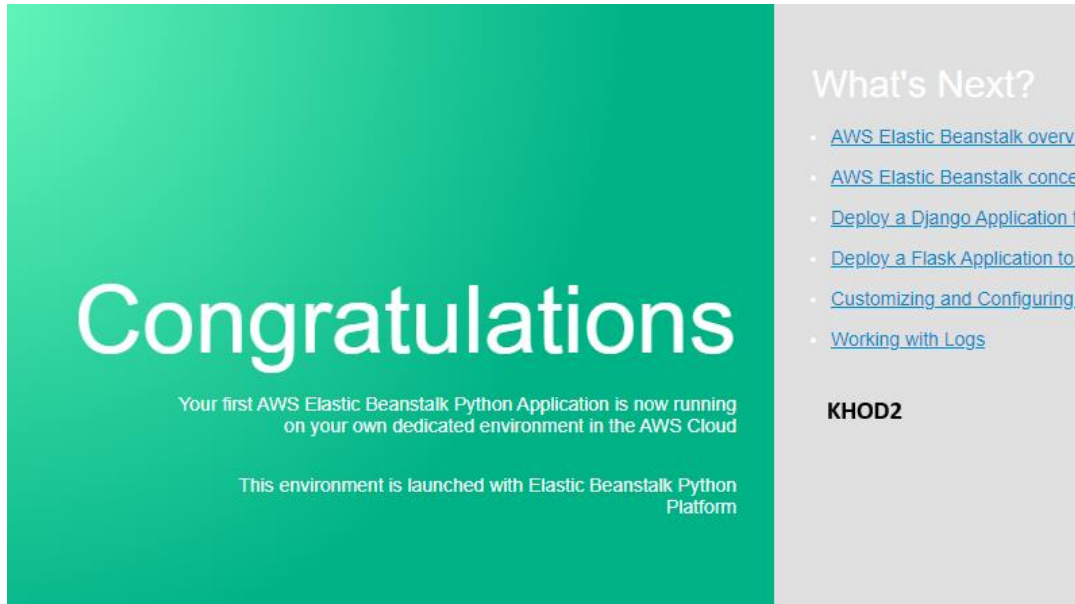


Lab 6 Notebook

6.1a

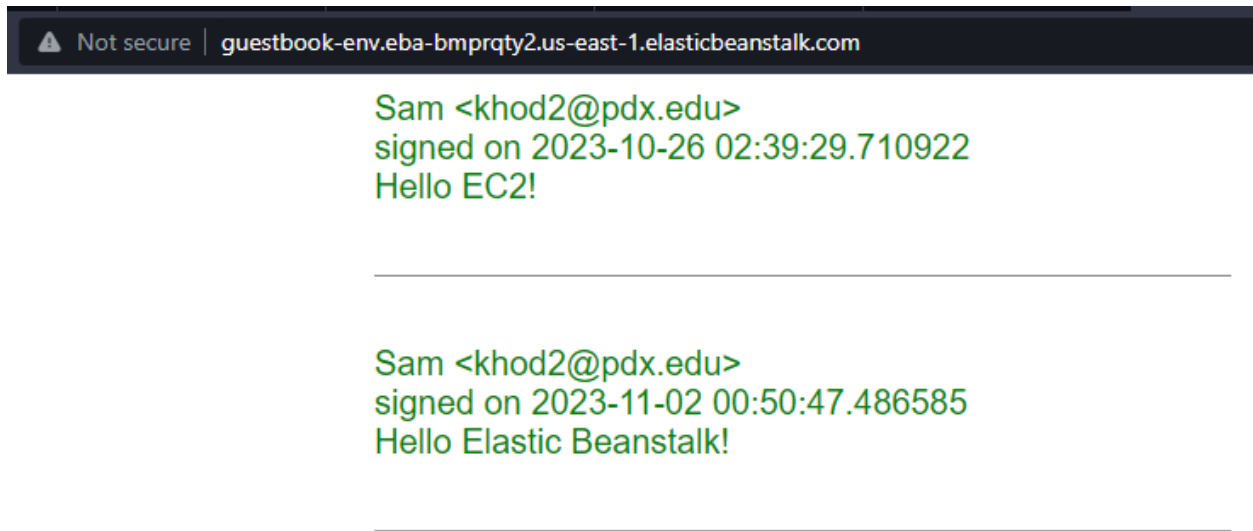
3. Take a screenshot showing it has been brought up successfully.



