Protegendo o seu BD Oracle com Autenticação em 2 etapas

Rodrigo Jorge

Nossos Patrocinadores

DELL EMC

TmaxSoft Brasil

STROHL Brasil

Timbira
A empresa brasileira de PostgreSQL

GREEN tecnologia

DBA4All
We care about your data

DB Academy

ORAMASTER

enkitec

accenture
High performance. Delivered.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

cpMBroxis

IBM

amdocs
embrace challenge e³perience success

Ipiranga

- Since Nov/2016
- Oracle Security Solution Architect

Elite

- Global systems integrator focused on the Oracle platform
- Consultants average 15+ years of Oracle experience
- Worldwide specialist in Engineered Systems implementations
- 16 Oracle ACE members, specialist recognized by Oracle for their technical expertise

Expertise

Oracle Specializations*

- Oracle Exadata
- Oracle Exalogic
- Oracle Database
- Oracle GoldenGate
- Oracle Data Integrator
- Oracle Database
- Oracle Data Warehouse
- Oracle Real Application Cluster
- Oracle Performance Tuning
- Oracle Database Security

Oracle Engineered Systems Numbers

- 700+ Oracle Engineered Systems which AEG have configured, patched or supported.
- 190 AEG resources which have an average 15+ years of Oracle experience
- AEG Support across 27 countries
- 150 Oracle Engineered Systems (Exadata/Exalogic etc) currently under management directly by AEG
- 205 customers in either the AEG Managed Services program or remoteDBA program
- 50,000 Accenture Oracle IDC resources that can be leveraged for Level 1 & Level 2 support

Success

ORACLE Diamond Partner

ORACLE Diamond Partner Global Cloud Elite

UKOUG Awards GOLD WINNER

Thought Leadership

Our consultants have been published in multiple subject areas and additional online resources that demonstrate Accenture's experience and expertise with the OES platform

*https://www.accenture.com/us-en/service-oracle-diamond-partner

Agenda

- O problema das senhas.
- O problema da Oracle.
- Entendendo o Two Factor.
- OraTOtP !
- Live Demo
- Conclusão

Pra começar …

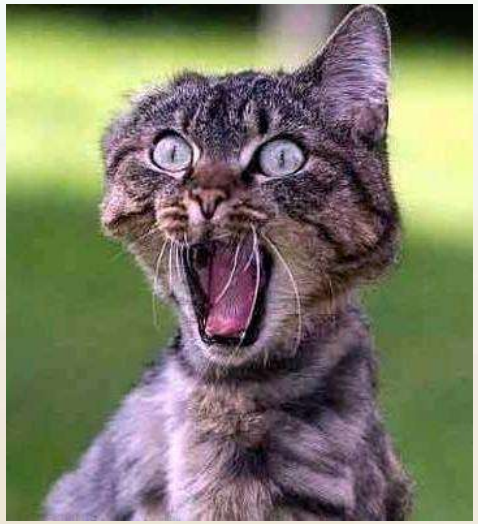
- Foi perguntado para 1000 pessoas acima de 18 anos se elas **reutilizam** ou não a **mesma senha** em **sites diferentes**:

Pra começar …

- Responderam que **SIM** :

87%

entre 18-30 anos



81%

31 anos ou acima

Source: http://www.bio-key.com/blog/bad_news.html

Você confia em todos os desenvolvedores?

Mais alguns dados:

90% das senhas atacadas são crackeadas em até 6 horas.

65% das pessoas usam a MESMA senha em todos os lugares.

21% das pessoas usam a mesma senha a mais de 10 anos.

30% das pessoas tem mais do que 10 senhas para memorizar.

75% das pessoas trocam apenas uma letra para criar uma senha que elas consideram únicas.

47% das pessoas usam a mesma senha a pelo menos 5 anos.

Source: https://assets.entrepreneur.com/static/1433198293-password-info.jpg

Top 5 senhas mais comuns:

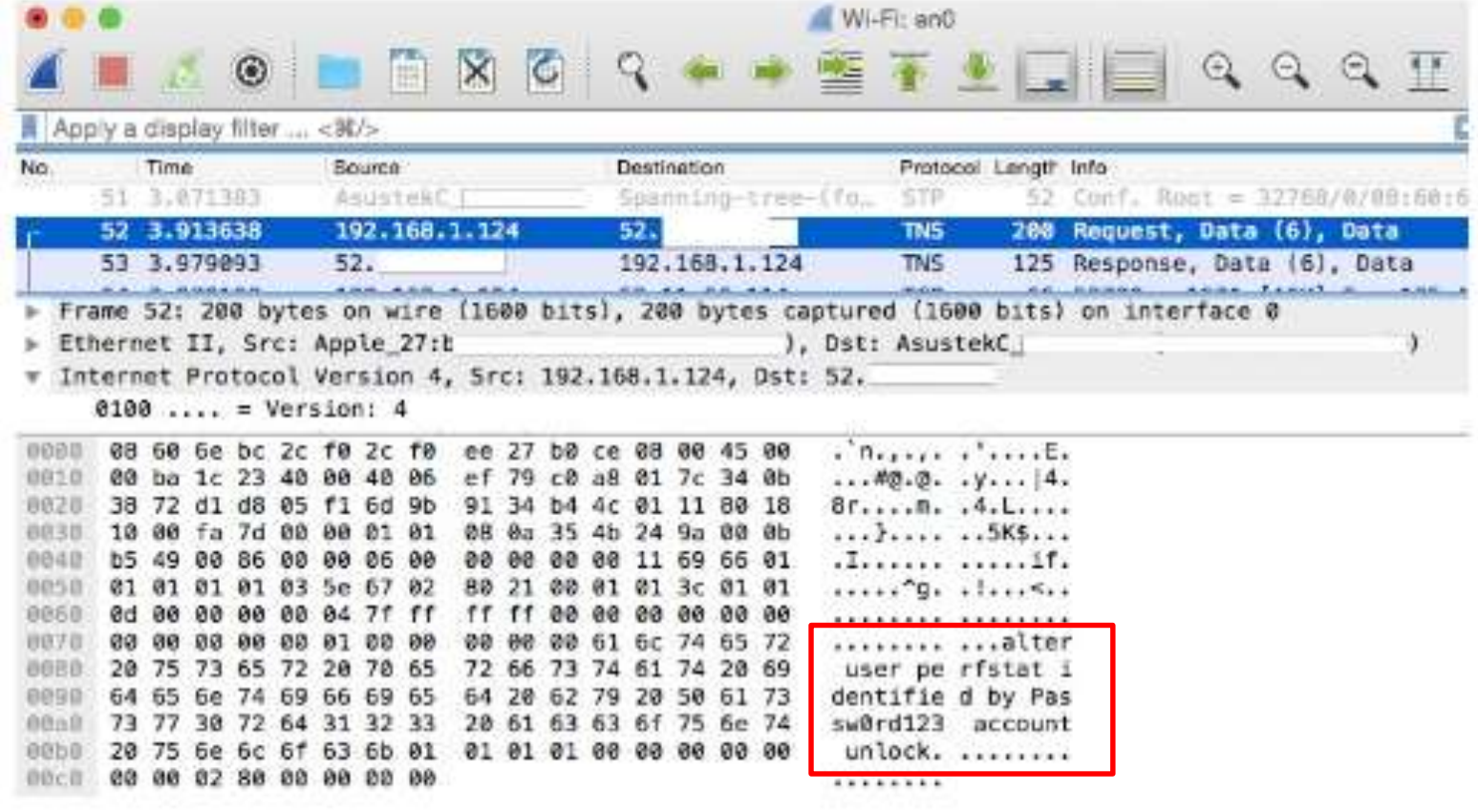
- 1. 123456
- 2. PASSWORD
- 3. 12345
- 4. 12345678
- 5. QWERTY

