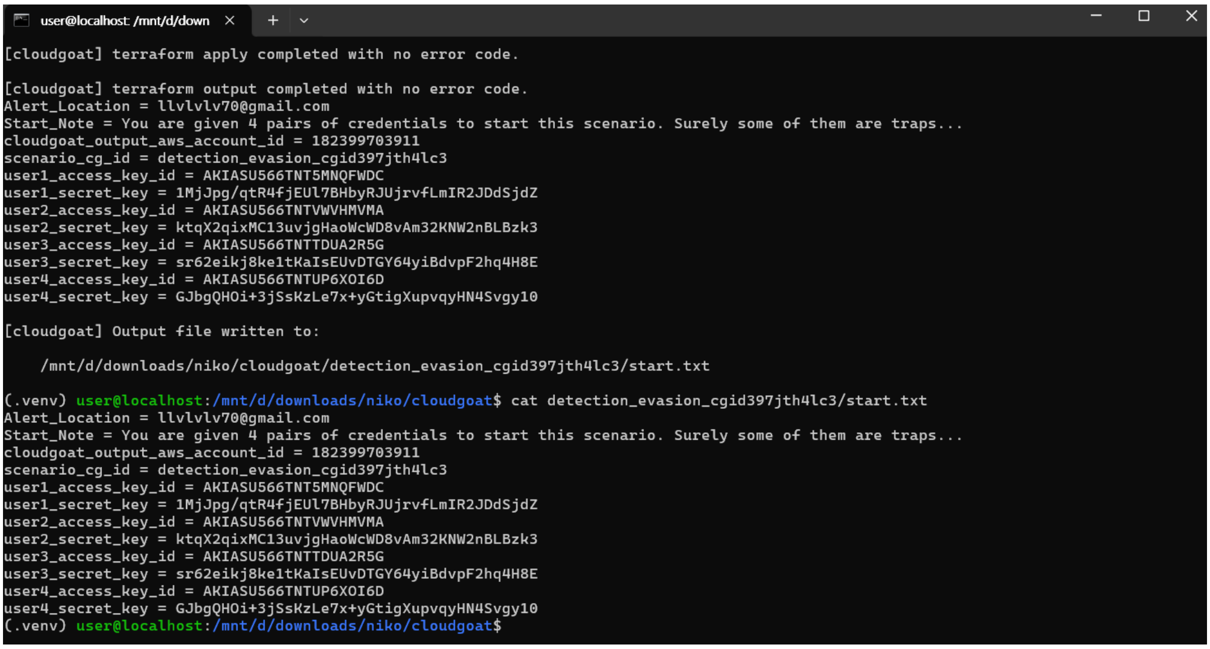
Cloud DFIR class I

Mentor	Niko
Submission Date	2024.08.13 (Tue)
Track	Digital Forensic
Name	Yu Seong-mo

목차



```
[cloudgoat] terraform apply completed with no error code.

[cloudgoat] terraform output completed with no error code.
Alert_Location = llvlvlv70@gmail.com
Start_Note = You are given 4 pairs of credentials to start this scenario. Surely some of them are traps...
cloudgoat_output_aws_account_id = 182399703911
scenario_cg_id = detection_evasion_cgid397jth4lc3
user1_access_key_id = AKIASU566TNT5MNQFWDC
user1_secret_key = 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
user2_access_key_id = AKIASU566TNTVWVHMVMA
user2_secret_key = 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
user3_access_key_id = AKIASU566TNTTDUA2R5G
user3_secret_key = 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
user4_access_key_id = AKIASU566TNTUP6XOI6D
user4_secret_key = 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

[cloudgoat] Output file written to:

    /mnt/d/downloads/niko/cloudgoat/detection_evasion_cgid397jth4lc3/start.txt

(.venv) user@localhost:/mnt/d/downloads/niko/cloudgoat$ cat detection_evasion_cgid397jth4lc3/start.txt
Alert_Location = llvlvlv70@gmail.com
Start_Note = You are given 4 pairs of credentials to start this scenario. Surely some of them are traps...
cloudgoat_output_aws_account_id = 182399703911
scenario_cg_id = detection_evasion_cgid397jth4lc3
user1_access_key_id = AKIASU566TNT5MNQFWDC
user1_secret_key = 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
user2_access_key_id = AKIASU566TNTVWVHMVMA
user2_secret_key = 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
user3_access_key_id = AKIASU566TNTTDUA2R5G
user3_secret_key = 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
user4_access_key_id = AKIASU566TNTUP6XOI6D
user4_secret_key = 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
(.venv) user@localhost:/mnt/d/downloads/niko/cloudgoat$
```

<Figure 1> Cloud Environment Setup

Key Components

4 IAM Users: Users with varying access permissions are set up from the start of the scenario.

2 EC2 Instances: Virtual server instances are used to execute some of the tasks within the scenario.

2 Secrets Manager Secrets: These secrets store critical information, and the objective is to read these secrets without triggering detection mechanisms.

Detection Mechanisms: AWS services like CloudTrail, S3, and CloudWatch are included, monitoring and recording user activities.

Primary Objectives

Read the Values of Two Secrets: The goal is to read the values of two secrets stored in AWS Secrets Manager without triggering the detection mechanisms.

Setup and Strategy

Use a Temporary Email Address: It is recommended to use a temporary email address to receive notifications. This is necessary during the CloudGoat setup, and it helps verify whether detection mechanisms have been triggered by email notifications.

Wait After Deployment: There is a necessary waiting period of 30-60 minutes after AWS resources are fully deployed and integrated. This time is needed for CloudWatch alarms to fully integrate with

CloudTrail logs.

Considerations

Detection Evasion Strategy: A crucial part of this scenario is finding ways to circumvent detection mechanisms. Careful consideration of IAM user permissions, logging configurations, and the characteristics of API calls is required.

Possibility of Replay: The scenario is designed to be played and experimented with multiple times, allowing for testing various strategies. Learning from both failures and successes can lead to more effective methods of bypassing security mechanisms.

This scenario serves as part of cloud security training, aiding in developing the ability to understand and respond to security threats in real cloud environments. Additionally, it provides an opportunity to gain practical insights into potential security issues in real work environments and to understand the limitations and strengths of detection systems.