Análise de Vulnerabilidade em um Banco de Dados Oracle e Teste de Eficiência na Correção a Partir de um *Patch*

Bruno da Cunha Felipe[1], José Dias Neto[1], Juliane Regina de Oliveira[1], Gustavo César Bruschi[1]

[1]Curso de Tecnologia em Banco de Dados – Faculdade de Tecnologia de Bauru (FATEC)

Rua Manoel, Bento Cruz, n° 30, Quadra 3 – Centro – 17.015-171- Bauru, SP – Brasil

{bruno.dc.felipe, diasneto27} @gmail.com, juoliveira95@hotmail.com, gustavo.bruschi@fatec.sp.gov.br

Abstract*. Nowadays, databases can be vulnerable to threats for several reasons. The vulnerabilities damage the data stored in databases, which decrease the data owner security. One of the vulnerabilities correction forms of the Oracle Database is the installation of patches, which are updates provided by manufacturers in order to correct these failures. It was concluded that the updates are really important to Oracle database maintenance in order to fix the vulnerabilities.*

Resumo. *Os bancos de dados atualmente podem sofrer e conter diversas vulnerabilidades e ameaças, causadas por diversos motivos. As vulnerabilidades prejudicam os dados armazenados nos banco de dados comprometendo, desta forma, a segurança das detentoras dos dados. Uma das formas de correção das vulnerabilidades dos Bancos de dados Oracle é a instalação dos patches que são atualizações fornecidas pelos fabricantes para correção destas falhas. Conclui-se que as atualizações são de grande importância para a manutenção dos Bancos de dados Oracle, a fim de corrigir as vulnerabilidades existentes.*

1. Introdução

As informações necessárias às empresas almejarem a vantagem competitiva são produzidas exponencialmente, juntamente à necessidade de gerenciamento e armazenamento das mesmas. Para tanto, é imprescindível a implantação de um conjunto de *softwares* capazes de gerenciar e possibilitar a confidencialidade, integridade e disponibilidade dos dados, os Sistemas Gerenciadores de Banco de Dados (SGBD). Buscando manter os dados íntegros, seguros e disponíveis, o Administrador de Banco de Dados, profissional também conhecido como *Database Administrator* (DBA), usufrui de todos os mecanismos existentes nos *softwares* de gerenciamento, fornecidos pelas ferramentas ou *features* que é o nome dado às ferramentas extras ou não do Banco de Dados que favorece ao administrador facilidades.

O Banco de Dados Oracle é um dos produtos da *Oracle Corporation* empresa fundada no ano de 1977. De acordo com Price (2009), o Banco de Dados Relacional foi conceituado em 1970 pelo Dr. E. F. Cood, que esboçou a sua teoria em um artigo chamado "*A Relational Model of Data for Larger Shared Data Banks*", que traduzido para a língua portuguesa "Um Modelo de Dados Relacional para Grandes Bancos de

Dados Compartilhados", publicado na revista *Comunications of the ACM* no ano de 1970.

A segurança dos dados pode ser interferida por ataques intermediados por ameaças e vulnerabilidades, segundo Ralph, Araújo e Reis (2007), alguns exemplos de ataques são SQL *injection*, *Buffer Overflow*, Negação de Serviços e Elevação de privilégios, para Santos et al (2014) a ameaça é uma ocorrência potencial que possibilita um efeito indesejado, em contrapartida, vulnerabilidade é uma característica que permite o surgimento de uma ameaça.

As vulnerabilidades e ameaças impelem a segurança do SGBD e a estagnação da segurança dos dados armazenados é corrompida, para solucioná-las, é expressa a necessidade da instalação do *patch*, que pode ser descrito como um pacote de atualização disponível a algum produto, cuja função é alterar pontos imprecisos à segurança da informação.

Os produtos da Oracle disponibilizados aos profissionais de tecnologia da informação, não estão ilesos das vulnerabilidades, para alguns desses empecilhos, o desfecho é o oferecimento trimestral do *patch* pela empresa, Oracle (2014) assegura que diversos profissionais colaboram fornecendo informações, observações ou sugestões a respeito das vulnerabilidades do *software* que impedem a preservação da segurança que podem resultar em alterações significativas aos produtos da Oracle ou documentações em versões futuras.

Este trabalho relata duas das principais atividades de um DBA: a manutenção do Banco de dados atualizado e a garantia da segurança da base de dados. O objetivo é explorar uma vulnerabilidade existente na versão 11.2.0.1.0 do Banco de Dados Oracle, que consiste em uma falha na duplicação do banco de dados para uma instância auxiliar, instalar o pacote atualizador (*Patch Set Update* para a versão 11.2.0.4.0) e verificar se a instalação do *patch* corrigiu a vulnerabilidade elencada.

2. Conceitos e Definições

2.1. Banco de Dados Relacionais

O conceito de banco de dados, proposto por Hernandez (2013), é uma coleção organizada de dados com a função de primar pela modelagem de algumas organizações ou processos organizacionais. Estas informações devem estar centralizadas e de maneira que possam ser facilmente acessadas, gerenciadas e atualizadas. Ainda segundo o autor, não é enfático o meio utilizado (papel ou um computador) para coleta e armazenagem dos dados, pois o agrupamento de dados para uma finalidade específica é a acepção de um banco de dados, podendo suportar variados conteúdos, como textos, numéricos e até mesmo imagens.

