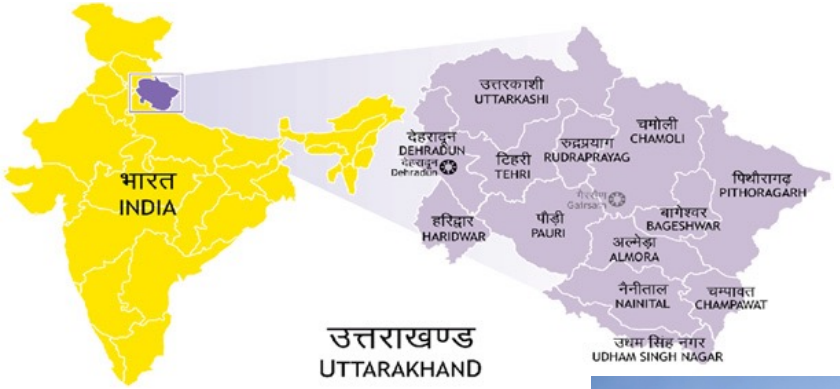
Defense Against the Dark Arts

- Aishwarya Kala

Pythian

About ME



- Lead Database Consultant with Pythian
- Presenter at Oracle GroundBreakers Tour, EMEA tour, OGYatra, SOUG, AIOUG, Sangam
- AIOUG – Director of Special Projects

Oracle ACE Associate

@aishwaryakala13 | https://oratrails-aish.com | aishwarya-kala-471b3616

About Pythian

25
Years in Business

400+
Experts Across 5 Continents

500+
Customers Globally

Google Cloud

Google Cloud Global Partner of the Year Data Management 2020

Google Cloud Partner Managed Service Provider

Premier Partner

140+ Certifications

8 Specializations

amazon web services

aws 50 CERTIFIED
AWS PARTNER NETWORK

Advanced Partner

175+ Certifications

Azure

Gold Partner

15+ Certifications

ORACLE

Platinum Partner

150+ Certifications

SAP

SAP Certified Partner

40+ Certifications

Oracle ACE Program

500+ technical experts helping peers globally

The **Oracle ACE Program** recognizes and rewards community members for their technical and community contributions to the Oracle community

3 membership tiers

Oracle ACE Director | Oracle ACE Pro | Oracle ACE Associate

For more details on Oracle ACE Program:
ace.oracle.com

Oracle ACE

Nominate

yourself or someone you know:

ace.oracle.com/nominate

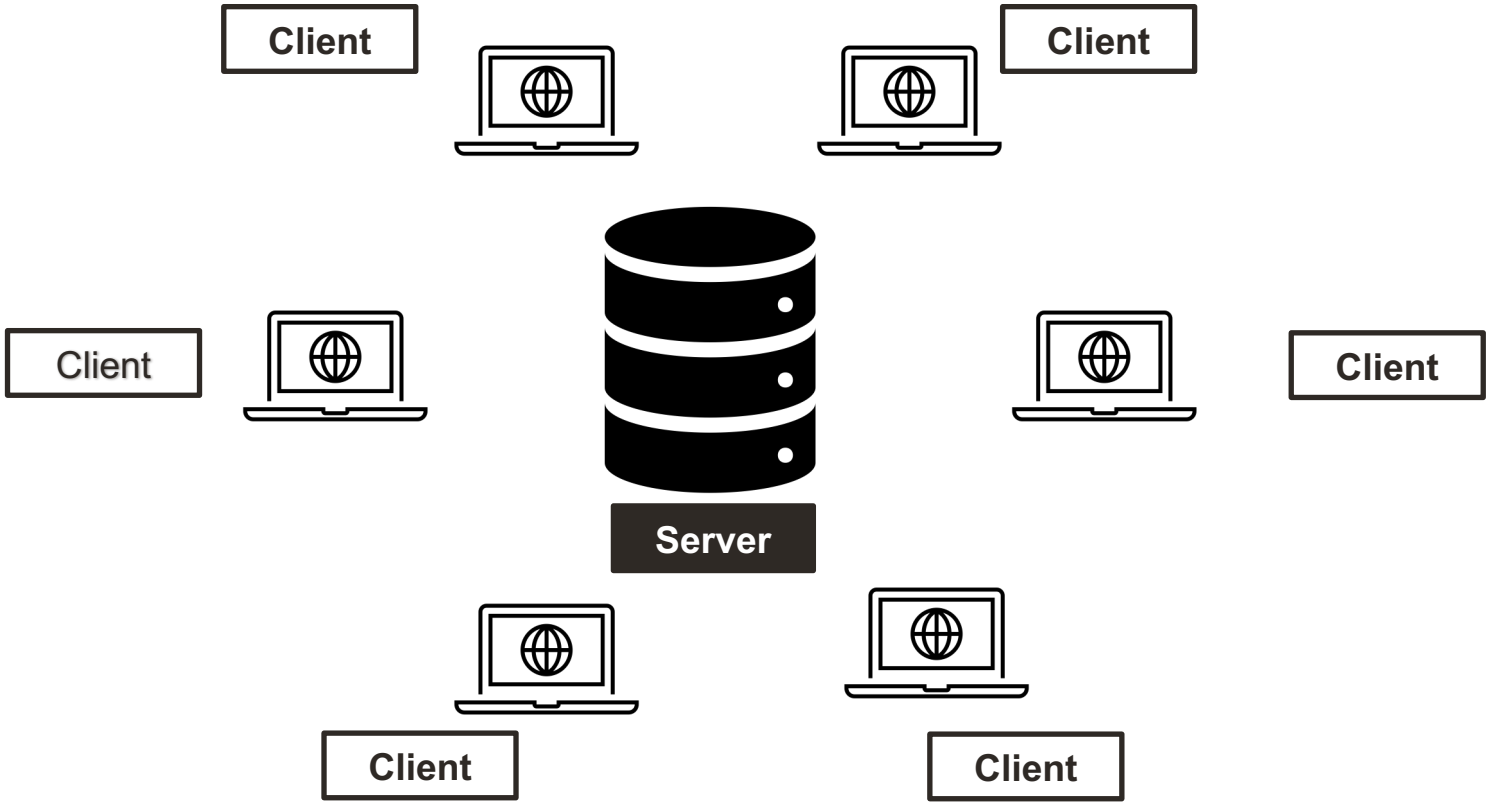
Connect: aceprogram_ww@oracle.com Facebook.com/OracleACEs @oracleace

What are the Dark Arts?

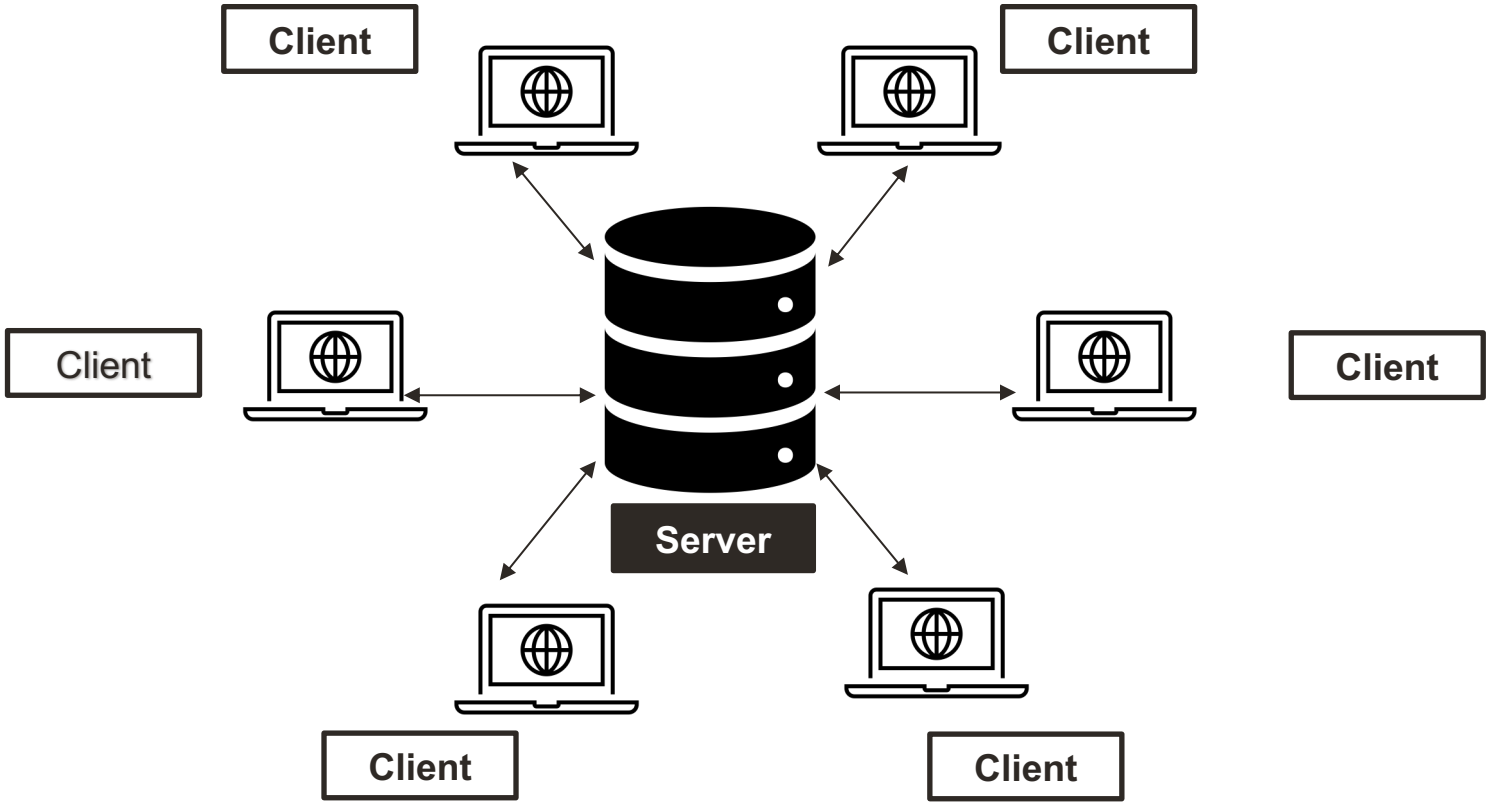

trust
perimeter
engineering
hackers
tools
perimeter-less
prevent
data
threats
breach
insider
model
security
zero
ddos
detect
exploit
cve
assess
social
authentication
phishing

