数据库审计测评基准 RC1

OWASP 中国数据安全及隐私保护项目组

目录

一、 数据库审计测评基准介绍

1. 目的

随着互联网技术的发展，数据库的核心地位越来越凸显，作为任何商业和公共安全中最具有战略性的资产，通常都保存着重要的国家、商业以及公民信息，这些信息需要被保护起来。数据库审计旨在帮助各事业单位、企业对核心数据进行全面的安全监控和审计，真正了解自己的数据动态。

目前安全行业中有不少厂家已经推出了相应的数据库审计解决方案，但是由于缺乏全面的评估基准，专业性很难体现，效果无法得到有效的保障，用户往往无从进行选择。

本基准的目的是为了创建一个第三方的、中立的数据库审计检测基准，以供安全组织与专家对数据库审计系统进行全面及公正的评估。

2. 范围

本基准适应于数据库安全审计类系统。

3. 技术背景

数据库的安全一直都在围绕了冗灾备份、渗透测试、安全加固、主机加固、授权控制等方向，这类安全管控方式都是间接对数据进行保护，不直接、不直观；随着大数据库的分析和应用的增加，安全的重点越来越趋向数据本身。如何有效监控数据的应用成为当下关注的重点。

数据库审计系统的诞生可以直接对数据库中的数据进行实时在线的安全监控和审计。数据库审计直观清晰的定位什么人、什么时间、什么工具、什么地方、对数据做了哪些操作。

4. 参与单位

本基准参与单位：深圳昂楷科技有限公司、深圳市网域科技股份有限公司、北京星网锐捷网络技术有限公司、中新网络信息安全股份有限公司、中安威士(北京)科技有限公司

本基准参与人员：王颉、邓丽华、张勤保、邓凯、赵春燕、赵玉燕、刘晨、项小升、蔡佩宸、郭艳杰、夏敏、徐晓微、吕铳、戴林、周礼、赵伟全

（排名不分先后）

5. 参考文献

《GBT 20945-2013 信息安全技术信息系统安全审计产品技术要求和测试评价方法》

《GAT 695-2014 信息安全技术网络通信审计产品技术要求》

GB/T 18336-2001《信息技术安全技术信息技术安全性评估准则》

BMB15-2004《涉及国家秘密的信息系统安全审计产品技术要求》

ISCCC GB/T 20945《信息安全技术信息系统安全审计产品技术要求和测试评价方法》

《ISO/IEC 27001 信息安全管理体系》

《计算机信息系统安全专用产品检测和销售许可证管理办法》

《公安部信息安全等级保护要求》

《工信部信息安全风险评估方法》

二、 技术能力介绍

1. 部署方式

现代数据库所在的网络环境越来越复杂，所以数据库审计系统既要支持传统的旁路部署也要支持非旁路部署，如虚拟化平台部署和云平台部署。

1.1 旁路部署

数据库审计系统旁路接到交换机上，通过交换机的端口镜像功能把需要审计的数据库流量引到审计系统上，该部署方式不会影响正常的业务；支持非 VLAN 环境和 VLAN 环境的审计。

1.2 虚拟化平台部署

数据库审计系统要求能部署在虚拟化平台中的虚拟机中，通过虚拟化平台中的 GRE 引流功能把数据库的流量通过 GRE 封装后发到数据库审计系统中，数据库审计系统能对 GRE 流量进行解封获取到数据库流量，从而对数据库进行审计。

1.3 云平台部署

数据库审计系统要求能部署在云平台中的云主机中，通过在数据库服务器或者客户端上部署轻量级插件把数据库流量引入到审计系统中，从而进行审计。

插件大小不超过 2M，CPU 利用率不超过 1%。数据库审计系统可以同时支持最少 128 个插件同时连接。

2. 基础功能

数据库审计系统应提供对审计和事务日志进行审查的能力，跟踪各种对数据库的实时在线操作行为，审计主要记录对数据库的操作、改变、执行该操作的人以及其他属性。针对数据库活动或状态进行实时在线监控，实时反馈数据库的各种变化，具备较高的准确性和完整性。

