Oracle Security for DBAs and Developers

Daniel A. Morgan
email: dmorgan@forsythe.com
mobile: +1 206-669-2949
skype: damorgan11g
twitter: @meta7solutions

May 18, 2017

Unsafe Harbor

- This room is an unsafe harbor
- You can rely on the information in this presentation to help you protect your data, your databases, your organization, and your career
- No one from Oracle has previewed this presentation
- No one from Oracle knows what I'm going to say
- No one from Oracle has supplied any of my materials
- Everything we will discuss is existing, proven, functionality

Introduction

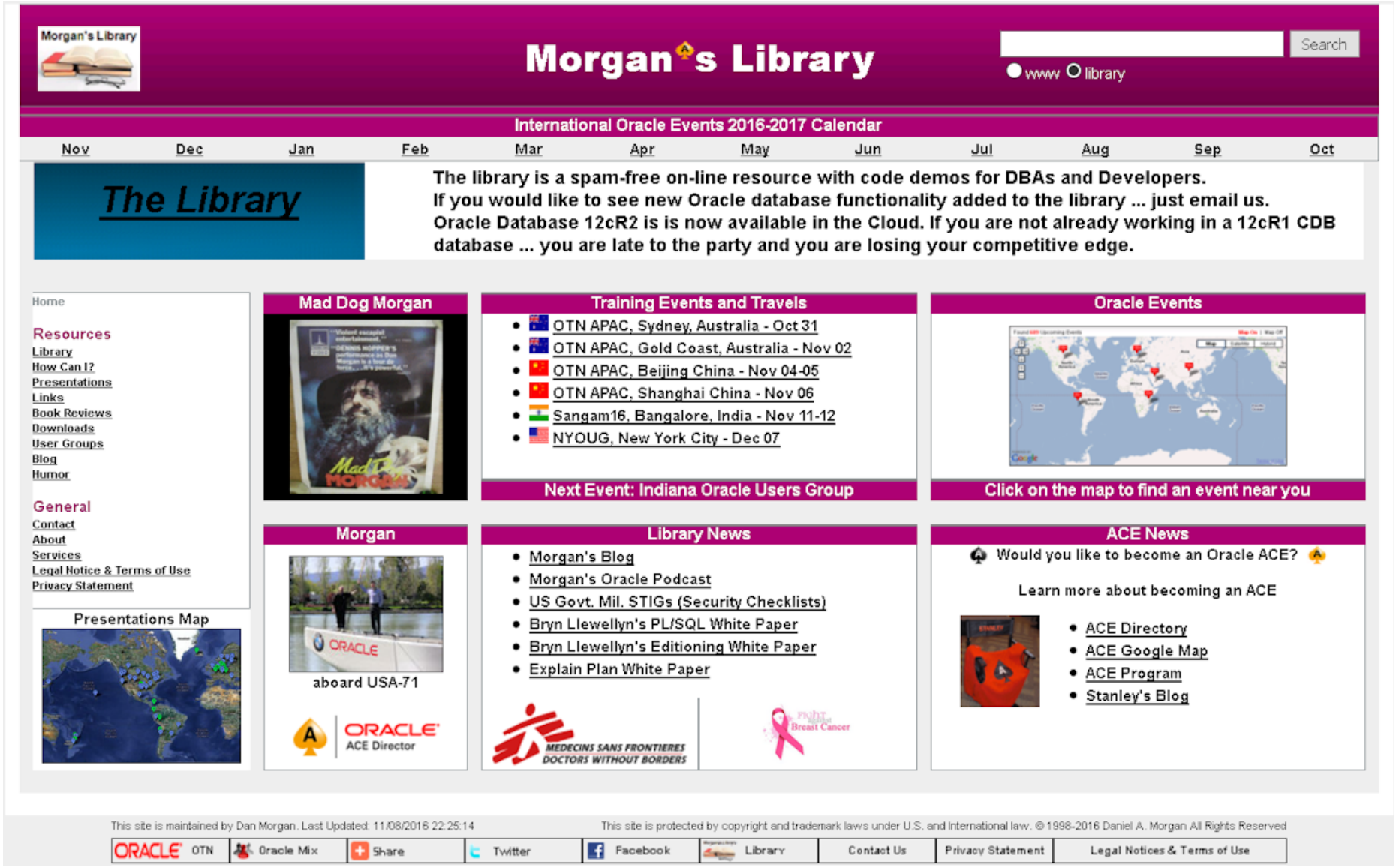
Daniel Morgan

- Oracle ACE Director
- Oracle Educator
  - Curriculum author and primary program instructor at University of Washington
  - Consultant: Harvard University
  - University Guest Lecturers
    - APAC: University of Canterbury (NZ)
    - EMEA: University of Oslo (Norway)
    - Latin America: Universidad Cenfotec, Universidad Latina de Panama, Technologico de Costa Rica
- IT Professional
  - First computer: IBM 360/40 in 1969: Fortran IV
  - Oracle Database since 1988-9
  - Beta Tester 10g, 11g, 12c, TimesTen, GoldenGate
  - The Morgan behind www.morganslibrary.org
  - Member Oracle Data Integration Solutions Partner Advisory Council
  - Co-Founder International GoldenGate Oracle Users Group
- Principal Adviser: Forsythe **Meta7**

System/370-145 system console

email: dmorgan@forsythe.com
Twitter: @damorgan12c

My Websites: Morgan's Library



www.morganslibrary.org`

Security Introduction

Why Am I Focusing On Oracle Database Security?

- Because what OEM's talk about products not security
- Because most organizations spend/waste their money on perimeter defense
- Because no one teaches operational security to Application Developers
- Because no one teaches operational security to System Admins
- Because no one teaches operational security to DBAs
- Because no one teaches operational security to IT Management
- Because what most organizations implement can be by-passed within minutes
- ... which is obvious given the number of systems broken into every day

Nothing To See Here ... Move Along ... Move Along

Breach exposes at least 58 million accounts, includes names, jobs, and more

With 2 months left, more than 2.2 billion records dumped so far in 2016.

DAN GOODIN - 10/12/2016, 2:29 PM

Ars Technica

Today's Rhetorical Question

- Would we want our surgeon to practice 1980s medicine?

- Then why are we "securing" our databases the way we did in the 80's?
- The threats have evolved but we have not

Content Density Warning

Take Notes ... Ask Questions

Presentation Caveats

- Security and Auditing are two entirely different things: Having one does not lessen the importance of having the other
- Auditing is critically important but essentially irrelevant to security

- Auditing
  - Auditing is the act of collecting and persisting metadata about activities: Who logged on, what did they do when they were logged on, when did they log off
  - Lots of organizations enable auditing ... but almost no one monitors the logs that are generated by audit activities
- Auditors
  - Auditors are people that, at least in theory, know enough about what your organization should be doing they can ascertain whether you are, indeed, actually doing it
  - Think about all of the internal and external audits your organization has passed over the years ... do you think that what got you past the audit made your organization secure?

Oracle Database Security

Database Risks

- Database related risks fall into three broad categories
  - Data Theft
  - Data Alteration
  - Transforming the database into an attack tool
- To accomplish the above activities requires gaining access and doing so generally falls into one of the following categories
  - Utilizing granted privileges or through privilege escalation
  - Access to Oracle built-in packages
  - SQL Injection attacks

A Dose Of DBA Reality (1:2)

```
SQL> select utl_inaddr.get_host_address('www.umn.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UMN.EDU')
------------------------------------------
134.84.119.107

SQL> select utl_inaddr.get_host_name('134.84.119.025') from dual;

UTL_INADDR.GET_HOST_NAME('134.84.119.025')
------------------------------------------
g-smtp-w.tc.umn.edu
```

- It takes precisely this much PL/SQL to compromise an internal network

```
DECLARE
 h_name  VARCHAR2(60);
 test_ip VARCHAR2(12) := '134.84.119.';
 suffixn NUMBER(3) := 0;
 suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

A Dose Of DBA Reality (2:2)

- The listing output

