**Cloud Security Vulnerabilities**

## **1- Common Vulnerabilities in Cloud Environments**

### **1. Misconfigured Cloud Services**

Misconfigurations, such as open storage buckets or insecure firewall rules, often lead to unauthorized access or data exposure. Ensuring proper configurations and regular auditing services are essential.

### **2. Insecure APIs**

APIs, vital for cloud service interactions, can be vulnerable if not properly secured. Issues like weak authentication, poor input validation, and lack of rate limiting can expose cloud environments to attacks like data breaches and denial-of-service (DoS).

### **3. Weak Identity and Access Management (IAM)**

Poorly implemented IAM policies can grant excessive permissions, enabling privilege escalation and insider threats. Implementing least-privilege access and multi-factor authentication (MFA) is key.

### **4. Data Breaches**

Insecure storage configurations, lack of encryption, and improper access control can lead to data leaks. Data should always be encrypted in transit and at rest, and access should be tightly controlled.

### **5. Vulnerable Containers and VMs**

Cloud environments using containers or virtual machines (VMs) are susceptible to attacks through outdated images or hypervisor vulnerabilities, potentially leading to host system compromise.

### 

### 

### **6. Weak Encryption**

Using deprecated encryption methods or mismanaging encryption keys can expose sensitive data. Always use strong, up-to-date encryption and proper key management practices.

### **7. Inadequate Monitoring**

Without proper logging and monitoring, detecting and responding to cloud security incidents becomes difficult. Continuous monitoring and integration with security tools are critical.

### **8. Denial of Service (DoS) Attacks**

Cloud services are targets for DoS attacks. Lack of robust protection can overwhelm resources, leading to service disruptions. Implementing DDoS protection is essential.

### **9. Shared Responsibility Model**

Misunderstanding the shared responsibility model can lead to gaps in security. While cloud providers secure the infrastructure, customers must secure their applications, configurations, and data.

**2- Vulnerability Assessment on The Cloud Environment**

* Firstly create a cloud environment on the AWS platform

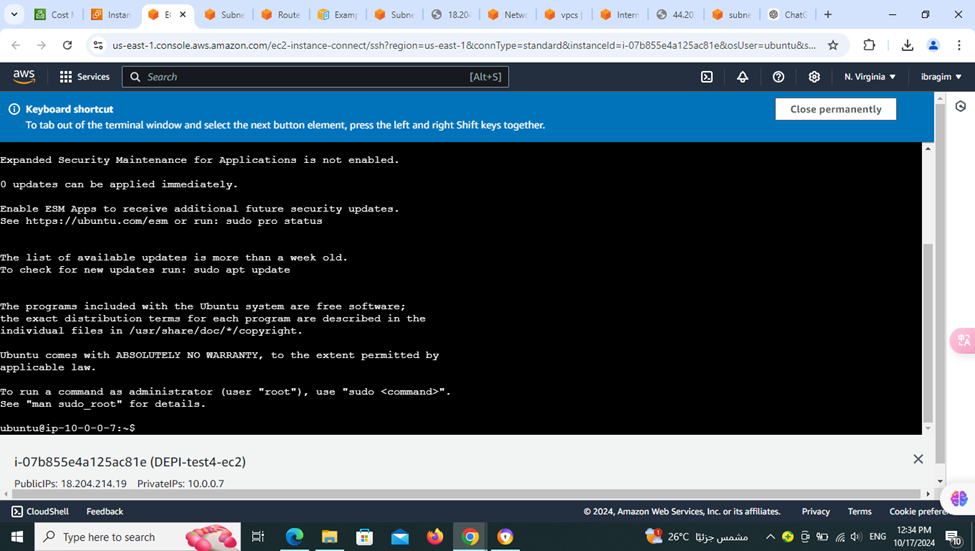
1-Set up the EC2 servers and create the VPC

