SPOUG SPAIN ORACLE USERS GROUP
KNOWLEDGE | NETWORKING | INFLUENCE
Unica asociación de usuarios en España reconocida por Oracle

Oracle Security for DBAs and Developers

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

25 September 2018

Unsafe Harbor Statement

- 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 am going to say
- No one from Oracle has supplied any of my materials
- Everything I present is existing, proven, functionality

Introduction

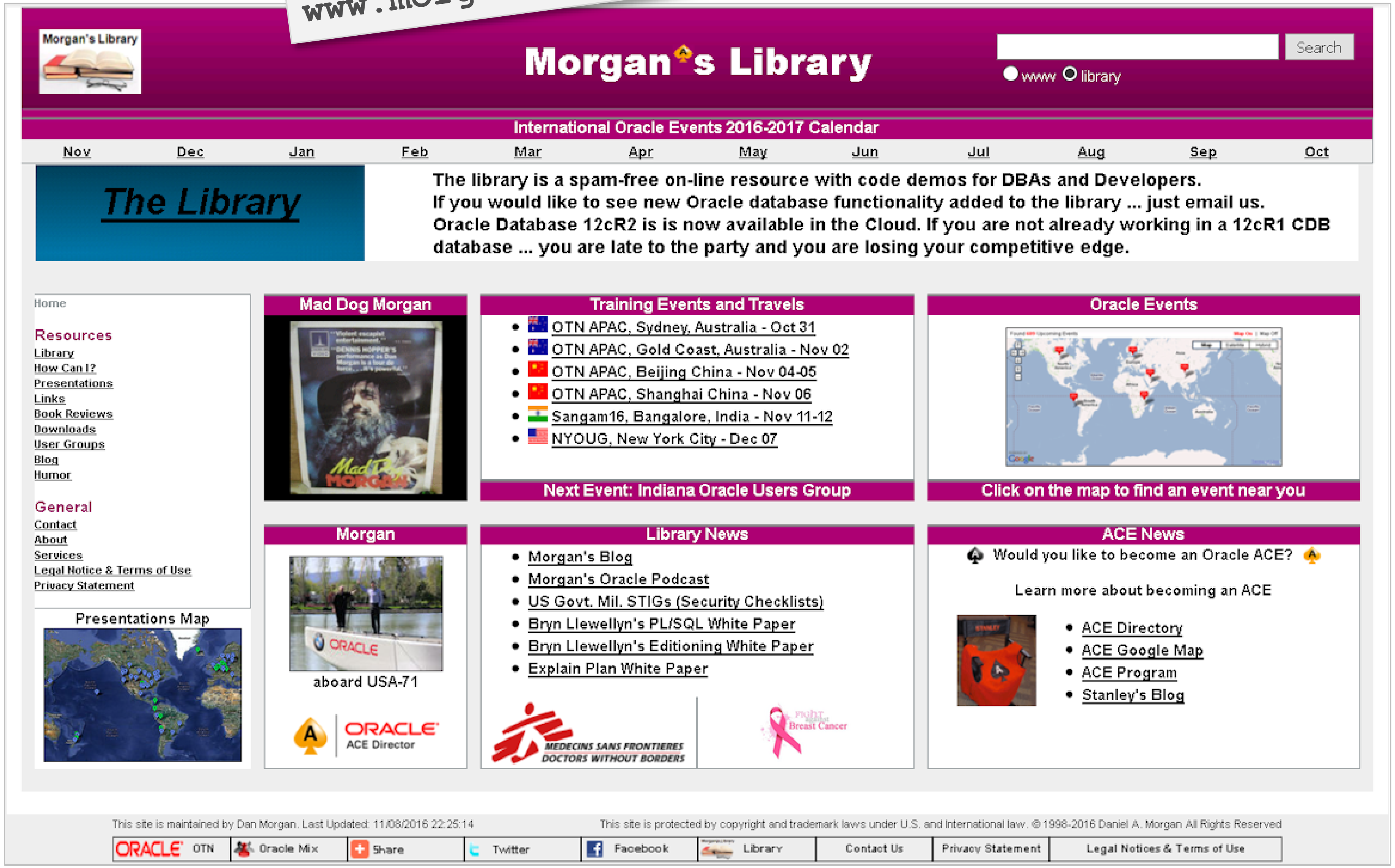
damorgan18c@dbsecworx.com

- Managing Director: Morgan's Library
- Oracle ACE Director Alumni
- Oracle Educator
  - Adjunct Professor, University of Washington, Oracle Program, 1998-2009
  - Consultant: Harvard University
  - Guest lecturer at universities in Canada, Chile, Costa Rica, New Zealand, Norway, Panama
  - Frequent lecturer at Oracle conferences … 130 countries (41 unique) since 2008
- IT Professional
  - 2019 will be my 50th year in IT
  - First computer: IBM 360/40 in 1969: Fortran IV
  - Oracle Database since 1988-9 and Oracle Beta tester
  - The Morgan behind www.morganslibrary.org
  - Member Oracle Data Integration Solutions Partner Advisory Council

System/370-145 system console

My Website

www.morganslibrary.org



Morgan's Library

Search
○ www ○ library

International Oracle Events 2016-2017 Calendar

Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct

The Library

The library is a spam-free on-line resource with code demos for DBAs and Developers.
If you would like to see new Oracle database functionality added to the library ... just email us.
Oracle Database 12cR2 is is now available in the Cloud. If you are not already working in a 12cR1 CDB database ... you are late to the party and you are losing your competitive edge.

Home

Resources
- Library
- How Can I?
- Presentations
- Links
- Book Reviews
- Downloads
- User Groups
- Blog
- Humor

General
- Contact
- About
- Services
- Legal Notice & Terms of Use
- Privacy Statement

Presentations Map

Mad Dog Morgan

Training Events and Travels
- OTN APAC, Sydney, Australia - Oct 31
- OTN APAC, Gold Coast, Australia - Nov 02
- OTN APAC, Beijing China - Nov 04-05
- OTN APAC, Shanghai China - Nov 06
- Sangam16, Bangalore, India - Nov 11-12
- NYOUG, New York City - Dec 07

Next Event: Indiana Oracle Users Group

Oracle Events

Click on the map to find an event near you

Morgan

aboard USA-71

ORACLE ACE Director

Library News
- Morgan's Blog
- Morgan's Oracle Podcast
- US Govt. Mil. STIGs (Security Checklists)
- Bryn Llewellyn's PL/SQL White Paper
- Bryn Llewellyn's Editioning White Paper
- Explain Plan White Paper

MEDECINS SANS FRONTIERES DOCTORS WITHOUT BORDERS

Fight Breast Cancer

ACE News

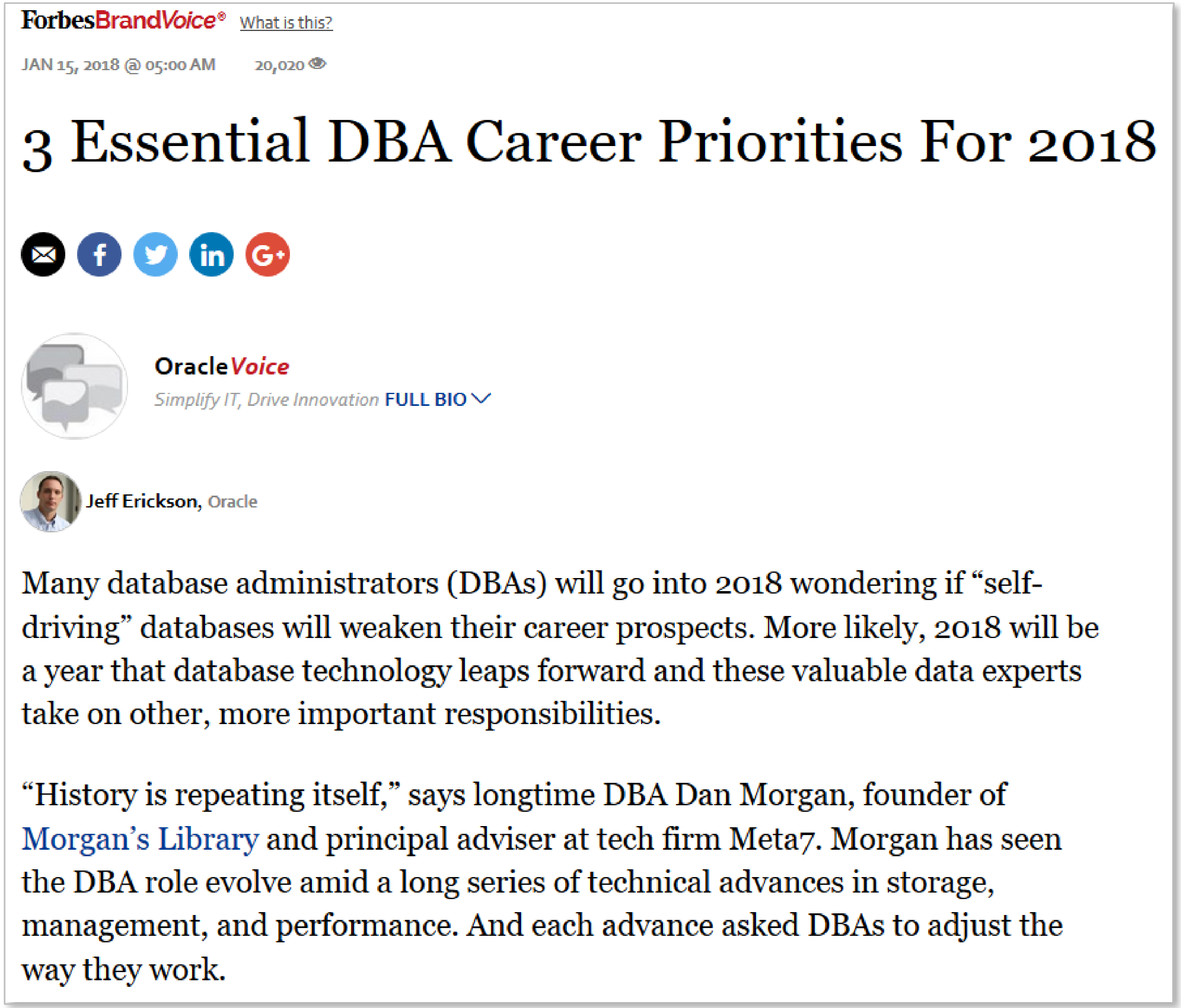
Would you like to become an Oracle ACE?

Learn more about becoming an ACE
- ACE Directory
- ACE Google Map
- ACE Program
- Stanley's Blog

This site is maintained by Dan Morgan. Last Updated: 11/08/2016 22:25:14 This site is protected by copyright and trademark laws under U.S. and International law. © 1998-2016 Daniel A. Morgan All Rights Reserved

ORACLE OTN | Oracle Mix | Share | Twitter | Facebook | Library | Contact Us | Privacy Statement | Legal Notices & Terms of Use

Forbes Magazine 2018



ForbesBrandVoice® What is this?

JAN 15, 2018 @ 05:00 AM 20,020 👁

3 Essential DBA Career Priorities For 2018

OracleVoice
Simplify IT, Drive Innovation FULL BIO

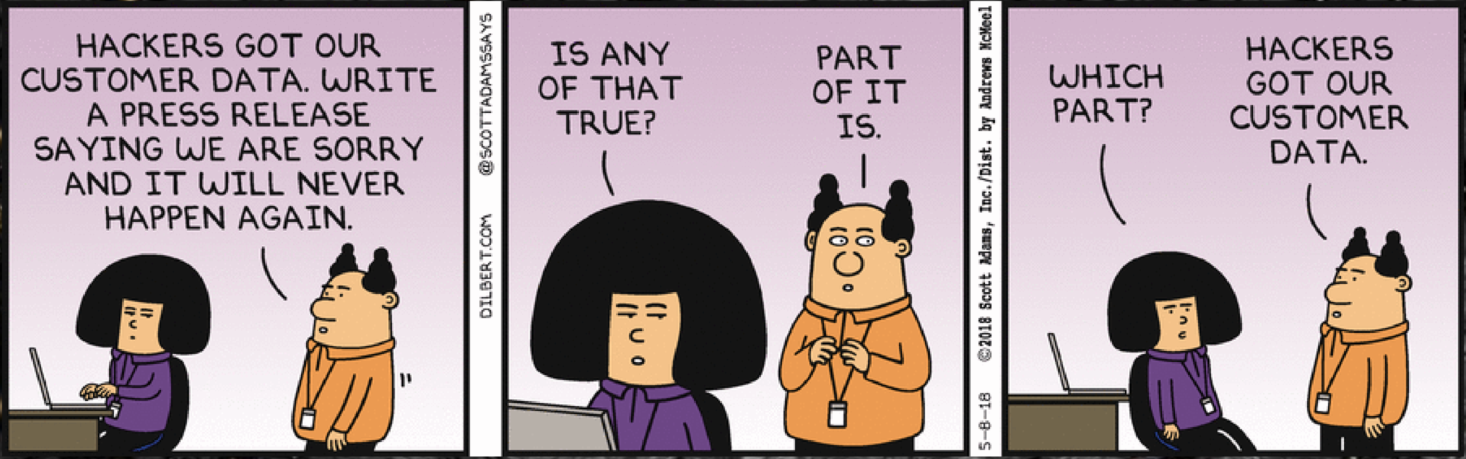
Jeff Erickson, Oracle

Many database administrators (DBAs) will go into 2018 wondering if "self-driving" databases will weaken their career prospects. More likely, 2018 will be a year that database technology leaps forward and these valuable data experts take on other, more important responsibilities.

"History is repeating itself," says longtime DBA Dan Morgan, founder of Morgan's Library and principal adviser at tech firm Meta7. Morgan has seen the DBA role evolve amid a long series of technical advances in storage, management, and performance. And each advance asked DBAs to adjust the way they work.

Travel Log: Chile 2010

Travel Log: Ecuador 2014


HACKERS GOT OUR CUSTOMER DATA. WRITE A PRESS RELEASE SAYING WE ARE SORRY AND IT WILL NEVER HAPPEN AGAIN.
DILBERT.COM
@SCOTTADAMSSAYS
IS ANY OF THAT TRUE?
PART OF IT IS.
5-8-18
© 2018 Scott Adams, Inc./Dist. by Andrews McMeel
WHICH PART?
HACKERS GOT OUR CUSTOMER DATA.

Introduction to Security

Why Am I Focusing On Oracle Database Security?

- Because OEM's, like Oracle, talk about their products not about security
- Because most organizations spend/waste their money on perimeter defense
- Because no one teaches operational security to
  - Application Admins
  - Network Admins
  - Storage Admins
  - System Admins
  - DBAs
  - Developers
  - IT Management
- Because most of what is implemented can be by-passed within minutes

  ... which is obvious given the number of systems broken into every day
- Because we are all under attack!

Security Training

- Show of hands please
  1. Has your current employer provided you with a Oracle Databases security training?
  2. Has your current employer paid for you to take formal security training?
  3. Does your current employer have a document that states security criteria that must be followed for your organization's Oracle databases?
  4. If so: Is it followed?
  5. Has anyone ever lost their job for violating it?
  6. Has any employer in your entire career provided you with training or a formally published security document specific to Oracle databases?
  7. Is the total extent of your personal on-the-job security training someone telling you not to open emails from Nigerian royalty offering you millions of dollars?
  8. Have you ever heard of any training where an employer could send you to receive training on how to secure an Oracle Database?

```
No, No, No, No, No, No, Yes, No
```

The 99:01 Rule

- Forget the 80:20 rule
- 99% of the efforts of the organizations we work for focus on passing audits
- 99% of the money spent on security focuses on
  - Compliance with government and industry regulations
  - Meeting contractually agreed-to terms
  - Auditing which is NOT security and is essentially irrelevant to security

General Data Protection Regulation

Office of the Privacy Commissioner of Canada

- Everyone in this room can name dozens of organizations broken into recently

Office of Personnel Management

Equifax

Experian

Uber

Yahoo

Sony

Verizon

Deep Root Analytics

SWIFT

Intercontinental Hotels

- Every one of them ... EVERYONE ... passed their audits

From A Security Standpoint This Is All Irrelevant Distraction

AMERICAS

- Sarbanes Oxley
- HIPAA
- PCI
- FDA CFR 21 Part 11
- OMB Circular A-123
- SEC and DoD Records Retention
- DFARS
- USA Patriot Act
- Gramm-Leach-Bliley Act
- Federal Sentencing Guidelines
- Foreign Corrupt Practices Act
- Market Instruments 52 (Canada)

EMEA

- EU Privacy Directives
- UK Companies Law
- GDPR

APAC

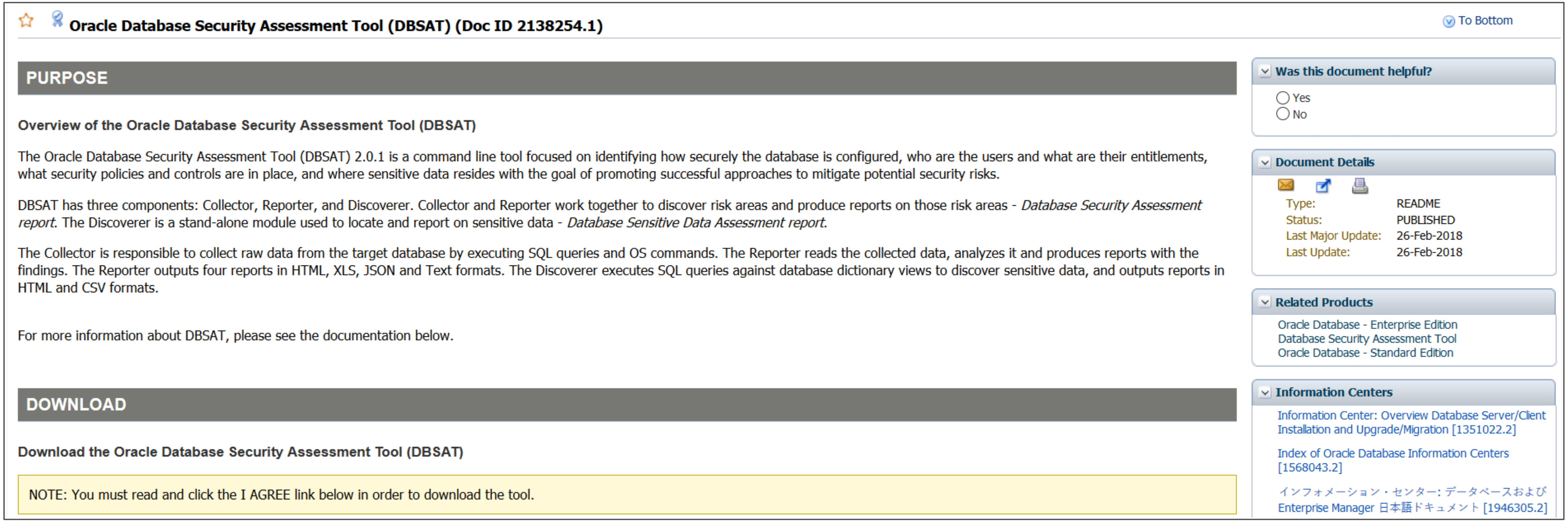
- J-SOX (Japan)
- CLERP 9: Audit Reform and Corporate Disclosure Act (Australia)
- Stock Exchange of Thailand Code on Corporate Governance

GLOBAL

- International Accounting Standards
- Basel II (Global Banking)
- OECD Guidelines on Corporate Governance

We Are Often Misdirected By Our Suppliers and Vendors

- A great tool for selling Data Masking, Data Redaction, and Advanced Security Option
- Not so great at doing what its title says it does



Oracle Database Security Assessment Tool (DBSAT) (Doc ID 2138254.1)

PURPOSE

Overview of the Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool (DBSAT) 2.0.1 is a command line tool focused on identifying how securely the database is configured, who are the users and what are their entitlements, what security policies and controls are in place, and where sensitive data resides with the goal of promoting successful approaches to mitigate potential security risks.