Securing Database Network

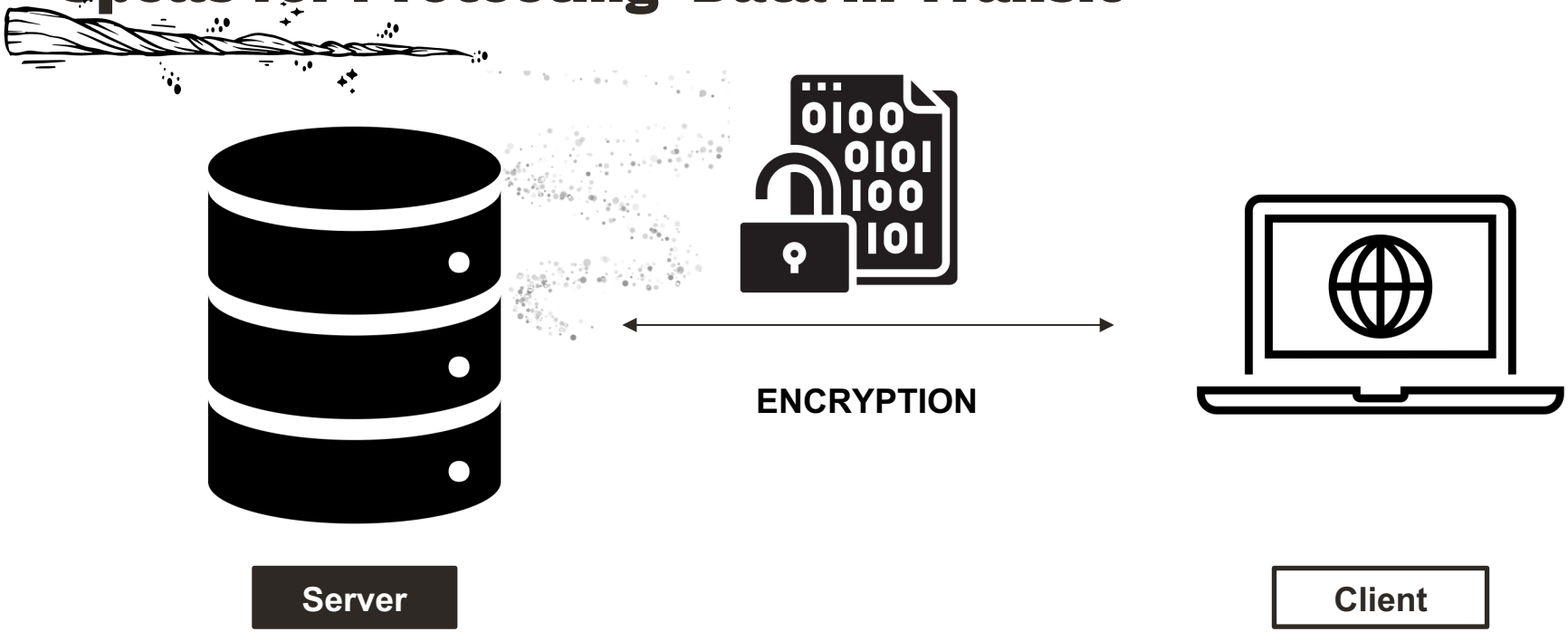
Data In Transit



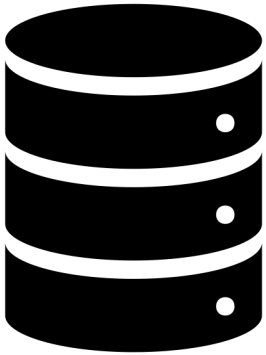
Data In Transit



Spells for Protecting ‘Data In Transit’

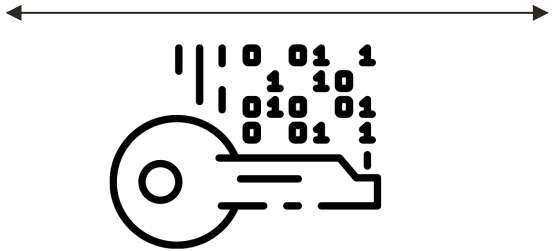


Spells for Protecting ‘Data In Transit’



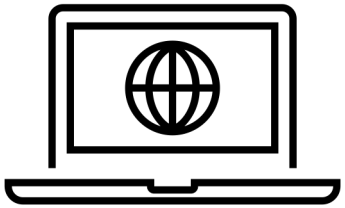
Server

ENCRYPTION



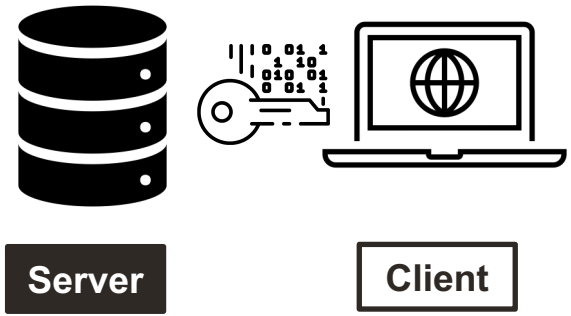
Native Network Encryption

SSL Encryption



Client

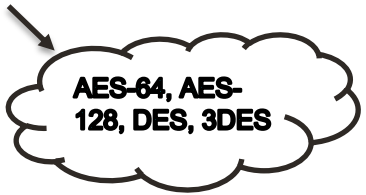
Spells for Protecting ‘Data In Transit’



Native Network Encryption

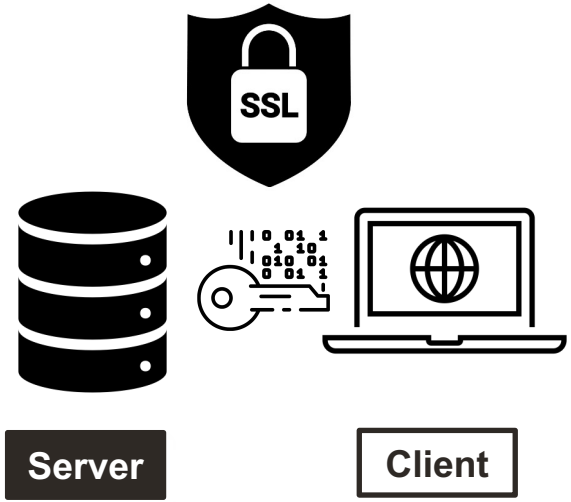
sqlnet.ora

- ENCRYPTION_[server | client]
- ENCRYPTION_TYPES_[server | client]



The initial password supplied for a connection is always encrypted

Spells for Protecting ‘Data In Transit’



SSL/TLS v1.3 Encryption

Signed Certificates

Wallets

Sqlnet.ora

Wallet_location
Ssl_version
Ssl_cipher_suites

Listener.ora → **Listener Config**

Wallet_location

Protocol → TCPS

Spells for Protecting ‘Data In Transit’

SSL/TLS v1.3 Encryption

Signed Certificates

```
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -trusted_cert -cert ./labwork1_certificate_interm1.cer -pwd ******
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -trusted_cert -cert ./labwork1_certificate_interm2.cer -pwd ******
orapki wallet add -wallet /opt/oracle/admin/testdb/wallet -user_cert -cert labwork1_certificate.cer -pwd *****



$ orapki wallet display -wallet /opt/oracle/admin/testdb/wallet

Enter wallet password:
Requested Certificates:
User Certificates:
Subject:        CN=labwork1.subnet.vcn.oraclevcn.com
Trusted Certificates:
 Subject: CN=InCommon RSA Server CA,OU=InCommon,O=Internet2,L=Ann Arbor,ST=MI,C=US
 Subject: CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB
```

Spells for Protecting ‘Data In Transit’

SSL/TLS v1.3 Encryption

Listener Modifications

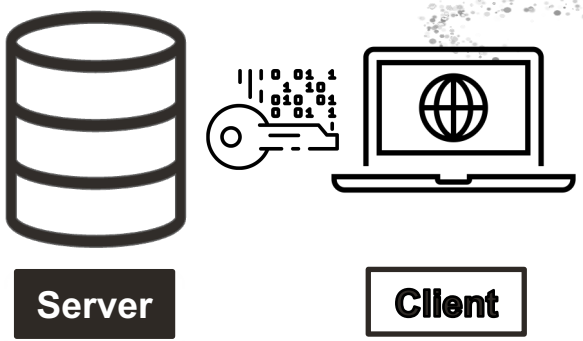
```
$ srvctl modify listener -p "TCP:1521/TCPS:2484"
$ srvctl modify scan_listener -p "TCP:1521/TCPS:2484"
```

```
select instance_name, sys_context('userenv','network_protocol') from v$instance;

INSTANCE_NAME
----------------
SYS_CONTEXT('USERENV','NETWORK_PROTOCOL')
--------------------------------------------------------------------------------
testdb
tcps
```

Spells for Maintaining Integrity of ‘Data In Transit’

Network Data Integrity



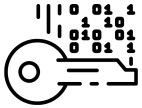
sqlnet.ora

- CRYPTO_CHECKSUM_[server | client]
- CRYPTO_CHECKSUM _TYPES_[server | client]