```
134.84.119.001 - x-134-84-119-1.tc.umn.edu
134.84.119.002 - x-134-84-119-2.tc.umn.edu
134.84.119.003 - x-134-84-119-3.tc.umn.edu
134.84.119.004 - x-134-84-119-4.tc.umn.edu
134.84.119.005 - lsv-dd.tc.umn.edu
134.84.119.006 - mta-w2.tc.umn.edu
134.84.119.007 - isrv-w.tc.umn.edu
134.84.119.010 - mta-a2.tc.umn.edu
134.84.119.011 - x-134-84-119-9.tc.umn.edu
134.84.119.012 - x-134-84-119-10.tc.umn.edu
134.84.119.013 - x-134-84-119-11.tc.umn.edu
134.84.119.014 - x-134-84-119-12.tc.umn.edu
134.84.119.015 - x-134-84-119-13.tc.umn.edu
134.84.119.016 - x-134-84-119-14.tc.umn.edu
134.84.119.017 - diamond.tc.umn.edu
134.84.119.020 - x-134-84-119-16.tc.umn.edu
134.84.119.021 - oamethyst.tc.umn.edu
134.84.119.022 - x-134-84-119-18.tc.umn.edu
134.84.119.023 - x-134-84-119-19.tc.umn.edu
134.84.119.024 - vs-w.tc.umn.edu
134.84.119.025 - g-smtp-w.tc.umn.edu
134.84.119.026 - mta-w1.tc.umn.edu
134.84.119.027 - x-134-84-119-23.tc.umn.edu
134.84.119.030 - x-134-84-119-24.tc.umn.edu
134.84.119.031 - x-134-84-119-25.tc.umn.edu
134.84.119.032 - x-134-84-119-26.tc.umn.edu
134.84.119.033 - x-134-84-119-27.tc.umn.edu
134.84.119.034 - x-134-84-119-28.tc.umn.edu
134.84.119.035 - mon-w.tc.umn.edu
134.84.119.036 - ldapauth-w.tc.umn.edu
134.84.119.037 - ldap-w.tc.umn.edu
134.84.119.040 - mta-w3.tc.umn.edu
134.84.119.041 - x-134-84-119-33.tc.umn.edu
134.84.119.042 - x-134-84-119-34.tc.umn.edu
134.84.119.043 - smtp-w2.tc.umn.edu
134.84.119.044 - relay-w2.tc.umn.edu
134.84.119.045 - x-134-84-119-37.tc.umn.edu
134.84.119.046 - x-134-84-119-38.tc.umn.edu
134.84.119.047 - x-134-84-119-39.tc.umn.edu
134.84.119.050 - x-134-84-119-40.tc.umn.edu
134.84.119.051 - x-134-84-119-41.tc.umn.edu
134.84.119.052 - x-134-84-119-42.tc.umn.edu
134.84.119.053 - x-134-84-119-43.tc.umn.edu
134.84.119.054 - x-134-84-119-44.tc.umn.edu
134.84.119.055 - lsv-w.tc.umn.edu
134.84.119.056 - x-134-84-119-46.tc.umn.edu
134.84.119.057 - lists.umn.edu
134.84.119.060 - x-134-84-119-48.tc.umn.edu
134.84.119.061 - plaza.tc.umn.edu
134.84.119.062 - x-134-84-119-50.tc.umn.edu
134.84.119.063 - x-134-84-119-51.tc.umn.edu
134.84.119.064 - x-134-84-119-52.tc.umn.edu
134.84.119.065 - x-134-84-119-53.tc.umn.edu
134.84.119.066 - x-134-84-119-54.tc.umn.edu
134.84.119.067 - x-134-84-119-55.tc.umn.edu
134.84.119.070 - x-134-84-119-56.tc.umn.edu
134.84.119.071 - x-134-84-119-57.tc.umn.edu
134.84.119.072 - x-134-84-119-58.tc.umn.edu
134.84.119.073 - x-134-84-119-59.tc.umn.edu
134.84.119.074 - isrv-d2.tc.umn.edu
134.84.119.075 - ldapauth-d2.tc.umn.edu.tc.umn.edu
134.84.119.076 - ldap-d2.tc.umn.edu.tc.umn.edu
134.84.119.077 - x-134-84-119-63.tc.umn.edu
134.84.119.100 - x-134-84-119-100.tc.umn.edu
134.84.119.101 - aquamarine.tc.umn.edu
134.84.119.102 - x-134-84-119-102.tc.umn.edu
134.84.119.103 - x-134-84-119-103.tc.umn.edu
134.84.119.104 - mon-m.tc.umn.edu
134.84.119.105 - mta-m2.tc.umn.edu
134.84.119.106 - x-134-84-119-106.tc.umn.edu
134.84.119.107 - isrv-m.tc.umn.edu
134.84.119.108 - mta-m4.tc.umn.edu
134.84.119.109 - x-134-84-119-109.tc.umn.edu
134.84.119.110 - x-134-84-119-110.tc.umn.edu
134.84.119.111 - x-134-84-119-111.tc.umn.edu
134.84.119.112 - x-134-84-119-112.tc.umn.edu
134.84.119.113 - x-134-84-119-113.tc.umn.edu
134.84.119.114 - oaqua.tc.umn.edu
134.84.119.115 - x-134-84-119-115.tc.umn.edu
134.84.119.116 - x-134-84-119-116.tc.umn.edu
134.84.119.117 - x-134-84-119-117.tc.umn.edu
134.84.119.118 - x-134-84-119-118.tc.umn.edu
134.84.119.119 - x-134-84-119-119.tc.umn.edu
134.84.119.120 - vs-m.tc.umn.edu
134.84.119.121 - g-smtp-m.tc.umn.edu
134.84.119.122 - mta-m1.tc.umn.edu
134.84.119.123 - x-134-84-119-123.tc.umn.edu
134.84.119.124 - x-134-84-119-124.tc.umn.edu
134.84.119.125 - x-134-84-119-125.tc.umn.edu
134.84.119.126 - g-smtp-m4.tc.umn.edu
134.84.119.127 - x-134-84-119-127.tc.umn.edu
134.84.119.128 - x-134-84-119-128.tc.umn.edu
134.84.119.129 - x-134-84-119-129.tc.umn.edu
134.84.119.130 - ldapauth-m.tc.umn.edu
134.84.119.131 - ldap-m.tc.umn.edu
134.84.119.132 - mta-m3.tc.umn.edu
134.84.119.133 - x-134-84-119-133.tc.umn.edu
134.84.119.134 - x-134-84-119-134.tc.umn.edu
134.84.119.135 - smtp-m2.tc.umn.edu
134.84.119.136 - relay-m2.tc.umn.edu
134.84.119.137 - x-134-84-119-137.tc.umn.edu
```

Oracle Database Security

The Concept

- To achieve a secure environment you must embrace the fact that the goal is not just to limit access: It is to secure data
- Securing the perimeter is a good first step
- Securing access is a step in the right direction but it does not secure data

If someone had unfettered access to your entire network for a year but couldn't get to your data ... there would be no risk!

- There is always someone inside the firewall, always someone with access, but there is a big difference between accessing one record ... and walking away with everything

- So let's take a quick look at the products and options Oracle makes available

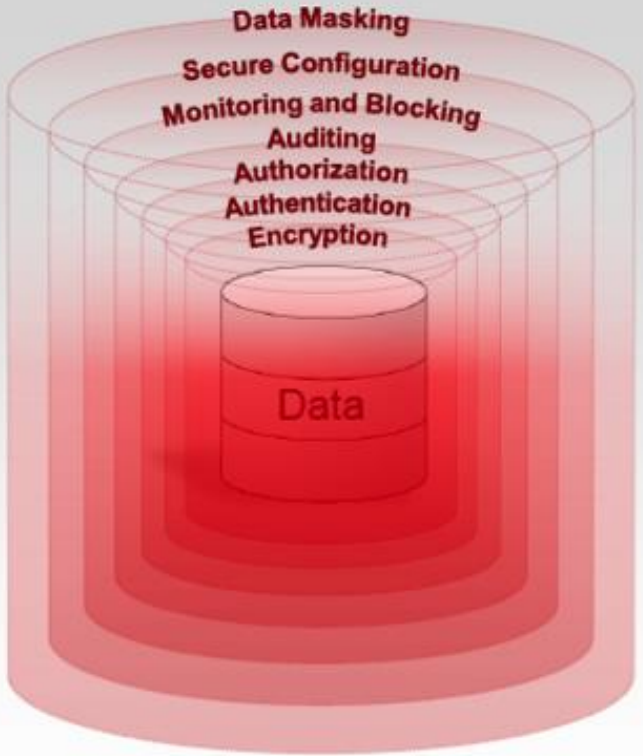
What The Leading Oracle Expert Says

Oracle's Larry Ellison decries poor state of security,

"We need much better security," Ellison said Tuesday in a speech at Oracle OpenWorld. "We need a next generation of security because we're not winning a lot of these cyberbattles. We haven't lost the war, but we're losing a lot of battles."

An Oracle Corporate View of Security

- Very valuable ... but insufficient



- Oracle Advanced Security
- Oracle Identity Management
- Oracle Database Vault
- Oracle Label Security
- Oracle Audit Vault
- Oracle Total Recall
- Oracle Database Firewall
- Oracle Configuration Management
- Oracle Data Masking

Comprehensive – Transparent – Easy to Deploy – Proven!

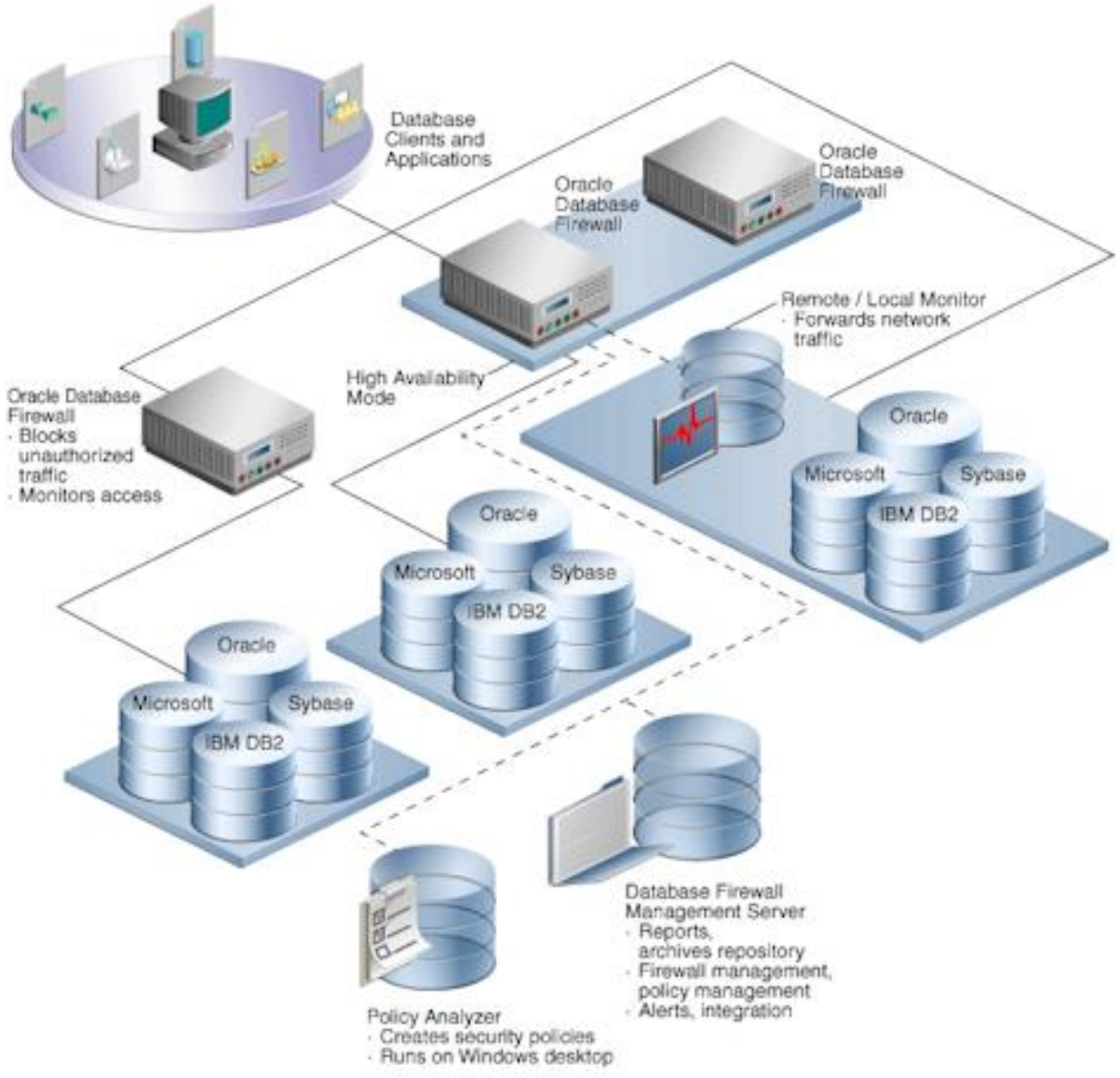
- Security requires that you implement what is "free" too

Oracle Security Products

- Oracle provides an extensive range of security products. Some focused solely on the database others focused on the entire technology stack: Among them
  - Monitoring and Blocking
    - Database Firewall
  - Auditing and Tracking
    - Oracle Total Recall
  - Access Control
    - Oracle Identity Management (OID)
    - Oracle Database Vault
    - Oracle Label Security
  - Encryption and Masking
    - Oracle Advanced Security
    - Oracle Secure Backup
    - Oracle Data Masking

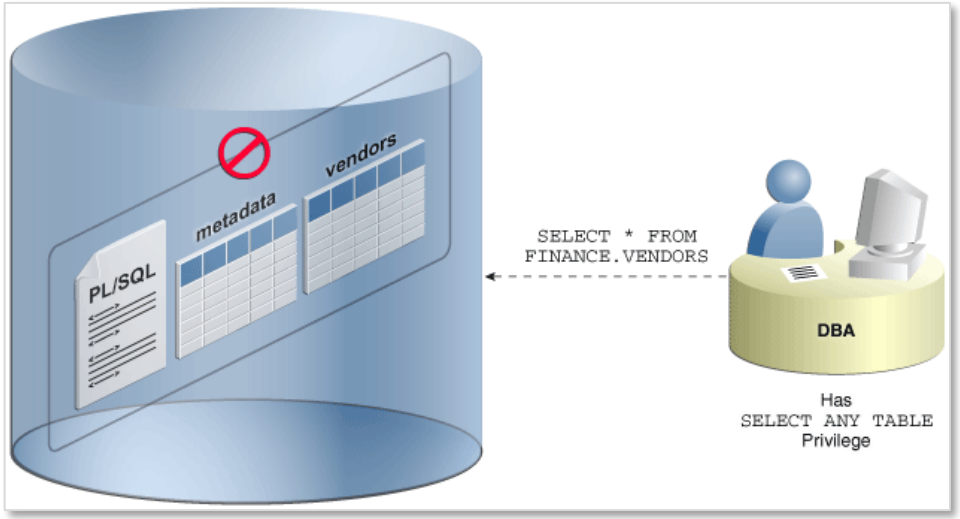
Database Firewall

- Secures and protects data in Oracle, MySQL, Microsoft SQL Server, Sybase Adaptive Server Enterprise (ASE), Sybase SQL Anywhere SQL, and IBM DB2 SQL
- Tools to assess vulnerabilities and enhances existing database security features, such as encryption and authentication
- Blocks attempted attacks, logs activity, and produces warnings
- Traditional systems test syntax of statements passed to the database, recognizing redefined expressions
- Analyzing the meaning of SQL and can prevent zero-day attack
- Protects against attacks originating from within the corporate network, as well as from external sources



Database Vault

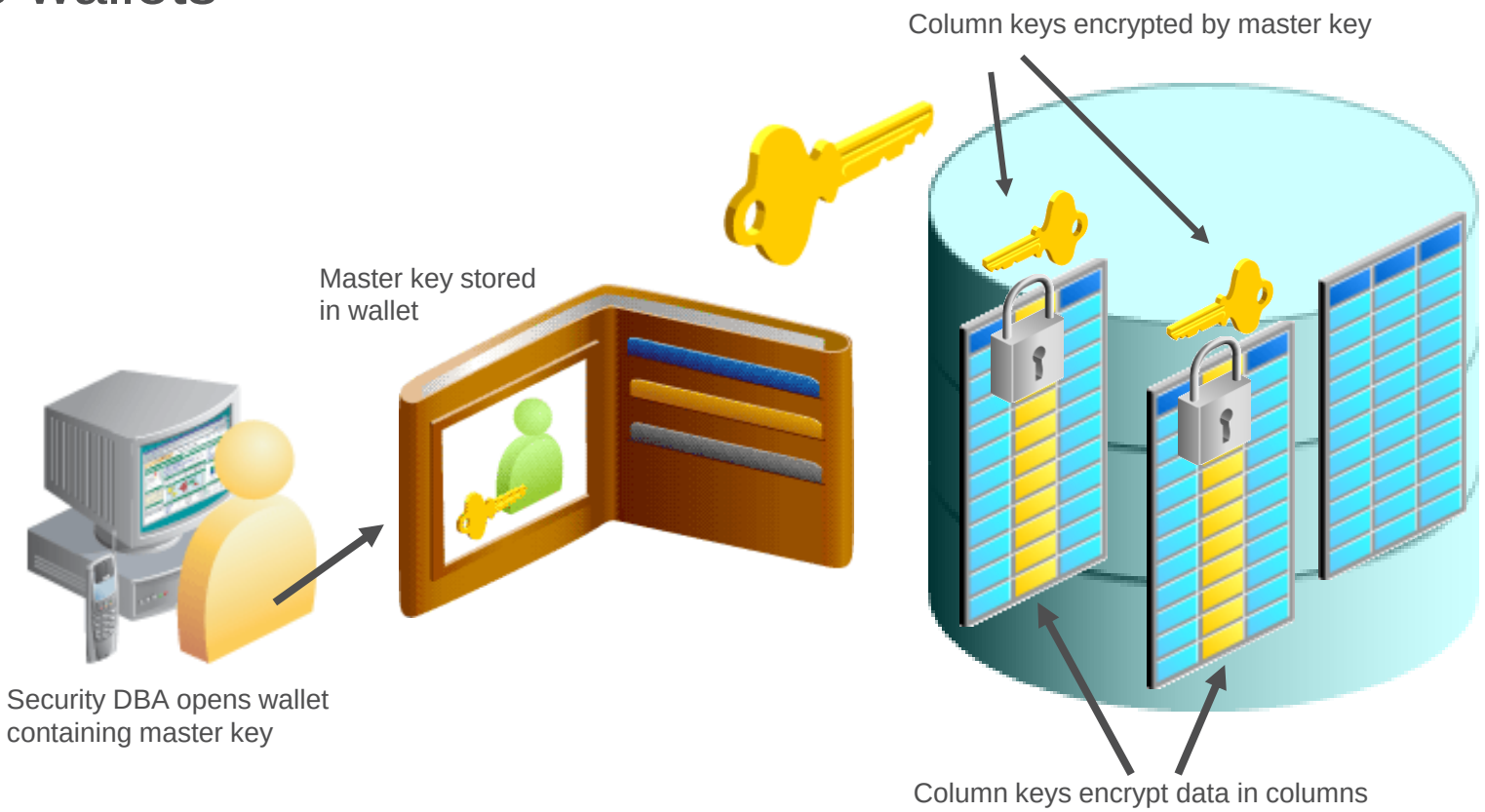
- Provides security controls to help protect application data from unauthorized access, and comply with privacy and regulatory requirements
- You can deploy controls to block privileged account access to application data and control sensitive operations inside the database using multi-factor authorization
- Secures existing database environments transparently, eliminating costly and time consuming application changes



- Creates an environment in which separation of duties can be effectively designed, deployed, and enforced through the creation of secure application roles that are enabled only by Database Vault rules

Wallets & Wallet Manager

- Wallets are a password-protected container used to store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL
- Wallet Manager supports the administrative tasks required for the creation and management of multiple wallets



Enterprise Edition Only (1:2)

- Advanced Security Option
  - Encryption through-out the database stack
- Data Masking
  - Selective, on-the-fly transformation to protect sensitive data
- Data Redaction (part of OAS)
  - Selective, on-the-fly redaction data transformation in SQL query results prior to display
- Database Vault
  - Protects sensitive data from access by users with privileged accounts
- Enterprise User Security
  - Integration of database user accounts with LDAP
- Label Security
  - Fine Grained Access Control extended to finer granularity and control
- Network Encryption (SSL/TLS)
  - Encryption of communications between the database and clients, applications, backups utilities, and DR facilities

Enterprise Edition Only (2:2)

- Privilege Analysis
  - Analyses assigned privileges
- Real Application Security
  - Second generation VPD
- Secure External Password Store
  - Uses an Oracle Wallet to hold password credentials
- Transparent Sensitive Data Protection
  - Grouping of columns for application of data masking (redaction) policies
- Virtual Private Database (Row Level Security)
  - Uses PL/SQL functions to create a WHERE clause or append to an existing WHERE clause preventing unauthorized row level data access

Data Redaction (1:2)

- Requires Enterprise Edition
- Requires Licensing
- Replaces traditional data masking with more robust policy based masking capabilities with the power of regular expressions to identify sensitive data
- Based on the built-in DBMS_REDACT package

Data Redaction (2:2)