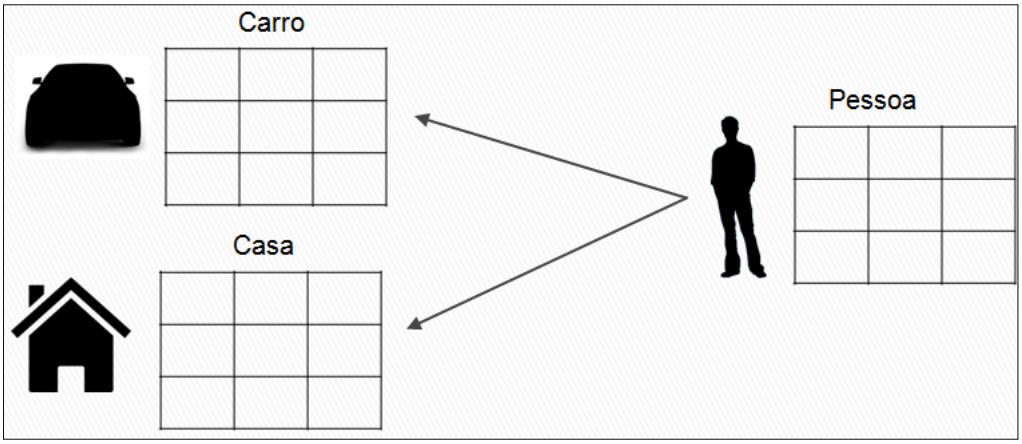

Figura 1. Representação do Modelo Relacional
Fonte: Autores

Na informática os dados são classificados de acordo com sua organização. A maneira habitualmente utilizada é o banco de dados relacional, que de acordo com a Figura 1 é notado que a tabela Pessoa se relaciona com as tabelas Carro e Casa, sendo uma característica enaltecedora nos bancos de dados relacionais o relacionamento entre as tabelas por meio das chaves primárias e estrangeiras, sendo que também existe o banco de dados não relacional, que engloba um conceito mais recente em comparação ao primeiro banco de dados.

O Banco de dados relacional surgiu na década de 70, primeiramente formulado e proposto em 1969 por Edgar F. Codd. Para Codd (1972), a proposta de um modelo relacional de dados é que qualquer base de dados formatada é vista como uma coleção de relações variáveis no tempo de granularidade variada.

Nos dois artigos de 1985, Edgar F. Codd, um dos pioneiros do banco de dados relacional, publicou regras ou princípios para que um sistema gerenciador de banco de dados possa ser considerado “completamente relacional”. Segundo Codd (1972), estes princípios são treze, numerados de zero a doze, os princípios fornecem um conjunto de padrões para julgar se um SGBD é totalmente relacional. As regras, no qual é um assunto de muito debate, são descritas abaixo:

A Regra Fundamental e a Regra da informação, significam, respectivamente, um SGBD relacional deve gerir os seus dados usando apenas suas capacidades relacionais e toda informação deve ser representada de uma única forma, como dados em uma tabela.

Segundo Sumathi e Esakkirajan (2010), o modelo relacional também é a combinação de três componentes: estrutura, integridade e dinamicidade. Para os autores a estrutura define o banco de dados como uma coleção de relações que é iniciada no significado de integridade, para tanto, é permanecido no modelo relacional usando chaves primárias e estrangeiras. A dinamicidade, utiliza-se da álgebra e cálculos relacionais que são ferramentas para manipular os dados em um banco de dados.

Em um banco de dados relacional, basicamente todos os registros são representados em tuplas agrupadas dentro de relacionamento, ou seja, organizados em tabelas, linhas e colunas, sendo as tabelas a representação estrutural de uma entidade, cada coluna da tabela representa um atributo desta entidade, e as linhas as instâncias, a partir desta estrutura, temos como base que estes dados armazenados podem ser acessados e organizados de diferentes formas.

2.2. Segurança da Informação

A informação é hoje um ativo de fundamental importância em qualquer organização do mundo. Por ser valiosa, é também ameaçada e, por tanto, deve ser protegida.

Para Peltier (2013), a segurança da informação pode ser entendida como um conjunto de ações que assegura a conservação da confidencialidade, integridade e disponibilidade de informação. De acordo com o autor, a Confidencialidade significa não fornecer acesso a informações para as pessoas ou sistemas que não deveriam ter este acesso. Segundo o autor a Integridade é manter os atributos originais da informação sem que estes sejam corrompidos. A disponibilidade garante que a informação sempre estará disponível quando necessário.

A segurança da informação, para Peltier (2013), é um meio para um fim e não o fim em si mesmo. Para o mesmo autor nas organizações, por exemplo, um programa de segurança de informação eficaz, se torna secundário em relação à necessidade de obter lucro que é algo primário em uma empresa, sendo o principal objetivo. O autor assevera que no setor público, não é diferente, a segurança da informação também é algo secundário em relação aos serviços da agência fornecidos a sua constância, estas são metas e objetivos que os profissionais de segurança não podem deixar de prezar.

Segundo Machado [2012 *apud* Fontes 2008], uma informação pode estar sujeita a riscos, mas antes de definir risco, é necessário o entendimento de ameaça cujo significado é qualquer evento capaz de prejudicar o andamento normal das atividades, por outro lado, risco é a possibilidade dessa ameaça se concretizar.

Para que ocorra a implementação da segurança da informação em um ambiente organizacional, primeiramente é indicado as ameaças e posteriormente os riscos, segundamente, devem ser aplicadas as técnicas preventivas a fim de remover as vulnerabilidades identificadas. Este é um círculo vicioso, conforme mais informações são alimentadas e tecnologias surgem, conseqüentemente, a necessidade de manter as informações cada vez mais protegidas em relação a toda esta evolução externa e interna cresce.

Segundo a Associação Brasileira de Normas Técnicas (ABNT, 2006), a segurança da informação, além da preservação da confidencialidade, integridade e disponibilidade da informação possuem outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade. A autenticidade é uma identificação para o acesso a um serviço. A responsabilidade é a garantia dada a uma pessoa que permitirá a existência da segurança. O não repúdio pode ser definido como o sinônimo de garantia da autoria de uma determinada ação, melhor exemplificando, o usuário que realizou uma determinada ação, não pode negar está atividade realizada, pois é notada a existência de meios para verificação do autor de uma determinada atividade. A confiabilidade pode ser definida como a qualidade da informação, a verificação se ela está correta.

2.3. Ameaças à Segurança em um Banco de Dados

Segundo Beaver (2014), o SGBD sofre a possibilidade de ataques gravíssimos, pois o mesmo é instalado e configurado para preservar as informações empresariais. A segurança do Banco de dados não é preservada devido às ameaças e vulnerabilidades existentes no *software* gerenciador.