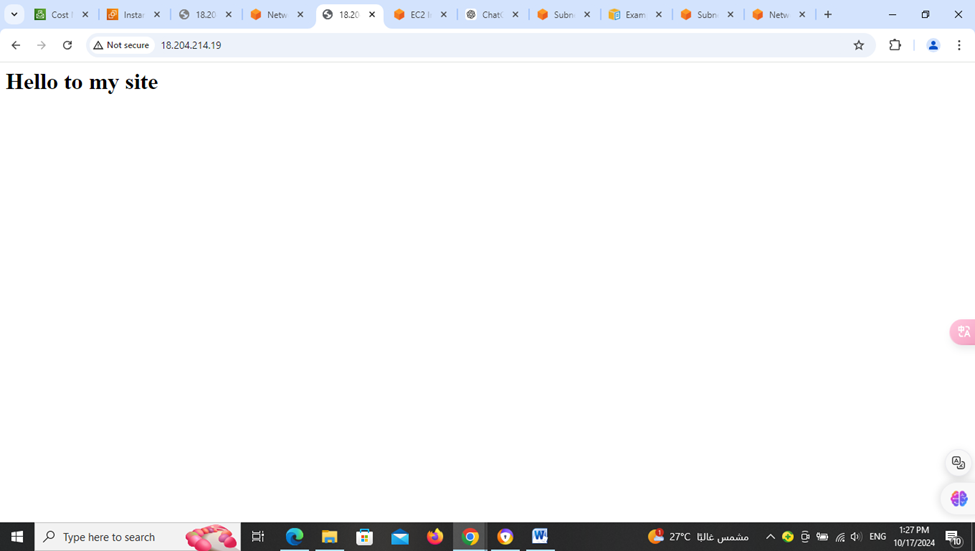
2-Set up the internet gateway

3-Add security group and IAM rules

* Applying the least privilege for the users to maintain the concept of zero trust
* Multi-factor authentication for the users

4-Access the EC2 servers and install Apache web server

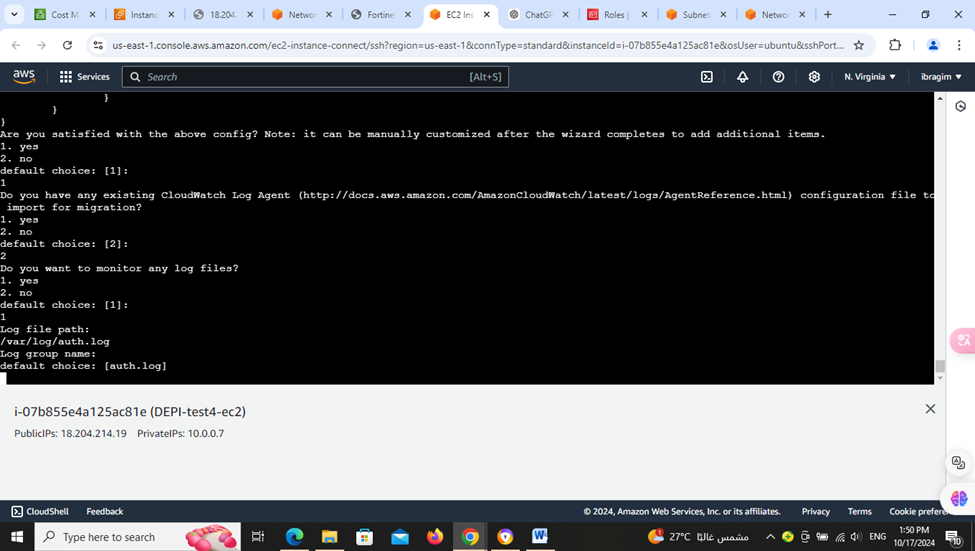




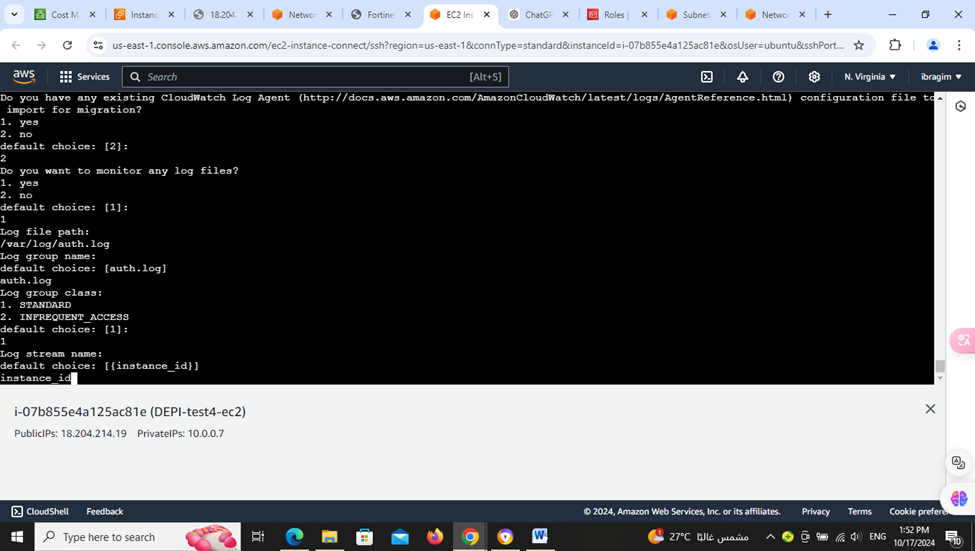
* Secondly setting up the monitoring tool and the log file