2.1 管理平台

数据库审计系统必须提供安全的管理平台，且为不同的管理人员提供功能各异的管理平台，通过该平台，管理人员可以操控其所属管理界面的所有功能，以行使相应的管理权限。平台至少包括三类：

- 系统管理平台
- 规则管理平台
- 审计管理平台

三者之间权限应相互隔离，相互监督，且有操作日志记录，以保障审计产品自身安全，可根据管理内容划分用户权限。

2.2 角色管理

数据库审计系统应具有为用户提供角色分配等管理权限功能，为不同的角色（用户）设定对应的操作权限。

2.3 登录认证

数据库审计系统的登录认证至少包含两种认证方式，以保证其登录身份合法有效。

密码复杂度至少包含字母大小写、数字、特殊符号，登录后可进行窗口锁定。

2.4 自身审计监控

数据库审计系统要求除了具备对外审计和事务日志进行审查的能力，还需具备对自身审计监控的能力，并提供系统运行日志，确保实时在线监控系统运行状况。

2.5 审计日志维护

数据库审计系统应具备给管理员提供用于查询审计安全相关事件的必要信息或方法，捕捉到的审计日志数据能够给管理员提供足够的审计安全信息，以此来判定和维护审计产品自身安全和审计数据安全的完整性事件，以供管理员调查、分析与之相关的事件。

3. 系统管理功能

3.1 系统维护

3.1.1 系统状态

数据库审计系统支持对系统本身运行状态的监控，监控内容有：CUP 使用率、内存使用率，每秒系统接收到的 sql 语句数量、网口接收的数据流量。

3.1.2 网络接口管理

数据库审计系统必须支持与外部网络对接的网络接口，其作为数据的传输，发出指令或者接收指令，完成与外部设备的相互相通。

3.1.3 时间管理

数据库审计系统作为一种网络设备，必须要有时间设置功能，保证与标准时间同步，保证数据的实时性。

3.2 系统升级

数据库审计系统必须能够提供软件升级的功能，可在操作平台上直接通过软件包形式升级产品，或是修复产品 bug。

3.3 数据维护

3.3.1 数据备份

数据库审计系统对系统本身的数据有备份的能力，备份数据包括系统配置信息，系统日志信息，审计日志数据。

备份数据要进行特殊加密，不允许其他非法工具直接进行读取。

3.3.2 数据恢复

数据库审计系统在系统正常或者异常原因导致系统出厂设置之外的数据丢失，可以按照系统本身备份出来的数据进行数据的恢复。

数据恢复可通过平台直接对备份数据进行导入。

3.3.3 数据清理

数据库审计系统在检测到磁盘满时可自动触发数据清理，从而保障最新的审计数据能及时入库。

3.4 数据库自动发现

数据库审计可以通过流量识别自动发现网络中的数据库，也可以通过主动探测发现网络中的数据库，支持主流数据库、国产数据库和 NoSQL 数据库的自动发现。在某些复杂的环境中，无法获取数据库的精准数量和地址时，可通过数据库自动发现功能获取到网络中的数据库地址，用于配置对应的审计策略。

3.5 系统日志

数据库审计系统捕捉到的日志数据能够给管理员提供足够的信息，以此来检查有可能影响到被测数据库审计系统自身安全和数据完整性的事件。

3.6 恢复出厂

数据库审计系统应具有在信息配置错误，软件出现异常，无法判断的情况下，对系统进行恢复出厂设置，达到初始正常状态。

4. 策略管理功能

4.1 审计对象管理

数据库审计系统审计对象管理应支持各种常见主流数据库及相关应用协议审计。

4.1.1 审计数据库类型

数据库审计系统应支持当前国内、外各种主流数据库类型，如：SQLSERVER、MYSQL、ORACLE、SYBASE、DB2、INFORMIX、POSTGRESQL、IP21、CACHé、达梦、人大金仓、南大通用等。