DBSAT has three components: Collector, Reporter, and Discoverer. Collector and Reporter work together to discover risk areas and produce reports on those risk areas - *Database Security Assessment report*. The Discoverer is a stand-alone module used to locate and report on sensitive data - *Database Sensitive Data Assessment report.*

The Collector is responsible to collect raw data from the target database by executing SQL queries and OS commands. The Reporter reads the collected data, analyzes it and produces reports with the findings. The Reporter outputs four reports in HTML, XLS, JSON and Text formats. The Discoverer executes SQL queries against database dictionary views to discover sensitive data, and outputs reports in HTML and CSV formats.

For more information about DBSAT, please see the documentation below.

DOWNLOAD

Download the Oracle Database Security Assessment Tool (DBSAT)

NOTE: You must read and click the I AGREE link below in order to download the tool.

Was this document helpful?

○ Yes
○ No

Document Details

Type:	README
Status:	PUBLISHED
Last Major Update:	26-Feb-2018
Last Update:	26-Feb-2018

Related Products

Oracle Database - Enterprise Edition
Database Security Assessment Tool
Oracle Database - Standard Edition

Information Centers

Information Center: Overview Database Server/Client Installation and Upgrade/Migration [1351022.2]

Index of Oracle Database Information Centers [1568043.2]

インフォメーション・センター: データベースおよび Enterprise Manager 日本語ドキュメント [1946305.2]

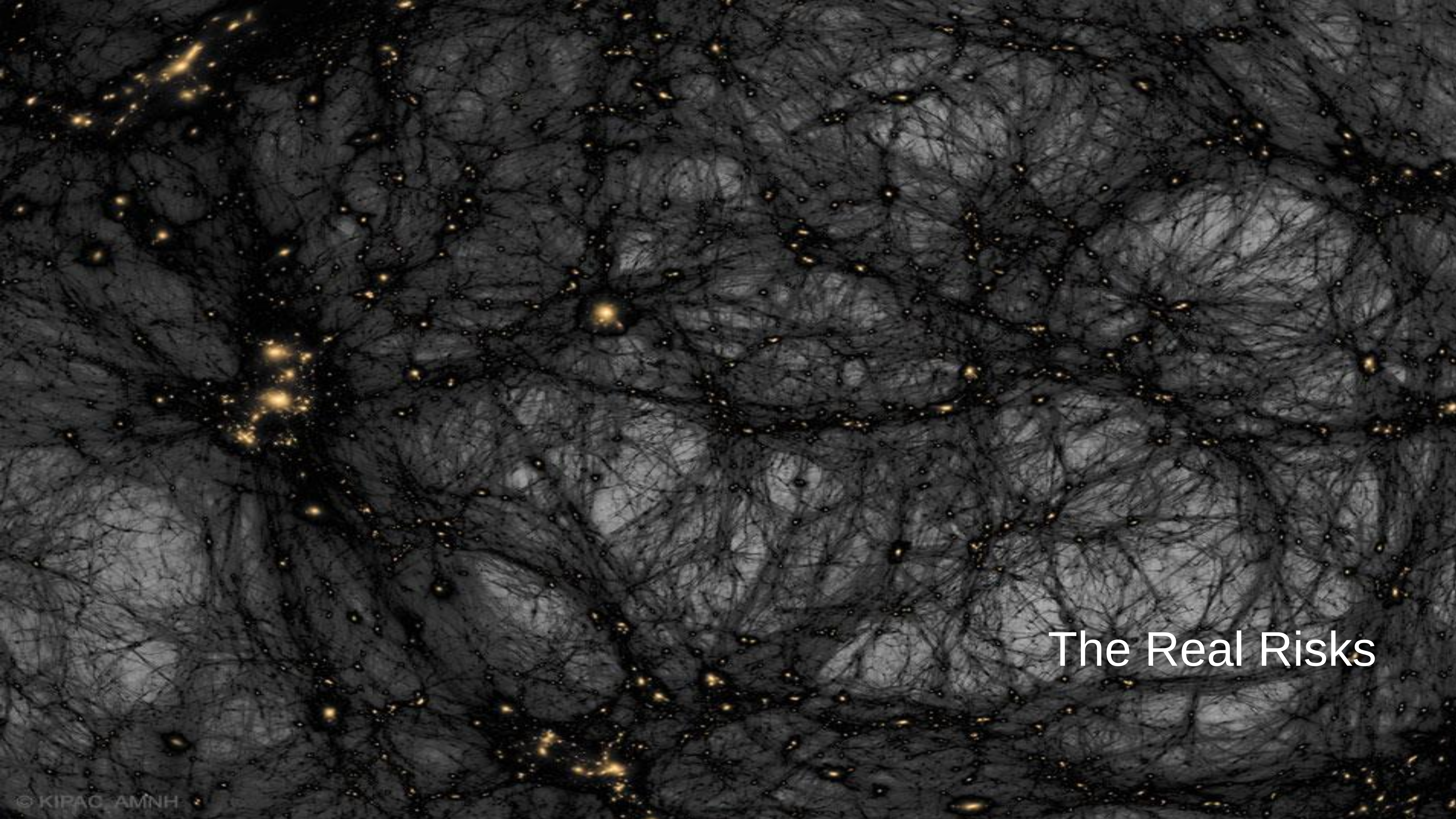
An Unpleasant Fact

- Governance is NOT security
- Auditing is NOT security
- Compliance is NOT security
- The overwhelming majority of encryption is NOT security

- In all of the news reports about all of the break-ins and data thefts
- Have you ever heard or seen the following announcement?

> Computers belonging to [company_name] was broken into, data on [###] billions of credit cards was stolen and it has been found that the company did not pass its compliance audits?

- You likely never will
- Essentially everyone passes every audit

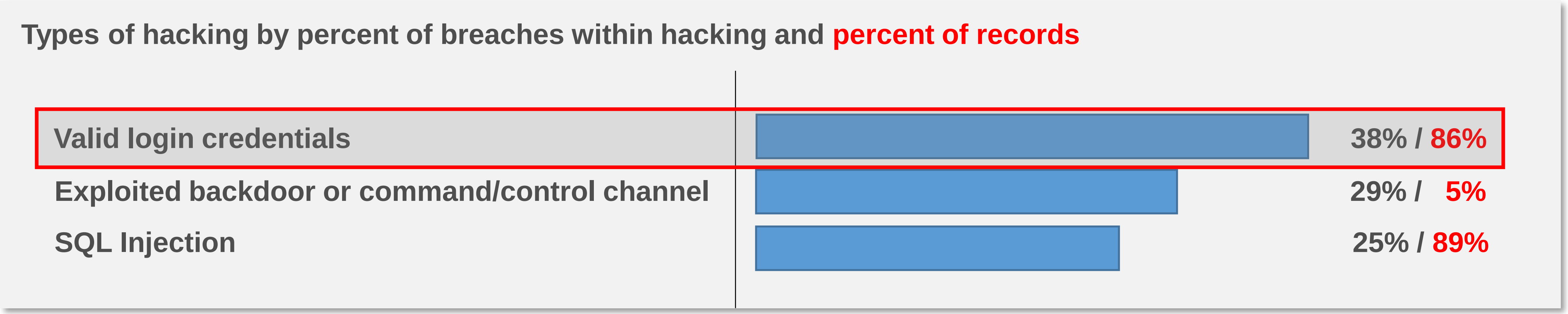


The Real Risks

© KIPAC, AMNH

How Database Breaches Really Occur

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



Types of hacking by percent of breaches within hacking and percent of records

- 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

Internal vs. External Threats

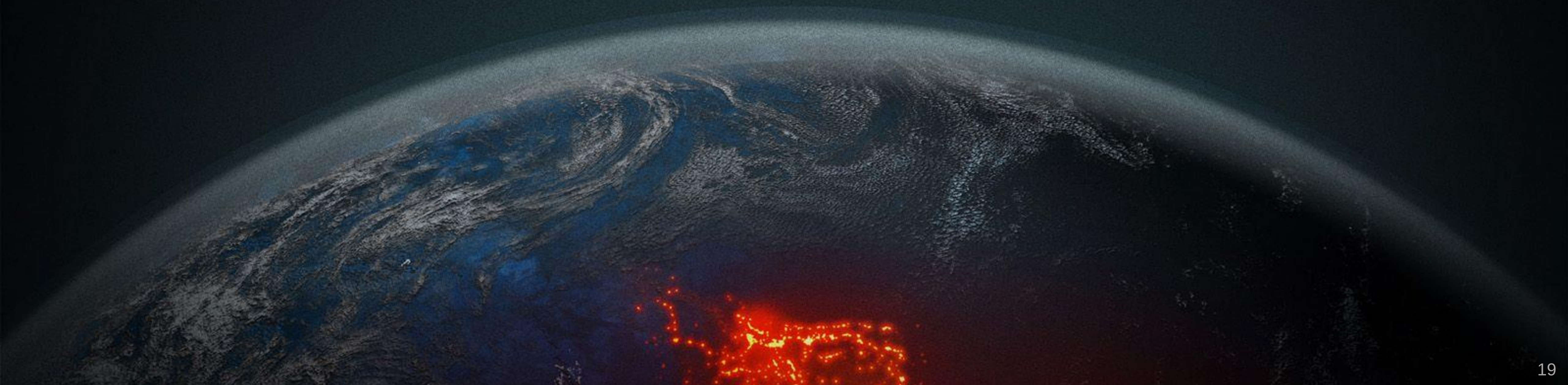
- Most organizations focus on the least likely threats and ignore what has been historically proven to be the greatest threat
- The following is quoted from "Reference for Business" on the subject of computer crimes

> **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.**

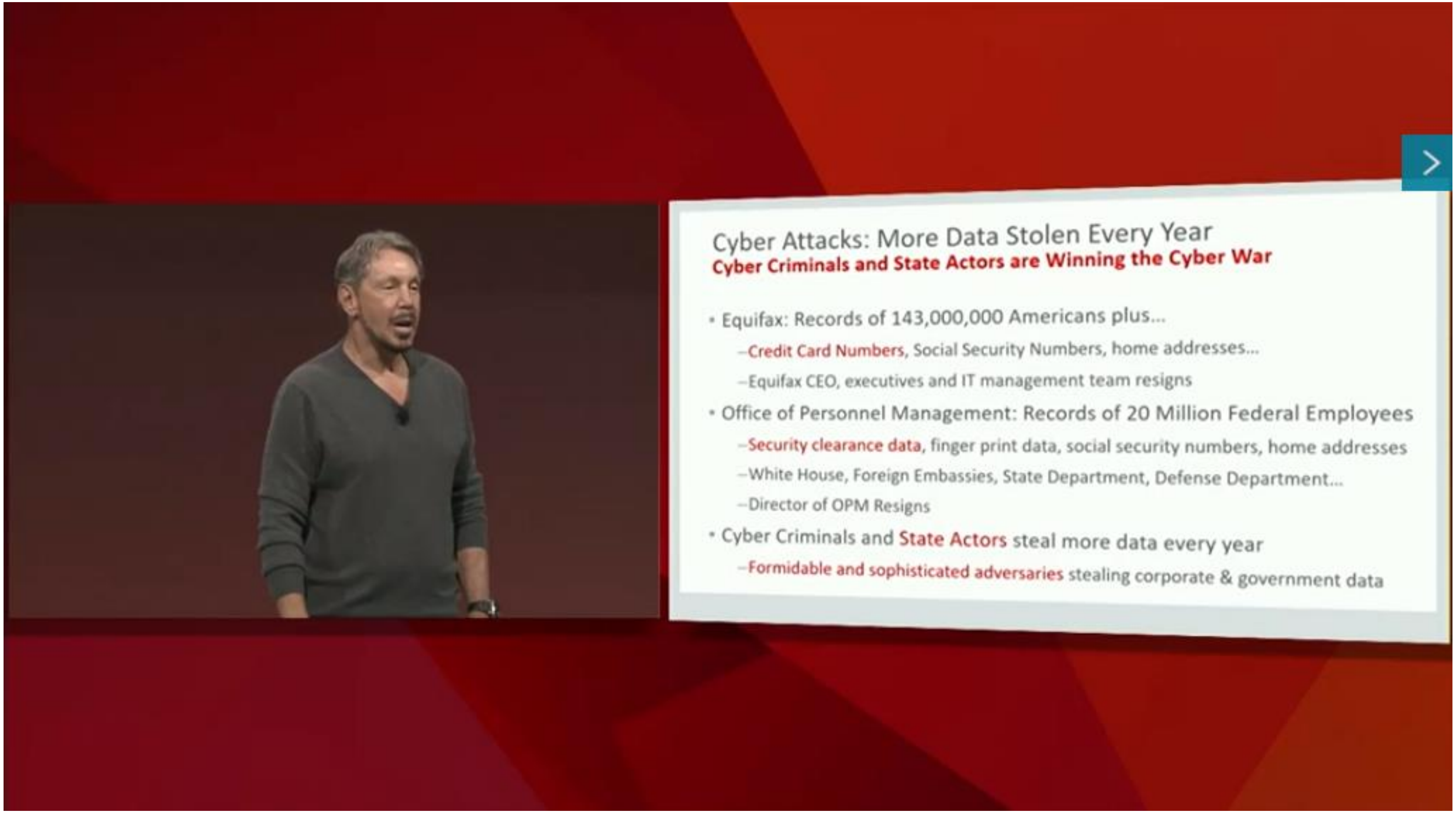
- When organizations focus on their firewall they are focusing on what is often the most expensive, yet least effective, protection against data theft
- Part of our job is to provide solutions that address vulnerabilities and minimize our organization's risk exposure
- The other part is to be educators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

CYBER WAR

A conflict without foot soldiers, guns, or missiles



Oracle Management & Security Cloud (1:2)



Cyber Attacks: More Data Stolen Every Year

Cyber Criminals and State Actors are Winning the Cyber War

- Equifax: Records of 143,000,000 Americans plus...
  - –Credit Card Numbers, Social Security Numbers, home addresses...
  - –Equifax CEO, executives and IT management team resigns
- Office of Personnel Management: Records of 20 Million Federal Employees
  - –Security clearance data, finger print data, social security numbers, home addresses
  - –White House, Foreign Embassies, State Department, Defense Department...
  - –Director of OPM Resigns
- Cyber Criminals and State Actors steal more data every year
  - –Formidable and sophisticated adversaries stealing corporate & government data

Oracle Management & Security Cloud (2:2)

Modern Cyber Security Requires More Automation

Cyber Defense: Our People versus Their Computers

- Most Data Thefts Occur After Security Fix Available
  - –Target did not detect the attack
  - –Target behind in applying security patches
    - Wrong priorities
    - Waiting for downtime window

It Must Be "Our Computers" vs "Their Computers"

Anyone want to play chess with Deep Blue?

Anyone want to take a shot at AlphaGo?

The Threat Map

The threat is not a bunch of 20 year old script kiddies

If the threat is an organized crime family you will find your data being sold on the dark web

If the threat is a nation-state you will find your data being used to attack your country, your community, your family

From The Standpoint Of Security: This Is Our Future

Database Risks

- Most databases break-ins are never detected and never reported
- What you hear about is the part of the iceberg above the water
- 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 and privilege escalation
  - Access to Oracle built-in packages
  - SQL Injection attacks

A Dose Of DBA Reality (1:4)

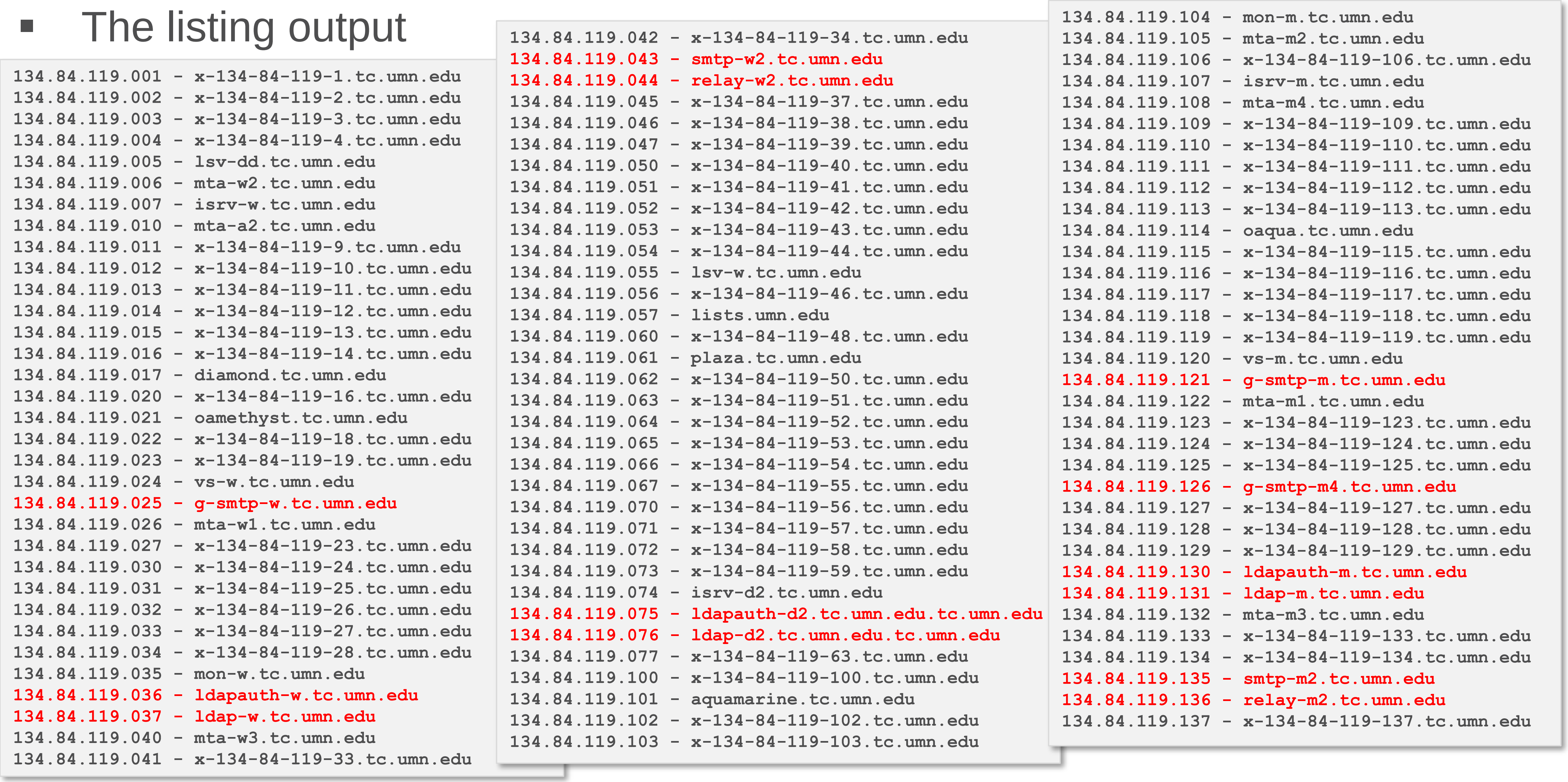
```
SQL> select utl_inaddr.get_host_address('www.umn.edu') from dual;

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 (2:4)

- 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
```