1- Set up CloudWatch tool

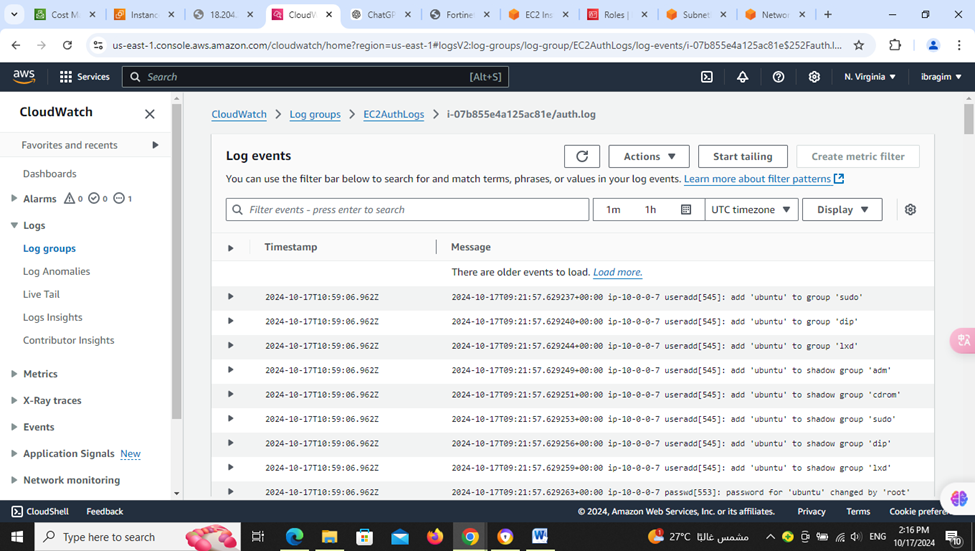
2- Set up the CloudAgent

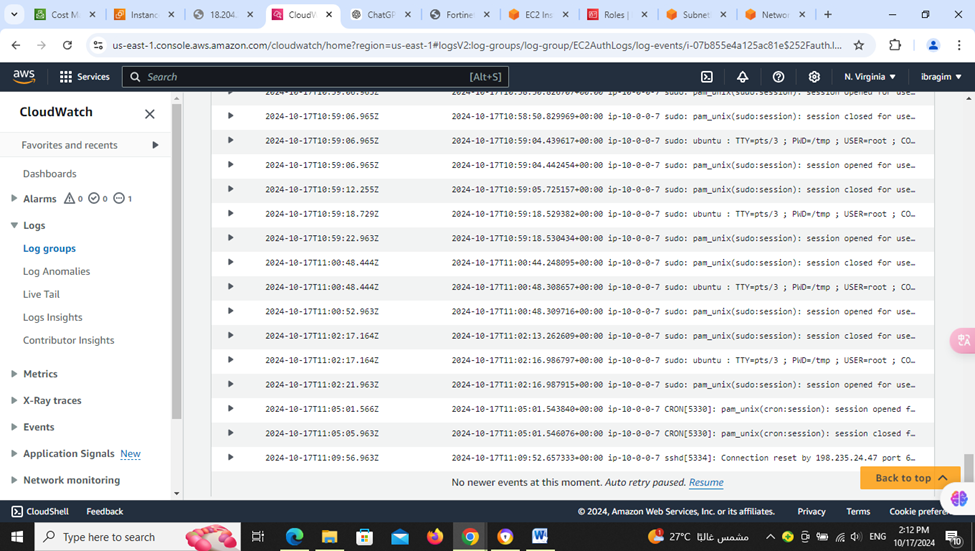


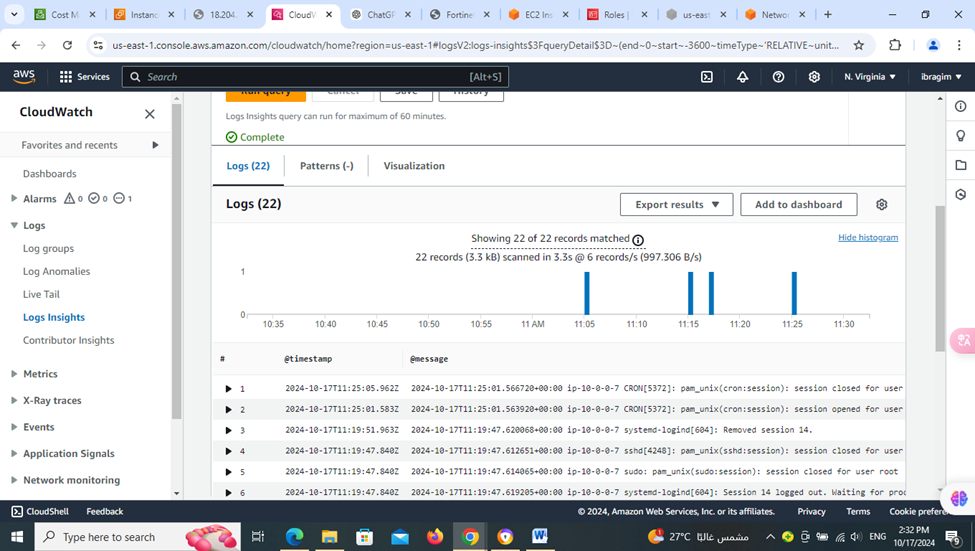
3-creating LogFile for storing the logs at the CloudWatch and monitoring it



