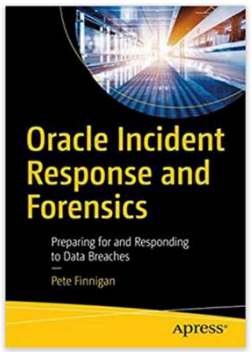

# Top 10 Things to Security Review in an Oracle Database


# Legal Notice

## Top 10 Things to Security Review in an Oracle Database

Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

PFCL
PETEFINNIGAN.COM LIMITED




# Pete Finnigan – Background, Who Am I?

- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Author of the Oracle Security step-by-step guide and “Oracle Expert Practices”, “Oracle Incident Response and Forensics” books
- Oracle ACE for security
- Member of the OakTable, SYM 42
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - http://www.petefinnigan.com for links


# Agenda

- Background
- Checklists
- Data Security
- The top 10

PFCL
PETEFINNIGAN.COM LIMITED

# Section

## Security Background


# Introduction

- I help customers secure their data
- When I explain all elements that could be done customers are overwhelmed (at first)
- Some customers use check lists like CIS
  - OK as a start
  - Not OK as a long term as these do not secure data
- Some ask me whats the top 3, 5, 10 things we can do
  - They look for an easy way out
- There is not a simple check list that secures all and any data

PFCL
PETEFINNIGAN.COM LIMITED

# CIS Benchmarks

- CIS Offer benchmarks for Oracle; You can download these for free from https://benchmarks.cisecurity.org/downloads/latest/
- There are a number of versions
  - V 1.2 – Oracle 8i
  - V 2.01 – 9i and 10g
  - V 11 – 11gR2 v1.0 – much different and similar to earlier
  - **V11gR2 1.0 and 2.2 (2012 and May 2016)**
  - **V12cr2 v3 (versions 12.1 and older 12.2 not available)**
  - **18c and 19c V1**
  - ASM, CDB mooted but never seen
- The earlier ones include policy, least privilege, questions, OS and networking, data security
- **Only the RED BOLD ones are now available – 5 in total**


There are lots of issues with CIS in my opinion, too many to cover here

# CIS 11g and 12c/18c/19c Benchmarks Compared

- Both 11g versions are different (previously similar but one is close to 8i and other close to 12)
- 12.1 version is essentially the same as 11g in terms of checks
- 12.2 version 18 parameters vs 19, O7_DICTIONARY_ACCESSIBLITY is missing - still in 18c so …
- 12.2 – three new packages added, DBMS_XMLSTORE, DBMS_XMLSAVE **(both deprecated in 18c)** and DBMS_REDACT – wow!
- 12.2 Standard audit reduced to 18 from 22 settings, ALTER|DROP USER|PROFILE gone, GRANT DIRECTORY gone DIRECTORY added
- 12.2 – 27 unified audit added – more than std? PROCEDURE as example
- Main issues
  - No 12c parameters, no PDB/CDB, No application containers, no sharding, no lockdown profiles, COMMON or LOCAL,
  - No 18c/19c i.e. CMU users, password less schemas…
  - Limited listener – i.e. no valid node
  - No OS – why?
  - No password strength checks
  - No data security / context based security
  - Why add DBMS_REDACT; includes SELECT ANY TABLE but not INSERT, UPDATE, READ, CREATE ANY PROCEDURE|TRIGGER|VIEW|INDEX…
  - No 12c privileges, no quotas, no resource,
  - No context based security..

Biggest issue is lack of real updates for more than 10 years and lack of consensus – too few people involved


# What is Data Security?

- Data security is the understanding of and protection of the actual data in your database
- This means you must know what that data is and who accesses it and how and when and why
- You do not need to secure all data - just important data
- You must understand all access paths to the data
- You must understand if multiple copies exist and where (not just in the database)
- Data security is not just about GRANT SELECT ON SCOTT.CREDIT_CARDS TO FRED


