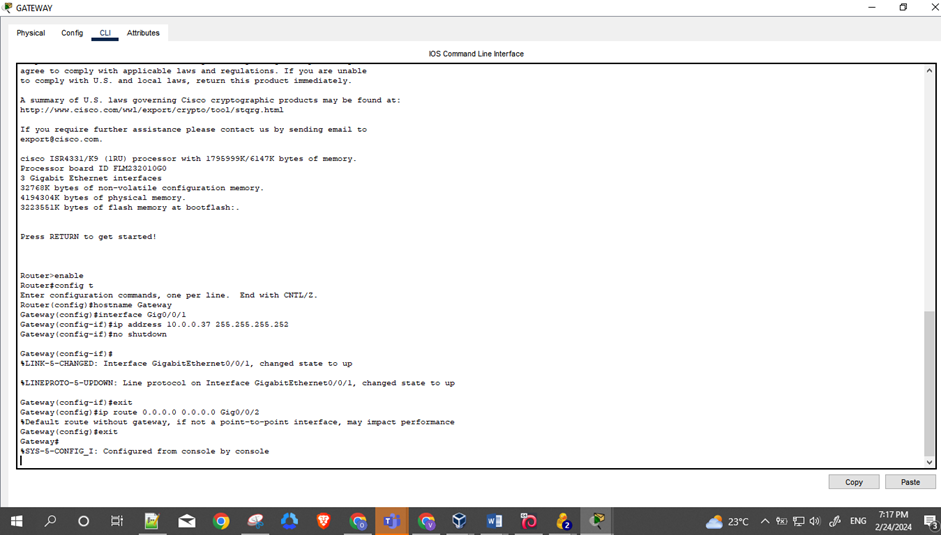
## **Instructions:**

* Answer **ALL** questions
* The exam should**NOT be**worked on in groups or with assistance from others.
* Use this file as your write-up reporting template as you complete each task outlined and answer the questions.
* **Rename this file with your full names e.g Firstname\_Lastname.docx**
* Once you have completed your work, save the file and upload it for marking.
* Before leaving the exam, ensure you have uploaded the correct file capturing all the work you have submitted for marking.
* Ensure you compile a **detailed report write-up** that outlines your approach to addressing the various exam challenges. Ensure that your write up is authentic. Show screenshots of the working for all answers showing how you got your answers.
* The screen shots should capture your full screen and display the command you ran to get the answer. Include a taskbar showing your machine taskbar and time stamp as shown below.



* **NOTE: You MUST take FULL SCREEN screenshots for each step(must show the taskbar and time stamp) of how you got your answers and submit the document as a PDF file. If you answer the question without providing the screenshots you WILL NOT be awarded any marks.**

**TOTAL MARKS = 30 mks  
TIME: 1 HOUR 15 MINUTES**

**Background:**

**As an incident responder we're granting you access to the AWS account called "Security" as an IAM user. This account contains a copy of the logs during the time period of the incident and has the ability to assume the "Security" role in the target account so you can look around to spot the source of the attack. Once you do, you will forward your findings to the Incident Response TEam.**

**NOTE: This lab requires you to use LINUX**

**Use the credentials below to set up your AWS CLI**

* **Profile Name: cloudsec**
* **Access Key: AKIAIUFNQ2WCOPTEITJQ**
* **Secret Key: paVI8VgTWkPI3jDNkdzUMvK4CcdXO2T7sePX0ddF**

**Questions:**

1. After setting up the profile and running the get caller identity command, what is the arn value associated with the account that you configured? (3mks)

*Paste screenshot here*

1. Use the **sync** command to download some file logs onto your machine from the following bucket **s3://flaws2-logs** (3 mks).

*Paste screenshot here*

1. Navigate to your **aws config file.**

* it is stored in **~/.aws/config**
* Edit the config file and add the following lines and save the changes (you can use a text editor. command: **nano ~/.aws/config** ): (3mks)

**[profile target\_security]**

**region=us-east-1**

**output=json**

**source\_profile = cloudsec**

**role\_arn = arn:aws:iam::653711331788:role/security**

*Paste screenshot here*

1. After completing step 3, run the get caller identity command on the profile **target\_security**. Display what you see. (2mks)

*Paste screenshot here*

1. List all the buckets that target\_security has access to. (2mks)  
   *Paste screenshot here*
2. Let's start digging into the log data we have. If you don't already have jq installed, you should install it using these commands:

* **sudo apt update**
* **sudo apt install jq**
* Verify the installation by using this command **jq --version.**

After installing jq, run these commands in the AWSLogs folder you downloaded in **step 2:**

* **find . -type f -exec gunzip {} \;**
* **find . -type f -exec cat {} \; | jq '.'**

You should see nicely formatting json data, but it's a lot of info, so let's just see the event names by running this command:

**find . -type f -exec cat {} \; | jq '.Records[]|.eventName'**

**What results are displayed after this query? (3mks)**

*Paste screenshot here*

1. Let us sort this data using the following command:

**find . -type f -exec cat {} \; | jq -cr '.Records[]|[.eventTime, .sourceIPAddress, .userIdentity.arn, .userIdentity.accountId, .userIdentity.type, .eventName]|@tsv' | sort**

Copy the output into an excel/spreadsheet for better viewing and screenshot the results. (3mks)

*Paste screenshot here*

1. Run the following command to view the source IP address (We'll view this IP as the attacker's IP) which is not an Amazon owned IP:

**find . -type f -exec cat {} \; | jq '.Records[]|select(.eventName=="ListBuckets")'**

This call came from the role level3, so let's look at that using this command:

**aws --profile target\_security iam get-role --role-name level3**

You'll see this role is only supposed to be run by the ECS service, as the AssumeRolePolicyDocument is only allowing that Principal, but we just saw this IP clearly did not come from the AWS IP space. Screenshot this and forward the complete report to the Incident Response Team. (3 mks)

*Paste screenshot here*

1. What are 4 key indicators of compromised credentials in a cloud environment (4 mks).
2. What are 4 strategies and best practices that can be implemented to prevent and mitigate credential theft in a cloud environment? (4mks)