Assignment 3-1: Stealing Data in the Cloud

Start Assignment

Due Sunday by 11:59pm **Points** 10 **Submitting** a text entry box or a file upload
Available Apr 23 at 12am - May 23 at 11:59pm about 1 month

Description:

By default hadoop clusters are insecure unless properly configured, and even when properly configured there are still sometimes holes. For this homework you will go through the steps of a **Privilege Escalation** Attack to steal information from the lab cloud. In the assignment you will be leveraging HIVE to run Quires which will steal information from the cloud nodes which normal users should not have access to.

Trouble shooting Virtual Environment Tips:
If you will be using the virtual environment for your homework note that you have now been given your own personal Hortonworks/Hadoop machine.
This means if you run into issue please feel free to leverage the VSphere controls to **revert snapshot** or login to the Hortonworks VM and reboot it.
The root user password for the Hortonworks VM is the same as your Administrator password for you student Windows VM.
One last note is since you have your own personal machine feel free to play with it and break it, you can always just revert snapshots to a clean state when you are done.

Using the Virtual Environment:

1) Open the V-Sphere console using your assigned Virtual Environment ID
2) Right click on the VM "Student*XX*-Hortonworks" and cilck "Open Console"
3) When the console opens and loads, take note of the IP Address of the VM, e.g:"http://192.168.2.XXX" -> IP in this case is 192.168.2.XXX
4) Now Close that Console Window, and open your Student Windows VM
5) In a browser visit the IP address you just noted earlier on port 8080, e.g:"http://192.168.2.XXX:8080", this will be your own personal hadoop cluster and ambari interface
6) login with "maria_dev" as both the username and password
7) Open "HDFS Files" view by first clicking the 3x3 grid icon in the top right next to the maria_dev username, then click "HDFS Files"

8) **take a screenshot of what folders are available and turn in the screenshot**
note mentally that the "etc" folder is not available
9) Open "Hive View", the same interface you used in the previous homework

10) In the "Query Editor" execute the following query

```
CREATE TABLE raw (line STRING)
   ROW FORMAT DELIMITED FIELDS TERMINATED BY '\t' LINES TERMINATED BY '\n';
```

11) Then execute the following query

```
LOAD DATA LOCAL INPATH '/etc/passwd' INTO TABLE raw;
```

12) Next read the actual data that you just took from the file by loading it

```
Select * From raw;
```

take a screenshot of the result returned to you, turn in this screenshot. Congratulations you just stole the password file from the machine.

13) the final step is to repeat steps 11 & 12 but for a different file of your choosing. Choose a file which through the HDFS view you are not normally able to see.
if you need help choosing a file, try **searching online** for a file in a CENTOS operating system that you do not see through the HDFS view, .conf files are a easy target.

Using a Locally Downloaded Hortonwork VM:

1) In a browser visit the ambari interface, the hortonworks vm IP address you just noted earlier on port 8080, e.g:"http://192.168.2.XXX:8080"
2) login with "maria_dev" as both the username and password
3) Open "HDFS Files" view by first clicking the 3x3 grid icon in the top right next to the maria_dev username, then click "HDFS Files"
4) **take a screenshot of what folders are available and turn in the screenshot**
note mentally that the "etc" folder is not available
5) Open "Hive View", the same interface you used in the previous homework10) In the "Query Editor" execute the following query

```
CREATE TABLE raw (line STRING)
   ROW FORMAT DELIMITED FIELDS TERMINATED BY '\t' LINES TERMINATED BY '\n';
```

6) Then execute the following query

```
LOAD DATA LOCAL INPATH '/etc/passwd' INTO TABLE raw;
```

7) Next read the actual data that you just took from the file by loading it

```
Select * From raw;
```

take a screenshot of the result returned to you, turn in this screenshot. Congratulations you just stole the password file from the machine.

8) the final step is to repeat steps 6 & 7 but for a different file of your choosing. Choose a file which through the HDFS view you are not normally able to see.
if you need help choosing a file, try **searching online** for a file in a CENTOS operating system that you do not see through the HDFS view, .conf files are a easy target.

To submit your assignment:

You will be turning in 3 screenshots total.

- Use the +Submit Assignment link located in the top right corner.
- Type your submission or find and upload your saved file.
- Click the Submit Assignment button to turn in your assignment.