支持审计常见的工控数据库，如 IP21；

支持云平台下 RDS 和 ESC 自建数据库的审计；

支持审计大数据平台下的数据库，如 MongoDB、HBase；

数据库产品应支持数据库各种维护及相关开发工具审计，如：NAVICAT、PL/SQL、WINSQL、SQLMANAGER、STUDIO 等。

支持审计不同的方式访问 HBase，如:Hive、JDBC、JAVA API 等；

支持审计 Telnet 方式访问数据库；

支持常见的应用协议审计：如 ftp、smtp、pop3、nfs、http。

4.1.2 审计数据库数量

数据库审计系统至少支持 128 个数据库同时审计，支持多种不同数据库类型同时审计。

4.2 审计策略管理

4.2.1 预定义策略管理

数据库审计系统应支持预定义策略管理，可以直接调用预定义策略而无需配置。系统内置各类安全规则如 SQL 注入、跨站脚本、口令猜测等攻击规则。

4.2.2 自定义策略管理

数据库审计系统应支持自定策略管理，根据不同规则条件制定不同的自定义策略，如：IP 地址、MAC 地址、子对象、关键字等条件。支持自定义策略的选项不低于 18 种。

4.2.3 组合策略管理

数据库审计系统应支持组合策略管理，能将不同的单个策略组合起来形成组合策略；并能对同一策略的多次告警进行统计。

4.2.4 策略生效时间管理

数据库审计系统应支持策略生效时间管理，通过制定时间对象关联策略，策略在关联时间段内生效。

5. 审计管理功能

5.1 审计效果

5.1.1 审计内容

数据库审计系统能审计出通过各种客户端访问数据库的操作，审计内容包含访问者源 IP、源 MAC、使用客户端进程、数据库账户、访问对象服务器 IP 地址、端口号、操作语句、执行响应、返回行数、返回结果等。

操作语句包括简单语句和复杂语句，如存储过程、函数、绑定变量等。

5.1.2 获取真实客户端 MAC

数据库审计的部署方式一般是旁路部署，通过端口镜像获取需要审计的流量，镜像过来的流量源 MAC 都是交换机的 MAC，所以审计到的审计记录源 MAC 是交换机 MAC，不是客户端的真实 MAC，为了精准定位到人，数据库审计系统需要获取到真实的客户端 Mac 替换交换机 MAC。

5.1.3 语句重述

数据库审计系统审计到的语句过于专业，直接展示审计结果比较难理解，可通过别名的方式，对审计结果进行重述成人使用的自然语句。

5.1.4 数据库攻击检测

数据库审计系统支持对数据库的攻击检测，包括常见的数据库漏洞攻击、SQL 注入攻击和跨站脚本攻击；

5.1.5 超长语句审计

数据库审计系统需要支持审计超长语句不截断，单条语句长度至少支持 3W 字节。

5.1.6 单双向审计

数据库审计系统支持对数据库流量进行单向和双向审计，两种审计方式可配置，由用户自行决定开启哪种方式。

5.1.7 应用审计关联

数据库审计系统支持三层架构的审计，在三层架构下能精准审计到人，能审计到什么人操作了什么语句。

支持 Weblogic、Tomcat 等主流的应用服务器，支持插件形式和非插件形式。

5.1.8 隐秘数据

数据库审计系统审计到返回结果，可对返回结果自动进行敏感数据识别，对敏感数据进行脱敏，防止数据二次泄密。

5.1.9 加密审计

数据库审计系统支持 SQLServer 登录加密的审计，在登录加密的情况下，能解密审计到数据库账号和工具等信息。

5.1.10 绑定变量值提取

数据库审计系统支持含绑定变量 sql 语句值提取。执行 sql 语句时，使用绑定变量，在流量报文中 sql 语句和绑定变量的值分离，审计日志最终应展示出绑定变量有效值。

5.2 智能识别风险

数据库审计系统支持通过 AI 学习后对审计到的大量 SQL 语句进行统计分析得出一个风险识别模型，进而通过该模型对数据行为进行风险级别判定，不需要配置规则也能识别出已知风险和未知风险。