# What Is Oracle Security?

- It is not Oracle's Security
- It is **our** security of **our** data


# Threats - Platform And Data Security

- There are two key threats
- **Data Theft:** The attackers goal is to steal your data, PII, Cards, Health, Business confidential or more
- **Platform Access:** The attacker is not interested in your data or simply does not see the value in it. Instead he sees your Oracle database as an easy target to attack and from there to access what he really wants – other services, websites or more
- **Therefore we must protect data as a key task but we must not neglect the Oracle platform as a potential target and lock it down as well**


# What is Platform Security?

- Platform security is patching of the operating system and the Oracle database software
- Platform security is hardening of the operating system and network
- Platform security is hardening of the database software, its network and OS interfaces
- Platform security is about stopping an attacker from using the Oracle database as a “jump off” point to attack the rest of your infrastructure
- In general by default the Oracle platform is not secured by Oracle for you – you have to do it!

PFCL
PETEFINNIGAN.COM LIMITED

## Vulnerabilities, Threats, Risks and Counter Measures

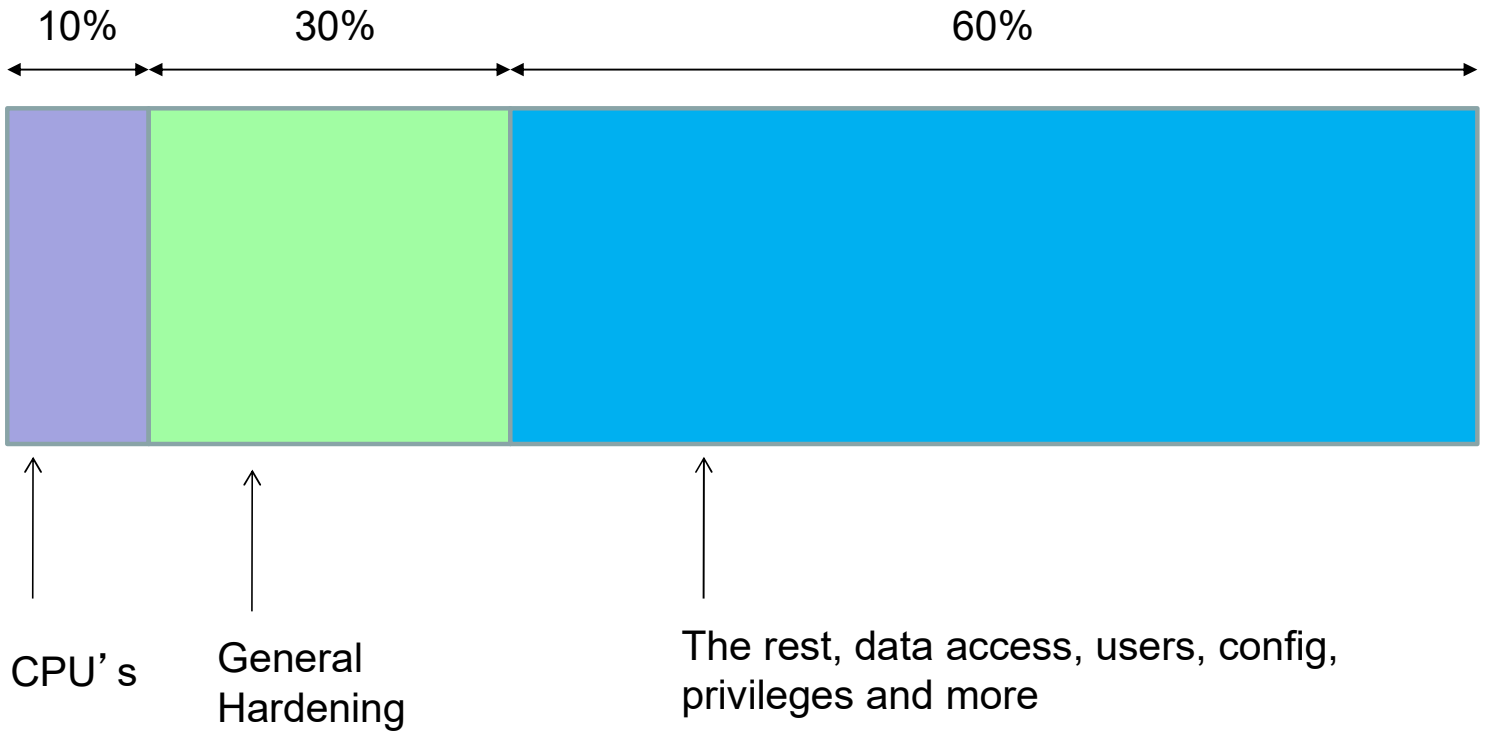
- The security building blocks are:
  - Vulnerabilities – settings, bad design, permissions and much more
  - Threats – Something someone can do to attack you
  - Risk – Usually considered as part of a Risk Assessment
    - risk = threat + vulnerability
  - Counter measures – the things you can do to mitigate risk


