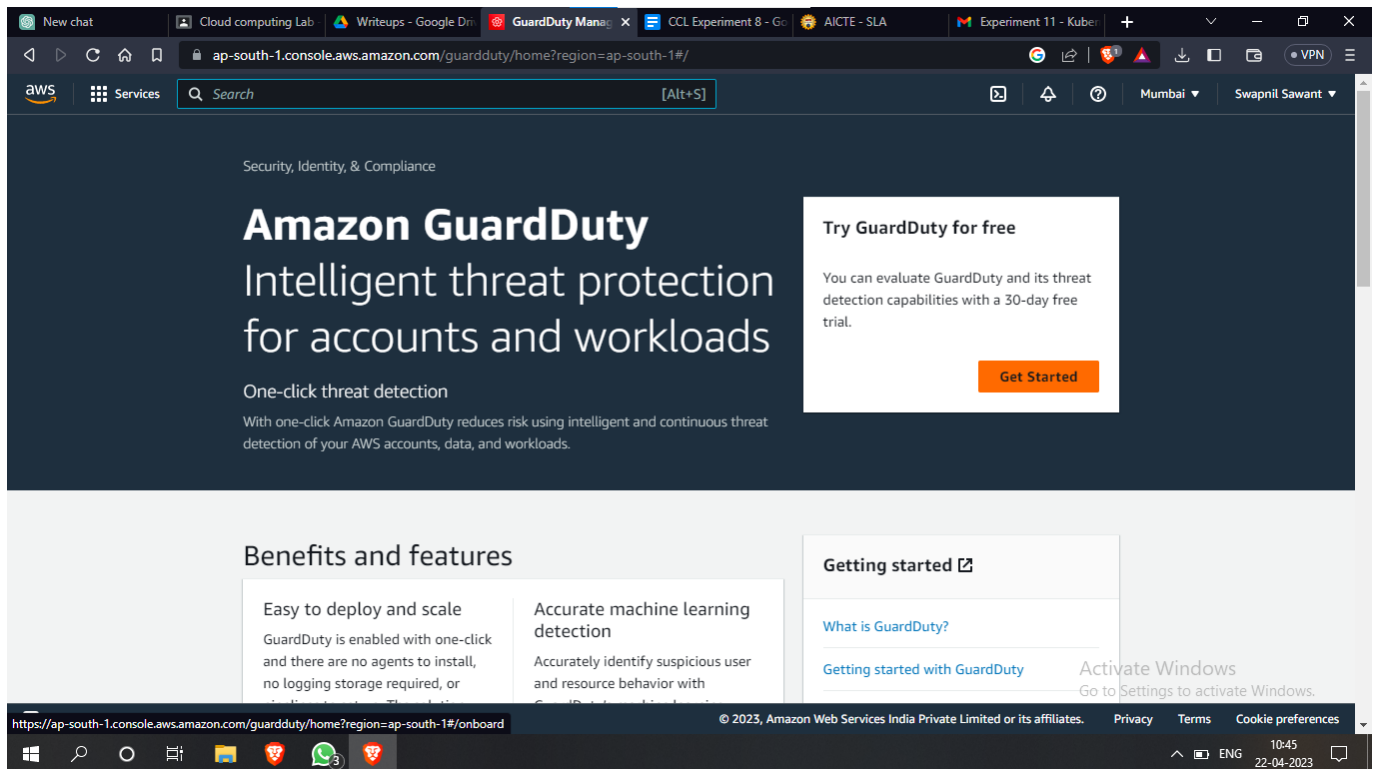


Name : Swapnil Sawant
Division : TE4
Roll No : 46
Batch : C
Subject : CCL

EXPERIMENT NO 8

Aim : To study and Implement Security as a Service on AWS.

Diagram :



GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection **New**

Malware Protection

RDS Protection **New**

Lambda Protection **New**

Accounts

What's New

Partners

You've successfully enabled GuardDuty.

New feature: GuardDuty Lambda Network Activity Monitoring

Amazon GuardDuty adds threat detection for AWS Lambda. After you enable Lambda Network Activity Monitoring, GuardDuty starts monitoring network activity, starting with VPC flow logs, for existing and new Lambda functions in your account. Current GuardDuty users can enable Lambda Network Activity Monitoring with a single step in the GuardDuty console for all the accounts in an organization by using AWS Organizations. [Learn more](#)

GuardDuty > Findings

Findings Info

Suppress Findings Info

Saved rules No saved rules

Current Add filter criteria

Finding type Resource Last... Count

You don't have any findings.