Source: https://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514

Formas de ataques de senhas:

- Interceptar a senha (hash ou raw) na rede (ex: Wireshark)

Wireshark



Source: https://www.slideshare.net/Pythian/2016-1160-paneppt

Formas de ataques de senhas:

- Interceptar a senha (hash ou raw) na rede (ex: Wireshark)
- Olhando o teclado (ex: “shoulder surfing”, camera)

Shoulder Surfing

Formas de ataques de senhas:

- Interceptar a senha (hash ou raw) na rede (ex: Wireshark)
- Olhando o teclado (ex: “shoulder surfing”, camera)
- Keylogger (ex: software, USB, PS/2 ou acoplado ao teclado)

Keylogger Level Hard

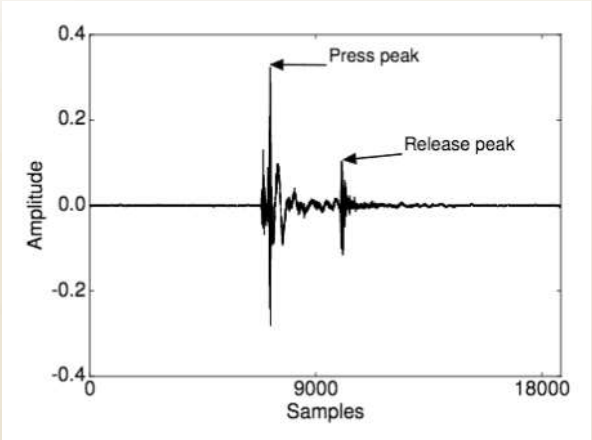
Price: $52.99 & FREE Shipping.

Price: $141.99 + $5.99 shipping

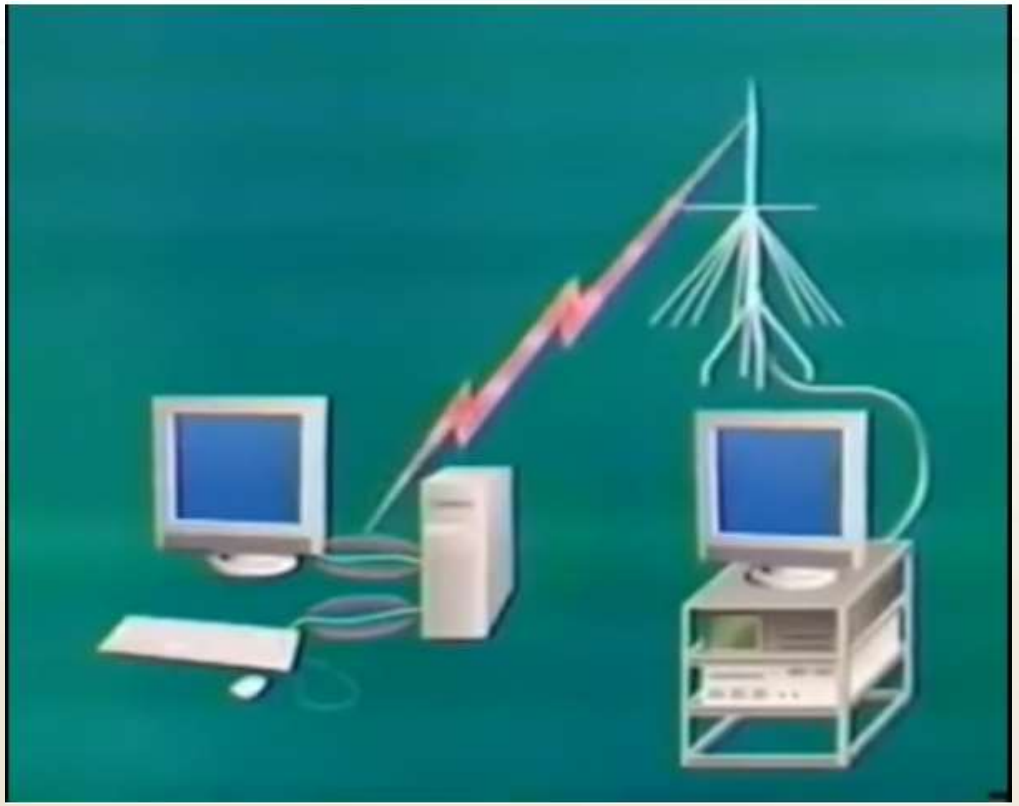
Source: amazon.com

Keyboard Eavesdropping

- "We examine the problem of keyboard acoustic emanations. We present a novel attack taking as input a 10-minute sound recording of a user typing English text using a keyboard and recovering up to 96% of typed characters."
- **Paper:** http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/tiss.preprint.pdf



Van Eck Phreaking



Example: https://www.youtube.com/watch?v=AFWgIAgMtiA

Formas de ataques de senhas:

- Interceptar a senha (hash ou raw) na rede (ex: Wireshark)
- Olhando o teclado (ex: “shoulder surfing”, camera)
- Keylogger (ex: software, USB, PS/2 ou acoplado ao teclado)
- Brute force attack (ex: com woraauthbf)
- Dictionary attack (ex: com checkpwd ou repscan)
- Rainbow Table attack (ex: com ophcrack ou cain)
- Authentication attack (ex: com woraauthbf ou orakel)

O PROBLEMA DA ORACLE

(Armazenamento de hashes)

Até Oracle 10gR2 (desde o Oracle 6)

- Senha armazenada em DES – 8 bytes – 16 hex characters.
- Case insensitive.
- Forma de geração:
  1. Converte Username para maiúscula: ‘sys’ vira ‘SYS’
  2. Converte Password para maiúscula: ‘pass’ vira ‘PASS’
  3. Concatena ambas as senhas, ‘SYSPASS’ e criptografa usando 3DES (TripleDES).
- Username é o SALT.
- Suscetível a Rainbow Attack!
- Coluna password da user$