A Dose Of DBA Reality (3:4)

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

UTL_INADDR.GET_HOST_ADDRESS('WWW.UTAH.EDU')
-------------------------------------------
155.97.137.55

SQL> select utl_inaddr.get_host_name('155.97.137.55') from dual;

UTL_INADDR.GET_HOST_NAME('155.97.137.55')
-------------------------------------------
test.www.utah.edu
```

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

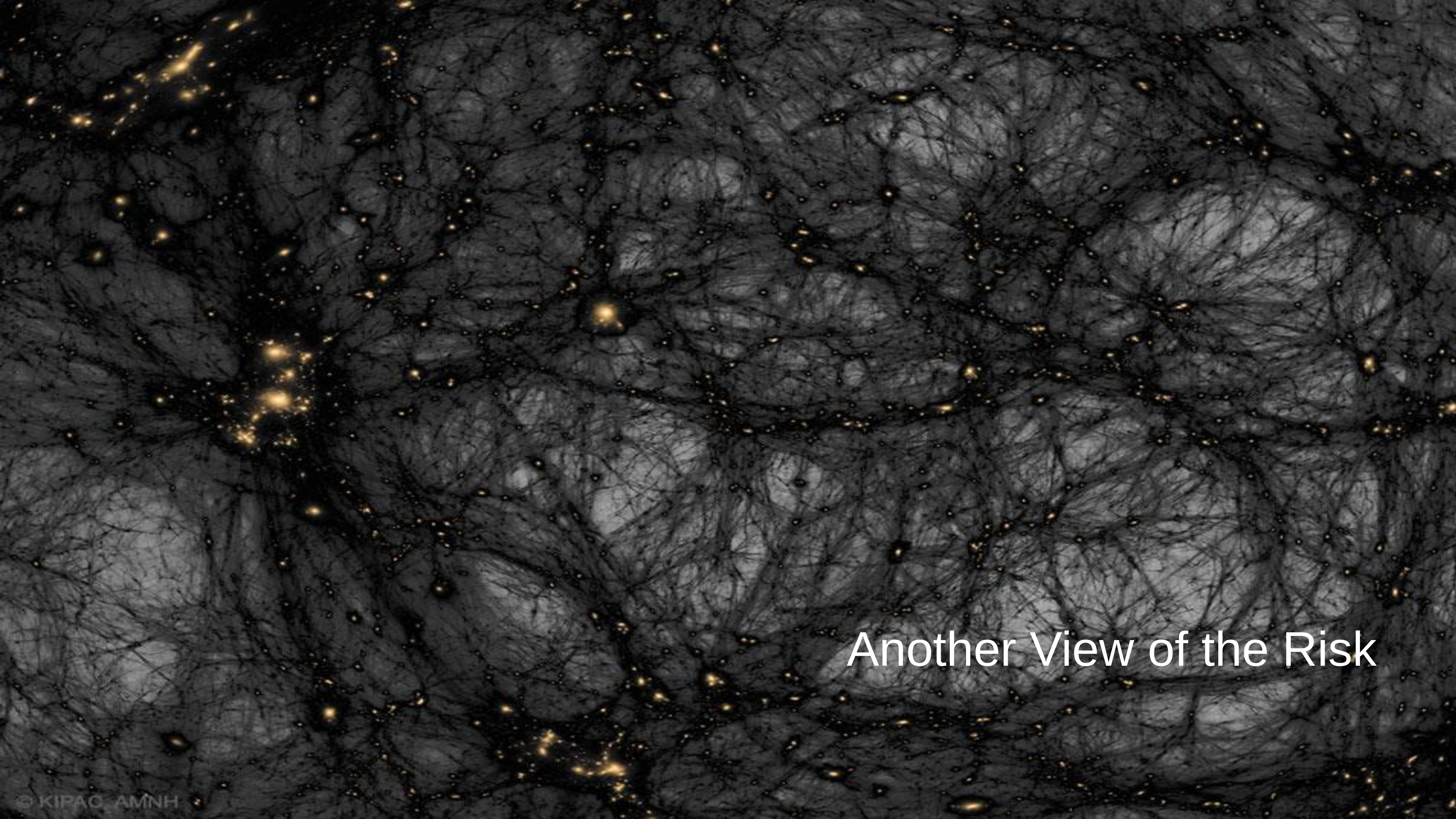
```
DECLARE
 h_name  VARCHAR2(60);
 test_ip VARCHAR2(12) := '155.97.137.';
 suffixn NUMBER(3) := 0;
 suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || 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 (4:4)

- From a conference room using personal wifi

```
155.97.136.006 - avaya-cms.vs.utah.edu
155.97.136.110 - dbw1.it.utah.edu
155.97.136.111 - sql-om.it.utah.edu
155.97.136.112 - sql-cm.it.utah.edu
155.97.136.113 - sql-bes.it.utah.edu
155.97.136.117 - dbw23.it.utah.edu
155.97.136.140 - d-ad.addev.utah.edu
155.97.136.141 - d-hsc.hscdev.addev.utah.edu
155.97.136.147 - d-mim.addev.utah.edu
155.97.136.148 - d-adfs.addev.utah.edu
155.97.136.149 - fim.addev.utah.edu
155.97.136.150 - d-ars.addev.utah.edu
155.97.136.153 - d-adlds.addev.utah.edu
155.97.136.157 - d-candes.addev.utah.edu
155.97.136.200 - b3.ddi.utah.edu

155.97.137.007 - slb1-campus-ddc-i11.net.utah.edu
155.97.137.010 - slb2-campus-ddc-j11.net.utah.edu
155.97.137.011 - slb-campus-ddc-vip.net.utah.edu
155.97.137.012 - slb3-campus-ddc-i11.net.utah.edu
155.97.137.021 - astra.utah.edu
155.97.137.022 - dars.sys.utah.edu
155.97.137.024 - webct.utah.edu
155.97.137.025 - jira.acs.utah.edu
155.97.137.026 - webctold.utah.edu
155.97.137.027 - stage.exchange.utah.edu
155.97.137.031 - my.utah.edu
155.97.137.032 - onboard.utah.edu
155.97.137.033 - uguest.utah.edu
155.97.137.034 - mytest.utah.edu
155.97.137.035 - campusmasterplan.utah.edu
155.97.137.036 - autodiscover.coe.utah.edu
```

```
155.97.137.040 - appdb.it.utah.edu
155.97.137.041 - gsa.search.utah.edu
155.97.137.043 - mrte.cc.utah.edu
155.97.137.044 - unite.utah.edu
155.97.137.045 - test.sys.utah.edu
155.97.137.046 - smtp.o365.umail.utah.edu
155.97.137.047 - vip-ipo.cc.utah.edu
155.97.137.050 - ipohsc.utah.edu
155.97.137.051 - staging.egi.utah.edu
155.97.137.052 - smtp.utah.edu
155.97.137.053 - ipo-forward.cc.utah.edu
155.97.137.054 - webstats8.utah.edu
155.97.137.055 - sdc8.utah.edu
155.97.137.060 - eq.utah.edu
155.97.137.061 - blocku.acs.utah.edu
155.97.137.062 - csmssl1.test.utah.edu
155.97.137.063 - sharepoint.it.utah.edu
155.97.137.066 - uitapp.it.utah.edu
155.97.137.067 - test.www.utah.edu
155.97.137.071 - ezproxy.test.utah.edu
155.97.137.072 - internalhub.umail.utah.edu
155.97.137.074 - legacy.umail.utah.edu
155.97.137.077 - ldap.acs.utah.edu
155.97.137.100 - go.utah.edu
155.97.137.102 - testvip2.sys.utah.edu
155.97.137.103 - ulogin.utah.edu
155.97.137.104 - jira.sys.utah.edu
155.97.137.105 - exc-sentry.med.utah.edu
155.97.137.106 - people.utah.edu
155.97.137.107 - www.test.utah.edu
155.97.137.109 - idp.idm.utah.edu
155.97.137.110 - gis-reporting.fm.utah.edu
155.97.137.114 - training.identity.utah.edu
155.97.137.118 - templates.utah.edu
155.97.137.150 - umailx.umail.utah.edu
155.97.137.223 - ese.idm.utah.edu
155.97.137.229 - test.go.utah.edu
155.97.137.232 - jira.test.utah.edu
155.97.137.234 - d-pki.addev.utah.edu
155.97.137.236 - gatetest.acs.utah.edu
155.97.137.237 - gatedev.acs.utah.edu
```



© KIPAC, AMNH

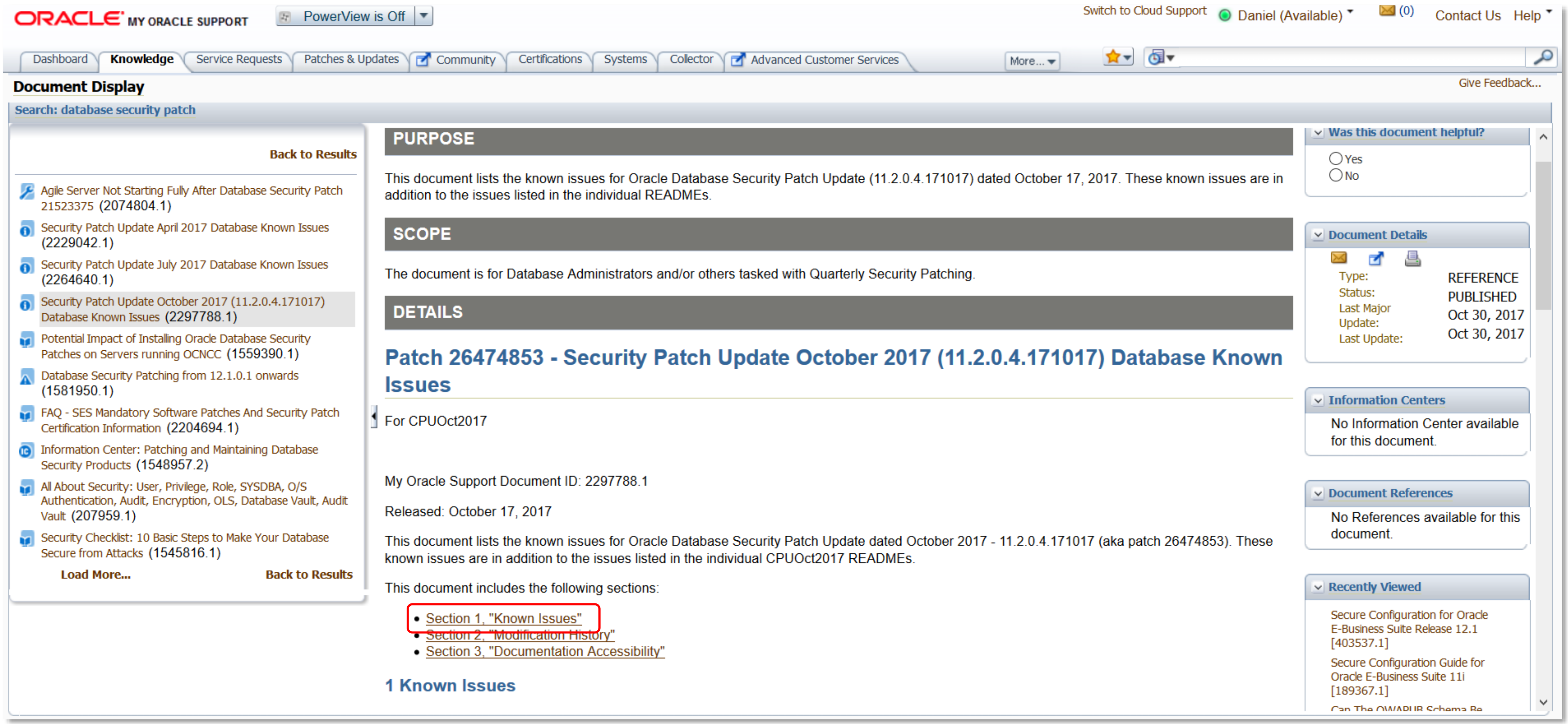
Another View of the Risk

Anatomy Of An IT Attack (1:6)

- Oracle releases a new security patch
- Attackers download it within minutes
- Attackers read the list of weaknesses
- Attackers know they have weeks to months before Oracle's customers will apply the latest patch

- I am going to teach everyone here how to attack any Oracle Database
  - With no escalated privileges
  - Without any tools or techniques such as SQL Injection
  - And with only one SQL statement and one line of code
- You have an ethical and moral responsibility to use this information only for the purpose of helping your organization understand the risk they are taking by not investing in data and database security

Anatomy Of An IT Attack (2:6)



Document Display

Search: database security patch

- Agile Server Not Starting Fully After Database Security Patch 21523375 (2074804.1)
- Security Patch Update April 2017 Database Known Issues (2229042.1)
- Security Patch Update July 2017 Database Known Issues (2264640.1)
- Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues (2297788.1)
- Potential Impact of Installing Oracle Database Security Patches on Servers running OCNCC (1559390.1)
- Database Security Patching from 12.1.0.1 onwards (1581950.1)
- FAQ - SES Mandatory Software Patches And Security Patch Certification Information (2204694.1)
- Information Center: Patching and Maintaining Database Security Products (1548957.2)
- All About Security: User, Privilege, Role, SYSDBA, O/S Authentication, Audit, Encryption, OLS, Database Vault, Audit Vault (207959.1)
- Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (1545816.1)

PURPOSE

This document lists the known issues for Oracle Database Security Patch Update (11.2.0.4.171017) dated October 17, 2017. These known issues are in addition to the issues listed in the individual READMEs.

SCOPE

The document is for Database Administrators and/or others tasked with Quarterly Security Patching.

DETAILS

Patch 26474853 - Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues

For CPUOct2017

My Oracle Support Document ID: 2297788.1

Released: October 17, 2017

This document lists the known issues for Oracle Database Security Patch Update dated October 2017 - 11.2.0.4.171017 (aka patch 26474853). These known issues are in addition to the issues listed in the individual CPUOct2017 READMEs.

This document includes the following sections:

- Section 1, "Known Issues"
- Section 2, "Modification History"
- Section 3, "Documentation Accessibility"

1 Known Issues

Was this document helpful?

○ Yes
○ No

Document Details

Type:	REFERENCE
Status:	PUBLISHED
Last Major Update:	Oct 30, 2017
Last Update:	Oct 30, 2017

Information Centers

No Information Center available for this document.

Document References

No References available for this document.

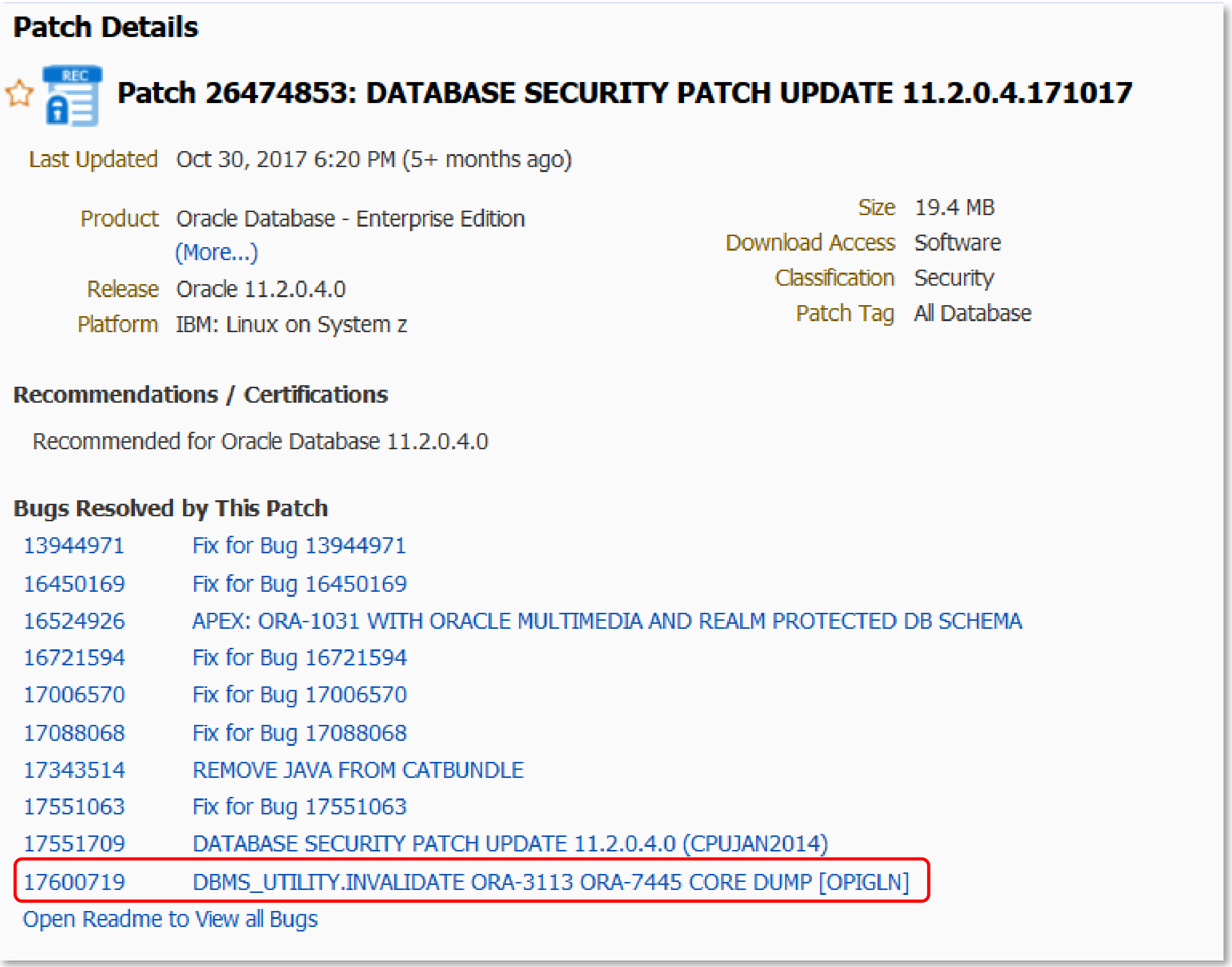
Recently Viewed

Secure Configuration for Oracle E-Business Suite Release 12.1 [403537.1]