Activate Windows

Go to Settings to activate Windows.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:45 22-04-2023

GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection **New**

Malware Protection

RDS Protection **New**

Lambda Protection **New**

Accounts

What's New

Partners

GuardDuty > Settings > S3 Protection

S3 Protection Info

30 days remaining **Free trial**

S3 Protection

Monitor and generate findings on S3 data events

S3 Protection is enabled on this account [Disable](#)

Learn more about how GuardDuty processes S3 Data Events. [Learn more](#)

Activate Windows

Go to Settings to activate Windows.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:46 22-04-2023

what is my ip

What's my IP

103.49.240.76

Your public IP address

Learn more about IP address

What Is My IP Address
https://whatismyipaddress.com

What Is My IP Address - S

Find out what your public IPv4 and IPv6 information shows your IP location; city

Update My IP Location

Before You Update Your IP Location

Whatismyipaddress IP Lookup

IP Addresses - Notepad

```
File Edit Format View Help
103.49.240.76
103.49.240.75
103.49.240.77
```

Ln 3, Col 14 100% Windows (CRLF) UTF-8

Activate Windows
Go to Settings to activate Windows.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

expt8bucket

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

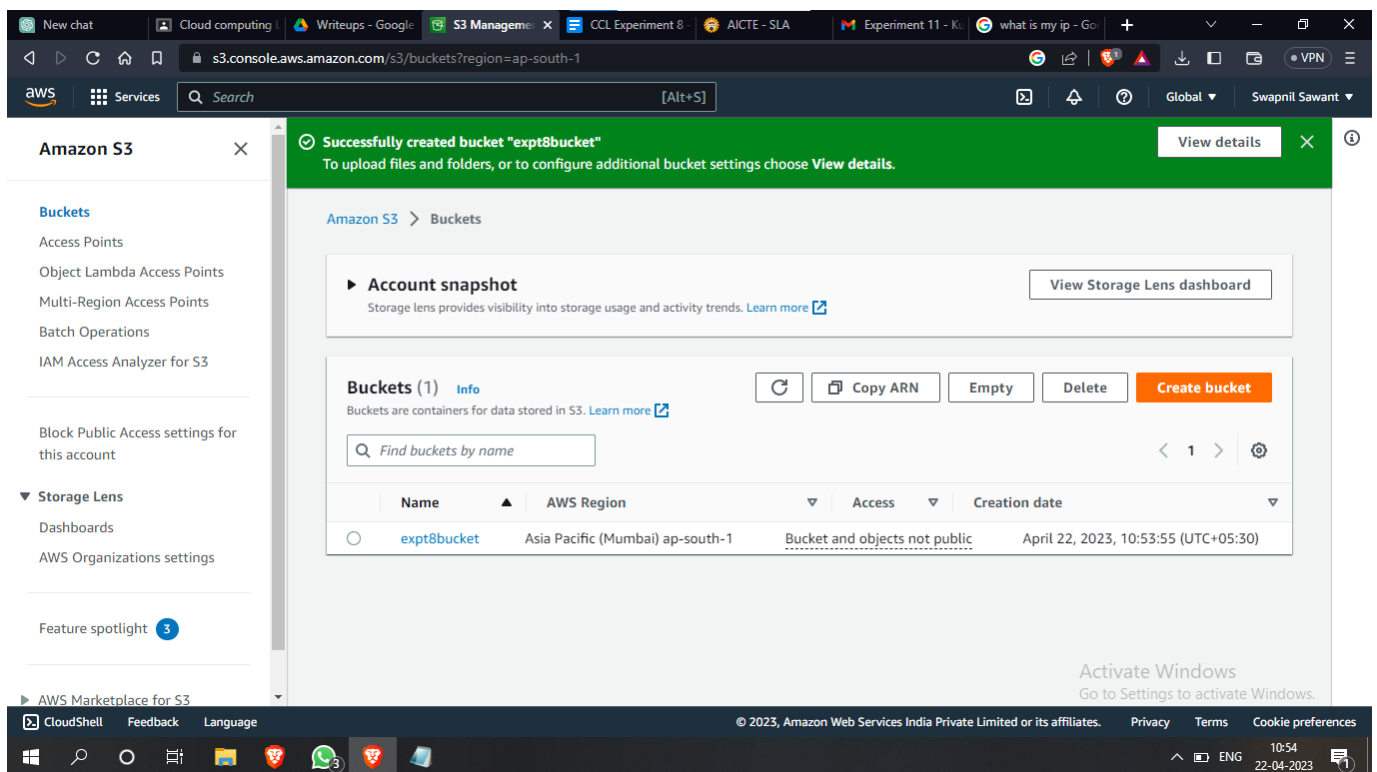
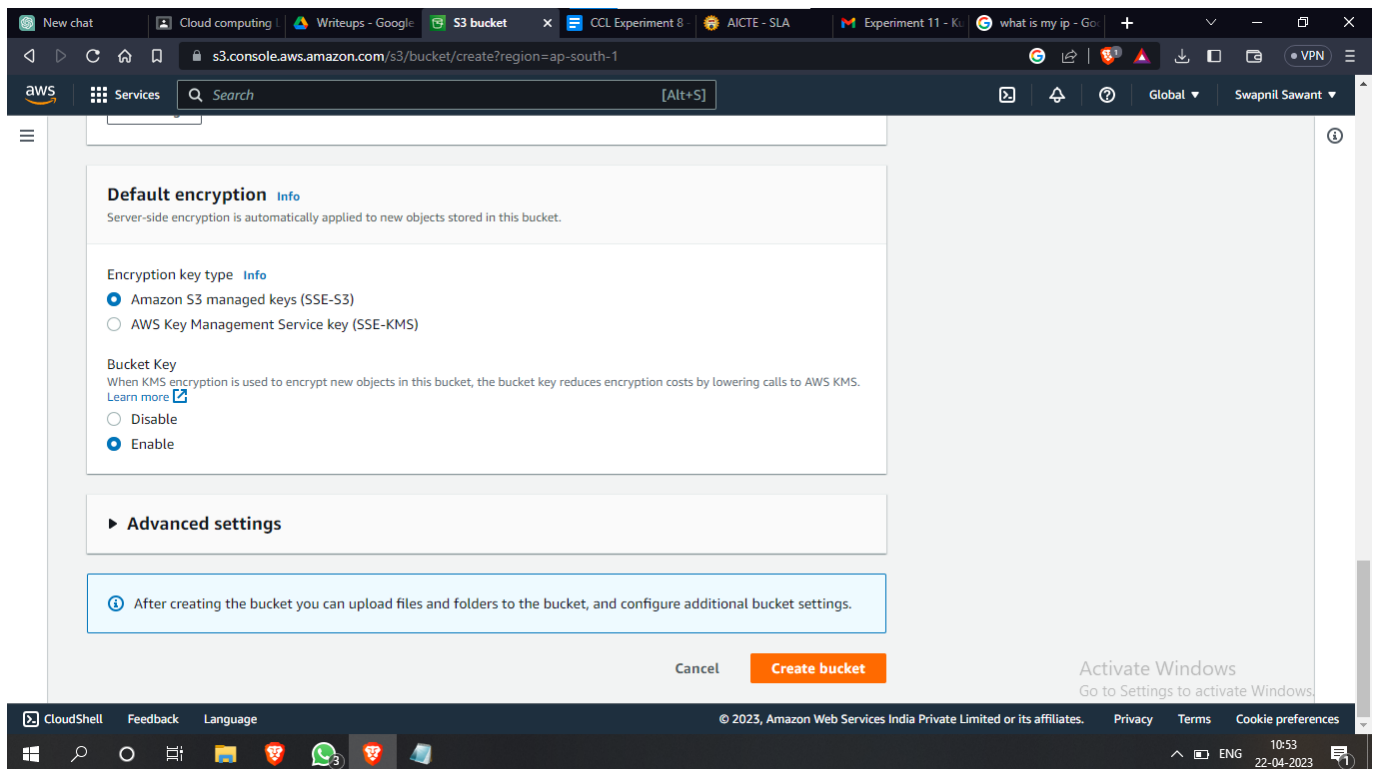
[Choose bucket](#)

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Activate Windows
Go to Settings to activate Windows.

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



Upload succeeded
View details below.

