H2HC
Cloud Village

Luiz Machado - H2HC - Cloud Village - 2024

SecBridge

Unificando ferramentas para enumeração

Luiz Machado - H2HC - Cloud Village - 2024

Luiz Machado (@cryptobr) 

Head de Cloud
Lider de comunidade - GYNSec
AWS Community Builder (Sec & Identity)
Entusiasta em Segurança da Informação

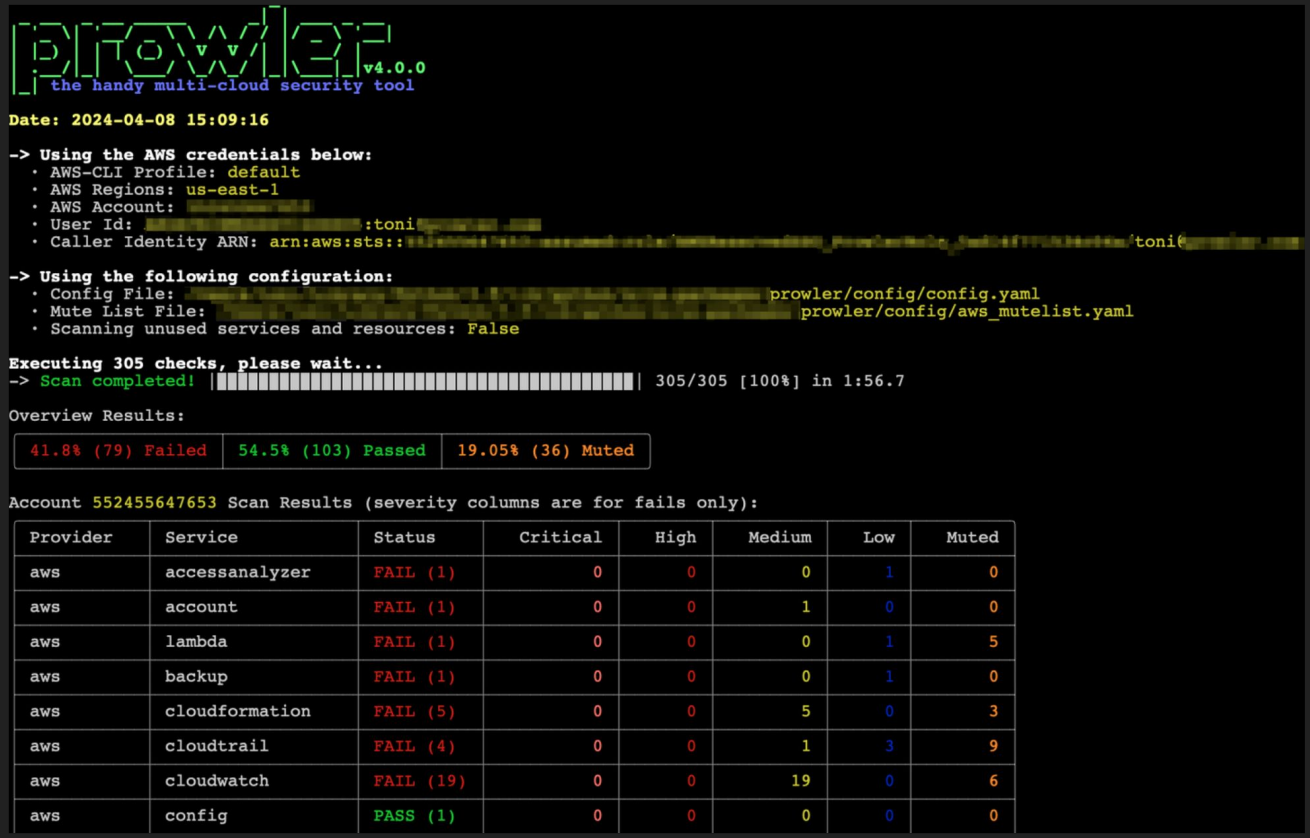
Agenda

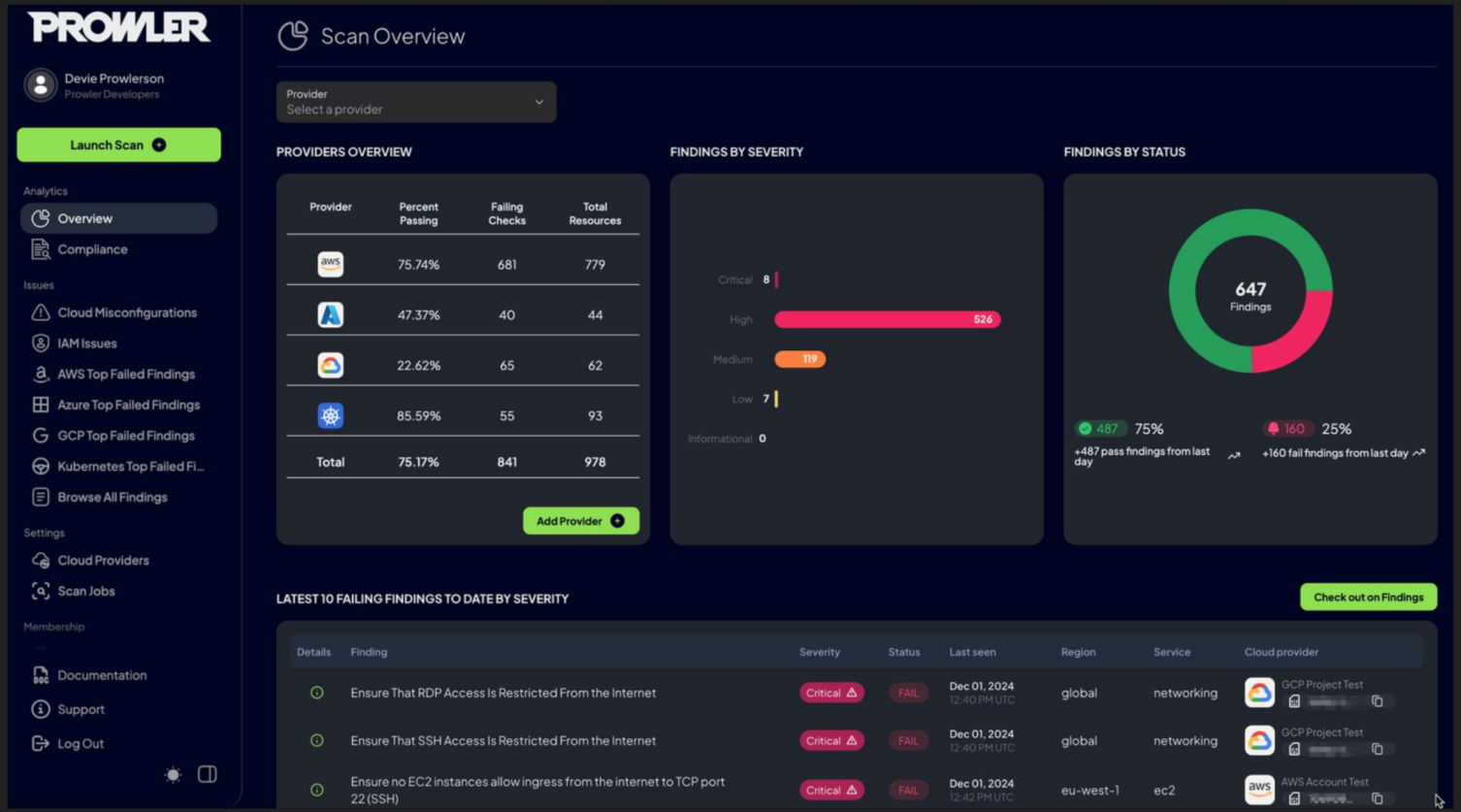
Ferramentas OpenSource
SecBridge
Autenticação na AWS
DEMO (Pawned Labs)