Secure Configuration Guide for Oracle E-Business Suite 11i [189367.1]

Can The OWAPUB Schema Be

Anatomy Of An IT Attack (3:6)



Patch Details

Patch 26474853: DATABASE SECURITY PATCH UPDATE 11.2.0.4.171017

Last Updated Oct 30, 2017 6:20 PM (5+ months ago)

Product	Oracle Database - Enterprise Edition (More...)	Size	19.4 MB
		Download Access	Software
Release	Oracle 11.2.0.4.0	Classification	Security
Platform	IBM: Linux on System z	Patch Tag	All Database

Recommendations / Certifications

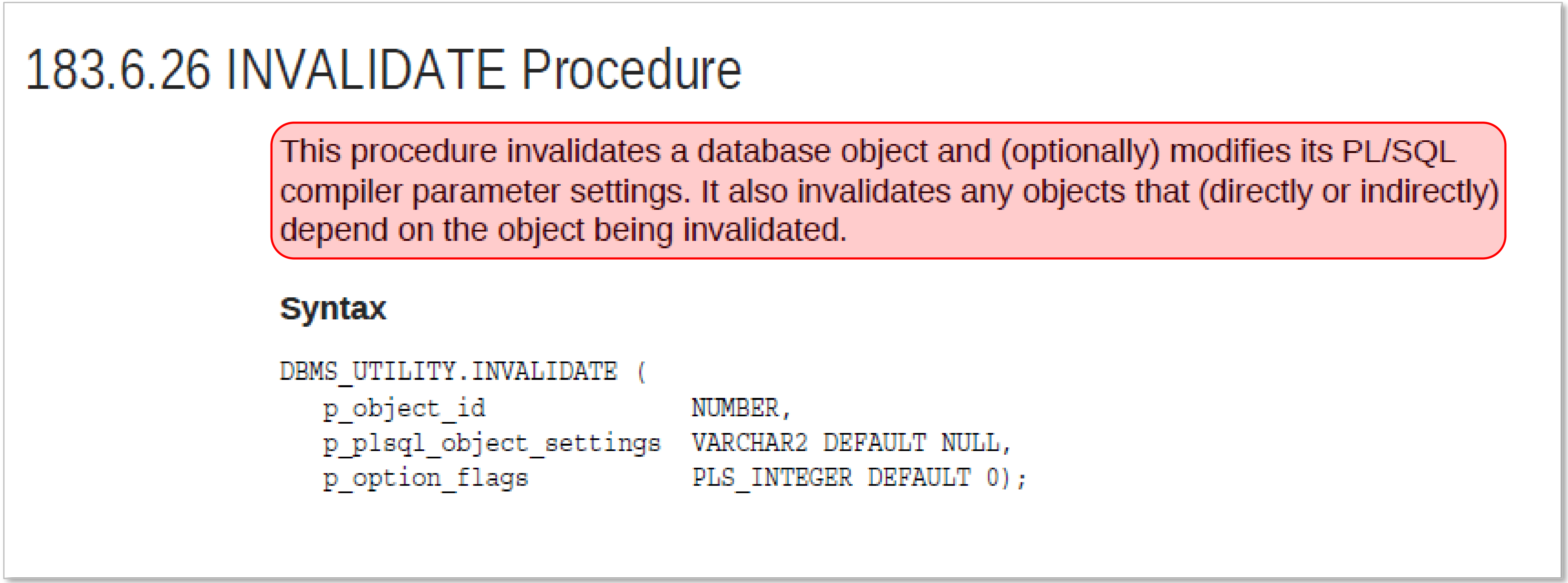
Recommended for Oracle Database 11.2.0.4.0

Bugs Resolved by This Patch

13944971	Fix for Bug 13944971
16450169	Fix for Bug 16450169
16524926	APEX: ORA-1031 WITH ORACLE MULTIMEDIA AND REALM PROTECTED DB SCHEMA
16721594	Fix for Bug 16721594
17006570	Fix for Bug 17006570
17088068	Fix for Bug 17088068
17343514	REMOVE JAVA FROM CATBUNDLE
17551063	Fix for Bug 17551063
17551709	DATABASE SECURITY PATCH UPDATE 11.2.0.4.0 (CPUJAN2014)
17600719	DBMS_UTILITY.INVALIDATE ORA-3113 ORA-7445 CORE DUMP [OPIGLN]

Open Readme to View all Bugs

Anatomy Of An IT Attack (4:6)



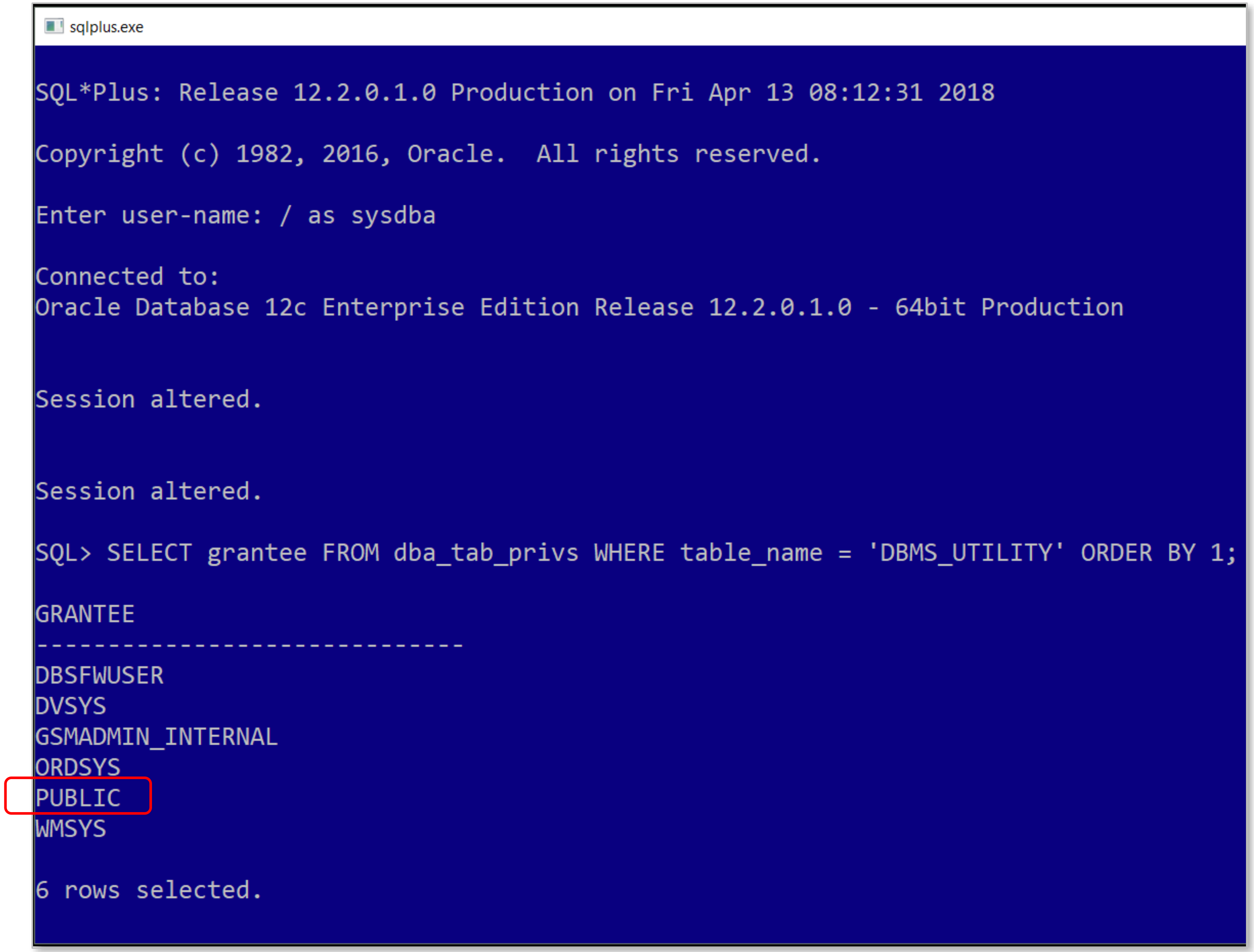
183.6.26 INVALIDATE Procedure

This procedure invalidates a database object and (optionally) modifies its PL/SQL compiler parameter settings. It also invalidates any objects that (directly or indirectly) depend on the object being invalidated.

Syntax

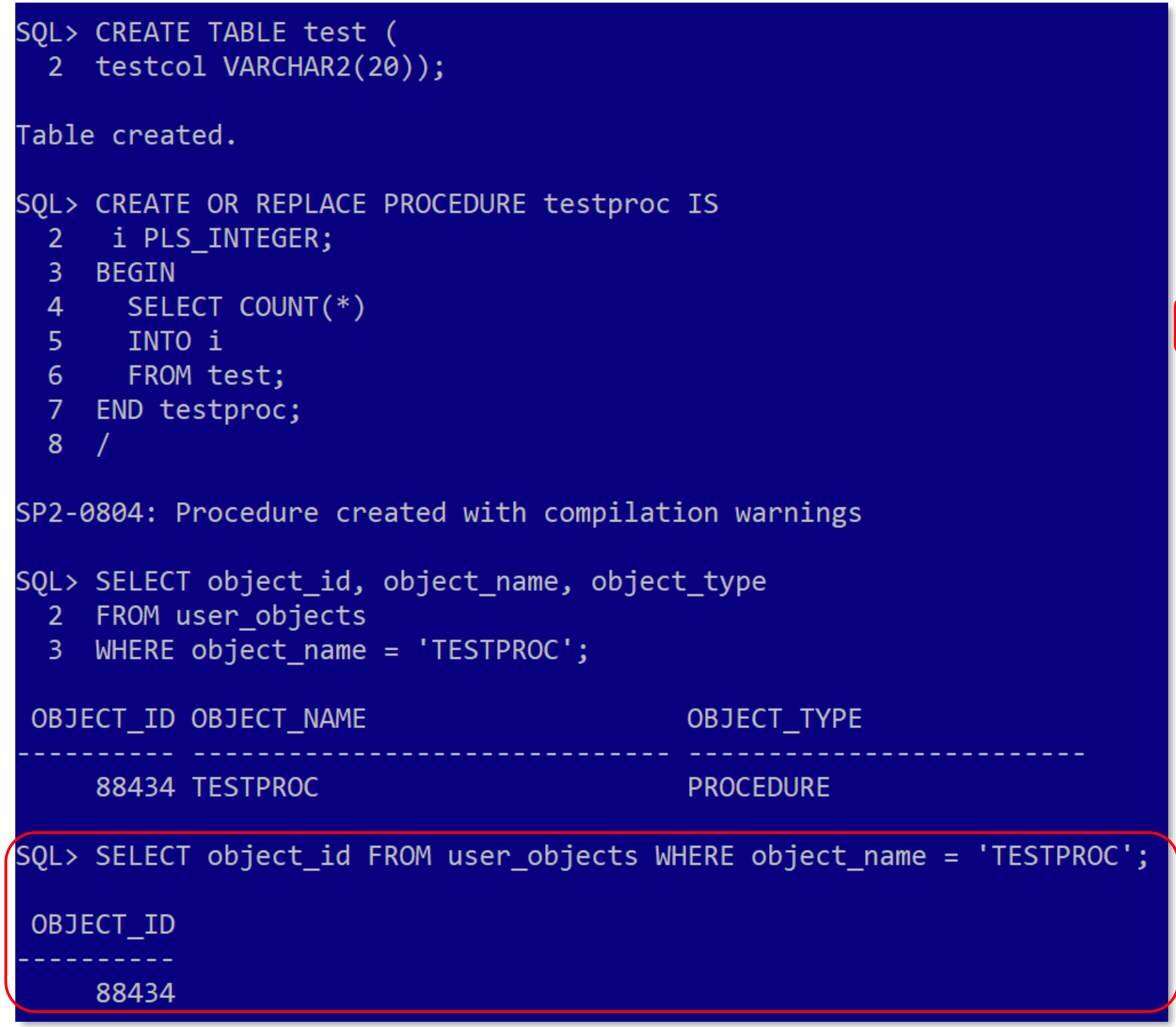
```
DBMS_UTILITY.INVALIDATE (
   p_object_id              NUMBER,
   p_plsql_object_settings  VARCHAR2 DEFAULT NULL,
   p_option_flags           PLS_INTEGER DEFAULT 0);
```

Anatomy Of An IT Attack (5:6)

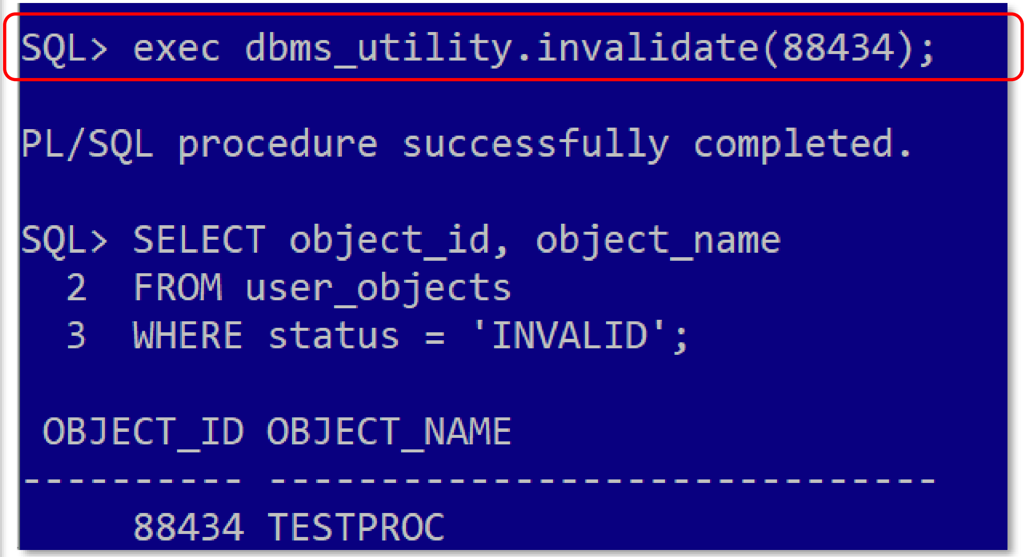


```
SQL*Plus: Release 12.2.0.1.0 Production on Fri Apr 13 08:12:31 2018

Copyright (c) 1982, 2016, Oracle.  All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production


Session altered.


Session altered.

SQL> SELECT grantee FROM dba_tab_privs WHERE table_name = 'DBMS_UTILITY' ORDER BY 1;

GRANTEE
------------------------------
DBSFWUSER
DVSYS
GSMADMIN_INTERNAL
ORDSYS
PUBLIC
WMSYS

6 rows selected.
```

Anatomy Of An IT Attack (6:6)



```
SQL> CREATE TABLE test (
  2  testcol VARCHAR2(20));

Table created.

SQL> CREATE OR REPLACE PROCEDURE testproc IS
  2   i PLS_INTEGER;
  3  BEGIN
  4    SELECT COUNT(*)
  5    INTO i
  6    FROM test;
  7  END testproc;
  8  /

SP2-0804: Procedure created with compilation warnings

SQL> SELECT object_id, object_name, object_type
  2  FROM user_objects
  3  WHERE object_name = 'TESTPROC';

 OBJECT_ID OBJECT_NAME                    OBJECT_TYPE
---------- ------------------------------ -------------------------
     88434 TESTPROC                       PROCEDURE

SQL> SELECT object_id FROM user_objects WHERE object_name = 'TESTPROC';

 OBJECT_ID
----------
     88434
```



```
SQL> exec dbms_utility.invalidate(88434);

PL/SQL procedure successfully completed.

SQL> SELECT object_id, object_name
  2  FROM user_objects
  3  WHERE status = 'INVALID';

 OBJECT_ID OBJECT_NAME
---------- ------------------------------
     88434 TESTPROC
```

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

Perimeter Defense (1:3)

- Perimeter defense has never worked
- Did any castle ever built survive all attacks?
- Did the "impenetrable" Maginot line protect France?
- Did every major break-in ir you have ever heard of onl succeed because the targe didn't have a firewall?
  Or Identity Management?

