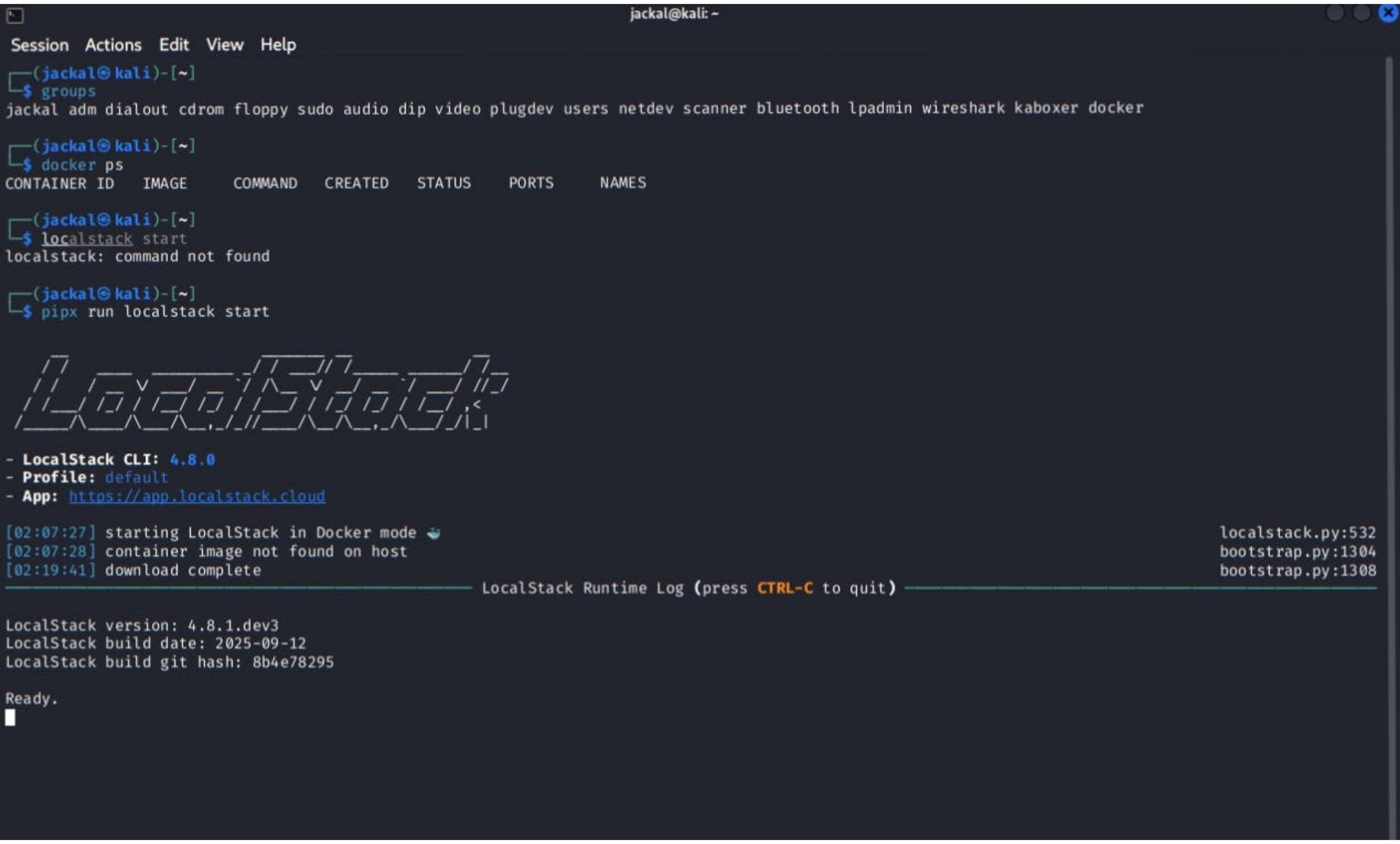
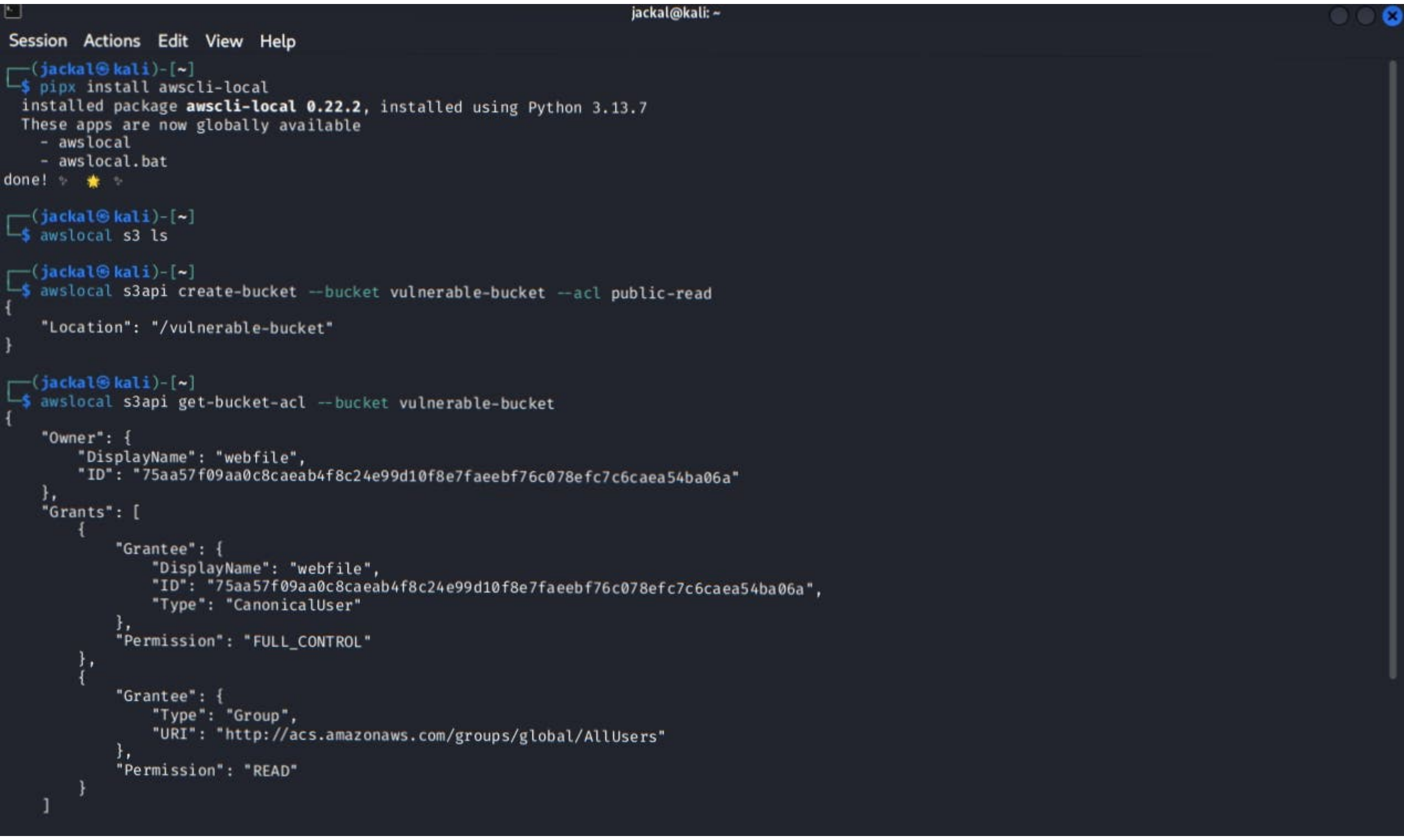
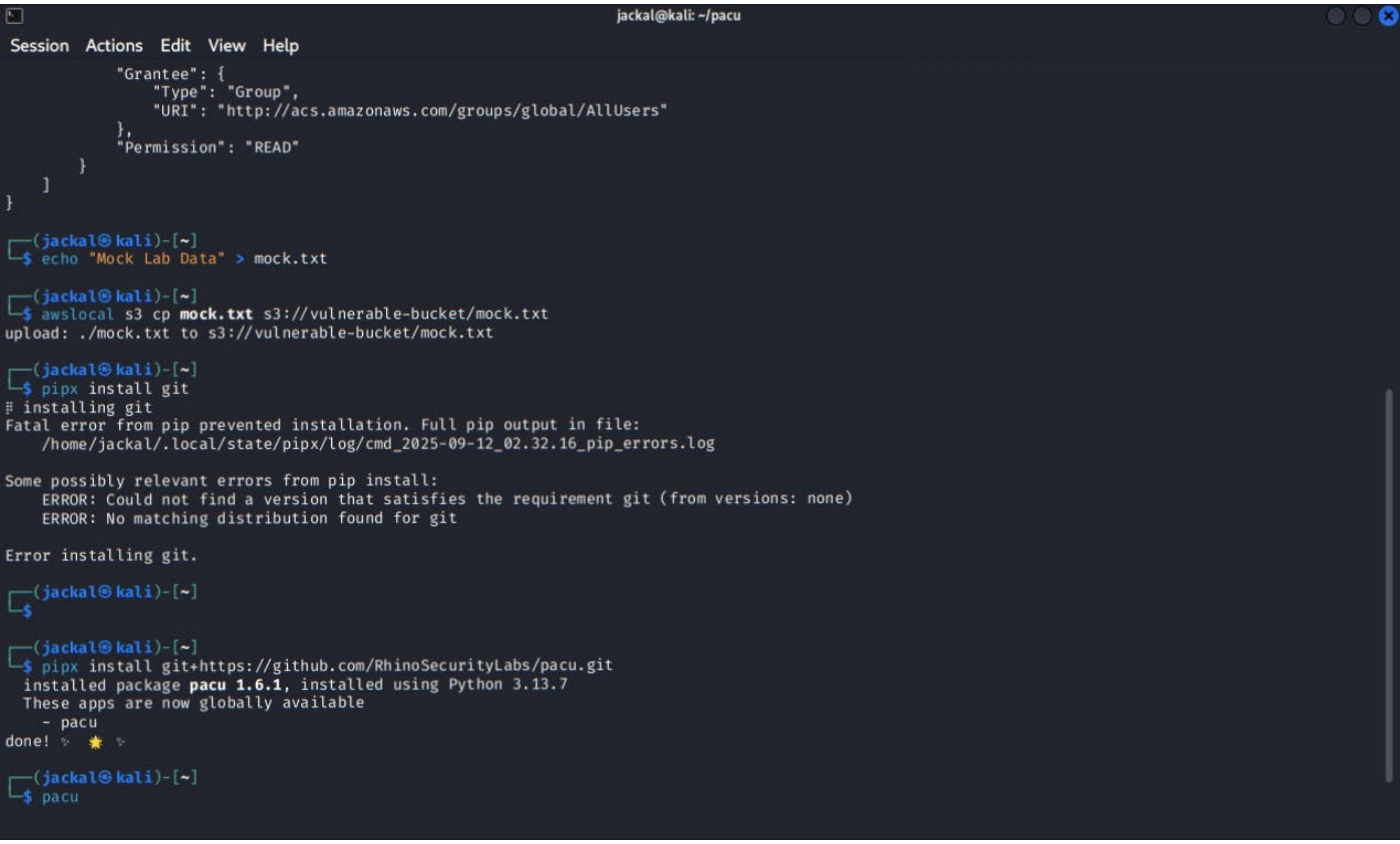


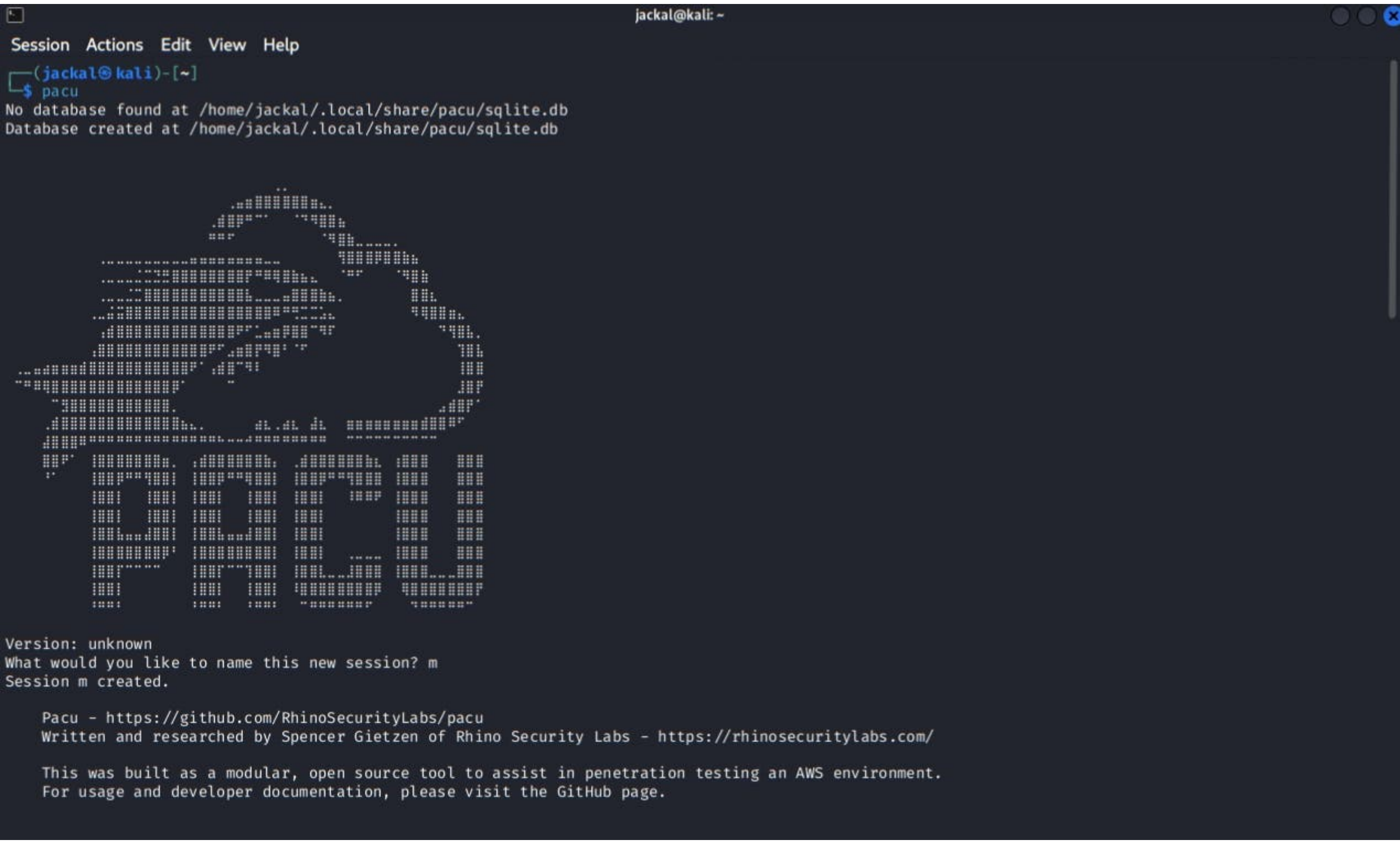
```
┌──(jackal㉿kali)-[~]
└─$ groups
jackal adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark kaboxer docker

┌──(jackal㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(jackal㉿kali)-[~]
└─$ localstack start
localstack: command not found

┌──(jackal㉿kali)-[~]
└─$ pipx run localstack start

     __                     _______ __             __
    / /   ____  _________ _/ / ___// /_____ ______/ /__
   / /   / __ \/ ___/ __ `/ /\__ \/ __/ __ `/ ___/ //_/
  / /___/ /_/ / /__/ /_/ / /___/ / /_/ /_/ / /__/ ,<
 /_____/\____/\___/\__,_/_//____/\__/\__,_/\___/_/|_|

- LocalStack CLI: 4.8.0
- Profile: default
- App: https://app.localstack.cloud

[02:07:27] starting LocalStack in Docker mode 🐳                                    localstack.py:532
[02:07:28] container image not found on host                                        bootstrap.py:1304
[02:19:41] download complete                                                        bootstrap.py:1308
──────────────────────── LocalStack Runtime Log (press CTRL-C to quit) ────────────────────────

LocalStack version: 4.8.1.dev3
LocalStack build date: 2025-09-12
LocalStack build git hash: 8b4e78295

Ready.