4. Take a screenshot of the replacement VM being started.

✓ Successfully terminated i-04b80e840725d416f

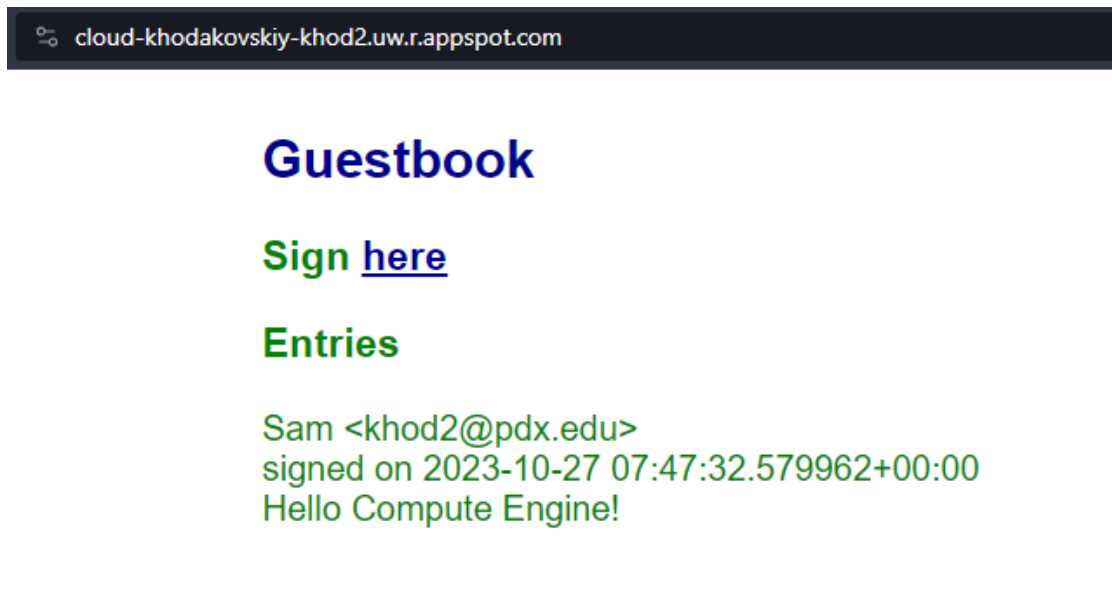
Instances (3) Info KHOD2						
Find Instance by attribute or tag (case-sensitive)						
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	
<input type="checkbox"/>	Eb-hello-env	i-0ef179594e4faaf69	✓ Running	t2.small	✓ 2/2 checks passed	
<input type="checkbox"/>	Eb-hello-env	i-04b80e840725d416f	⊖ Terminated	t2.small	-	
<input type="checkbox"/>	Eb-hello-env	i-02bbf90b7323f4a95	✓ Running	t2.small	⌚ Initializing	