A vulnerabilidade é definida por Dantas (2011) como uma fragilidade que pode vir a causar um dano, para tanto, é necessário um agente causador, todavia, ela é encontrada em processos, políticas, equipamentos e recursos humanos. O autor ainda afirma que a origem das vulnerabilidades são instalações físicas inadequadas, desastres naturais, materiais de construção inadequados, ausência de política de segurança,

funcionário sem treinamento, ausência de controle de acesso, equipamentos obsoletos, *software* sem *patch* e sem licença de funcionamento.

A exploração da vulnerabilidade pode ser feita na rede mundial de computadores (internet) ou rede interna, por invasores externos ou usuários mal-intencionados. Freitas (2009), afirma que os tipos de ameaças e vulnerabilidades se diversificam de acordo com o ambiente interno e externo à organização, exemplificando, organização dos processos, cultura de segurança dos usuários, política de segurança de informação e a infraestrutura dos dados e rede. Segundo o autor não há ambiente completamente seguro, mesmo com a adoção de tecnologias de segurança, o mesmo continuará com as interferências humanas.

As vulnerabilidades no Banco de Dados permitem o surgimento de ameaças e facilita alguns ataques ao servidor de Banco de Dados: SQL *injection*, *Buffer Overflow*, Negação de Serviços e Elevação de privilégios.

O SQL *injection* é definido por Elmasri e Navathe (2011), como uma das ameaças mais comuns ao sistema de Banco de Dados, as aplicações *web* que acessam uma base de dados possibilitam o envio de comandos da *Structured Query Language* (SQL) linguagem de consulta estruturada e dados ao banco de dados. Ainda, segundo o autor, o ataque de injeção de SQL é definido como a inserção de incalculáveis caracteres por meio de uma aplicação que altera os comandos SQL existentes neste local, tornando visíveis os dados da base de dados.

O *Denial of Service* (DoS), ataque de negação de serviço é segundo Elmasri e Navathe (2011), a indisposição de recursos aos usuários intencionados da empresa, ou chamado de (*Distributed Denial of Service*) DDOS ataque distribuído de negação de serviço, o acesso às aplicações ou aos dados da rede é negado aos usuários legítimos devido ao *Buffer Overflow* (estouro no *buffer*) e a ultrapassagem dos recursos disponíveis.

O Banco de Dados empresarial é acessado por calculáveis usuários do empreendimento, pela serventia de armazenar os dados e correlatos da empresa, necessários à fruição do trabalho realizado no negócio e escalando a organização às competições empresarias. Entretanto a existência de um programa de controle dos usuários é imprescindível, para que haja uma correta determinação dos privilégios fornecidos pelo DBA que conhecerá as funções dos colaboradores e delimitará o Banco de Dados para as necessidades dos colaboradores na empresa, não fomentando o acesso total aos dados, prejudicial à organização. Isto poderá fornecer informações importantes a intrusos que, segundo Elmasri e Navathe (2011), utilizarão da escalada de privilégios para elevar o seu privilégio e se beneficiando das vulnerabilidades nos sistemas de Banco de dados.

Conforme McClure, Scambray e Kurtz (2012), o mundo *online* se conecta ao nosso estilo de vida, o ataque ao banco de dados torna-se uma ameaça exponencial ao comércio mundial. Esse tipo de ameaça baseia-se em muitas das mesmas técnicas de penetração usadas para superar mecanismos de confidencialidade, integridade e disponibilidade. Uma maneira de prevenção das ameaças é instalação dos *patches* de atualizações e adotar as configurações de melhores práticas.

2.4. Atualizações em um Banco de Dados Oracle

As vulnerabilidades e ameaças aos *softwares* de Gerenciamento e armazenamento dos Bancos de Dados prejudicam a segurança dos dados armazenados, afetando negativamente os negócios. Ralph, Araújo e Reis (2007) asseveram que os *patches* são capazes de solucionar as vulnerabilidades existentes nos Banco de Dados e podem acrescentar novas funcionalidades ao *software*.

A prontidão dos *patches* para a implantação no *software* de Banco de Dados Oracle é proposta no *web site* do *My Oracle Support*, endereço oferecedor de suporte da empresa Oracle *Corporation*. Matishak e Fuler (2011) asseguram que este é um dos recursos de suporte da Oracle, as outras maneiras de amparo são por Telefone e Ferramenta de Diagnóstico Remoto *Oracle Direct Connect* (ODC). Estes apoiadores proporcionam aos usuários administradores dos *softwares* a manutenção do correto funcionamento do Banco de Dados.

As alterações que são realizadas no Banco de Dados Oracle é o fator classificador dos *patches*. Segundo Maurice (2014) os *Critical Patch Update* (CPU) são as atualizações críticas de segurança, um conjunto de CPU forma um *Patch Set Update* (PSU) que é aplicado para modificar a versão do banco de dados, assim é simplificado o processo, pois não é possível instalar todos os CPU lançados em uma *release*. Segundo a empresa o PSU é um pacote aplicado em uma release, em contrapartida, Oracle *PatchSet* são os pacotes de atualização normalmente no formato .zip que possibilita a instalação de produtos Oracle em diferentes plataformas e arquiteturas computacionais.

A Matriz de Risco é uma forma tabular de descrever as vulnerabilidades que serão corrompidas pelo pacote atualizador, os privilégios para a exploração da vulnerabilidade e os componentes afetados e apresenta *Common Vulnerabilities and Exposures* (CVE) e *Common Vulnerability Score System* (CVSS). O CVE são os identificadores das vulnerabilidades, que estão pormenorizados no site da Oracle com as mesmas desarraigadas. O CVSS são os classificadores da Oracle das vulnerabilidades, segundo Oracle (2014) é um método padronizado para avaliá-las.

