

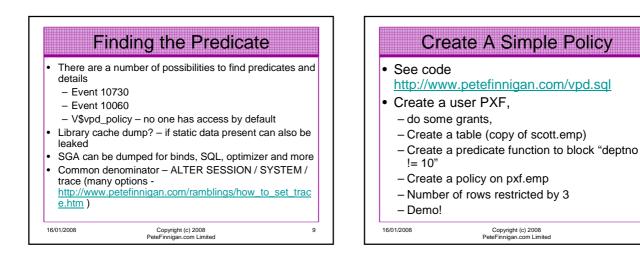
Securing VPD

- Leaking predicates
- Leaking policies
- RBAC on VPD structure / configuration
- Bypassing VPD by means of exception
- SQL Injection issues
- Direct data access

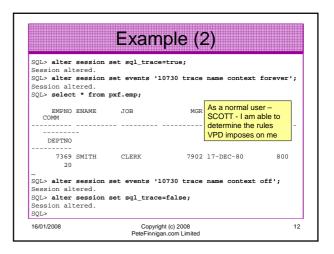
Copyright (c) 2008 PeteFinnigan.com Limited

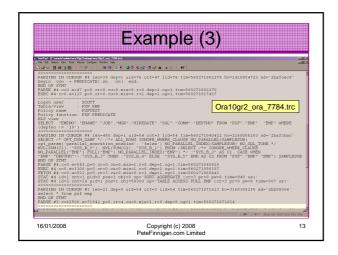
8

10



	Example
who_has_priv: R	Release 1.0.3.0.0 - Production on Wed Jan 16 19:13:16 2008
Copyright (c) 2	2004 PeteFinnigan.com Limited. All rights reserved.
PRIVILEGE TO CH OUTPUT METHOD S	IECK [SELECT ANY TABLE]: ALTER SESSION Screen/File [S]: S
 Privilege => AL	JTER SESSION has been granted to =>
Role =>	> DBA (ADM = YES) which is granted to =>
	User => SYS (ADM = YES)
	User => SYSMAN (ADM = NO)
	User => SYSTEM (ADM = YES)
	User => TESTUSER (ADM = NO)
	SYS (ADM = NO)
	IX (ADM = NO)
	SH (ADM = NO) RECOVERY CATALOG OWNER (ADM = NO) which is granted to =>
KOIE =>	User => SYS (ADM = YES)
	BI (ADM = NO)
	CTXSYS (ADM = NO)
	OLAP_USER (ADM = NO) which is granted to =>
KOIE ->	User => SYS (ADM = YES)
Theorem and	<pre>> SCOTT (ADM = NO)</pre>
	HR (ADM = NO)
	DMSYS (ADM = NO)
User =>	
	XDB (ADM = NO)

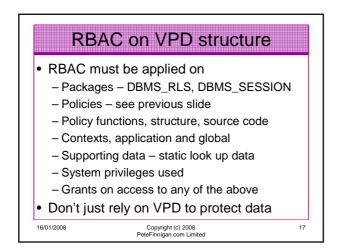


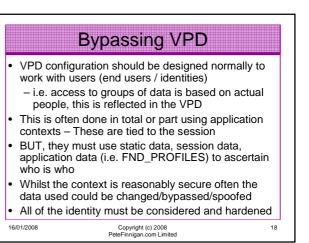




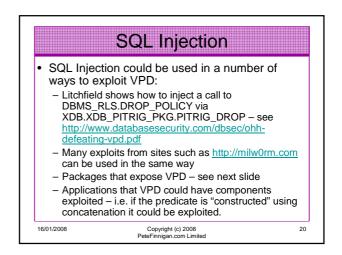
	Example	9
19:30:16 2008	elease 1.0.3.0.0 - Prod 4 PeteFinnigan.com Limi	uction on Wed Jan 16 ted. All rights reserved.
OWNER OF THE OBJ OUTPUT METHOD Sc FILE NAME FOR OU	reen/File PUT [priv. [DIRECTORY or file (/t JSERS	SER]: SYS [S]: S lst]:
 Object type is = Privileg	what po	s by default anyone can see licies exist that affect them
16/01/2008	Copyright (c) 2008 PeteFinnigan.com Limit	ed 1