Ferramentas OpenSource

PROWLER

Luiz Machado - H2HC - Cloud Village - 2024


prowler
v4.0.0
the handy multi-cloud security tool
Date: 2024-04-08 15:09:16
-> Using the AWS credentials below:
· AWS-CLI Profile: default
· AWS Regions: us-east-1
· AWS Account:
· User Id: :toni
· Caller Identity ARN: arn:aws:sts:: toni
-> Using the following configuration:
· Config File: prowler/config/config.yaml
· Mute List File: prowler/config/aws_mutelist.yaml
· Scanning unused services and resources: False
Executing 305 checks, please wait...
-> Scan completed! | 305/305 [100%] in 1:56.7
Overview Results:
41.8% (79) Failed
54.5% (103) Passed
19.05% (36) Muted
Account 552455647653 Scan Results (severity columns are for fails only):
Provider Service Status Critical High Medium Low Muted
aws accessanalyzer FAIL (1) 0 0 0 1 0
aws account FAIL (1) 0 0 1 0 0
aws lambda FAIL (1) 0 0 0 1 5
aws backup FAIL (1) 0 0 0 1 0
aws cloudformation FAIL (5) 0 0 5 0 3
aws cloudtrail FAIL (4) 0 0 1 3 9
aws cloudwatch FAIL (19) 0 0 19 0 6
aws config PASS (1) 0 0 0 0 0


PROWLER
Devie Prowlerson
Prowler Developers
Launch Scan
Analytics
Overview
Compliance
Issues
Cloud Misconfigurations
IAM Issues
AWS Top Failed Findings
Azure Top Failed Findings
GCP Top Failed Findings
Kubernetes Top Failed Fi...
Browse All Findings
Settings
Cloud Providers
Scan Jobs
Membership
Documentation
Support
Log Out
Scan Overview
Provider
Select a provider
PROVIDERS OVERVIEW
Provider
Percent Passing
Failing Checks
Total Resources
75.74% 681 779
47.37% 40 44
22.62% 65 62
85.59% 55 93
Total 75.17% 841 978
Add Provider
FINDINGS BY SEVERITY
Critical 8
High 526
Medium 119
Low 7
Informational 0
FINDINGS BY STATUS
647
Findings
487 75%
+487 pass findings from last day
160 25%
+160 fail findings from last day
LATEST 10 FAILING FINDINGS TO DATE BY SEVERITY
Check out on Findings
Details
Finding
Severity
Status
Last seen
Region
Service
Cloud provider
Ensure That RDP Access Is Restricted From the Internet
Critical
FAIL
Dec 01, 2024
12:40 PM UTC
global
networking
GCP Project Test
Ensure That SSH Access Is Restricted From the Internet
Critical
FAIL
Dec 01, 2024
12:40 PM UTC
global
networking
GCP Project Test
Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)
Critical
FAIL
Dec 01, 2024
12:42 PM UTC
eu-west-1
ec2
AWS Account Test

Provider	Checks	Services	Compliance Frameworks	Categories
AWS	561	81 -> `prowler aws --list-services`	30 -> `prowler aws --list-compliance`	9 -> `prowler aws --list-categories`
GCP	77	13 -> `prowler gcp --list-services`	3 -> `prowler gcp --list-compliance`	2 -> `prowler gcp --list-categories`
Azure	139	18 -> `prowler azure --list-services`	4 -> `prowler azure --list-compliance`	2 -> `prowler azure --list-categories`
Kubernetes	83	7 -> `prowler kubernetes --list-services`	1 -> `prowler kubernetes --list-compliance`	7 -> `prowler kubernetes --list-categories`

ScoutSuite
CloudSploit

Luiz Machado - H2HC - Cloud Village - 2024

PACU Framework

PACU Framework

AWS exploitation framework

- `pacu --help` will display the help menu
- `pacu --session <session name>` sets the session to use for commands that require one
- `pacu --list-modules` will list all modules available (does not require session)
- `pacu --pacu-help` will list the pacu help window (does not require session)
- `pacu --module-name <module name>` the name of a module to perform an action on, you can execute or get information on the module
- `pacu --exec` execute the module provided in `--module-name`
- `pacu --module-info` get information on the module provided in `--module-name`
- `pacu --data <service name || all>` query the local SQLAlchemy database to retrieve enumerated information
- `pacu --module-args="<arg1> <value> <arg2> <value>"` supply optional module arguments to the module being executed
- `pacu --set-regions <region1 region2 || all>` set the regions to use in the session, separate regions by a space or enter `all` for all regions
- `pacu --whoami` get information about the current user