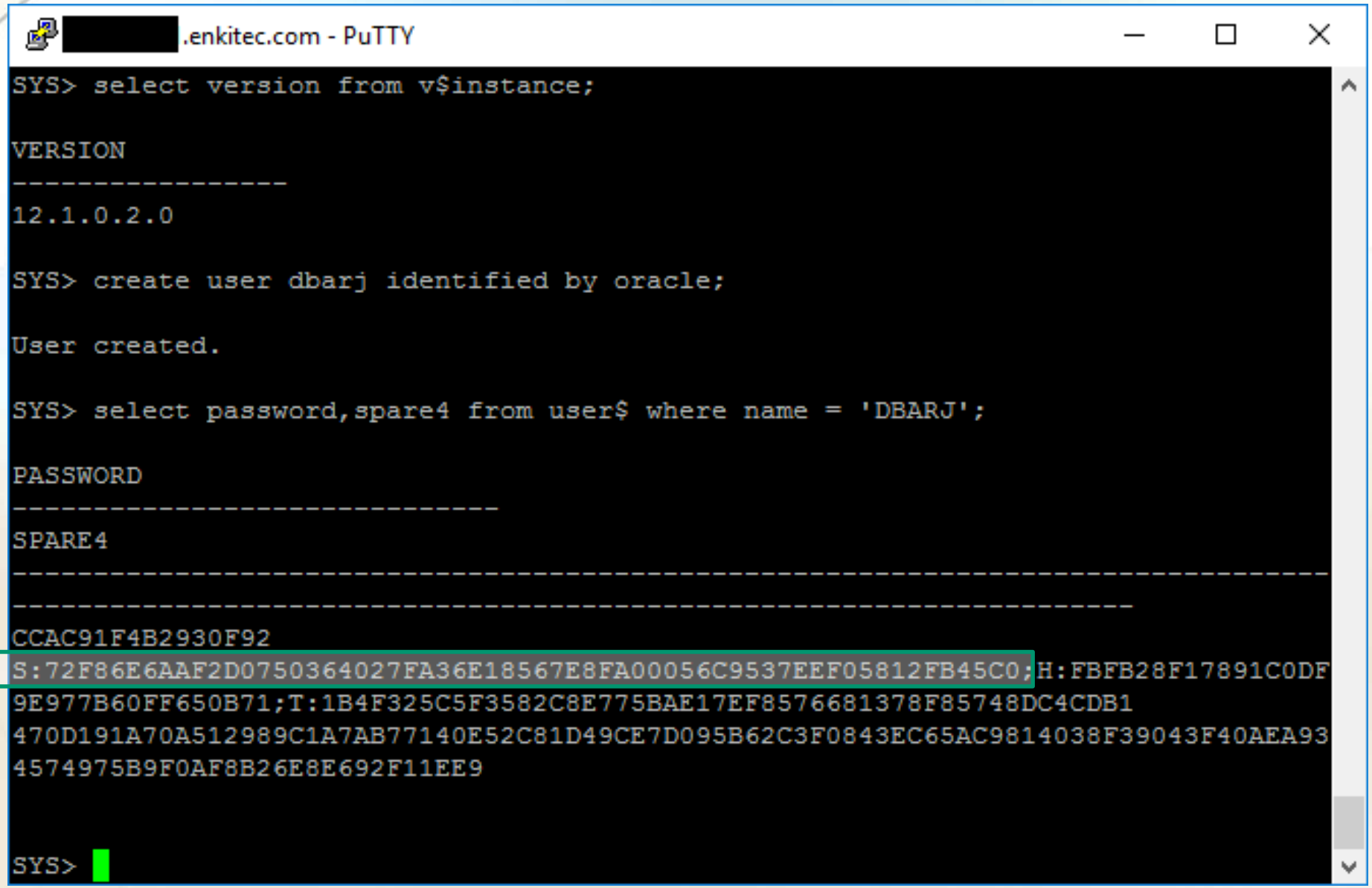
[redacted].enkitec.com - PuTTY

```
SYS> select version from v$instance;

VERSION
-----------------
12.1.0.2.0

SYS> create user dbarj identified by oracle;

User created.

SYS> select password,spare4 from user$ where name = 'DBARJ';

PASSWORD
------------------------------
SPARE4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CCAC91F4B2930F92
S:72F86E6AAF2D0750364027FA36E18567E8FA00056C9537EEF05812FB45C0;H:FBFB28F17891C0DF
9E977B60FF650B71;T:1B4F325C5F3582C8E775BAE17EF8576681378F85748DC4CDB1
470D191A70A512989C1A7AB77140E52C81D49CE7D095B62C3F0843EC65AC9814038F39043F40AEA93
4574975B9F0AF8B26E8E692F11EE9


SYS>
```

DES

Oracle 11g

- Senha armazenada em SHA-1 – 20 bytes – 40 hex characters + 10 bytes SALT
- SALT aleatório.
- Forma de geração:
  1. Gera um Salt aleatório de 10 bytes.
  2. Concatena a senha com o SALT.
     Ex: Senha ‘pass123’ -> ‘pass123’ + 0x6271691FC55C1F56554A
  3. Criptografa usando SHA-1.
- Coluna spare4 da user$, atributo “S:”.
- Crackear SHA-1 é mais rapido do que DES (~9.5x).


[redacted].enkitec.com - PuTTY
SYS> select version from v$instance;
VERSION
12.1.0.2.0
SYS> create user dbarj identified by oracle;
User created.
SYS> select password,spare4 from user$ where name = 'DBARJ';
PASSWORD
SPARE4
CCAC91F4B2930F92
S:72F86E6AAF2D0750364027FA36E18567E8FA00056C9537EEF05812FB45C0;H:FBFB28F17891C0DF
9E977B60FF650B71;T:1B4F325C5F3582C8E775BAE17EF8576681378F85748DC4CDB1
470D191A70A512989C1A7AB77140E52C81D49CE7D095B62C3F0843EC65AC9814038F39043F40AEA93
4574975B9F0AF8B26E8E692F11EE9
SYS>
SHA1

Oracle 12c

- Senha armazenada em SHA2 – 80 bytes – 160 hex characters.
- Combina o SHA2 – (SHA512) e o algorítmo PBKDF2:
  - PBKDF2 é executado no cliente.
  - SHA2 é terminado no lado do servidor.
- Coluna spare4 da user$, atributo “T:”.
- Crackear SHA2 é mais devagar do que SHA-1 (~84.000x).

