(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108629201 A
(43)申请公布日 2018.10.09

(21)申请号 201810370396.7

(22)申请日 2018.04.24

(71)申请人 山东华软金盾软件股份有限公司
地址 250101 山东省济南市高新区舜华路1号齐鲁软件园5号楼(创业广场E座)A408、A410、A412房间

(72)发明人 杨健

(74)专利代理机构 济南泉城专利商标事务所 37218
代理人 支文彬

(51)Int.Cl.
G06F 21/62(2013.01)
H04L 29/06(2006.01)

权利要求书1页 说明书3页

(54)发明名称

一种对数据库非法操作进行阻断的方法

(57)摘要

一种对数据库非法操作进行阻断的方法，基于IP地址、MAC地址、用户、应用程序等对访问者进行身份认证，形成多重认证，可以弥补单一口令验证方式安全性的不足。用户身份验证通过后，也可以实时检测用户对数据库进行的非法操作，并阻断其非法操作行为，同时详细的记录非法操作发生的时间、来源IP、来源MAC、用户名、访问SQL等信息。通过桥接方式部署在数据库服务器和应用服务器之间，可以屏蔽直接对数据库访问的通道，防止数据库隐通道对数据库的攻击。

CN 108629201 A

1.一种对数据库非法操作进行阻断的方法,其特征在于,包括如下步骤:

a)设定可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略;

b)通过桥接部署方式捕获客户端与Oracle数据库服务器的数据流,获取到TNS协议数据包;

c)根据已知的TNS协议结构解析获取到的数据包,从TNS协议数据包的Connect类型数据包中获取访问数据库的IP地址和MAC地址,从TNS协议数据包连接部分的后续数据交互部分获取数据库的用户、应用程序。

2.客户端主机名称信息;

d)判断获取的访问数据库中的IP地址和MAC地址是否存在再步骤a)中设定的IP和MAC的黑名单策略中,如果存在则直接给访问数据库的客户端返回TNS协议的Refuse类型数据包,如果不存在,则执行步骤e);

e)从TNS协议数据包的DATA类型的数据包中查找0x035e和0x1169标识的数据包,过滤出执行的SQL语句,提取出具体的操作类型和操作的结构名称信息;

f)通过步骤a)设定的可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略对步骤e)中获取的操作类型及结构名称信息进行匹配,如果检测到对某结构进行了非法访问和异常操作时,直接将此数据包丢弃,并记录操作发生的时间、来源IP、MAC、用户名、操作代码信息。

3.根据权利要求1所述的对数据库非法操作进行阻断的方法,其特征在于:步骤e)中提取的具体的操作类型为select操作、delete操作、alter操作及insert操作。

4.根据权利要求1所述的对数据库非法操作进行阻断的方法,其特征在于:步骤e)中提取的操作的结构名称信息为table信息、view信息及procedure信息。

一种对数据库非法操作进行阻断的方法

技术领域

[0001] 本发明涉及计算机安全领域，具体涉及一种对数据库非法操作进行阻断的方法。

背景技术

[0002] 随着计算机技术和网络技术的发展，数据库的应用十分广泛，深入到各个领域，成为各单位处理数据的重要工具。在众多的数据库系统中，Oracle数据库以其强大的功能，有效的安全性和完整性控制、分布式数据处理模式等特点而被众多企业和部门所采用。作为一种大型数据库系统，Oracle数据库主要用在处理大批量数据和网络运用中。由于Oracle数据库系统被广泛应用，因而数据库的安全性问题也变得尤为重要。数据库的数据安全以及防止其被非法用户入侵，成为数据库运用中最常见的安全性问题。虽然数据库系统都有各自的安全机制来保护数据，大部分也都是通过验证用户名密码和设定权限，限制对数据库数据的随意存取。但是，只要有不法人员存在，任何安全系统都不是绝对安全的，总会受到有意的攻击和破坏。以Oracle数据库为例，Oracle提供的审计功能缺乏有效的分析工具使用。面对海量数据时，DBA虽然能自己去分析审计数据，但这样并不容易发现攻击、非法访问和操作等方面的安全问题。

