# Segurança em Banco de Dados: Teste de Quebra de Senha por Força Bruta no Banco de Dados Oracle 11G.

**André L. Martins, Edgar F. Lima, Gustavo Bruschi.**

Curso de Tecnologia em Banco de Dados - Faculdade de Tecnologia de Bauru (FATEC)
Rua Manoel Bento da Cruz, nº 30 Quadra 3 - Centro - 17.015-171 - Bauru, SP - Brasil
{andre.martins12, edgar.lima2, gustavo.bruschi}@fatec.sp.gov.br

***Abstract.*** *Information security is a much discussed topic in the information, protect data in a database appears to be simple, but there are several ways of getting into a Database Management System (DBMS), and others to protect. This research aims to guide Database administrators the importance of security knowledge of Oracle databases and other database. The method used to show the invasion of Oracle database was password cracking by brute force with a tool (OPWG) for the system most widely used database in the country. It was concluded that it is possible to use the brute force attack on a DBMS, which reinforces the importance of using complex for users passwords..*

***Resumo.*** *Segurança da Informação é um tema muito discutido na era da informação, proteger os dados em um banco de dados parece ser simples, mas existem várias formas de invadir um Sistema Gerenciador de Banco de Dados (SGDB) e outras de se proteger. Esta pesquisa tem como objetivo orientar os Administradores de Banco de dados a importância do conhecimento de segurança dos bancos de dados da Oracle e outros bancos. O método utilizado para mostrar a invasão do Banco de Dados Oracle, foi quebra de senha por força bruta, utilizando uma ferramenta (OPWG) para o sistema o banco de dados mais utilizado no país. Conclui-se que é possível utilizar com sucesso o ataque de força bruta em um SGBD, o que reforça a importância de se utilizar senhas complexas para os usuários.*

## 1. Introdução

Atualmente, com o avanço do capitalismo no mundo todo, e com a queda das principais potências socialista, o mundo depende cada vez mais de segurança na troca de informações e na guarda de dados. Por isso, cada vez mais, as grandes corporações e órgãos governamentais dependem de um sistema de tecnologia da informação eficiente e que possam armazenar grandes volumes de dados com consistência, escalabilidade, integridade e segurança.

O principal objetivo deste trabalho foi explorar os possíveis pontos vulneráveis dos bancos de dados existentes, principalmente através de um ataque de dicionário de dados.

Existem vários Sistemas Gerenciadores de Banco de Dados (SGBD) disponíveis no mercado, alguns possuem licença pagas e outros podem ser obtidos de forma gratuita

com código fonte aberto. Esses SGBDs oferecem diversos recursos voltados para segurança, porém é possível constatar que os que oferecem maiores recursos, são os que possuem valores comerciais elevados. Um deles é o Oracle Database que, além de diversos recursos relacionados a segurança, possui também recursos relacionados à alta disponibilidade, criptografia dos dados, replicação, entre outros.

Lima (2014) realizou uma pesquisa com base no ranking da db-engines e publicou em seu artigo quais são os bancos de dados mais utilizados atualmente. Este ranking comprova a liderança do banco de dados Oracle e a queda do SQL Server para o terceiro lugar, o MYSQL assumiu a vice-liderança e tem obtido um crescimento expressivo. A Figura 1 a seguir, mostra os bancos de dados mais utilizados no mundo no mês de maio de 2016, segundo o site db-engines.com.

| CLASSIFICAÇÃO | SGBD | MODELO DE BANCO DE DADOS | PONTUAÇÃO | ALTERAÇÕES |
|---|---|---|---|---|
| 1 | Oracle | Relacional | 1468.06 | Menos 149.13 |
| 2 | MySQL | Relacional | 1309.29 | Mais 55.02 |
| 3 | Microsoft SQL Server | Relacional | 1205.87 | Menos 28.58 |
| 4 | Postgre SQL | Relacional | 230.96 | Mais 40.12 |
| 5 | DB2 | Relacional | 190.61 | Mais 24.71 |
| 6 | MongoDB | Não Relacional | 183.07 | Mais 21.20 |
| 7 | Microsoft Access | Relacional | 171.67 | Mais 30.07 |
| 8 | SQLite | Relacional | 99.50 | Mais 20.72 |
| 9 | Sybase | Relacional | 95.28 | Mais 17.53 |
| 10 | Cassandra | Não Relacional | 80.51 | Mais 22.93 |

**Figura 1. Ranking dos principais bancos de dados utilizados nas organizações no mundo.**
**Fonte: http://db-engines.com/en/ranking**

O Oracle nasceu em 1977 e foi o primeiro banco de dados relacional comercializado no mundo. Sua última versão é o Oracle 12C, que é voltada para computação em nuvens, mas de acordo com a Oracle Corporation mantem a maioria da funcionalidade das versões anteriores.

