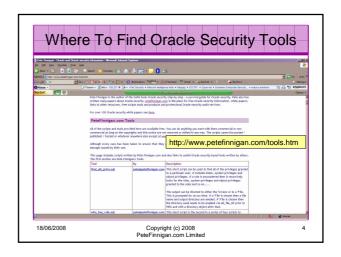




# Agenda Where to find Oracle security tools Look at the types of tools (categorize) Consider free and commercial tools Protecting against Oracle Security tools A quick look at what Oracle provides Demo and summarise some of the key tools that can be used Copyright (c) 2008 ReteFirnigan.com Limited 3



# Discovery tools User enumeration – OAK toolkit Sid guessing – RDS, Cqure, THC Connect brute force – bfora.pl SYSDBA brute force – Paul Wright Listener enumerators – nmap, metacortex, tnsprobe, WinSID Testing tools Password crackers – orabf, woraauthbf, checkpwd Listener enumeration – integrigy, DokFleed, tnscmd Default passwords – PeteFinnigan.com Inguma – Joxean Koret Backtrack CD - 18/06/2008 - Copyright (c) 2008 PeteFinnigan.com Limited

# Oracle Security Tool Categories (2) Scanners Listener scanners – Integrigy, DokFleed CIS Benchmark – old but the best free scanner Scuba - Imperva RoraScanner – Rory McCune Audit scripts (who\_has\_priv) – Pete Finnigan Commercial – AppDetective, Squirrel, AuditPro Fuzzers – Joxean Koret script + inguma Hardening scripts (similar to SQLsecurity.com for SQL Server) – none that I know of | 18/06/2008 | Copyright (c) 2008 | PeterFinnigan.com Limited | Copyright (c) 2008 | PeterFinnigan

### 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

18/06/2008

Copyright (c) 2008 PeteFinnigan.com Limited

Commercial Discovery Testing Х Scanner Х Х Х Fuzzing Hardening Audit Trail X IDS / IPS / Patching Х Encryption This is not scientific but a simple look at the spread of tools between commercial and free - a trend is visible Copyright (c) 2008 PeteFinnigan.com Limited

Free And Commercial

## 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

18/06/2008

Copyright (c) 2008 PeteFinnigan.com Limited \_\_\_

### 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

18/06/2008

Copyright (c) 2008 PeteFinnigan.com Limited

# 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

18/06/2008

Copyright (c) 2008

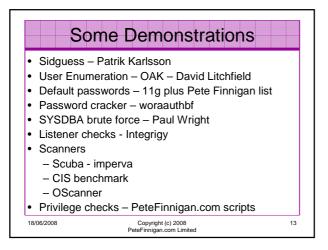
## Security Issues With Tools

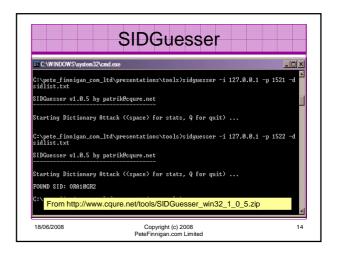
- Protect against tools run on your own databases
- Just as you can use for audit / testing etc these tools can also be used against you
- Beware some \*rare\* tools have virus/worm code included to allow the author to take over your machine
- One legitimate tool is recognised as a virus / worm
- Choose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

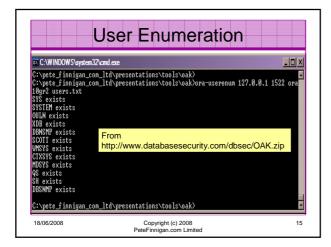
18/06/2008

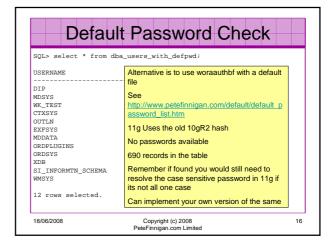
Copyright (c) 2008 PeteFinnigan.com Limited 12

