Mysql

In order for Splunk to connect to the database, the database must be properly configured. To start with, we will have to create a user for Splunk to connect to the database with. Log into mysql as the root using using the command ***mysql -u root -p***. When prompted enter the root user password (by default the password after running the FB_CTF setup script is “root”. Once logged in, we will create a splunk user. Enter the command ***grant select on fbctf.* to 'Splunk'@'%' identified by '<password>';*** This will create a user (Splunk) that has read-only access to the fbctf tables. This user is able to login from any IP address although if you are able to specify a static IP address, replace the % with the IP address.

Next mysql must be configured the allow access from outside computers. By default, mysql is only listening on the 127.0.0.1 interface which means it's not accessible from other systems. Open /etc/mysql/my.cnf and find the line for bind-address (should be line 47 by default) and edit it to 0.0.0.0. Exit and save the configuration and the restart mysql using the command ***service mysql restart***. Enter the command ***netstat -anto*** and confirm that TCP port 3306 is listening on 0.0.0.0 now.

DB_Connect

The splunk DB_Connect app is required in order for the FB_CTF app to work. This is how the system querys the mysql database and gets all of the current information. The app can be downloaded from Splunkbase at https://splunkbase.splunk.com/app/2686/.

In order for DB_Connect to work, you must install Java, and the required mysql driver.

Configuration

Once the DB_Connect app is installed, it is time to create a connection. Click on **Configuration**, and then **Identities** and then **New Identity**. Enter the following information:

Identity Name: fb_ctf
Username: Splunk
Password: <your password>

Next click on the **Connection** tab and then **New Connection**. Enter the following information:

Connection Name: fbctf (this matters!)
Identity: fb_ctf
Connection Type: MySQL
Timezone: ETC/GMT
Host: IP Address of the game server
Port: 3306
Default Database: fbctf

fb_ctf App

Untar the fb_ctf app into <Splunk Home>/etc/apps/ and then restart Splunk. The DB_Connect app uses something called a rising column value to the track what records have been imported before. Unfortunately I haven't figured out how to reset this, so that means you have to do it yourself. Under the DB_Connect app click on **Data Lab** and then **Inputs**. One at a time, go into each input and on the column on the right, enter '0' under **Checkpoint Value** (you may have to click **Unlock & Edit** to enter the value). Once you have done that, click on **Execute SQL** and then **Next**, and then **Finish**. Repeat this for all of the inputs.

That's it. The app is now configured and within a few minutes it should be populated with any information that is already in the database (levels, players who have registered, etc.). Once the compitition goes live it will update the information about every minute or so.

Got a comment or suggestion? Feel free to create an issue on my github.
https://github.com/pyrodie18/fb_ctf