Segundo a Oracle (2014) informa que o custo de uma licença perpétua do database na versão 12c Enterprise Edition custaria hoje por volta de US$ 47.500 por CPU (até 2 Core).

Segundo Prado (2012) a partir de 1985 pode ser instalado em múltiplas plataformas. A versão Enterprise da Oracle tem uma documentação muito bem detalhada possui, mais recursos de segurança comparada com outros bancos.

De acordo com a Oracle (2012) desde a sua fundação em 1977, ela tem sido comprometida com a segurança em seus projetos. Ao longo dos anos, governos e empresas comerciais em todo o mundo têm vindo a contar com a Oracle por suas capacidades de segurança incomparáveis. Com uma boa relação com os clientes a Oracle permitiu-lhe permanecer na vanguarda de banco de dados. Além de desenvolver tecnologias líderes de segurança, a Oracle está comprometida com a segurança da informação. Avaliações de segurança tem sido uma tradição na Oracle para mais de uma

década. Esta tradição tem permitido a Oracle de integrar firmemente as informações dos princípios de garantia em seus processos de desenvolvimento.

A cada versão do banco de dados Oracle, foi se melhorando em todos os aspectos seu banco de dados em nível de segurança, e sempre em cada nova versão se prioriza uma melhoria em alguma ferramenta de segurança:

- Na versão 5 em 1985 a Oracle adicionou o *Audit Vault* para a auditoria do banco, o que ajudaria a determinar quem e quando alguém acessou o banco de dados (colocar fonte)
- Em 1992, já na versão 7, ela desenvolveu a *Auditória de Grão Fino* (FGA) recurso de auditoria proporcionando total controle de quem, quando e o que os usuários estavam fazendo no banco de dados, também permitiu monitorar cada comando, o uso de privilégios e acesso do usuário para um determinado item
- Na versão 8i lançada em 1997 a Oracle surpreendeu adicionando as ferramentas *Transparent Data Encryption* (TDE) e a *Advanced Security*, a TDE projetado para oferecer aos clientes a capacidade de aplicar de forma transparente criptografia dentro do banco de dados sem afetar os aplicativos existentes em quanto a *Advanced Security*, uma ótima opção comumente usados com o Oracle Database Enterprise Edition, fornece dois controles preventivos importantes para proteger dados sensíveis na fonte, incluindo criptografia de banco de dados ( Data Encryption Transparente (TDE) ).
- Em 2001 na versão 9i foi adicionada a *Security Network*, como objetivo de criptografar o tráfego de rede entre um cliente Oracle e banco de dados Oracle e verificar a integridade dos dados.
- A *Label Security* foi composta na versão 10g que foi lançada em 2003, podendo armazenar as habilitações de segurança para todo o empreendimento, está arquitetura oferece às empresas uma solução altamente escalável para gerenciamento de usuários corporativos, um usuário corporativo pode ser propiciado uma vez por aplicativo com autorizações de acesso, certificados, single sign-on web digitais para autenticação PKI, S / MIME e assinatura digital,
- Na versão 11g a ferramenta *data-base firewall* fornece uma primeira linha de defesa para bancos de dados e consolidam dados de auditoria de bancos de dados, sistemas operacionais e diretórios.
- Na versão 12c podemos ver que houve melhorias nas ferramentas de segurança como *Data Masking*, também conhecido como embaralhamento de dados e anonimização de dados que são os processos de substituição de informações confidenciais copiados de bancos de dados de produção, mas limpo, os dados baseados em regras de máscara, *Security Radius* é um protocolo de segurança cliente/servidor utilizado para habilitar a autenticação remota e acesso do banco de dados.