[redacted].enkitec.com - PuTTY

```
SYS> select version from v$instance;

VERSION
-----------------
12.1.0.2.0

SYS> create user dbarj identified by oracle;

User created.

SYS> select password,spare4 from user$ where name = 'DBARJ';

PASSWORD
------------------------------
SPARE4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CCAC91F4B2930F92
S:72F86E6AAF2D0750364027FA36E18567E8FA00056C9537EEF05812FB45C0;H:FBFB28F17891C0DF
9E977B60FF650B71;T:1B4F325C5F3582C8E775BAE17EF8576681378F85748DC4CDB1
470D191A70A512989C1A7AB77140E52C81D49CE7D095B62C3F0843EC65AC9814038F39043F40AEA93
4574975B9F0AF8B26E8E692F11EE9


SYS>
```

SHA512

Crackeando hashes

- Grande evolução de hardware das placas gráficas.
- Grande evolução dos algoritmos de password crack.
- Péssima evolução da complexidade das hashes nos SGBDs

Brutalis

- **Product:** Sagitta Brutalis 1080 (PN S3480-GTX-1080-2697-128)
- **Software:** Hashcat v3.00-beta-145-g069634a, Nvidia driver 367.18
- **Accelerator:** 8x Nvidia GTX 1080 Founders Edition

21,169.00 USD

Benchmarks

Hashtype	Speed (H/s)
Oracle: DES:: Type: (Oracle: 7+)	7.208.400.000
Oracle: S:: Type: (Oracle: 11+)	68.697.900.000
Oracle: T:: Type: (Oracle: 12+)	818.000

Source: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

Benchmarks

Hashtype	Speed (H/s)
Oracle: DES:: Type: (Oracle: 7+)	7.208.400.000
Oracle: S:: Type: (Oracle: 11+)	68.697.900.000
Oracle: T:: Type: (Oracle: 12+)	818.000
Office 2013	70.884

Source: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

Oracle: DES:: Type: (Oracle: 7+)

Password Length	Time - CS 10	Time - CS 26	Time - CS 36	Time - CS 50
8	0 secs	28 secs	6 mins	1 hours
9	0 secs	12 mins	3 hours	3 days
10	1 secs	5 hours	5 days	5 months
11	13 secs	5 days	7 months	21 years
12	2 mins	5 months	21 years	1088 years

```
CS 10 = 0-9
CS 26 = A-Z
CS 36 = CS10 + CS26
CS 50 = CS36 + !@#$%^&*()-_+=
```

Oracle: S:: Type: (Oracle: 11+)

Password Length	Time - CS 10	Time - CS 26	Time - CS 36	Time - CS 50	Time - CS 76
8	0 secs	3 secs	41 secs	9 mins	4 hours
9	0 secs	1 mins	24 mins	7 hours	14 days
10	0 secs	34 mins	14 hours	16 days	3 years
11	1 secs	14 hours	22 days	2 years	228 years
12	14 secs	16 days	2 years	114 years	17378 years

```
CS 10 = 0-9
CS 26 = A-Z
CS 36 = CS10 + CS26
CS 50 = CS36 + !@#$%^&*()-_+=
CS 76 = CS50 + a-z
```

Oracle: T:: Type: (Oracle: 12+)

Password Length	Time - CS 10	Time - CS 26	Time - CS 36	Time - CS 50	Time - CS 76
8	2 mins	2 days	1 months	1 years	43 years
9	20 mins	2 months	3 years	76 years	3324 years
10	3 hours	5 years	143 years	3838 years	252677 years
11	1 days	144 years	5173 years	191911 years	19203481 years
12	14 days	3750 years	186234 years	9595563 years	1459464583 years

```
CS 10 = 0-9
CS 26 = A-Z
CS 36 = CS10 + CS26
CS 50 = CS36 + !@#$%^&*()-_+=
CS 76 = CS50 + a-z
```

Oracle 12c Password Hash

- O novo algorítmo é bom…
- Porém ……

- Surgiu algo estranho…

[redacted].enkitec.com - PuTTY

```
SYS> select version from v$instance;

VERSION
-----------------
12.1.0.2.0

SYS> create user dbarj identified by oracle;

User created.

SYS> select password,spare4 from user$ where name = 'DBARJ';

PASSWORD
------------------------------
SPARE4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CCAC91F4B2930F92
S:72F86E6AAF2D0750364027FA36E18567E8FA00056C9537EEF05812FB45C0;H:FBFB28F17891C0DF
9E977B60FF650B71;T:1B4F325C5F3582C8E775BAE17EF8576681378F85748DC4CDB1
470D191A70A512989C1A7AB77140E52C81D49CE7D095B62C3F0843EC65AC9814038F39043F40AEA93
4574975B9F0AF8B26E8E692F11EE9


SYS>
```

??????

Oracle 12c Password Hash

- Enquanto um time da Oracle trabalha cuidando da segurança ..
- Existe um outro time responsável pela implementação de webdav / EM Express Edition ..
- E aparentemente esse outro time não entende nada de segurança ..
- Pois resolveu autenticar os usuário do EM Express baseado em uma RFC de 1999.

Source: https://www.ietf.org/rfc/rfc2617.txt

Oracle 12c Password Hash

- Usando UNSALTED MD5 !!!!!!!!!!
- Pra cada hash de senha “T:” segura em PBKDF2 você possui, vem junto um hash “H:” em MD5.
- Quebrar 1 hash em PBKDF2 equivale a 245.000 hashes em MD5.

Oracle 12c – HTTP Digest

- Atributo “H:”. Abreviação para HTTP Digest Authentication.
- Digest -> MD5 -> LIXO
- Senha armazenada em MD5 – 16 bytes – 32 hex characters.
- Apesar de maior número de bytes que DES, é quebrada 27x mais rápido.

[redacted].enkitec.com - PuTTY

```
SYS> select version from v$instance;

VERSION
-----------------
12.1.0.2.0

SYS> create user dbarj identified by oracle;

User created.

SYS> select password,spare4 from user$ where name = 'DBARJ';

PASSWORD
------------------------------
SPARE4
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
CCAC91F4B2930F92
S:72F86E6AAF2D0750364027FA36E18567E8FA00056C9537EEF05812FB45C0;H:FBFB28F17891C0DF
9E977B60FF650B71;T:1B4F325C5F3582C8E775BAE17EF8576681378F85748DC4CDB1
470D191A70A512989C1A7AB77140E52C81D49CE7D095B62C3F0843EC65AC9814038F39043F40AEA93
4574975B9F0AF8B26E8E692F11EE9


SYS>
```

MD5

Benchmarks

Hashtype	Speed (H/s)
Oracle: DES:: Type: (Oracle: 7+)	7,208,400,000
Oracle: S:: Type: (Oracle: 11+)	68,697,900,000
Oracle: T:: Type: (Oracle: 12+)	818,000
Oracle: MD5:: Type: (Oracle: 12+)	200,300,000,000