```
DECLARE
  lSchema       redaction_policies.object_owner%TYPE := USER;
  lObject       redaction_policies.object_name%TYPE := 'PERSON';
  lPolicy       redaction_policies.policy_name%TYPE := 'PERSON_SSN_REDACT';
  lDescript     redaction_policies.policy_description%TYPE := 'SSN Obfuscation';
  lColumn       redaction_columns.column_name%TYPE := 'SSN';
  lColDes       redaction_columns.column_description%TYPE := 'SSN Masking Test';
  lFuncType     BINARY_INTEGER := dbms_redact.full;
  lFuncParam    redaction_columns.function_parameters%TYPE := '';
  lExpression   VARCHAR2(60) := 'SYS_CONTEXT(''SYS_SESSION_ROLES'', ''SUPERVISOR'') = ''FALSE''';
  lEnable       BOOLEAN := FALSE;
  lREPattern    redaction_columns.regexp_pattern%TYPE := NULL;
  lReplString   redaction_columns.regexp_replace_string%TYPE := NULL;
  lREPosition   BINARY_INTEGER := 1;
  lREOccur      BINARY_INTEGER := 0;
  lREMatchParm redaction_columns.regexp_match_parameter%TYPE := NULL;
 BEGIN
   dbms_redact.add_policy(lSchema, lObject, lPolicy, lDescript, lColumn, lColDes,
                          lFuncType, lFuncParam, lExpression, lEnable, lREPattern,
                          lReplString, lREPosition, lREOccur, lREMatchParm);
 END;
 /
```

Enterprise User Security

- Requires Enterprise Edition
- Requires Licensing
- Enterprise users are those users that are defined in a directory and their identity remains constant throughout the enterprise
- Enterprise User Security relies on Oracle Identity Management infrastructure, which in turn uses an LDAP-compliant directory service to centrally store and manage users

Label Security (OLS)

- Requires Enterprise Edition
- Requires Licensing
- Use to secure your database tables at the row level, and assign rows different levels of security based on the row's data
- For example, rows that contain highly sensitive data can be assigned a label entitled HIGHLY SENSITIVE; rows that are less sensitive can be labeled as SENSITIVE; rows that all users can have access to can be labeled PUBLIC

```
SQL> SELECT object_type, COUNT(*)
  2  FROM dba_objects
  3  WHERE owner = 'LBACSYS'
  4  GROUP BY object_type
  5* ORDER BY 1;

OBJECT_TYPE             COUNT(*)
------------------- ----------
FUNCTION                    24
INDEX                       30
LIBRARY                     11
PACKAGE                     23
PACKAGE BODY                22
PROCEDURE                    9
SEQUENCE                     3
TABLE                       22
TRIGGER                      3
TYPE                         9
TYPE BODY                    4
VIEW                        77
```

Oracle Advanced Security (OAS)

- Only available with Enterprise Edition
- Additional licensing cost
- Required for Transparent Data Encryption (TDE) which transparently to an application encrypts data in datafiles
  - Provides no protection against any theft other than an attempt to copy physical data files
- Required for encrypting RMAN backups to disk
- Required for encrypting DataPump exports
- Required for encrypting Data Guard traffic
- Required for Transparent Data Encryption master key storage

Privilege Analysis

- Requires Enterprise Edition
- Requires Database Vault license
- Implemented with the DBMS_PRIVILEGE_CAPTURE built-in package
- Contains the following objects
  - CREATE_CAPTURE
  - DISABLE_CAPTURE
  - DROP_CAPTURE
  - ENABLE_CAPTURE
  - GENERATE_RESULT

```
DECLARE
 rlist role_name_list;
BEGIN
  rlist := role_name_list(NULL);
  rlist(1) := 'CONNECT';
  rlist.extend;
  rlist(2) := 'EXECUTE_CATALOG_ROLE';

  dbms_privilege_capture.create_capture('
       UWPrivCapt',
       'Test policy',
       dbms_privilege_capture.g_role,
       rlist,
       NULL);
  dbms_privilege_capture.enable_capture('UWPrivCapt');
  dbms_privilege_capture.disable_capture('UWPrivCapt');
  dbms_privilege_capture.generate_result('UWPrivCapt');
END;
/
```

Real Application Security (RAS)

- Requires Enterprise Edition (no extra licensing required)
- Provides a declarative model that enables security policies that encompass not only the business objects being protected but also the principals (users and roles) that have permissions to operate on those business objects
- A policy-based authorization model that recognizes application-level users, privileges, and roles within the database, and then controls access on both static and dynamic collections of records representing business objects
- With built-in support for securely propagating application users' sessions to the database, Oracle RAS allows security policies on data to be expressed directly in terms of the application users, their roles and security contexts
- Can also act as an authorization decision service to assist the application in enforcing security within the middle-tier
- Creates and uses Access Control Lists (ACL) which are a collection of privilege grants or Access Control Entries (ACE), where an ACE grants or denies privileges to a user or a role

Secure External Password Store

- Requires Enterprise Edition
- Requires Licensing
- Uses an external wallet to hold database passwords

```
-- create wallet directory
mkdir $ORACLE_BASE/admin/orabase/wallet

-- modify SQLNET.ORA
NAMES.DIRECTORY_PATH = (TNSNAMES, EZCONNECT)
ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD=FILE) (METHOD_DATA = (DIRECTORY = /u01/oracle/admin/orabase\wallet)))
```

Transparent Sensitive Data Protection (TSDP)

- Requires Enterprise Edition
- Requires Licensing
- Permits creating sets of columns with the same sensitive type (like credit card number) on the database level
- Data Redaction is used on the policies for masking sets of columns the same way across a database
- Implemented with the DBMS_TSDP_MANAGE and DBMS_TSDP_PROTECT built-in packages

```
exec dbms_tsdp_manage.add_sensitive_type('FIN_TYPE', 'Finanical Information');

SELECT * FROM dba_tsdp_policy_type;

exec dbms_tsdp_manage.add_sensitive_column('SCOTT', 'EMP', 'SAL', 'FIN_TYPE', 'Employee Salaries');

SELECT * FROM dba_tsdp_policy_protection;
```

Virtual Private Database aka Row Level Security (VPD / RLS)

- Provides row-level security at the database table or view level
- Can be extended to provide column-level security as well
- Essentially, creates or modifies an existing WHERE clause rewriting a query in the optimizer so that the query cannot return restricted rows or columns
- Based on the built-in DBMS_RLS package

```
FUNCTION empview_sec(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2 IS
 predicate VARCHAR2(2000);
BEGIN
  IF (sys_context('exp_rpt', 'exp_role') = 'manager') THEN
    predicate := 'cost_center_id = sys_context(''exp_rpt'', ''cc_number'')';
  ELSE
    predicate := 'employee_id = sys_context(''exp_rpt'', ''emp_number'')';
  END IF;
  RETURN predicate;
END empview_sec;
```

Perimeter Defense

Database Networks

- Attempts are being made essentially 7 x 24 x 365 to attack your organizations
- If you do not know this then you have insufficient monitoring and most likely many of the attempts are success
- A small division of one of America's largest retailers has not been able to identify a single 24 hour period in the last 5 years during which there was not at least one serious, professional, attempt to access their data

Database Networks

- Every Oracle Database deployment requires multiple network connections

Name	Protocol	Utilization
Management	TCP/IP	System Admin connection to the server's light's-out management card
Public	TCP/IP	Access for applications, DBAs, exports, imports, backups: No keep-alive if RAC
SAN Storage	Fibre Channel	Server connection to a Storage Area Network (SAN)
NAS Storage	TCP/IP or IB	Connection to an NFS or DNFS mounted storage array
RAC Cache Fusion interconnect	UDP or IB	Jumbo Frames, no keep-alive, with custom configured read and write caching
Replication	TCP/IP	Data Guard and GoldenGate
Backup and Import/Export	TCP/IP	RMAN, DataPump, CommVault, Data Domain, ZFS, ZDLRA

- Every one of these networks provides access to critical infrastructure
- No conversation on networking is complete without considering firewalls, DNS and NTP servers, load balancers, and a large variety of mobile and Internet of Things devices

Firewalls (1:2)

- Many organizations think they are protected because they have a firewall
- The following example is real and came from a customer security audit
- The firewall's configuration, discovered during the audit, allowed direct access from the internet to the database servers
- The organization's employees did not fully understand the implications of the rules they were writing

```
ICMP Allowed from outside to Business-Data Zone

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match source-address any

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match destination-address any

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match application junos-ping

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping then permit

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping then log session-close
```

Firewalls (2:2)

- The fact that a firewall has been purchased and configured should give you no sense of comfort
- Here is another firewall rule setting discovered during a security audit
- This example cancels the stateful feature of the firewall and make it just like a switch or router with security rules (ACLs)
- All traffic is allowed both from/to the outside interface with security level 0

```
dc-fwsm-app configurations

1094 access-list INBOUND-CAMPUS extended permit ip any any
3735 access-group INBOUND-CAMPUS in interface OUTSIDE
1096 access-list OUTBOUND-CAMPUS extended permit ip any any
3736 access-group OUTBOUND-CAMPUS out interface OUTSIDE

dc-fwsm-db configurations

access-list INBOUND-CAMPUS extended permit ip any any
access-group INBOUND-CAMPUS in interface OUTSIDE

