



## Oracle Security Tool Categories (3)

- Audit Trail software
  - many e.g. SQL Guard from Guardium
  - No free solutions in same space
  - Many built in solutions
- Database IDS / IPS
  - Many e.g. Hedgehog from Sentrigo
  - No other free solutions in same space
- In-line Patching – BlueLane patchpoint and virtualshield
- Encryption
  - small number of players including Application Security Inc
  - Some free software but no GUI solutions

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

7

## Free And Commercial

Area	Free	Commercial
Discovery	X	X
Testing	X	X
Scanner	X	X
Fuzzing	X	
Hardening		
Audit Trail		X
IDS / IPS / Patching	1	X
Encryption		X

This is not scientific but a simple look at the spread of tools between commercial and free - a trend is visible

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

8

## Does Oracle Provide Anything?

- None of the tool types listed above are supplied by Oracle as complete tools BUT
  - Oracle supplies a default password tool
  - 11gR1 has a default password check built in
  - There are no Oracle scanners (at least not public)
  - Oracle does provide various audit scripts (quite old) on Metalink
  - Oracle includes many built in audit solutions and audit vault. There are some issues – e.g. user\$
  - Oracle also provides many encryption solutions

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

9

## Support And Maintenance

- All Commercial products can include – support and upgrade
- Free tools – depends on developers and
  - Is this an issue?
  - We have source code in lots of cases
  - A lot of tools can be extended
  - A problem of research? – stop/start
  - A problem of wasted (duplicate) efforts
  - Commercial / free requires careful considerations

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

10

## Supporting Role Tools

- Whilst we are talking about Oracle security tools we should not ignore the platform and network
  - This should include database discovery using network security tools such as nmap, amap, nessus
  - This should also include platform checks. The CIS benchmark tools are very good as a start in this area

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

11

## Security Issues With Tools

- Protect against tools run on your own databases
- Just as you can use for audit / testing etc these tools can also be used against you
- Beware some \*rare\* tools have virus/worm code included to allow the author to take over your machine
- One legitimate tool is recognised as a virus / worm
- Choose extendable tools with source, then from trusted sources.
- Protection methods? – many and varied

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

12

## Some Demonstrations

- Sidguess – Patrik Karlsson
- User Enumeration – OAK – David Litchfield
- Default passwords – 11g plus Pete Finnigan list
- Password cracker – woraauthbf
- SYSDBA brute force – Paul Wright
- Listener checks - Integrity
- Scanners
  - Scuba - imperva
  - CIS benchmark
  - OScanner
- Privilege checks – PeteFinnigan.com scripts

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

13

## SIDGuesser

```
C:\WINDOWS\system32\cmd.exe
C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 127.0.0.1 -p 1521 -d sidlist.txt
SIDGuesser v1.0.5 by patrik@cqure.net
Starting Dictionary Attack <<space> for stats, Q for quit) ...
C:\pete_finnigan_com_ltd\presentations\tools>sidguesser -i 127.0.0.1 -p 1522 -d sidlist.txt
SIDGuesser v1.0.5 by patrik@cqure.net
Starting Dictionary Attack <<space> for stats, Q for quit) ...
FOUND SID: ORA10GR2
C:\pete_finnigan_com_ltd\presentations\tools>
From http://www.cqure.net/tools/SIDGuesser_win32_1_0_5.zip
```

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

14

## User Enumeration

```
C:\WINDOWS\system32\cmd.exe
C:\pete_finnigan_com_ltd\presentations\tools>oak
C:\pete_finnigan_com_ltd\presentations\tools>oak ora-userenum 127.0.0.1 1522 ora
10gr2 users.txt
SYS exists
SYSTEM exists
OUTLN exists
XDB exists
DBMSMP exists
SCOTT exists
UMMSYS exists
CTASYS exists
HDSYS exists
QS exists
SH exists
DBSNMP exists
C:\pete_finnigan_com_ltd\presentations\tools>oak
From
http://www.databasesecurity.com/dbsec/OAK.zip
```

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

15

## Default Password Check

```
SQL> select * from dba_users_with_defpwd;

USERNAME
-----
DIP
MDSYS
WK_TEST
CTXSYS
OUTLN
EXFSYS
MDDATA
ORDPLUGINS
ORDSYS
XDB
ST_INFORMTN_SCHEMA
WMSYS

12 rows selected.

Alternative is to use woraauthbf with a default file
See
http://www.petefinnigan.com/default/default_password_list.htm
11g Uses the old 10gr2 hash
No passwords available
690 records in the table
Remember if found you would still need to resolve the case sensitive password in 11g if its not all one case
Can implement your own version of the same
```