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

Perimeter Defense (2:3)

- 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 an audit, allowed direct access from the internet (UNTRUST) to the database servers (BUSINESS-DATA)
- The organization's employees did not understand the rules they wrote

```
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
```

Perimeter Defense (3:3)

- A firewall should give you no sense of comfort
- Here is another firewall rule set-up 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
```

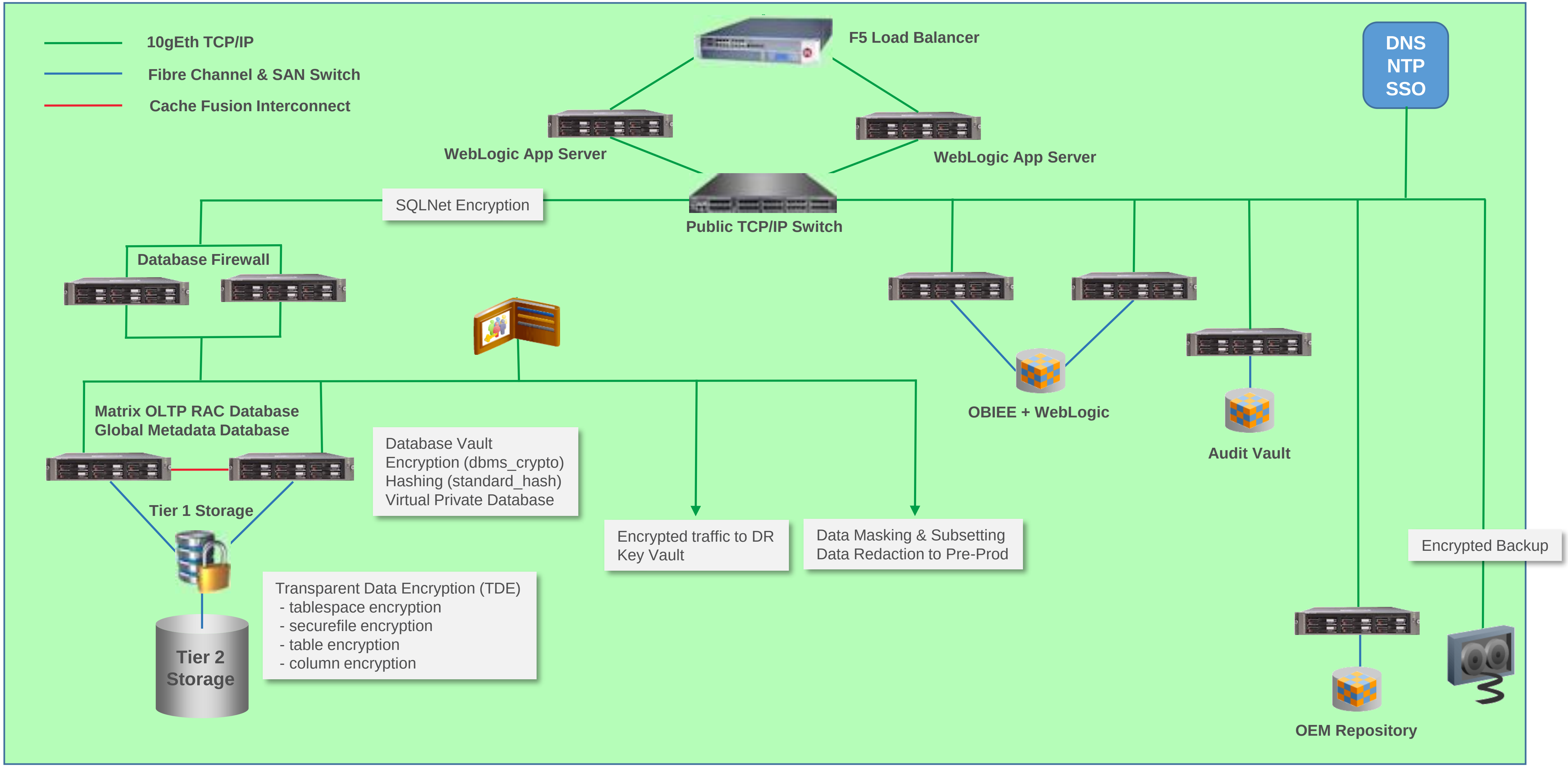
Database Networks

- 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

Example of a Minimum Network Environment



10gEth TCP/IP

Fibre Channel & SAN Switch

Cache Fusion Interconnect

F5 Load Balancer

DNS
NTP
SSO

WebLogic App Server

WebLogic App Server

SQLNet Encryption

Public TCP/IP Switch

Database Firewall

OBIEE + WebLogic

Audit Vault

Matrix OLTP RAC Database
Global Metadata Database

Database Vault
Encryption (dbms_crypto)
Hashing (standard_hash)
Virtual Private Database

Tier 1 Storage

Encrypted traffic to DR
Key Vault

Data Masking & Subsetting
Data Redaction to Pre-Prod

Encrypted Backup

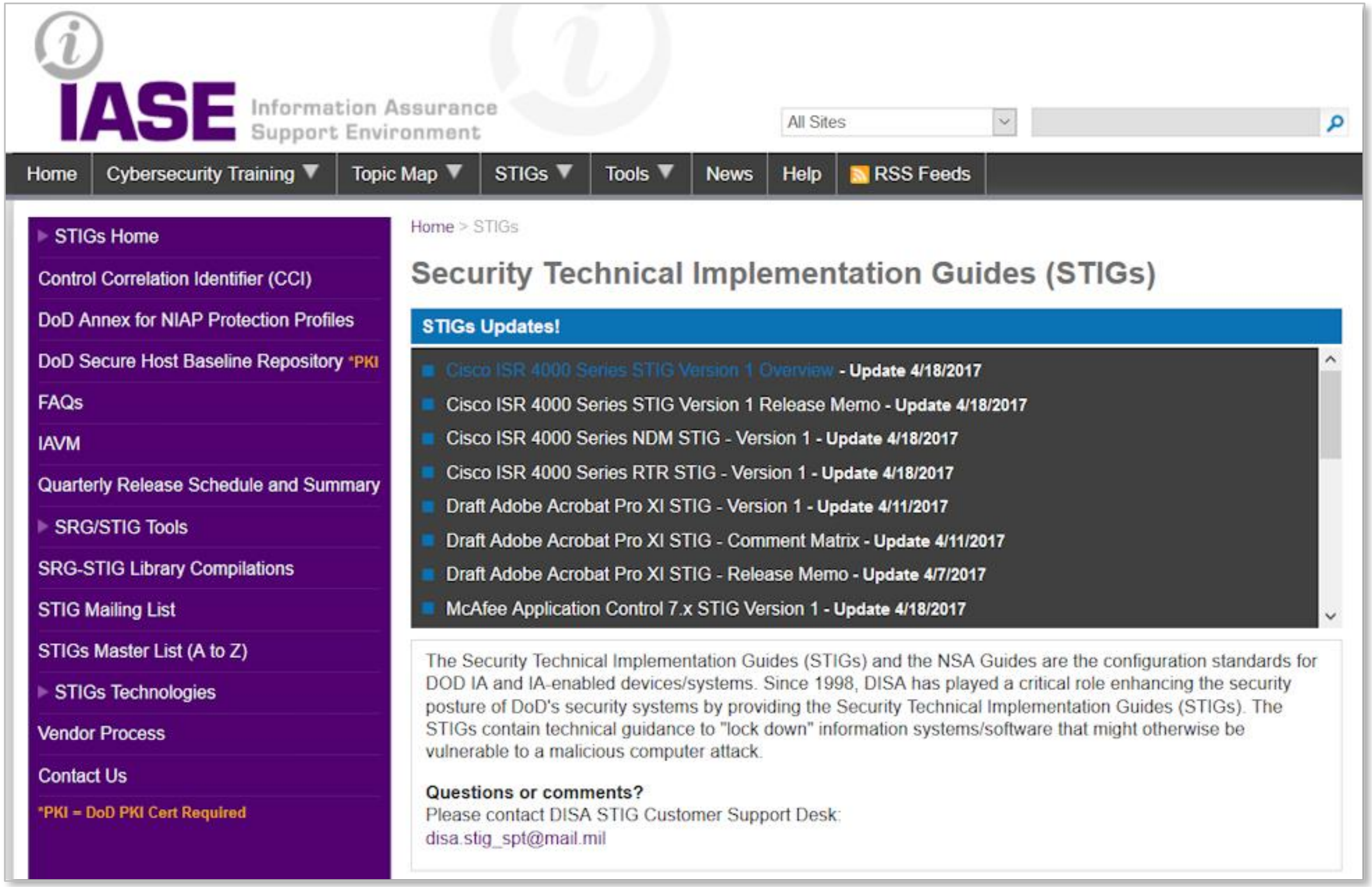
Transparent Data Encryption (TDE)
- tablespace encryption
- securefile encryption
- table encryption
- column encryption

Tier 2
Storage

OEM Repository

Security Support Resources

STIG (1:3)



IASE Information Assurance Support Environment
All Sites
Home
Cybersecurity Training ▼
Topic Map ▼
STIGs ▼
Tools ▼
News
Help
RSS Feeds
▸ STIGs Home
Control Correlation Identifier (CCI)
DoD Annex for NIAP Protection Profiles
DoD Secure Host Baseline Repository *PKI
FAQs
IAVM
Quarterly Release Schedule and Summary
▸ SRG/STIG Tools
SRG-STIG Library Compilations
STIG Mailing List
STIGs Master List (A to Z)
▸ STIGs Technologies
Vendor Process
Contact Us
*PKI = DoD PKI Cert Required
Home > STIGs

Security Technical Implementation Guides (STIGs)

STIGs Updates!

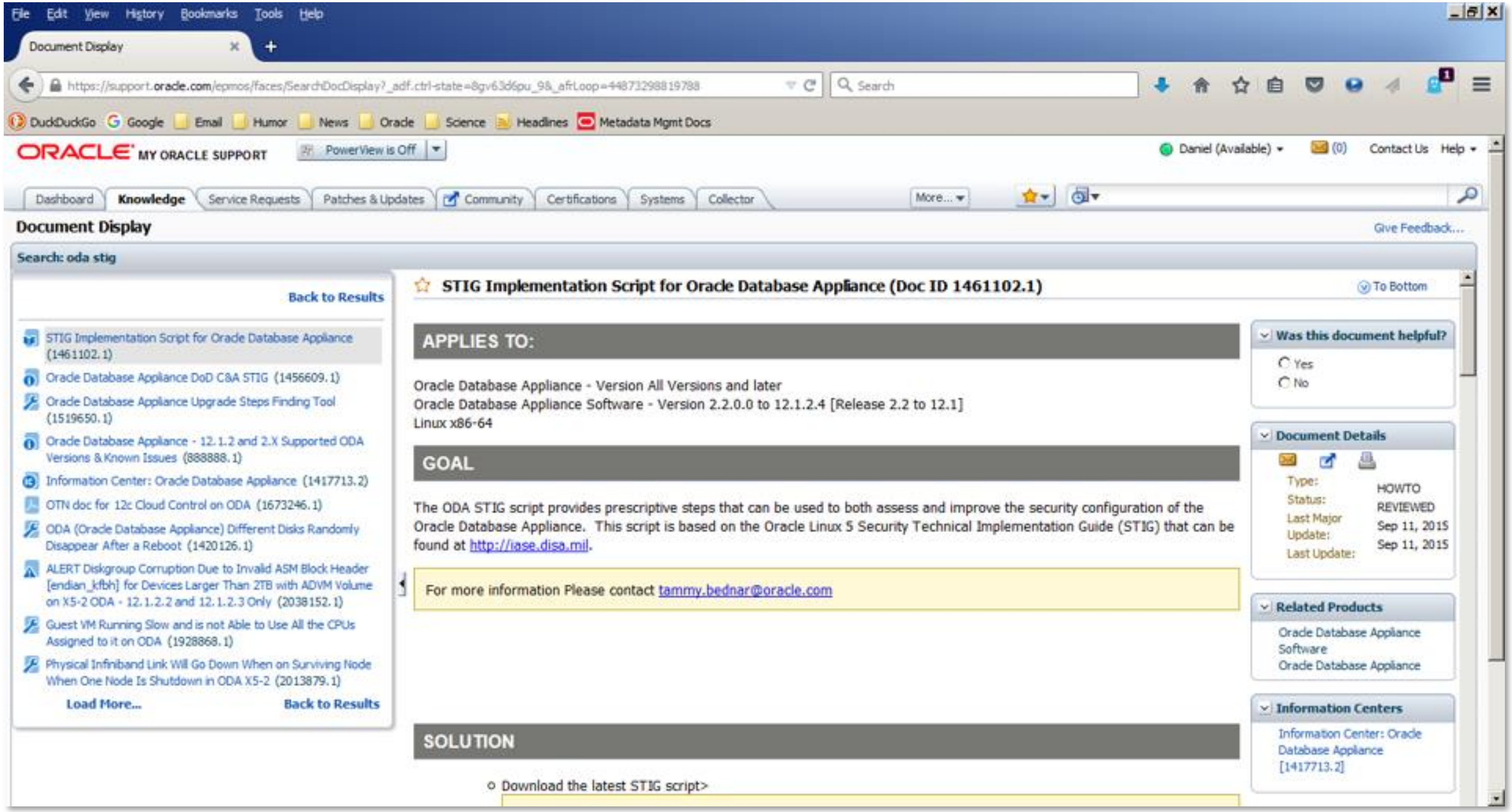
- Cisco ISR 4000 Series STIG Version 1 Overview **- Update 4/18/2017**
- Cisco ISR 4000 Series STIG Version 1 Release Memo **- Update 4/18/2017**
- Cisco ISR 4000 Series NDM STIG - Version 1 **- Update 4/18/2017**
- Cisco ISR 4000 Series RTR STIG - Version 1 **- Update 4/18/2017**
- Draft Adobe Acrobat Pro XI STIG - Version 1 **- Update 4/11/2017**
- Draft Adobe Acrobat Pro XI STIG - Comment Matrix **- Update 4/11/2017**
- Draft Adobe Acrobat Pro XI STIG - Release Memo **- Update 4/7/2017**
- McAfee Application Control 7.x STIG Version 1 **- Update 4/18/2017**

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Questions or comments?
Please contact DISA STIG Customer Support Desk:
disa.stig_spt@mail.mil

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

STIG (2:3)


File Edit View History Bookmarks Tools Help
Document Display
https://support.oracle.com/epmos/faces/SearchDocDisplay?_adf.ctrl-state=8gv63d6pu_9&_afrLoop=44873298819788
Search
DuckDuckGo Google Email Humor News Oracle Science Headlines Metadata Mgmt Docs
ORACLE MY ORACLE SUPPORT
PowerView is Off
Daniel (Available)
(0)
Contact Us
Help
Dashboard Knowledge Service Requests Patches & Updates Community Certifications Systems Collector
More...
Give Feedback...
To Bottom
Back to Results
Load More...
Back to Results

Document Display

Search: oda stig

- 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)

STIG Implementation Script for Oracle Database Appliance (Doc ID 1461102.1)

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]

STIG (3:3)

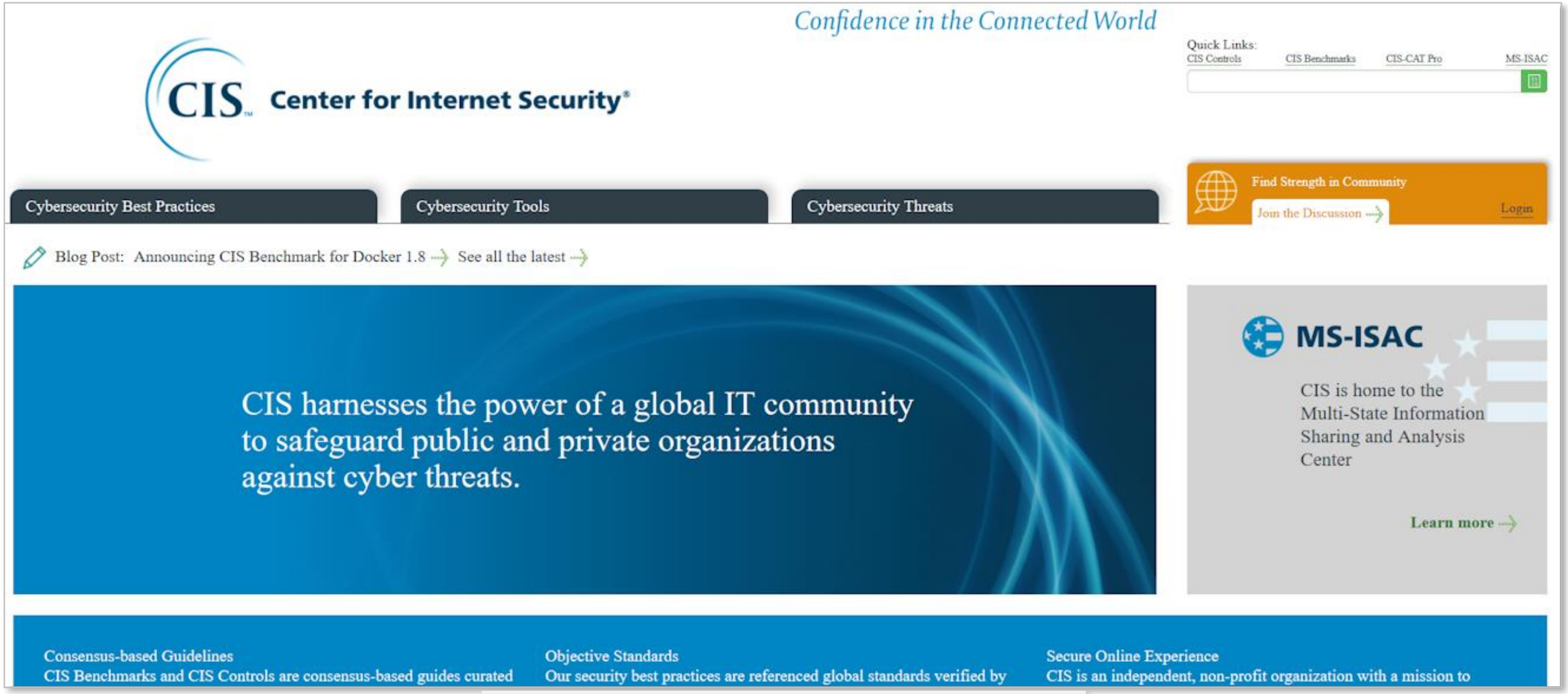
- A STIG is a Security Technical Implementation Guide produced or approved by the US Department of Defense
- Oracle has published STIGs at My Oracle Support for Exadata and ODA
  - But the "CHECK" option can be run on any Linux server
- Oracle Support provides a downloadable script that can be used to 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

Center for Internet Security (CIS)

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



Blog Post: Announcing CIS Benchmark for Docker 1.8 See all the latest

CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

CIS is home to the Multi-State Information Sharing and Analysis Center

Consensus-based Guidelines
CIS Benchmarks and CIS Controls are consensus-based guides curated

Objective Standards
Our security best practices are referenced global standards verified by

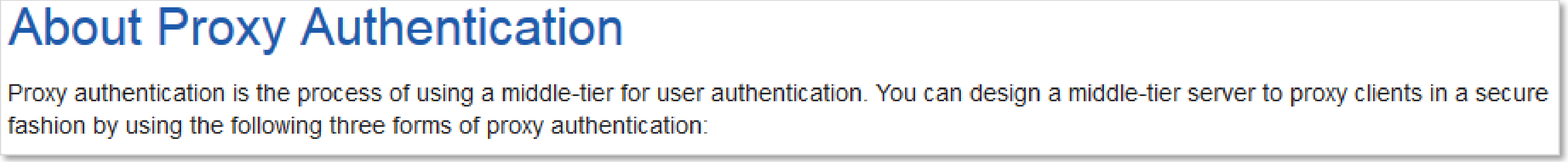
Secure Online Experience
CIS is an independent, non-profit organization with a mission to

`https://www.cisecurity.org`

User Management

Proxy Users (1:3)

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

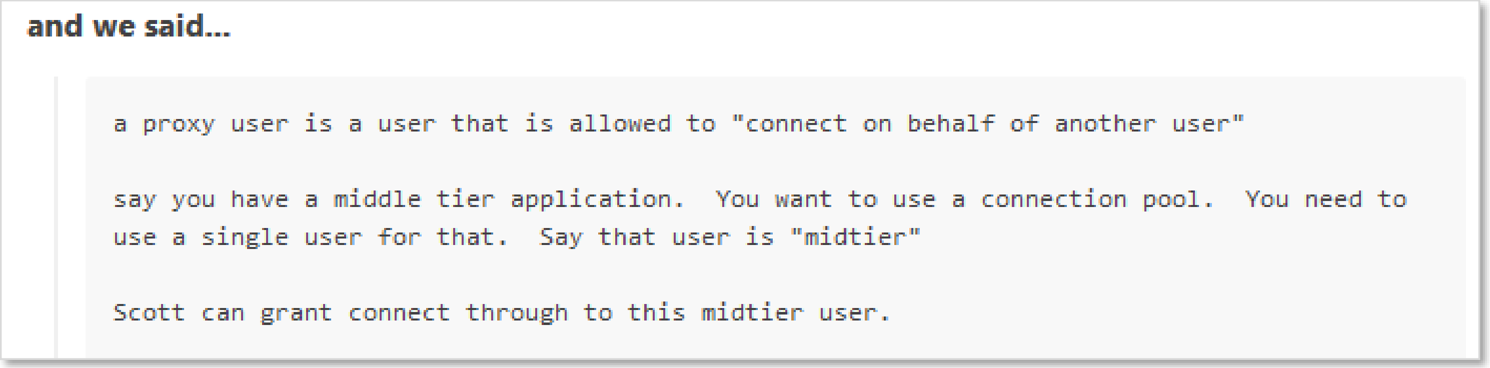


About Proxy Authentication

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 ...



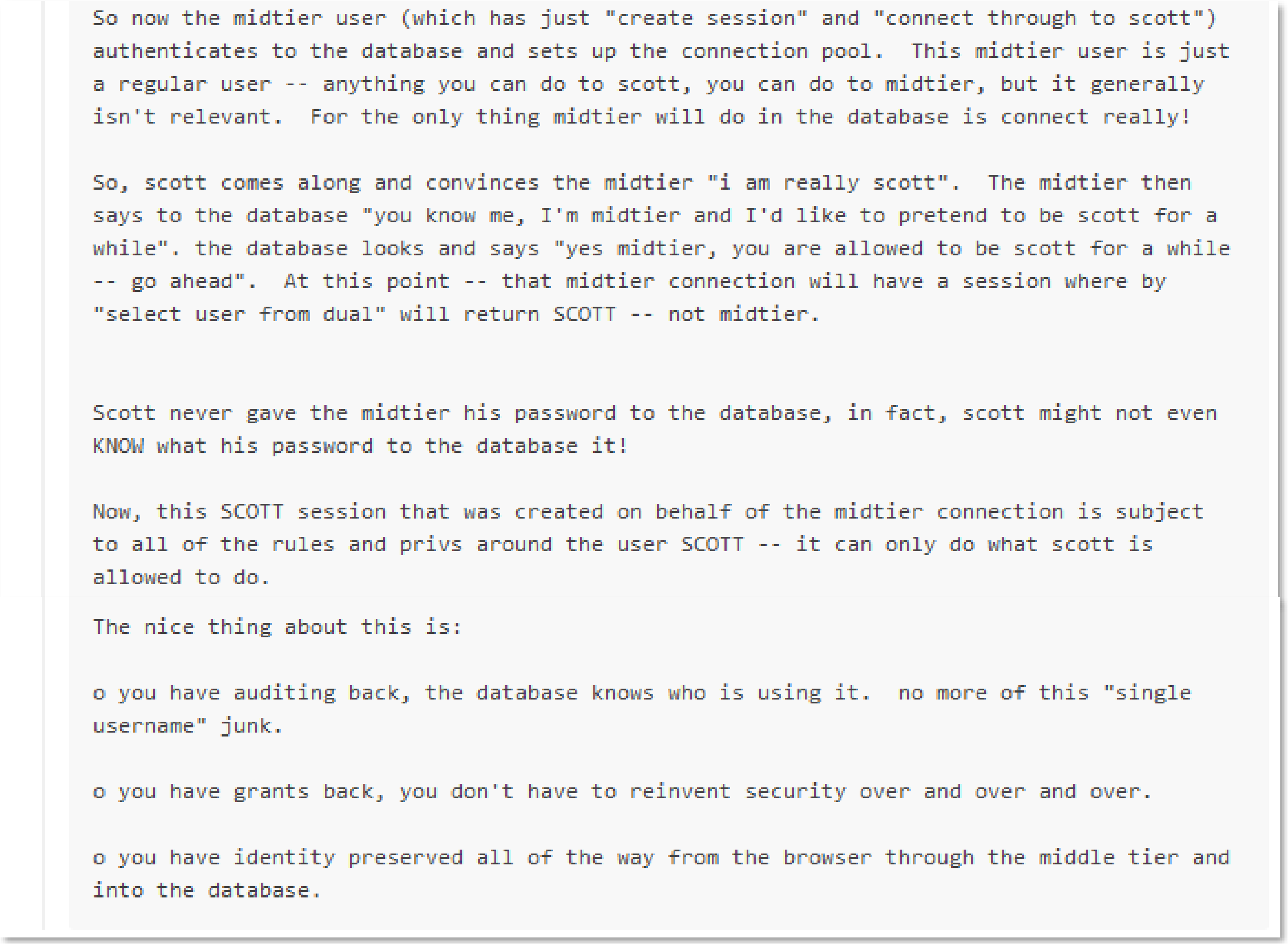
and we said...

