

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

The screenshot shows the AWS IAM console 'Review and create' page. The user name is 'prowler', the console password type is 'None', and 'Require password reset' is 'No'. The permissions summary shows two policies: 'SecurityAudit' and 'ViewOnlyAccess', both of type 'AWS managed - job function'. The tags section is empty, with a note that you can add up to 49 more tags. At the bottom, there are 'Cancel', 'Previous', and 'Create user' buttons.

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/prowler-cloud/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.

```
Date: 2023-11-24 11:46:13
[accessanalyzer_enabled] Check if IAM Access Analyzer is enabled - accessanalyzer [low]
[accessanalyzer_enabled_without_findings] Check if IAM Access Analyzer is enabled without findings - accessanalyzer [low]
[account_maintain_current_contact_details] Maintain current contact details. - account [medium]
[account_maintain_different_contact_details_to_security_billing_and_operations] Maintain different contact details to security, billing and operations. - account [medium]
[account_security_contact_information_is_registered] Ensure security contact information is registered. - account [medium]
[account_security_questions_are_registered_in_the_aws_account] Ensure security questions are registered in the AWS account. - account [medium]
[acm_certificates_expiration_check] Check if ACM certificates are about to expire in specific days or less - acm [high]
[acm_certificates_transparency_logs_enabled] Check if ACM certificates have Certificate Transparency logging enabled - acm [medium]
[apigateway_restag_api_authorizers_enabled] Check if API Gateway has configured authorizers. - apigateway [medium]
[apigateway_restag_client_certificate_enabled] Check if API Gateway Stage has client certificate enabled to access your backend endpoint. - apigateway [medium]
[apigateway_restag_public] Check if API Gateway endpoint is public or private. - apigateway [medium]
[apigateway_restag_public_with_authorizer] Check if API Gateway public endpoint has an authorizer configured. - apigateway [medium]
[apigateway_restag_waf_acl_attached] Check if API Gateway Stage has a WAF ACL attached. - apigateway [medium]
[apigateway_v2_api_access_logging_enabled] Ensure API Gateway V2 has Access Logging enabled. - apigateway [medium]
[apigateway_v2_api_authorizers_enabled] Checks if API Gateway V2 has configured authorizers. - apigateway [medium]
[appstream_fleet_default_internet_access_disabled] Ensure default Internet Access from your Amazon AppStream Fleet streaming instances should remain unchecked. - appstream [medium]
[appstream_fleet_maximum_session_duration] Ensure user maximum session duration is no longer than 10 hours. - appstream [medium]
[appstream_fleet_session_disconnect_timeout] Ensure session disconnect timeout is set to 5 minutes or less. - appstream [medium]
[appstream_fleet_session_idle_disconnect_timeout] Ensure session idle disconnect timeout is set to 10 minutes or less. - appstream [medium]
[athena_workgroup_encryption] Ensure that encryption at rest is enabled for Amazon Athena query results stored in Amazon S3 in order to secure data and meet compliance requirements for data-at-rest encryption. - athena [medium]
[athena_workgroup_enforce_configuration] Ensure that workgroup configuration is enforced so it cannot be overridden by client-side settings. - athena [medium]
[autoscaling_find_secrets_ec2_launch_configuration] Find secrets in EC2 Auto Scaling Launch Configuration - autoscaling [critical]
[autoscaling_group_multiple_az] EC2 Auto Scaling Group should use multiple Availability Zones - autoscaling [medium]
[aws_lambda_function_invoke_api_operations_cloudtrail_logging_enabled] Check if Lambda functions invoke API operations are being recorded by CloudTrail. - lambda [low]
[aws_lambda_function_no_secrets_in_code] Find secrets in Lambda functions code. - lambda [critical]
[aws_lambda_function_no_secrets_in_variables] Find secrets in Lambda functions variables. - lambda [critical]
[aws_lambda_function_not_publicly_accessible] Check if Lambda functions have resource-based policy set as Public. - lambda [critical]
[aws_lambda_function_url_cors_policy] Check Lambda Function URL CORS configuration. - lambda [medium]
[aws_lambda_function_url_public] Check Public Lambda Function URL. - lambda [high]
[aws_lambda_function_using_supported_runtimes] Find obsolete Lambda runtimes. - lambda [medium]
[backup_plans_exist] Ensure that there is at least one AWS Backup plan - backup [low]
[backup_reports_exist] Ensure that there is at least one AWS Backup report plan - backup [low]
[backup_vaults_encrypted] Ensure that AWS Backup vaults are encrypted with AWS KMS - backup [medium]
[backup_vaults_exist] Ensure AWS Backup vaults exist - backup [low]
[cloudformation_stack_outputs_find_secrets] Find secrets in CloudFormation outputs - cloudformation [critical]
[cloudformation_stacks_termination_protection_enabled] Enable termination protection for CloudFormation Stacks - cloudformation [medium]
[cloudfront_distributions_field_level_encryption_enabled] Check if CloudFront distributions have Field Level Encryption enabled. - cloudfront [low]
[cloudfront_distributions_geo_restrictions_enabled] Check if Geo restrictions are enabled in CloudFront distributions. - cloudfront [low]
[cloudfront_distributions_https_enabled] Check if CloudFront distributions are set to HTTPS. - cloudfront [medium]
[cloudfront_distributions_logging_enabled] Check if CloudFront distributions have logging enabled. - cloudfront [medium]
[cloudfront_distributions_using_deprecated_ssl_protocols] Check if CloudFront distributions are using deprecated SSL protocols. - cloudfront [low]
[cloudfront_distributions_using_waf] Check if CloudFront distributions are using WAF - cloudfront [medium]
[cloudtrail_bucket_requires_mfa_delete] Ensure the S3 bucket CloudTrail bucket requires MFA delete - cloudtrail [medium]
[cloudtrail_cloudwatch_logging_enabled] Ensure CloudTrail trails are integrated with CloudWatch Logs - cloudtrail [low]
[cloudtrail_insights_exist] Ensure CloudTrail Insight is enabled - cloudtrail [low]
[cloudtrail_logs_encryption_enabled] Ensure CloudTrail logs are encrypted at rest using KMS CMKs - cloudtrail [medium]
[cloudtrail_logs_file_validation_enabled] Ensure CloudTrail log file validation is enabled - cloudtrail [medium]
[cloudtrail_logs_s3_bucket_access_logging_enabled] Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket - cloudtrail [medium]
[cloudtrail_logs_s3_bucket_is_not_publicly_accessible] Ensure the S3 bucket CloudTrail logs is not publicly accessible - cloudtrail [critical]
```