	Example(2)	
	<pre>owner,object_name,policy_name, pf_owner,function ies;</pre>	
OBJECT_OWNER	OBJECT_NAME	
POLICY_NAME	PF_OWNER	
PF_OWNER	FUNCTION	
SCOTT PXFPOL SYS	EMP SYS HACK	
PXF PXFTEST PXF 2 rows selected		ne , I can also ne policies
16/01/2008	Copyright (c) 2008 PeteFinnigan.com Limited	16

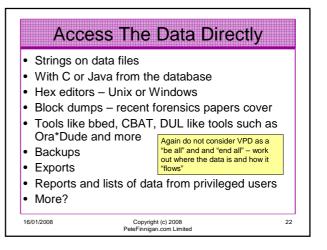




	Exempt Access Policy	
who_has_pri 2008	v: Release 1.0.3.0.0 - Production on Wed Jan 16 16	:26:56
	c) 2004 PeteFinnigan.com Limited. All rights reser	ved.
OUTPUT METH FILE NAME F		OLICY
	<pre>> EXEMPT ACCESS POLICY has been granted to => r => X (ADM = NO)</pre>	
PL/SQL proc	edure successfully completed.	
For updates	please visit http://www.petefinnigan.com/tools.ht	m
SQL>	http://www.petefinnigan.com/who_has_priv.sql	
16/01/2008	Copyright (c) 2008	19



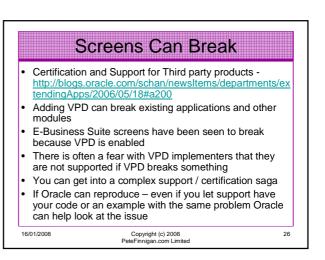
2 from	dba dependencies	
3 where	e referenced_name	"DBMS_RLS';
OWNER	NAME	TYPE
PUBLIC	DBMS RLS	SYNONYM
SYS	DBMS RLS	PACKAGE BODY
SYS	LTUTIL	PACKAGE BODY
SYS	LTADM	PACKAGE BODY
XDB	DBMS_XDBZ0	PACKAGE BODY
XDB	DBMS_XDBZ0	PACKAGE BODY
SQL> seled	t grantee,table_	name from dba_tab_privs
2 where	e table_name in ('LTUTIL','LTADM','DBMS_XDBZ0');
		TABLE NAME
GRANTEE		IADLE_NAME
GRANTEE		TABLE_NAME
		_
WMSYS	DATABASE	LTADM

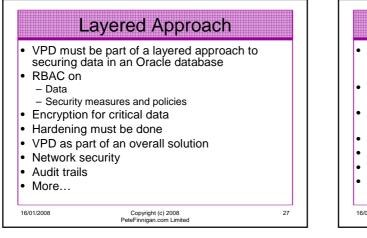


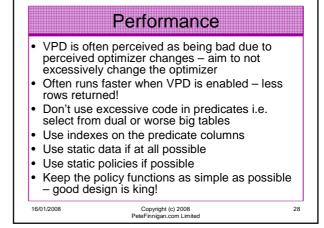
SQL> select distinct dbms_rowid_rowid_block_number(rowid) blk, dbms_rowid_rowid_relative_fno(rowid) fno from paf.emp;				
BLK	FNO			
420	4			
1 row selected.				
SQL> select file 2 where file	_name from dba_data_files id=4;			
FILE_NAME				
C:\ORACLE\ORADA1	A\ORA10GR2\USERS01.DBF			
1 row selected.				
16/01/2008	Copyright (c) 2008 PeteFinnigan.com Limited	23		