7. Take a screenshot of the Guestbook including the URL with the entry in it.**Take a screenshot of them.**

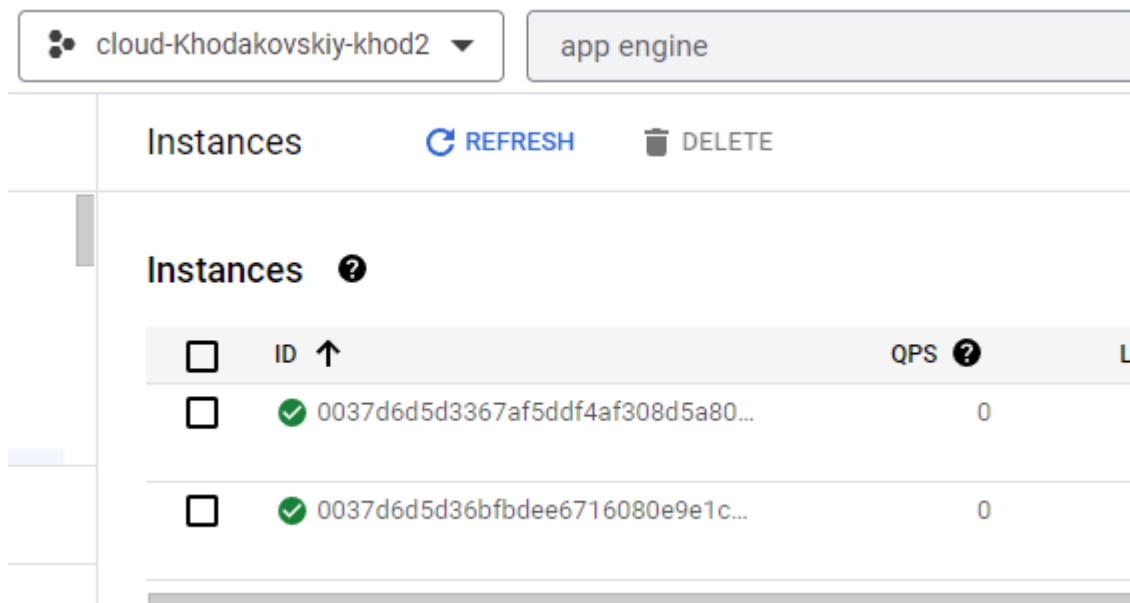
Instances (3) Info						
<div><div><div></div></div><div>Find Instance by attribute or tag (case-sensitive)</div></div>						
<div><div>running</div><div>Clear filters</div><div>KHOD2</div></div>						
<input type="checkbox"/>	Name ✎	Instance ID	Instance state	Instance type	Status	
<input type="checkbox"/>	guestbook-env	i-03422c4828aae6b4a	Running	t3.micro	2/3	
<input type="checkbox"/>	guestbook-env	i-0dd19706c2c803cb6	Running	t3.micro	2/3	
<input type="checkbox"/>	guestbook-env	i-00bee32f09d72b6c2	Running	t3.micro	2/3	

6.1g

3. Take a screenshot of the output that includes the URL in the address bar for your lab notebook.

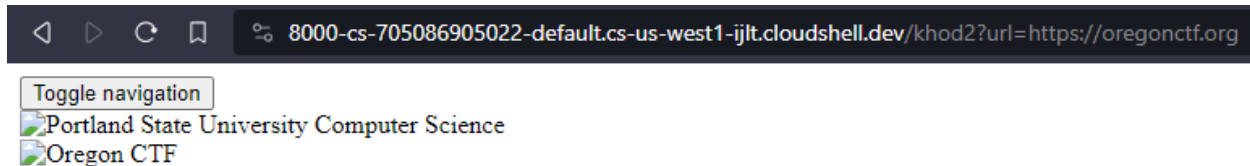


4. Take a screenshot of them.



6.2g

8. Take a screenshot of the proxy and its results including the URL containing your OdinID.



Capture-the-Flag security games and codelabs

Ones we've developed:

- Computer Systems Programming (CS 205) [CTF](#)
- Malware Reverse Engineering (CS 492) [CTF](#)
- angr Symbolic Execution (CS 492) [CTF](#)
- Cloud Security (CS 430/495) [Thunder CTF](#)
- Fuzzing (CS 492) [codelab](#)
- Smart contract symbolic execution (CS 410) [codelabs](#)
- Divergent Cryptography and Security (CyberPDX camp) [CTF](#)