```
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)

- ... proxy users are far more secure than regular users



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 (1:3)

- 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,lock and expire the account, or drop it
- 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
- With applications such as EBS, SAP, Peoplesoft, Siebel, we are finding a truly staggering number of accounts that are still using unchanged default passwords
- Do not force users to change passwords on a regular basis

User Authentication and Permissions (2:3)

Explanation	Default passwords are passwords that have been created for purposes of installation and testing and that have been published and most often widely distributed. Not changing default passwords immediately after installation creates a substantial security risk.

Validation	SELECT d.username, u.account_status
	FROM dba_users_with_defpwd d, dba_users u
	WHERE d.username = u.username
	AND u.account_status = 'OPEN';

Findings	USERNAME ACCOUNT_STATUS ------------------------------ -------------------- ABM OPEN AP OPEN -- Accounts Payable APPLSYSPUB OPEN AR OPEN -- Accounts Receivable FA OPEN -- Fixed Assets GL OPEN -- General Ledger JE OPEN -- Journal Entry SCOTT OPEN USER1 OPEN VIDEO5 OPEN
Action	The EBS application has little protection against a breach and no way to determine, after the fact, that a breach has taken place. All default passwords should be changed to complex passwords containing a combination of upper case, lower case, numbers, and special characters and these should be changed at least once each year.

User Authentication and Permissions (3:3)

- NIST Special Publication 800-63: Digital Identity Guidelines (May 31, 2018)
  - https://pages.nist.gov/800-63-FAQ/#q-b5

“Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”

- Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future.
- When those changes do occur, they often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password.
- This practice provides a false sense of security if any of the previous secrets has been compromised since attackers can apply these same common transformations.
- But if there is evidence that the memorized secret has been compromised, such as by a breach of the verifier’s hashed password database or observed fraudulent activity, subscribers should be required to change their memorized secrets.
- However, this event-based change should occur rarely, so that they are less motivated to choose a weak secret with the knowledge that it will only be used for a limited period of time.

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_strong_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

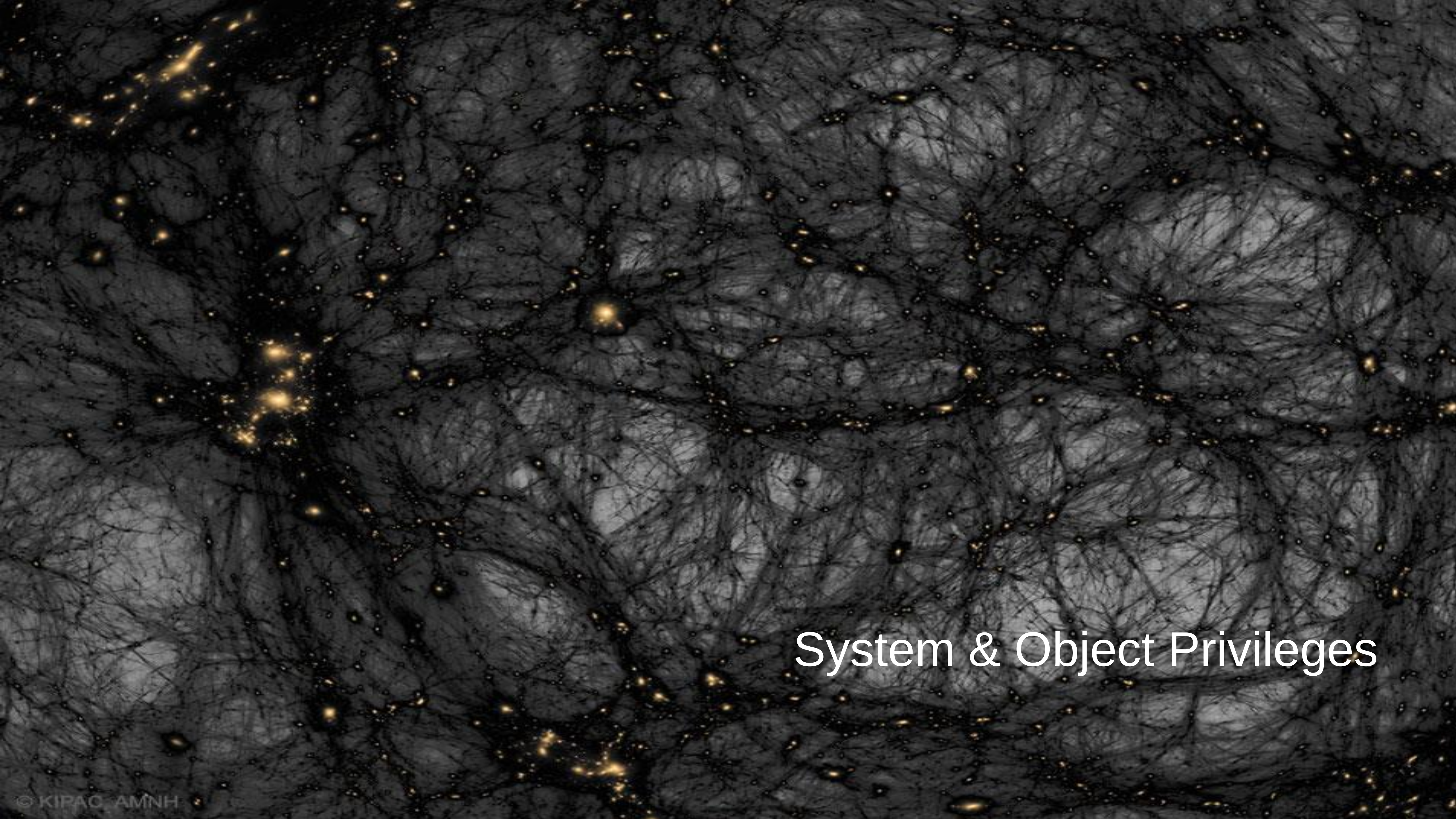
- A script run in 12c+ as part of installation that creates a "secure configuration"
- Review the script **`$ORACLE_HOME/rdbms/admin/secconf.sql`**

```
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.
```

Performs 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



System & Object Privileges

© KIPAC AMNH

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.
```

Do you "NEED" the DBA role?

If you think so feel free to explain why you need any of the privileges highlighted in red

New System Privileges ... Learn Them

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 Granted To PUBLIC (1:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT UNIQUE 'REVOKE EXECUTE ON ' || table_name || ' FROM PUBLIC;' AS
RUN_SCRIPT
FROM dba_tab_privs dtp
WHERE dtp.grantee = 'PUBLIC'
AND dtp.privilege = 'EXECUTE'
AND dtp.type = 'PACKAGE'
AND ((dtp.table_name LIKE 'DBMS%') OR (dtp.table_name LIKE 'UTL%'))
ORDER BY 1;

RUN_SCRIPT
-------------------------------------------------------------
REVOKE EXECUTE ON DBMS_ADDM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_APPLICATION_INFO FROM PUBLIC;
REVOKE EXECUTE ON DBMS_APP_CONT_PRVT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQJMS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_CMT_TIME_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_DEQUEUELOG_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_HISTORY_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_INDEX_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_QUEUES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_QUEUE_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_SIGNATURE_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_SUBSCRIBER_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_EXP_TIMEMGR_TABLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_IMP_INTERNAL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AQ_INV FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ASSERT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AUTO_REPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AUTO_TASK FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AW FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AW_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AW_STATS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_AW_XML FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (2:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_CDC_ISUBSCRIBE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CDC_SUBSCRIBE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CLOBUTIL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_COMPRESSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CREDENTIAL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CRYPTO_TOOLKIT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CSX_INT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CSX_INT2 FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE_ADVISE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE_ADVISE_SEC FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE_LOG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_CUBE_UTIL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DATAPUMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DATA_MINING FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DATA_MINING_TRANSFORM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DB_VERSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DDL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DEBUG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DEBUG_JDWP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DEBUG_JDWP_CUSTOM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DESCRIBE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DIMENSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DM_MODEL_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_DM_MODEL_IMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_EDITIONS_UTILITIES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_EPG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ERRLOG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_EXPORT_EXTENSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_FBT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_FILE_GROUP_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_FILE_GROUP_IMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_FREQUENT_ITEMSET FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (3:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_GOLDENGATE_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_GOLDENGATE_IMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_GSM_NOPRIV FROM PUBLIC;
REVOKE EXECUTE ON DBMS_HEAT_MAP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_HIERARCHY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_HS_PARALLEL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ILM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_INDEX_UTL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_INMEMORY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ITRIGGER_UTL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JAVA FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JAVASCRIPT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_JSON FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LCR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LDAP_UTL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOBUTIL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOGREP_EXP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOGREP_IMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_LOGSTDBY_CONTEXT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_MACOLS_SESSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_MACSEC_ROLES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_MDX_ODBO FROM PUBLIC;
REVOKE EXECUTE ON DBMS_METADATA FROM PUBLIC;
REVOKE EXECUTE ON DBMS_METADATA_DIFF FROM PUBLIC;
REVOKE EXECUTE ON DBMS_MVIEW_STATS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_NETWORK_ACL_UTILITY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_OBJECTS_UTILS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ODCI FROM PUBLIC;
REVOKE EXECUTE ON DBMS_OUTPUT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PARALLEL_EXECUTE FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (4:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_PART FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PCLXUTIL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PICKLER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PLSQL_CODE_COVERAGE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PREDICTIVE_ANALYTICS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PREPROCESSOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PROFILER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_PSP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_REFRESH FROM PUBLIC;
REVOKE EXECUTE ON DBMS_REPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RESCONFIG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RESOURCE_MANAGER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RESOURCE_MANAGER_PRIVS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RESULT_CACHE_API FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RMGR_GROUP_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RMGR_PACT_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RMGR_PLAN_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RMIN FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ROWID FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULEADM_INTERNAL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_ADM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_EXP_EV_CTXS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_EXP_RULES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_EXP_RULE_SETS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_EXP_UTLI FROM PUBLIC;
REVOKE EXECUTE ON DBMS_RULE_IMP_OBJ FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_ATTRIBUTE_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_CHAIN_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_CLASS_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_CONSTRAINT_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_CREDENTIAL_EXPORT FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (5:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_SCHED_EXPORT_CALLOUTS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_FILE_WATCHER_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_JOB_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_PROGRAM_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_SCHEDULE_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_WINDOW_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCHED_WINGRP_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SCN FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SESSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SNAPSHOT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SNAPSHOT_UTL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SODA_DOM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SPACE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SPD FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SPM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQLDIAG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQLPA FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQLTUNE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQLTUNE_UTIL2 FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL_MONITOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL_TRANSLATOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SQL_TRANSLATOR_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STANDARD FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STATS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STATS_ADVISOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STAT_FUNCS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STAT_FUNCS_AUX FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STREAMS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_STREAMS_PUB_RPC FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SUMMARY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SUM_RWEQ_EXPORT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_SYNC_REFRESH FROM PUBLIC;
REVOKE EXECUTE ON DBMS_TF FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (6:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_TRACE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_TRANSACTION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_TRANSFORM_EXIMP FROM PUBLIC;
REVOKE EXECUTE ON DBMS_TYPES FROM PUBLIC;
REVOKE EXECUTE ON DBMS_UTILITY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_WARNING FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XA FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDBNFS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDBRESOURCE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDBUTIL_INT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDBZ FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDBZ0 FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_CONFIG FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_CONSTANTS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_CONTENT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_PRINT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_REPOS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XDB_VERSION FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XEVENT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XLSB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLDOM FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLINDEX FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLINDEX0 FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLPARSER FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLQUERY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSAVE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSCHEMA FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSCHEMA_ANNOTATE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSCHEMA_INT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSCHEMA_LSB FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSTORAGE_MANAGE FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XMLSTORE FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (7:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_XMLTRANSLATIONS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XPLAN FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XQUERY FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XQUERYINT FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XSLPROCESSOR FROM PUBLIC;
REVOKE EXECUTE ON DBMS_XS_SESSIONS FROM PUBLIC;
REVOKE EXECUTE ON DBMS_ZHELP_IR FROM PUBLIC;
REVOKE EXECUTE ON UTL_CALL_STACK FROM PUBLIC;
REVOKE EXECUTE ON UTL_COLL FROM PUBLIC;
REVOKE EXECUTE ON UTL_COMPRESS FROM PUBLIC;
REVOKE EXECUTE ON UTL_ENCODE FROM PUBLIC;
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
REVOKE EXECUTE ON UTL_GDK FROM PUBLIC;
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
REVOKE EXECUTE ON UTL_I18N FROM PUBLIC;
REVOKE EXECUTE ON UTL_IDENT FROM PUBLIC;
REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;
REVOKE EXECUTE ON UTL_LMS FROM PUBLIC;
REVOKE EXECUTE ON UTL_MATCH FROM PUBLIC;
REVOKE EXECUTE ON UTL_NLA FROM PUBLIC;
REVOKE EXECUTE ON UTL_RAW FROM PUBLIC;
REVOKE EXECUTE ON UTL_REF FROM PUBLIC;
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
REVOKE EXECUTE ON UTL_URL FROM PUBLIC;
```

DBA_ Object Privileges Granted To PUBLIC

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT 'REVOKE SELECT ON ' || table_name || ' FROM PUBLIC;' AS RUN_SCRIPT
FROM dba_tab_privs
WHERE grantee = 'PUBLIC'
AND table_name LIKE 'DBA%'
ORDER BY 1;

RUN_SCRIPT
-------------------------------------------------------------
REVOKE SELECT ON DBA_AUTO_SEGADV_CTL FROM PUBLIC;
REVOKE SELECT ON DBA_AUTO_SEGADV_SUMMARY FROM PUBLIC;
REVOKE SELECT ON DBA_COL_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_COL_USAGE_STATISTICS FROM PUBLIC;
REVOKE SELECT ON DBA_DBFS_HS_FIXED_PROPERTIES FROM PUBLIC;
REVOKE SELECT ON DBA_EDITIONING_VIEW_COLS FROM PUBLIC;
REVOKE SELECT ON DBA_EDITIONING_VIEW_COLS_AE FROM PUBLIC;
REVOKE SELECT ON DBA_EXPRESSION_STATISTICS FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE_TS FROM PUBLIC;
REVOKE SELECT ON DBA_HEAT_MAP_SEGMENT FROM PUBLIC;
REVOKE SELECT ON DBA_HEAT_MAP_SEG_HISTOGRAM FROM PUBLIC;
REVOKE SELECT ON DBA_IND_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_JAVA_CLASSES FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_MAPS FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_STYLES FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_THEMES FROM PUBLIC;
REVOKE SELECT ON DBA_SR_PARTN_OPS FROM PUBLIC;
REVOKE SELECT ON DBA_SR_STLOG_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_SYNC_CAPTURE_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_HISTGRM_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_STAT_PREFS FROM PUBLIC;
REVOKE SELECT ON DBA_TSTZ_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_XMLSCHEMA_LEVEL_VIEW FROM PUBLIC;
```

ALL_ Object Privileges Granted To PUBLIC

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT 'REVOKE SELECT ON ' || table_name || ' FROM PUBLIC;' AS RUN_SCRIPT
FROM dba_tab_privs
WHERE grantee = 'PUBLIC'
AND table_name LIKE 'ALL%'
ORDER BY 1;

REVOKE SELECT ON ALL_ALL_TABLES FROM PUBLIC;
REVOKE SELECT ON ALL_DB_LINKS FROM PUBLIC;
REVOKE SELECT ON ALL_EDITIONING_VIEWS_AE FROM PUBLIC;
REVOKE SELECT ON ALL_ENCRYPTED_COLUMNS FROM PUBLIC;
REVOKE SELECT ON ALL_JAVA_ARGUMENTS FROM PUBLIC;
REVOKE SELECT ON ALL_OBJECTS FROM PUBLIC;
REVOKE SELECT ON ALL_OBJECTS_AE FROM PUBLIC;
REVOKE SELECT ON ALL_OPERATORS FROM PUBLIC;
REVOKE SELECT ON ALL_OPERATOR_COMMENTS FROM PUBLIC;
REVOKE SELECT ON ALL_PROCEDURES FROM PUBLIC;
REVOKE SELECT ON ALL_SOURCE FROM PUBLIC;
REVOKE SELECT ON ALL_SOURCE_AE FROM PUBLIC;
```

```
SQL*Plus: Release 12.2.0.1.0 Production on Wed Feb 21 22:35:10 2018
Copyright (c) 1982, 2016, Oracle.  All rights reserved.
Enter user-name: / as sysdba
Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

SQL> SELECT grantee
  2  FROM dba_tab_privs
  3  WHERE table_name = 'ALL_SOURCE';

GRANTEE
------------------------------
PUBLIC
DV_SECANALYST
```