5.3 态势感知

数据库审计系统支持对审计到的数据进行数据分析和挖掘，通过周期性学习，能感知到陌生人对数据库的访问，从而识别出风险。

支持对数据库整体安全状况进行评估和打分，预知未来的安全风险。

5.4 审计报表

5.4.1 预定义报表

数据库审计系统根据数据库审计行业及产品标准，有预定义报表，通过各预定义报表，统计分析当前数据库访问情况及风险分析，有符合相关合规性检查的预定义报表。

5.4.2 自定义报表

数据库审计可根据客户实际需求，根据客户自身对数据库审计日常报表的需求自定义相关报表数据，便于客户相关审计数据工作汇报及风险分析。

5.4.3 报表导出

数据库审计系统可导出报表数据，生成报告，导出方式至少支持 Word、Excel 和 PDF；支持自定义时间的报表导出。

5.5 审计日志检索

5.5.1 精确检索

被测产品能通过审计到的内容做精确检索，可支持数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（含开始结束日期）等

5.5.2 模糊检索

数据库审计能通过审计到的内容做模糊检索，可支持数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（含开始结束日期）等。

5.6 告警方式

数据库审计系统可设置告警策略，通过告警策略指定需要告警的内容和告警接收人。告警方式至少支持邮件、短信、短信平台、syslog 和 snmp。告警内容包括审计内容告警和系统告警。

5.7 旁路阻断

旁路部署方式下，数据库审计系统支持旁路阻断功能，在发现风险后可以阻断风险，对正常业务零风险。

5.8 事件回放管理

数据库审计可通过定向行为分析，可以明确出某指定客户端在某段时间内所有的操作记录，从而进行现场重建，录像回放，真实再现完整操作过程，进行电子取证，为溯源和取证提供有力的证据。

5.9 白名单管理

数据库审计可通过预定义白名单进行监控，对内部安全访问做白名单管理与设置，提前防范，真正做到事前+事中+事后全方位的防护体系。

5.10 审计日志导出

数据库审计可根据查询的对应审计数据进行审计日志的导出 ,导出文件类型包含但不限于 word、xcle、pdf 等常用数据查看类型文件，便于对审计数据进行查看与分析。

5.11 流量统计

支持审计对象的流量统计功能并以图表的形式实时展示。

6. 自身安全性

6.1 管理端安全

数据库审计系统必须通过测试，证明不能获得未经授权的管理功能。

被测数据库审计系统必须能将审计出敏感数据做隐匿处理，防止二次泄露，WEB 管理平台支持 HTTPS 身份认证通信加密方法，管理账号支持登录次数限制、密码复杂度规则。

6.2 黑白名单管理

数据库审计系统必须支持白名单管理，对加入白名单的 IP、系统语句等对象不做审计。

6.3 攻击测试

A.数据库审计系统必须通过测试，证明系统是不易受攻击。

B.数据库审计系统集成了第三方操作系统（如：linux,windows）

C.数据库审计系统必须提供合理和合适的措施保护主机操作系统免受任何攻击。

6.4 支持日志存储耗尽处理机制

在数审工作过程中,应提供内置或自定义策略应对在日志将磁盘耗尽环境下,如日志转储、覆盖等策略，确保设备正常运行。

7. 性能测试

7.1 SQL 处理性能

对 SQL 语句的语义分析，尽可能的将操作数据库的 SQL 语句进行细粒度解析，比如账号名、数据库名等，no sql 的审计面向对象的 M 语言安全审计能力，如 Caché 数据库审计，包括客户端工具 Studio 、Terminal、 Portal、MedTrak、Sqlmanager 等。

7.1.1 误报率

数据库审计过程中应为零误报率，通过全面深度的监控与审计对所有数据库访问操作进行准确的审计，达到电子取证的准确与有效性。

7.1.2 漏报率

数据库审计过程中应为零漏报率，全面审计所有数据库访问操作，对任何时候任何客户端对数据库做任何操作均能正常审计，保证数据的完整性。

7.2 流量测试

数据库流量的处理能力进行弹性测试，测试数据库审计的最大峰值处理能力能够满足客户实际的数据流量环境。

7.3 会话并发数

数据库连接长会话、短会话都存在，测试数据库审计的多会话并发处理能够满足客户实际的网络环境下会话要求。

7.4 日志检索性能

审计日志的快速检索，容易操作，如数据量在 1 亿左右的级别时，查询响应时间在 10 分钟以下的数量级。