Cloud DFIR class

Detection_evasion

Author : Siwoo Park (박시우)

Mentor : Niko

Track : Digital Forensic

Date : 2024/08/13

Content

1. Summary 1

2. Progress 1

2.1 environment setup 1

1. Summary

This assignment focuses on researching DFIR (Digital Forensics and Incident Response) in cloud environments, The task involves using CloudGoat to set up a practical environment, deploying a specific scenario, and archieving the scenario's objectives.

Cloudgoat is a tool designed to simulate cloud security incidents, allowing users to practice responding to various cases that might occur in cloud systems.

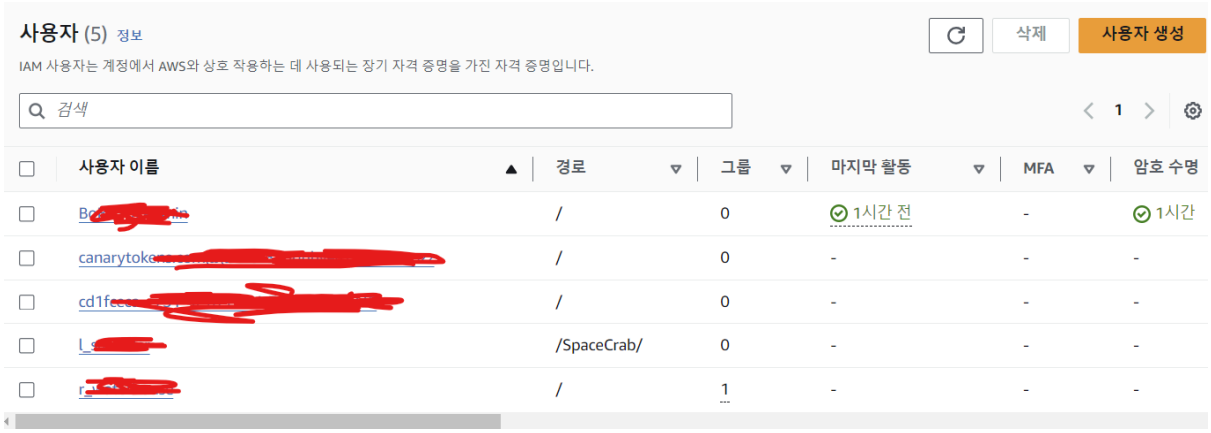
My assigned part is detection evasion, where the goal is to perform specific actions in the cloud while avoiding detection.

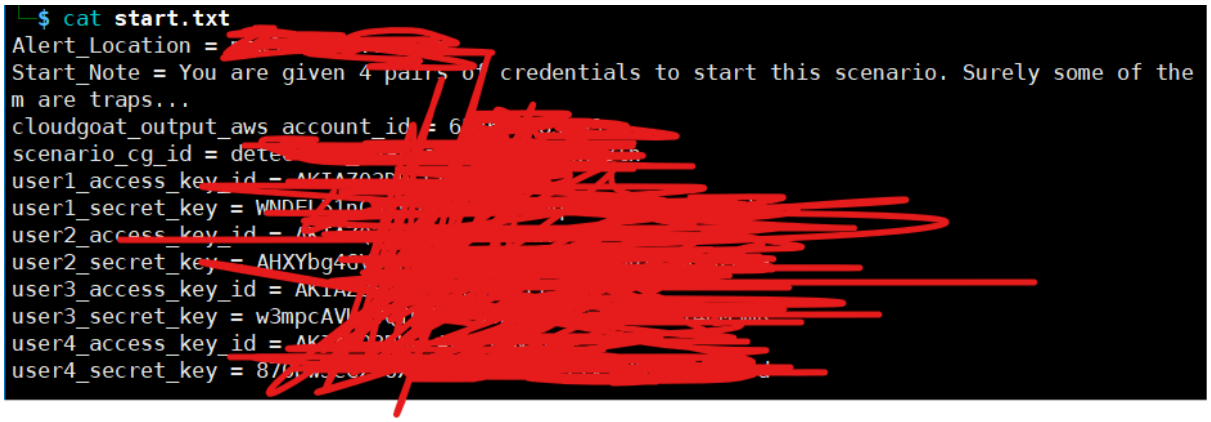
This document is for check progress about assignment.

2. Progress

2.1 environment setup

First, install AWS CLI and Cloudgoat, and configure them to link with my AWS account.





The cloud environment setup has been completed, and four accounts necessary for the exercise have been created as indicated in the `start.txt` file.

Now, using this account information, the next step is to achieve the objectives outlined in the scenario.

This is the current progress in my task.