# Objective: Recover the Cloud Ring—Questions Only

Much of the basic knowledge you need to work in the cloud is the same as you need when your hardware lives on-premises: operating systems (especially Linux), networking, scripting, and cryptography for starters. For cloud technology you need to add another layer of scripting using the provider’s tools to assemble the pieces of cloud functions into a solution. This challenge will teach you some of the basics for using the AWS cloud. The terminals all have the AWS CLI installed, so you won’t need to do that.

A picture containing text, sign

Description automatically generated

## AWS CLI Intro

The AWS Command Line Interface (CLI) is a set of tools provided by [AWS that you install](https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html) on your workstation or server. AWS also supports a [web-based management console](https://aws.amazon.com/console/), but for an installation of any size it is cumbersome and time consuming. Large installations are almost always created and maintained through AWS CLI or through a scripting language like [Terraform](https://aws.amazon.com/blogs/apn/terraform-beyond-the-basics-with-aws/) that leverages the AWS CLI. The CLI is based on an executable named aws, so all the commands start with aws.

Graphical user interface

Description automatically generated with medium confidence

A screenshot of a video game

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sts/get-caller-identity.html>

### Trufflehog Search

Unless the developer takes [explicit actions to remove them](https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository), any credentials mistakenly submitted to a Git repository remain there for the life of the repository. Attackers can find these credentials and use them to compromise your installation.

A picture containing text, toy

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence

Text

Description automatically generated with low confidence<https://haugfactory.com/asnowball/aws_scripts.git>

You need to find the AWS secrets that Alabaster [left in this repository](https://haugfactory.com/asnowball/aws_scripts.git) using the Trufflehog tool. Gerty does not have a terminal, but you can skip ahead to Sulfrod’s terminal which has Trufflehog installed. Alabaster’s repository is on the public Internet, so you can also install Trufflehog on your own machine. Interestingly, the version of Trufflehog I installed found the credentials immediately without needing to open previous commits.

A picture containing text

Description automatically generated

### Question

Use Trufflehog to find the name of the file where Alabaster stored his credentials. If you use Sulfrod’s tmux terminal, the results will scroll off the top. You can [regain your scrolling functions in tmux](https://superuser.com/questions/209437/how-do-i-scroll-in-tmux) by pressing CNTL-b, then [. When you want to enter commands again, use CNTL-c.

## Exploitation via the AWS CLI

This challenge picks up where we left off at Sulfrod’s terminal. You will use the AWS credentials that Alabaster left in the Git repository to gain access to his AWS to see what you can find, and learn about AWS policies on the way. The talk by Chris Elgee is a good place to start, especially the demonstration towards the end.

Text

Description automatically generated  
<http://www.youtube.com/watch?v=t-xDvVUialo> Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html>

The terminal leads you through this challenge, although you do have to read the reference URLs carefully