Ones we like to teach from:

- bandit (Linux tools) [CTF](#)
- natas (Web Security) [CTF](#)
- PortSwigger (Web Security) [CTF](#)
- OWASP Damn Vulnerable NodeJS Application (Web Security) [CTF](#)
- flaws.cloud (Cloud Security) [v1](#) | [v2](#)
- CloudGoat (Cloud Security) [exercises](#)
- Microcorruption (Reverse Engineering) [CTF](#)
- Security Innovation (Ethereum) [CTF](#)
- Ethernaut (Ethereum) [CTF](#)
- CryptoPals (Cryptanalysis) [CTF](#)

Portland State's CTF Slack channel [here](#)

Resources

Some recommended resources include:

- Download a Windows XP VM with IDA Pro Free installed [here](#)
 - Or download IDA Pro Free [here](#)
 - Download a Linux OS Box [here](#)
 - PSU's CS 205 Computer Systems Programming [course](#)
 - PSU's CS 430 Internet, Web, and Cloud Systems [course](#)
 - PSU's CS 495 Web and Cloud Security [course](#)
 - PSU's CS 492 Malware Reverse Engineering [course](#)
 - PSU's CS 410 Blockchain Development and Security [course](#)
-


What is the security advantage of passing in the secret proxy route as an environment variable?

I am assuming that because of SSRF, where the website has some kind of URL evaluation that the user can ask for, (we enter our URL into the proxy input and the application will take us there), the user can have it go to URLs that are meant to be only internal to the app's permissions. If we have this route as an env var and the user couldn't reasonably know what route would get us to a potential SSRF entry point, then this is more safe? This relies on the service account of the container to be not restricted correctly?

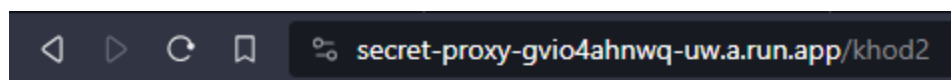
9. Take a screenshot of the image in the registry that shows the size of the container for your lab notebook.

secret-proxy

gcr.io > cloud-khodakovskiy-khod2 > secret-proxy

Filter Enter property name or value ?					
<input type="checkbox"/>	Name	Tags	Virtual Size ?	Created	Uploaded ↓
<input type="checkbox"/>	 f45cdbbb3416	latest	51.2 MB	1 minute ago	1 minute ago

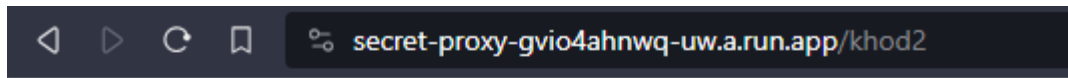
10. Take a screenshot of it that includes the proxy URL for your lab notebook.



Proxy

Enter URL to access by proxy:

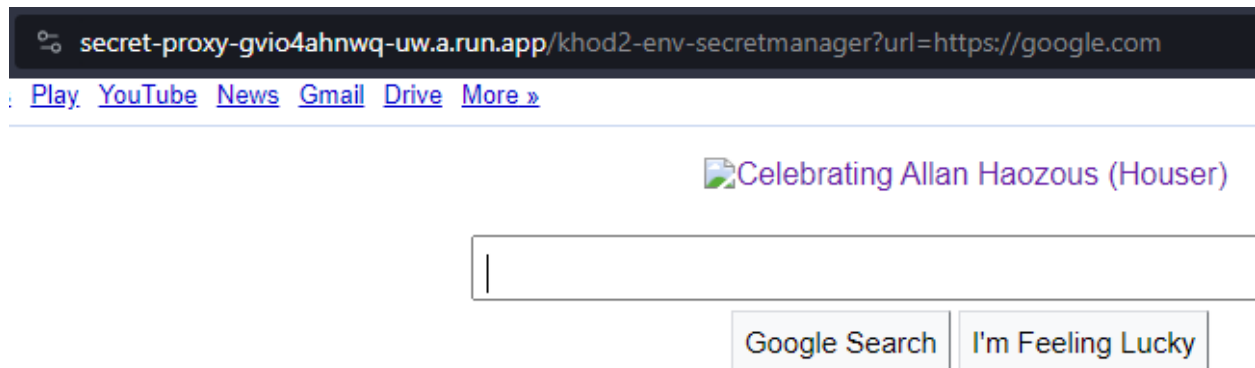
Take a screenshot of the error page that includes the proxy URL for your lab notebook.