```



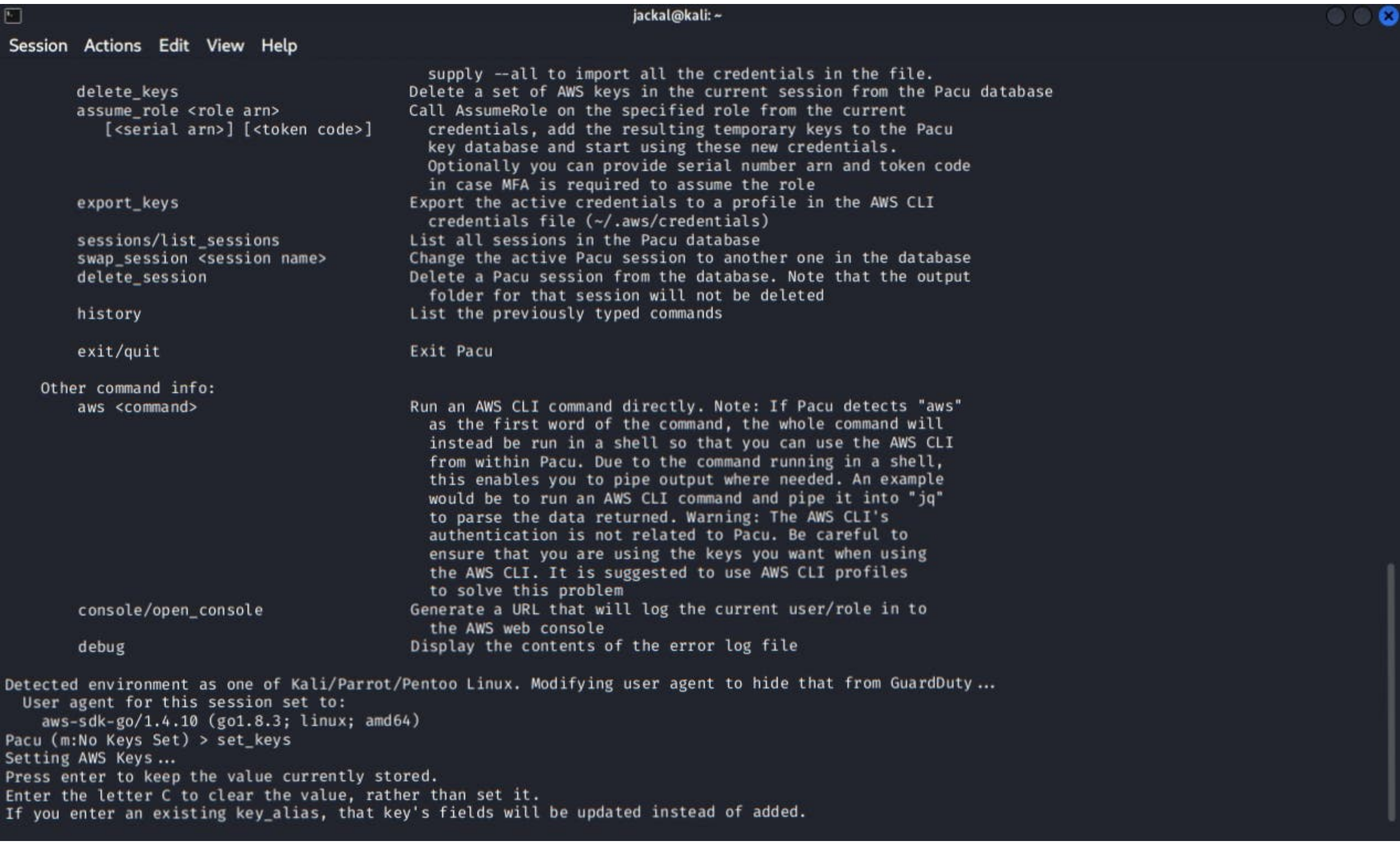
```
┌──(jackal㉿kali)-[~]
└─$ pipx install awscli-local
  installed package awscli-local 0.22.2, installed using Python 3.13.7
  These apps are now globally available
    - awslocal
    - awslocal.bat
done! ✨ 🌟 ✨

┌──(jackal㉿kali)-[~]
└─$ awslocal s3 ls

┌──(jackal㉿kali)-[~]
└─$ awslocal s3api create-bucket --bucket vulnerable-bucket --acl public-read
{
    "Location": "/vulnerable-bucket"
}

┌──(jackal㉿kali)-[~]
└─$ awslocal s3api get-bucket-acl --bucket vulnerable-bucket
{
    "Owner": {
        "DisplayName": "webfile",
        "ID": "75aa57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "webfile",
                "ID": "75aa57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