Anteriormente ao processo de atualização, a cópia dos dados pertencentes ao banco de dados, denominada *backup*. Gregolewitsch (2011) ressalta que este arquivo favorece a restauração dos mesmos em caso de falhas. O *snapshot* é uma imagem da situação do banco de dados no momento em que a foto foi feita, estes são procedimentos favoráveis à conservação dos dados e do *software* gerenciador no modo anterior à implantação do *patch*, apesar da ocorrência de falhas e interrupções durante a atualização do Banco de Dados.

O Manual fornecido pela Oracle é o fomentador do conhecimento a respeito do procedimento adequado na atualização, adquirido pelo profissional responsável pela atividade. O procedimento elegido para a atualização deve ser conformado pela Oracle, assume-se, acautela dos clientes, a fim de garantir o suporte da mesma perante a uma eventual indisponibilidade ou falha do serviço de Banco de Dados. Oracle (2014) enaltece a recomendação da instalação do *patch* sem detença. De acordo com Oracle (2015) apesar das correções fornecidas pela Oracle é enviado à empresa, periodicamente, relatórios das vulnerabilidades que continuam a ser exploradas, pelo motivo dos clientes não atualizarem suas bases de dados.

A Oracle homologa diversos métodos para a atualização do software de gerenciamento e armazenamento dos dados: *Database Upgrade Assistant* (DBUA), *Manual Upgrade* e *Data Pump*.

O DBUA, um assistente gráfico utilizado para a atualização, comumente usado em múltiplos *softwares* de gerenciamento e armazenamento do Banco de Dados, o domínio na atividade é mínimo, diferentemente, de executar comandos. O *Manual Upgrade* é método de atualização baseado em um conjunto de comandos necessários para a efetivação da atualização. O *Data Pump* é usado para gerar e importar os arquivos no formato .dmp que possuem todos os comandos necessários para a criação dos objetos e inserção dos dados, assim é preparado, instalado e configurado um novo ambiente e software de banco de dados.

3. Materias e Métodos

Para elaboração do cenário para a demonstração do experimento, foi necessário um computador hospedeiro, ou seja, aquele que contém as máquinas virtuais utilizadas para a realização dos testes, constituído pelo Sistema Operacional *Windows 8.1* 64 *bits*, processador Intel *core* i3, memória total 4 *gigabytes* (GB) e armazenagem aproximada de 500 GB.

As Máquinas Virtuais foram criadas no *software Oracle VM VirtualBox*® versão 4.3.30 r101610, que pertence ao tipo de virtualização *hosted*, com a característica principal, de dependência do sistema operacional da máquina hospedeira. As Máquinas Virtuais são formadas pelo Sistema Operacional *Windows Server 2008 Release 2 Standard 64 bits*, com 1024 MB de memória base.

Foram utilizados o *Oracle Database Enterprise Edition Release* 11.2.0.1.0 64 *bits* – versão que continha a vulnerabilidade a ser explorada e a versão 11.2.0.4.0 64 *bits* – versão com a vulnerabilidade corrigida, com as instâncias BD1 e BD2, sendo a primeira instância designada ao banco de dados produção e a instância BD2 selecionada para conter o banco de dados de produção duplicado.

O Banco de Dados 11.2.0.1.0 foi atualizado para a versão 11.2.0.4.0, mediante a instalação do *Patch Set Update* 11.2.0.4.0, os arquivos utilizados são p13390677_112040_MSWIN-x86-64_1of7.zip e p13390677_112040_MSWIN-x86-64_2of7.zip. As versões foram escolhidas com base em pesquisas realizadas nos materias publicados no *site* da Oracle e documentações disponibilizadas pela empresa, que determinou a vulnerabilidade a ser testada, as versões do Banco de dados Oracle e o *patch* instalado.

Alguns utilitários da Oracle foram necessários para a realização dos testes que são de fundamental importância, pois garantem a conclusão e efetivação das atividades de valia para a exploração da vulnerabilidade. Estas ferramentas estão dispostas no Quadro 1 com a descrição.

Utilitário	Descrição
SQL*Plus	É uma ferramenta que fornece uma *interface* por linhas de comandos permitindo o acesso e manipulação do Banco de dados Oracle
DBCA (*Database Configuration Assistant*)	Segundo Oracle (2015), o utilitário é uma maneira de criar banco de dados de forma automatizada.
RMAN(*Recovery Manager*)	Para Oracle (2015), o RMAN é uma ferramenta que conclui tarefas de *backup* e recuperação do banco de dados e facilita a administração das estratégias de *backup*.
DBUA	Oracle (2004) assevera que o DBUA é uma ferramenta auxiliadora durante o processo de atualização e configura o banco de dados para a nova versão. Segundo a empresa o DBUA automatiza o processo de atualização e realiza recomendações para as opções de configuração.
NETCA(*Network Configuration Assistant*)	É um utilitário usado para a configuração de rede.

Quadro 1. Descrição dos utilitários
Fonte: Autores

As *views*, consultas pré-armazenadas, são utilizadas durante a realização dos testes para descrever alguns detalhes sobre os arquivos existentes no banco de dados. Estes objetos utilizados estão explanados no Quadro 2.

VIEWS	COLUNAS UTILIZADAS NA CONSULTA	DESCRIÇÃO
V$DBFILE	*FILE#, NAME*	Segundo Oracle (2015), está *view* lista todos os *datafiles*, arquivos de dados, que integra o banco de dados e são preservados para compatibilidade histórica. Esta *view* exibe os nome do arquivo e também o número que ele pertence no banco de dados.
V$DATAFILE	*NAME, STATUS*	Segundo Oracle (2015), está visão exibe informações dos *datafiles* do banco de dados a partir do *controlfile*. Segundo Oracle (2015), os arquivos de controle são criados durante a criação e configuração do banco de dados, contudo é imprescindível a criação de no mínimo uma cópia do arquivo de controle, pois é garantido ao servidor de banco de dados a escrita de informações nestes arquivos que são importantes para a montagem do banco de dados. Com esta *view* será visualizado o nome dos arquivos do banco de dados e o *status* destes arquivos.
X$KCVFH	HXFIL, FHDBI	A *view* exibe o arquivo de dados e o seu respectivo DBID, identificação do banco de dados.