# Actors

- To assess security of data in an Oracle database we must know who the “actors” are – **not Johnny Depp** but
  - Real people who access the database –
    - job roles that are allowed to connect to the database and why
    - Individuals who are allowed to connect and why – when its not a clear job role
  - Processes –
    - Feeds and extracts
  - Business tasks –
    - Reporting
- Unless we know about who connects and why we cannot secure the Oracle database

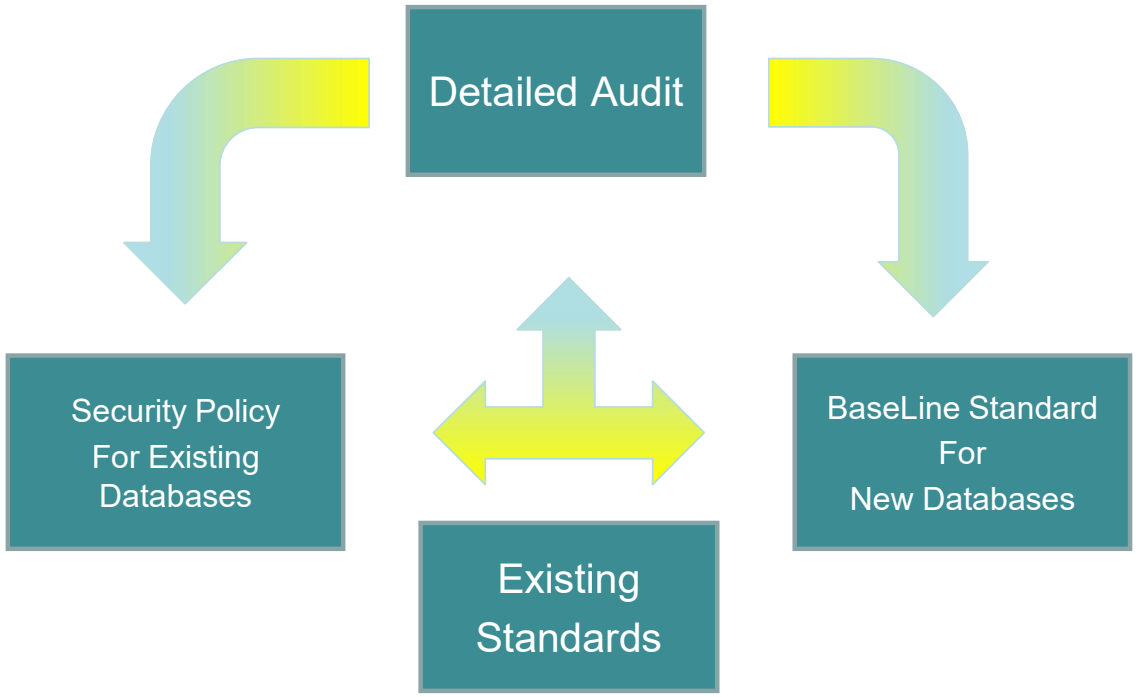
PFCL
PETEFINNIGAN.COM LIMITED

# Compartmentalise Data Security?



PFCL
PETEFINNIGAN.COM LIMITED

# What Is Involved In Securing A Database?



PFCL
PETEFINNIGAN.COM LIMITED

# Section

## Conclusions of Hacking Analysis


# The Hacks We Did In The Demo

| | | | | | Problems | | | |
|---|---|---|---|---|---|---|---|---|
| Hack | Access | authenticated | Injection | Audited | code | data sep | permissions | Conn Obj Own |
| Turn off audit on CREDIT_CARD | web | none | DDL -> PL/SQL -> SQL(PHP) | No | yes | yes | no | yes |
| Turn off audit on ORABLOG_CRYPTO | web | none | DDL -> PL/SQL -> SQL(PHP) | No | yes | yes | no | yes |
| Turn off audit on WP_USERS | web | none | DDL -> PL/SQL -> SQL(PHP) | No | yes | no | no | yes |
| View credit card details | web | none | SQL(PHP) | No | yes | yes | no | yes |
| reset logon Password | web | none | DDL -> PL/SQL -> SQL(PHP) | No | yes | yes | no | yes |
| Access DBA_USERS | client | POWER | SQL (ORA) -> SQL in PL/SQL | No | yes | yes | yes | no |
| Access ALL_USERS | client | POWER | SQL (ORA) -> SQL in PL/SQL | No | yes | yes | yes | no |
| Access credit cards from SQL*Plus | client | POWER | SQL (ORA) No Injection | No | yes | yes | yes | no |
| Access credit cards from SQL*Plus | client | DBA | SQL (ORA) No Injection | Yes | yes | no | yes | no |
| Read data with no Read permissions | client | POWER | SQL (ORA) No Injection | No | no | no | yes | no |
| Escalate to SYSDBA via Apex | client | POWER | SQL (ORA) Replacement | No | no | no | yes | no |
| View meta data and encryption key | web | none | SQL(PHP) | No | yes | yes | no | yes |
| escalate to SYSDBA via ALTER USER | client | POWER | SQL (ORA) -> SQL in PL/SQL | No | yes | no | yes | no |
| access data via SGA | client | POWER | SQL (ORA) No Injection | No | no | no | yes | no |