Summary

Destination s3://expt8bucket	Succeeded 1 file, 43.0 B (100.00%)	Failed 0 files, 0 B (0%)
---------------------------------	---------------------------------------	-----------------------------

Files and folders | Configuration

Files and folders (1 Total, 43.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
IP Addresses.txt	-	text/plain	43.0 B	Succeeded	-

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Amazon S3 > Buckets > expt8bucket > IP Addresses.txt

IP Addresses.txt Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

Object overview

Owner 45bfd49984b1c00805f305d90ffd2dd233e8c39d456f772a6c60bd1785b5305d	S3 URI s3://expt8bucket/IP Addresses.txt
AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::expt8bucket/IP Addresses.txt
Last modified April 22, 2023, 10:55:42 (UTC+05:30)	Entity tag (Etag) 1470c1a46fe634e8cbd7e2ffca14be59
Size 43.0 B	Object URL https://expt8bucket.s3.ap-south-1.amazonaws.com/IP+Addres ses.txt
Type	

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

GuardDuty > Settings > Lists

List management Info

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.

[+ Add a trusted IP list](#)

List name	List file URL	Format	Tags	Active
-----------	---------------	--------	------	--------

Trusted IP lists
Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

Threat IP lists

Threat IP lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat IP lists.

[+ Add a threat IP list](#)

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:59 22-04-2023

GuardDuty > Settings > Lists

List management Info

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

[+ Add a trusted IP list](#)

List name	List file URL	Format	Tags	Active
-----------	---------------	--------	------	--------

Trusted IP lists
Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

Threat IP lists

Threat IP lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat IP lists.

[+ Add a threat IP list](#)

Add a trusted IP list

GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

List name

Location

Format

Use TXT for files that contain simple IP lists.
By adding this list, you accept and agree to the GuardDuty service terms, including those related to third-party threat intelligence, and direct GuardDuty to read data from this resource.

☒ I agree

[Cancel](#) [Add list](#)

Activate Windows
Go to Settings to activate Windows.

11:01 22-04-2023

GuardDuty

Findings
Usage
Malware scans

Settings

Lists

S3 Protection
EKS Protection **New**
Malware Protection
RDS Protection **New**
Lambda Protection **New**
Accounts

What's New
Partners

Successfully created the list.

GuardDuty > Settings > Lists

List management **Info**

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.

+ Add a trusted IP list

Delete existing list before adding a new one.

List name	List file URL	Format	Tags	Active
ip address	https://expt8bucket.s3.ap-south-1.amazonaws...	TXT	Add tags	<input type="radio"/>

Threat IP lists

Threat IP lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat IP lists.

Activate Windows

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

11:02 22-04-2023

GuardDuty

Findings
Usage
Malware scans

Settings

Lists

S3 Protection
EKS Protection **New**
Malware Protection
RDS Protection **New**
Lambda Protection **New**
Accounts

What's New
Partners

GuardDuty > Findings

Showing 1 of 1 **1** **0** **0**

Findings **Info**

Suppress Findings **Info**

Saved rules No saved rules

Current Add filter criteria

Finding type	Resource	L	C..
<input type="checkbox"/> Policy:IAMUser/RootCredentia...	S3 Bucket: expt8bucket 6 mi...	33	

Policy:IAMUser/RootCre... **Q** **Q** **X**

Finding ID: c2c3d3b4b2450306003bd751a4a1b8be **Feedback**

Low API ListObjects was invoked using root credentials from IP address 103.49.240.76. **Info**

Investigate with Detective

Overview

Severity	LOW	Q Q
Region	ap-south-1	
Count	33	
Account ID	510027780046	Q Q
Resource ID	expt8bucket	
Created at	04-22-2023 10:51:54 ...	
Updated at	04-22-2023 11:05:44 ...	

Resource affected

Go to Settings to activate Windows

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

11:06 22-04-2023

GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection New

Malware Protection

RDS Protection New

Lambda Protection New

Accounts

What's New

Partners

GuardDuty > Settings > Lists

List management Info

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.

+ Add a trusted IP list

Delete existing list before adding a new one.

List name	List file URL	Format	Tags	Active
ip address	https://expt8bucket.s3.ap-south-1.amazonaws....	TXT	Add tags	<input type="radio"/> <input checked="" type="radio"/>

Threat IP lists

Threat IP lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat IP lists.

+ Add a threat IP list

List name	List file URL	Format	Tags	Active
-----------	---------------	--------	------	--------

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

11:07

22-04-2023

GuardDuty

Findings

Usage

Malware scans

Settings

Lists

S3 Protection

EKS Protection New

Malware Protection

RDS Protection New

Lambda Protection New

Accounts

What's New

Partners

GuardDuty > Settings > Lists

List management Info

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.