MD5, SHA1, SHA2

If data is altered
Data Modification, Replay Attack

Spells for Protecting ‘Data In Transit’



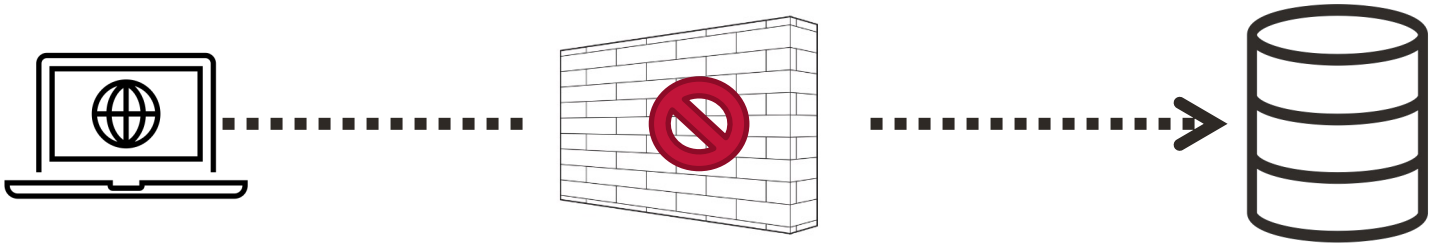
Network Data Integrity

select NETWORK_SERVICE_BANNER from v$session_connect_info
where sid = sys_context(‘USERENV’,’SID’);

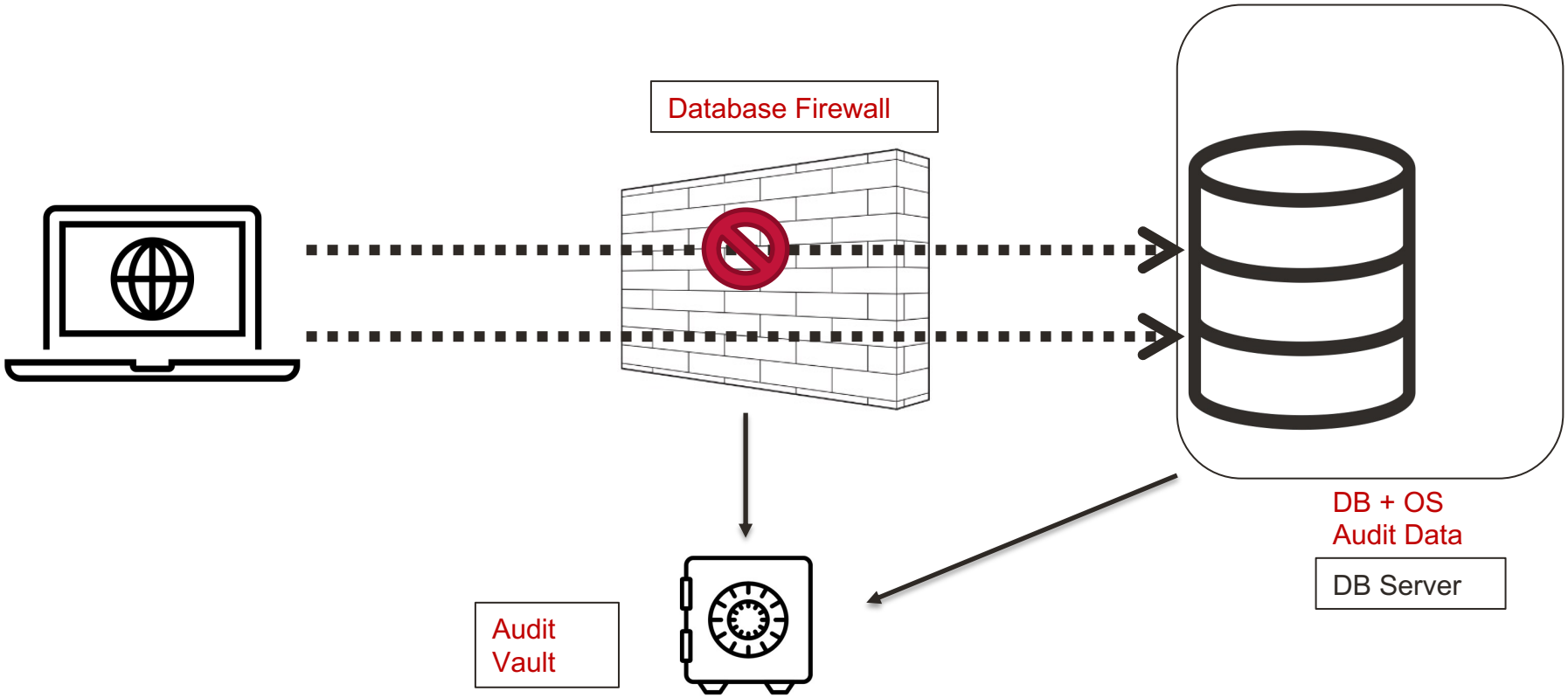
```
NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------------------------------
TCP/IP NT Protocol Adapter for Linux: Version 19.0.0.0.0 - Production
Encryption service for Linux: Version 19.0.0.0.0 - Production
AES128 Encryption service adapter for Linux: Version 19.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 19.0.0.0.0 - Production
MD5 Crypto-checksumming service adapter for Linux: Version 19.0.0.0.0 - Production
```

Spells for Filtering connections

- **Oracle Audit Vault and Database Firewall** (AVDF)
- “AVDF is a complete Database Activity Monitoring (DAM) solution that combines native audit data with network-based SQL traffic capture. “

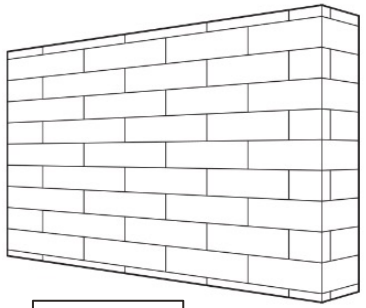


AVDF



AVDF - Benefits

- Collect, Analyze, and Report
- Use of Machine Learning for Anomaly Detection
- Control of Traffic to the Database
- Ability to prevent SQL Injection Attacks




Securing
Servers

CVE – Common Vulnerabilities and Exposures

- Published Vulnerabilities

Bad Actors know about this !!!

- Oracle Releases Quarterly patches- for all its products
  - OS
    - Servers as well as workstations
  - Database, OEM, Exadata, ODA
    - Tuesday closest to 17th of Jan, Apr, July, Oct
    - Do Not Forget to Apply **OJVM** !

PSU, RU, RUR, Exadata Bundle Patches, Windows Bundle Patches, ODA Bundle Patches…….

Security Patches

https://www.oracle.com/security-alerts/cpujul2022.html#AppendixDB

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below. The product area is shown in the Patch Availability Document column.

Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

Affected Products and Versions	Patch Availability Document
Autonomous Health Framework	Oracle Autonomous Health Framework
Big Data Spatial and Graph, versions prior to 23.1	Database
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	Enterprise Manager
Enterprise Manager for MySQL Database	Enterprise Manager
Enterprise Manager Ops Center, version 12.4.0.0	Enterprise Manager
JD Edwards EnterpriseOne Orchestrator, versions 9.2.6.3 and prior	JD Edwards
JD Edwards EnterpriseOne Tools, versions 9.2.6.3 and prior	JD Edwards
MySQL Cluster, versions 7.4.36 and prior, 7.5.26 and prior, 7.6.22 and prior, 8.0.29 and prior, and8.0.29 and prior	MySQL
MySQL Enterprise Monitor, versions 8.0.30 and prior	MySQL
MySQL Server, versions 5.7.38 and prior, 8.0.29 and prior	MySQL
MySQL Shell, versions 8.0.28 and prior	MySQL
MySQL Shell for VS Code, versions 1.1.8 and prior	MySQL
MySQL Workbench, versions 8.0.29 and prior	MySQL
Oracle Agile Engineering Data Management, version 6.2.1.0	Oracle Supply Chain Products
Oracle Agile PLM, version 9.3.6	Oracle Supply Chain Products
Oracle Agile Product Lifecycle Management for Process, versions 6.2.2, 6.2.3	Oracle Supply Chain Products
Oracle Application Express, versions prior to 22.1.1	Database
Oracle Application Testing Suite, version 13.3.0.1	Enterprise Manager

Oracle provides severity ratings – known as **Base Score**, for each vulnerability (based on CVSS 3.1)

Oracle Database Server Risk Matrix

This Critical Patch Update contains 9 new security patches plus additional third party patches noted below for Oracle Database Products. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. 1 of these patches is applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found here.