| access data via ALTER SYSTEM | client | POWER | SQL (ORA) No Injection | No | no | no | yes | no |

- We did a limited number of hacks this time that illustrate a number of issues:
  - Is the hacker authenticated?
  - Was the action audited?
  - Was the issue caused by code problems?
  - Was the issue caused by the connection user as the schema?
  - Was the issue caused by database permissions?
  - Was the issue caused by data separation?


# Fix or Not

- The main kick backs and issues I get from customers are:
  - We can't change anything because it will break the application
  - We can't change anything because the vendor would need to approve it
  - We can't change any settings because there is no change window
  - We can't add security because there is only budget for performance and functional issues to be fixed


# Cost Options

- Cost options and Enterprise features such as
  - DV,VPD, TSDP, REDACT, Masking, TDE, OLS, RAS and more …
- These are great applications
  - Yes, they are applications, security applications
  - Most are built in at the C level to some extent
  - Most are declarative
  - Most can be simulated to some extent
  - They all require to be secured
- Focus


# Cloud or Not Cloud

- Cloud might have better hardware and network security BUT
  - Depends on the cloud model (DB, Bare Metal,…) risk of producer / consumer responsibilities – access to backups and data
  - If you have a badly designed application (legacy) and database data model just moving to the cloud does not fix the problems and make it secure
  - The design of your application and data model is yours
  - The security of data and the database is the same whether the database is hosted on your own site or in a cloud

PFCL
PETEFINNIGAN.COM LIMITED

# Section

## The Top Ten


# Bad News

- **There is no simple top ten list of specific items like a check list**
- There is no golden bullet simple set of commands that works on every Oracle database
- i.e.

```
SQL> alter database make_secure=true;
```

- It would be great if that were true BUT its not. As we will see each “idea” can involve lots of decisions and component parts


Each item is not simply set this parameter or permission. There are often layers of things that can and should be done