Quadro 2. Descrição das *views*
Fonte: Autores

O utilitário RMAN, segundo Oracle (2015), possui a *feature* de duplicação do banco de dados realizada com o comando *duplicate*, diferente de um banco de dados *standby* que detêm a missão estar ativo, quando o banco de dados de produção tiver um evento de falha, o banco de dados duplicado, é responsável pela realização de diversos testes. A empresa assevera que a instância pode estar no mesmo *host* do banco de dados

de produção ou em outro *host*, para que, desta forma, garanta a segurança dos dados armazenados. A finalidade do comando *duplicate*, segundo a empresa, é duplicar o banco de dados de produção com um DBID diferente, não ocorrendo este fato ao realizar a duplicação por meio do sistema operacional.

A atividade de exploração da vulnerabilidade do banco de dados nas duas versões consiste em criar uma *tablespace*, que é o armazenamento lógico dos arquivos, com dois *datafiles*, posteriormente alterar um deles para o modo *offline* e por fim realizar o *backup* das alterações do banco de dados. Uma instância auxiliar será necessária para receber o banco de dados duplicado, contudo serão editados alguns arquivos para a elaboração da exploração da vulnerabilidade. A exploração da vulnerabilidade no Banco de dados 11.2.0.1.0 foi efetivada em uma máquina virtual e a atualização do Banco de dados para a versão 11.2.0.4.0 foi realizada em outra máquina virtual com as mesmas configurações.

3.1. Configurações para a exploração da vulnerabilidade do Banco de dados Oracle 11.2.0.1.0

O ambiente de pesquisa designado ao desenvolvimento do teste para resultar em uma iniciativa de duplicação do banco de dados relatado como uma vulnerabilidade do Banco de dados Oracle foi utilizado o utilitário RMAN.

O ambiente foi constituído inicialmente por uma instância denominada BD1 que contém uma *tablespace* denominada teste com dois *datafiles* (teste01.dbf e teste02.dbf), sendo um deles alterado para o modo *offline*. Como pode ser observado na Figura 2, que contém uma consulta à *view* V$DBFILE com os arquivos de dados existentes elencados.

```
SQL> SELECT * FROM V$DBFILE;

     FILE# NAME
---------- ------------------------------------------------------
         4 C:\APP\ADMINISTRATOR\ORADATA\BD1\USERS01.DBF
         3 C:\APP\ADMINISTRATOR\ORADATA\BD1\UNDOTBS01.DBF
         2 C:\APP\ADMINISTRATOR\ORADATA\BD1\SYSAUX01.DBF
         1 C:\APP\ADMINISTRATOR\ORADATA\BD1\SYSTEM01.DBF
         5 C:\APP\ADMINISTRATOR\ORADATA\BD1\EXAMPLE01.DBF
         6 C:\APP\ADMINISTRATOR\ORADATA\BD1\TESTE01.DBF
         7 C:\APP\ADMINISTRATOR\ORADATA\BD1\TESTE02.DBF
```

Figura 2. Consulta à view V$DBFILE
Fonte: Autores

Utilizando o utilitário RMAN foi realizado o *backup* das alterações do banco de dados ao finalizar, o *datafile* foi alterado para o modo *online*.

A instância auxiliar BD2 que receberá o banco de dados da instância BD1, criada utilizando o utilitário DBCA. A Figura 3 representa um resumo da criação da segunda instância apresentando todas as suas informações.

