Task 3 - Social Engineering

(Computer Forensics, Metadata Analysis, Encryption Tools)

Points: 150

Good news -- the decrypted key file includes the journalist's password for the Stepinator app. A Stepinator is a wearable fitness device that tracks the number of steps a user walks. Tell us the associated username and password for that account. We might be able to use data from that account to track the journalist's location!

Provided files

- Archive of data from jouralist's computer (for tasks 1-3) (`home.zip`)

Prompt

- Enter the username for the Stepinator account
- Enter the password for the Stepinator account

Prerequisites

```
~$ apt install sqlite3
```

Solution

We start by inspecting the decrypted credentials file `keychain`.

```
~$ file keychain
keychain: SQLite 3.x database, last written using SQLite version 3027002
```

We see that it's an `SQLite 3` database, so we can use `sqlite3` to view the contents.

```
~$ sqlite3 decrypted
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE services(
                                                    id integer PRIMARY KEY,
                                                    service text NOT NULL,
                                                    keyused integer,
                                                    keyexpired integer);
INSERT INTO services VALUES(1,'email',1,0);
INSERT INTO services VALUES(2,'bank',1,0);
INSERT INTO services VALUES(3,'blog',1,0);
INSERT INTO services VALUES(4,'work server',1,0);
INSERT INTO services VALUES(5,'music',1,0);
INSERT INTO services VALUES(6,'login',1,0);
INSERT INTO services VALUES(7,'house alarm',1,0);
INSERT INTO services VALUES(8,'stepinator',1,0);
CREATE TABLE passwords(
                                                    id integer PRIMARY KEY,
                                                    service integer NOT NULL,
                                                    username text,
                                                    pwd text NOT NULL,
                                                    valid integer NOT NULL,
                                                    FOREIGN KEY (service) REFERENCES services (id));
INSERT INTO passwords VALUES(1,1,'Jade_Orchids','<~95/Hg<b6;gAS#m93AE8~>',1);
```

```
INSERT INTO passwords VALUES(2,2,'JOrchids','<~0JYCC>%)G[~>',1);
INSERT INTO passwords VALUES(3,3,'Zara-Jade','<~:NBrYBk1CUEa\~>',1);
INSERT INTO passwords VALUES(4,4,'JOrchids4814','<~>%)G[0JYCC~>',1);
INSERT INTO passwords VALUES(5,5,'Jade_Orchids','<~0etO=8Rl=!Eb/Zr;djQSGA1Q#~>',1);
INSERT INTO passwords VALUES(6,6,'JadeOrchids745','<~0JP:;=)VnuATDL&AH~>',1);
INSERT INTO passwords VALUES(7,7,'665364814','<~8Rl=!Eb/Zr;djQSGA1Q#~>',1);
INSERT INTO passwords VALUES(8,8,'Zara_Orchids_0910','<~:NBrYBk1CUEa^XW1,q!D1GA~>',1);
COMMIT;
```

We notice there are two tables: `services` and `passwords`. The 8th entry in the `services` table is titled `stepinator`. We therefore look at the 8th entry of the `passwords` table to see that the username for the journalist's Stepinator account is `Zara_Orchids_0910`.

The corresponding password for that entry is `<~:NBrYBk1CUEa^XW1,q!D1GA~>`. Since all the passswords are framed with `<~` and `~>`, the passwords were likely encoded using Adobe's Ascii85 format. We can therefore decode the password using Python's `base64` library.

```
~$ python3
>>> from base64 import a85decode
>>> a85decode('<~:NBrYBk1CUEa^XW1,q!D1GA~>', adobe=True)
b'OrchidZara02281230'
```

The password for the Stepinator account is therefore `OrchidZara02281230`.

Answer

- Enter the username for the Stepinator account
  - `Zara_Orchids_0910`
- Enter the password for the Stepinator account
  - `OrchidZara02281230`

Author

- **Aviv Brook**