access-list OUTBOUND-CAMPUS extended permit ip any any
access-group OUTBOUND-CAMPUS out interface OUTSIDE
```

Security Breach Root Cause Analysis

Internal vs. External Threats

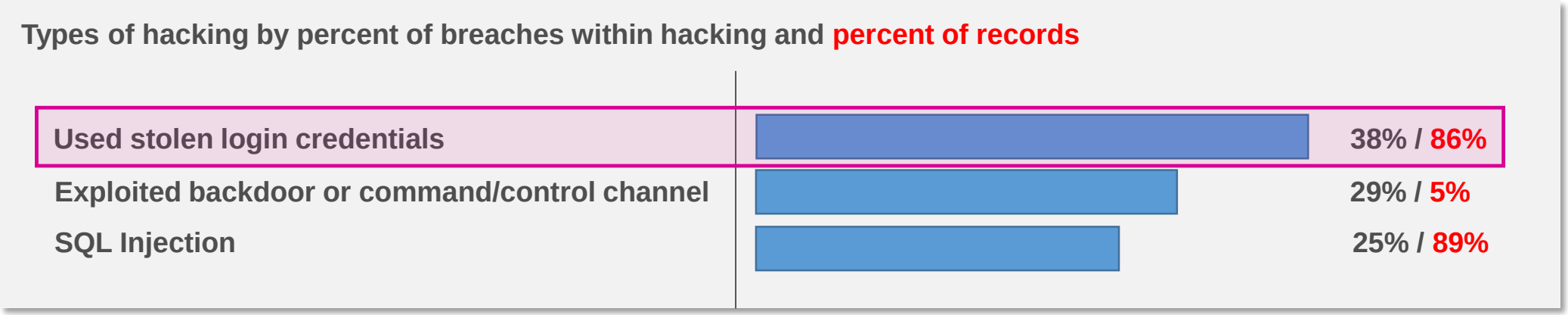
- Most organizations focus on the least likely threats and ignore what has been historically proven to be the largest threat
- The following is quoted from "Reference for Business" on the subject of computer crimes

> **As criminologist and computer-insurance executive Ron Hale indicated to Tim McCollum of *Nation's Business,* one of the most unsettling facts about computer crime is that the greatest threat to information security for small businesses is their employees. As McCollum noted, "a company's employees typically have access to its personal computers and computer networks, and often they know precisely what business information is valuable and where to find it." The reasons for these betrayals are many, ranging from workplace dissatisfaction to financial or family difficulties.**

- When organizations focus on their firewall they are focusing on what is often the most expensive, yet least effective, protection against data theft
- Part of our job is to provide solutions that address vulnerabilities and minimize our organization's risk exposure
- The other part is educational ... to educate our internal and external customers on the nature of real-world threats
- The education needs to come from us ... not from someone in sales

Real World Threats: How Database Breaches Really Occur

- 48% involve privilege misuse
- 40% result from hacking



- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

Percentages do not add up to 100% because many breaches employed multiple tactics in parallel or were outliers

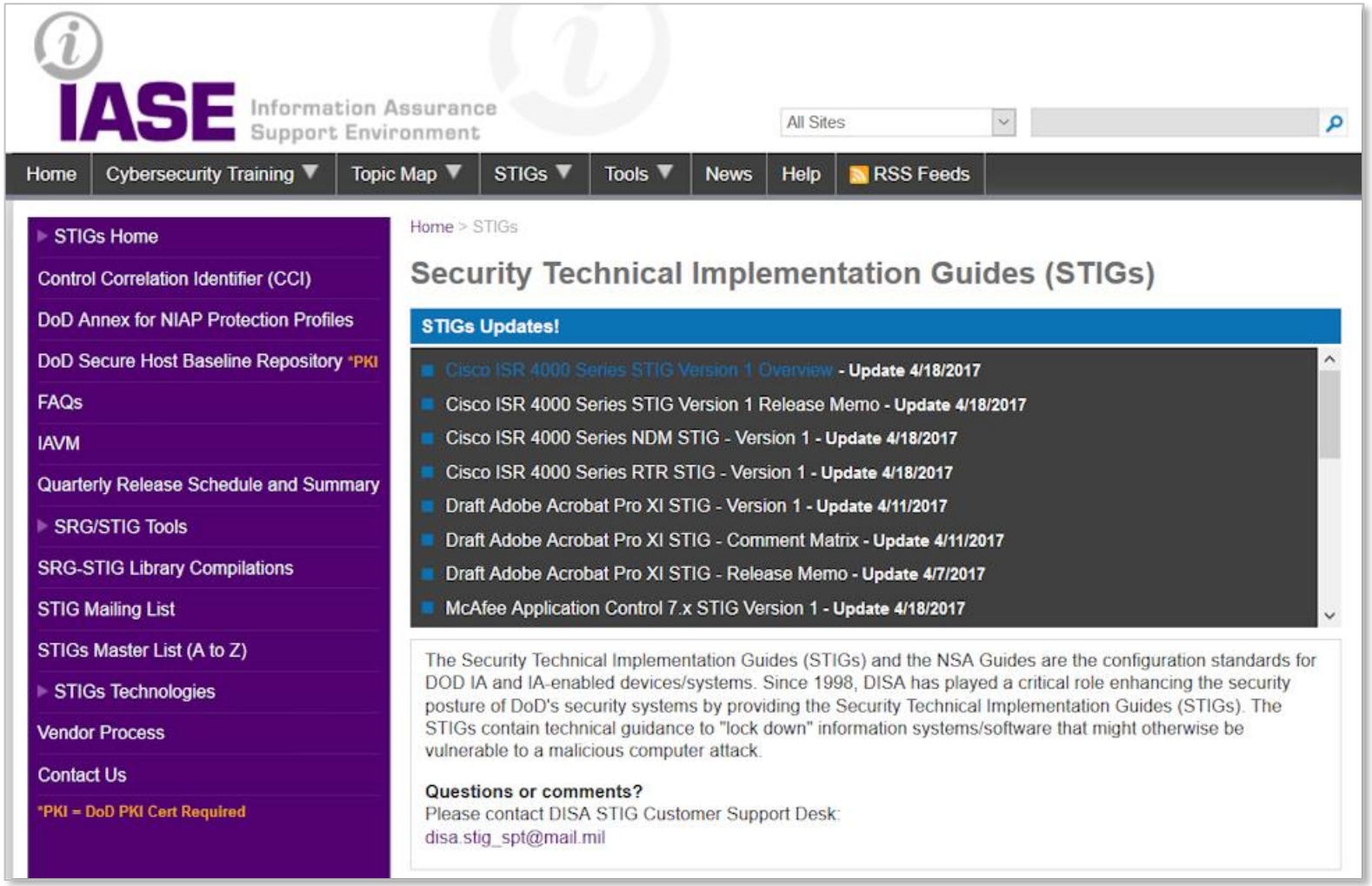
Misdirected By The Media

- What does the IC3 have to do with securing data?
- Nothing!
- All of this is focused on how cyber-criminals get login credentials
- Not one byte relates to how, once credentials are stolen, the data can be protected

- Business E-mail Compromise
  Thu, 22 Jan 2015
- University Employee Payroll Scam
  Tue, 13 Jan 2015
- Scam Targeting University Students
  Tue, 13 Jan 2015

Gaining Access

STIG (2:3)



http://iase.disa.mil/stigs/Pages/index.aspx

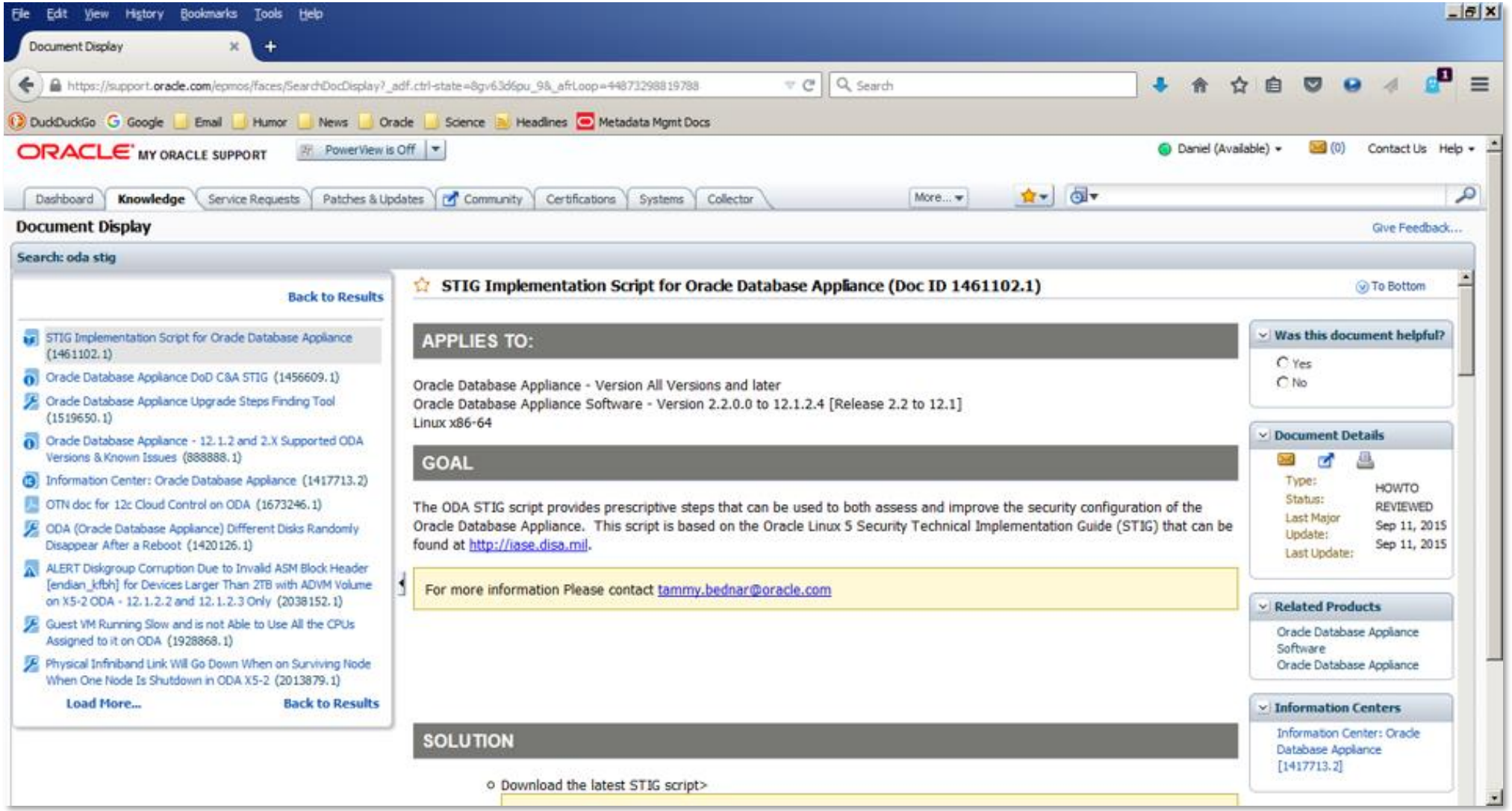
STIG (1:3)

- A STIG is a Security Technical Implementation Guide produced or approved by the US Department of Defense
- Oracle has published STIGs at My Oracle Support for Exadata and ODA
  - But the "CHECK" option can be run on any Linux server
- Oracle Support provides a downloadable script that can be used to check an ODA against STIG requirements and identify three levels of violations
- We strongly recommend running the script with the **`-check`** option but recommend having your Linux System Admin correct those issues you wish to correct manually

Warning: Never run the STIG script with the -fix option

- Ctrl-Alt-Del combination to shutdown system is enabled
- Password for grub not enabled
- Privilege account 'halt' is present
- Privilege account 'shutdown' is present
- RealVNC rpm is installed on system
- sendmail decode command is not commented in /etc/aliases
- Support for USB device found in kernel

STIG (3:3)


Document Display
MY ORACLE SUPPORT
Dashboard
Knowledge
Service Requests
Patches & Updates
Community
Certifications
Systems
Collector
Document Display
Search: oda stig
Back to Results
STIG Implementation Script for Oracle Database Appliance (1461102.1)
Oracle Database Appliance DoD C&A STIG (1456609.1)
Oracle Database Appliance Upgrade Steps Finding Tool (1519650.1)
Oracle Database Appliance - 12.1.2 and 2.X Supported ODA Versions & Known Issues (888888.1)
Information Center: Oracle Database Appliance (1417713.2)
OTN doc for 12c Cloud Control on ODA (1673246.1)
ODA (Oracle Database Appliance) Different Disks Randomly Disappear After a Reboot (1420126.1)
ALERT Diskgroup Corruption Due to Invalid ASM Block Header [endian_kfbh] for Devices Larger Than 2TB with ADVM Volume on X5-2 ODA - 12.1.2.2 and 12.1.2.3 Only (2038152.1)
Guest VM Running Slow and is not Able to Use All the CPUs Assigned to it on ODA (1928868.1)
Physical Infiniband Link Will Go Down When on Surviving Node When One Node Is Shutdown in ODA X5-2 (2013879.1)
Load More...
Back to Results
STIG Implementation Script for Oracle Database Appliance (Doc ID 1461102.1)
To Bottom
APPLIES TO:
Oracle Database Appliance - Version All Versions and later
Oracle Database Appliance Software - Version 2.2.0.0 to 12.1.2.4 [Release 2.2 to 12.1]
Linux x86-64
GOAL
The ODA STIG script provides prescriptive steps that can be used to both assess and improve the security configuration of the Oracle Database Appliance. This script is based on the Oracle Linux 5 Security Technical Implementation Guide (STIG) that can be found at http://iase.disa.mil.
For more information Please contact tammy.bednar@oracle.com
SOLUTION
Download the latest STIG script>
Was this document helpful?
Yes
No
Document Details
Type: HOWTO
Status: REVIEWED
Last Major Update: Sep 11, 2015
Last Update: Sep 11, 2015
Related Products
Oracle Database Appliance Software
Oracle Database Appliance
Information Centers
Information Center: Oracle Database Appliance [1417713.2]

Center For Internet Security (CIS)

- CIS is the source of audit guidelines and auditors for e-commerce websites

`https://www.cisecurity.org`

User Management

Application Access

- At many major Oracle customers there are two types of users defined
  - human: a sentient human will user this user-id to log on
  - mechid: an application or application server will use this user-id to connect
- All application schemas should be created with a mechid
- Application schemas should be granted the privileges required to create objects then
  - Revoke all system privileges from the application schema
  - Lock the schema and expire the password
  - Audit attempts to log onto the application schema directly

```
SQL> ALTER USER ps ACCOUNT LOCK;
SQL> REVOKE create session FROM ps;
SQL> REVOKE create table FROM ps;
SQL> REVOKE create procedure FROM ps;
SQL> REVOKE create view FROM ps;
SQL> ... enable auditing
```

Users

New: 12cR1

AUDSYS
GSMADMIN_INTERNAL
GSMCATUSER
GSMUSER
PDBADMIN
SYSBACKUP
SYSDG
SYSKM

New: 12cR2

APEX_050100
APEX_INSTANCE_ADMIN_USER
APEX_LISTENER
APEX_REST_PUBLIC_USER
DBJSON
DBSFWUSER
GGSYS
HRREST
OBE
ORDS_METADATA
ORDS_PUBLIC_USER
PDBADMIN
REMOTE_SCHEDULER_AGENT
RESTFUL
SYS$UMF
SYSRAC
XDBEXT
XDBPM
XFILES

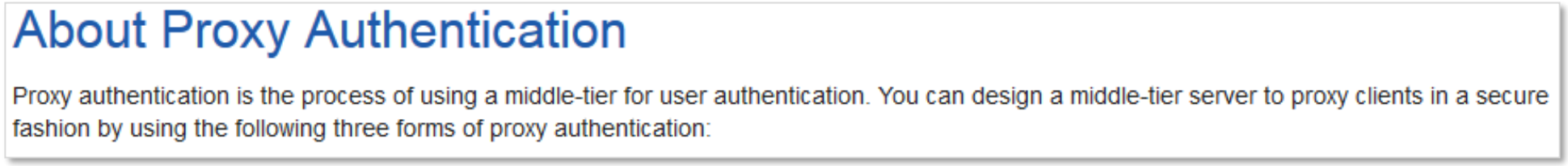
Dropped
BI, OE, PM, SH, and SPATIAL_WFS_USR

New Users With Escalated Privs

USERNAME	Usage
GGSYS	The internal account used by Oracle GoldenGate. It should not be unlocked or used for a database login.
SYSBACKUP	This privilege allows a user to perform backup and recovery operations either from Oracle Recovery Manager (RMAN) or SQL*Plus.
SYSDG	This privilege allows a user to perform Data Guard operations can use this privilege with either Data Guard Broker or the DGMGRL command-line interface.
SYSKM	This privilege allows a user to perform Transparent Data Encryption keystore operations.
SYSRAC	This privilege allows the Oracle agent of Oracle Clusterware to perform Oracle Real Application Clusters (Oracle RAC) operations. SYSRAC facilitates Oracle Real Application Clusters (Oracle RAC) operations by connecting to the database by the Clusterware agent on behalf of Oracle RAC utilities such as SRVCTL.

Proxy Users (1:3)

- Here's what the Oracle docs say about proxy users: They are not wrong but incomplete and misleading



About Proxy Authentication

Proxy authentication is the process of using a middle-tier for user authentication. You can design a middle-tier server to proxy clients in a secure fashion by using the following three forms of proxy authentication:

  - The source of the above statement is the "Database JDBC Developer's Guide

- Here's what Tom Kyte wrote ...

and we said...

a proxy user is a user that is allowed to "connect on behalf of another user"

say you have a middle tier application. You want to use a connection pool. You need to use a single user for that. Say that user is "midtier"

Scott can grant connect through to this midtier user.

- And, of course Tom Kyte was correct

Proxy Users (2:3)

- ... and proxy users cannot be spoofed

So now the midtier user (which has just "create session" and "connect through to scott") authenticates to the database and sets up the connection pool. This midtier user is just a regular user -- anything you can do to scott, you can do to midtier, but it generally isn't relevant. For the only thing midtier will do in the database is connect really!

So, scott comes along and convinces the midtier "i am really scott". The midtier then says to the database "you know me, I'm midtier and I'd like to pretend to be scott for a while". the database looks and says "yes midtier, you are allowed to be scott for a while -- go ahead". At this point -- that midtier connection will have a session where by "select user from dual" will return SCOTT -- not midtier.

Scott never gave the midtier his password to the database, in fact, scott might not even KNOW what his password to the database it!

Now, this SCOTT session that was created on behalf of the midtier connection is subject to all of the rules and privs around the user SCOTT -- it can only do what scott is allowed to do.

The nice thing about this is:

o you have auditing back, the database knows who is using it. no more of this "single username" junk.

o you have grants back, you don't have to reinvent security over and over and over.

o you have identity preserved all of the way from the browser through the middle tier and into the database.

Proxy Users (3:3)

```
-- create a non-human database user
SQL> CREATE USER mechid
  2  IDENTIFIED BY "A1Ac9C81292FC1CF0b8A40#5F04C0A"
  3  DEFAULT TABLESPACE uwdata
  4  TEMPORARY TABLESPACE temp
  5  QUOTA 100M ON uwdata;

User created.

SQL> ALTER USER mechid ACCOUNT LOCK;

Grant succeeded.

SQL> AUDIT CONNECT BY scott ON BEHALF OF mechid;

Audit succeeded.

-- create proxy for mechid
SQL> ALTER USER mechid GRANT CONNECT THROUGH scott;

User altered.

SQL> SELECT * FROM sys.proxy_info$;

   CLIENT#     PROXY# CREDENTIAL_TYPE#      FLAGS
---------- ---------- ---------------- ----------
       142        109                0          5
```

```
SQL> conn scott[MECHID]/tiger@pdbdev
Connected.