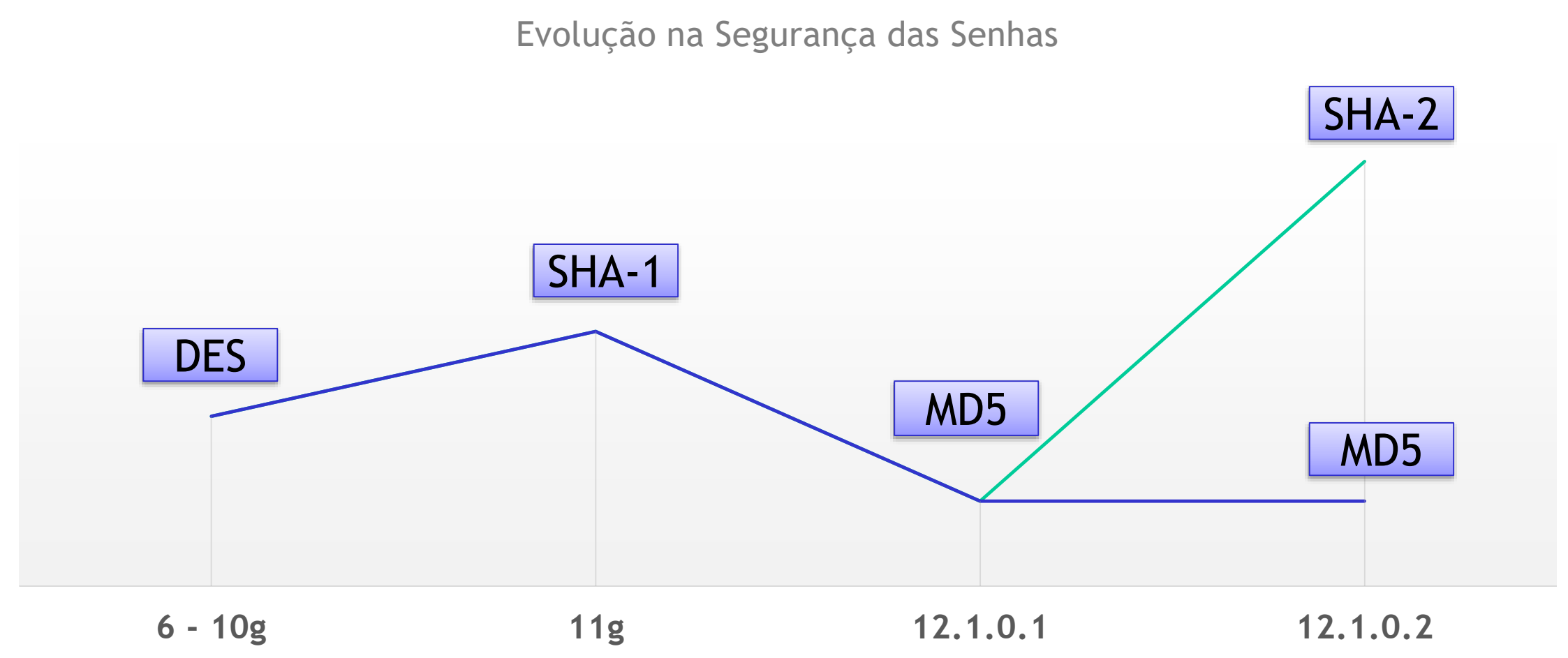
Source: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

Oracle: MD5:: Type: (Oracle: 12+)

Password Length	Time - CS 10	Time - CS 26	Time - CS 36	Time - CS 50	Time - CS 76
8	0 secs	1 secs	14 secs	3 mins	1 hours
9	0 secs	27 secs	8 mins	2 hours	4 days
10	0 secs	11 mins	5 hours	5 days	1 years
11	0 secs	5 hours	7 days	9 months	78 years
12	4 secs	5 days	9 months	39 years	5960 years

```
CS 10 = 0-9
CS 26 = A-Z
CS 36 = CS10 + CS26
CS 50 = CS36 + !@#$%^&*()-_+=
CS 76 = CS50 + a-z
```

Evolução da Senha no Oracle



Um problema de todos

Hash Type	Speed (H/s)
MSSQL(2000)	69,234,100,000
MSSQL(2005)	69,331,000,000
MSSQL(2012)	8,623,700,000
MySQL323	414,400,000,000
MySQL4.1/MySQL5	30,793,600,000
MySQL: Challenge-Response: Aut	18,395,900,000
Oracle: H:: Type: (Oracle: 7+)	7,208,400,000
Oracle: S:: Type: (Oracle: 11+)	68,697,900,000
Oracle: T:: Type: (Oracle: 12+)	818,000
Oracle: MD5:: Type: (Oracle: 12+)	200,300,000,000
PostgreSQL	200,100,000,000
PostgreSQL: Challenge-Response	53,706,200,000
Sybase: ASE	3,209,400,000

Controlar os tipos de hashes armazenados

- SQLNET.ALLOWED_LOGON_VERSION_SERVER

```
Default = 8 -> TODAS HASHES são armazenadas
= 10  -> TODAS HASHES são armazenadas
= 11  -> Remove as hashes em DES (user$.password)
= 12  -> Corrige CVE-2012-3137 / 11.2.0.3 ou maior.
= 12a -> Remove as hashes em SHA1 (user$.spare4)
```

- Como remover MD5 (HTTP Digest) hashes ?

```
update user$
set spare4 = regexp_replace(spare4,'H:([[:digit:]]|[A-F])*(;)?','')
where instr(spare4, 'H:')>0;
```

** USE POR SUA CONTA E RISCO! NÃO HOMOLOGADO PELA ORACLE!

Automatizando:

```
CREATE OR REPLACE TRIGGER Sys_User_Remove_Digest
AFTER ALTER ON DATABASE
WHEN (ora_dict_obj_type = 'USER')
BEGIN
  update user$
  set spare4 = regexp_replace(spare4,'H:([[:digit:]]|[A-F])*(;)?','')
  where instr(spare4, 'H:')>0 and name=ora_dict_obj_name;
END;
/
```

**** USE POR SUA CONTA E RISCO! NÃO HOMOLOGADO PELA ORACLE!**

Antes

```
SQL> alter user c##DBARJ identified by oracle;

User altered.

SQL> select password, spare4 from user$ where name='C##DBARJ';

PASSWORD
---------------
SPARE4
--------------------------------------------------------------------------------
099284AE54251642
S:36A79DEC4FA97F7F2A3AA58CE151F71BB32D78D9DE5839BB9208FAAAFFD8;H:6747F421C1E3C9B
ABE3E7CE6EB6FD08A;T:F561744F19996B34313890FEE14459D903CB1B61552AAA25C45F765DB67A
5B491169553772 62F9AB6B3E52FF60BEECFFCB8010A37ABBD19A243B3300A2543610495AC1F86703
AC121AD6FCAA5DD80FB6

SQL>
```

Depois

```
SQL> alter user c##DBARJ identified by oracle;

User altered.

SQL> select password, spare4 from user$ where name='C##DBARJ';

PASSWORD
---------------
SPARE4
------------------------------------------------------------------------------

T:9422131E48E716A30788F5A5748A67A656FAEF40A0883C9238F24C0BD0CDF095113D01B6CA1B3B
8BEC93FEE92A11955748D6663F1BCE3478A4FBB9A79A1A0EFFD5071A921389ED7EDA91FD54428674
F3

SQL>
```

Não confie em Senhas !