```



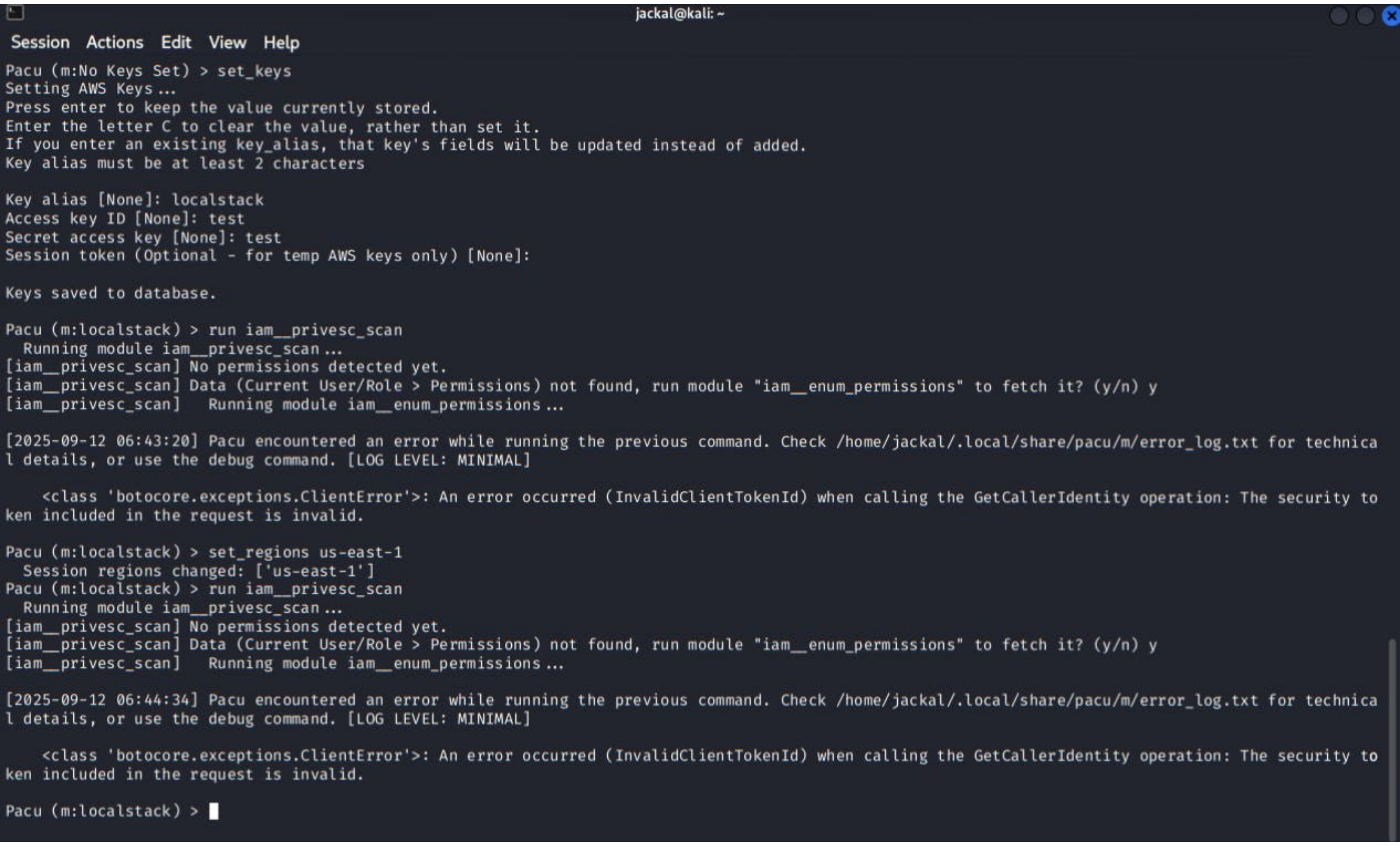
```
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}

┌──(jackal㉿kali)-[~]
└─$ echo "Mock Lab Data" > mock.txt

┌──(jackal㉿kali)-[~]
└─$ awslocal s3 cp mock.txt s3://vulnerable-bucket/mock.txt
upload: ./mock.txt to s3://vulnerable-bucket/mock.txt

┌──(jackal㉿kali)-[~]
└─$ pipx install git
⣾ installing git
Fatal error from pip prevented installation. Full pip output in file:
    /home/jackal/.local/state/pipx/log/cmd_2025-09-12_02.32.16_pip_errors.log

Some possibly relevant errors from pip install:
    ERROR: Could not find a version that satisfies the requirement git (from versions: none)
    ERROR: No matching distribution found for git

Error installing git.