4- monitor the EC2 servers



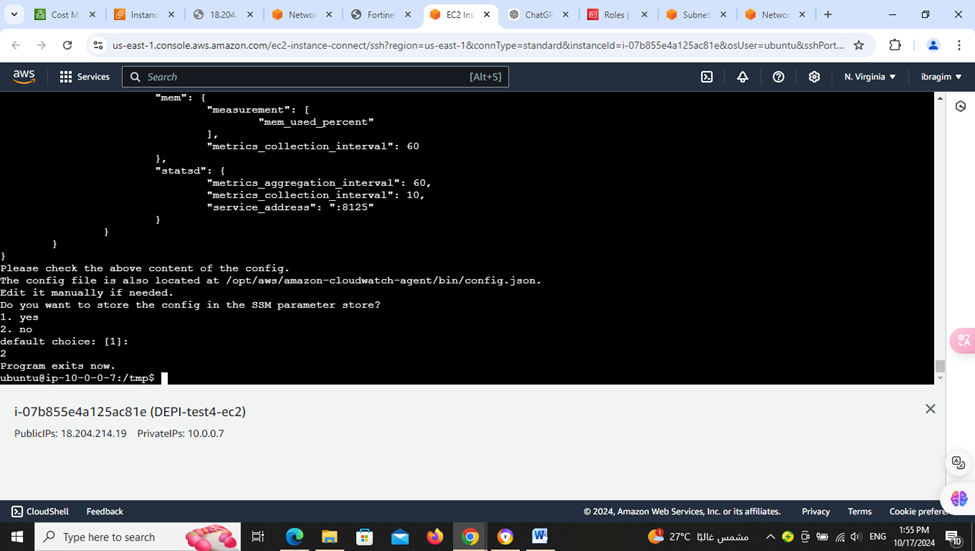


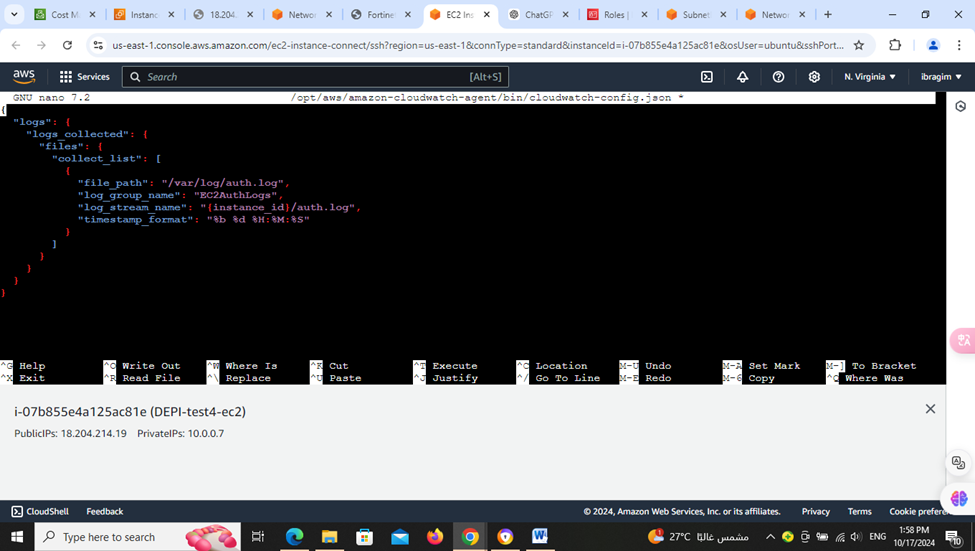


* Thirdly make alarm and responding techniques during DDos attack

1- set up an alarm that detects the frequent accesses of the servers during definite intervals of time

2- creating metrics for making the specs of the alarm requirement to take actions





3- set up the SNS tool to send an alert if the cloud environment is

being attacked specially by Dos attack to alert us due to the

criticality of the Dos attack that can be a bridge for another

attacks