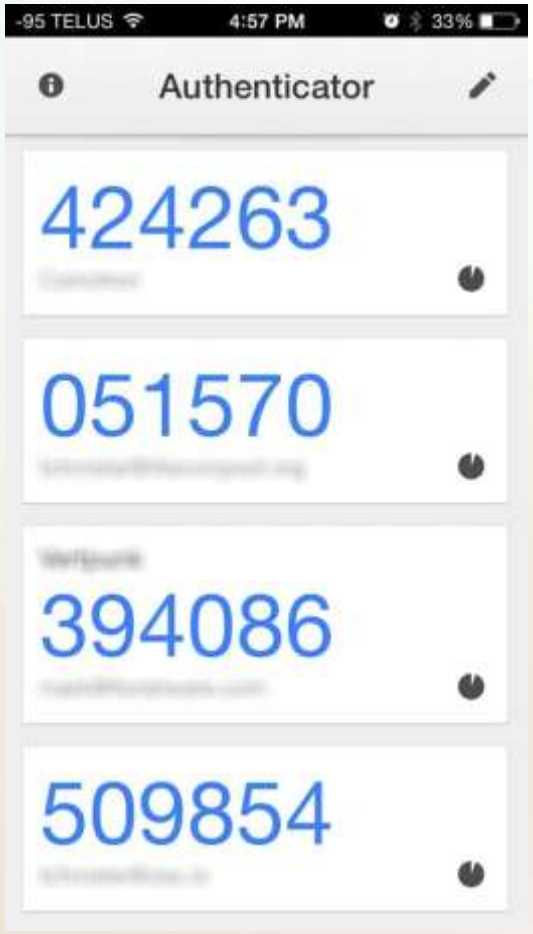
- Senhas são fáceis de quebrar.
- Senhas são fáceis de se obter.
- Confiar em que?
  - TWO FACTOR AUTHENTICATION !

Two Factor Authentication

- Autenticação de 2 diferentes componentes:
  - Algo que você sabe: SUA SENHA
  +
  - Algo que você **não** sabe: TOKEN

- Token:

Two Factor Authentication



Solução Oracle de 2FA

- Usando Oracle SSO com External Authentication

+

1. 2FA Authentication

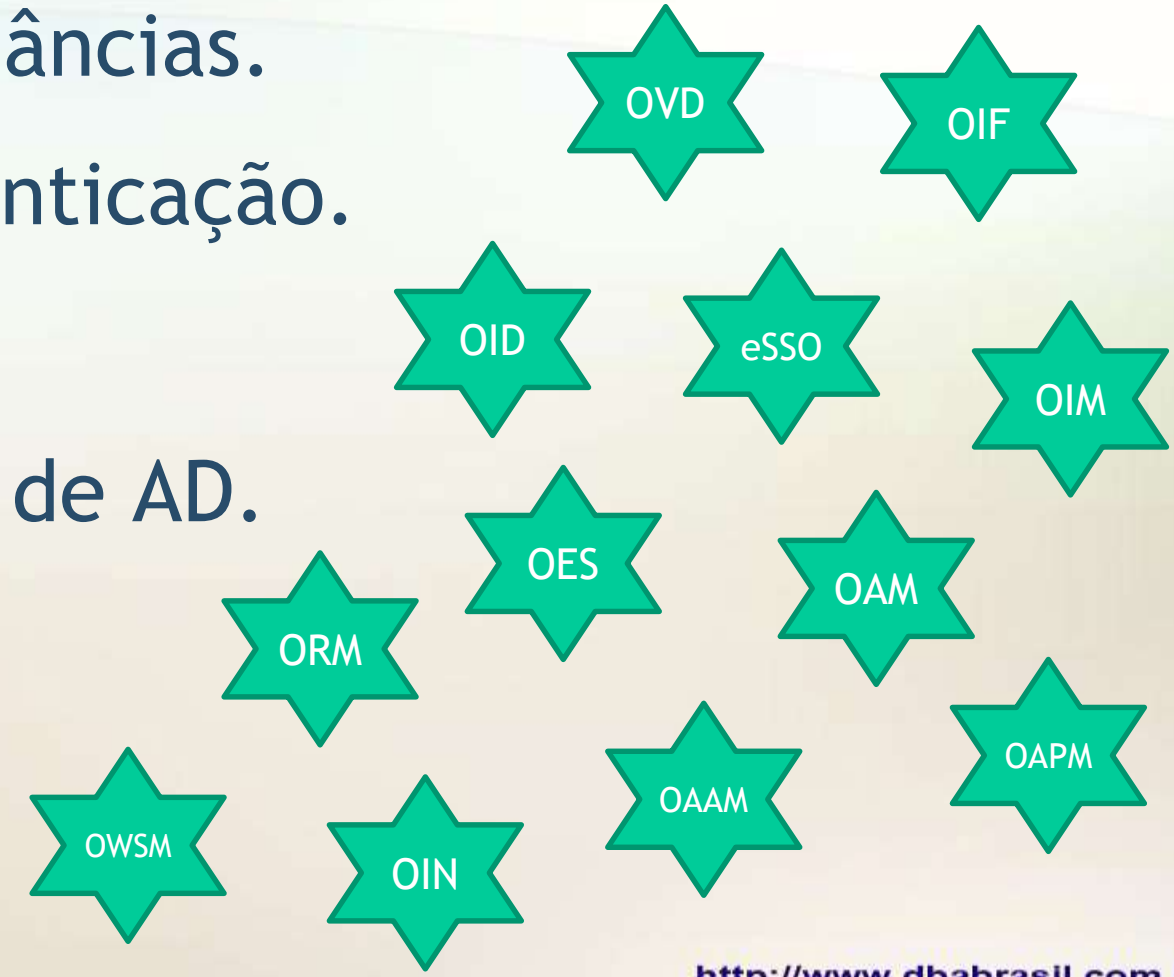
2. SSO cookie

SSO Server

3. Access without credentials

Solução Oracle de 2FA

- Mais servidores, mais redundâncias.
- Mudança no formato de autenticação.
- Licenciamentos = $$$
- Necessidade de implantação de AD.
- Alta complexidade.



Como fugir de tudo isso?

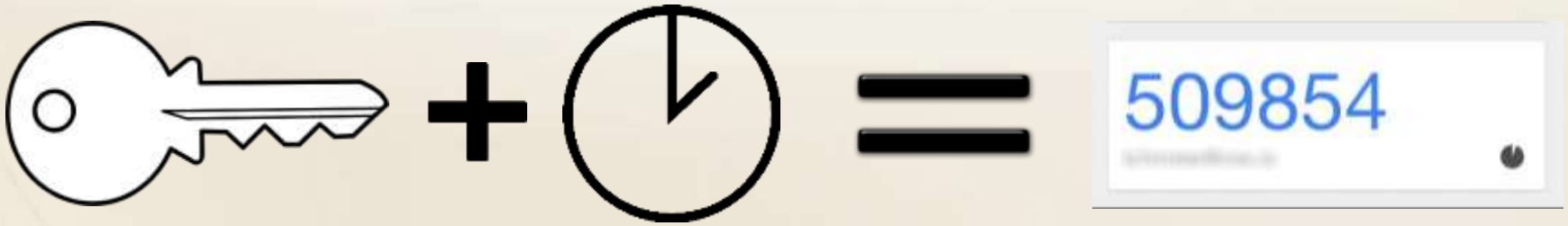
OraTOtP

https://github.com/dbarj/OraTOtP

TOTP

- **TOTP - Time-based One-time Password Algorithm**
  - **Chave secreta compartilhada**
  - **Contador ativado pelo tempo (normalmente 30 segundos)**

***



RFC 6238

Desafio

- Interceptar o algorítmo de autenticação do Oracle DB.
- Como o código é fechado, tive que contornar.