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.1 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2020-35169	Oracle Database - Enterprise Edition	None	TCPS	Yes	9.1	Network	Low	None	None	Un-changed	High	High	None	12.1.0.2, 19c, 21c	
CVE-2022-21510	Oracle Database - Enterprise Edition Sharding	Local Logon	None	No	8.8	Local	Low	Low	None	Changed	High	High	High	None	See Note 1
CVE-2022-21511	Oracle Database - Enterprise Edition Recovery	EXECUTE ON DBMS_IR.EXECUTESQLSCRIPT	Oracle Net	No	7.2	Network	Low	High	None	Un-changed	High	High	High	None	See Note 1
CVE-2022-21565	Java VM	Create Procedure	Oracle Net	No	6.5	Network	Low	Low	None	Un-changed	None	High	None	12.1.0.2, 19c, 21c	
CVE-2022-24729	Oracle Application Express (CKEditor)	User Account	HTTP	No	5.7	Network	Low	Low	Required	Un-changed	None	None	High	Prior t	

The problem with storing password in scripts

```
-bash-4.2$ ls -ltrh
total 4.0K
-rw-r--r--. 1 oracle oinstall 25 Jul  5 19:09 some-script.sh
-bash-4.2$
-bash-4.2$ ls -ltrh
total 4.0K
-rw-r--r--. 1 oracle oinstall 25 Jul  5 19:09 some-script.sh
-bash-4.2$
-bash-4.2$
-bash-4.2$ grep -i config some-script.sh
. ./.some-script.config
-bash-4.2$
-bash-4.2$
-bash-4.2$ cat ./.some-script.config
PASSWORD=critical_password
-bash-4.2$
```

The problem with storing password in scripts

```
[akala@lab1~]$ ps -ef | grep rman
oracle    4669 26916  1 00:22 pts/1    00:00:01 rman target / catalog rman/rman_password@catalog_db
akala    20213 11800  0 00:23 pts/0    00:00:00 grep --color=auto rman
```

```
-bash-4.2$ strings /proc/841/environ | grep -i rman
RMAN_PASSWORD=mypassword
RMAN_USER=c##rman
```

“Secure External Password Store (SEPS)”

WALLET

- **Oracle Wallet Manager (OWM)**
- **mkstore**
- **orapki**

```
$mkstore  -wrl /opt/oracle/admin/testdb/wallet  -listCredential
Oracle Secret Store Tool Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
Copyright (c) 2004, 2019, Oracle and/or its affiliates. All rights reserved.

Enter wallet password:
List credential (index: connect_string username)
1: testdb_bkp sys
```

“Secure External Password Store (SEPS)”

SQLNET.ORA

- WALLET_OVERRIDE=TRUE
- WALLET_LOCATION= the location of your wallet

TNSNAMES.ORA

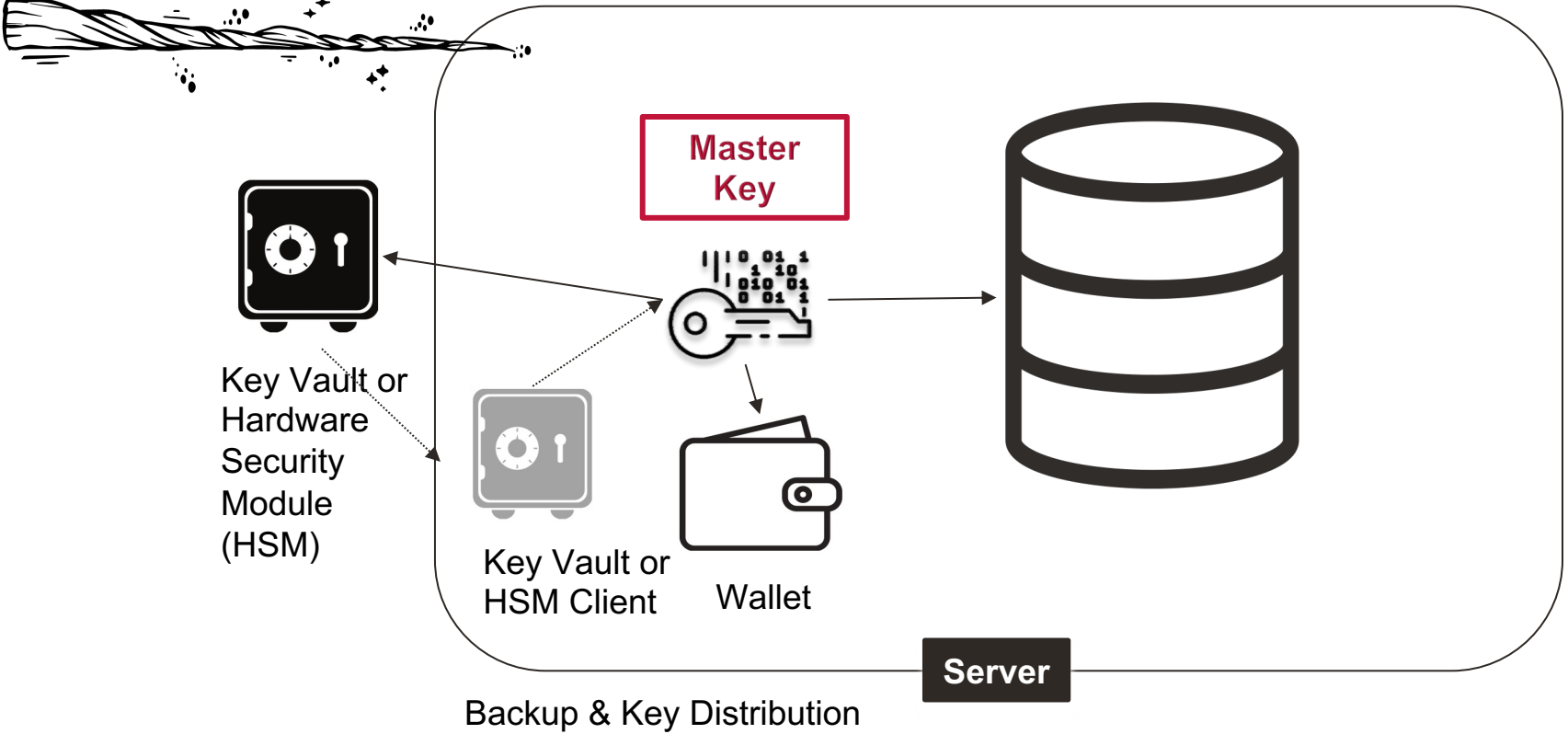
- MY_WALLET_DIRECTORY = < the location of your wallet >

```
$ sqlplus /@testdb_bkp
```

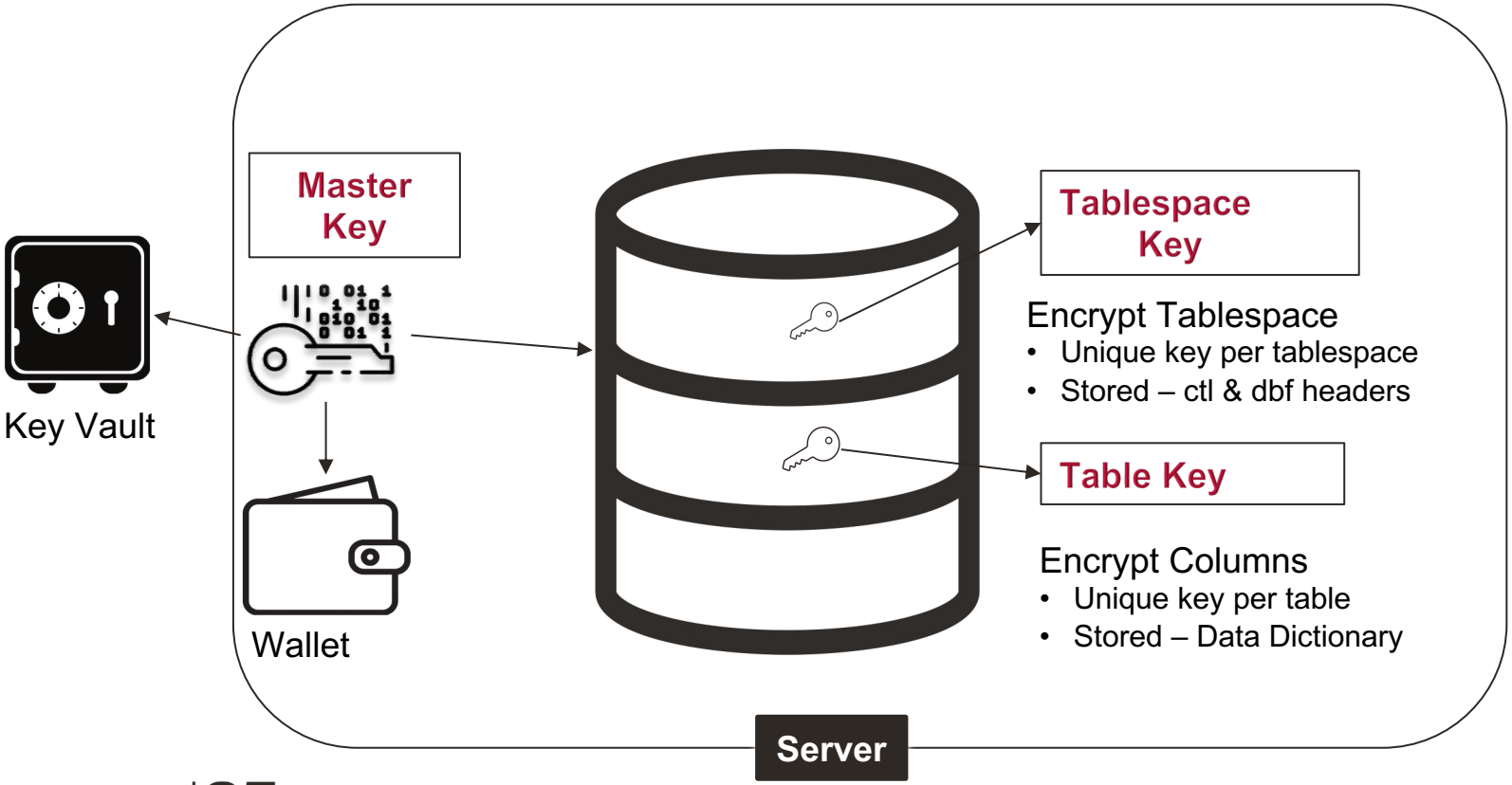
Data at Rest – How is that vulnerable ?

