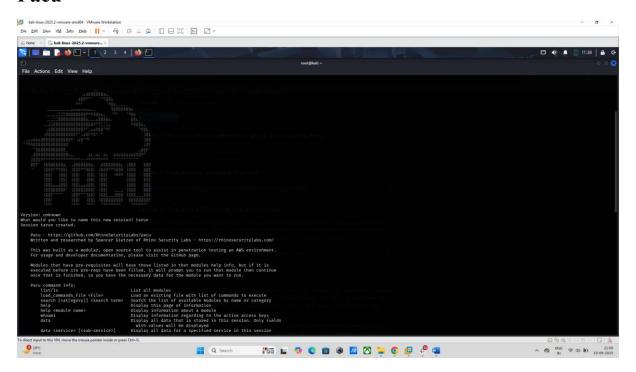


2. Cloud Attack Lab Activities:

- Tools: Pacu, awscli, CloudGoat.
- Tasks: Enumerate cloud assets, escalate privileges, exfiltrate data.
- Brief:
 - o Cloud Recon: Enumerate S3 buckets with awscli. Log:

- Privilege Escalation: Exploit an IAM misconfiguration using Pacu. Summarize in 50 words.
- Exfiltration: Extract mock data from an S3 bucket; confirm receipt in logs.

Pacu





```
to parse the data returned. Warning: The AWS CLI's authentication is not related to Pacu. Be careful to ensure that you are using the keys you want when using the AWS CLI. It is suggested to use AWS CLI profiles to solve this problem Generate a URL that will log the current user/role in to the AWS web console

Pacu (asdf:admin) > run iam_privesc_scan
Running module iam_privesc_scan...

[iam_privesc_scan] Escalation methods for current user:

[iam_privesc_scan] CONFIRMED: CreateNewPolicyVersion

[iam_privesc_scan] CONFIRMED: SetExistingDefaultPolicyVersion

[iam_privesc_scan] CONFIRMED: CreateNewPolicyVersion

[iam_privesc_scan] CONFIRMED: CreateNewPolicyVersion

[iam_privesc_scan] CONFIRMED: UpdateLoginProfile

[iam_privesc_scan] CONFIRMED: AttachUserPolicy

[iam_privesc_scan] CONFIRMED: AttachUserPolicy

[iam_privesc_scan] CONFIRMED: PutUserPolicy

[iam_privesc_scan] CONFIRMED: PutUserPolicy

[iam_privesc_scan] Attempting confirmed privilege escalation methods...

[iam_privesc_scan] Is there a specific policy you want to target? Enter its AFN now (just hit enter to automatically figure out a valid policy to target):
```



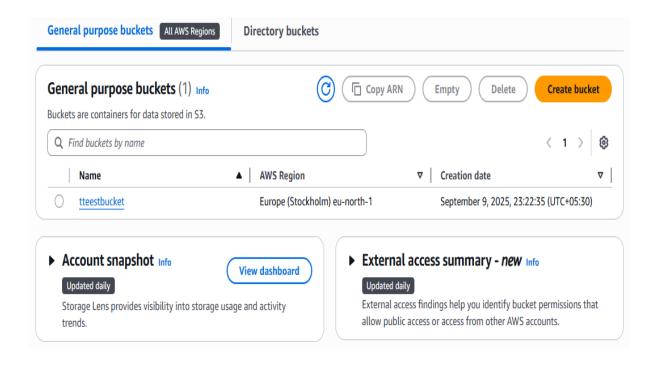
• Cloud Recon: Enumerate S3 buckets with awscli. Log:

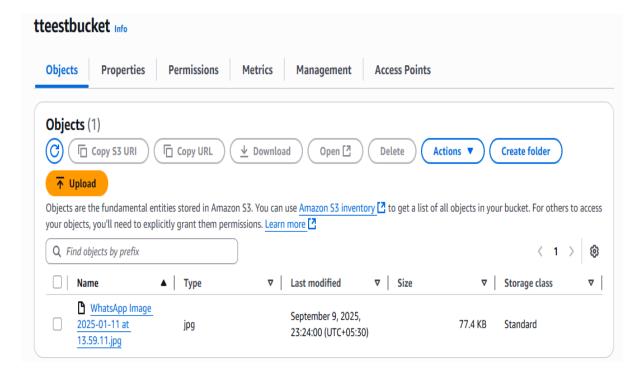
Summary:

Each project's session data is stored in a different session using Pacu. Any monitoring service, such as cloud trail, cloud watch alarms, guard duty, etc., can also conceal actions. Disabling monitoring services is another option.



Exfiltration: Extract mock data from an S3 bucket; confirm receipt in logs.







Properties

Permissions

Versions

Object overview

Owne

97 be 001 b12 fbe 0663 ad 248435 ca 6b422 d4e 33 ab 15e 2b661852 cedb64 db dbdd67

AWS Region

Europe (Stockholm) eu-north-1

Last modified

September 9, 2025, 23:24:00 (UTC+05:30)

Size

77.4 KB

Type

jpg

Key

WhatsApp Image 2025-01-11 at 13.59.11.jpg

S3 URI

s3://tteestbucket/WhatsApp Image 2025-01-11 at 13.59.11.jpg

Amazon Resource Name (ARN)

arn:aws:s3:::tteestbucket/WhatsApp Image 2025-01-11 at 13.59.11.jp g

Entity tag (Etag)

72ea0a004b62d5a20dd69d58da6e1ec8

Object URL

https://tteestbucket.s3.eu-north-1.amazonaws.com/WhatsApp+Image+2025-01-11+at+13.59.11.jpg