SQL> sho user
USER is "MECHID"

SQL> SELECT sys_context('USERENV', 'CURRENT_SCHEMA')
  2  FROM dual;

SYS_CONTEXT('USERENV','CURRENT_SCHEMA')
--------------------------------------------------
MECHID

SQL> SELECT sys_context('USERENV', 'CURRENT_USER')
  2  FROM dual;

SYS_CONTEXT('USERENV','CURRENT_USER')
--------------------------------------------------
MECHID

SQL> SELECT sys_context('USERENV', 'PROXY_USER')
  2  FROM dual;

SYS_CONTEXT('USERENV','PROXY_USER')
--------------------------------------------------
SCOTT
```

User Authentication and Permissions

- No user should be created using the default profile
- Check for default password usage
  - If you find default passwords being used either change the passwords or lock and expire the account
- Do not use externally authenticated users such as OPS$ unless you can prove that O/S access is secure and will stay that way which, of course, you cannot do
- CIS audit check 4.07 specifically checks for the use of externally authenticated access

```
SQL> SELECT d.con_id, d.username, u.account_status
  2  FROM cdb_users_with_defpwd d, cdb_users u
  3  WHERE d.username = u.username
  4  AND u.account_status = 'OPEN'
  5  ORDER BY 3,1, 2;

    CON_ID USERNAME                       ACCOUNT_STATUS
---------- ------------------------------ --------------
         1 SYS                            OPEN
         1 SYS                            OPEN
         1 SYSTEM                         OPEN
         1 SYSTEM                         OPEN
         3 HR                             OPEN
         3 OE                             OPEN
         3 PM                             OPEN
         3 SCOTT                          OPEN
         3 SH                             OPEN
         3 SYS                            OPEN
         3 SYS                            OPEN
         3 SYSTEM                         OPEN
         3 SYSTEM                         OPEN
```

Profiles (1:3)

12cR1 Default

COMPOSITE_LIMIT	UNLIMITED
CONNECT_TIME	UNLIMITED
CPU_PER_CALL	UNLIMITED
CPU_PER_SESSION	UNLIMITED
FAILED_LOGIN_ATTEMPTS	10
IDLE_TIME	UNLIMITED
LOGICAL_READS_PER_CALL	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
PASSWORD_GRACE_TIME	7
PASSWORD_LIFE_TIME	180
PASSWORD_LOCK_TIME	1
PASSWORD_REUSE_MAX	UNLIMITED
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_VERIFY_FUNCTION	NULL
PRIVATE_SGA	UNLIMITED
SESSIONS_PER_USER	UNLIMITED

12cR2 ORA_STIG_PROFILE

COMPOSITE_LIMIT	UNLIMITED
CONNECT_TIME	UNLIMITED
CPU_PER_CALL	UNLIMITED
CPU_PER_SESSION	UNLIMITED
FAILED_LOGIN_ATTEMPTS	3
IDLE_TIME	15
INACTIVE_ACCOUNT_TIME	35
LOGICAL_READS_PER_CALL	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
PASSWORD_GRACE_TIME	5
PASSWORD_LIFE_TIME	60
PASSWORD_LOCK_TIME	UNLIMITED
PASSWORD_REUSE_MAX	10
PASSWORD_REUSE_TIME	265
PASSWORD_VERIFY_FUNCTION	ORA12C_STIG_VERIFY_FUNCTION
PRIVATE_SGA	UNLIMITED
SESSIONS_PER_USER	UNLIMITED

Starting with this release, you can use the INACTIVE_ACCOUNT_TIME parameter to automatically lock the account of a database user who has not logged in to the database instance in a specified number of days.

Profiles (2:3)

- Run $ORACLE_HOME/rdbms/admin/utlpwdmg.sql

```
-- This script alters the default parameters for Password Management
-- This means that all the users on the system have Password Management
-- enabled and set to the following values unless another profile is
-- created with parameter values set to different value or UNLIMITED
-- is created and assigned to the user.

ALTER PROFILE DEFAULT LIMIT
FAILED_LOGIN_ATTEMPTS        10
INACTIVE_ACCOUNT_TIME UNLIMITED
PASSWORD_GRACE_TIME           7
PASSWORD_LIFE_TIME    UNLIMITED
PASSWORD_LOCK_TIME            1
PASSWORD_REUSE_TIME   UNLIMITED
PASSWORD_REUSE_MAX    UNLIMITED
PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
```

Profiles (3:3)

- Uncomment the CIS or STIG profiles for improved security

```
/**
The below set of password profile parameters would take into consideration
recommendations from Center for Internet Security[CIS Oracle 11g].

ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX  UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 1
INACTIVE_ACCOUNT_TIME UNLIMITED
PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
*/

/**
The below set of password profile parameters would take into
consideration recommendations from Department of Defense Database
Security Technical Implementation Guide[STIG v8R1].

ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_REUSE_TIME 365
PASSWORD_REUSE_MAX  5
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_VERIFY_FUNCTION ora12c_strong_verify_function;*/
```

Secure Configuration

- A script run as part of installation that creates a "secure configuration"
- Review the script **`$ORACLE_HOME/rdbms/admin/secconf.sql`**

```
Rem     Secure configuration settings for the database include a reasonable
Rem     default password profile, password complexity checks, audit settings
Rem     (enabled, with admin actions audited), and as many revokes from PUBLIC
Rem     as possible. In the first phase, only the default password profile is included.
```

Can perform the following

- Modifies the Default profile
- Creates audit policy: ORA_ACCOUNT_MGMT
- Creates audit policy: ORA_DATABASE_PARAMETER
- Creates audit policy: ORA_LOGON_FAILURES
- Creates audit policy: ORA_SECURECONFIG
- Creates audit policy: ORA_CIS_RECOMMENDATIONS

- Executed indirectly when **`$ORACLE_HOME/rdbms/admin/catproc.sql`** is run

Roles (1:2)

- Roles can be further protected through passwords and PL/SQL package validation

```
-- role secured by password
CREATE ROLE read_only IDENTIFIED BY "S0^Sorry";

-- role secured by PL/SQL package
CREATE OR REPLACE PACKAGE db_security AUTHID CURRENT_USER IS
  PROCEDURE enable_role;
END db_security;
/

CREATE OR REPLACE PACKAGE BODY db_security IS
  PROCEDURE enable_role IS
  BEGIN
    dbms_session.set_role('read_only');
  END enable_role;
END db_security;
/

SELECT * FROM dba_application_roles;

CREATE ROLE read_only IDENTIFIED USING db_security;
```

  - A PL/SQL package can perform numerous tests to verify the identity of the user and their connection before granting access
  - If the package object returns an exception the role is not granted

Roles (2:2)

12cR1 New
ADM_PARALLEL_EXECUTE_TASK
APEX_GRANTS_FOR_NEW_USERS_ROLE
AUDIT_ADMIN
AUDIT_VIEWER
CAPTURE_ADMIN
CDB_DBA
DBAHADOOP
DV_AUDIT_CLEANUP
DV_GOLDENGATE_ADMIN
DV_GOLDENGATE_REDO_ACCESS
DV_MONITOR
DV_PATCH_ADMIN
DV_STREAMS_ADMIN
DV_XSTREAM_ADMIN
EM_EXPRESS_ALL
EM_EXPRESS_BASIC
GSMADMIN_ROLE
GSMUSER_ROLE
GSM_POOLADMIN_ROLE
HS_ADMIN_SELECT_ROLE
LBAC_DBA
OPTIMIZER_PROCESSING_RATE
PDB_DBA
PROVISIONER
XS_CACHE_ADMIN
XS_NAMESPACE_ADMIN
XS_RESOURCE
XS_SESSION_ADMIN

12cR1 Dropped
DELETE_CATALOG_ROLE

12cR2 New
APEX_ADMINISTRATOR_READ_ROLE
APPLICATION_TRACE_VIEWER
DATAPATCH_ROLE
DBJAVASCRIPT
DBMS_MDX_INTERNAL
DV_POLICY_OWNER
GGSYS_ROLE
RDFCTX_ADMIN
RECOVERY_CATALOG_OWNER_VPD
SODA_APP
SYSUMF_ROLE
XFILES_ADMINISTRATOR
XFILES_USER
XS_CONNECT

12cR2 Dropped
DBAHADOOP
SPATIAL_WFS_ADMIN
WFS_USR_ROLE
XS_RESOURCE

System & Object Privs

System Privileges

- The rule is simple ... never grant privileges in excess of those required to perform a specified job function
- Don't grant "ANY" privileges without documented justification
- If you have not done so in the last 12 months review all users for their system privileges and revoke those not required
- There is literally no excuse for granting Oracle's DBA role to any user
  - No one should have privileges they don't need and don't know what they do

System Privileges Granted to the DBA Role

```
SQL> select privilege
  2  FROM dba_sys_privs
  3  WHERE grantee = 'DBA'
  4  ORDER BY 1;

PRIVILEGE
----------------------------------
-------
ADMINISTER ANY SQL TUNING SET
ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SQL MANAGEMENT OBJECT
ADMINISTER SQL TUNING SET
ADVISOR
ALTER ANY ASSEMBLY
ALTER ANY CLUSTER
ALTER ANY CUBE
ALTER ANY CUBE BUILD PROCESS
ALTER ANY CUBE DIMENSION
ALTER ANY DIMENSION
ALTER ANY EDITION
ALTER ANY EVALUATION CONTEXT
ALTER ANY INDEX
ALTER ANY INDEXTYPE
ALTER ANY LIBRARY
ALTER ANY MATERIALIZED VIEW
ALTER ANY MEASURE FOLDER
ALTER ANY MINING MODEL
ALTER ANY OPERATOR
ALTER ANY OUTLINE
ALTER ANY PROCEDURE
ALTER ANY ROLE
ALTER ANY RULE
ALTER ANY RULE SET
ALTER ANY SEQUENCE
ALTER ANY SQL PROFILE
ALTER ANY SQL TRANSLATION PROFILE
ALTER ANY TABLE
ALTER ANY TRIGGER
ALTER ANY TYPE
ALTER DATABASE
ALTER PROFILE
ALTER RESOURCE COST
ALTER ROLLBACK SEGMENT
ALTER SESSION
ALTER SYSTEM
ALTER TABLESPACE
ALTER USER
ANALYZE ANY
ANALYZE ANY DICTIONARY
AUDIT ANY
AUDIT SYSTEM
BACKUP ANY TABLE
BECOME USER
CHANGE NOTIFICATION
COMMENT ANY MINING MODEL
COMMENT ANY TABLE
CREATE ANY ASSEMBLY
CREATE ANY CLUSTER
CREATE ANY CONTEXT
CREATE ANY CREDENTIAL
CREATE ANY CUBE
CREATE ANY CUBE BUILD PROCESS
CREATE ANY CUBE DIMENSION
CREATE ANY DIMENSION
CREATE ANY DIRECTORY
CREATE ANY EDITION
CREATE ANY EVALUATION CONTEXT
CREATE ANY INDEX
CREATE ANY INDEXTYPE
CREATE ANY JOB
CREATE ANY LIBRARY
CREATE ANY MATERIALIZED VIEW
CREATE ANY MEASURE FOLDER
CREATE ANY MINING MODEL
CREATE ANY OPERATOR
CREATE ANY OUTLINE
CREATE ANY PROCEDURE
CREATE ANY RULE
CREATE ANY RULE SET
CREATE ANY SEQUENCE
CREATE ANY SQL PROFILE
CREATE ANY SQL TRANSLATION
PROFILE
CREATE ANY SYNONYM
CREATE ANY TABLE
CREATE ANY TRIGGER
CREATE ANY TYPE
CREATE ANY VIEW
CREATE ASSEMBLY
CREATE CLUSTER
CREATE CREDENTIAL
CREATE CUBE
CREATE CUBE BUILD PROCESS
CREATE CUBE DIMENSION
CREATE DATABASE LINK
CREATE DIMENSION
CREATE EVALUATION CONTEXT
CREATE EXTERNAL JOB
CREATE INDEXTYPE
CREATE JOB
CREATE LIBRARY
CREATE MATERIALIZED VIEW
CREATE MEASURE FOLDER
CREATE MINING MODEL
CREATE OPERATOR
CREATE PLUGGABLE DATABASE
CREATE PROCEDURE
CREATE PROFILE
CREATE PUBLIC DATABASE LINK
CREATE PUBLIC SYNONYM
CREATE ROLE
CREATE ROLLBACK SEGMENT
CREATE RULE
CREATE RULE SET
CREATE SEQUENCE
CREATE SESSION
CREATE SQL TRANSLATION PROFILE
CREATE SYNONYM
CREATE TABLE
CREATE TABLESPACE
CREATE TRIGGER
CREATE TYPE
CREATE USER
CREATE VIEW
DEBUG ANY PROCEDURE
DEBUG CONNECT SESSION
DELETE ANY CUBE DIMENSION
DELETE ANY MEASURE FOLDER
DELETE ANY TABLE
DEQUEUE ANY QUEUE
DROP ANY ASSEMBLY
DROP ANY CLUSTER
DROP ANY CONTEXT
DROP ANY CUBE
DROP ANY CUBE BUILD PROCESS
DROP ANY CUBE DIMENSION
DROP ANY DIMENSION
DROP ANY DIRECTORY
DROP ANY EDITION
DROP ANY EVALUATION CONTEXT
DROP ANY INDEX
DROP ANY INDEXTYPE
DROP ANY LIBRARY
DROP ANY MATERIALIZED VIEW
DROP ANY MEASURE FOLDER
DROP ANY MINING MODEL
DROP ANY OPERATOR
DROP ANY OUTLINE
DROP ANY PROCEDURE
DROP ANY ROLE
DROP ANY RULE
DROP ANY RULE SET
DROP ANY SEQUENCE
DROP ANY SQL PROFILE
DROP ANY SQL TRANSLATION PROFILE
DROP ANY SYNONYM
DROP ANY TABLE
DROP ANY TRIGGER
DROP ANY TYPE
DROP ANY VIEW
DROP PROFILE
DROP PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM
DROP ROLLBACK SEGMENT
DROP TABLESPACE
DROP USER
EM EXPRESS CONNECT
ENQUEUE ANY QUEUE
EXECUTE ANY ASSEMBLY
EXECUTE ANY CLASS
EXECUTE ANY EVALUATION CONTEXT
EXECUTE ANY INDEXTYPE
EXECUTE ANY LIBRARY
EXECUTE ANY OPERATOR
EXECUTE ANY PROCEDURE
EXECUTE ANY PROGRAM
EXECUTE ANY RULE
EXECUTE ANY RULE SET
EXECUTE ANY TYPE
EXECUTE ASSEMBLY
EXEMPT DDL REDACTION POLICY
EXEMPT DML REDACTION POLICY
EXPORT FULL DATABASE
FLASHBACK ANY TABLE
FLASHBACK ARCHIVE ADMINISTER
FORCE ANY TRANSACTION
FORCE TRANSACTION
GLOBAL QUERY REWRITE
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
IMPORT FULL DATABASE
INSERT ANY CUBE DIMENSION
INSERT ANY MEASURE FOLDER
INSERT ANY TABLE
LOCK ANY TABLE
LOGMINING
MANAGE ANY FILE GROUP
MANAGE ANY QUEUE
MANAGE FILE GROUP
MANAGE SCHEDULER
MANAGE TABLESPACE
MERGE ANY VIEW
ON COMMIT REFRESH
QUERY REWRITE
READ ANY FILE GROUP
READ ANY TABLE
READ ANY TABLE
REDEFINE ANY TABLE
RESTRICTED SESSION
RESUMABLE
SELECT ANY CUBE
SELECT ANY CUBE BUILD PROCESS
SELECT ANY CUBE DIMENSION
SELECT ANY DICTIONARY
SELECT ANY MEASURE FOLDER
SELECT ANY MINING MODEL
SELECT ANY SEQUENCE
SELECT ANY TABLE
SELECT ANY TRANSACTION
SET CONTAINER
UNDER ANY TABLE
UNDER ANY TYPE
UNDER ANY VIEW
UPDATE ANY CUBE
UPDATE ANY CUBE BUILD PROCESS
UPDATE ANY CUBE DIMENSION
UPDATE ANY TABLE
USE ANY SQL TRANSLATION PROFILE