# 1 – Stop People Connecting to the Database

- I mean people directly connecting to the database who should not
  - Hacking a password, finding a password, stealing a password, open terminal, …
  - Refine this to be the other way around “only allow people to connect when they absolutely need to and never any other time”
- How? – many possible parts
  - Strong passwords OR CMU or Kerberos or EUS or ??
  - Enforce password with password verify
  - Strong profile design; force password changes
  - Stop the DBA from removing any of the protections – DDL triggers
  - Logon triggers to prevent connections when not authorized
  - Can use DV of course as well

PFCL
PETEFINNIGAN.COM LIMITED

Demo: orablog.sql

# 2 – Least Privileges

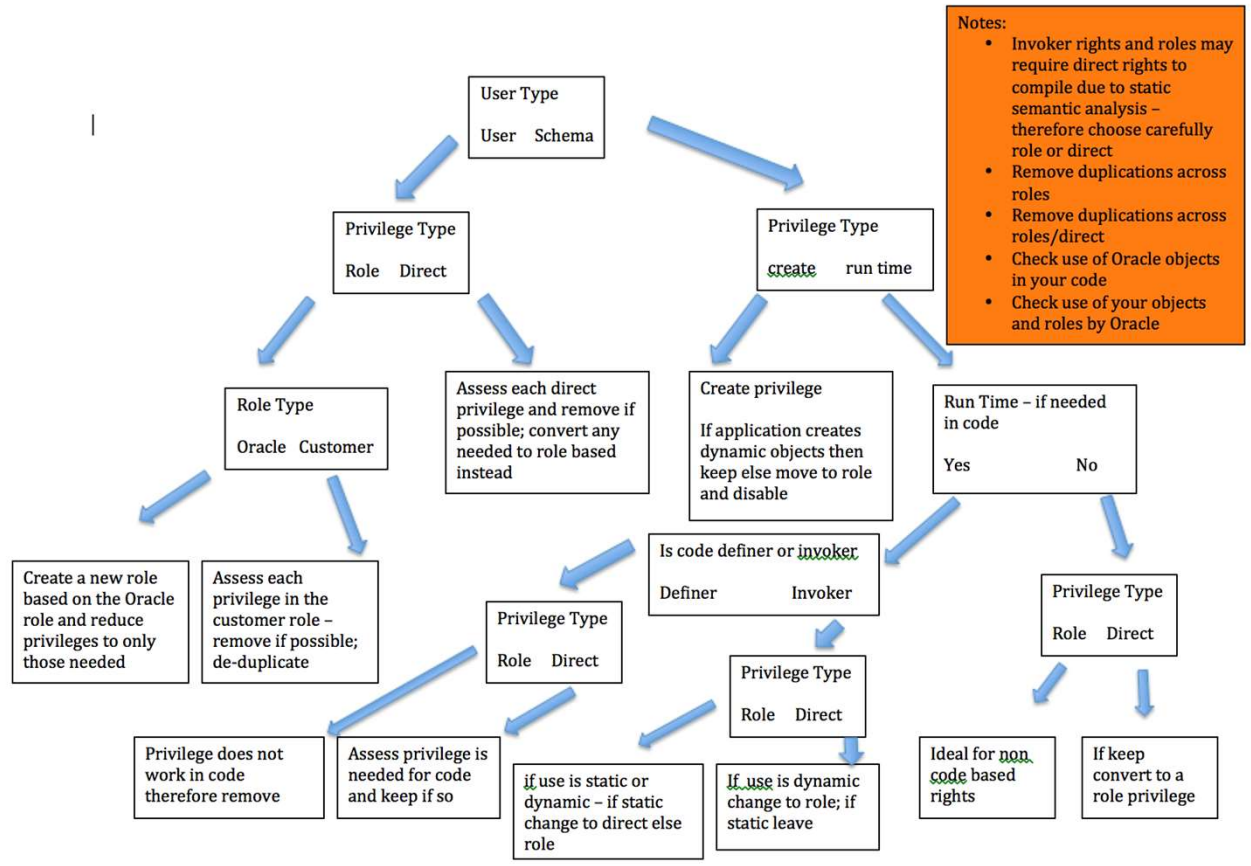
- First concentrate on the use of Oracle designed roles
  - These are inappropriate for Orablog and BOF
- Create new ORABLOG roles with the same rights
- Transfer ORABLOG to these new roles
- Remove privileges to suit the current ORABLOG design and use from these new roles
- Analyse how ORABLOG works and remove these roles completely
- Also analyse compile time rights and show how they could be removed
- Also note the risk in doing this
- Review all direct rights and remove where not justified for Orablog and BOF