┌──(jackal㉿kali)-[~]
└─$

┌──(jackal㉿kali)-[~]
└─$ pipx install git+https://github.com/RhinoSecurityLabs/pacu.git
  installed package pacu 1.6.1, installed using Python 3.13.7
  These apps are now globally available
    - pacu
done! ✨ 🌟 ✨

┌──(jackal㉿kali)-[~]
└─$ pacu
```



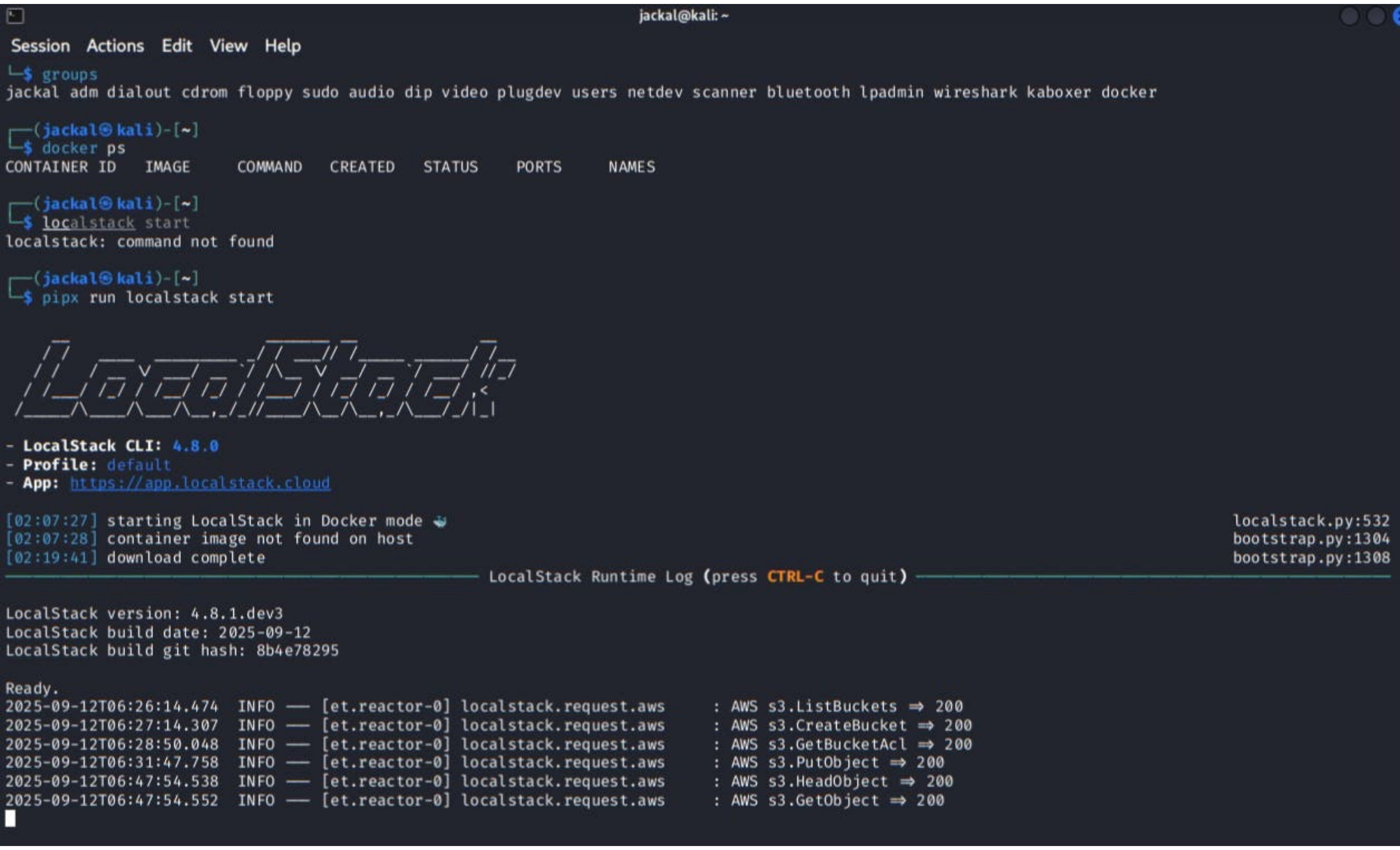
```
┌──(jackal㉿kali)-[~]
└─$ pacu
No database found at /home/jackal/.local/share/pacu/sqlite.db
Database created at /home/jackal/.local/share/pacu/sqlite.db

Version: unknown
What would you like to name this new session? m
Session m created.