220 rows selected.
```

Think you "NEED" the DBA role?

Feel free to explain why you need any of the privileges highlighted in red

System Privileges

12cR1 New
ADMINISTER KEY MANAGEMENT
ALTER ANY CUBE BUILD PROCESS
ALTER ANY MEASURE FOLDER
ALTER ANY SQL TRANSLATION PROFILE
CREATE ANY CREDENTIAL
CREATE ANY SQL TRANSLATION PROFILE
CREATE CREDENTIAL
CREATE PLUGGABLE DATABASE
CREATE SQL TRANSLATION PROFILE
DROP ANY SQL TRANSLATION PROFILE
EM EXPRESS CONNECT
EXEMPT ACCESS POLICY
EXEMPT DDL REDACTION POLICY
EXEMPT DML REDACTION POLICY
EXEMPT IDENTITY POLICY
EXEMPT REDACTION POLICY
INHERIT ANY PRIVILEGES
KEEP_DATE TIME
KEEP_SYSGUID
LOGMINING
PURGE DBA_RECYCLEBIN
REDEFINE ANY TABLE
SELECT ANY CUBE BUILD PROCESS
SELECT ANY MEASURE FOLDER
SET CONTAINER
SYSBACKUP
SYSDG
SYSKM
TRANSLATE ANY SQL
USE ANY SQL TRANSLATION PROFILE

12cR2 New
ALTER ANY ANALYTIC VIEW
CREATE ANALYTIC VIEW
CREATE ANY ANALYTIC VIEW
DROP ANY ANALYTIC VIEW

ALTER ANY ATTRIBUTE DIMENSION
CREATE ANY ATTRIBUTE DIMENSION
CREATE ATTRIBUTE DIMENSION
DROP ANY ATTRIBUTE DIMENSION

ALTER ANY HIERARCHY
CREATE ANY HIERARCHY
CREATE HIERARCHY
DROP ANY HIERARCHY

ALTER LOCKDOWN PROFILE
CREATE LOCKDOWN PROFILE
DROP LOCKDOWN PROFILE

DEBUG CONNECT ANY

INHERIT ANY REMOTE PRIVILEGES

SYSRAC

USE ANY JOB RESOURCE

12cR2 Modified
SELECT ANY DICTIONARY (altered in 12.1.0.2 to exclude some objects)

Object Privileges

- The rule is simple ... never grant privileges to objects that are not required
- If granting access to a table you have choices
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
- If granting update privileges control by column whenever possible

```
GRANT UPDATE (first_name, last_name) ON person TO uwclass;
```

- No data has ever been stolen because the privileges were too granular

V$ Object Access (1:2)

- Anyone that can query Oracle X$ and/or V$ objects can bypass the vast majority of Oracle Database security
- Some of the objects that are critically important to protect are
  - V_$MAPPED_SQL
  - V_$SQL
  - V_$SQLAREA
  - V_$SQLAREA_PLAN_HASH
  - V_$SQLSTATS
  - V_$SQLSTATS_PLAN_HASH
  - V_$SQLTEXT
  - V_$SQLTEXT_WITH_NEWLINES
  - V_$SQL_BIND_CAPTURE
  - V_$SQL_BIND_DATA
  - V_$SQL_OPTIMIZER_ENV
  - V_$SQL_PLAN

V$ Object Access (2:2)

- If data is not encrypted before DML the original statement can be recovered
- Transparent Data Encryption (TDE) offers no protection from this attack

```
SQL> CREATE TABLE credit_card (
  2  ccno  VARCHAR2(19),
  3  cname VARCHAR2(25));

Table created.

SQL> INSERT /* memtest */ INTO credit_card
  2  VALUES ('5123-4567-8901-2345', 'Dan Morgan');

1 row created.

SQL> SELECT sql_id, sql_fulltext
  2  FROM v$sqlarea
  3  WHERE sql_fulltext LIKE '%memtest%';

SQL_ID        SQL_FULLTEXT
------------- --------------------------------------------------------------------------
fy44ug06np5w4 INSERT /* memtest */ INTO credit_card
              VALUES ('5123-4567-8901-2345', 'Dan Morgan')

5d4p3uz59b0a1 SELECT sql_id, sql_fulltext♂FROM v$sqlarea♂WHERE sql_fulltext LIKE '%memtest3%'
```

SQL*Net

Net Services Security

- Here's what Oracle says about Net Services aka SQL*Net

> Local listener administration is secure through local operating system authentication, which restricts listener administration to the user who started the listener or to the super user. By default, remote listener administration is disabled.

- For secure communications you need to consider the following parameters (some of which require the Advanced Security Option)
  - NAMES.LDAP_AUTHENTICATE_BIND
  - NAMES.LDAP_CONN_TIMEOUT
  - NAMES.LDAP_PERSISTENT_SESSION
  - SQLNET.ALLOWED_LOGON_VERSION_CLIENT
  - SQLNET.ALLOWED_LOGON_VERSION_SERVER
  - SQLNET.AUTHENTICATION_SERVICES
  - SQLNET.CLIENT_REGISTRATION
  - SQLNET.CRYPTO_CHECKSUM_CLIENT
  - SQLNET.CRYPTO_CHECKSUM_SERVER
  - SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
  - SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
  - SQLNET.ENCRYPTION_CLIENT
  - SQLNET.ENCRYPTION_SERVER
  - SQLNET.ENCRYPTION_TYPES_CLIENT
  - SQLNET.ENCRYPTION_TYPES_SERVER
  - SQLNET.EXPIRE_TIME
  - SQLNET.INBOUND_CONNECT_TIMEOUT
  - SSL_CERT_REVOCATION
  - SSL_CERT_FILE
  - SSL_CERT_PATH
  - SSL_CIPHER_SUITES
  - SSL_EXTENDED_KEY_USAGE
  - SSL_SERVER_DN_MATCH
  - SSL_VERSION
  - TCP.CONNECT_TIMEOUT
  - WALLET_LOCATION

Oracle Listener Port

- Have you changed the default port of your database from 1521 to something else to thwart an attack?
- Netstat can narrow down the choices an attacker must check in a single command
- Changing the port is item 2.11 on the CIS audit but it secures nothing

```
[oracle@gg00a dirprm]$ netstat -lntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5801            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5901            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6001            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:56754           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:2208          0.0.0.0:*               LISTEN
tcp        0      0 :::47406                :::*                    LISTEN
tcp        0      0 :::1526                 :::*                    LISTEN
tcp        0      0 :::6001                 :::*                    LISTEN
tcp        0      0 :::7809                 :::*                    LISTEN
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp        0      0 0.0.0.0:627             0.0.0.0:*
udp        0      0 0.0.0.0:630             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:34070           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:45534           0.0.0.0:*
udp        0      0 :::5353                 :::*
udp        0      0 :::49517                :::*
udp        0      0 ::1:63872               :::*
udp        0      0 ::1:39693               :::*
udp        0      0 :::59798                :::*
udp        0      0 ::1:19812               :::*
```

DDOS Attack

- A Distributed Denial of Service attack can make a database unusable by flooding it with connection requests
- The connection rate limiter feature in Oracle Net Listener enables a DBA to limit the number of new connections handled by the listener
- When enabled, Oracle Net Listener imposes a user-specified maximum limit on the number of new connections handled by the listener every second. Depending on the configuration, the rate can be applied to a collection of endpoints, or to a specific endpoint

```
LISTENER=
(ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521)(RATE_LIMIT=yes))

LISTENER= (ADDRESS_LIST=
   (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521)(RATE_LIMIT=5))
   (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1522)(RATE_LIMIT=10))
   (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1523))
)
```

```
CONNECTION_RATE_LISTENER=10
  LISTENER=
     (ADDRESS_LIST=
     (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521)(RATE_LIMIT=yes))
     (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1522)(RATE_LIMIT=yes))
     (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1523)))
```

Valid Node Checking (1:2)

- 38% of breaches are performed with stolen credentials ... 86% of records stolen are from breaches with stolen credentials
- To prevent someone with a valid userid and password from gaining access enable Valid Node Checking in your SQLNET.ORA file

```
valid_node_checking_registration_listener=on

tcp.invited_nodes=(sales.meta7.com, hr.us.mlib.com, 144.185.5.73)

tcp.excluded_nodes=(blackhat.hacker.com, mktg.us.acme.com, 144.25.5.25)
```

- "Best practice" is to hard-code in the IP addresses of
  - Application servers
    - This has the added benefit of forcing the organization to communicate with the DBA team when new application servers are added
    - If a new app server is not added to the invited list it cannot connect to the database
  - Reporting servers (Business Objects, Cognos, Crystal Reports, ...)
  - Replication servers (GoldenGate, Informatica, SharePlex...)
  - DBA team members

Valid Node Checking (2:2)

Explanation	This parameter in SQLNET.ORA causes the listener to matches incoming connection requests to invited and excluded node lists. A valid user-id/password combination is only valid if it comes in from an invited and unexcluded node.
Validation	**`grep -i tcp.validnode_checking sqlnet.ora`**

Finding	Valid node checking not enabled in the current PROD environment. The QA system contains the following:
	
	`VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN3=OFF`
	`VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN2=OFF`
	`VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN1=OFF`
	`VALID_NODE_CHECKING_REGISTRATION_LISTENER = SUBNET`
	`VALID_NODE_CHECKING_REGISTRATION_MGMTLSNR=SUBNET`
	`REGISTRATION_INVITED_NODES_LISTENER_SCAN2=()`
	`REGISTRATION_INVITED_NODES_LISTENER_SCAN3=()`
	
	Which enables SUBNET level valid node checking but given that no lists are provided does not provide any security.

Action	Set **`tcp.validnode_checking=YES`** in $ORACLE_HOME/network/admin/sqlnet.ora

SEC_PROTOCOL_ERROR_TRACE_ACTION

Explanation	Specify the action a database should take when a bad packet is received. TRACE generates a detailed trace file and should only be used when debugging. ALERT or LOG should be used to capture the event. Use currently established procedures for checking console or log file data to monitor these events.
Validation	**SELECT value** **FROM v$parameter** **WHERE name = 'sec_protocol_error_trace_action';** The return value should be LOG or ALERT
Finding	VALUE ---------- TRACE
Action	**ALTER SYSTEM SET sec_protocol_error_trace_action = 'ALERT'** **COMMENT='Set to ALERT on 15-MAR-2016'** **SID='*'** **SCOPE=BOTH;**

Built-in Packages

File System Access Risks (1:5)

- The Oracle database contains a number of built-in components that can be utilized to enable reading and writing to file systems
  - Secure data can be written
  - External files can be read
- Some have execute granted to PUBLIC and the public privileges should be revoked
- What you need to secure is
  - DBMS_ADVISOR
  - DBMS_LOB
  - DBMS_SQL
  - DBMS_XSLPROCESSOR
  - UTL_FILE

- Does this look like security by default?

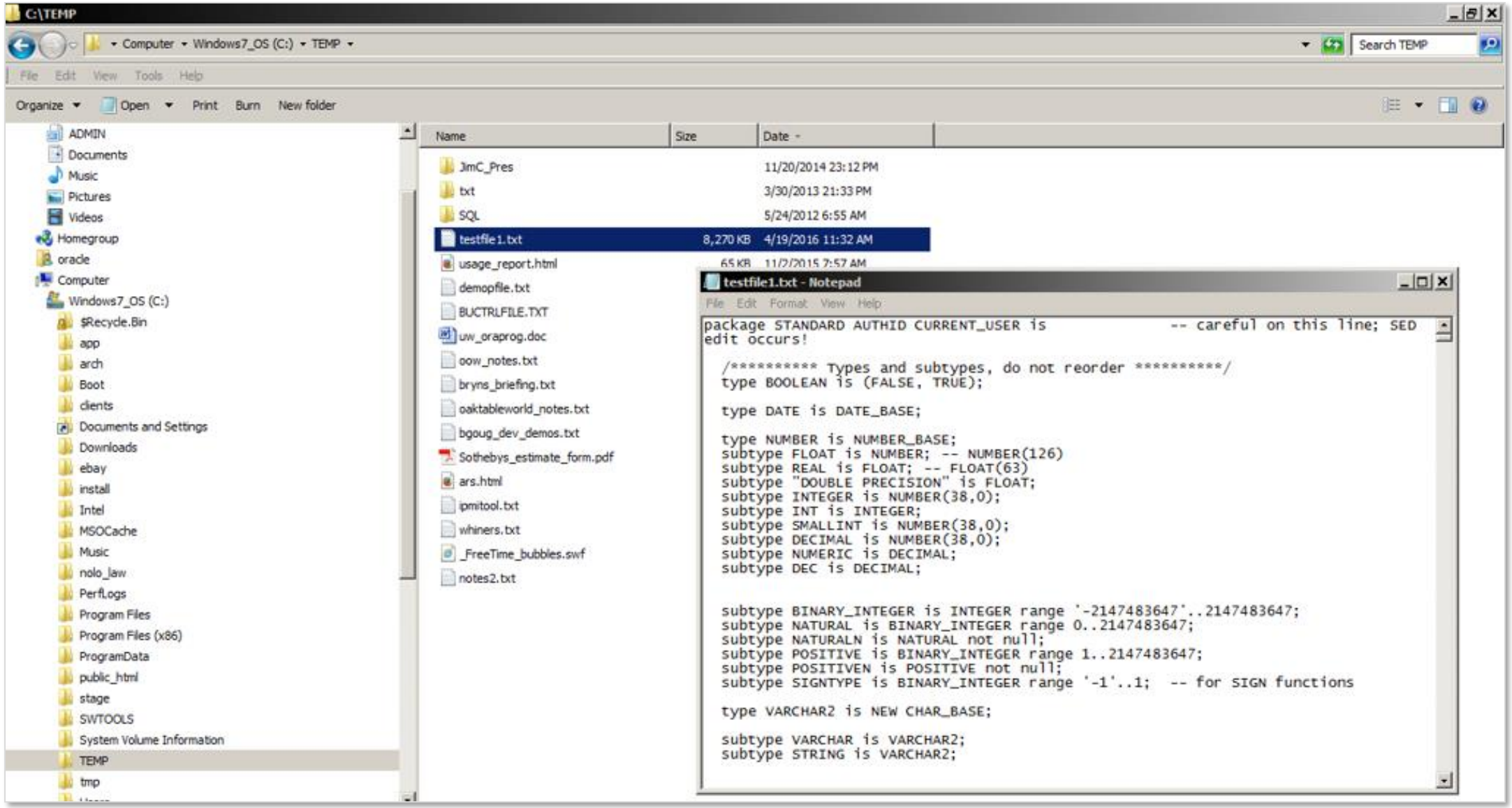
```
SQL> SELECT DISTINCT grantee, table_name AS OBJECT_NAME, privilege
  2  FROM cdb_tab_privs
  3  WHERE table_name IN ('DBMS_ADVISOR',
                          'DBMS_LOB',
                          'DBMS_SCHEDULER'
                          'DBMS_SQL',
                          'DBMS_XSLPROCESSOR',
                          'UTL_FILE')
  4  AND grantee = 'PUBLIC'
  5* ORDER BY 2;

GRANTEE  OBJECT_NAME         PRIVILEGE
-------- ------------------- -----------
PUBLIC   DBMS_ADVISOR        EXECUTE
PUBLIC   DBMS_LOB            EXECUTE
PUBLIC   DBMS_SCHEDULER      EXECUTE
PUBLIC   DBMS_SQL            EXECUTE
PUBLIC   DBMS_XSLPROCESSOR   EXECUTE
PUBLIC   UTL_FILE            EXECUTE
```

File System Access Risks (2:5)

```
SQL> conn uwclass/uwclass@pdbdev
Connected.