- Access to unencrypted datafiles on your storage
- Compromised Database backups
- Compromised Database Exports

Transparent Data Encryption

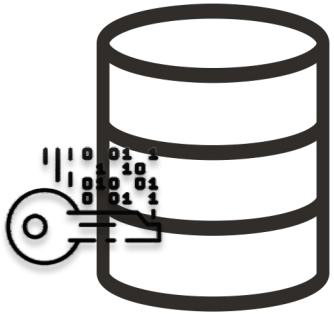


Transparent Data Encryption



Transparent Data Encryption

- Integrated with Compression, Datapump, RMAN !



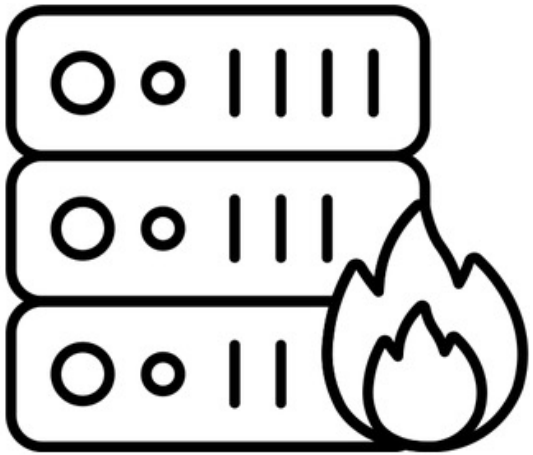
Save the TDE Key based on your backup retention!

You will need them if you restore

Advanced Security Option

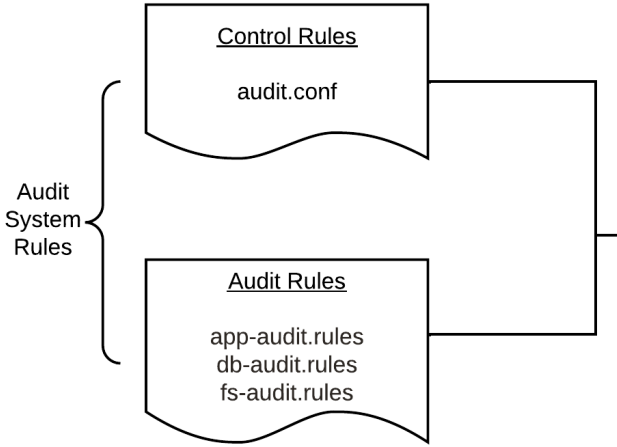
OS & Audit Logs

- A bad actor with root or super privileges could edit the audit log and mask the audited actions
- Edit/modification of the messages, syslog files to **hide** suspicious activity



Save the logs to an external location

OS Logs & Auditing

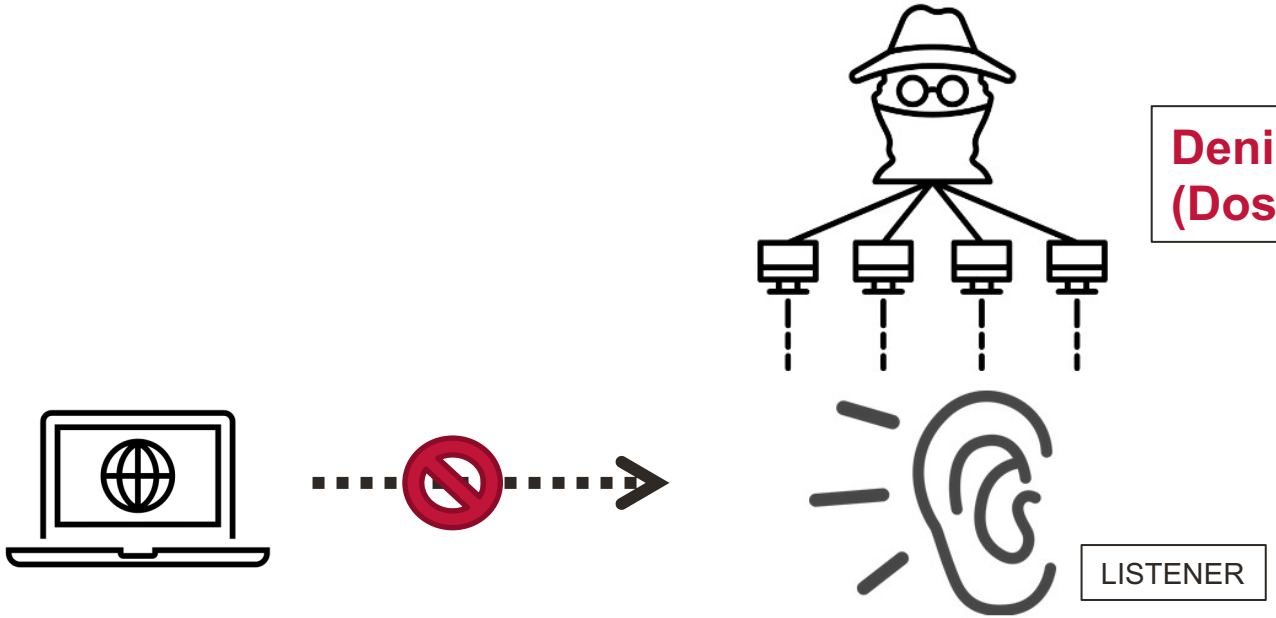


- Examples Audit Rules for user actions
  - Audit all OS Commands by users in the group " DBA"
  - Audit all OS Commands by oracle & grid accounts
  - Audit all OS Commands under sudo /sudo su shells
- Examples Audit Rules for DB files
  - Rule to Audit any changes to the Files like parameter, listener, oratab, sudoers, audit config, rsyslog, messages,
- Lock the config !

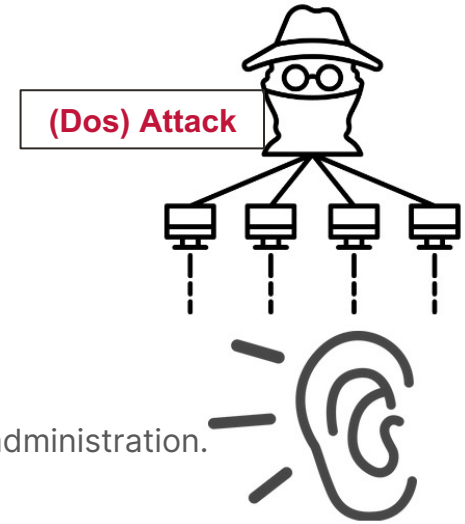
```
# Rule to Audit any changes to the database parameter files
-w /u01/app/oracle/admin/<sid>/pfile/init_sid.ora -p wa -k sid-init-change
```

Protecting Data

Connecting to your database



Securing the Listener



- Avoid the use of DEFAULT (1521) Port & name LISTENER.
- Protect the listener config
  - Listener password – deprecated since 12.1 since it enables remote listener administration.
  - OS Based Authentication
- Limit the time that the resources can be held before authentication.
  - sqlnet.INBOUND_CONNECT_TIMEOUT
  - listener.INBOUND_CONNECT_TIMEOUT_listener_name

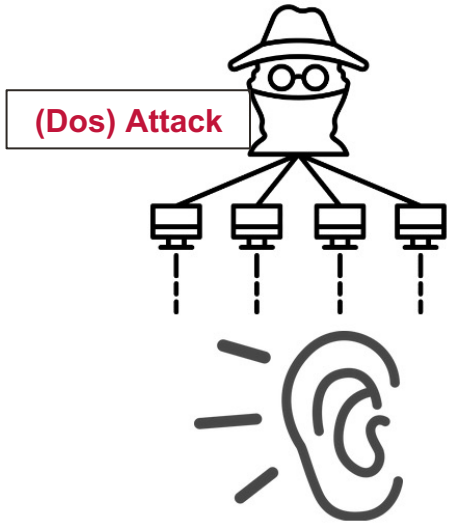
Establish the connection + complete authentication

IP logged !

Send the connection request to listener

Listener timeout value Lower than sqlnet value !

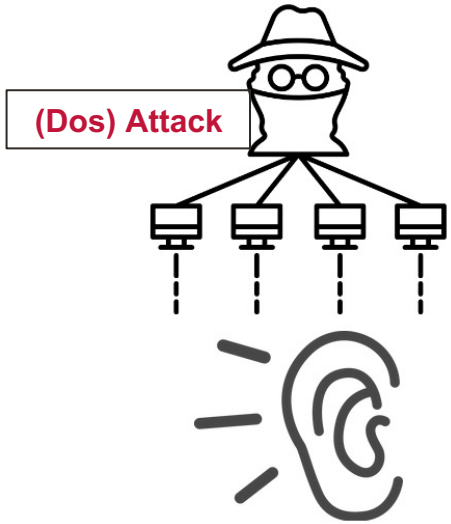
Securing the Listener



- Restrict the Services that can register with a listener
  - Prevents registration of malicious services running on remote notes
- Valid Node Checking (VNCR).
- Values
  - OFF | 0
  - ON | 1 | LOCAL
  - SUBNET | 2

```
VALID_NODE_CHECKING_REGISTRATION_listener_name = ON
```

Securing the Listener

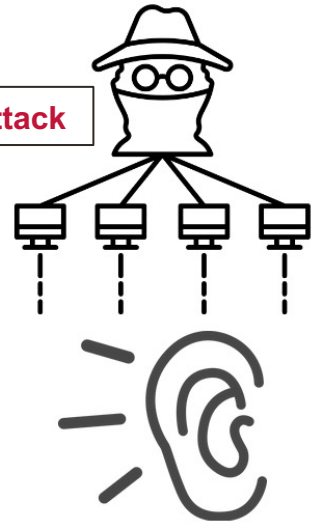


- Restrict the Services that can register with a listener
  - Prevents registration of malicious services running on remote notes
- Valid Node Checking (VNCR).
- Values
  - OFF | 0
  - ON | 1 | LOCAL
  - SUBNET | 2

