**Cloud Infiltration**

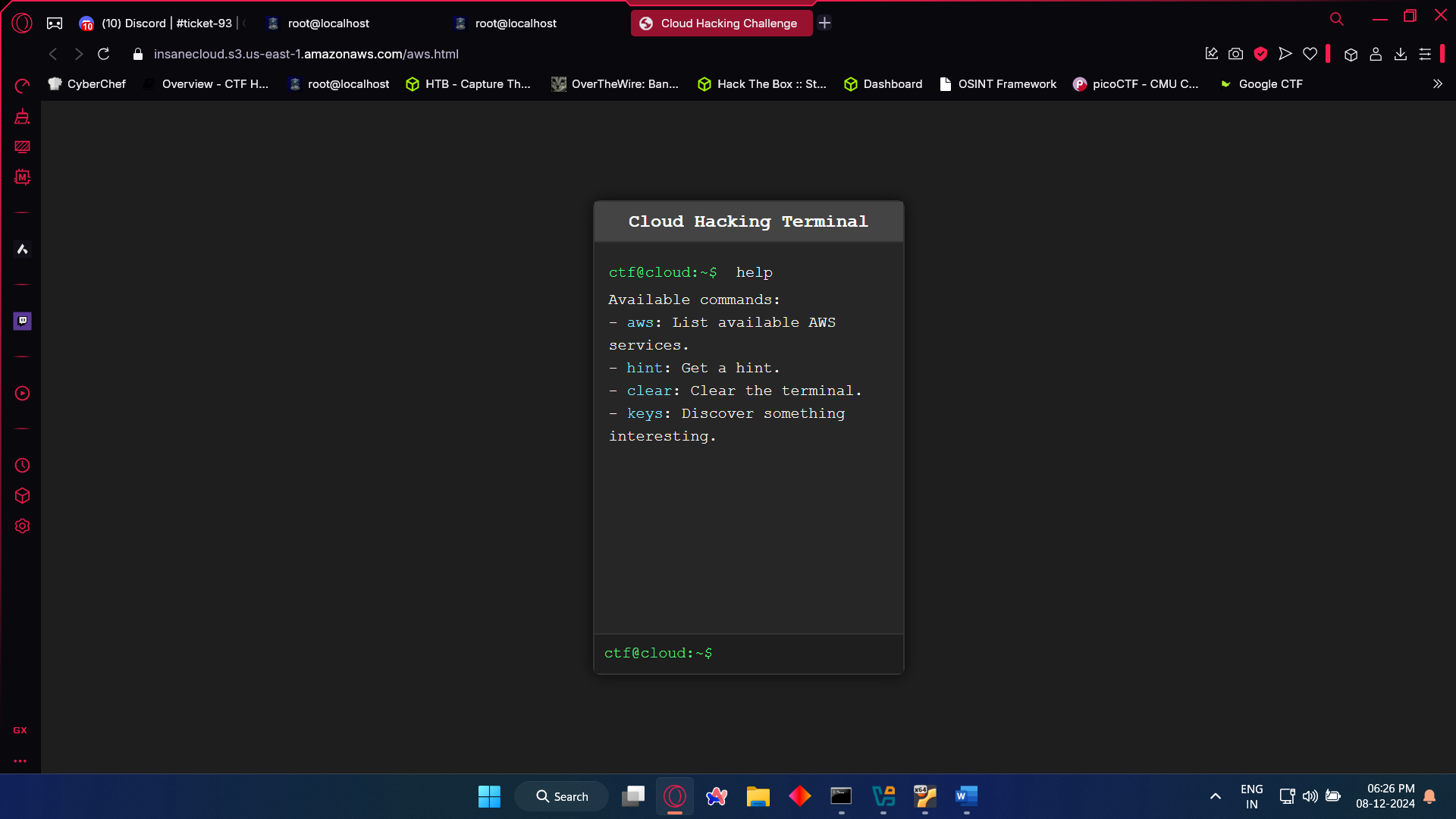
Tools Used:

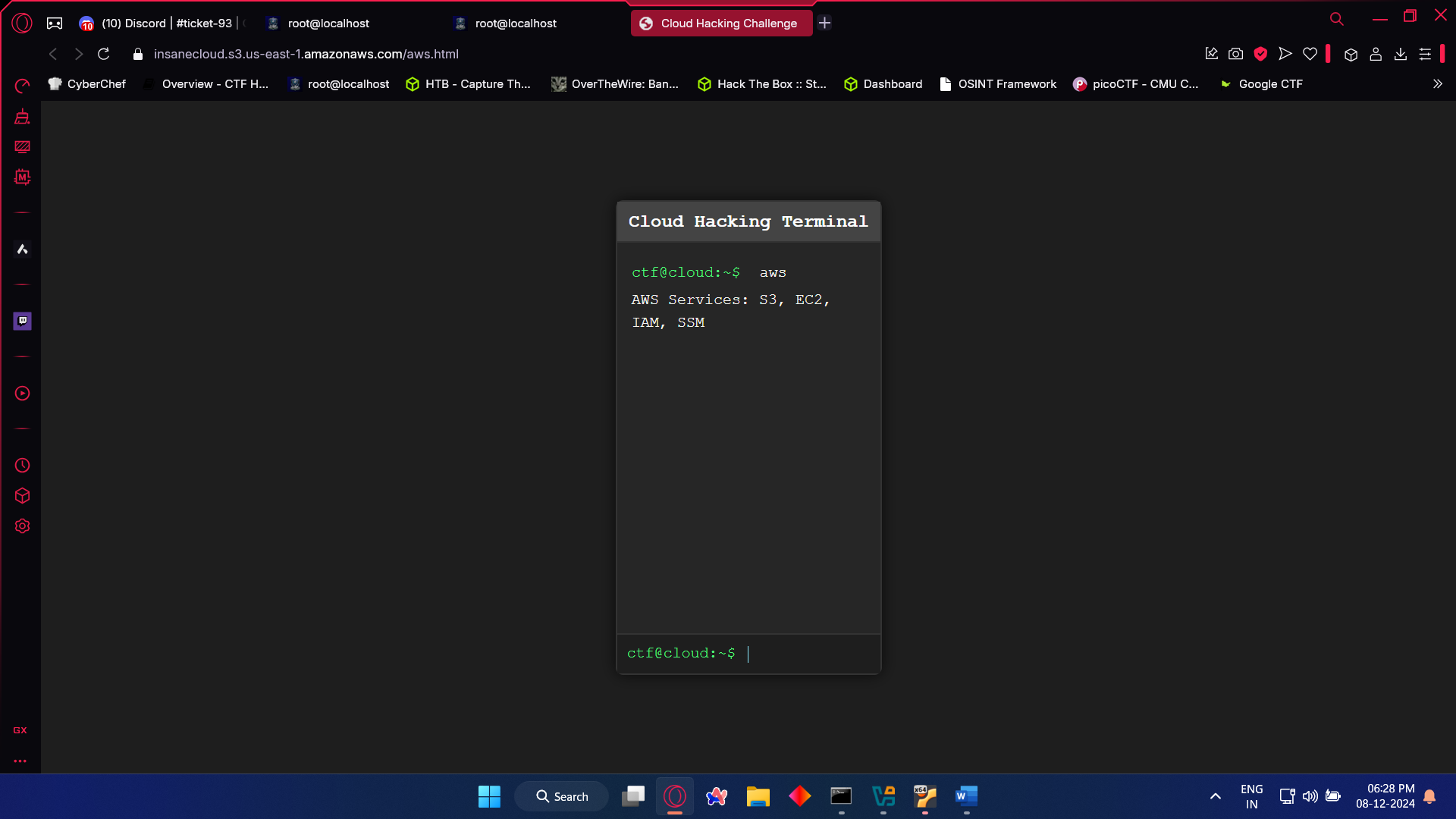
Awscli

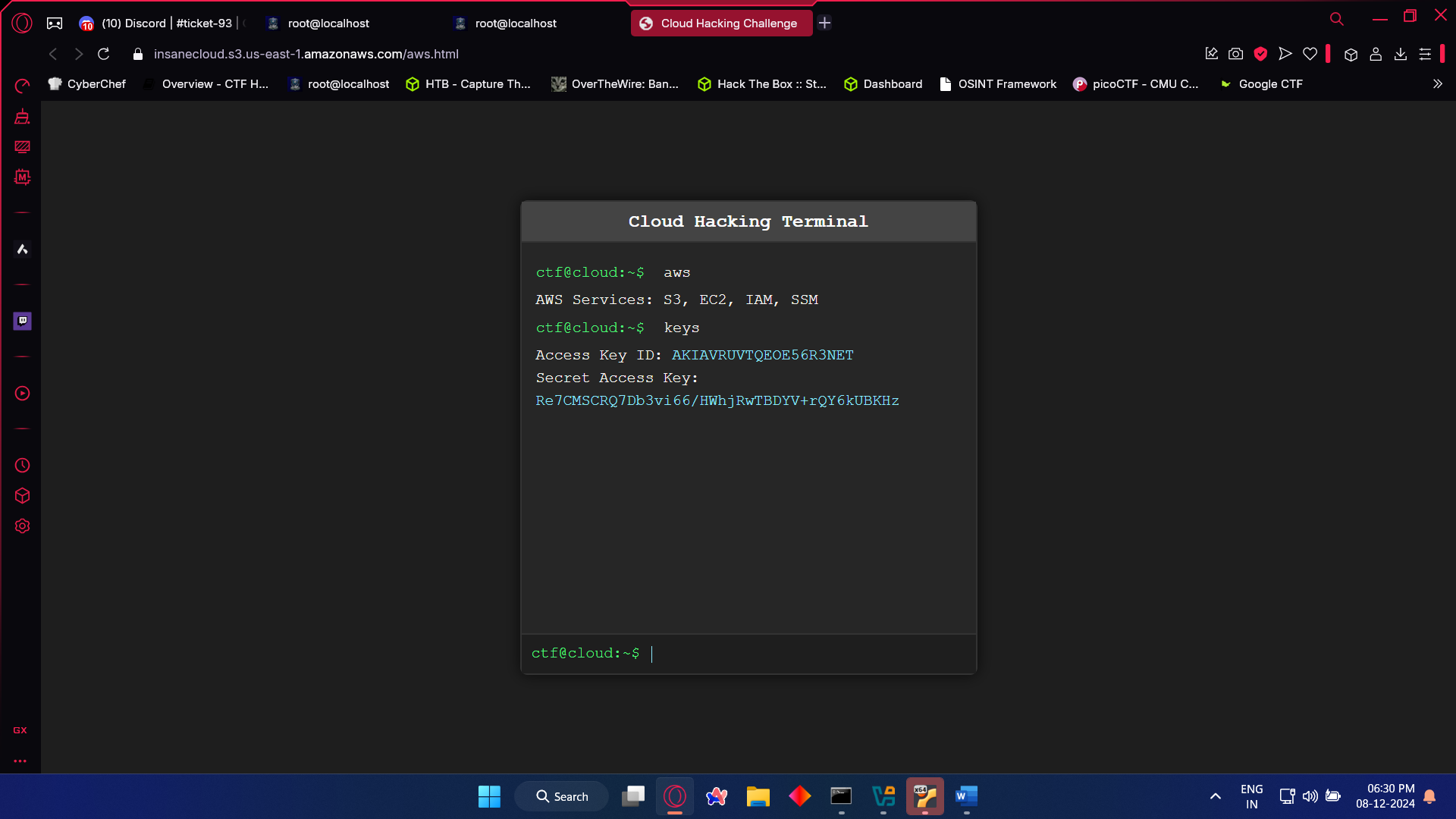