## 2. Formas de Ataques e Vulnerabilidades de Banco de Dados

É de extrema importância o devido entendimento das formas e métodos que um banco de dados possa ser atacado, assim como as vulnerabilidades que um SGBD possa apresentar em determinadas condições, tal conhecimento permite que os profissionais responsáveis pela base de dados tenham condições de elaborar métodos que asseguram o banco de dados e a informação contida no mesmo. Um banco de dados é um serviço

utilizado na rede. Dessa forma, a segurança da rede está altamente relacionada a segurança e a integridade das informações contidas no banco de dados.

## 2.1. Privilégios de Usuários

Segundo Atkinson e Dill (2007) os bancos de dados de uma empresa contêm um grande volume de dados e provavelmente um grande volume de usuários que necessitam ter acesso a estes dados, porém nem todos precisam ter acesso a todos esses dados.

O controle de tais permissões é de extrema importância para o administrador do banco de dados a partir do momento em que um indivíduo tenha acesso total a todos esses dados sem o devido conhecimento ou consciência dos riscos, o mesmo pode alterar ou inserir dados que possam chegar a comprometer toda a base de dados ou a confiabilidade de tais informações.

De acordo com Lima (2014), caso o SGBD seja instalado manualmente e o responsável pelo mesmo não alterar as senhas ou bloquear os usuários padrões que vem pré-configurados no SGBD, tais credenciais podem ser utilizadas por um hacker e o mesmo terá acesso ao banco de dados. Além de tudo é necessário que o administrador de banco de dados tenha um bom conhecimento como a SQL Injection, Malware e portas vulneráveis no banco de dados, com isso se consegue ter ótimos resultados na segurança.

## 2.2. SQL Injection ou Input Injection

De acordo com Medeiros (2014) *SQL Injection* consiste em inserções de comandos SQL em um procedimento SQL través da entrada de dados em uma página de web. Tais comandos combinados com parâmetros específicos alteram os códigos da estrutura da página, aplicação ou banco de dados de maneira indevida e os executa de maneira que os mesmos podem expor dados escondidos, sobrescrevem dados importantes ou até mesmo executar comandos que possam de alguma forma prejudicar o servidor.

## 2.3. Malware

Para Baruque, Grécio e Geus (2011), *Malwares* são programas que englobam como vírus, *worms* e *trojam* (cavalos-de-troia) que infectam maquinas e servidores. Tais programas maliciosos podem ser utilizados de diversas formas como, por exemplo, roubar informações, corromper arquivos ou até mesmo inviabilizar o uso do computador ou servidor.

Atualmente existem alguns vírus que modificam a extensão dos arquivos e criptografam os dados, o "*cryptolocker*", esse vírus é conhecido como "sequestro de dados" e é quase impossível de reverter os dados, os hackers solicitam muito dinheiro para poder devolver os dados originais, mas as empresas têm medo, pois não sabe se vão ter os dados de volta.

## 3. Ataque Através de Força Bruta

Um ataque de força bruta consiste em realizar de forma não autorizada, múltiplas tentativas de acessos a um banco de dados. [Pichiliani 2014]. Esse ataque consiste basicamente em utilizar ferramentas (software) no sentido de descobrir pontos vulneráveis e possíveis brechas deixadas pelo administrador do banco de dados.

Fayó (2010) disponibilizou importantes informações sobre as vulnerabilidades detectadas no protocolo de autenticação do banco de dados Oracle, ele apresentou suas descobertas e métodos pelos quais elas podem ser exploradas.

Embora a Oracle tenha corrigido algumas falhas com o lançamento de um conjunto de patches, Fayó disse que não houve nenhuma correção para as versões 11.1 e 11.2 do banco de dados porque a atualização não foi incluída em qualquer um dos comunicados regulares da Oracle em relação aos "patches de correção crítico".

Se esse protocolo não for ativado manualmente pelos administradores de banco de dados, o banco vai continuar a utilizar a versão vulnerável**.** Um administrador de banco de dados não deixar as configurações padrão de configuração de segurança, quando se quer ter um bom gerenciamento.

Fayó (2011) diz que quando uma tentativa de *login* é feita, o servidor de banco de dados inicialmente envia uma chave de sessão e o salt value do hash de senha. Aparentemente, os potenciais atacantes requerem apenas o nome de um usuário e de um arquivo de banco de dados, pois podem então abortar a comunicação com o servidor e iniciar um ataque de força bruta contra a senha (offline). Porém, este método não causa qualquer falha na tentativa de *login* registrada nos arquivos de log.