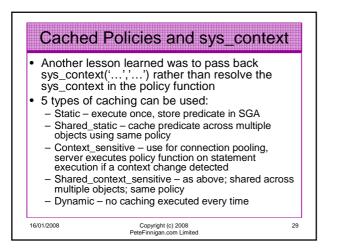
		Examp	le (2	2)	
System alto SQL> connec Connected.	ered. ct sys/ch	ump datafile 4 1 ange_on_install pxf.emp where d o	as sysdł	Da	
EMPNO COMM	ENAME	JOB	MGR	HIREDATE	SAL
DEPTNO					
7782 10	CLARK	MANAGER	7839	09-JUN-81	2450
7839 10	KING	PRESIDENT		17-NOV-81	5000
7934 10	MILLER	CLERK	7782	23-JAN-82	1300
16/01/2008		Copyright (PeteFinnigan.c			24

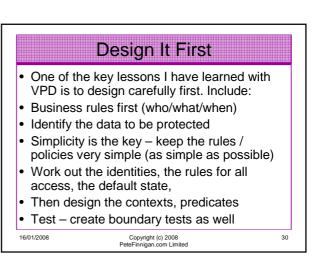
Tenfed (Eventive/monol/product/seal/seal/seal/seal/seal/seal/seal/seal	2494D06 [P#.MIL] ;720753 [LER.CLERK., NS.w.]
8229DE0 01011701 0EC20201 0BC102FF 0: 8229DF0 040350C2 44524F46 414E4107 54 8229E00 434CC203 0CE57707 01010103 FF	308002C [] 153594C [.P.:FORD.ANALYST] 17FC202 [.LC.W]
8229E10 2C15C102 C2020800 414A0550 05 8229E20 52454C43 4DC2034B E5770763 01 8229E30 0AC20301 C102F733 08002C1F 4E 8229E40 41444105 4305534D 4E52454C 55	101030C [CLERKMc.w] 04FC203 [3
8229E50 05BB7707 01010117 FF0CC202 20 8229E60 C2030800 54062D4F 454E5255 41 8229E70 4D53454C C2034E41 7707634D 01	215C102 [.w] 1530852 [O.TURNER.SA] 0689985 [LESMAN. N.C.w]
8229EA0 B57707FF 0101110B 33C20201 0E	4E4544 [(.KING.PRESIDENT]
8229EC0 53594C41 4CC20354 BB770743 01 8229ED0 1FC20201 15C102FF 0308002C 05 8229EE0 52414C43 414D074B 4547414E 43	011304 [ALVSTLC.W] 5534EC2 [
8229EF0 B5770728 01010906 19C20301 C 8229F00 08003COB 634DC203 414C4205 40 8229F10 47414E41 C2035245 7707284F 01 8229F20 C2030101 02F531D 002CFC1 41	207454B [Mc.BLAKE.M] 10105B5 [ANAGERO(.w]
8229F30 414D0637 4E495452 4C415308 41 8229F40 4DC2034E B5770763 01011C09 0E 8229F50 0FC20233 2C1FC102 C2030800 44	14D5345 [7.MARTIN.SALESMA] X20301 [N.Mc.w] 05434G [3LC.J]
8229F60 53454E4F 4E414D07 52454741 23 8229F70 04B57707 01010102 4C1EC203 15 8229F80 0308002C 04164CC2 44524157 40	C102FF [.w] 2415308 [L. WARD.SAL]
8229F90 414D5345 4DC2034E B5770763 01	











ultiple Policy Issu	es		Conclusions	
n example from the trenches single table is needed as part of e redicate lot of other tables access this table repredicate generation lot of policies created, identities de ontexts created roblem: The single table cannot be ith VPD as it breaks all other polici PD needs, hardening, RBAC etc as complete" solution	e as part of esigned, protected es	 What car How VPI How the outside c How to c 	D can be bypassed and why data could still be accessed	
Copyright (c) 2008 PeteFinnigan.com Limited	31	16/01/2008	Copyright (c) 2008 PeteFinnigan.com Limited	3