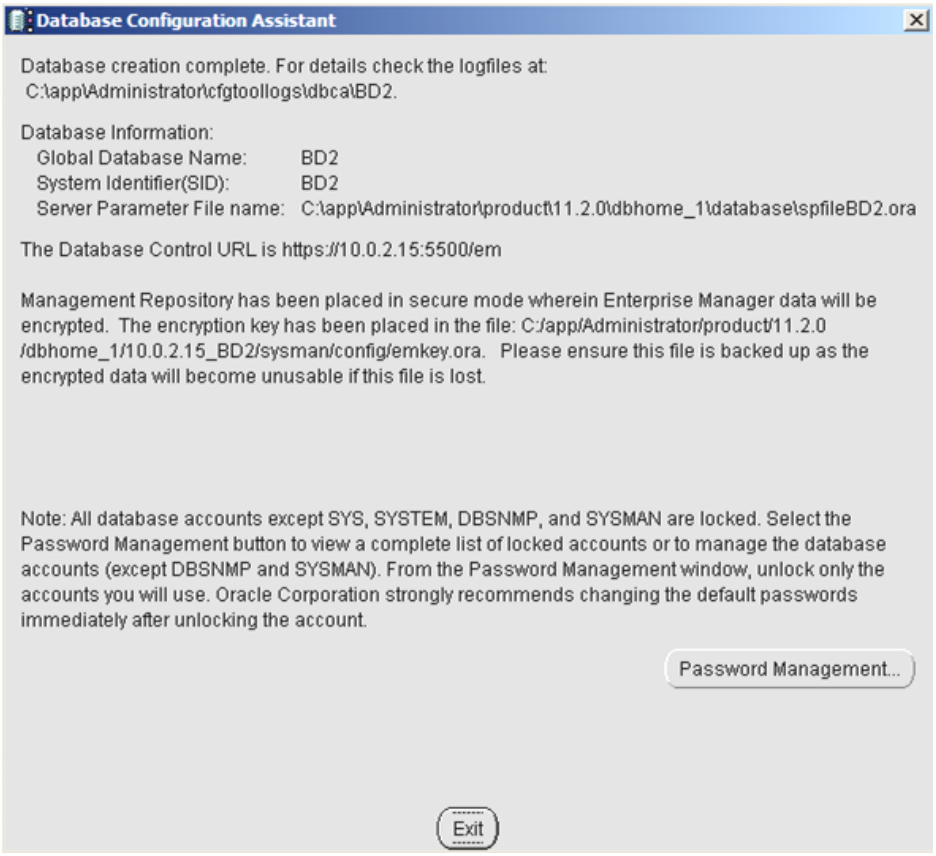

Figura 3. Instância BD2
Fonte: Autores

Os arquivos INITbd2.ora (arquivo de inicialização da instância BD2) e *listener.ora* foram modificados a fim de garantir a comunicação entre as instâncias BD1 e BD2. O arquivo de inicialização da instância auxiliar foi editado a fim de adicionar dois parâmetros para a inicialização da instância, o primeiro DB_FILE_NAME_CONVERT, responsável por converter os nomes dos arquivos de dados e arquivos temporários da instância de produção para o banco de dados duplicados, o segundo LOG_FILE_NAME_CONVERT, designado a nomear os arquivos de *logs* para o banco de dados duplicado. O arquivo listener.ora, que contém a configuração do *listener*, foi editado para receber as requisições da instância auxiliar.

A duplicação do banco de dados para a instância auxiliar foi iniciada utilizando o utilitário RMAN conectado à instância BD2, no comando de duplicação é especificado o caminho do *backup* realizado anteriormente.

A Figura 4 retrata o utilitário RMAN conectado à instância BD2 (não montada) para a duplicação do banco de dados.

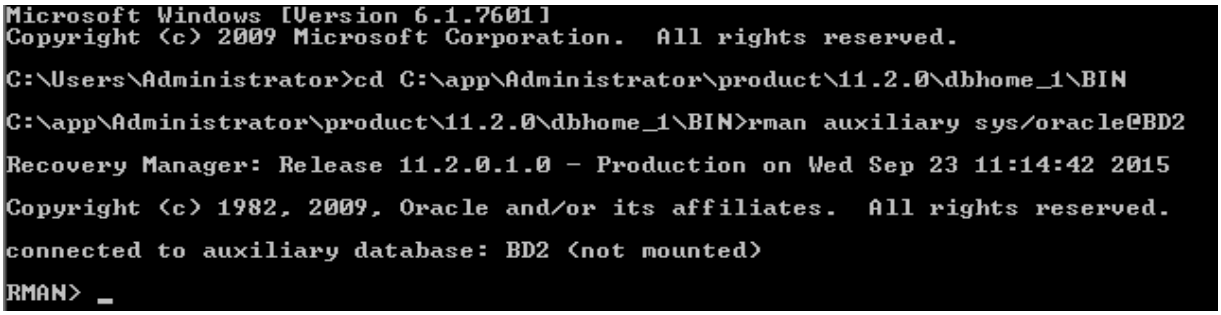

Figura 4. RMAN
Fonte: Autores

3.2. Instalação *Patch Set Update* 11.2.0.4.0 do Banco de Dados Oracle

Para a instalação do *Patch Set Update* foi necessário a descompactação de dois arquivos denominados p13390677_112040_MSWIN-x86-64_1of7.zip e p13390677_112040_MSWIN-x86-64_2of7.zip baixados do *site My Oracle Support*.

O processo consiste na utilização do utilitário DBUA para as configurações da nova versão instalada. Com a instalação da nova versão 11.2.0.4.0 foi criado um novo diretório de instalação do banco de dados (*Oracle_Home*). O nome da instância permaneceu o mesmo. O Quadro 3 apresenta os resultados obtidos durante a utilização do DBUA.

DATABASE	***TARGET DATABASE***
BD1	BD1
11.2.0.1.0	11.2.0.4.0
C:\app\administrator\product\11.2.0\dbhome_1	C:\app\administrator\product\11.2.0\dbhome_2

Quadro 3. *Database Upgrade Summary*
Fonte: Autores

3.3. Configurações para a exploração da vulnerabilidade do Banco de dados Oracle após a instalação do *Patch Set Update*

As configurações realizadas para a exploração da vulnerabilidade após a instalação do P*atch Set Update*, ou seja, com o banco de dados na versão 11.2.0.4.0 foram as mesmas concluídas anteriormente com o banco de dados na versão 11.2.0.1.0.

4. Resultados

A Figura 5 representa a falha na tentativa de duplicação do Banco de dados Oracle versão 11.2.0.1.0 que está localizado na instância BD1 para a instância BD2.

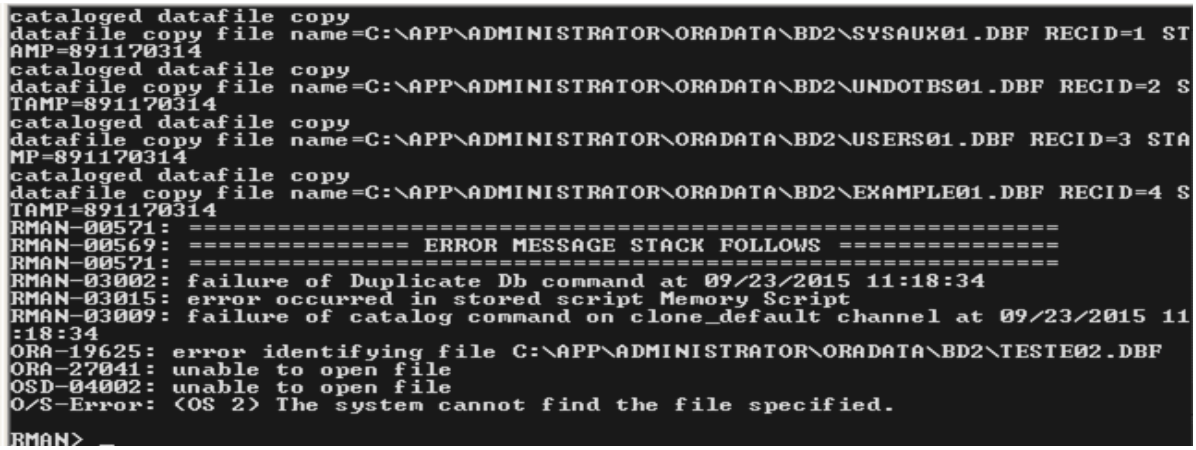

Figura 5. Falha na duplicação do Banco de dados
Fonte: Autores

Na tentativa de duplicação do banco de dados, a descrição dos erros obtidos são demonstrados no Quadro 5.