RAC
MOS Doc ID 1600630.1

VALID_NODE_CHECKING_REGISTRATION_listener_name
REGISTRATION_INVITED_NODES_listener_name

Securing the Listener



- Secure the $TNS_ADMIN – review file permissions
- Using Logging EFFECTIVELY !
  - SEC_PROTOCOL_ERROR_TRACE_ACTION = { NONE | **TRACE** | LOG | ALERT }
- Remove unused Services

```
SELECT
        b.username,
       a.client_version, a.osuser,
       b.machine, b.module, b.program,
       a.client_charset , a.client_driver,
       b.service_name
  FROM gv$session_connect_info a, gv$session b
 WHERE a.sid = b.sid
       and a.serial# = b.serial#
       and a.AUTHENTICATION_TYPE !='INTERNAL'
       ORDER BY client_version, username;

USERNAME        CLIENT_VERSION      OSUSER          MACHINE                         MODULE          PROGRAM         CLIENT_CHARSET
                CLIENT_DRIVER       SERVICE_NAME
--------------- ------------------- --------------- ------------------------------- --------------- --------------- ----------------
SCOTT               12.1.0.2.0      abc001          AD\APP-P-REM033                 salesforce.exe  salesforce.exe  WE8MSWIN1252
                                    SALES
SCOTT               12.1.0.2.0      abc360          AD\APP-P-REM033                 salesforce.exe  salesforce.exe  WE8MSWIN1252
                                    SALES
SCOTT               12.1.0.2.0      abc360          AD\APP-P-REM033                 salesforce.exe  salesforce.exe  WE8MSWIN1252
                                    SALES
SCOTT               12.1.0.2.0      abc591          AD\APP-P-REM013                 salesforce.exe  salesforce.exe  WE8MSWIN1252
                                    SALES
SCOTT               12.1.0.2.0      abc591          AD\APP-P-REM013                 salesforce.exe  salesforce.exe  WE8MSWIN1252
                                    SALES
SCOTT               19.0.16.0.0     salesforceconnect   APPPOOL\APP-P-BOOKI01       booking.exe     booking.exe     WE8MSWIN1252
                CDPM.NET : 19.1.0.0.0   OE
SCOTT               19.0.16.0.0     salesforceconnect   APPPOOL\APP-P-BOOKI02       booking.exe     booking.exe     WE8MSWIN1252
                CDPM.NET : 19.1.0.0.0   OE
SCOTT               19.0.16.0.0     salesforceConnect   APPPOOL\APP-P-BOOKI02       booking.exe     booking.exe     WE8MSWIN1252
                CDPM.NET : 19.1.0.0.0   OE
SCOTT               19.0.16.0.0     salesforceconnect   APPPOOL\APP-P-BOOKI02       booking.exe     booking.exe     WE8MSWIN1252
                CDPM.NET : 19.1.0.0.0   OE
```

If required – Capture the history

```
SELECT
        b.username,
       a.client_version, a.osuser,
       b.machine, b.module, b.program,
       a.client_charset , a.client_driver,
       b.service_name
 FROM gv$session_connect_info a, gv$session b
 WHERE a.sid = b.sid
       and a.serial# = b.serial#
        and a.AUTHENTICATION_TYPE !='INTERNAL'
        ORDER BY client_version, username;


USERNAME             CLIENT_VERSION       OSUSER               MACHINE                                  MODULE               PROGRAM              CLIENT_CHARSET
                CLIENT_DRIVER                SERVICE_NAME
-------------------- -------------------- -------------------- ---------------------------------------- -------------------- -------------------- ----------------------------
-------------- ------------------------------
SCOTT                12.1.0.2.0           abc001               AD\APP-P-REM033                          salesforce.exe       salesforce.exe       WE8MSWIN1252
                                          SALES
SCOTT                12.1.0.2.0           abc360               AD\APP-P-REM033                          salesforce.exe       salesforce.exe       WE8MSWIN1252
                                          SALES
SCOTT                12.1.0.2.0           abc360               AD\APP-P-REM033                          salesforce.exe       salesforce.exe       WE8MSWIN1252
                                          SALES
SCOTT                12.1.0.2.0           abc591               AD\APP-P-REM013                          salesforce.exe       salesforce.exe       WE8MSWIN1252
                                          SALES
SCOTT                12.1.0.2.0           abc591               AD\APP-P-REM013                          salesforce.exe       salesforce.exe       WE8MSWIN1252
                                          SALES
SCOTT                19.0.16.0.0          salesforceconnect      APPPOOL\APP-P-BOOKI01                    booking.exe            booking.exe          WE8MSWIN1252
               ODPM.NET : 19.1.0.0.0        OE
SCOTT                19.0.16.0.0          salesforceconnect      APPPOOL\APP-P-BOOKI02                    booking.exe            booking.exe          WE8MSWIN1252
               ODPM.NET : 19.1.0.0.0        OE
SCOTT                19.0.16.0.0          salesforceConnect      APPPOOL\APP-P-BOOKI02                    booking.exe            booking.exe          WE8MSWIN1252
               ODPM.NET : 19.1.0.0.0        OE
SCOTT                19.0.16.0.0          salesforceconnect      APPPOOL\APP-P-BOOKI02                    booking.exe            booking.exe          WE8MSWIN1252
               ODPM.NET : 19.1.0.0.0        OE
```

Authentication

- Weak Passwords
- Default Passwords for sys, system and other privileges accounts
- Weak Policies
- Compromised Passwords

Brute Force Attack

Strengthening Authentication

Brute Force Attack

The Obvious

- Strong Passwords – Password Verify Function
  - ora12c_verify_function & ora12c_strong_verify_function - utlpwdmg.sql

Create your Own
MOS Doc ID 2475845.1

- Init Parameters
  - SEC_MAX_FAILED_LOGIN_ATTEMPTS
  - SEC_CASE_SENSITIVE_LOGON

Misleading ORA-01017: Invalid username/password;

Be aware of issues with Password Versions when using SQLNET.ALLOWED_LOGON_VERSION_xx

A Great Blog by Mike Detrich https://mikedietrichde.com/2017/04/24/having-some-fun-with-sec_case_sensitive_

MOS Note: 2040705.1

Strengthening Authentication

Brute Force Attack

- Account Profile
  - SESSIONS_PER_USER
  - FAILED_LOGIN_ATTEMPTS
  - INACTIVE_ACCOUNT_TIME
  - PASSWORD_ROLLOVER_TIME (Backported to 19.12+!)

DBA_USERS -> LAST_LOGIN

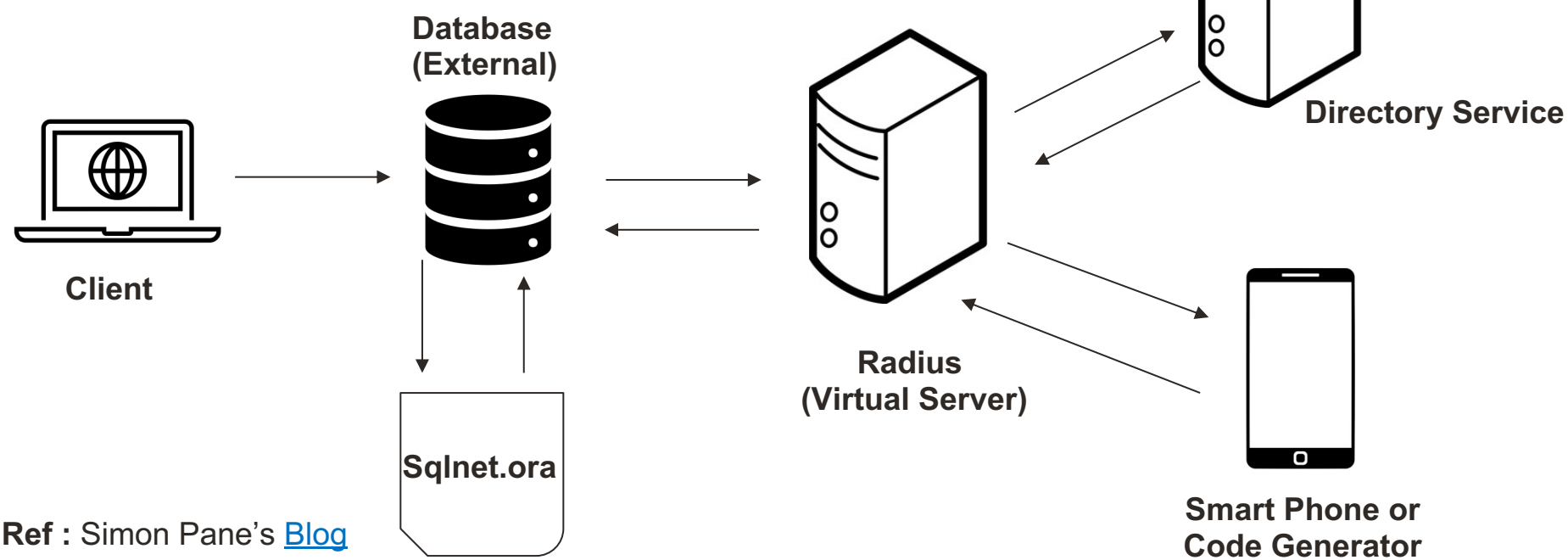
- DBA_PROFILES
- Enforcing Best Practices for DBA's as well as users
  - Use nominative accounts (default)
  - For Privileged Tasks (use sysdba account)

Using Strong Authentication

- Global Authentication and authorization.
  - SSL, Kerberos, or Windows native authentication
  - Centrally Managed Users **(Doc ID 2462012.1)**
- External Authentication
  - OS Based (e.g. SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, and SYSKM)
  - Network Based (e.g. Kerberos , Radius)

Multi Factor Authentication !!

