## **PROWLER**

#### Introduction:

Prowler is an open-source security tool tailored for Amazon Web Services (AWS). It automates security assessments, auditing AWS configurations for adherence to best practices in areas like IAM, logging, networking, and more. Developed by security experts, Prowler helps identify vulnerabilities and misconfigurations, empowering users to strengthen the security of their AWS environments. It's highly configurable, integrates with AWS CLI, and provides a valuable toolset for routine assessments, continuous monitoring, and incident response. Regular updates ensure alignment with AWS changes and evolving security standards.

## Where we can run prowler:

- 1. Workstation,
- 2. EC2 instance.
- 3. Fargate or any other container,
- 4. Codebuild,
- 5. CloudShell

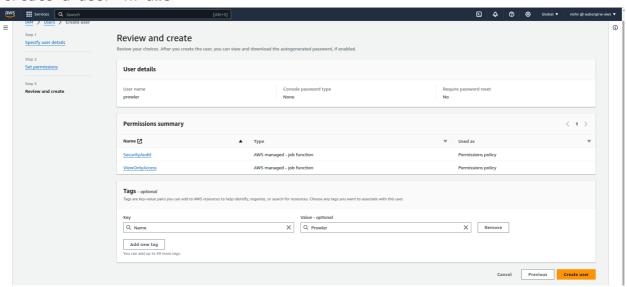
## \*\*Prerequisites:

- 1. Python >= 3.9
- 2. Poetry
- 3. AWS credentials (access key and security key) with appropriate Roles required for prowler:
  - 1. arn:aws:iam::aws:policy/SecurityAudit
  - 2. arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

#### **Installation:**

- 1. git clone https://github.com/prowler-cloud/prowler
- 2. cd prowler
- 3. poetry shell
- 4. poetry install
- 5. python prowler.py -v

6. Create a user in aws



allow only programmatic access with cli (access key and secret key)

```
    Access key created
    This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later, However, you can create a new access key any time.
```

- 7. here we are running it on local system but it is recommended to use any computing device having more than GB of RAM.
- 8. install python and poetry on Ubuntu
- 9. clone the PROWLER Reop \*\*git clone https://github.com/prowlercloud/prowler\*\*
- 10. list prowler ls
- 11. cd prowler
- 12. sudo apt install python3-poetry
- 13. aws configure
  - set AWS access key and secret key for the account which you want to audit
- 14. to check for prowler version python prowler.py -v
- 15. run prowler aws --list-checks command.

```
Inter 2021-11-24 11-46-13

Concessablyzer analled) Check if IM Access Malyzer is enabled accessablyzer (analled) Inthout, findings) Check if IM Access Analyzer is enabled without findings - accessablyzer (low)

accessablyzer (analled) Inthout, findings) Check if IM Access Analyzer is enabled without findings - accessablyzer (low)

account, ministrat, crief (context, check) Lot security, billing, and operations of Accessablyzer (low)

account, security, centrol, crief (context, check) Lot security, billing, and operations of Accessablyzer (low)

account, security, questions, are registered in the age, account) finence security prestricts are registered in the AMS account. Increase (low)

account, security, questions, are registered in the age, account) finence security appetitions are registered in the AMS account. Increase (low)

analyzer (low) questions, are registered in the age, account) finence security appetitions are registered in the AMS account. Increase (low)

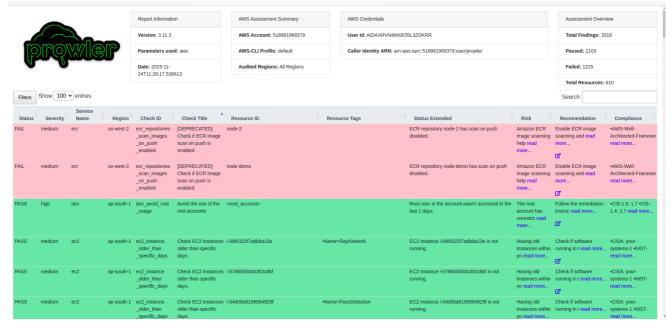
analyzer (low) questions, are registered in the age, account) finence security appetitions, and account (low) and account (low
```

#### 17. if you face this issue

[Module: utils] CRITICAL: Ooops! You reached your user session maximum open files. To solve this issue, increase the shell session limit by running this command ulimit -n 4096. For more info visit <a href="https://docs.prowler.cloud/en/latest/troubleshooting/">https://docs.prowler.cloud/en/latest/troubleshooting/</a>

run this command ulimit -n 4096

18. to run html output run Xdg-open file\_location command



# 19. Commands that might be useful: To check for only specific services

prowler aws --services s3 ec2

#### To list all the compliances available

prowler aws --list-compliance