Schwade Júnior (2008) esclarece que os scanners de portas realizam inspeções no host alvo com a finalidade de encontrar portas que permitam conexões. Seu objetivo é listar os serviços de rede TCP/IP disponíveis, fazendo com que respondam quando consultados. Existem também os scanners de portas classificados como "invisíveis", que utilizam técnicas de não conexão ou conexão incompleta para não serem detectados. Uma vez que um hacker esteja dentro de sua rede, acessada através de uma porta que estava vulnerável, o mesmo pode muito bem prejudicar as informações do banco de dados ou o acesso a elas.

Para Paula (2014) todo sistema de acesso restrito é acessível através do conjunto nome de usuário e senha, um ataque de força bruta significa tentar adivinhar o conjunto por meio de tentativa e erro. Existem muitas senhas óbvias em contas pelo mundo afora, se um invasor descobrir pelo menos o nome do usuário já tem um bom caminho andado, pois só precisará descobrir a senha. Mesmo considerando a fragilidade apresentada pela maioria de contas de usuários, é inviável deferir um ataque de força bruta manualmente a menos que você seja um daqueles que ganha na loteria quase todo mês, por isso, é preciso utilizar métodos e ferramentas específicas para a realização de um ataque coordenado de força bruta.

## 4. Materiais e Métodos

Com o objetivo de demonstrar um ataque ao banco de dados através de quebra de senha por força bruta no BD Oracle, montou-se um ambiente em rede com um servidor de banco de dados Oracle com a versão 11g Enterprise Edition instalado no Sistema Operacional Windows Server 2008 R2. Para realizar o ataque por força bruta foi

utilizado a ferramenta opwg (ORACLEPWGUESS) que pertence ao toolkit OAT (Oracle Auditing Tools).

Segundo Kevin Orrey (2012), O Oracle Auditing Tools é um conjunto de ferramentas que podem ser utilizadas para enumerar as contas padrão, consultar o TNS, utiliza-se o prompt de comando SQL ou configurar uma sessão TFTP para a transferência de um arquivo executável netcat ao banco de dados remoto. Já o **opwg** Oracle PW Guess é usado para enumerar uma SID múltiplas com nomes de usuários e senhas padrão. O arquivo padrão embutido contém mais de 120 pares de nomes de usuários e senhas que serão carregados automaticamente.

O banco de dados Oracle foi instalado em uma máquina virtual (Oracle VM Virtual Box) da Oracle, com 1GB de memória RAM e 2 GB de HD (verificar isso), a máquina virtual simula um ambiente real. Esta VM foi criada em um Desktop Intel QuadCore 4 GB de memória RAM e 1 TB de HD com o Sistema Operacional Windows Seven Professional x64. Já para a instalação do software de quebra de senha, o OPWG, utilizou um Notebook Intel dual Core com 8 GB de memória RAM e 500 GB de HD, as máquinas foram conectadas através de cabo LAN em um ambiente em rede, também simulou-se um ataque de que quebra de senha por força bruta localmente (localhost), a finalidade de executar os testes em dois ambientes, foi verificar a performance individualmente em cada ambiente.