ERRO	DESCRIÇÃO
RMAN-03002	Falha no comando
RMAN-03015	Erro ocasionado por uma falha do *script* de memória
RMAN-03009	Falha do catálogo de comando no clone_default
ORA-19625	Erro na identificação do *datafile* C:\APP\ADMINISTRATOR\ORADATA\BD2\TESTE02.DBF
ORA-27041	Incapaz de abrir o arquivo

Quadro 5. Descrição Erros da Duplicação
Fonte: Autores

Mediante a tentativa de acessar a instância BD1 é averiguado que o *datafile* 7, pertencente a *tablespace* teste, a mesma que contém o *datafile* 6, que foi alterado para *offline* e posteriormente ao *backup* foi modificado para *online*, não está contido no banco de dados da instância BD1. A partir, como na Figura 6, da visão x$kcvfh é notado os arquivos da instância BD1.

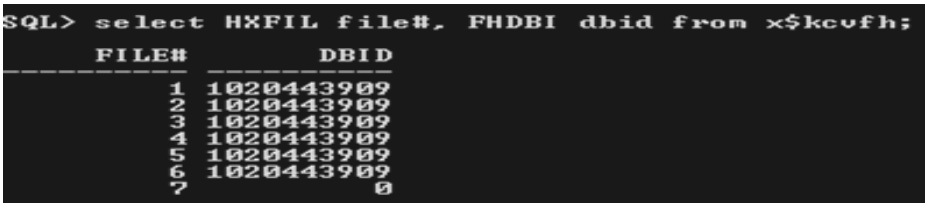

Figura 6. Representa os *datafiles* do Banco de dados da instância BD1
Fonte: Autores

Na instância BD2 ocorreu uma falha no momento de abrir o banco de dados, como visualizado na Figura 7.

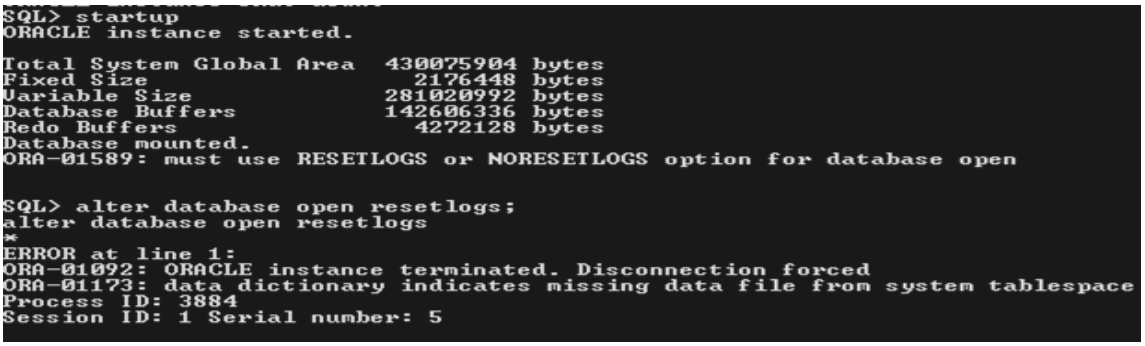

Figura 7. Abrindo o Banco de dados da instância BD2
Fonte: Autores

Após a instalação do *Patch Set Update* 11.2.0.4.0, a duplicação do banco de dados da instância BD1 para a instância BD2 na versão 11.2.0.4.0 ocorreu sem os erros salientados na versão anterior (11.2.0.1.0), mas a *tablespace* teste foi apagada. Como analisado na Figura 8.

Figura 8. Finalização da Duplicação
Fonte: Autores

A Figura 9 retrata os resultados obtidos a partir de uma consulta na *view* x$kcvfh do banco de dados da instância BD1 obtendo os arquivos existentes na base de dados com seu DBID.

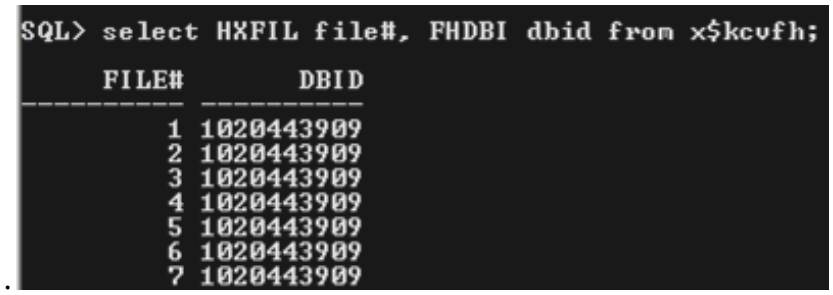

Figura 9. *Datafiles* instância BD1
Fonte: Autores

A Figura 10 demonstra os resultados obtidos de uma consulta à *view* x$kcvfh do banco de dados da instância BD2 é facilmente observado que os *datafiles* existentes da *tablespace* teste (TESTE01.DBF e TESTE02.DBF) foram apagados no momento de finalização da duplicação do banco de dados.

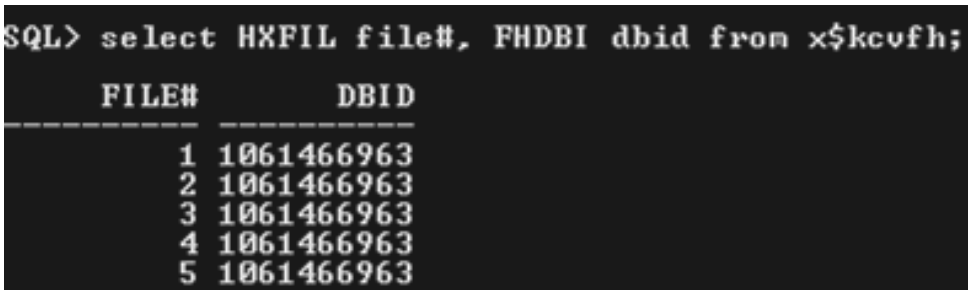

Figura 10. *Datafiles* instância BD2
Fonte: Autores

5. Conclusão

As vulnerabilidades e ameaças existentes em um banco de dados podem ser sanadas através da instalação de pacotes de atualizações disponibilizados pelo fabricante do produto, na medida em que as vulnerabilidades vão sendo conhecidas cabe ao DBA garantir a segurança da base de dados e mantê-la atualizada.

