Objective--Data Repo Analysis (part 1)

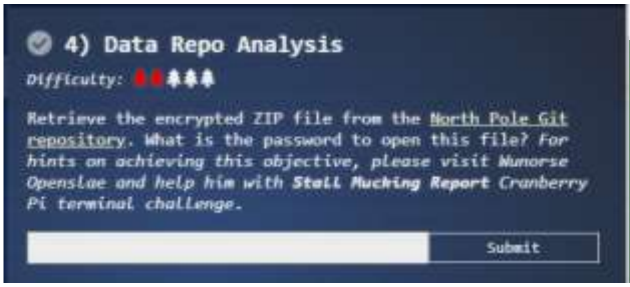
What you can learn from this

More and more, developers are using web-based version control tools to help them collaborate on software. However, these tools pose a risk if sensitive information like passwords and cryptographic keys are inadvertently made public. Brian Hostetler lists several of the recent breaches this has caused in his talk. Repositories keep running logs of all changes made to software, so just removing a password in the current version will not help you. Previous version, and the change logs themselves, will still store that password.

This challenge will demonstrate how publicly available tools make it easy to find credentials buried in public repositories. It will also demonstrate how to clone a Git repository so that you can install software on your local computer.

Objective and hints

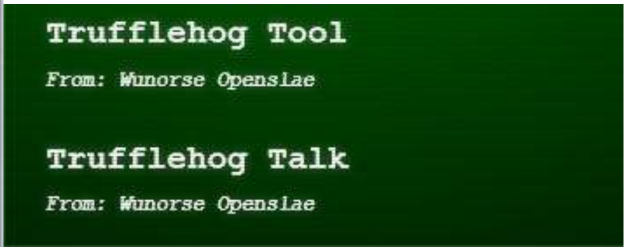
Since you have solved Wunorse's problem with uploading his report, he has given you hints in his dialog and your badge (assuming you remembered to click on him after solving his problem.)



4) Data Repo Analysis

Difficulty:

Retrieve the encrypted ZIP file from the North Pole Git repository. What is the password to open this file? For hints on achieving this objective, please visit Wunorse Openslae and help him with Stall Mucking Report Cranberry Pi terminal challenge.



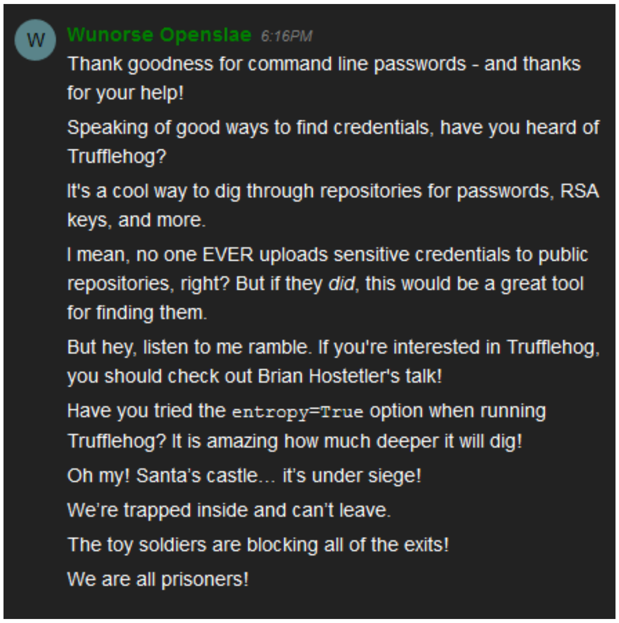
Trufflehog Tool

From: Wunorse Openslae

Trufflehog Talk

From: Wunorse Openslae

Although Wunorse mentions the `entropy=True` option in Trufflehog, he is a little out of date. Apparently, the option is so helpful it has been made the default, so you don't need to use it. Do be sure not to use its opposite and set entropy to false; that will cause you to miss what you are looking for.



W Wunorse Openslae 6:16PM

Thank goodness for command line passwords - and thanks for your help!

Speaking of good ways to find credentials, have you heard of Trufflehog?