ssm

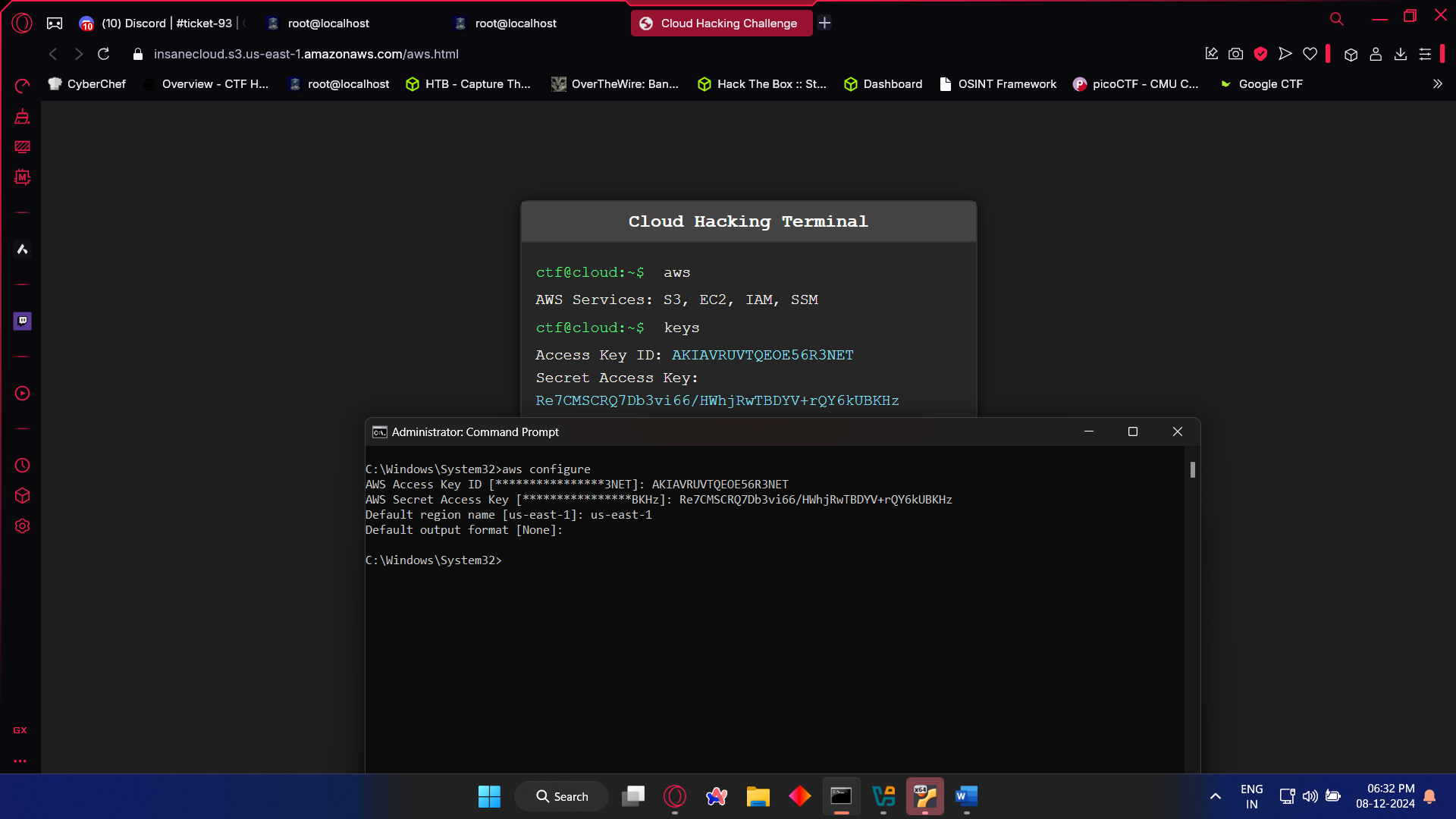
Steps:

1.Get an idea of what commands the machine allows you to use.  
ctf@cloud:~ $help

