AWS Auditing Tools Overview

by tacticaljmp
https://github.com/tacticaljmp

The following findings present an overview of existing tools that can be useful for Amazon Web Services auditing purposes. The non-detailed section delivers basic information about the tool, which is gathered from the tool's own description of advertised features and is, in addition, based on subjective first impression, if the tool was tested.
The detailed comparison section contrasts actual functionality of some of the discussed tools, as produced by evaluation in a small test environment.

Cloudsploit

Language:	Javascript
Installation:	Clone from Github. Requires Node.js
Tested:	Yes
Source:	[1]

Features:
+ Comprehensive scan via tool
+ Offers free web-based online scan with well-formatted output (multiple accesses may be limited)
+ Works with SecurityAudit policy

- No EBS snapshot check
- No output highlighting
- Development and convenience features are priced

Prowler

Language:	Shell script
Installation:	Clone script from github
Tested:	Yes
Source:	[2]

Features:
+ Colourful output
+ Follows well-defined guidelines (see CIS AWS Benchmark [3])
+ Performs extra checks:
  * Do all AdministratorAcess users have MFA enabled?
  * Ensure no EBS snapshots are set as public.
  * Ensure no S3 bucket has public access.
+ Iron Maiden reference

- Requires custom policy (Script provided to generate user with adequate auditing rights)

Zeus

Language:	Shell script
Installation:	Clone script from github
Tested:	Yes, v1.0
Source:	[4]

Features:
+ Colourful output

- Few documentation
- Claims to follow CIS AWS Foundations Benchmark 1.1, but provides less than specified

Scout2

Language: Python
Installation: Via pip
Tested: Yes, v3.0.3

Source: [5]

Features:
+ Generates HMTL report
+ Huge amount of checks
+ Works with SecurityAudit policy

Security Monkey

Language: Python
Installation: Non-trivial, runs on EC2 instance
Tested: No

Source: [6]

Features:
+ Near real-time monitoring
+ Comprehensive management UI

- Runs in the cloud on an EC2 instance
- Non-trivial setup

Nessus Plugin

Language: XML-based audit files
Installation: Nessus required
Tested: No

Source: [7]

Features:
+ Integrated in Nessus
+ Requires read-only access to AWS

- Nessus dependency may be undesirable

Nimbostratus

Language: Python
Installation: Clone from git, then pip install requirements
Tested: No

Source: [8]

Features:
+ Post-exploitation tool
+ Fingerprinting functionality:
    * Dump account credentials

    * Dump permissions for exploited account
    * Dump instance meta-data
    * Create DB snapshot

+ Persistence:
    * Create new user (for future backdoor etc.)
    * SQS Celery queue exploit (execute arbitrary commands)

- No real account settings auditing (offensive tool)
- Credentials and read access already given in general auditing scenario

Repokid

Language: Python
Installation: Clone from git
Tested: No

Source: [9]

Features:
+ Evaluates which of the granted AWS permissions are actually used, so that the granted permissions converge to the minimum required set
+ Integration with Amazon DynamoDB
+ Can schedule evaluation

- Non-trivial setup
- Dependency: Relies on Aardvark [10], which provides a RESTful API for the queries that needs to be setup separately

Detailed Tool Comparison

All tests were performed with SecurityAudit permissions.

🟩	Successfully checked.
🟨	Generates incorrect or buggy output.
🟥	Not checked.
🟦	Unclear if checked.

Due to the huge amount of checks performed, Scout2 is not yet included in the table.

	Prowler	**Zeus**	**Cloudsploit**
IAM			
Users with AdministratorAccess policy have MFA enabled	🟩	🟥	🟥
Avoid use of root account	🟩	🟥	🟩
MFA enabled for all users with console password	🟩	🟩	🟩
Credentials unused for >90 days disabled	🟩	🟩	🟩
Ensure access key rotation <=90 days	🟩	🟩	🟩
Password policy requires at least one uppercase letter	🟩	🟩	🟩
Password policy requires at least on lowercase letter	🟩	🟩	🟩
Password policy requires at least one symbol	🟩	🟩	🟩