# Are System Privileges Needed?

- Most system privileges are not needed by “actors” or schemas
  - In general schemas need system privileges only to create their objects and maintain them and not for run time
- Privilege management can provide additional layers of security whilst working towards least privileges
- Some privileges are confusing
  - Does CREATE TABLE allow you to only create a table?
    - It can be used to write and read files!

PFCL
PETEFINNIGAN.COM LIMITED

# Privilege Reduction Flow Chart




# Least Privilege – SoD and CoI

- The most common issue I see is a lack of least privilege
- (SoD) Separation of Duties:
  - This is the idea that more than one person **is required** to complete a task
  - In business the sharing of a task between two or more people is known as a **security control**.
- (CoI) Conflict of Interest:
  - A situation where a person or party has the potential to undermine their impartiality
- These issues can exist in the database layer, application layer or in the database code / data where the database provides controls for the application layer
- SoD Example: A user has the ability to create a loan and also approve it
- CoI Example: A batch user has application rights and also developer rights

PFCL
PETEFINNIGAN.COM LIMITED

# 3 – Remove Unnecessary Users

Highlight those accounts to remove or keep by color coding

- Green – KEEP – schemas, known end users, processes
- Red – REMOVE – developers, DBA like accounts, not used, no privileges…

| Typ | Rol | RB | RR | RS | RO | Sys | Ob | Tab | PL | User | Statu |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2 | B | 2 | 9 | 0 | 4 | 8 | 32 | 64 | ORABLOG | OPEN |
| | 0 | | | | | 1 | 5 | 0 | 0 | ERIC | OPEN |
| | 1 | N | 1 | 0 | 2 | 1 | 2 | 0 | 0 | EMIL | OPEN |
| | 0 | | | | | 1 | 0 | 0 | 0 | ZULIA | OPEN |
| | 0 | | | | | 2 | 1 | 0 | 0 | PETE | OPEN |
| | 0 | | | | | 2 | 2 | 0 | 0 | FRED | OPEN |
| | 0 | | | | | 1 | 2 | 0 | 0 | BILL | OPEN |
| | 1 | N | 1 | 0 | 2 | 1 | 2 | 0 | 0 | JIM | OPEN |
| | 3 | B | 7 | 89 | 2588 | 1 | 1 | 1 | 0 | IMPORTER | OPEN |
| | 1 | N | 1 | 0 | 18 | 1 | 10 | 0 | 0 | USER01 | OPEN |
| | 1 | N | 1 | 0 | 18 | 1 | 10 | 0 | 0 | USER02 | OPEN |
| | 1 | N | 1 | 0 | 18 | 1 | 10 | 0 | 0 | USER03 | OPEN |
| | 1 | N | 1 | 0 | 18 | 1 | 11 | 0 | 0 | USER04 | OPEN |
| | 2 | N | 3 | 0 | 36 | 1 | 1 | 0 | 0 | USER05 | OPEN |
| | 2 | N | 3 | 0 | 36 | 1 | 1 | 0 | 0 | USER06 | OPEN |
| | 2 | N | 3 | 0 | 36 | 1 | 2 | 0 | 0 | USER07 | OPEN |
| | 3 | B | 11 | 91 | 5223 | 1 | 0 | 0 | 0 | BACK01 | OPEN |
| | 3 | B | 5 | 0 | 2498 | 1 | 0 | 0 | 0 | BATCH01 | OPEN |
| | 3 | B | 5 | 0 | 2498 | 1 | 0 | 0 | 0 | FEED01 | OPEN |
| | 4 | B | 8 | 9 | 2498 | 2 | 0 | 0 | 0 | DEV01 | OPEN |
| | 4 | B | 8 | 9 | 2498 | 2 | 0 | 0 | 0 | DEV02 | OPEN |
| | 4 | B | 8 | 9 | 2498 | 3 | 1 | 0 | 0 | DEV03 | OPEN |
| | 1 | N | 1 | 0 | 18 | 1 | 8 | 0 | 0 | RISK01 | OPEN |
| | 1 | N | 1 | 13 | 0 | 0 | 0 | 0 | 2 | SHAREDDBA | OPEN |
| | 1 | N | 1 | 0 | 5 | 1 | 0 | 0 | 0 | DBACLIENT1 | OPEN |
| | 1 | N | 1 | 0 | 5 | 1 | 0 | 0 | 0 | DBACLIENT2 | OPEN |
| | 2 | B | 2 | 9 | 0 | 1 | 0 | 0 | 0 | DEV2 | OPEN |
| | 3 | B | 44 | 452 | 15962 | 1 | 0 | 0 | 0 | ORABLOGDBA | OPEN |
| | 2 | B | 87 | 895 | 31924 | 2 | 0 | 0 | 0 | AA | OPEN |
| | 1 | B | 42 | 443 | 15962 | 2 | 0 | 0 | 0 | BB | OPEN |
| | 0 | | | | | 9 | 6 | 0 | 8 | ILO | OPEN |
| | 1 | B | 1 | 1 | 0 | 5 | 7 | 3 | 18 | LOG4 | OPEN |
| | 2 | B | 2 | 9 | 0 | 2 | 0 | 0 | 14 | JSON | OPEN |
| | 0 | | | | | 3 | 1 | 0 | 0 | ORASCAN | OPEN |