SQL> CREATE TABLE uwclass.t (
  2  textcol CLOB);

Table created.

SQL>
SQL> DECLARE
  2   c CLOB;
  3   CURSOR scur IS
  4   SELECT text
  5   FROM dba_source
  6   WHERE rownum < 200001;
  7  BEGIN
  8    EXECUTE IMMEDIATE 'truncate table uwclass.t';
  9    FOR srec IN scur LOOP
 10     c := c || srec.text;
 11    END LOOP;
 12    INSERT INTO uwclass.t VALUES (c);
 13    COMMIT;
 14  END;
 15  /

PL/SQL procedure successfully completed.

SQL> SELECT LENGTH(textcol) FROM uwclass.t;

LENGTH(TEXTCOL)
---------------
        8258936
```

```
SQL> set timing on
SQL> DECLARE
  2   buf CLOB;
  3  BEGIN
  4    SELECT textcol
  5    INTO buf
  6    FROM uwclass.t
  7    WHERE rownum = 1;
  8
  9    dbms_advisor.create_file(buf, 'CTEMP', 'testfile1.txt');
 10  END;
 11  /

PL/SQL procedure successfully completed.

Elapsed: 00:00:00.61
```

File System Access Risks (3:5)



File System Access Risks (4:5)

- EXTERNAL TABLES
  - The CREATE TABLE privilege grants the privilege to create external tables
  - Does this make you feel secure?
  - Maybe you don't have a directory object pointing to $ADR_HOME/trace but what directory objects exist in your database by default?

```
CREATE OR REPLACE DIRECTORY bdump AS 'c:\app\oracle\diag\rdbms\orabase\orabase\trace\';

CREATE TABLE log_table (TEXT VARCHAR2(400))
ORGANIZATION EXTERNAL (
TYPE oracle_loader
DEFAULT DIRECTORY bdump
ACCESS PARAMETERS (
  RECORDS DELIMITED BY NEWLINE
  NOBADFILE NODISCARDFILE NOLOGFILE
  FIELDS TERMINATED BY '0x0A'
  MISSING FIELD VALUES ARE NULL)
LOCATION ('alert_orabase.log'))
REJECT LIMIT unlimited;

SELECT * FROM log_table;
```

Carefully monitor use of the CREATE ANY DIRECTORY privilege

File System Access Risks (5:5)

- DBMS_SCHEDULER
  - First available in version 10gR1 file watchers became available with version 11gR2
  - A File Watcher is a program that watches for a file to be created

```
-- create job credential
exec dbms_scheduler.create_credential('uw_credential', 'uwclass', 'uwclass');

-- create program in disabled state
exec dbms_scheduler.create_program('file_watcher', 'stored_procedure', 'load_file', 1);

 -- define program argument
exec dbms_scheduler.define_metadata_argument('file_watcher', 'EVENT_MESSAGE', 1);

-- enable program
exec dbms_scheduler.enable('file_watcher');

-- create file watcher
exec dbms_scheduler.create_file_watcher('UW_FWatch', 'STAGE', 'democlob.txt', 'uw_credential');
```

Network Access Risks (1:2)

- The Oracle database contains a number of built-in components that can be utilized to enable communications to the intranet and internet
- Configure access control lists with DBMS_NETWORK_ACL_ADMIN and do not grant privileges to the following packages without strict controls
  - DBMS_NETWORK_ACL_ADMIN
  - DBMS_NETWORK_ACL_UTILITY
  - UTL_HTTP
  - UTL_INADDR
  - UTL_MAIL
  - UTL_SMTP
  - UTL_TCP

- Does this look like security by default?

```
SQL> SELECT grantee, table_name
  2  FROM cdb_tab_privs
  3  WHERE table_name IN ('DBMS_NETWORK_ACL_ADMIN',
                          'DBMS_NETWORK_ACL_UTILITY',
                          'UTL_HTTP',
                          'UTL_INADDR',
                          'UTL_MAIL',
                          'UTL_SMTP',
                          'UTL_TCP')
  4  ORDER BY 2,1;

GRANTEE                TABLE_NAME
---------------------- -----------
APEX_040200            UTL_HTTP
DBA                    DBMS_NETWORK_ACL_ADMIN
EXECUTE_CATALOG_ROLE   DBMS_NETWORK_ACL_ADMIN
PUBLIC                 DBMS_NETWORK_ACL_UTILITY
ORDPLUGINS             UTL_HTTP
PUBLIC                 UTL_HTTP
ORACLE_OCM             UTL_INADDR
PUBLIC                 UTL_INADDR
APEX_040200            UTL_SMTP
PUBLIC                 UTL_SMTP
PUBLIC                 UTL_TCP
```

Network Access Risks (2:2)

- DBMS_NETWORK_ACL_ADMIN
  - Use to create Access Control Lists
- DBMS_NETWORK_ACL_UTILITY
  - Provides the utility functions that facilitate managing network access permissions
- UTL_HTTP
  - Has been used to capture websites and their content including code, images, and video
- UTL_INADDR
  - Can be used to interrogate DNS resources
- UTL_MAIL
  - Can be used to send data out of the database
- UTL_SMTP
  - Can be used to send data out of the database
- UTL_TCP
  - Supports application communications with external TCP/IP-based servers

DBMS_NETWORK_ACL_ADM/UTILITY (1:2)

```
SQL> SELECT DECODE(
  2    dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
  3    'UWCLASS', 'connect'), 1, 'GRANTED', 0, 'DENIED', NULL) PRIVILEGE
  4  FROM DUAL;
  dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
  *
ERROR at line 2:
ORA-46114: ACL name /sys/acls/mlib-org-permissions.xml not found.

SQL> BEGIN
  2    dbms_network_acl_admin.create_acl(acl => 'mlib-org-permissions.xml',
  3    description => 'Network permissions for *.morganslibrary.org',
  4    principal => 'UWCLASS', is_grant => TRUE, privilege => 'connect');
  5  END;
  6  /

PL/SQL procedure successfully completed.

SQL> SELECT DECODE(
  2    dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
  3    'UWCLASS', 'connect'), 1, 'GRANTED', 0, 'DENIED', NULL) PRIVILEGE
  4  FROM DUAL;

PRIVILEGE
----------
GRANTED
```

DBMS_NETWORK_ACL_ADM/UTILITY (2:2)

```
SQL>  SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual;
 SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual
        *
ERROR at line 1:
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

UTL_HTTP

```
DECLARE
 req   utl_http.req;
 resp  utl_http.resp;
 value VARCHAR2(1024);
BEGIN
  req := utl_http.begin_request('http://www.morganslibrary.org');
  utl_http.set_header(req, 'User-Agent', 'Mozilla/4.0');
  resp := utl_http.get_response(req);
  LOOP
    utl_http.read_line(resp, value, TRUE);
    dbms_output.put_line(value);
  END LOOP;
  utl_http.end_response(resp);
EXCEPTION
  WHEN utl_http.end_of_body THEN
    utl_http.end_response(resp);
END;
/
```

Other Built-In Packages

DBMS_CREDENTIAL (1:2)

- First released in 12cR1 credentials are database objects that hold a username/password pair for authenticating and impersonating
  - EXTPROC callout functions
  - Remote jobs
  - External jobs
  - DBMS_SCHEDULER file watchers
- Credentials are created using the CREATE_CREDENTIAL procedure in the built-in package
- The package allows specifying the Windows domain for remote external jobs executed against a Windows server

```
SQL> SELECT DISTINCT grantee, table_name AS OBJECT_NAME, privilege
  2  FROM cdb_tab_privs
  3  WHERE table_name = 'DBMS_CREDENTIAL';

GRANTEE  OBJECT_NAME        PRIVILEGE
-------- ------------------ -----------
PUBLIC   DBMS_CREDENTIAL    EXECUTE
```

DBMS_CREDENTIAL (2:2)

```
DECLARE
 cname   user_credentials.credential_name%TYPE := 'UWCRED';
 uname   user_credentials.username%TYPE := 'UWCLASS';
 pwd     sys.scheduler$_credential.password%TYPE := 'ZzYzX6*';
 dbrole  VARCHAR2(30) := NULL;
 windom  sys.scheduler$_credential.domain%TYPE := NULL;
 comment user_credentials.comments%TYPE := 'Test Cred';
 enable  BOOLEAN := FALSE;
BEGIN
  dbms_credential.create_credential(cname, uname, pwd, dbrole, windom, comment, enable);
END;
/

SELECT * FROM scheduler$_credential;
```

Database Link Communications (1:2)

- Database Links can be a valuable productivity tool
- They can also be an attack vector
- Regularly audit existing links and creation of new links

Explanation	Database links are objects that allow creation of an almost transparent connection between databases that can be used to select, insert, update, and/or delete data.

Validation	`SELECT *`
	`FROM dba_db_links`
	`ORDER BY 1,2;`

Finding	

```
OWNER      DB_LINK                      USERNAME  HOST    CREATED
---------- ---------------------------- --------- ------- ---------
PUBLIC     EPMPRD.???.EDU               SYSADM    EPMPRD  19-APR-12
PUBLIC     FINPRD.???.EDU               SYSADM    FINPRD  10-NOV-11
PUBLIC     HRRPT.???.EDU                SYSADM    HRRPT   10-NOV-11
PUBLIC     HRTRN.???.EDU                SYSADM    HRTRN   10-NOV-11
PUBLIC     OEPRD.???.EDU                PS_READ   oeprd   07-DEC-11
PUBLIC     OUDWH.???.EDU                PS_READ   ??DWH   10-NOV-11
PUBLIC     OUPRD.???.EDU                PS_READ   ??PRD   10-NOV-11
PUBLIC     PROD.???.EDU                 PS_READ   PROD    10-NOV-11
SPOTLIGHT  QUEST_SOO_HRPRD1.???.EDU              hrprd1  02-DEC-11
SPOTLIGHT  QUEST_SOO_HRPRD2.???.EDU              hrprd2  02-DEC-11
SPOTLIGHT  QUEST_SOO_HRPRD3.???.EDU              hrprd3  02-DEC-11
```

Database Link Communications (2:2)

- DBMS_DISTRIBUTED_TRUST_ADMIN
  - First released with in 2001, contains procedures to maintain the Trusted Servers List
  - Use the package to define whether a server is trusted. If a database is not trusted, Oracle refuses current user database links from the database
    - Cannot stop PDB to PDB links in the same CDB

```
SQL> exec dbms_distributed_trust_admin.deny_all;

PL/SQL procedure successfully completed.

SQL> SELECT * FROM ku$_trlink_view;

V V NAME                           FUNCTION                                      TYPE
- - ------------------------------ ---------------------------------------- ----------
1 0 -*                             DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL            0

SQL> exec dbms_distributed_trust_admin.allow_server('BIGDOG.MLIB.ORG');

PL/SQL procedure successfully completed.

SQL> SELECT * FROM ku$_trlink_view;

V V NAME                           FUNCTION                                      TYPE
- - ------------------------------ ---------------------------------------- ----------
1 0 -*                             DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL            0
1 0 BIGDOG.MLIB.ORG                DBMS_DISTRIBUTED_TRUST_ADMIN.ALLOW_SERVER        1
```

SQL Injection

SQL Injection

- 25% of all attacks are by SQL Injection ... and 89% of all data stolen is the result of a SQL Injection attack
- If you do not know how to attack your databases ... you cannot prevent an attack?
- To prevent SQL Injection attacks
  - Use Bind Variables
  - Use DBMS_ASSERT

```
SQL> SELECT dbms_assert.sql_object_name('UWCLASS.SERVERS')
  2  FROM dual;

DBMS_ASSERT.SQL_OBJECT_NAME('UWCLASS.SERVERS')
------------------------------------------------------------
UWCLASS.SERVERS

SQL> SELECT dbms_assert.sql_object_name('UWCLASS.SERVERZ')
  2  FROM dual;
SELECT dbms_assert.sql_object_name('UWCLASS.SERVERZ')
       *
ERROR at line 1:
ORA-44002: invalid object name
ORA-06512: at "SYS.DBMS_ASSERT", line 383
```

Miscellaneous Topics

ACCESSIBLE BY Clause

- Used in PL/SQL to control access within a schema so packages, procedures, and functions can only be executed by specifically named objects

```
CREATE OR REPLACE FUNCTION test_src RETURN PLS_INTEGER
ACCESSIBLE BY (FUNCTION test_yes) AUTHID DEFINER IS
BEGIN
  RETURN 42;
END test_src;
/

CREATE OR REPLACE FUNCTION test_yes RETURN PLS_INTEGER AUTHID
DEFINER IS
BEGIN
  RETURN test_src;
END test_yes;
/

CREATE OR REPLACE FUNCTION test_no RETURN PLS_INTEGER AUTHID DEFINER
IS
BEGIN
  RETURN test_src;
END test_no;
/

Warning: Function created with compilation errors.

SQL> show err
Errors for FUNCTION TEST_NO:

LINE/COL ERROR
-------- ------
3/3      PL/SQL: Statement ignored
3/10     PLS-00904: insufficient privilege to access object TEST_SRC
```

Encryption & Hashing

- In the database you can implement many different types of encryption: Each one optimized for a specific purpose some of which require extra licensing such as TDE
  - DBMS_CRYPTO
  - STANDARD_HASH
- Encryption is of limited value unless executed by the application before the values get to the database

```
SQL> DECLARE
  2   enc_val   RAW(2000);
  3   l_key     RAW(2000);
  4   l_key_len NUMBER := 128/8; -- convert bits to bytes
  5   l_mod     NUMBER := dbms_crypto.ENCRYPT_AES128+dbms_crypto.CHAIN_CBC+dbms_crypto.PAD_ZERO;
  6  BEGIN
  7    l_key := dbms_crypto.randombytes(l_key_len);
  8    enc_val := dbms_crypto.encrypt(utl_i18n.string_to_raw('4114-0113-1518-7114', 'AL32UTF8'), l_mod, l_key);
  9    dbms_output.put_line(enc_val);
 10  END;
 11  /
3DBA29959C45EE0E54B5BE6F2304BC1CFB2FFACA2D44A43A2C1E071E2ACA98D7

PL/SQL procedure successfully completed.
```