+ Add a trusted IP list

Delete existing list before adding a new one.

List name	List file URL	Format	Tags	Active
ip address	https://expt8bucket.s3.ap-south-1.amazonaws....	TXT	Add tags	<input type="radio"/> <input checked="" type="radio"/>

Threat IP lists

Threat IP lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat IP lists.

+ Add a threat IP list

List name	List file URL	Format	Tags	Active
-----------	---------------	--------	------	--------

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

11:07

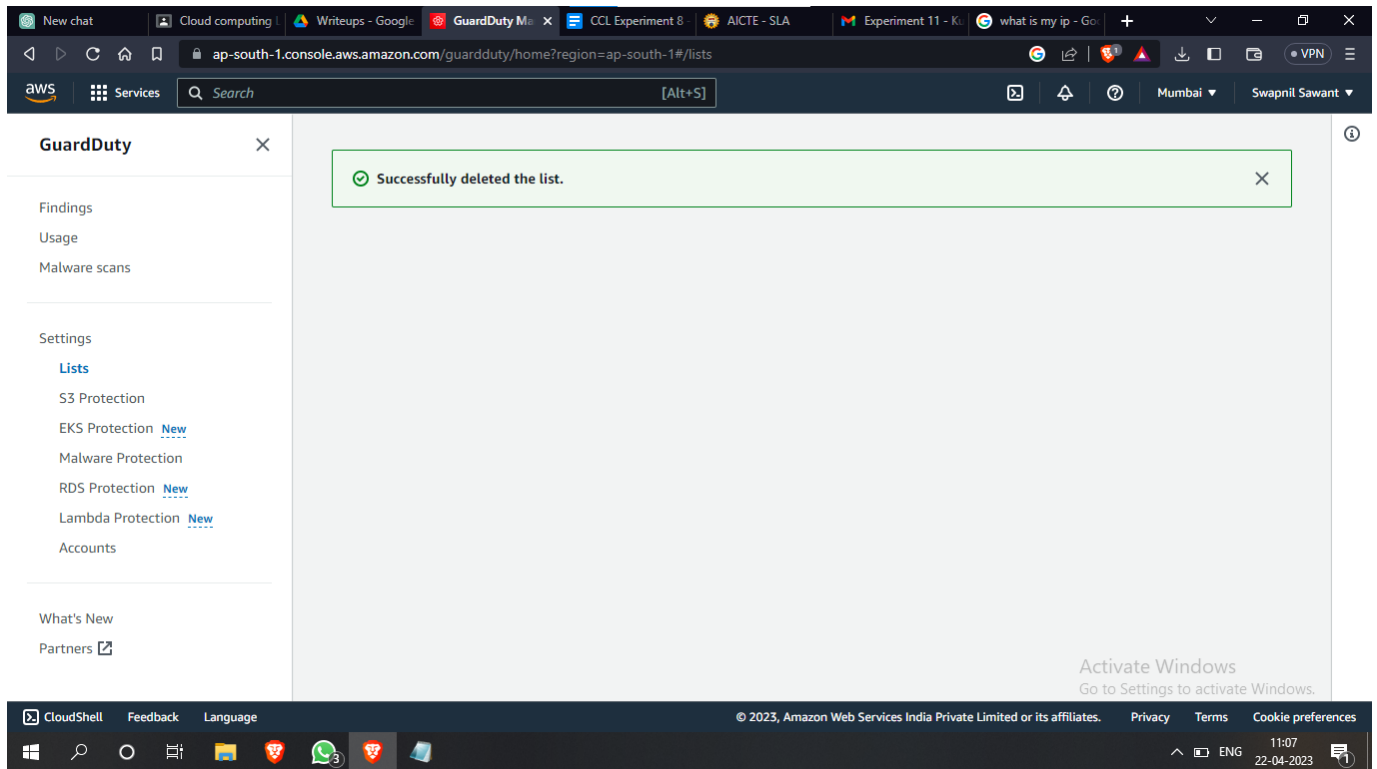
22-04-2023

Delete trusted IP list

Are you sure you want to delete this list?

Cancel

Delete



Conclusion : Hence we have studied the Security As a Service using Guard Duty Service.