Solução

1. Autenticação com senha

2. Usuário conectado

mas sem qualquer privilégio ativo

3. Digitar o Token do 2FA

4. Permissões liberadas

Requisitos

- Testado em todas versões de Oracle Database (SE e EE) de **10gR2 até 12c.**
- Schema habilitado pelo 2FA não deve ser usado por aplicações ou batch jobs.
- **Não** precisa estar conectado na internet.
- Horário do smartphone e servidor alinhados.

Requisitos

Local Time: 3:30 PM

Local Time: 8:30 AM

Instalando

```
[oracle@mydbserver ~]$ sqlplus /nolog

SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 18 13:54:08 2016

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

SQL> @INSTALL
Schema Name for 2-Factor [TOTP]: TOTP
String to connect as SYS [/ as sysdba]: / as sysdba
Connected.
DB Vault Users script skipped - Database Vault not enabled.
Connected.
User created.
Connected.
User privs granted.
Connected.
Objects created.
Policies created.
Connected.
DB Vault Realms script skipped - Database Vault not enabled.
=> SCRIPT EXECUTED SUCCESSFULLY! <=
```

1º Criar uma role protegida pelo 2FA

Ex 1:

```
SQL> CREATE ROLE RO_CREATE_OBJECTS IDENTIFIED USING TOTP.ENABLE_ROLE;

Role created.

SQL> GRANT CREATE TABLE, CREATE VIEW, CREATE PROCEDURE, CREATE
SEQUENCE, CREATE TRIGGER to RO_CREATE_OBJECTS;

Grant succeeded.
```

1º Criar uma role protegida pelo 2FA

Ex 2:

```
SQL> CREATE ROLE DBA_2FA IDENTIFIED USING TOTP.ENABLE_ROLE;

Role created.

SQL> GRANT DBA to DBA_2FA;

Grant succeeded.
```

1º Criar uma role protegida pelo 2FA

Ex 3:

```
SQL> ALTER ROLE RESOURCE IDENTIFIED USING TOTP.ENABLE_ROLE;

Role altered.
```

** NÃO RECOMENDADO

2º Configurando usuário para utilizar o 2FA

Ex:

```
SQL> CREATE USER teste IDENTIFIED BY oracle;

User created.

SQL> GRANT CREATE SESSION TO teste;

Grant succeeded.
```

2º Configurando usuário para utilizar o 2FA

Ex:

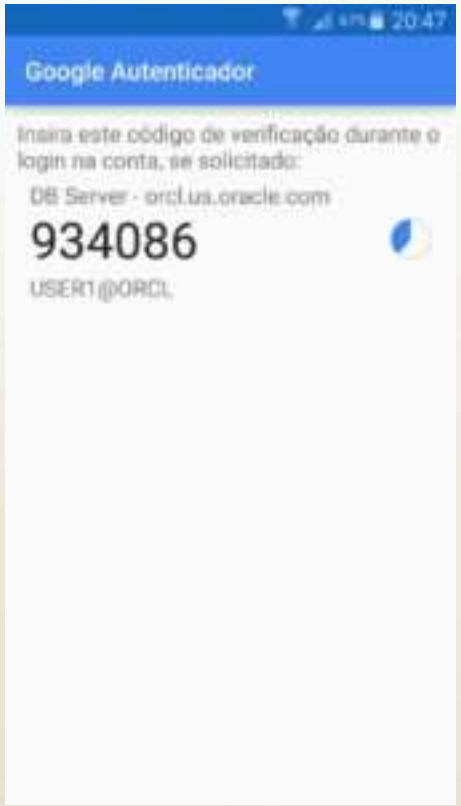
```
SQL> conn teste/oracle
Connected.

SQL> exec twofactor.setup;
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=%6F%74%70
%61%75%74%68%3A%2F%2F%74%6F%74%70%2F%54%45%53%54%45%40%50%44%42%30
%31%3F%73%65%63%72%65%74%3D%53%57%4E%4D%4D%4F%44%4A%54%44%32%33%5
7%57%33%5A%26%69%73%73%75%65%72%3D%44%42%20%53%65%72%76%65%72%20%2
D%20%70%64%62%30%31

PL/SQL procedure successfully completed.
```

2º Configurando usuário para utilizar o 2FA

Ex:

2º Configurando usuário para utilizar o 2FA

Ex:



2º Configurando usuário para utilizar o 2FA

Ex:

```
SQL> exec twofactor.validate(205962);

PL/SQL procedure successfully completed.
```

3º Habilitando a Role

Ex:

```
SQL> conn / as sysdba
Connected.
SQL> grant DBA_2FA to teste;

Grant succeeded.
```

3º Habilitando a Role

Ex:

```
SQL> conn teste/oracle
Connected.
SQL> set role DBA_2FA;
set role DBA_2FA
*
ERROR at line 1:
ORA-01924: role 'DBA_2FA' not granted or does not exist

SQL> select * from session_roles;

no rows selected
```

3º Habilitando a Role

Ex:

```
SQL> conn teste/oracle
Connected.
SQL> exec twofactor.authenticate(335712);

PL/SQL procedure successfully completed.

SQL> exec enable_role('DBA_2FA');

PL/SQL procedure successfully completed.
```

3º Habilitando a Role

Ex:

```
SQL> select * from session_roles;

ROLE
----------------------
DBA_2FA
……

25 rows selected.
```

Perguntas

- Eu preciso autenticar e habilitar a role manualmente toda vez que eu faço um login?

R: Sim.

3º Adicionando origem confiável

Ex:

```
SQL> exec twofactor.remember(583916);

PL/SQL procedure successfully completed.

SQL> conn teste/oracle
Connected.
SQL> select * from session_roles;

ROLE
----------------------
DBA_2FA
……

25 rows selected.
```

3º Removendo origem confiável

Ex:

```
SQL> exec twofactor.forget;

PL/SQL procedure successfully completed.

SQL> conn teste/oracle
Connected.
SQL> select * from session_roles;

no rows selected
```

LIVE DEMO

Funcionalidades

- “Remember Me”
- Reconfiguração ao trocar de telefone ou app.
- O “shared secret” é guardado criptografado no BD.
- Proteção contra brute-force attacks.