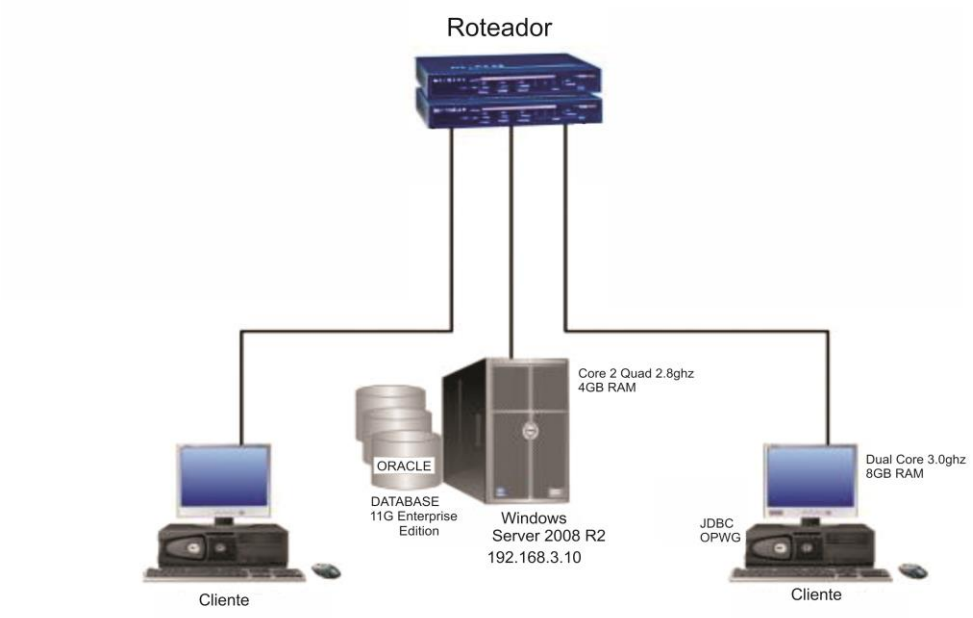


Figura 2: Ambiente de teste (fonte: elaborado pelos autores)

De acordo com a Oracle seu SGBD possui diversas ferramentas e componentes, como:Ferramentas de administração, comunicação, desenvolvimento, gênio de software e decisão. Muitas vezes, cada um destes componentes possui seu próprio login e senha. Sendo assim, para o teste de penetração por força bruta verificou-se a possibilidade de descobrir a senha do usuário SYS através de tentativas de conexão com uma instância

simples. O usuário SYS é o administrador máster de um banco de dados, ele possui todos os privilégios tanto para criar como excluir tabelas, alterar, conceder privilégios, revogar, excluir, entre outros.

Assim como o SQL Server, o Oracle também pode trabalhar com modos de autenticação que utilizem a senha do sistema operacional, apesar de tal prática não ser muito comum. Durante o processo de instalação do Oracle o DBA deve indicar qual é a senha para dois logins com permissões administrativas: SYS e SYSTEM.

Também é importante destacar que o Oracle pode conter diversos logins padrão habilitados para testes ou outros propósitos. Este conjunto de logins padrão representa uma vulnerabilidade de segurança, sendo responsabilidade de o DBA ficar ciente deste fato e gerenciar o catálogo de usuários que podem acessar o banco de dados Oracle. Há também como configurar opções para garantir o bloqueio de senha depois de um número fixo de tentativas e evitar muitas tentativas de conexão em um curto período de tempo.

A ferramenta OPWG é executada e configurada na máquina cliente junto com o conjunto de driver JDBC. Além disso, é necessário dois arquivos no formato *txt: o primeiro* com a listagem de *strings* representando os usuários (quando não se sabe nenhum usuário do banco) e o segundo com as senhas para realizar as combinações, possibilitando os testes para quebra de senha. O software realiza uma sequência de combinações entre cada nome (*string*) listado no primeiro arquivo com todas as strings do segundo arquivo, representando as senhas, conforme pode ser visualizado na Figura 3.

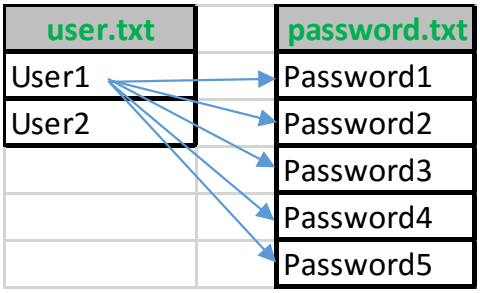


Figura 3: Sequência de teste de usuário e senha da ferramenta opwg (fonte: os autores)

## 5. Resultados obtidos

Para elaboração dos testes, foram utilizados alguns arquivos de usuários e senhas encontrados na Internet, que foram baixados do site vulnerabilityassessment. co.uk, para escolha das senhas, tomou-se como base as senhas e logins mais utilizados por usuários e DBA's.

A Figura 4 mostra o uso do programa opwg. Para tentar descobrir um usuário e senha do banco de dados Oracle, foi encontrado o usuário SYS em uma instância do Oracle sendo executado na mesma rede, com a senha "oracle".