Operating System Configuration

- As a server boots it needs to know the mapping of some hostnames to IP addresses before DNS can be referenced
- The mapping is kept in the `/etc/hosts` file
- In the absence of a name server, a network program on your system consults this file to determine the IP address that corresponds to a host name
- Be sure that the file does not contain any mappings that are not essential ... unnecessary mappings compromise security

```
# Do not remove the following line, or various programs that require network functionality will fail.
 ::1 localhost6.localdomain6 localhost6

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.16 orclsys-scan.example.com orclsys-scan

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan

192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan

# Following added by OneCommand
127.0.0.1 localhost.localdomain localhost

# PUBLIC HOSTNAMES

# PRIVATE HOSTNAMES
192.168.16.24 orclsys1-priv0.example.com orclsys1-priv0
192.168.16.25 orclsys2-priv0.example.com orclsys2-priv0
192.168.17.24 orclsys1-priv1.example.com orclsys1-priv1
192.168.17.25 orclsys2-priv1.example.com orclsys2-priv1

# VIP HOSTNAMES
192.0.2.20 orclsys1-vip.example.com orclsys1-vip
192.0.2.21 orclsys2-vip.example.com orclsys2-vip

# NET(0-3) HOSTNAMES
192.0.2.18 orclsys1.example.com orclsys1
192.0.2.19 orclsys2.example.com orclsys2

#SCAN IP
192.0.2.22 orclsys-scan.example.com orclsys-scan
```

Patching: A Risk Hiding In Plain Sight

Recyclebin

- Tables contain data and when tables are dropped, unless the PURGE keyword is used, the table and its indexes remain queryable and recoverable in the recyclebin
- Always drop table with PURGE
  `drop table <table_name> PURGE;`

```
SQL> CREATE TABLE dropme (soc_sec_no VARCHAR2(11));

SQL> INSERT INTO dropme (soc_sec_no)
  2  VALUES ('523-14-0963');

SQL> COMMIT;

SQL> DROP TABLE dropme;

SQL> SELECT object_name, original_name, type, related, base_object
  2  FROM user_recyclebin;

SQL> SELECT * FROM "BIN$eVwc/lghQwq9QkrmYD1vRg==$0";

SQL> FLASHBACK TABLE dropme TO BEFORE DROP;

SQL> desc dropme

SQL> SELECT * FROM dropme;
```

Startup Initialization Parameters

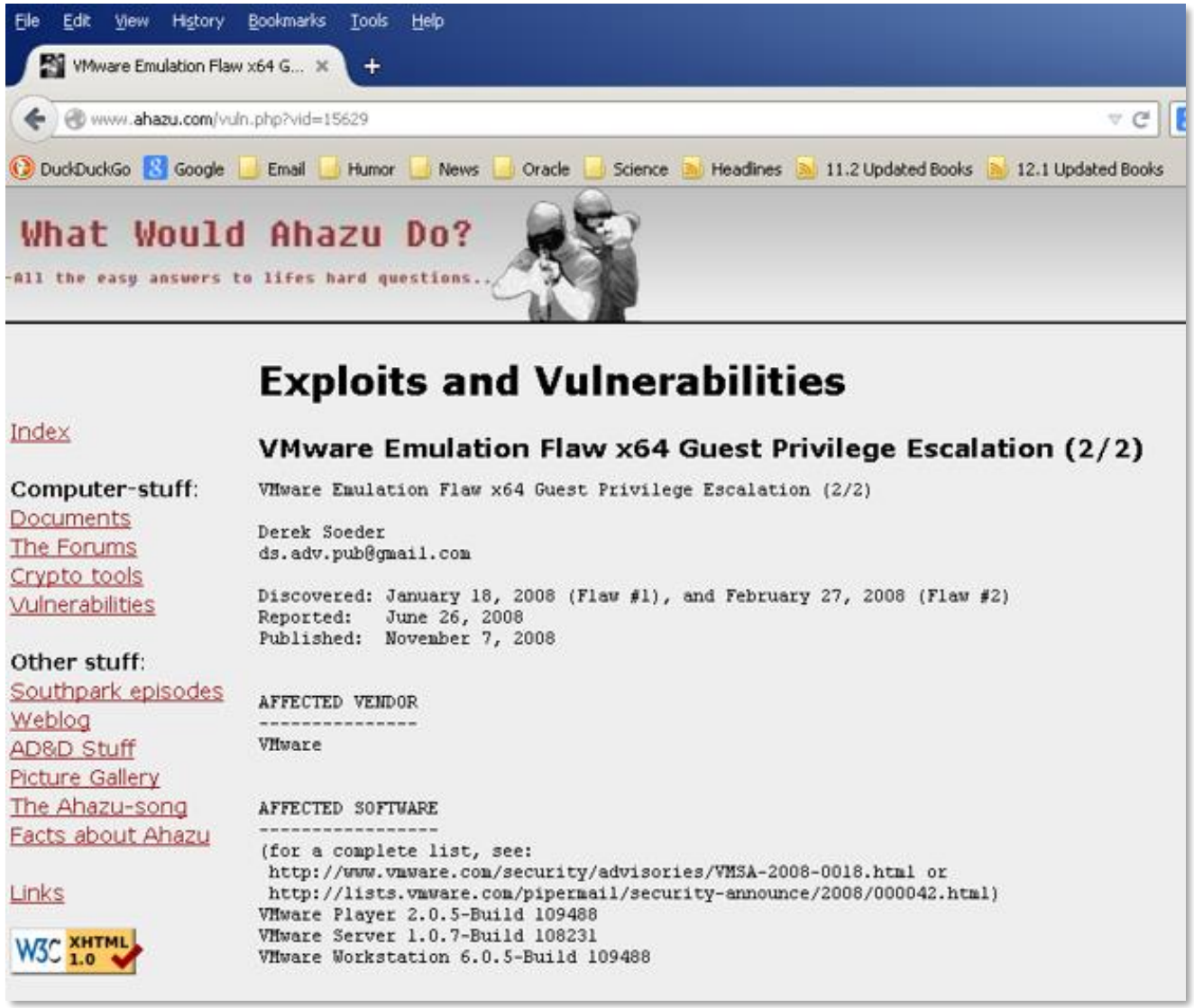
- There are a number of init.ora/spfile parameters that can contribute to creating a more secure environment
  - O7_DICTIONARY_ACCESSIBILITY
  - LDAP_DIRECTORY_ACCESS
  - LDAP_DIRECTORY_SYSAUTH
  - OS_AUTHENT_PREFIX
  - OS_ROLES
  - REMOTE_LISTENER
  - REMOTE_LOGIN_PASSWORDFILE
  - REMOTE_OS_ROLES
  - SEC_CASE_SENSITIVE_LOGON
  - SEC_MAX_FAILED_LOGIN_ATTEMPTS
  - SEC_PROTOCOL_ERROR_FURTHER_ACTION
  - SEC_PROTOCOL_ERROR_TRACE_ACTION
  - SEC_RETURN_SERVER_RELEASE_BANNER
  - SQL92_SECURITY

Storage

- The following are all locations commonly used to store data assets or information that can be used to compromise access to those assets
  - Data Files (both file systems and ASM)
  - Standby Databases
  - Archived redo logs
  - On-site Backups
  - Courier shipments
  - Exports
  - RMAN scripts
  - Data Pump export and import scripts
  - Shell scripts and cron jobs
  - Replication tools such as GoldenGate, ODI, Informatica
  - Used storage drives
  - The entire $ORACLE_BASE file system
    - /rdbms/admin directory
    - Trace files

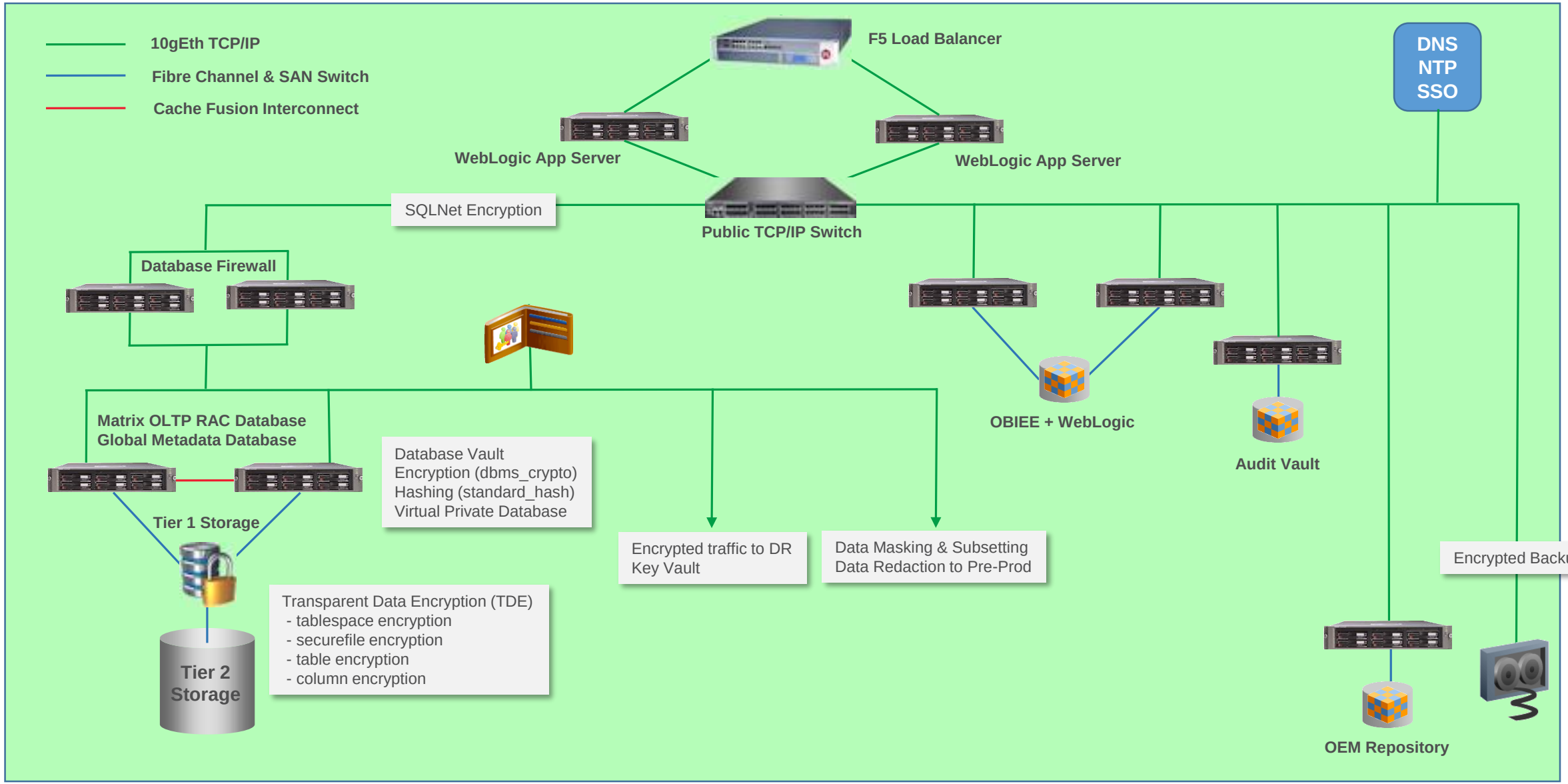
Virtual Machines

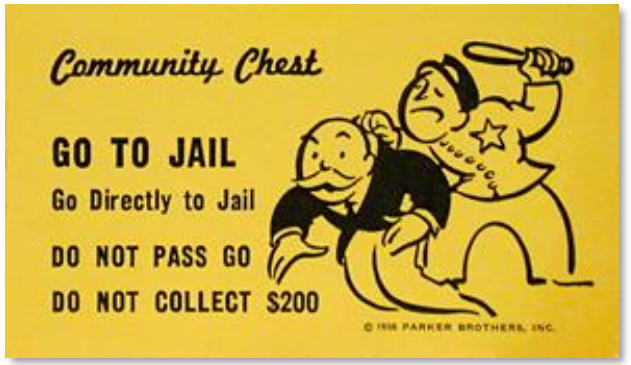
- Virtual machines are not more secure than any other operating environment
  - Implement regular password changes as a matter of policy and procedure
  - Force password complexity
  - Track the names of all persons with access to the password
  - Determine whether ESXi Credentials in use and if not implement them
  - Regularly review logs that live, by default, in the vmdk hypervisor



A Case Study

Matrix Minimum Environment (1:2)




Community Chest
GO TO JAIL
Go Directly to Jail
DO NOT PASS GO
DO NOT COLLECT $200
© 1936 PARKER BROTHERS, INC.

Wrap Up

Both Of These This Train Wrecks Were Avoidable

```
DIR=/opt/oracle/scripts
. /home/oracle/.profile_db

DB_NAME=hrrpt
ORACLE_SID=$DB_NAME"1"
export ORACLE_SID

SPFILE=`more $ORACLE_HOME/dbs/init$ORACLE_SID.ora | grep -i spfile`
PFILE=$ORACLE_BASE/admin/$DB_NAME/pfile/init$ORACLE_SID.ora
LOG=$DIR/refresh_$DB_NAME.log
RMAN_LOG=$DIR/refresh_$DB_NAME"_rman".log

PRD_PWD=sys_pspr0d
PRD_SID=hrprd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrprd/rman_bk
SEQUENCE=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $5 }'`
THREAD=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $4 }'`

BK_DIR=/backup/$DB_NAME/rman_bk
EXPDIR=/backup/$DB_NAME/exp
DMPFILE=$EXPDIR/exp_sec.dmp
IMPLOG=$EXPDIR/imp_sec.log
EXPLOG=$EXPDIR/exp_sec.log
EXP_PARFILE=$DIR/exp_rpt.par
IMP_PARFILE=$DIR/imp_rpt.par

uname=rman_pshrprd
pwd=pspr0d11

rman target sys/$PRD_PWD@$PRD_SID catalog $PRD_R_UNAME/$PRD_R_PWD@catdb auxiliary / << EOF > $RMAN_LOG
  run{
     set until $SEQUENCE $THREAD;
     ALLOCATE AUXILIARY CHANNEL aux2 DEVICE TYPE DISK;
     duplicate target database to $DB_NAME;
  }
EOF
```

Conclusions (1:2)

- Securing the Perimeter has proven that its primary value is to companies selling products that claim to secure the perimeter
- Auditing is not security
- Passing audits is not security
- What is wrong with the way our industry views security is that we must secure data not software
  - Oracle is generic software
  - We build our own database structure/layout/design
  - We build our own applications (APEX, JAVA, JavaScript, C#, Python, C++, PHP, Ruby)
  - We must also build our own security
  - Security is not done well or forgotten in the rush implement features and performance
  - Our focus, for years, has been on hardening not securing
- To begin securing data we must utilize the Oracle Database's built-in features
- To fully secure data we must utilize additional tools many of which Oracle makes available and fully integrates into the Red Stack

Conclusions (2:2)

- It is difficult to dig yourself out of a hole after the sides have fallen in
- Very few organizations have employees with the skill set required to secure their databases and broader Oracle environments: Less than 1% of DBA "training" involves security

```
*
ERROR at line 1:
ORA-00028: your session has been killed
```

Thank you