V$ Object Access (1:2)

- Anyone that can query Oracle X$ and/or V$ objects can bypass the overwhelming majority of Oracle Database security
- Many of these objects are critically important to protect
  - 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 and Database Vault offer no protection

```
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%'
```

X$ Object Access

- X$ objects are a queryable view of database memory

```
SQL> SELECT inst_id, con_id, dzdpsupsfnm, kzdpsupsffn, kzdpsupsfcom
  2  FROM X$KZDPSUPSF;

INST_ID CON_ID KZDPSUPSFNM                 KZDPSUPSFFN             KZDPSUPSFCOM
------- ------ --------------------------- ----------------------- ------------------------------------------------------------
      1      0 DATA REDACTION              ALL                     Supports all data redaction functionality (DBMS_REDACT).
      1      0 VIRTUAL PRIVATE DATABASE    OBJECT-LEVEL POLICY     Supports object-level VPD policies.
      1      0 VIRTUAL PRIVATE DATABASE    COLUMN-LEVEL POLICY     Supports column-level VPD policies. This corresponds to the
                                                                   parameter functionality provided by DBMS_RLS.ADD_POLICY.
      1      0 UNIFIED AUDIT               OBJECT-LEVEL POLICY     Supports object-level Unified Audit policies.
      1      0 FINE GRAINED AUDIT          ALL                     Supports all fine grained audit functionality (DBMS_FGA).
      1      0 TRANSPARENT DATA ENCRYPTION COLUMN-LEVEL ENCRYPTION Supports TDE Column level encryption.
```

ORADEBUG

- Anyone with access to ORADEBUG can view everything in the database's memory structures
- You can control access to ORADEBUG access in a Database Vault environment using $ORACLE_HOME/rdbms/admin/catmacp.sql

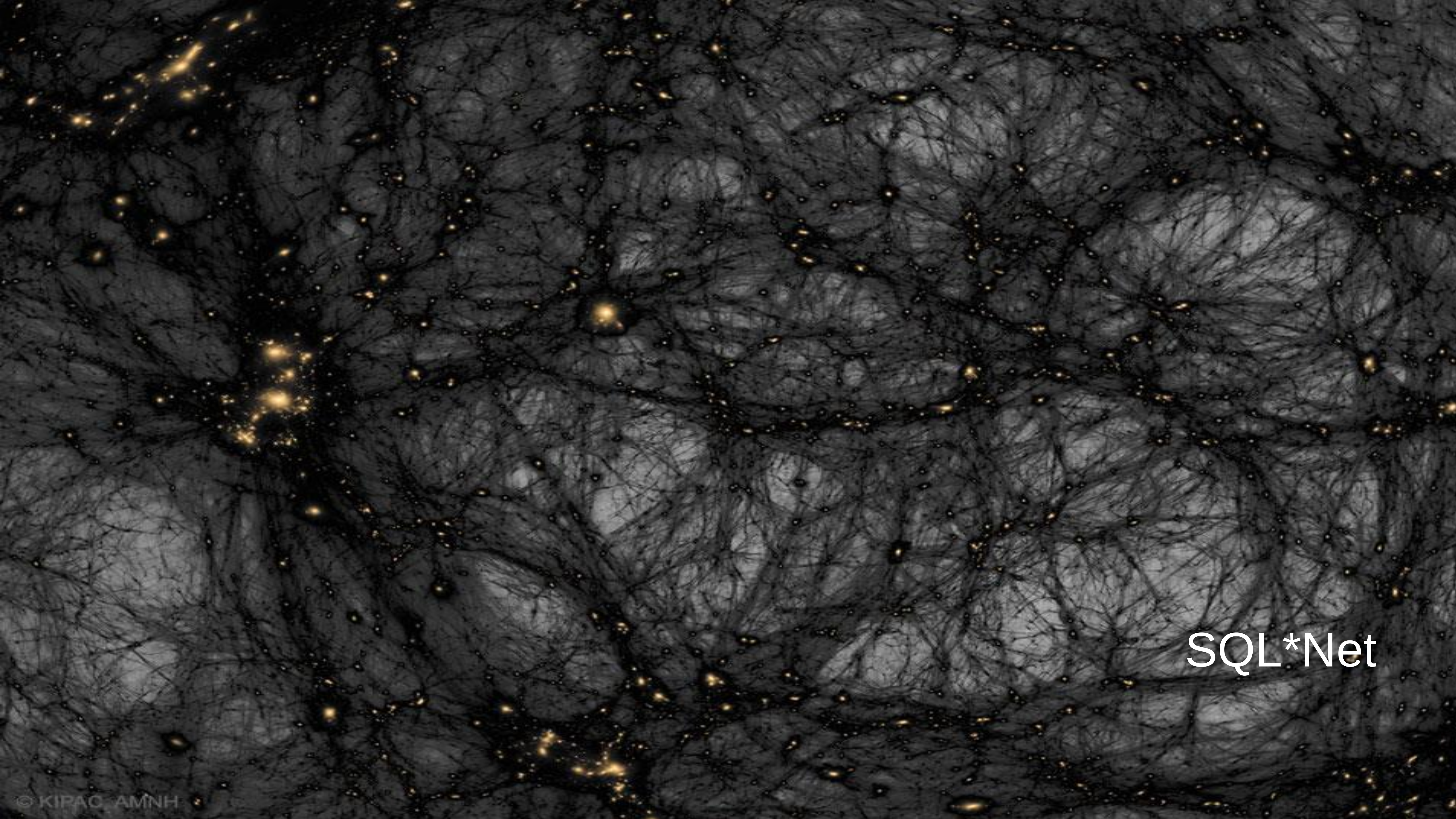
```
PROCEDURE enable_oradebug;
PRAGMA SUPPLEMENTAL_LOG_DATA(enable_oradebug, AUTO_WITH_COMMIT);

PROCEDURE disable_oradebug;
PRAGMA SUPPLEMENTAL_LOG_DATA(disable_oradebug, AUTO_WITH_COMMIT);
```

DBMS_SYS_SQL

- The most dangerous PL/SQL package inside your Oracle Database
  - PARSE_AS_USER allows a statement to be parsed as any user
  - 32 Overloads

```
CREATE OR REPLACE PROCEDURE create_sequence(seqname IN VARCHAR2, uname IN VARCHAR2)
AUTHID DEFINER IS
 c      NUMBER;
 DDLStr CLOB := 'CREATE SEQUENCE ';
 retVal NUMBER;
 uid    dba_users.user_id%TYPE;
BEGIN
  c := dbms_sql.open_cursor;

  DDLStr := DDLStr || seqname;

  SELECT user_id
  INTO uid
  FROM dba_users
  WHERE username = dbms_assert.schema_name(uname);

  dbms_sys_sql.parse_as_user(c, DDLStr, dbms_sql.NATIVE, uid);
  retVal := dbms_sql.execute(c);
  dbms_sql.close_cursor(c);
END create_sequence;
/
```

```
Overload 4 syntax

dbms_sys_sql.parse_as_user(
c              IN NUMBER,
statement      IN CLOB,
language_flag  IN NUMBER,
userid         IN NUMBER);
```

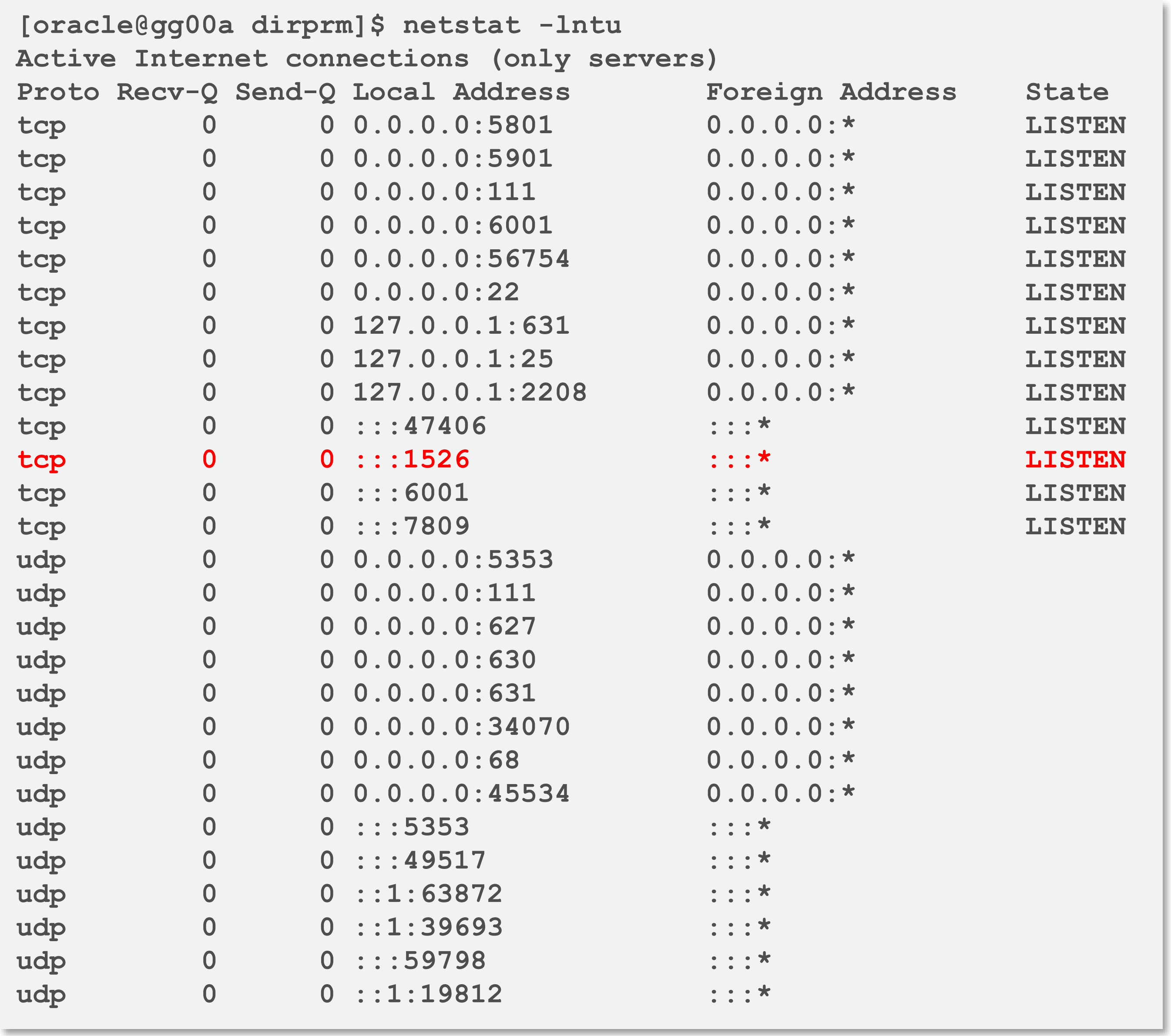


SQL*Net

© KIPAC, AMNH

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                   :::*
```

SQLNET.ALLOWED_LOGON_VERSION

- Specifies the minimum client version that is allowed to connect to the database
- Someone with a valid userid and password, but the wrong Oracle client version is prevented from making a connection

Explanation	Set the login version to 11. The higher setting prevents logins by older version clients that do not use strong authentication to pass the login credentials.
Validation	**`grep -i ALLOWED_LOGIN_VERSION sqlnet.ora`**
Finding	Allowed logon version not configured.
Action	Set **`SQLNET.ALLOWED_LOGON_VERSION=12a`** to restrict access to version 12-18 clients.

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

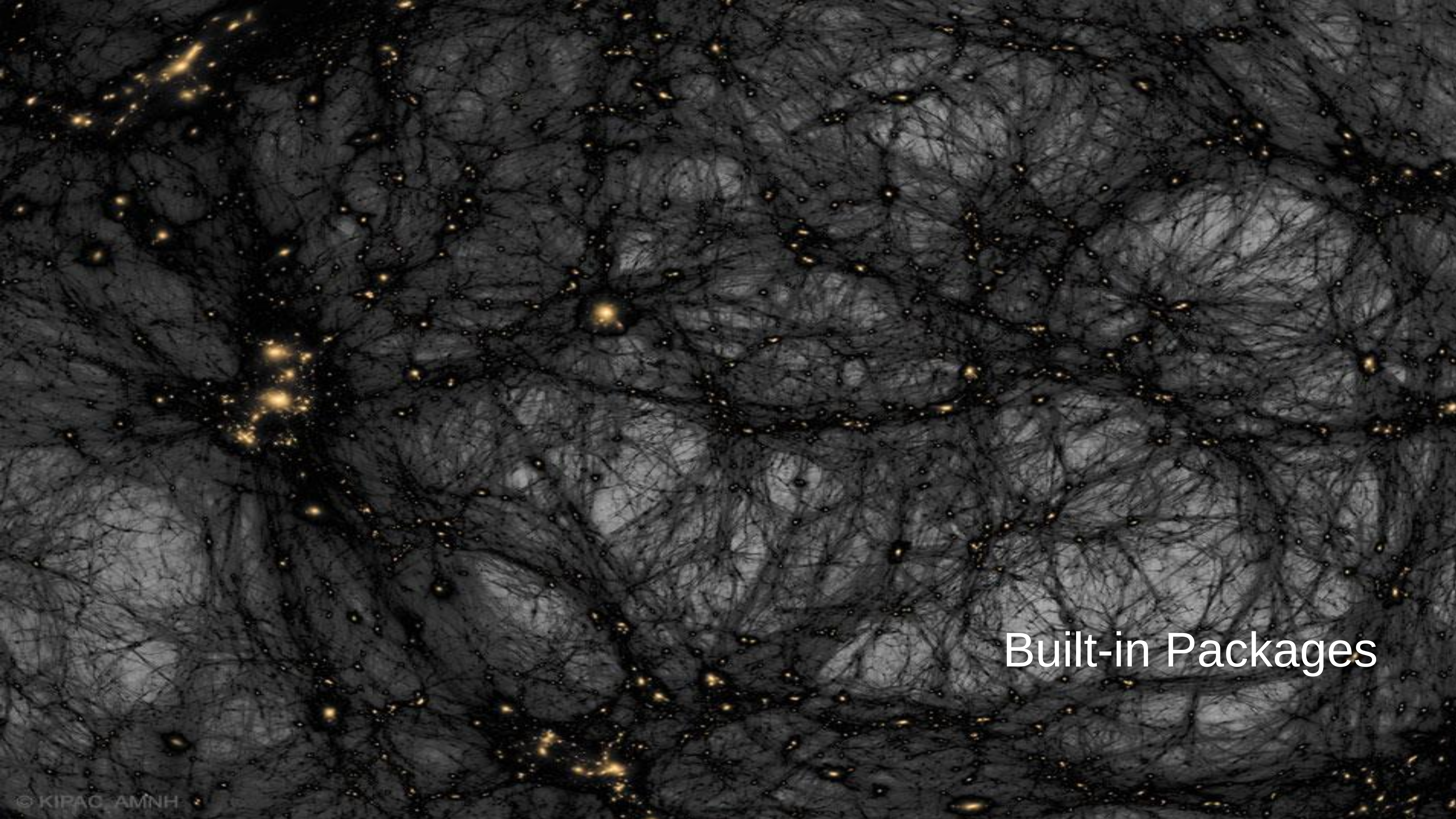
Valid Node Checking (2:2)

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

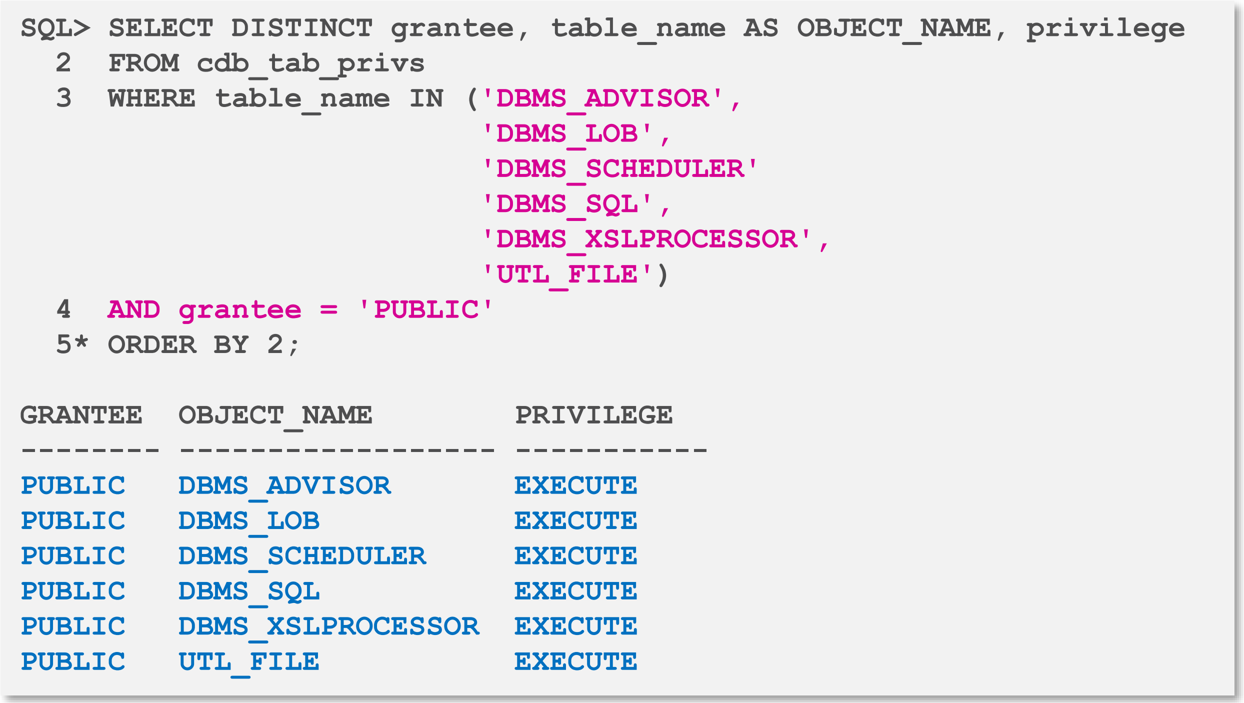
Built-in Packages



© KIPAC, AMNH

File System Access Risks (1:4)

- 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



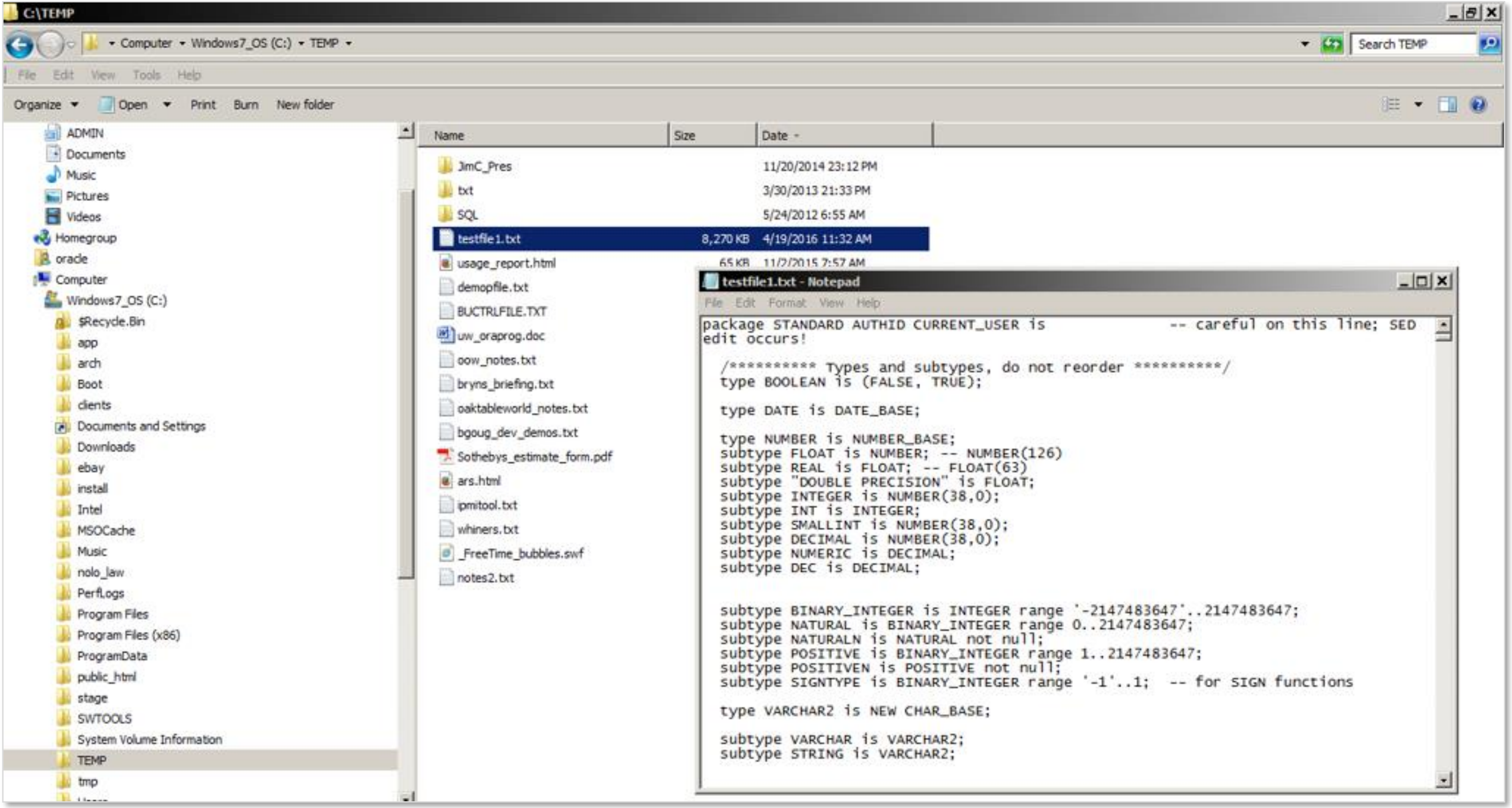
```
SQL> SELECT DISTINCT grantee, table_name AS OBJECT_NAME, privilege
  2  FROM cdb_tab_privs
  3  WHERE table_name IN ('DBMS_ADVISOR',
                          'DBMS_LOB',
                          'DBMS_SCHEDULER'
                          'DBMS_SQL',
                          'DBMS_XSLPROCESSOR',
                          '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 (2:4)

```
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 (3:4)



Name	Size	Date
JimC_Pres		11/20/2014 23:12 PM
txt		3/30/2013 21:33 PM
SQL		5/24/2012 6:55 AM
testfile1.txt	8,270 KB	4/19/2016 11:32 AM
usage_report.html	65 KB	11/2/2015 7:57 AM
demopfile.txt		
BUCTRLFILE.TXT		
uw_oraprog.doc		
oow_notes.txt		
bryns_briefing.txt		
oaktableworld_notes.txt		
bgoug_dev_demos.txt		
Sothebys_estimate_form.pdf		
ars.html		
ipmitool.txt		
whiners.txt		
_FreeTime_bubbles.swf		
notes2.txt		