Password policy requires at least one number	🟩	🟩	🟩
Password policy requires length >=14	🟩	🟩	🟩
Password policy prevents password reuse	🟩	🟥	🟩
Password policy expires passwords with age >90 days	🟩	🟥	🟩
No root account access key exists	🟩	🟩	🟩
MFA enabled for root account	🟩	🟩	🟩
Hardware MFA enabled for root account	🟩	🟥	🟥
Security questions registered	🟨	🟩	🟥
Policies only attached to groups/roles	🟩	🟨	🟥
Detailed billing enabled	🟨	🟥	🟥
IAM Master and IAM Manager roles active	🟩	🟥	🟥
Maintain current contact details	🟨	🟥	🟥
Security contact information registered	🟨	🟥	🟥
Instance roles used for AWS resource access from instances	🟨	🟥	🟥
Support role to manage incidents with AWS support exists	🟩	🟥	🟥
No access key setup for all users with console password	🟩	🟥	🟥
No policies with full administrative privileges	🟩	🟥	🟥
No empty IAM groups	🟥	🟥	🟩
No IAM certificates expired	🟥	🟥	🟩
IAM SSH keys rotated	🟥	🟥	🟩
Logging			
CloudTrail enabled in all regions	🟩	🟨	🟩
CloudTrail log file validation enabled	🟩	🟨	🟩
CloudTrail log buckets not publicly accessible	🟩	🟨	🟩
Trails integrated with CloudWatch	🟩	🟨	🟩
AWS Config enabled in all regions	🟩	🟥	🟩
S3 bucket access logging enabled on log buckets	🟩	🟨	🟩
CloudTrail logs encrypted	🟩	🟩	🟩
Rotation for customer-created keys	🟩	🟨	🟦
No public S3 CloudFront origin	🟥	🟥	🟩
No CloudFront origin without HTTPS or insecure protocols	🟥	🟥	🟩
Log buckets have MFA delete enabled	🟥	🟥	🟩
Monitoring			
Log metric filter and alarm for unauthorized API calls	🟩	🟥	🟦
Log metric filter and alarm for management console sign-in without MFA	🟩	🟥	🟦
Log metric filter and alarm for root account usage	🟩	🟥	🟦
Log metric filter and alarm for policy changes	🟩	🟥	🟦
Log metric filter and alarm for CloudTrail changes	🟩	🟥	🟦
Log metric filter and alarm for management console authentication failures	🟩	🟥	🟦
Log metric filter and alarm for disabling/deleting customer-created keys	🟩	🟥	🟦

Log metric filter and alarm for S3 bucket policy changes	🟩	🟥	🟦
Log metric filter and alarm for AWS Config changes	🟩	🟥	🟦
Log metric filter and alarm for security group changes	🟩	🟥	🟦
Log metric filter and alarm for NACL changes	🟩	🟥	🟦
Log metric filter and alarm for network gateway changes	🟩	🟥	🟦
Log metric filter and alarm for route table	🟩	🟥	🟦
Log metric filter and alarm for VPC changes	🟩	🟥	🟦
Appropriate subscribers to each SNS topic	🟩	🟥	🟦
Networking			
VPC flow logging enabled in all VPCs	🟩	🟩	🟩
Default VPC security groups restrict all traffic	🟩	🟥	🟩
Routing tables for VPC peering are “least access”	🟩	🟥	🟥
Multiple VPC subnets used	🟥	🟥	🟩
Elastic IP limit not exceeded	🟥	🟥	🟩
VPC Elastic IP limit not exceeded	🟥	🟥	🟩
No excessive amount of security groups	🟥	🟥	🟩
No public open CIFS ports	🟥	🟥	🟩
No public open DNS ports	🟥	🟥	🟩
No public open FTP ports	🟥	🟥	🟩
No public open MySQL ports	🟥	🟥	🟩
No public open NetBIOS ports	🟥	🟥	🟩
No public open PostgreSQL ports	🟥	🟥	🟩
No public open RDP ports	🟩	🟩	🟩
No public open RPC ports	🟥	🟥	🟩
No public open SMBoTCP ports	🟥	🟥	🟩
No public open SMTP ports	🟥	🟥	🟩
No public open Open SQL Server ports	🟥	🟥	🟩
No public open SSH ports	🟩	🟩	🟩
No public open Telnet ports	🟥	🟥	🟩
No public open VNC client ports	🟥	🟥	🟩
No public open VNC server ports	🟥	🟥	🟩
EBS			
No public EBS snapshots	🟩	🟥	🟥
S3			
No public S3 buckets	🟩	🟥	🟩
EC2			
EC2 instance limit not exceeded	🟥	🟥	🟩
Detect EC2 Classic instances	🟥	🟥	🟩
No public EC2 AMI images	🟥	🟥	🟩
AMIs encrypted	🟥	🟥	🟩
Check instance IAM roles	🟥	🟥	🟩
ELB			

No insecure ciphers used	🟥	🟥	🟩
KMS			
KMS key rotation enabled	🟥	🟥	🟩
RDS			
Check RDS automated backups	🟥	🟥	🟩
RDS encryption enabled	🟥	🟥	🟩
No RDS instanced publicly accessible	🟥	🟥	🟩
Check RDS restorable	🟥	🟥	🟩
Route53			
Check domain auto-renew	🟥	🟥	🟩
Check domain expiry	🟥	🟥	🟩
Check domain transfer lock	🟥	🟥	🟩
SES			
Check Email DKIM	🟥	🟥	🟩
SNS			
Check SNS topic policies	🟥	🟥	🟩
Lambda			
Check for old runtimes	🟥	🟥	🟩
Redshift			
Encryption enabled	🟥	🟥	🟩
No Redshift cluster publicly accessible	🟥	🟥	🟩

References

[1] Cloudsploit
https://github.com/cloudsploit/scans

[2] Prowler
https://github.com/Alfresco/prowler

[3] AWS CIS Foundations Benchmark
https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

[4] Zeus
https://github.com/Trietptm-on-Security/Zeus-2

[5] Scout2
https://github.com/nccgroup/Scout2

[6] Security Monkey
https://github.com/Netflix/security_monkey

[7] AWS Audit Nessus Plugin

https://docs.tenable.com/nessus/compliancechecksreference/Content/AmazonWebServices_AWS_ComplianceFileReference.htm

[8] Nimbostratus
https://github.com/andresriancho/nimbostratus

[9] Repokid
https://github.com/Netflix/Repokid

[10] Aardvark
https://github.com/Netflix-Skunkworks/aardvark