Question 1

Examine this command that Is executed:

```
BEGIN
  DBMS_TSDP_PROTECT.ENABLE_PROTECTION_COLUMN(
    schema_name            => 'HR',
    table_name             => 'EMPLOYEES',
    column_name            => 'SALARY',
    policy                 => 'REDACT_AUDIT');
END;
/
```

What is the result?

Options:

A- The salary column is fine grain audited.

B- The salary column is nullified when queried by the database users.

C- The bind variables for the salary column are masked In trace files and vS views.

D- The salary column is encrypted using TDE column encryption.

E- The salary column is redacted when queried by database users.
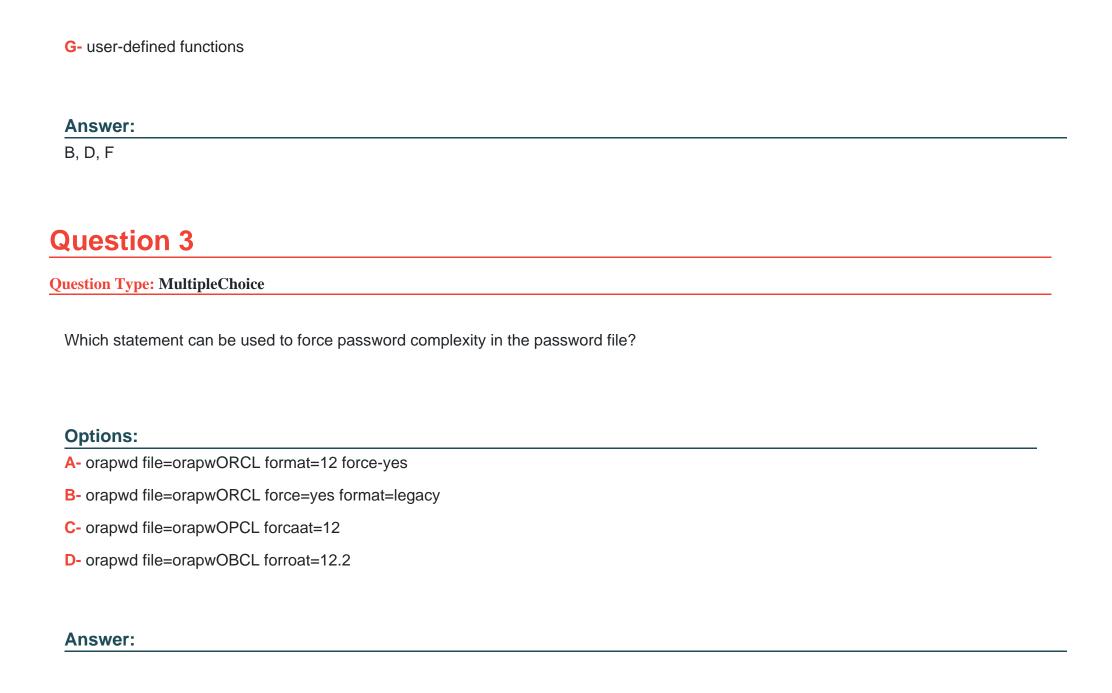
Answer:

E

Question 2

Question Type: MultipleChoice

Data Masking uses a combination of data patterns to discover sensitive dat

a. Which three items are used?

Options:

A- column names

B- encrypted masks

C- column privileges

D- table privileges

E- column comments

F- column data

G- user-defined functions

Question 3

Question Type: **MultipleChoice**

Which statement can be used to force password complexity in the password file?

Options:

A- orapwd file=orapwORCL format=12 force-yes

B- orapwd file=orapwORCL force=yes format=legacy

C- orapwd file=orapwOPCL forcaat=12

D- orapwd file=orapwOBCL forroat=12.2

Answer:

D

Question 4

Examine this list of capabilities:

1. You can automatically restrict common users from accessing pluggable database (PDB).

2. Enabling Database Vault Operations Control In cdbsroot does not automatically enable It In PDBs.

3. Any common user granted the dv_admin role can enable Database Vault Operations Control.

4. To enable Database Vault Operations Control, use the dbms_macadm.enable_app_protection.

5. Common users' and Invokers' right procedures that must access PDB local data can be added to an exception list.

6. To disable Database Vault Operations Control, use the dbms_macadm.disable_app_protection.

Which statements describe Database Vault Operations Control?

Options:

A- 3, 5, 6

B- 2, 3. 6

C- 2, 4, 6

D- 1, 4, 6

E- 1, 2, 3, 5

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which CVSS Version 3.1 metric indicates how close an attacker needs to be to the vulnerable component?

Options:

A- Privileges Required

B- User Interaction

C- Attack Vector

D- Scope

E- Availability

F- Attack Complexity

Answer:

D

Question 6

Question Type: MultipleChoice

What is true about the client identifier?

Options:

A- The client Identifier is automatically included In the audit trail.

B- The client Identifier is automatically set by the SQL-Net layer.

C- A session can have multiple client Identifier values set simultaneously.

D- The client Identifier cannot be changed during the session.

Answer:

B

Question 7

Question Type: **MultipleChoice**

You develop an HR application that must allow multiple sessions to share application attributes. Which statement is executed while implementing the requirement?

Options:

A- CREATE CONTEXT global_hr USING hr_pkg;

B- CREATE CONTEXT global_hr USING hr_pkg ACCESSED GLOBALLY;

C- CREATE CONTEXT global_hr USING hr_pkg INITIALIZED GLOBALLY;

D- CREATE CONTEXT global_hr USING hr_pkg INITIALIZED EXTERNALLY;

Question 8

Question Type: **MultipleChoice**

Examine these commands and responses:

```
SQL> connect karen@ORCL

Connected.

SQL> show user

USER is "GUEST"
```

User Karen is an enterprise user.

Which two commands are used to allow this login?

Options:

A- GRANT CREATE SESSION TO karan;

B- CREATE USER guest IDENTIFIED BY karen;

C- CREATE USER karen IDENTIFIED BY guest;

D- CREATE USER guest IDENTIFIED GLOBALLY as '';

E- GRANT CREATE SESSION TO guest;

Answer:

D