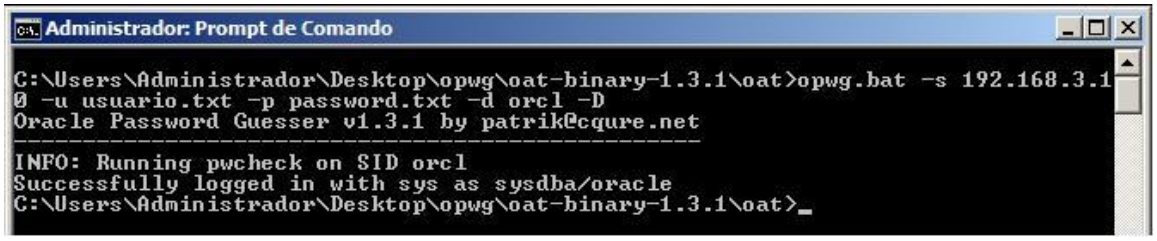


*Figura 4. Uso do programa opwg para testes de penetração por força bruta no Oracle. (fonte: os autores)*

Na linha de comando, foi utilizado os seguintes parâmetros exigidos pelo software:

- *–s 192.168.3.10*: indica o endereço IP do servidor de banco de dados Oracle.
- -u users.txt: indica o arquivo com a lista de strings representando o usuário a ser quebrado.
- -p password.txt: indica o arquivo com a lista de strings representando a senha.
- -d orcl: representa o nome de identificação da instância.
- -D: indica que não serão testados logins e senhas comuns armazenadas na ferramenta.

Como a Figura 4 apresenta, o resultado da execução do ORACLEPWGUESS indica que ele encontrou a credencial para acessar o Oracle dentre os valores armazenados nos arquivos *usuario.txt* (para os logins) e *password.txt* (para as senhas).

Além disso, foram realizados alguns testes para avaliar o desempenho da ferramenta em relação ao tempo para a descoberta de usuário e senhas, com seis arquivos no formato (*.txt*), três arquivos *usuário.txt* e três *password.txt* e com quantidades diferentes de combinações. A Gráfico 1 apresenta a quantidade de combinações realizadas, além do tempo total de cada teste.