Not Found

The requested URL was not found on the server. If you entered the URL manually

12. Take a screenshot of it that includes the proxy URL for your lab notebook.

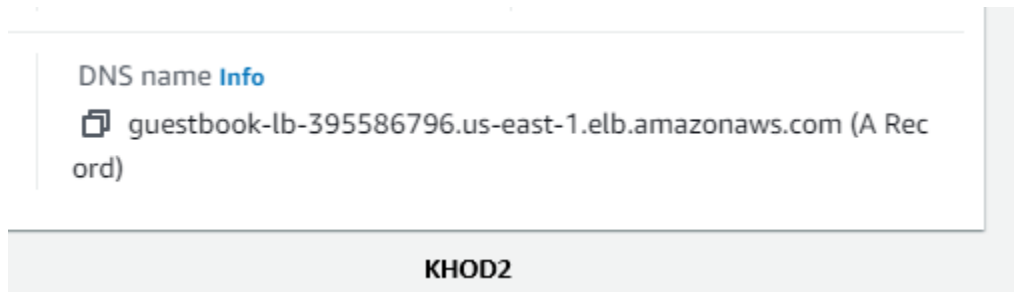


Identify the vulnerability in your lab notebook that Google has prevented.

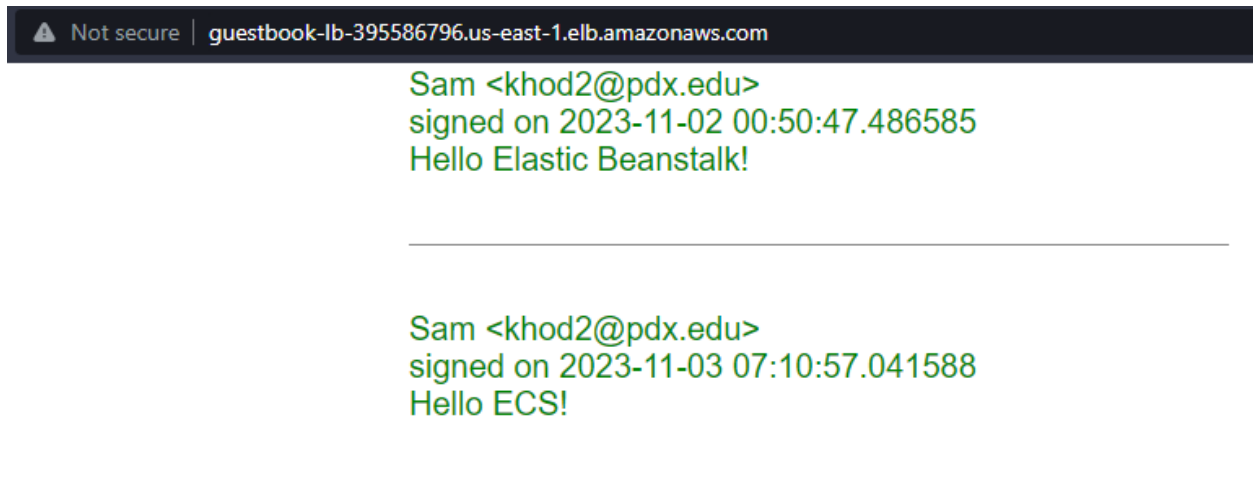
Google doesn't allow us to go to any URLs that should only be accessed internally by the service account of the container, so we can't go and list all the sensitive information in the compute metadata db.