PACU Framework

EXFIL

RECON_UNAUTH

EXPLOIT

LATERAL_MOVE

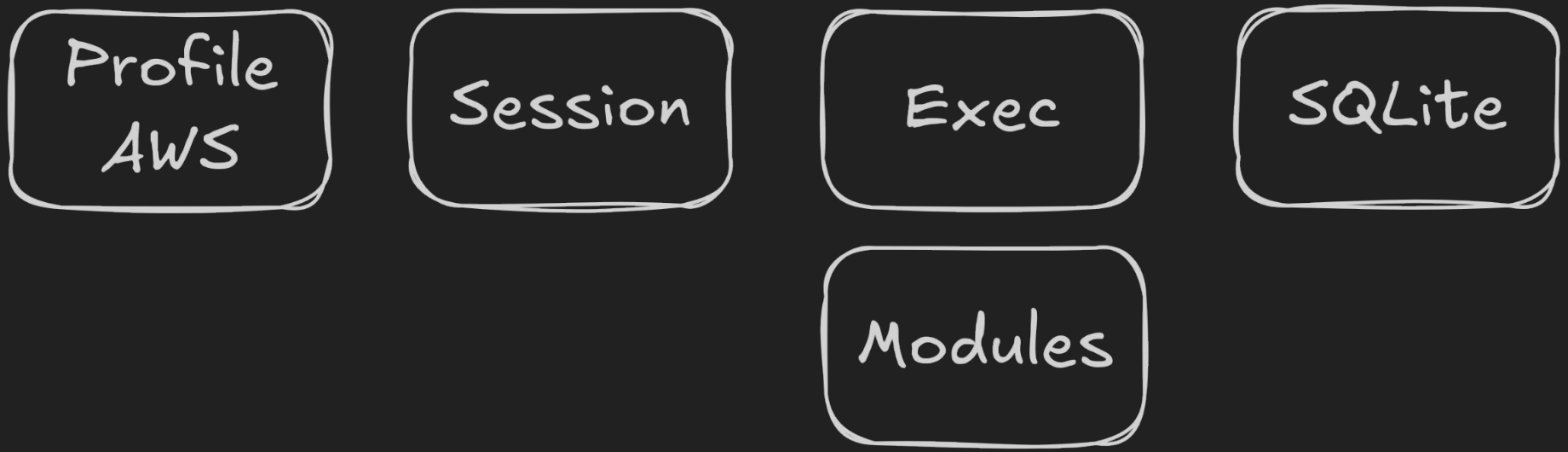
ESCALATE

EVADE

PERSIST

ENUM

PACU Framework



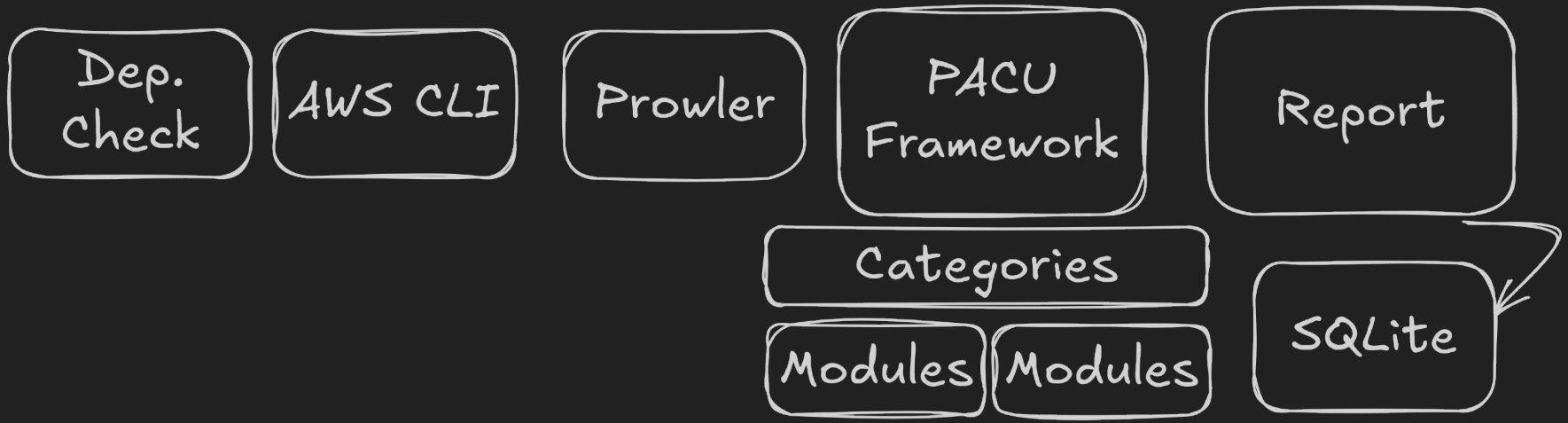
Nimbostratus
AWS_PWN
WeirdAAL (AWS Attack Library)