How MFA/2FA Works



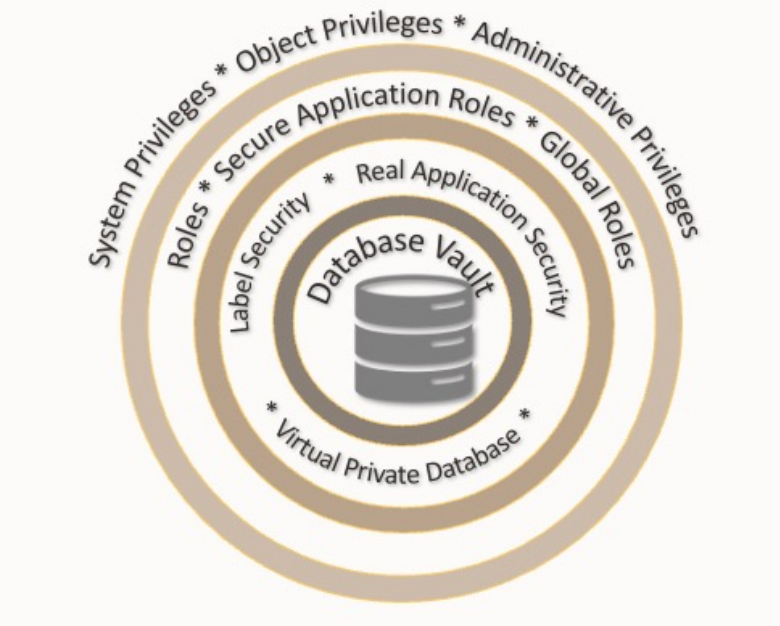
Ref : Simon Pane's Blog

Insider Threats

- Employee negligence
- Lack of robust security by a third-party vendor
- Susceptibility to Social Engineering Attack
- Malicious Actions of Employees

Control Data Access

Tools



Choose based on your requirement.

e.g. DBA's shouldn't view the data in application tables.

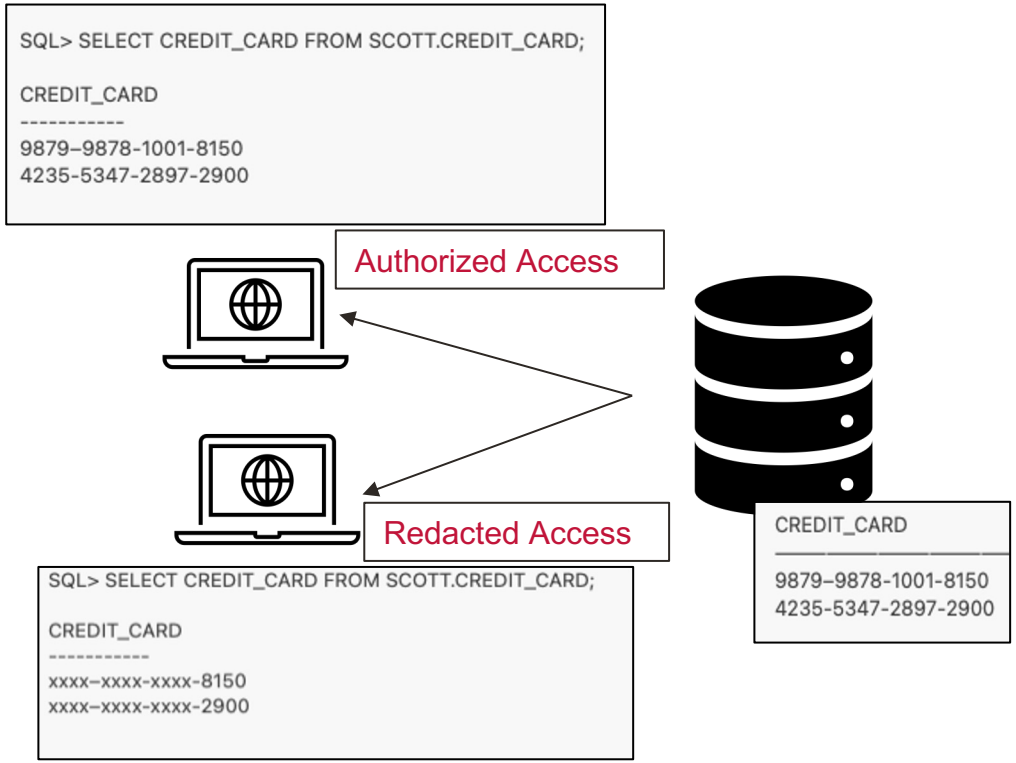
- Separation of Duties, privileged user controls (Data Vault)
- Row-level control (VPD,RAS,OLS)
- Column-level control (VPD,RAS)

Hide The Data

Data Redaction

- Dynamic Data Masking of the result-set
- Based on username, IP, application context, and other session factors
- No changes to the data stored.

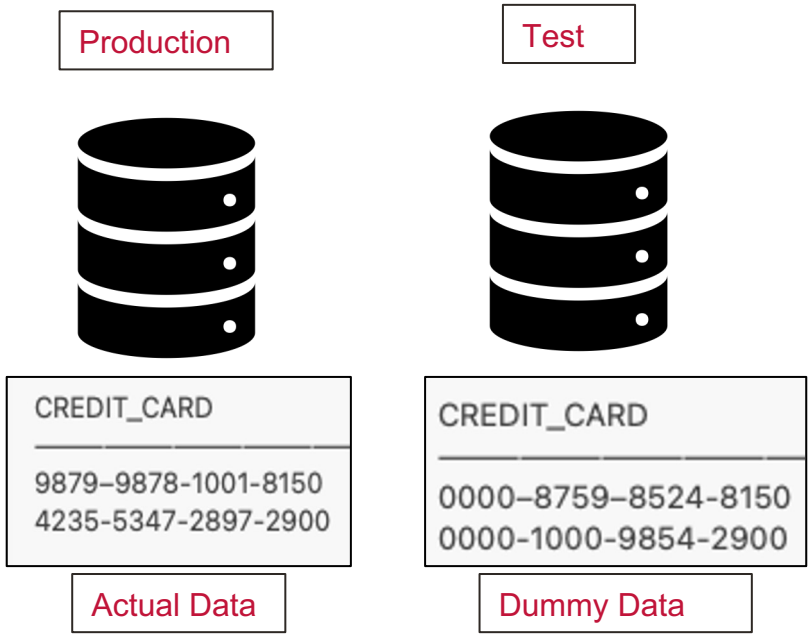
Advanced Security Option (with TDE)



Hide The Data

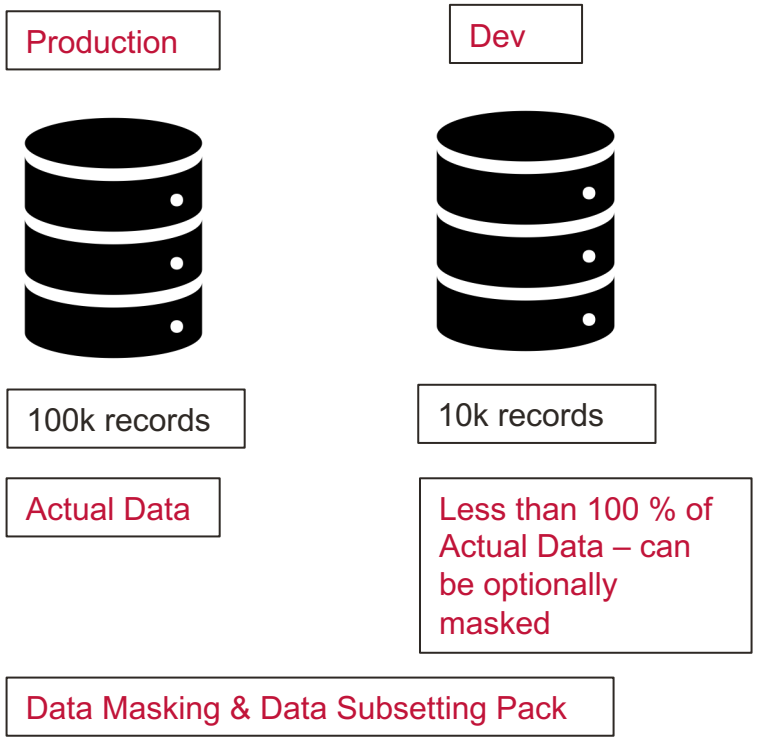
- Data Redaction
- **Data Masking**
  - Substituting or replace the values based on rules
  - For non-production, load testing environments
  - Mask based on conditions generate random values with the same format, shuffle records

Data Masking & Data Subsetting Pack



Hide The Data

- Data Redaction
- Data Masking
- **Data Subsetting**
  - Remove the values based on rules i.e. Subset
  - Size down e.g. Development environment or a customer-specific test
  - Can Integrate with Masking
  - Conditions, Relative tables size i.e 5% of table data, Partitioning



And Remember..