6.3a

5. Take a screenshot of the DNS name of the guestbook-lb load balancer for your lab notebook.



6. Take a screenshot of the Guestbook app running in a browser that includes the DNS name of the site.



6.3g

2. Take a screenshot that includes the output of the command and the time it took to execute.

✓ Successful: d10835f1-ba5f-41e3-8b75-4d84d4293cf3

Started on Nov 3, 2023, 12:20:53 AM

Source

gs://cloud-khodakovskiy-khod2_cloudbuild/source/1698996040.640711-203704da7f3b440c98ac738d3ffd5ba5.tgz

Steps	Duration	BUILD LOG	EXECUTION DETAILS	BUILD ARTIFACTS
✓ Build Summary 1 Step	00:03:49	<input type="checkbox"/> Wrap lines <input type="checkbox"/> Show newest entries first		
✓ 0: gcr.io/cloud-builders/do... build --network cloudbuild -...	00:01:31	<pre> 158 ---> 9758eeab2e05 159 Successfully built 9758eeab2e05 160 Successfully tagged gcr.io/cloud-khodakovskiy-khod2/gcp_gb:latest 161 PUSH 162 Pushing gcr.io/cloud-khodakovskiy-khod2/gcp_gb 163 The push refers to repository [gcr.io/cloud-khodakovskiy-khod2/gcp_gb] 164 adb422b9e8b4: Preparing 165 cc915d0c8052: Preparing 166 b22d0e3c4441: Preparing </pre>		

3. Take a screenshot showing the container image and its virtual size

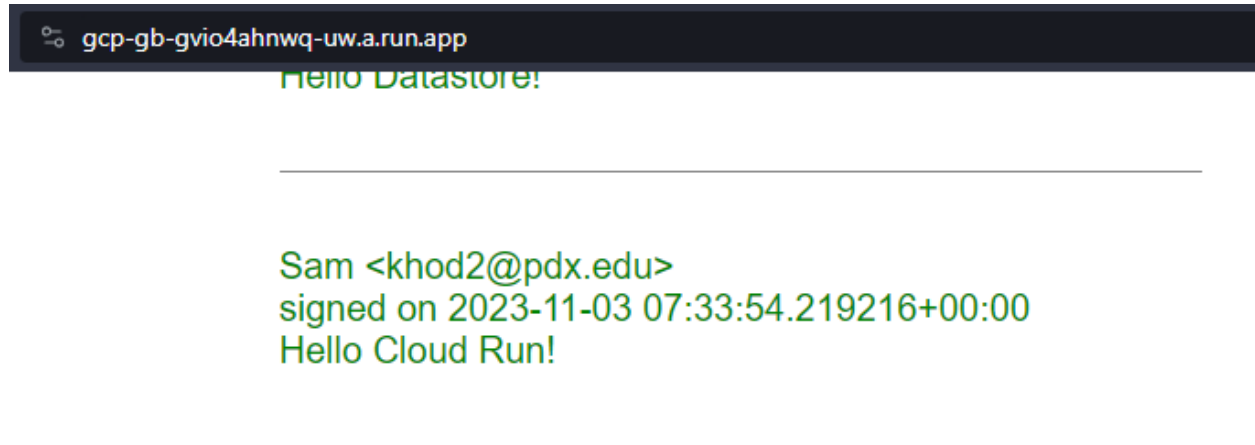
gcp_gb

gcr.io > cloud-khodakovskiy-khod2 > gcp_gb

Filter Enter property name or value

<input type="checkbox"/>	Name	Tags	Virtual Size	Created
<input type="checkbox"/>	707bbdb10795	latest	1.1 GB	5 minutes ago

5. Take a screenshot that includes the URL Cloud Run has created for your site.



What port do container instances listen on?

The container instances listen on port 8080.

What are the maximum number of instances Cloud Run will autoscale up to for your service?

100.