Luiz Machado - H2HC - Cloud Village - 2024

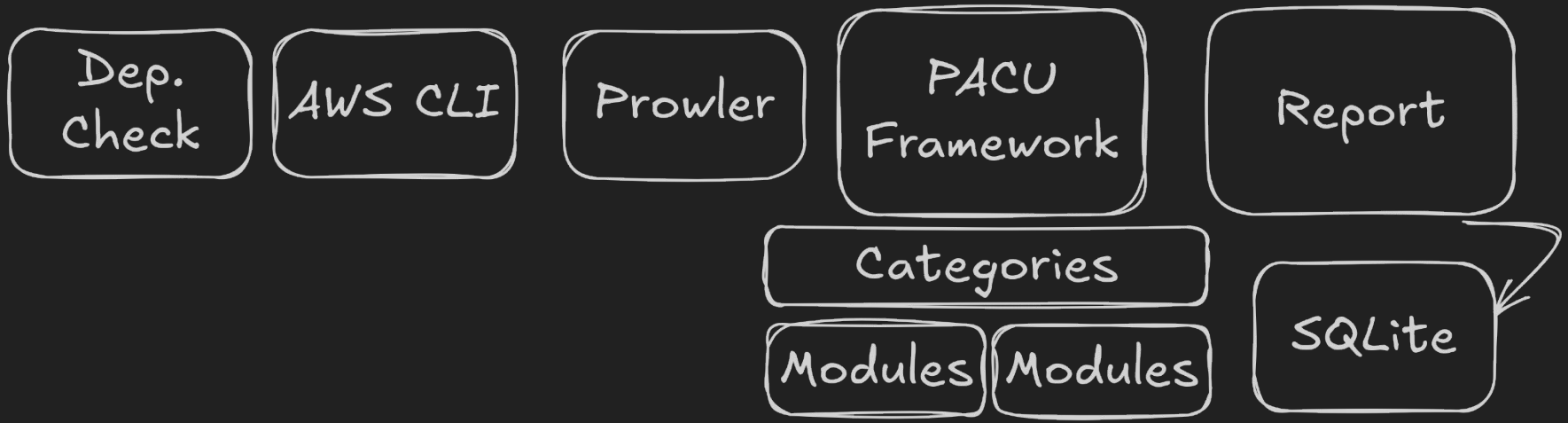
SecBridge

Luiz Machado - H2HC - Cloud Village - 2024

SecBridge


Dep. Check
AWS CLI
Prowler
PACU Framework
Report
Categories
Modules
Modules
SQLite

SecBridge


Dep. Check
AWS CLI
Prowler
PACU Framework
Report
Categories
Modules
Modules
SQLite

Autenticação na AWS

Luiz Machado - H2HC - Cloud Village - 2024

Autenticação na AWS

Tudo é chamada de API
IAM Role
IAM Policy
STS (Security Token Service)

Autenticação na AWS

DEMO - SHOW ME THE CODE

Exemplo básico - Pawned Labs

TEM O GIT ???

TEM O GIT ???

Dúvidas

Obrigado

@luizmachadoaws