```
package STANDARD AUTHID CURRENT_USER is              -- careful on this line; SED
edit occurs!

  /********** Types and subtypes, do not reorder **********/
  type BOOLEAN is (FALSE, TRUE);

  type DATE is DATE_BASE;

  type NUMBER is NUMBER_BASE;
  subtype FLOAT is NUMBER; -- NUMBER(126)
  subtype REAL is FLOAT; -- FLOAT(63)
  subtype "DOUBLE PRECISION" is FLOAT;
  subtype INTEGER is NUMBER(38,0);
  subtype INT is INTEGER;
  subtype SMALLINT is NUMBER(38,0);
  subtype DECIMAL is NUMBER(38,0);
  subtype NUMERIC is DECIMAL;
  subtype DEC is DECIMAL;


  subtype BINARY_INTEGER is INTEGER range '-2147483647'..2147483647;
  subtype NATURAL is BINARY_INTEGER range 0..2147483647;
  subtype NATURALN is NATURAL not null;
  subtype POSITIVE is BINARY_INTEGER range 1..2147483647;
  subtype POSITIVEN is POSITIVE not null;
  subtype SIGNTYPE is BINARY_INTEGER range '-1'..1;  -- for SIGN functions

  type VARCHAR2 is NEW CHAR_BASE;

  subtype VARCHAR is VARCHAR2;
  subtype STRING is VARCHAR2;
```

File System Access Risks (4:4)

- 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

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

```
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_ADMIN (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_ADMIN (2:2)

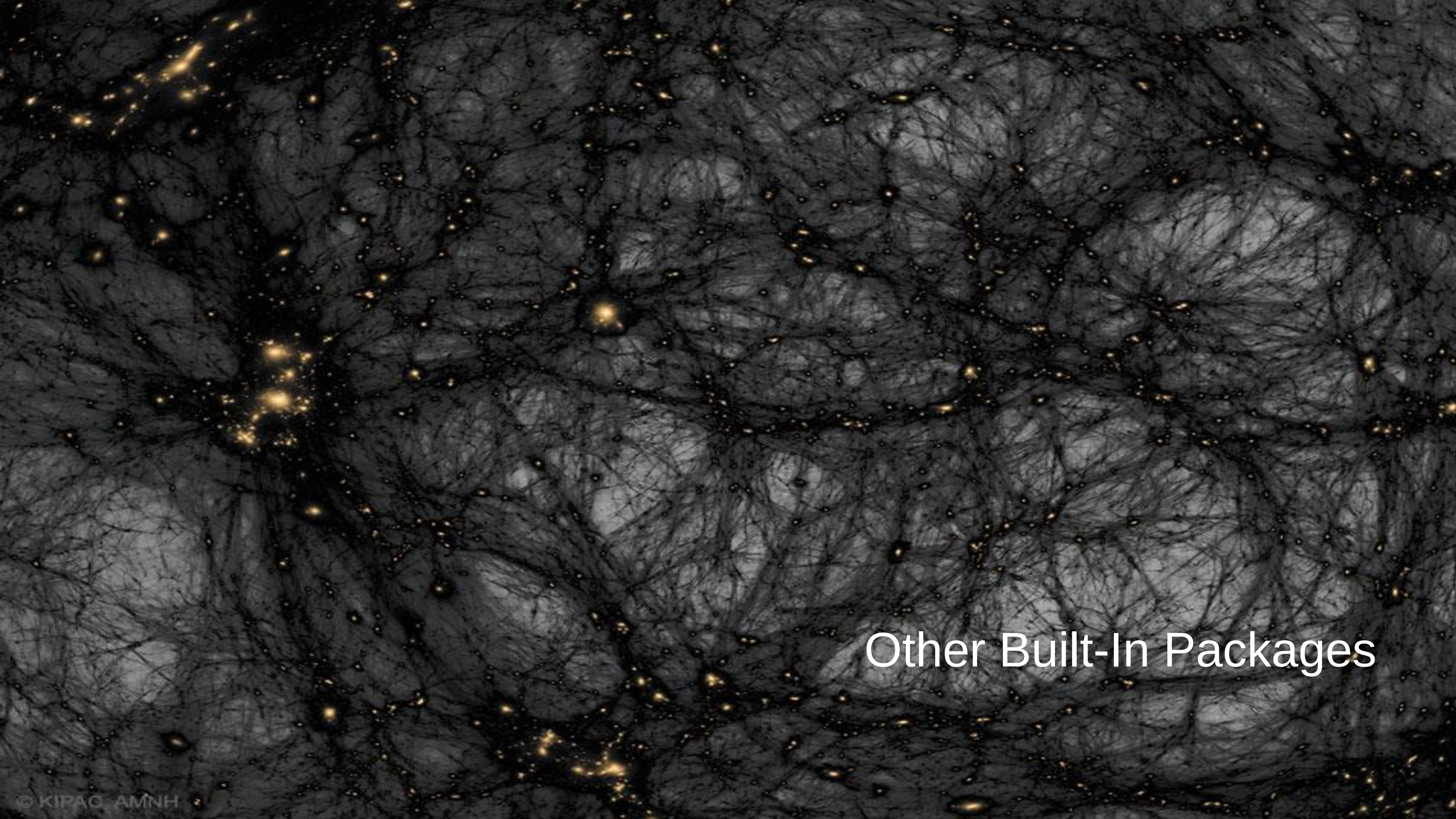
- With a Network Access Control list created it is not possible to access a different IP address

```
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

- This package can be used to extract the contents of entire web sites and store them in your database as a CLOB

```
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

© KIPAC, AMNH

Database Links (1:2)

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

<table>
<tr><td>Explanation</td><td>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.</td></tr>
<tr><td>Validation</td><td><pre>
SELECT *
FROM dba_db_links
ORDER BY 1,2;
</pre></td></tr>
<tr><td>Finding</td><td><pre>
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
</pre></td></tr>
</table>

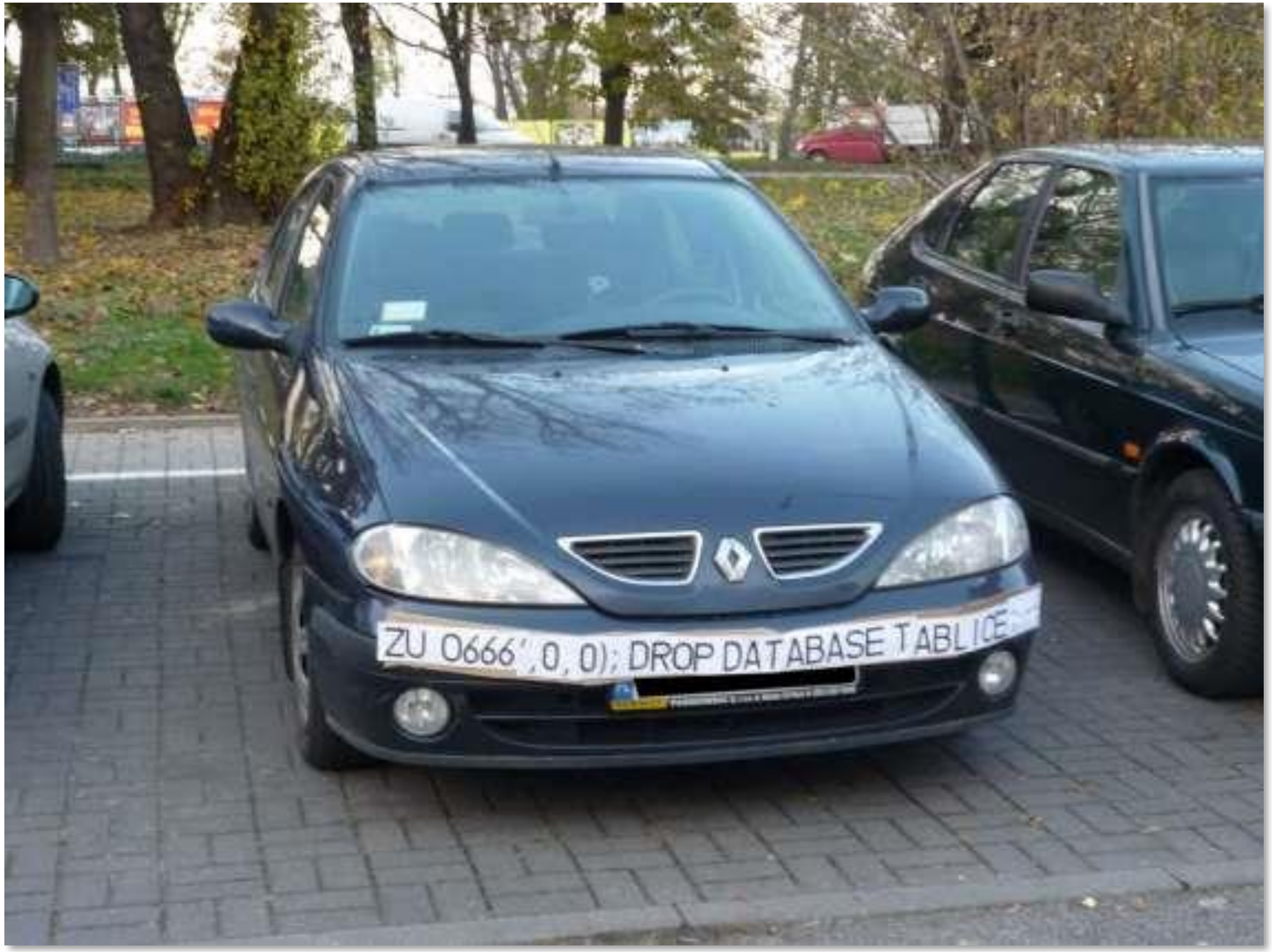
Database Links (2:2)

- DBMS_DISTRIBUTED_TRUST_ADMIN
  - First released with in 2001, contains procedures that maintain a Trusted Servers List
  - Use the package to define whether a server is trusted
  - If a server is not trusted ... a database link cannot be created
    - Cannot be used to stop creation of 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 Attacks (1:2)

- 89% of all data stolen was attacked using SQL Injection



SQL Injection Attacks (2:2)

- 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_AS

```
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
```

© KIPAC, AMNH

Shifting Your Paradigm

First Paradigm Shift

- To be successful you must accept that ...

Break-ins will occur.

Those who fail to study history are doomed to repeat it.

Second Paradigm Shift

- To be successful you must accept that ...

Your job is to increase the difficulty for those breaking in.

If your management doesn't grasp this reality then it is your responsibility to explain it to them.

Securing existing databases is more important than deploying more insecure databases.

Third Paradigm Shift

- To be successful you must accept that ...

The database must be configured to limit the damage.

On Installation

- Disable the DEFAULT profile
- Revoke almost all privileges granted to PUBLIC
- Enable all of the database's default security capabilities

After Installation

- Apply security patches immediately
- Stop using cron - use DBMS_SCHEDULER
- Change passwords regularly - automate the process
- Do not grant the CONNECT, RESOURCE, or DBA roles ever
- Use Proxy Users for every connecting user you create
- Implement Database Vault
- Implement Row Level Security

- There is always someone inside the firewall
- There is always someone with access
- There is a big difference between accessing one record ... and accessing everything
- Most databases in the are configured so that once someone breaks in they get everything
- Make it impossible to SELECT all rows

Included In Your Existing Licenses - Have You Enabled Them?

- Network Encryption - SQLNET.ORA
- Valid Node Checking - SQLNET.ORA
- Password Verify Function - utlpwdmg.sql
- Network Access Control List - DBMS_NETWORK_ACL_ADMIN
- Database Link Management - DBMS_DISTRIBUTED_TRUST_ADMIN
- Created your own secure profiles and revoked the DEFAULT from all users
- Created your own internal roles with only minimum privileges required to do the job
  - Verified no one has CONNECT, RESOURCE, or DBA roles
- Perform all backups as SYSBACKUP
- Perform all Data Guard management as SYSDG
- Perform all Key Management as SYSKM
- Replaced all human-use connections with Proxy Users

Both Train Wrecks Were Avoidable: Only One Was An Accident

```
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 (1:3)

- Securing the Perimeter has proven its primary value is to companies selling products that claim to secure the perimeter
- Auditing is not security
- Passing audits is not security and gives a false sense of security to management
- We must secure data as well as 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
  - We must assume break-ins will take place
- To begin securing data we must utilize the Oracle Database's built-in features
- To fully secure data we must enable built-in features and we must invest real effort ... not just throw money at the problem

Conclusions (2:3)

- 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 operational environments: Less than 1% of DBA "training" involves security
- If you don't have the internal skills to know what to protect and how to protect it you need to go outside your organization and ask for help

Conclusions (3:3)

- We need to arm ourselves with new skills and a new way of thinking about our jobs

```
SELECT more_information
FROM experience
WHERE tool = 'Oracle Database'
AND topic = 'Security';
```

```
email: damorgan18c@dbsecworx.com
web:   www.dbsecworx.com
       www.morganslibrary.org
```

```
*
ERROR at line 1:
ORA-00028:tu sesión ha sido asesinada
```

```
*
ERROR at line 1:
S'ha matat la vostra sessió
```

Thank you

Appendix A: Important Terms

- Attack Surface
  - Any node on the network that can be attacked. It can be the UI, People, anything or anybody that accesses data
- Exploit
  - Take advantage of a flaw or feature
- Hack
  - Anything that can be hacked. Do something it was not intended to do or something you did not think it could do
- Leak
  - Sensitive data has spilled outside of it's protected environment. It has been compromised.
- Spillage
  - Sensitive data has "spilled" outside it's protected environment. It may not have been compromised