A vulnerabilidade do Banco de dados Oracle na versão 11.2.0.1.0 que causa uma falha na duplicação devido à comparação realizada entre o catálogo do RMAN e os arquivos da instância do banco de dados de produção, pois um determinado arquivo de dados estava *offline* na realização do *backup*, posteriormente alterado para *online* foi corrigida por meio da instalação do *Patch Set Update* 11.2.0.4.0.

Esta afirmação é notada por meio da análise dos resultados obtidos durante o processo de duplicação do banco de dados nas duas versões do *software* gerenciador e a verificação dos arquivos de dados nas duas instâncias dos bancos de dados em ambas as versões por meio de consultas às *views*, sendo assim foi possível observar a conclusão com êxito da duplicação do banco de dados após a instalação do *Patch Set Update*.

Considerando que as vulnerabilidades podem ocasionar prejuízos aos dados armazenados nos bancos de dados, conclui-se que a instalação dos *patches* é uma forma de correção das vulnerabilidades apontadas pela fabricante. É apontado como sugestão para trabalhos futuros promover disponibilidade no ambiente durante a aplicação do *patch*.

6. Referências

Associação Brasileira de Normas Técnicas (2006) “NBR-ISSO-IEC-27001 – Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos”, Rio de Janeiro.

Beaver, K. (2014) “Hacking para leigos”, Rio de Janeiro, Alta Books, 3ª edição.

Codd, E. F. (1972) “Relational Completeness of database sublanguages”, http://www.iai.unibonn.de/III/lehre/vorlesungen/Informationssysteme/WS05/materialien/Codd72a.pdf, Maio.

Dantas, M. L. (2011) “Segurança da informação: Uma abordagem focada em gestão de riscos”, Olinda, Livro Rápido, 1ª edição.

Elmasri, R.; Navathe, S. (2011) “Sistemas de Banco de dados”, São Paulo, Pearson Addison Wesley.

Freitas, E. A. M. (2009) “Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação”, http://bd.camara.gov.br/bd/handle/bdcamara/3564, Maio.

Gregolewitsch, F. R. (2011) “Conceitos de Backup e Recover em relação ao Oracle”, http://www.oracle.com/technetwork/pt/articles/database-performance/conceito-backup-e-recover-em-oracle-1384601-ptb.html, Maio.

Hernandez, M. J. (2013) “Database Design for Mere Mortals: A Hands- On Guide to Relational Database Design”, Addison Wesley, 3ª edição.

Machado, M. J. (2012) “Segurança da informação: Uma visão geral sobre as soluções adotadas em ambientes organizacionais”, Curitiba, Universidade Federal do Paraná.

Matishak, D.; Fuller, M. (2011) “Oracle Database 11g: Workshop de Administração I Guia do Aluno”, Oracle Corporation, 2ª edição, 2 v.

Maurice, E. P. “April 2015 Critical Patch Update Released”, https://blogs.oracle.com/security/, Maio.

Mcclure, S., Scambray, J., Kurtz, G. (2012) “Hacker expostos”, Porto Alegre, Bookman, 7ª edição.

Oracle (2015) “Creating a Database with DBCA”, https://docs.oracle.com/cd/B28359_01/server.111/b28310/create002.htm, Outubro.

_____ (2015) “Duplicating a Database”, http://docs.oracle.com/cd/B28359_01/backup.111/b28270/rcmdupdb.htm, Agosto.

_____ (2015) “Getting Started with RMAN”, https://docs.oracle.com/cd/E11882_01/backup.112/e10642/rcmquick.htm, Outubro.

_____ (2014) “Oracle Critical Patch Update Advisory - July 2014”, http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html, Maio.

_____ (2014) “Text Form of Oracle Critical Patch Update - July 2014 Risk Matrices”, http://www.oracle.com/technetwork/topics/security/cpujul2014verbose-1972958.html#DB, Maio.

_____ (2004) “Upgrading a Database”, https://docs.oracle.com/cd/B16351_01/doc/server.102/b14196/install004.htm, Outubro.

_____ (2015) “V$DATAFILE”, http://docs.oracle.com/cd/B28359_01/server.111/b28320/dynviews_1089.htm, Outubro.

Peltier, T. R. (2013) “Information Security Fundamentals”, CRC Press, 2ª edição.

Price, J. (2009) “Oracle Database 11g: Domine SQL e PL/SQL no Banco de Dados Oracle”, Porto Alegre, Bookman, 1ª edição.

Ralph, A. J., Araújo, M. A. P., Reis, E. S. dos. (2007) “Atualizações no Oracle: Saiba como manter seu banco de dados atualizado e não corra riscos de segurança”, http://www.devmedia.com.br/artigo-sql-magazine-44-atualizacoes-no-oracle-saiba-Lcomo-manter-seu-banco-de-dados-atualizado-e-nao-corra-riscos-de-seguranca/7093, Dezembro.

Santos, V. S. et al. (2014) “Segurança em Banco de Dados: Uma visão geral sobre segurança e suas principais deficiências”, http://www.fepeg.unimontes.br/sites/default/files/resumos/arquivo_pdf_anais/seguranca_em_banco_de_dados_uma_visao_geral_sobre_seguranca_e_as_principais_deficiencias_na_seguranca.pdf, Maio.

Sumathi, S.; Esakkirajan, S. (2010) “Fundamentals of Relational Database Management System”, Springer.