# 4 – Remove all Defaults

- Remove all default users
- Remove grants to Oracle roles
- Remove default passwords
- Don’t use Oracle profiles
- **Remove all things related to ensure least rights**
- **Design your own “things”**


# 5 – DBA and SYSDBA

- DBA staff should not use SYS, SYSTEM or oracle or SYSDBA
- DBA staff should not grant DBA, SYSDBA or ALL PRIVILEGES
- SYS and SYSTEM and oracle should be locked
- Prevent SYSDBA access other than by password
- Implement Breakglass to allow access to SYSDBA when needed
- Create a dba role that does not allow access to all data and does not allow escalation back to SYSDBA or similar
- Create individual DBA accounts for each real person DBA – possibly use a shared DBA account and proxy access or CMU
- Audit all access via a shared account or all dba access


# 6 – Code Security

- If we
  - stop people connecting
  - Limit defaults
  - Limit privileges if someone does get in
  - Limit super user access
- Then the only way to exploit is through code vulnerabilities
- Review all code (PL/SQL, php, ADF, Java or …)
- Ensure that the code is not vulnerable to SQL Injection or resource abuse and much more


# 7 – Network Security

- Use network firewalls to limit direct connections to the database
- Use the simple valid node checking to limit IP or ranges
- Use logon triggers to limit users/programs
- Use encrypted listeners

PFCL
PETEFINNIGAN.COM LIMITED

# 8 – Apply Security Patches

- Apply security patches within the quarter or
- Apply the last patch at the start of the current quarter
  - This ensures that the patch is fully tested by others and reliable

PFCL
PETEFINNIGAN.COM LIMITED

# 9 – Implement Audit Trails

- Design and implement comprehensive audit trails
- For the database engine
- For the applications
- Attempt to detect attacks in semi or real time
- Create alerts
- Create regular reporting

PFCL
PETEFINNIGAN.COM LIMITED

# 10 – Do Basic Hardening

- We must still do basic hardening
- If we cover all of the other areas then CIS is a reasonable starting point
- BUT, do not just do CIS items only
- Change parameters
- Remove permissions and privileges


# Conclusions

- Stop people connecting
- If people get in limit privileges available
- Remove as much stuff that we don't need
- Patch and harden
- Secure the applications code
- Secure the network
- Limit super users
- Design audit trails to monitor the database engine

PFCL
PETEFINNIGAN.COM LIMITED

# Questions

?

If Anyone has questions, please ask now or catch me during the event!!


# Top 10 Things to Security Review in an Oracle Database