Brute Force

```
begin
 for i in (select lpad(rownum,6,'0') code from dual connect by level <= 999999)
 loop
  begin
   twofactor.authenticate(i.code);
   exit;
  exception when others then null;
  end;
 end loop;
end;
/
```

Modos de Proteção

- Com DB Vault
  - Apenas OraTOtP Admin tem acesso as tabelas de controle.
  - Possível exigir 2FA com segurança no acesso de todos os usuários, inclusive DBA's.
- Sem DB Vault
  - DBA's tem acesso as tabelas de controle.
  - Possível exigir 2FA com segurança no acesso de todos os usuários, exceto os DBA's.

CONCLUSÃO

Conclusão

1. Não confie em senhas.
2. Não confie em outros sites.
3. Não confie no que você acha que é seguro.

Principais aplicativos

- Google Authenticator
  - Android

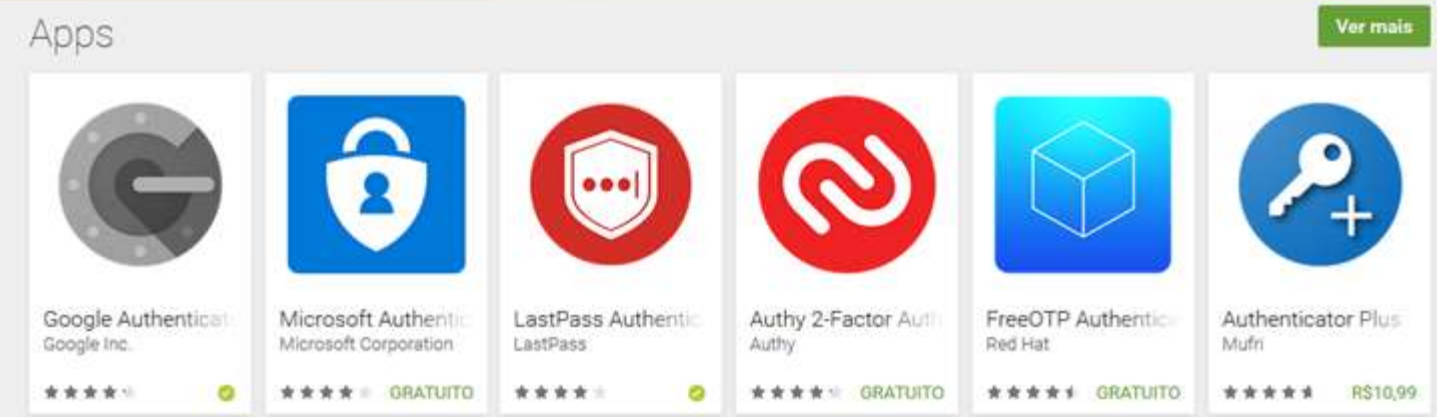
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

  - iOS

https://itunes.apple.com/br/app/google-authenticator/id388497605

  - Windows Phone

https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj

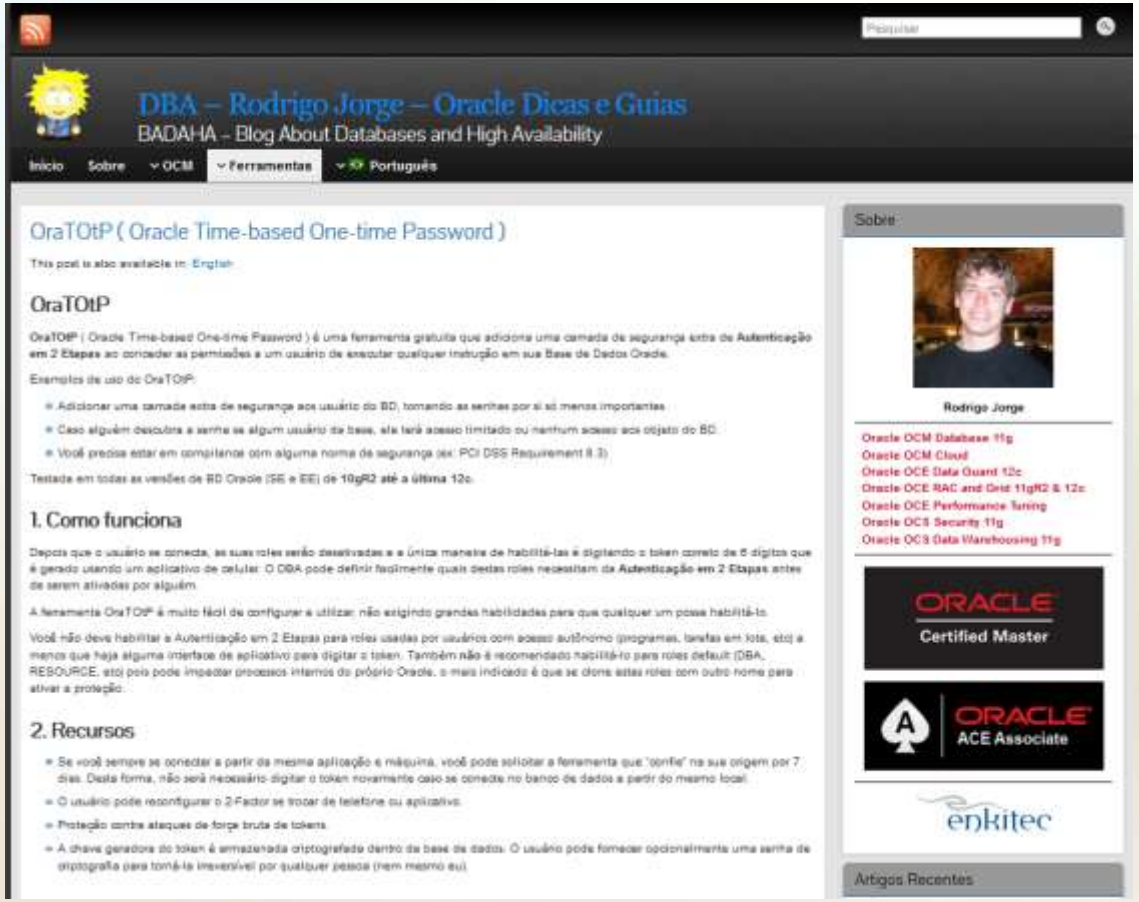


Mais informações

- OraTOtP
  - https://github.com/dbarj/OraTOtP
  - https://github.com/dbarj/OraTOtP/archive/master.zip
- Manual e tutorial
  - http://www.dbarj.com.br/oratotp-oracle-time-based-one-time-password/
- Essa apresentação
  - www.dbarj.com.br ou www.dbabr.com.br

Outras Informações de Segurança

www.dbarj.com.br



Referências

- Pete Finnigan:
  - PeteFinningan.com
- David Litchfield
  - www.davidlitchfield.com
- Alexander Kornbrust
  - www.red-database-security.com

Nossos Patrocinadores

DELL EMC

TmaxSoft Brasil

STROHL Brasil

Timbira
A empresa brasileira de PostgreSQL

GREEN tecnologia

DBA4All
We care about your data

DB Academy

ORAMASTER

PERGUNTAS ?

OBRIGADO