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

16

## Password Cracker (1)

Run in SQL\*Plus [http://soonerorlater.hu/download/woraauthbf\\_src\\_0.2.zip](http://soonerorlater.hu/download/woraauthbf_src_0.2.zip)  
[http://soonerorlater.hu/download/woraauthbf\\_0.2.zip](http://soonerorlater.hu/download/woraauthbf_0.2.zip)

```
Select u.name||':'||u.password
||':'||substr(u.spare4,3,63)
||':'||d.name||':'
||sys_context('USERENV','SERVER_HOST')||':'
from sys.user$ u, sys.V_$DATABASE d where u.type#=1;
```

Create a text file with the results – mine is called 11g\_test.txt

```
SCOTT:9B5981663723A979:71C46D7FD2AB8A607A93489E899C0
8FFDA75B147030761978E640EF57C35:ORA11G:vostok:
```

Then run the cracker

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

17

## Password Cracker (2)

```
C:\WINDOWS\system32\cmd.exe
C:\lazzlo\release_code_cracker\woraauthbf_0.2\woraauthbf -p 11g_test2.txt -t 11g
10g -m 5 -c alphanum
The number of processors: 2
Number of puds to check: 60466176
Number of puds to check by thread: 30233088
Password file: 11g_test2.txt, charset: alphanum, maximum length: 5, type: 11g10g
Start: 0 End: 30233088
Password found: SCOTT:Cra3k:ORA11G:vostok
Elapsed time: 11s
Checked passwords: 1070392
Password / Second: 100000
C:\lazzlo\release_code_cracker\woraauthbf_0.2>
```

As you can see the password is found – running at over 1million hashes per second  
Woraauthbf can also be used to crack from authentication sessions  
Woraauthbf can be used in dictionary or brute force mode

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

18

## SYSDBA Brute Force

```
C:\tools\brute_wright>orabrute 127.0.0.1 152
2 ora10gr2 100
Orabrute v 1.2 by Paul M. Wright and David J. Morgan:
orabrute <hostip> <port> <sid> <millitimetwait>sqlplus.exe -S -L
"SYS/AASH@127.0.0.1:1522/ora10gr2" as sysdba @selectpassword.sql
```

NAME	PASSWORD
----	-----
SYS	B024681DBF11A33E
PUBLIC	
CONNECT	
RESOURCE	
DBA	
SYSTEM	D4DF7931AB130E37
SELECT_CATALOG_ROLE	
EXECUTE_CATALOG_ROLE	
DELETE_CATALOG_ROLE	
EXP_FULL_DATABASE	
IMP_FULL_DATABASE	

<http://www.ngssoftware.com/research/papers/oraclepasswords.zip>

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

19

## Listener Check

Description	Result	Notes	More Information
Listener Version	Pass	TNS Listener Version = 10.2.0.1.0	
Listener Password	Pass	Oracle 10g, password not required (TNS-01189)	<a href="#">Info</a>
Admin Restrictions	Pass	Oracle 10g, no ADMIN_RESTRICTIONS (TNS-01189)	<a href="#">Info</a>
Listener Logging	Pass	Oracle 10g, unable to check logging (TNS-01189)	<a href="#">Info</a>
Local OS Auth (10g)	Pass	LOCAL_OS_AUTHENTICATION=ON (TNS-01189)	<a href="#">Info</a>

Works with 10gR2  
Can enumerate SIDS using TNS commands  
From: <http://www.integrity.com/downloads/lsnrcheck.exe>

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

20

## Sample Audit Checks Using SCUBA

[http://www.imperva.com/application\\_defense\\_center/scuba/](http://www.imperva.com/application_defense_center/scuba/)

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

21

## Sample Audit Checks Using SCUBA

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

22

## Sample Audit Checks Using SCUBA

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

23

## CIS Benchmark

Level	Host Files	Database Access	Policy and Procedure	Total
Level 1	3.97	4.91	0.81	3.20
Level 2	2.14	1.00	2.56	1.91
Appendix A				0.00

100% complete (269/269)

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

24



## PeteFinnigan.com Limited

```
create or replace function get_startip_john
return int_4 as
  v_ip varchar(15) := null;
begin
  v_ip := get_startip_john;
  return v_ip;
end;
/
```

Oracle Security Expertise

### Contact - Pete Finnigan

PeteFinnigan.com Limited  
9 Beech Grove, Acomb  
York, YO26 5LD

Phone: +44 (0) 1904 791188  
Mobile: +44 (0) 7742 114223  
Email: [pete@petefinnigan.com](mailto:pete@petefinnigan.com)

20/06/2008

Copyright (c) 2008  
PeteFinnigan.com Limited

31