    Pacu - https://github.com/RhinoSecurityLabs/pacu
    Written and researched by Spencer Gietzen of Rhino Security Labs - https://rhinosecuritylabs.com/

    This was built as a modular, open source tool to assist in penetration testing an AWS environment.
    For usage and developer documentation, please visit the GitHub page.
```



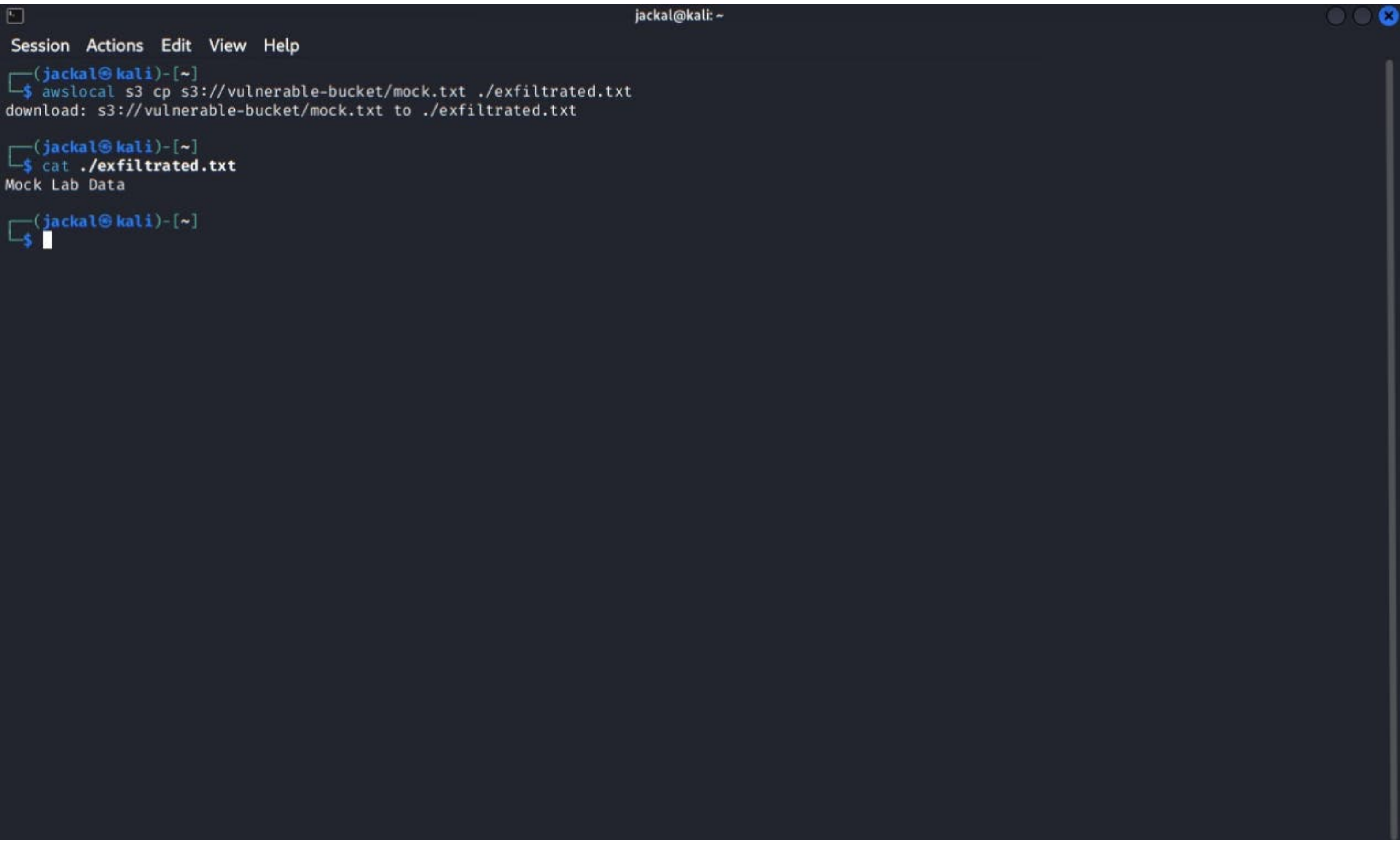
```
                                              supply --all to import all the credentials in the file.
        delete_keys                         Delete a set of AWS keys in the current session from the Pacu database
        assume_role <role arn>              Call AssumeRole on the specified role from the current
           [<serial arn>] [<token code>]      credentials, add the resulting temporary keys to the Pacu
                                              key database and start using these new credentials.
                                              Optionally you can provide serial number arn and token code
                                              in case MFA is required to assume the role
        export_keys                         Export the active credentials to a profile in the AWS CLI
                                              credentials file (~/.aws/credentials)
        sessions/list_sessions              List all sessions in the Pacu database
        swap_session <session name>         Change the active Pacu session to another one in the database
        delete_session                      Delete a Pacu session from the database. Note that the output
                                              folder for that session will not be deleted
        history                             List the previously typed commands

        exit/quit                           Exit Pacu

    Other command info:
        aws <command>                       Run an AWS CLI command directly. Note: If Pacu detects "aws"
                                              as the first word of the command, the whole command will
                                              instead be run in a shell so that you can use the AWS CLI
                                              from within Pacu. Due to the command running in a shell,
                                              this enables you to pipe output where needed. An example
                                              would be to run an AWS CLI command and pipe it into "jq"
                                              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
        console/open_console                Generate a URL that will log the current user/role in to
                                              the AWS web console
        debug                               Display the contents of the error log file

Detected environment as one of Kali/Parrot/Pentoo Linux. Modifying user agent to hide that from GuardDuty ...