16. run PROWLER using `prowler aws` command


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 <https://docs.prowler.cloud/en/latest/troubleshooting/>

run this command `ulimit -n 4096`

18. to run html output run `Xdg-open file_location` command



Report Information			AWS Assessment Summary			AWS Credentials			Assessment Overview		
Version: 3.11.3			AWS Account: 518981969379			User Id: AIDAXRVN4MXR35L3ZDKRR			Total Findings: 3318		
Parameters used: aws			AWS-CLI Profile: default			Caller Identity ARN: arn:aws:iam::518981969379:user/prowler			Passed: 2103		
Date: 2023-11-24T11:28:17.536613			Audited Regions: All Regions						Failed: 1215		
									Total Resources: 610		

Filters Show 100 entries

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	medium	ecr	us-west-2	ecr_repositories_scan_images_on_push_enabled	[DEPRECATED] Check if ECR image scan on push is enabled	node-2		ECR repository node-2 has scan on push disabled.	Amazon ECR image scanning help read more...	Enable ECR image scanning and read more...	•AWS-Well-Architected-Framework read more...
FAIL	medium	ecr	us-west-2	ecr_repositories_scan_images_on_push_enabled	[DEPRECATED] Check if ECR image scan on push is enabled	node-demo		ECR repository node-demo has scan on push disabled.	Amazon ECR image scanning help read more...	Enable ECR image scanning and read more...	•AWS-Well-Architected-Framework read more...
PASS	high	iam	ap-south-1	iam_avoid_root_usage	Avoid the use of the root accounts	<root_account>		Root user in the account wasn't accessed in the last 1 days.	The root account has unrestricted read more...	Follow the remediation instruct read more...	•CIS-1.5.1.7 •CIS-1.4.1.7 read more...
PASS	medium	ec2	ap-south-1	ec2_instance_older_than_specific_days	Check EC2 Instances older than specific days.	i-09f4322f7adb8a13e	*Name=RayNetwork	EC2 Instance i-09f4322f7adb8a13e is not running.	Having old instances within yo read more...	Check if software running in t read more...	•CISA: your-systems-1 •NIST read more...
PASS	medium	ec2	ap-south-1	ec2_instance_older_than_specific_days	Check EC2 Instances older than specific days.	i-07885550d4302c8bf		EC2 Instance i-07885550d4302c8bf is not running.	Having old instances within yo read more...	Check if software running in t read more...	•CISA: your-systems-1 •NIST read more...
PASS	medium	ec2	ap-south-1	ec2_instance_older_than_specific_days	Check EC2 Instances older than specific days.	i-04d00a9199564929f	*Name=FaceDetection	EC2 Instance i-04d00a9199564929f is not running.	Having old instances within yo read more...	Check if software running in t read more...	•CISA: your-systems-1 •NIST read more...

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
```