- Elevated Privileges
  - Grant Execute ANY Procedure

Can lead to users creating procedures that can truncate tables in ANY schema

- SQL92_SECURITY
  - Set to TRUE

Users have SELECT privilege on a table when executing an UPDATE or DELETE

- SQL Injection Prevention Best Practices
  - Use BIND Variables
  - Avoid concatenated inputs for Dynamic SQL
  - Explore DBMS_ASSERT

- Use Schema-only accounts.
- AUDIT as needed

Mantra ! Reduce the Attack Surface

Mantra ! Reduce the Attack Surface

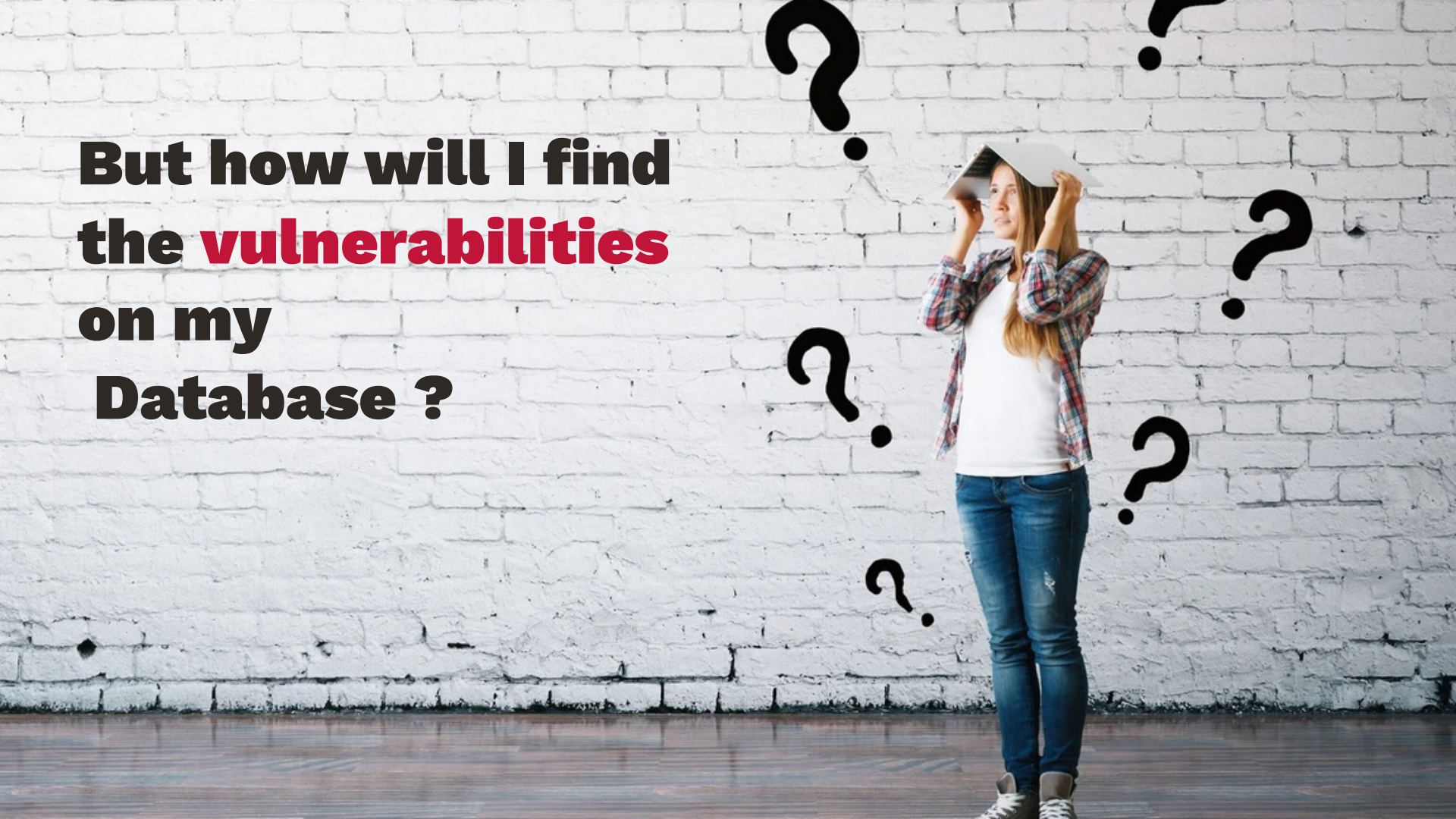
- **Remove Not used database components**

  e.g. APEX (Doc ID 1518046.1)

- **User, roles**
- **DB links**

As a thumb rule, never have anything that you do not need on your database!

But how will I find the vulnerabilities on my Database ?



DB Security Assessment Tool (DBSAT)

Free !!!

Oracle Database Security Assessment

Highly Confidential

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Fri Apr 06 2018 21:22:00	Fri Apr 06 2018 21:27:28	2.0.1 (December 2017) - d526

Database Identity

Name	Platform	Database Role	Log Mode	Created
[redacted]	Linux x86 64-bit	PRIMARY	ARCHIVELOG	Fri Oct 14 2016 14:27:00

https://www.oracle.com/in/database/technologies/security/dbsat.html

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	4	0	0	3	4	0	11
Privileges and Roles	3	16	0	0	0	0	19
Authorization Control	0	0	2	0	0	0	2
Data Encryption	0	1	1	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	3	5	1	0	3	0	12
Database Configuration	6	3	0	1	2	1	13
Network Configuration	1	0	0	0	1	0	2
Operating System	2	1	0	1	1	0	5
Total	**19**	**26**	**9**	**5**	**11**	**2**	**72**

Basic Information

Sample Schemas

USER.SAMPLE	CIS
Status	Medium Risk
Summary	Found 1 sample schema.
Details	`Sample schemas: SCOTT`
Remarks	Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the database.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.3

Inactive Users

USER.INACTIVE	
Status	Low Risk
Summary	Found 4 unlocked users inactive for more than 30 days.
Details	`Inactive users:` [redacted]
Remarks	If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active.

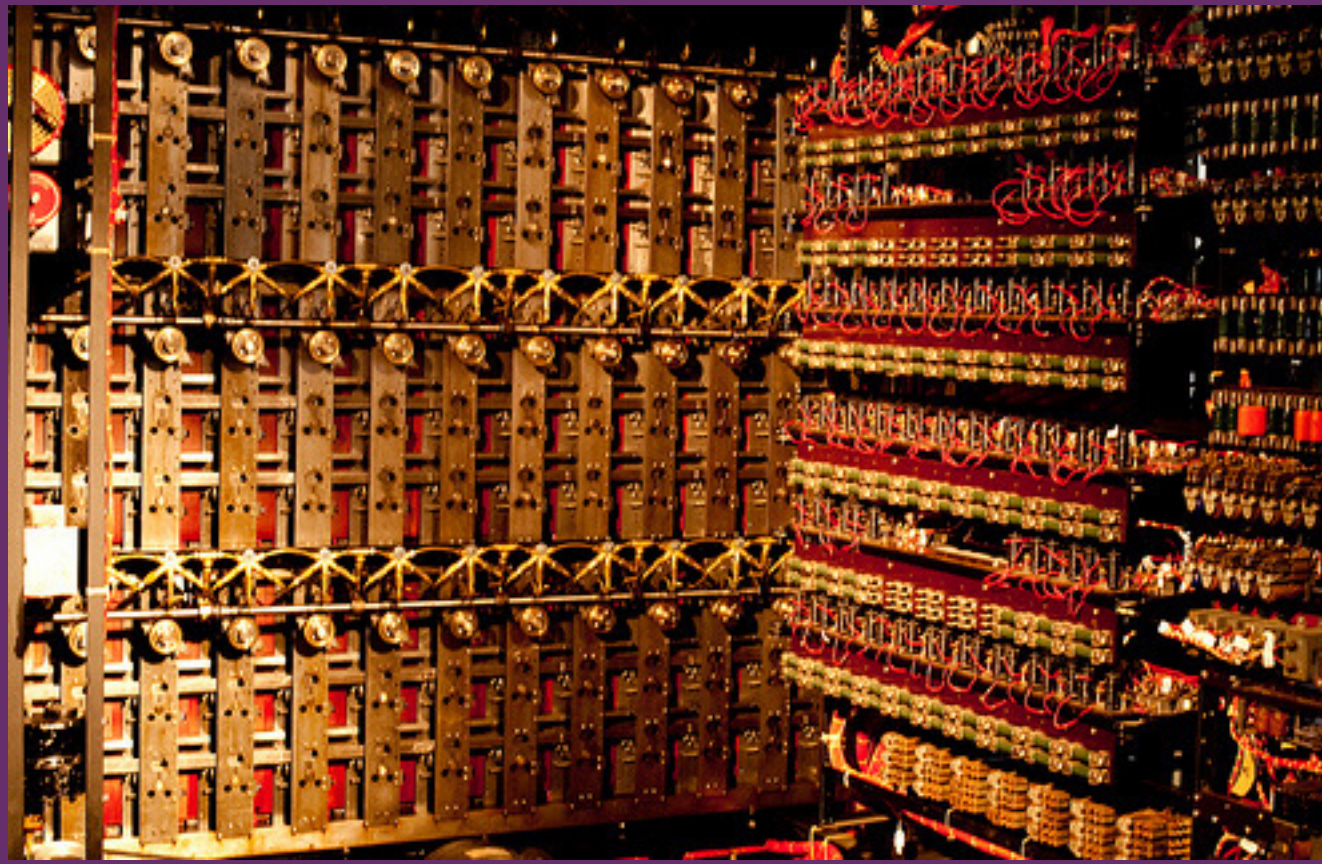
Other Things

- DBSat provides privilege analysis as well a review of roles and user accounts
- Be on a lookout for Configuration Drift
- Use orachk diff report to keep a lookout on the health of your system

References

- https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/
- TDE Explainer by Russ
- https://mikedietrichde.com/2017/04/24/having-some-fun-with-sec_case_sensitive_logon-and-ora-1017/
- https://blog.pythian.com/oracle-database-and-two-factor-authentication-2fa/
- Elevate Privileges & DBSat https://www.youtube.com/watch?v=8YsGxIiLs2k
- https://www.oracle.com/in/database/technologies/security/dbsat.html
- https://blog.pythian.com/token-based-authentication-for-adb-with-iam-part-1/
- https://www.slideshare.net/AishwaryaKala/demystifying-the-use-of-wallets-and-ssl-with-your-database

THANK YOU !!



You can reach me

@aishwaryakala13

aishwarya-kala-471b3616

oratrails-aish.com