发明内容

[0003] 本发明为了克服以上技术的不足，提供了一种对不符合认证规则或进行非法操作的访问者直接阻止访问行为的对数据库非法操作进行阻断的方法。

[0004] 本发明克服其技术问题所采用的技术方案是：

一种对数据库非法操作进行阻断的方法，包括如下步骤：

a)设定可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略；

b)通过桥接部署方式捕获客户端与Oracle数据库服务器的数据流，获取到TNS协议数据包；

c)根据已知的TNS协议结构解析获取到的数据包，从TNS协议数据包的Connect类型数据包中获取访问数据库的IP地址和MAC地址，从TNS协议数据包连接部分的后续数据交互部分获取数据库的用户、应用程序。客户端主机名称信息；

d)判断获取的访问数据库中的IP地址和MAC地址是否存在再步骤a)中设定的IP和MAC的黑名单策略中，如果存在则直接给访问数据库的客户端返回TNS协议的Refuse类型数据包，如果不存在，则执行步骤e)；

e)从TNS协议数据包的DATA类型的数据包中查找0x035e和0x1169标识的数据包，过滤出执行的SQL语句，提取出具体的操作类型和操作的结构名称信息；

f)通过步骤a)设定的可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略对步骤e)中获取的操作类型及结构名称信息进行匹配，如果检测到对某结构进行了非法访问和异常操作时，直接将此

数据包丢弃，并记录操作发生的时间、来源IP、MAC、用户名、操作代码信息。

[0005] 进一步的，步骤e)中提取的具体的操作类型为select操作、delete操作、alter操作及insert操作。

[0006] 进一步的，步骤e)中提取的操作的结构名称信息为table信息、view信息及procedure信息。

[0007] 本发明的有益效果是：基于IP地址、MAC地址、用户、应用程序等对访问者进行身份认证，形成多重认证，可以弥补单一口令验证方式安全性的不足。用户身份验证通过后，也可以实时检测用户对数据库进行的非法操作，并阻断其非法操作行为，同时详细的记录非法操作发生的时间、来源IP、来源MAC、用户名、访问SQL等信息。通过桥接方式部署在数据库服务器和应用服务器之间，可以屏蔽直接对数据库访问的通道，防止数据库隐通道对数据库的攻击。

具体实施方式

[0008] 下面对本发明做进一步说明。

[0009] 一种对数据库非法操作进行阻断的方法，包括如下步骤：

a)设定可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略；

b)通过桥接部署方式捕获客户端与Oracle数据库服务器的数据流，获取到TNS协议数据包；

c)根据已知的TNS协议结构解析获取到的数据包，从TNS协议数据包的Connect类型数据包中获取访问数据库的IP地址和MAC地址，从TNS协议数据包连接部分的后续数据交互部分获取数据库的用户、应用程序。客户端主机名称信息；

d)判断获取的访问数据库中的IP地址和MAC地址是否存在再步骤a)中设定的IP和MAC的黑名单策略中，如果存在则直接给访问数据库的客户端返回TNS协议的Refuse类型数据包，如果不存在，则执行步骤e)；

e)从TNS协议数据包的DATA类型的数据包中查找0x035e和0x1169标识的数据包，过滤出执行的SQL语句，提取出具体的操作类型和操作的结构名称信息；

f)通过步骤a)设定的可访问数据库的客户端的IP及MAC的白名单和黑名单、可访问数据库的用户和用户权限以及可访问数据库的应用程序的策略对步骤e)中获取的操作类型及结构名称信息进行匹配，如果检测到对某结构进行了非法访问和异常操作时，直接将此数据包丢弃，并记录操作发生的时间、来源IP、MAC、用户名、操作代码信息。

[0010] 基于IP地址、MAC地址、用户、应用程序等对访问者进行身份认证，形成多重认证，可以弥补单一口令验证方式安全性的不足。用户身份验证通过后，也可以实时检测用户对数据库进行的非法操作，并阻断其非法操作行为，同时详细的记录非法操作发生的时间、来源IP、来源MAC、用户名、访问SQL等信息。通过桥接方式部署在数据库服务器和应用服务器之间，可以屏蔽直接对数据库访问的通道，防止数据库隐通道对数据库的攻击。

[0011] 优选的，步骤e)中提取的具体的操作类型为select操作、delete操作、alter操作及insert操作。

[0012] 优选的，步骤e)中提取的操作的结构名称信息为table信息、view信息及

procedure信息。