分；  开发测试库不可用，或数据库不完整，得0分 | 500分 |
| 按要求数据脱敏 | 正确脱敏的字段数/待脱敏的数据字段总数\*200分 | 200分 |

三、注意事项

1、比赛环境不包含相关工具，建议选手自行携带包括备份类、脱敏类、敏感数据发现类、分类分级类等工具。工具不限制品牌、产品、是否开源。

2、解题过程中需使用第三方软件的，可自行在服务器中安装相关程序。

3、每道赛题结果只能提交一次，多次提交本题成绩作废。

4、因服务器资源调配问题，每个队在比赛过程中将有1小时的休息时间。

5、参赛队伍应严格遵守比赛规则，任何违规行为一经发现，主办方有权取消其参赛资格及已获得的成绩。

6、参赛队伍需自行负责其参赛过程中的数据安全与隐私保护，主办方不承担因参赛行为导致的任何数据泄露或隐私侵犯责任。

四、平台操作手册

1、参赛队伍使用主办方分配的账号、密码登录平台。

图形用户界面, 应用程序

描述已自动生成

2、登陆平台后，每位参赛选手将看到本次比赛所有的赛题及每道赛题的答题时间，请选手在规定时间内答题，规定时间外将无法进行赛题作答。



蓝色的屏幕

描述已自动生成

3、点击“参赛”进入答题页面，其中“题目列表”页列出可以答题的赛题，点击赛题进入到赛题信息页面。



4、在答题页面点击“启动”按钮启动场景、点击“提交”按钮可完成赛题作答。

图形用户界面, 文本, 应用程序, Teams

描述已自动生成

5、启动完成后，“场景描述”处会显示操作机的详细信息（包括ip地址、端口、账号和密码）。

图形用户界面, 文本, 应用程序, 电子邮件, Teams

描述已自动生成

6、通过Windows远程桌面的方式登录到操作机，通过操作机测试资源列表中服务器的网络连通性，确定服务器资源都是可用状态后可开始比赛，若有问题请及时联系工作人员。

7、查看桌面文件《ZL01新型数据安全治理参赛手册》，根据手册内容进行赛题作答。

8、点击“提交”完成赛题作答。

