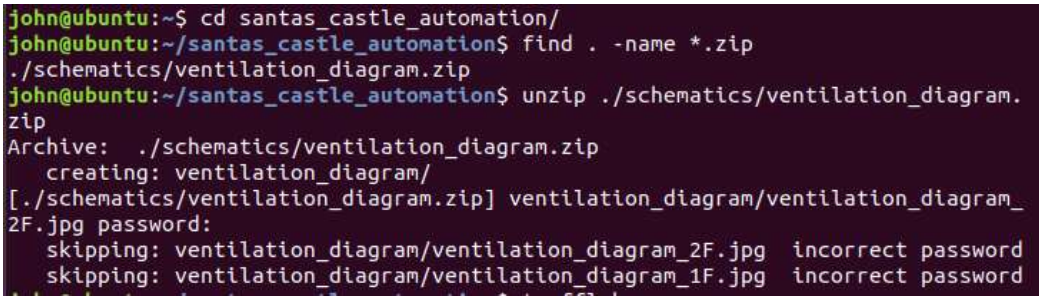
Objective--Data Repo Analysis (part 2)

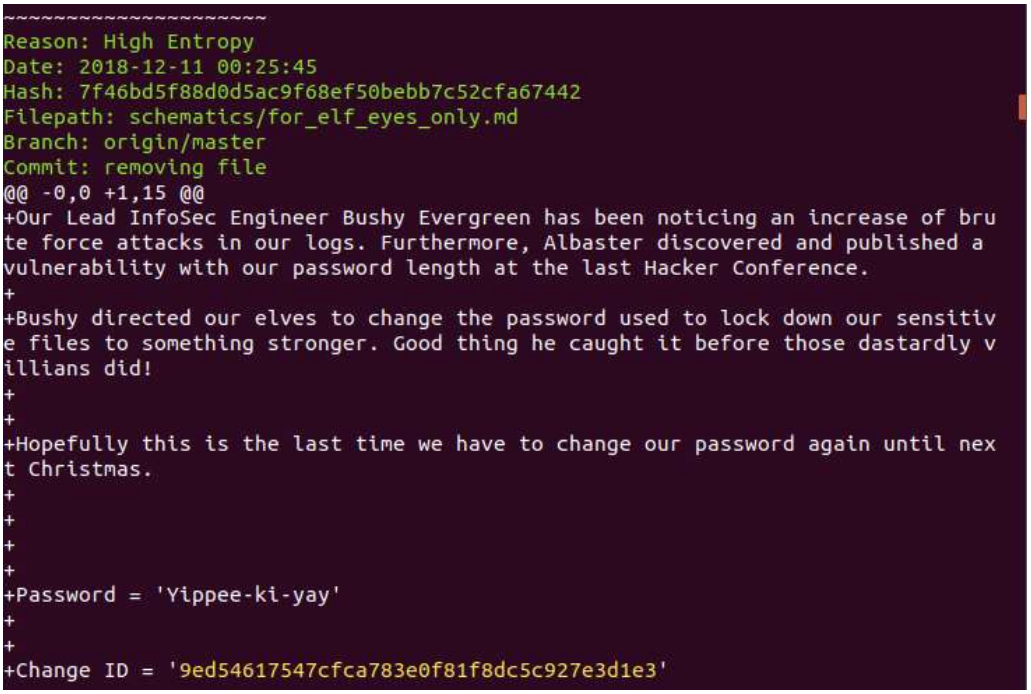
Solution

It just takes a second to find the zip file, and it is indeed encrypted. Note that the schematics directory is hidden (starts with a period) so it won't be seen by normal browsing.



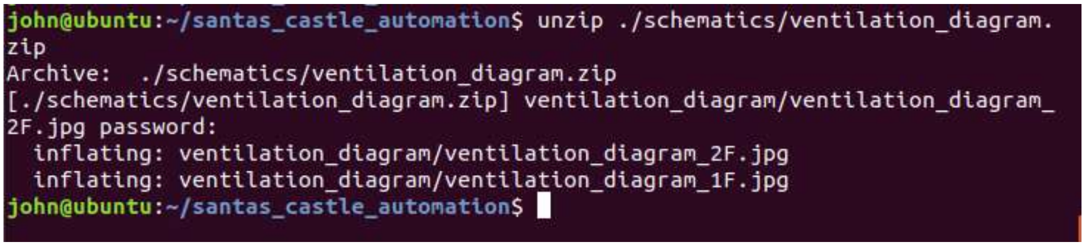
```
john@ubuntu:~$ cd santas_castle_automation/
john@ubuntu:~/santas_castle_automation$ find . -name *.zip
./schematics/ventilation_diagram.zip
john@ubuntu:~/santas_castle_automation$ unzip ./schematics/ventilation_diagram.
zip
Archive:  ./schematics/ventilation_diagram.zip
   creating: ventilation_diagram/
[./schematics/ventilation_diagram.zip] ventilation_diagram/ventilation_diagram_
2F.jpg password:
   skipping: ventilation_diagram/ventilation_diagram_2F.jpg  incorrect password
   skipping: ventilation_diagram/ventilation_diagram_1F.jpg  incorrect password
```

A search with Trufflehog (used cd .. to go back to my home directory) leads us to some notes in a comment:



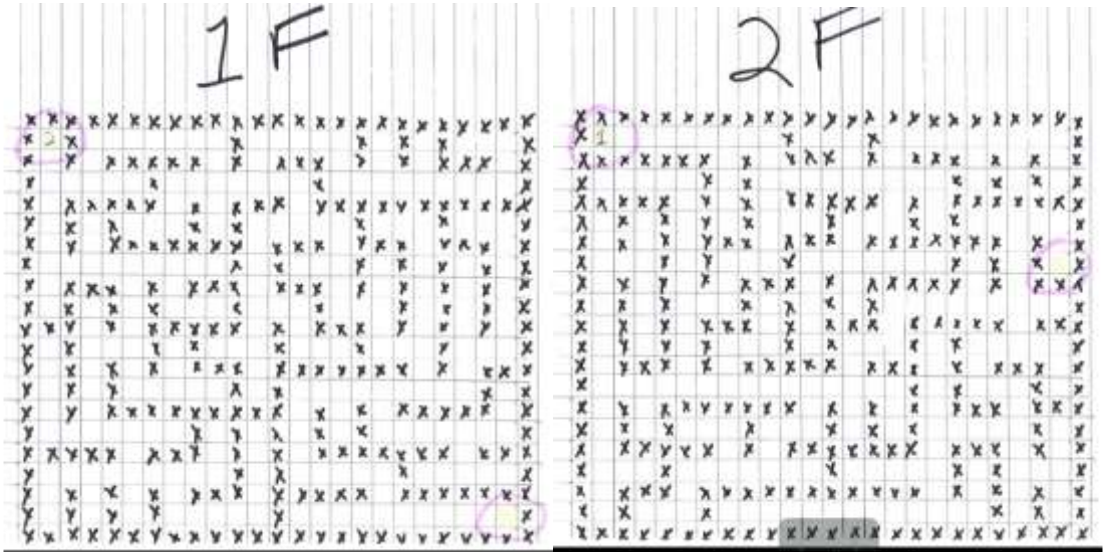
```
~~~~~~~~~~~~~~~~~~~~~
Reason: High Entropy
Date: 2018-12-11 00:25:45
Hash: 7f46bd5f88d0d5ac9f68ef50bebb7c52cfa67442
Filepath: schematics/for_elf_eyes_only.md
Branch: origin/master
Commit: removing file
@@ -0,0 +1,15 @@
+Our Lead InfoSec Engineer Bushy Evergreen has been noticing an increase of bru
te force attacks in our logs. Furthermore, Albaster discovered and published a
vulnerability with our password length at the last Hacker Conference.
+
+Bushy directed our elves to change the password used to lock down our sensitiv
e files to something stronger. Good thing he caught it before those dastardly v
illians did!
+
+
+Hopefully this is the last time we have to change our password again until nex
t Christmas.
+
+
+
+
+Password = 'Yippee-ki-yay'
+
+
+Change ID = '9ed54617547cfca783e0f81f8dc5c927e3d1e3'
```

Using Yippee-ki-yay as a password unzips the files.

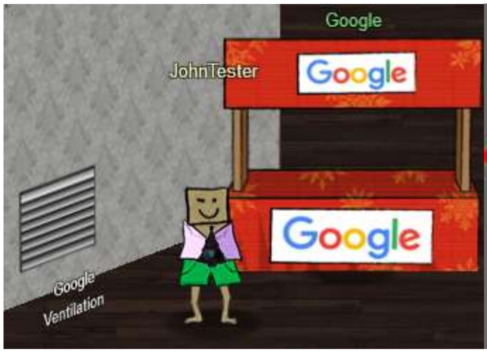


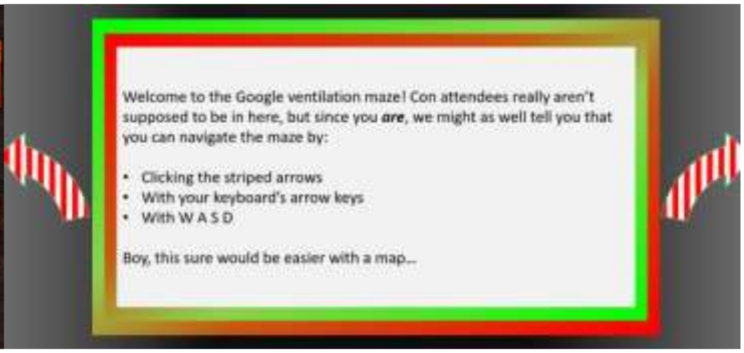
```
john@ubuntu:~/santas_castle_automation$ unzip ./schematics/ventilation_diagram.
zip
Archive:  ./schematics/ventilation_diagram.zip
[./schematics/ventilation_diagram.zip] ventilation_diagram/ventilation_diagram_
2F.jpg password:
  inflating: ventilation_diagram/ventilation_diagram_2F.jpg
  inflating: ventilation_diagram/ventilation_diagram_1F.jpg
john@ubuntu:~/santas_castle_automation$
```

The ventilation diagrams appear to be maps:



In fact, those maps are very handy if you decide to attempt the Google ventilation maze.





Welcome to the Google ventilation maze! Con attendees really aren't supposed to be in here, but since you *are*, we might as well tell you that you can navigate the maze by:

- Clicking the striped arrows
- With your keyboard's arrow keys
- With W A S D

Boy, this sure would be easier with a map...

The maze is not necessary to complete the challenges, but it is fun.

Google provided SANS and CounterHack free access to Google Cloud to host this year's challenge!

Up Next

The next Objective, AD Privilege Discovery, tells us to visit Holly Evergreen to help her with the CURLing Master terminal. She's on the left side of the first floor, so off we go.