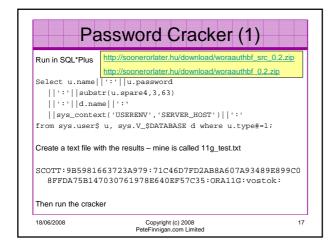
10

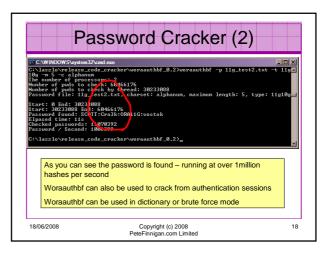


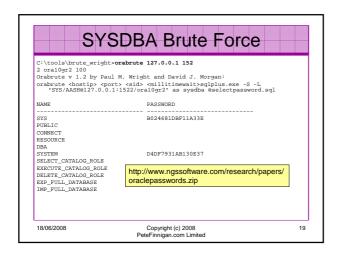


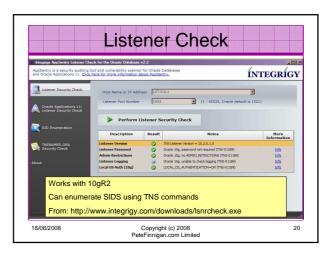


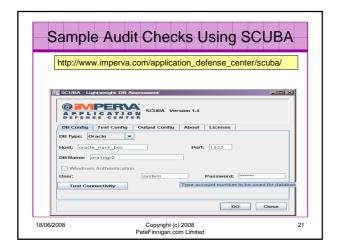


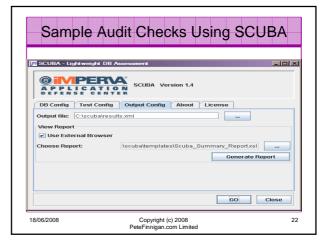


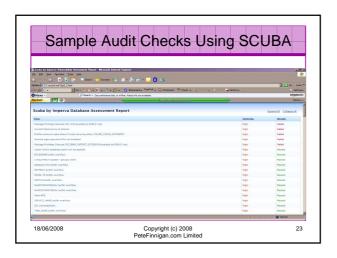


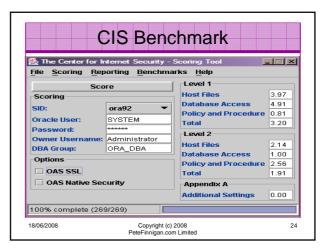


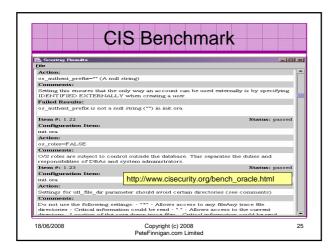


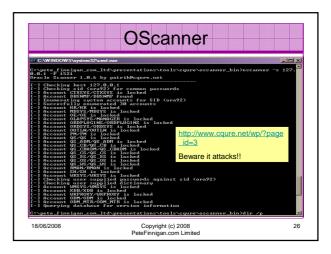


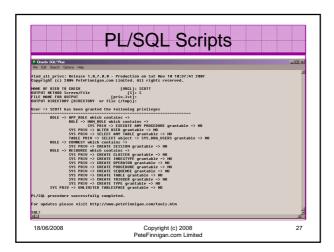


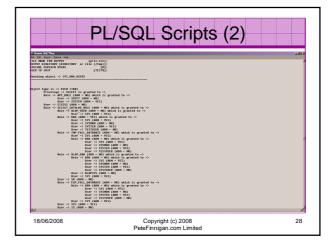












# Conclusions Looked at where to find Oracle security tools Look at the types of tools and categorized them Considered free and commercial tools Looked at protecting against Oracle Security tools A quick look at what Oracle provides Demonstrated some of the key tools that can be used The free tools tend to occupy the enumerate, test and scan areas



## PeteFinnigan.com Limited

r utl\_file.file type:=null; ile varchar2(105);='log start'; 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

18/06/2008

Copyright (c) 2008 PeteFinnigan.com Limited