Plunder Public RDS Snapshots

Analyse the challenge

The challenge involves an attacker to find a flag in a public RDS snapshot in a given AWS account. The flag is in the format of an MD5 hash.

Plan of action

1. **Configure AWS CLI:** Set up the AWS CLI with appropriate credentials to interact with the target AWS account.
2. **Enumerate Public Snapshots:** Use the AWS CLI to search for public RDS snapshots, specifically cluster snapshots, within the target account ID and the specified region (us-east-1).
3. **Identify Target Snapshot:** Locate a relevant public snapshot, likely named "orders-private".
4. **Restore Snapshot:** Restore the identified snapshot to a new RDS instance.
5. **Modify Database Password:** Since the original password is unknown, modify the master password of the restored RDS instance.
6. **Connect to Database:** Connect to the restored RDS instance using a PostgreSQL client.
7. **Explore Database:** Navigate through the databases and tables within the instance.
8. **Retrieve Flag:** Query the relevant table (likely "orders" within the "cust_orders" database) to find the flag.
9. **Configure AWS CLI:**
    - Configure using `aws configure` to set up the AWS CLI. This requires having an IAM user in your own AWS account with sufficient permissions to access RDS.

   - This step is crucial for interacting with AWS services. - Ensure the IAM user has the necessary permissions, such as `rds:DescribeDBClusterSnapshots`, `rds:RestoreDBClusterFromSnapshot`, `rds:ModifyDBCluster`, etc. - The region should be set to `us-east-1` as specified in the walkthrough.
10. **Enumerate Public Snapshots:**
    - Use the command `aws rds describe-db-cluster-snapshots --snapshot-type public --include-public --region us-east-1 | grep 104506445608` to list public cluster snapshots.
    - The command filters the output to show only snapshots belonging to the target account ID (104506445608).

   - This command is the core of the enumeration process. - The `--snapshot-type public` and `--include-public` flags ensure that only public snapshots are listed. - The `grep` command filters the results to show only snapshots associated with the target account. - The region `us-east-1` is correctly specified.

11. **Identify Target Snapshot:**
    - The output of the previous command should reveal a snapshot named "orders-private".

    - The name "orders-private" suggests that it might contain sensitive data. - This is the snapshot we need to restore.

12. **Restore Snapshot:**
    - Navigate to the RDS service in the AWS console (us-east-1 region).
    - Go to "Snapshots" and then the "Public" tab.
    - Search for "private" to find the "orders-private" snapshot.
    - Select the snapshot and choose "Restore snapshot" from the "Actions" menu.
    - Use default settings, provide a DB instance identifier, select "Burstable classes" and "db.t3.medium" for instance configuration.
    - Set "Public access" to "No" under "Connectivity".
    - Create a new security group.
    - Click "Restore DB cluster".

    - Restoring the snapshot creates a new RDS instance from the snapshot data. - The instance type "db.t3.medium" is a cost-effective option for this lab. - Setting "Public access" to "No" is important for security. - Creating a new security group helps isolate the instance.

13. **Modify Database Password:**
    - Once the cluster is restored, select it and choose "Set up EC2 connection" (optional, but recommended for easier access).
    - Create or select an existing EC2 instance.
    - Click "Modify" on the cluster.
    - Set a new master password.
    - Choose "Apply immediately" and click "Modify cluster".

    - Modifying the password is necessary because we don't know the original password. - Applying the changes immediately ensures we can connect to the database without waiting.

14. **Connect to Database:**
    - Copy the endpoint of the writer instance from the "Connectivity & security" tab.
    - SSH to the EC2 instance (if created in step 5).
    - Install the PostgreSQL client: `sudo apt-get install -y postgresql-client`
    - Connect to the database using: `psql -h <endpoint> -U postgres`
    - Enter the new password when prompted.

    - The endpoint is the address of the database instance. - The PostgreSQL client is needed to interact with the database. - Using the username "postgres" is the default for PostgreSQL.

15. **Explore Database:**
    - List databases: `\list`
    - Connect to the "cust_orders" database: `\c cust_orders`
    - List tables: `\dt`

    - These commands help navigate the database structure. - The "cust_orders" database likely contains the relevant data.

16. **Retrieve Flag:**
    - Query the "orders" table: `select * from orders;`
    - Query the "flag" table: `select * from flag;`

    - The "orders" table might contain sensitive data, as suggested earlier. - The "flag" table is expected to contain the flag we are looking for. - The output of the query will show the flag.

The flag can be retrieved by following these steps:

1. **Configure AWS CLI:** Ensure your AWS CLI is configured with credentials that have sufficient permissions to access RDS in the `us-east-1` region.
2. **Enumerate Public Snapshots:** Run the following command in your terminal:

   ```
   aws rds describe-db-cluster-snapshots --snapshot-type public --
   include-public --region us-east-1 | grep 104506445608
   ```

   This will list public cluster snapshots belonging to the target account.
3. **Identify Target Snapshot:** Look for a snapshot named "orders-private" in the output.
4. **Restore Snapshot:**
   - Go to the AWS console, navigate to RDS, and select the `us-east-1` region.
   - Click on "Snapshots" and then the "Public" tab.
   - Search for "private" and select the "orders-private" snapshot.
   - From the "Actions" menu, choose "Restore snapshot".
   - Provide a DB instance identifier (e.g., "my-restored-db").
   - Under "Instance configuration", select "Burstable classes" and choose "db.t3.medium".
   - Under "Connectivity", set "Public access" to "No" and create a new security group.
   - Click "Restore DB cluster".
5. **Modify Database Password:**
   - Once the cluster is restored, select it and choose "Set up EC2 connection" (optional).
   - Create or select an existing EC2 instance.
   - Click "Modify" on the cluster.
   - Set a new master password (e.g., "mynewpassword").
   - Choose "Apply immediately" and click "Modify cluster".
6. **Connect to Database:**
   - Copy the endpoint of the writer instance.
   - SSH to your EC2 instance (if created).
   - Install the PostgreSQL client: `sudo apt-get install -y postgresql-client`
   - Connect to the database: `psql -h <endpoint> -U postgres`
   - Enter the new password when prompted.
7. **Explore Database:**

- List databases: `\list`
- Connect to "cust_orders": `\c cust_orders`
- List tables: `\dt`

8. **Retrieve Flag:**
   - Query the "flag" table: `select * from flag;`

   The output will contain the flag, which is an MD5 hash.