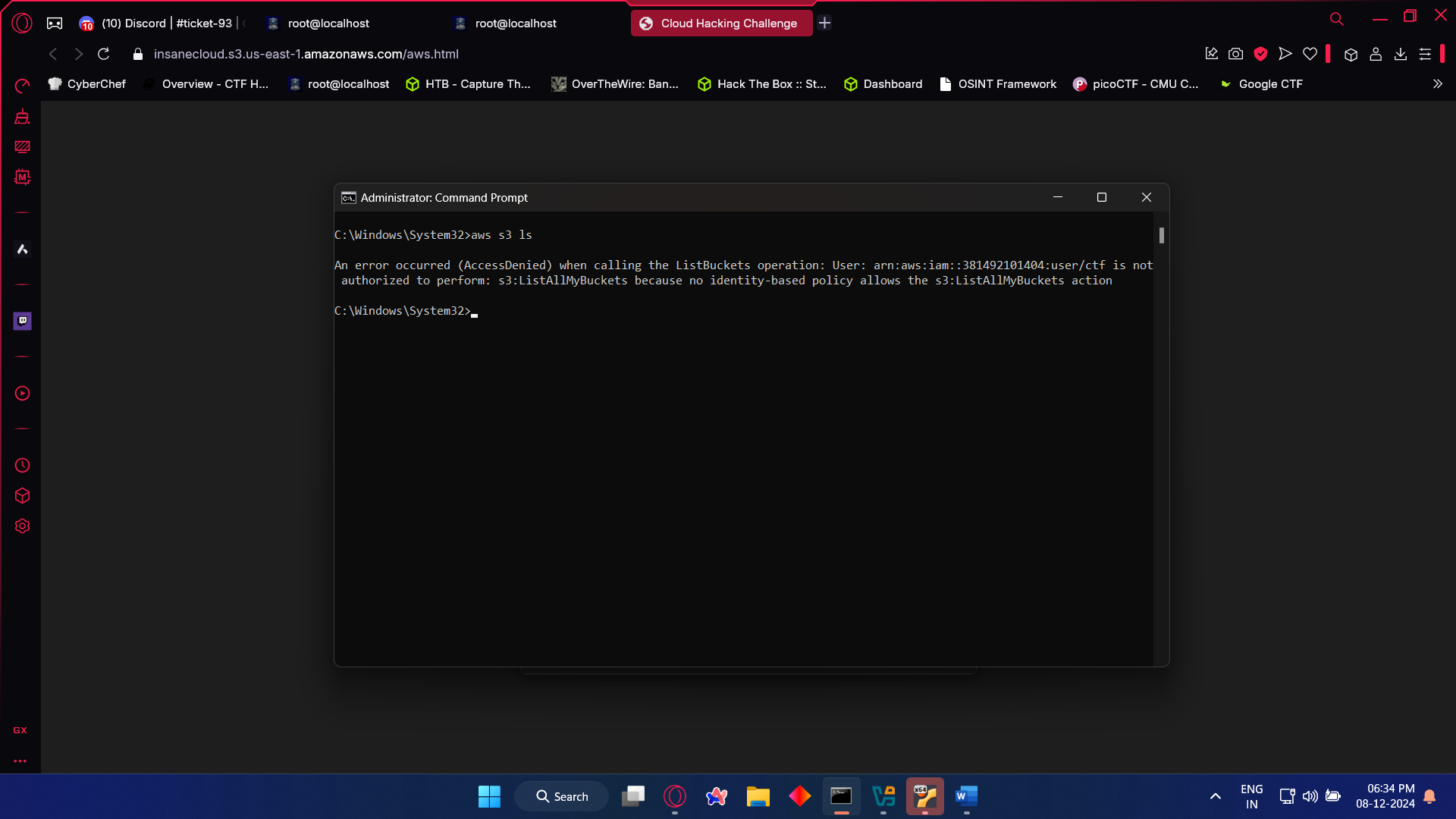
  
  
2. Now we need to know which services are available. To do so,

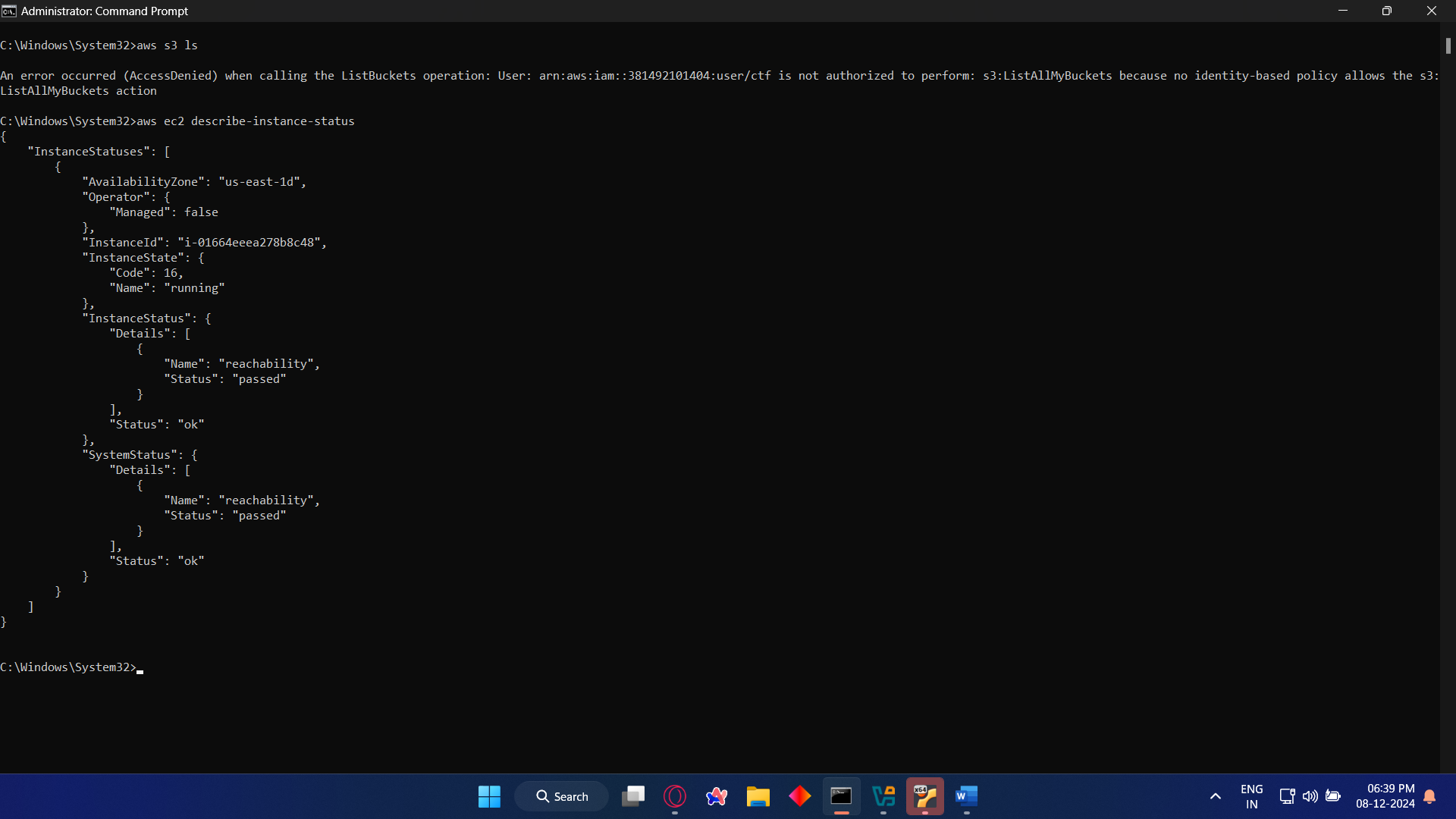
ctf@cloud:~ $aws   


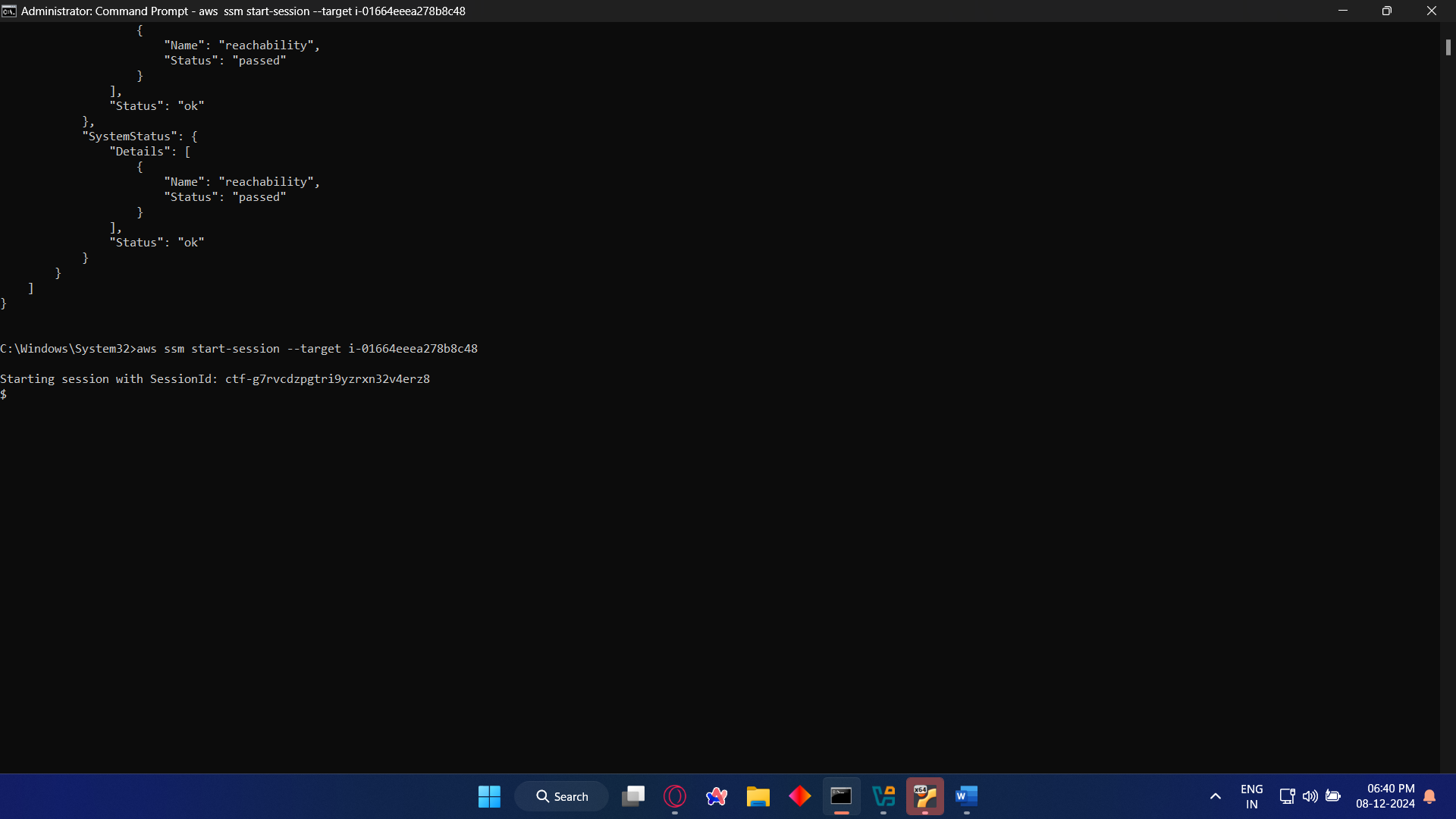
3. We need keys to configure AWS,  
ctf@cloud:~ $keys  


4. Open Command Prompt and configure it, using the cmd “aws configure”  


5. We are going to try to access the files using “aws s3 ls”, but we get an error that tells us,



6. Now we will use ssm to access these files, for that we need instance id which can be obtained using this cmd “aws ec2 describe-instance-status”  


7. Now we can use ssm using “aws ssm start-session --target Instance\_id”  


8. Use the cmd “ls” to show the folder contents  
9. Use cmd “sudo cat /home/ubuntu/flag.txt” to get the flag.  
  
Flag: r00t@localhost{c10udy\_d4ys\_4re\_fun\_1f\_y0u\_h4ve\_r41npr00f\_ge4r\_4nd\_l0ts\_0f\_cr34tiv3\_th1ngs\_t0\_d0}