It's a cool way to dig through repositories for passwords, RSA keys, and more.

I mean, no one EVER uploads sensitive credentials to public repositories, right? But if they *did*, this would be a great tool for finding them.

But hey, listen to me ramble. If you're interested in Trufflehog, you should check out Brian Hostetler's talk!

Have you tried the `entropy=True` option when running Trufflehog? It is amazing how much deeper it will dig!

Oh my! Santa's castle… it's under siege!

We're trapped inside and can't leave.

The toy soldiers are blocking all of the exits!

We are all prisoners!

Again, the link to Brian's talk is here. Please watch it.

Installing Trufflehog.

We will install Trufflehog on a Linux virtual machine (VM) because, well, it's cool and it works well. Trufflehog is written in Python, and Python has its own repository called PIP. That makes the installation of Trufflehog very easy, except that you may need to install PIP first. (Trufflehog installation instructions are on the Trufflehog Git repository.

Before installing software, it is a good idea to update your Linux OS, as older versions may have libraries that are incompatible with new installations. In Ubuntu or other Debian-based systems, update with:

```
sudo apt-get update
sudo apt-get upgrade
```

In CentOS or other RedHat-based systems, use

```
sudo yum update
```

To install PIP in Ubuntu or other Debian-based systems use:

```
sudo apt-get install python-pip
```

In CentOS or other RedHat-based systems, use:

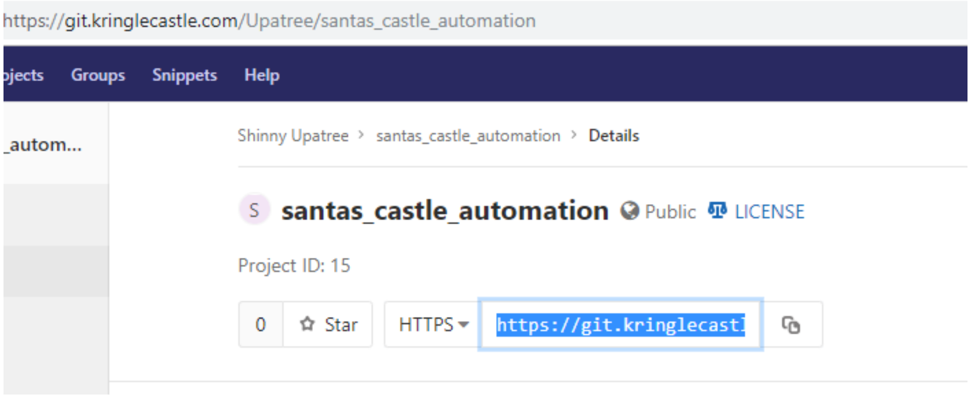
```
sudo yum install epel-release
sudo yum update
sudo yum install python-pip
```

With that out of the way, installing Trufflehog is simple. Run PIP from your Linux terminal (BASH), not from inside Python.

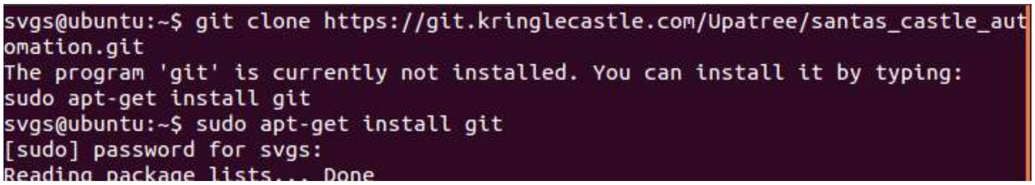
```
sudo pip install trufflehog
```

Objective

We have been asked to find some encrypted zip files in the North Pole Git Repository, which is available here. The Git repository has search tools, but sometimes it is just as easy to create a local copy using the `git clone` command. Git repositories make it easy to copy the link to the repository.