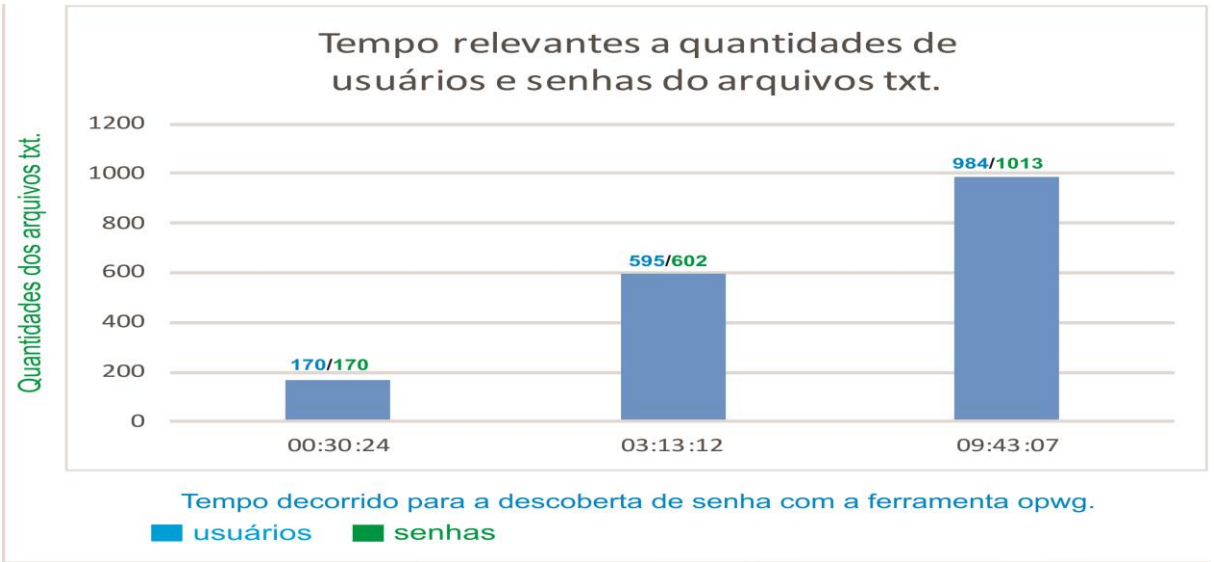


**Gráfico 1. Tempo de descoberta de senha com a ferramenta opwg**
**Fonte: Elaborado pelos autores.**

## 6. Conclusão

Este trabalho apresenta um estudo relacionado a segurança da informação em SGBDs, com ênfase no Oracle Database 11G. Foi possível avaliar a ferramenta opwg, como ela atua na tentativa de quebra de senhas através de força bruta. Na avaliação geral, os objetivos propostos foram alcançados, porém, foram encontrados muitos obstáculos para a execução dos testes devido à falta de documentação específica do tema. A ferramenta opwg foi encontrada no site Vunerability Assment e foi utilizada o driver JDBC "classes12.zip", encontrado no site do Java.

Após muitas tentativas, simulando um ambiente em rede com o banco de dados instalado em um Server 2008, como cliente utilizamos um computador com Windows 7 x64bits, foi possível realizar com sucesso um ataque de força bruta, obtendo o usuário e senha através de arquivos com combinações de strings representando os usuários e senhas, estes disponíveis na Internet.

Desta forma, confirma-se que a escolha de uma senha complexa, utilizando-se de letras e números deve ser uma regra para o DBA, pois com pouco esforço e com pouco conteúdo para explorar o tema, foi possível executar a quebra de senha de um dos melhores e mais seguro banco de dados disponível no mercado.

De forma geral, os SGBDs possuem diversos recursos para reforçar a segurança e impedir acessos indevidos, porém cabe aos administradores de banco de dados a utilização de boas práticas para evitar maiores problemas.

## 7. Referências


Atkinson, R; Dill e Sergio L. (2007) “Segurança em banco de dados: conceitos fundamentais”. http://www.devmedia.com.br/artigo-sql-magazine-27-seguranca-em-banco-de-dados-conceitos-fundamentais/6903#. Artigo SQL Magazine 27.

Baruque, A. O. C.; Gregio, A. R. A. e Geus, P. L. (2011) “Análise visual de comportamento de código malicioso”. In: JORNADA DE INICIAÇÃO CIENTÍFICA DO CENTRO DE TECNOLOGIA DA INFORMAÇÃO RENATO ARCHER, 13. Campinas. Anais... Campinas: CTI, 2011. p. 179-187.

Fayó E.M. (2011) “Vulnerabilidades detectadas no protocolo de autenticação do banco de dados Oracle” http://www.diegomacedo.com.br/possiveis-ataques-de-forca-bruta-em-senhas-da-oracle.

Ferramenta OPWG (2012) – Vulnerability Assessment - Patrik Karlsson http://www.vulnerabilityassessment.co.uk/oat.htm.

Lima, A.G.B. (2014) “Sete erros comuns na segurança do banco de dados”. http://www.devmedia.com.br/sete-erros-comuns-na-seguranca-de-bancos-dados/31549.

Medeiros, H. (2014) “SQL Injection em múltiplas plataformas”. http://www.devmedia.com.br/sql-injection-em-multiplas-plataformas/31389.

Oracle (2012) “Big Data, Big Challenges, Big Opportunities” http://www.ioug.org/researchwire.

Orrey K (2008) – Vulnerability Assesment.
http:// http://www.vulnerabilityassessment.co.uk/

Paula F.B. (2014) “Técnicas de tentativas de invasão de sistemas”
https://www.vivaolinux.com.br/artigo.

Pichiliani M. (2014) “Testando a senha do banco de dados”.
http://www.devmedia.com.br/testando-a-senha-do-banco-de-dados/30667

Prado F. (2012) “Qual é o melhor banco de dados Oracle ou SQLServer”.

http://www.fabioprado.net/2012/01/qual-e-o-melhor-banco-de-dados-oracle.html.
Silberschatz, A; Korth, H.F. e Sudarshan, S. (1999) “Sistemas de bancos de dados. São Paulo: Makron Books”3 ª edição.

Schwade Junior O. (2010) “Roteiro para a Realização de Testes de Penetração em Cenários TURN-KEYS” Trabalho de Conclusão de Curso- Universidade do vale do Itajaí, Itajaí- SC.