6.4g

4. After downloading the file from the bucket, where is it stored?

Mkstemp() creates a temporary file (without garbage collection) and stores it in a designated directory on the local file system, so it would be stored in one of the cloud shell directories.


What class in the ImageMagick package is used to do the blurring of the file?

The image class in ImageMagick.wand is used.

What lines of code perform the blurring of the image and its storage back into the filesystem?

Lines 72-74 blur the image and save it to the temporary file in the filesystem.

7. Take a screenshot of the blurred image in the output bucket for your lab notebook.

 cloud-Khodakovskiy-khod2 ▼


storage

[←](#) Bucket details

analyzed_bucket_430


Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Subject to object ACLs	None


[OBJECTS](#)
[CONFIGURATION](#)
[PERMISSIONS](#)
[PROTECTION](#)
[LIFECYC](#)

Buckets > analyzed_bucket_430 

[UPLOAD FILES](#)
[UPLOAD FOLDER](#)
[CREATE FOLDER](#)
[TRANSFER DATA ▼](#)
[MA](#)

Filter by name prefix only ▼

 Filter Filter objects and folders

<input type="checkbox"/>	Name	Size	Type
<input type="checkbox"/>	 zombie-949916_1280.jpg	116.6 KB	application/octet-stream

```
LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: j84384xyv6pc
TIME_UTC: 2023-11-04 06:16:21.452
LOG: Blurred image uploaded to: gs://analyzed_bucket_430/zombie-949916_1280.jpg

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: j84384xyv6pc
TIME_UTC: 2023-11-04 06:16:21.318
LOG:

KHOD2

LEVEL: I
NAME: blur_offensive_images
EXECUTION_ID: j84384xyv6pc
TIME_UTC: 2023-11-04 06:16:21.318
LOG: Image zombie-949916_1280.jpg was blurred.
```

11. Why are there no items returned?

There are no items listed, I'm assuming, because we created the subscription after publishing a message to the topic. There were no subscribers, so PubSub deleted the message.

12. What is the `messageId` of the published message?

```
khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$ gcloud pubsub t
message="Message #2"
messageIds:
- '9568833364735306'
khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$
```

Take a screenshot of the output of the successful pull that includes the message and its messageId.

```
khod2@pubsub:~$ gcloud pubsub subscriptions pull sub-${USER}
```

DATA	MESSAGE_ID	ORDERING_KEY	ATTRIBUTES
Message #2	9568833364735306		

```
khod2@pubsub:~$
```

15. Take a screenshot showing the messageIds and messages sent.

```
(env) khod2@cloudshell:~ (cloud-khodakovskiy-khod2)$ python3 publisher.py
Enter a message to send: Message 3!
Published 9569855567096679 to topic projects/cloud-khodakovskiy-khod2/topics/my_topic
Enter a message to send: Hi there, message 1.
Published 9568699060522205 to topic projects/cloud-khodakovskiy-khod2/topics/my_topic
Enter a message to send: Message 2 sent.
Published 9569940576977294 to topic projects/cloud-khodakovskiy-khod2/topics/my_topic
Enter a message to send: Finishing with message 3!
Published 8987394447429045 to topic projects/cloud-khodakovskiy-khod2/topics/my_topic
Enter a message to send:
```

Take a screenshot showing the same messageIds and messages received.

```
Problems khod2@pubsub: ~ x cloud-khodakovskiy-khod2
(env) khod2@pubsub:~$ python3 subscriber.py
Received message 9568699060522205: 2023-11-04 08:00:18 (projects/cloud-khodakovskiy-khod2/topics/my_topic) : Hi there, message 1.
Received message 9569940576977294: 2023-11-04 08:00:34 (projects/cloud-khodakovskiy-khod2/topics/my_topic) : Message 2 sent.
Received message 8987394447429045: 2023-11-04 08:00:40 (projects/cloud-khodakovskiy-khod2/topics/my_topic) : Finishing with message 3!
```