  User agent for this session set to:
    aws-sdk-go/1.4.10 (go1.8.3; linux; amd64)
Pacu (m:No Keys Set) > set_keys
Setting AWS Keys ...
Press enter to keep the value currently stored.
Enter the letter C to clear the value, rather than set it.
If you enter an existing key_alias, that key's fields will be updated instead of added.
```



```
Pacu (m:No Keys Set) > set_keys
Setting AWS Keys...
Press enter to keep the value currently stored.
Enter the letter C to clear the value, rather than set it.
If you enter an existing key_alias, that key's fields will be updated instead of added.
Key alias must be at least 2 characters

Key alias [None]: localstack
Access key ID [None]: test
Secret access key [None]: test
Session token (Optional - for temp AWS keys only) [None]:

Keys saved to database.

Pacu (m:localstack) > run iam__privesc_scan
  Running module iam__privesc_scan...
[iam__privesc_scan] No permissions detected yet.
[iam__privesc_scan] Data (Current User/Role > Permissions) not found, run module "iam__enum_permissions" to fetch it? (y/n) y
[iam__privesc_scan]   Running module iam__enum_permissions...

[2025-09-12 06:43:20] Pacu encountered an error while running the previous command. Check /home/jackal/.local/share/pacu/m/error_log.txt for technica
l details, or use the debug command. [LOG LEVEL: MINIMAL]

    <class 'botocore.exceptions.ClientError'>: An error occurred (InvalidClientTokenId) when calling the GetCallerIdentity operation: The security to
ken included in the request is invalid.

Pacu (m:localstack) > set_regions us-east-1
  Session regions changed: ['us-east-1']
Pacu (m:localstack) > run iam__privesc_scan
  Running module iam__privesc_scan...
[iam__privesc_scan] No permissions detected yet.
[iam__privesc_scan] Data (Current User/Role > Permissions) not found, run module "iam__enum_permissions" to fetch it? (y/n) y
[iam__privesc_scan]   Running module iam__enum_permissions...

[2025-09-12 06:44:34] Pacu encountered an error while running the previous command. Check /home/jackal/.local/share/pacu/m/error_log.txt for technica
l details, or use the debug command. [LOG LEVEL: MINIMAL]

    <class 'botocore.exceptions.ClientError'>: An error occurred (InvalidClientTokenId) when calling the GetCallerIdentity operation: The security to
ken included in the request is invalid.

Pacu (m:localstack) > 
```



```
└─$ groups
jackal adm dialout cdrom floppy sudo audio dip video plugdev users netdev scanner bluetooth lpadmin wireshark kaboxer docker

┌──(jackal㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(jackal㉿kali)-[~]
└─$ localstack start
localstack: command not found

┌──(jackal㉿kali)-[~]
└─$ pipx run localstack start

     __                     _______ __             __
    / /   ____  _________ _/ / ___// /_____ ______/ /__
   / /   / __ \/ ___/ __ `/ /\__ \/ __/ __ `/ ___/ //_/
  / /___/ /_/ / /__/ /_/ / /___/ / /_/ /_/ / /__/ ,<
 /_____/\____/\___/\__,_/_//____/\__/\__,_/\___/_/|_|

- LocalStack CLI: 4.8.0
- Profile: default
- App: https://app.localstack.cloud

[02:07:27] starting LocalStack in Docker mode 🐳                                                                  localstack.py:532
[02:07:28] container image not found on host                                                                      bootstrap.py:1304
[02:19:41] download complete                                                                                      bootstrap.py:1308
─────────────────────────────────────────── LocalStack Runtime Log (press CTRL-C to quit) ───────────────────────────────────────────

LocalStack version: 4.8.1.dev3
LocalStack build date: 2025-09-12
LocalStack build git hash: 8b4e78295

Ready.
2025-09-12T06:26:14.474  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.ListBuckets => 200
2025-09-12T06:27:14.307  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.CreateBucket => 200
2025-09-12T06:28:50.048  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.GetBucketAcl => 200
2025-09-12T06:31:47.758  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.PutObject => 200
2025-09-12T06:47:54.538  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.HeadObject => 200
2025-09-12T06:47:54.552  INFO --- [et.reactor-0] localstack.request.aws     : AWS s3.GetObject => 200
```



```
┌──(jackal㉿kali)-[~]
└─$ awslocal s3 cp s3://vulnerable-bucket/mock.txt ./exfiltrated.txt
download: s3://vulnerable-bucket/mock.txt to ./exfiltrated.txt

┌──(jackal㉿kali)-[~]
└─$ cat ./exfiltrated.txt
Mock Lab Data

┌──(jackal㉿kali)-[~]
└─$ 
```