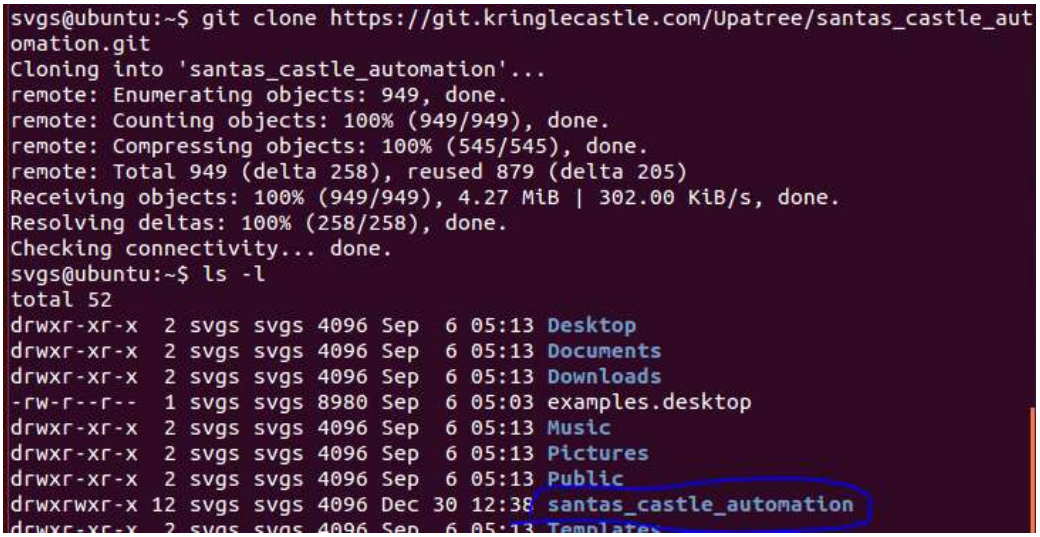


Just navigate to a directory where you would like to store a copy and execute: (one line)
`git clone`
[`https://git.kringlecastle.com/Upatree/santas_castle_automation.git`](https://git.kringlecastle.com/Upatree/santas_castle_automation.git)



```
svgs@ubuntu:~$ git clone https://git.kringlecastle.com/Upatree/santas_castle_aut
omation.git
The program 'git' is currently not installed. You can install it by typing:
sudo apt-get install git
svgs@ubuntu:~$ sudo apt-get install git
[sudo] password for svgs:
Reading package lists... Done
```

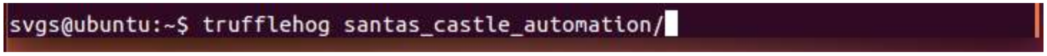
(oops)



```
svgs@ubuntu:~$ git clone https://git.kringlecastle.com/Upatree/santas_castle_aut
omation.git
Cloning into 'santas_castle_automation'...
remote: Enumerating objects: 949, done.
remote: Counting objects: 100% (949/949), done.
remote: Compressing objects: 100% (545/545), done.
remote: Total 949 (delta 258), reused 879 (delta 205)
Receiving objects: 100% (949/949), 4.27 MiB | 302.00 KiB/s, done.
Resolving deltas: 100% (258/258), done.
Checking connectivity... done.
svgs@ubuntu:~$ ls -l
total 52
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Desktop
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Documents
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Downloads
-rw-r--r--  1 svgs svgs 8980 Sep  6 05:03 examples.desktop
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Music
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Pictures
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Public
drwxrwxr-x 12 svgs svgs 4096 Dec 30 12:38 santas_castle_automation
drwxr-xr-x  2 svgs svgs 4096 Sep  6 05:13 Templates
```

Now just search the new directory for zip files using your usual tools.

To search for passwords, we might as well search the files we just cloned to our computer.
`trufflehog santas_castle_automation/`



```
svgs@ubuntu:~$ trufflehog santas_castle_automation/
```

Note: The Trufflehog Read.Me file recommends using the `--entropy=False` option to cut down on noise. Don't do that, as you will miss the passwords. Entropy is a measure of randomness. Cryptographic keys and good passwords should have a high degree of randomness. Trufflehog calculates the entropy for the strings it finds and displays any that rise above a preset threshold.

Hand In

1) What is the name of the encrypted zip file?

2) What is the password?

3) What does the encrypted zip file contain?