ScoutSuite Report

What is ScoutSuite?

ScoutSuite is an open-source security auditing tool, designed for cloud environments such as AWS, Azure, Google Cloud Platform, etc (ScouteSuite, 2024). It allows security teams to check the setup of their cloud resources, and to identify potential security issues and configuration errors.

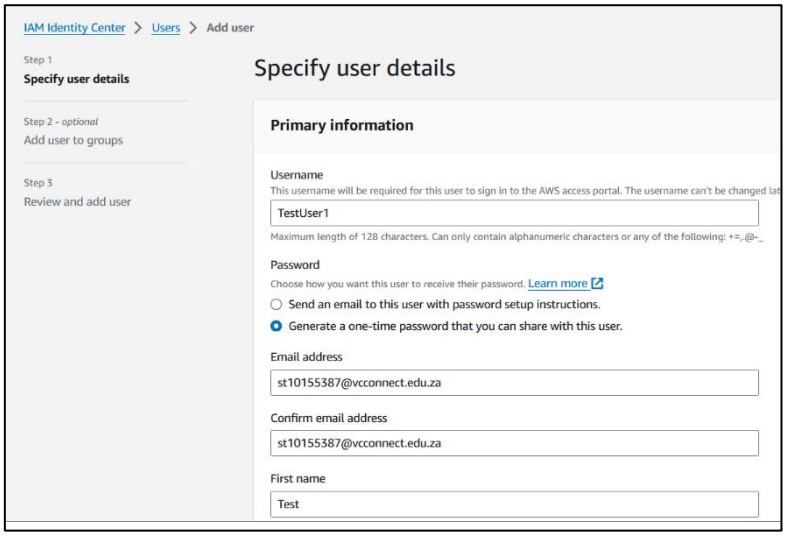
Why ScoutSuite is Useful?

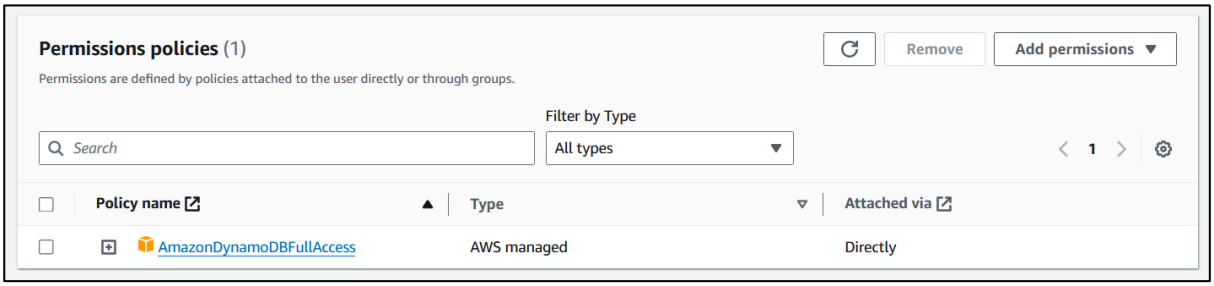
Scout Suite performs well at cloud security auditing because it is agentless, meaning it does not require installation on individual servers, lowering security risks and operational resource use (ScouteSuite, 2024). It creates detailed results in an HTML format, making it simple to see vulnerabilities. The multi-cloud support ensures that it can audit many different environments, including AWS, Azure, and Google Cloud Platform. The capability to detect common cloud misconfigurations, such as excessive permissions or insecure storage, makes it a useful tool for maintaining a strong security standard.

Implementing ScouteSuite:

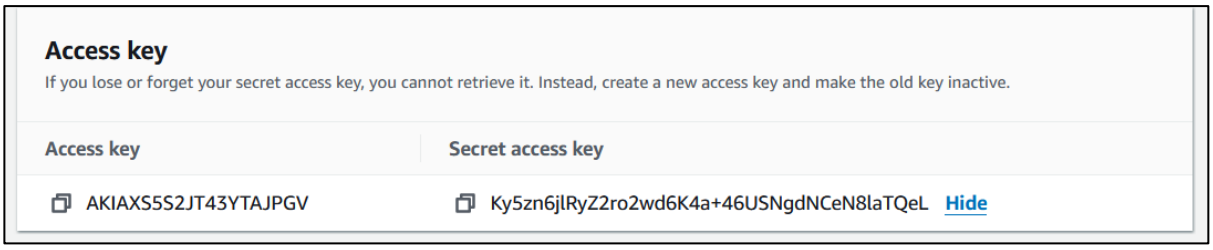
Creating AWS Account and User:

After creating an Amazon account, we created a test user and provided him with permissions as in the video:





Next we created an access key, for ScouteSuite to use for its tests:



Using ScouteSuite in the CLI:

After installing the AWS CLI, we have 2 choices:

Configure the with the created user credentials to test with and use the stored data:

```
PS C:\WINDOWS\system32> aws configure
AWS Access Key ID [None]: AKIA27XCHXURGTCZ4T6Q
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
PS C:\WINDOWS\system32> S
```

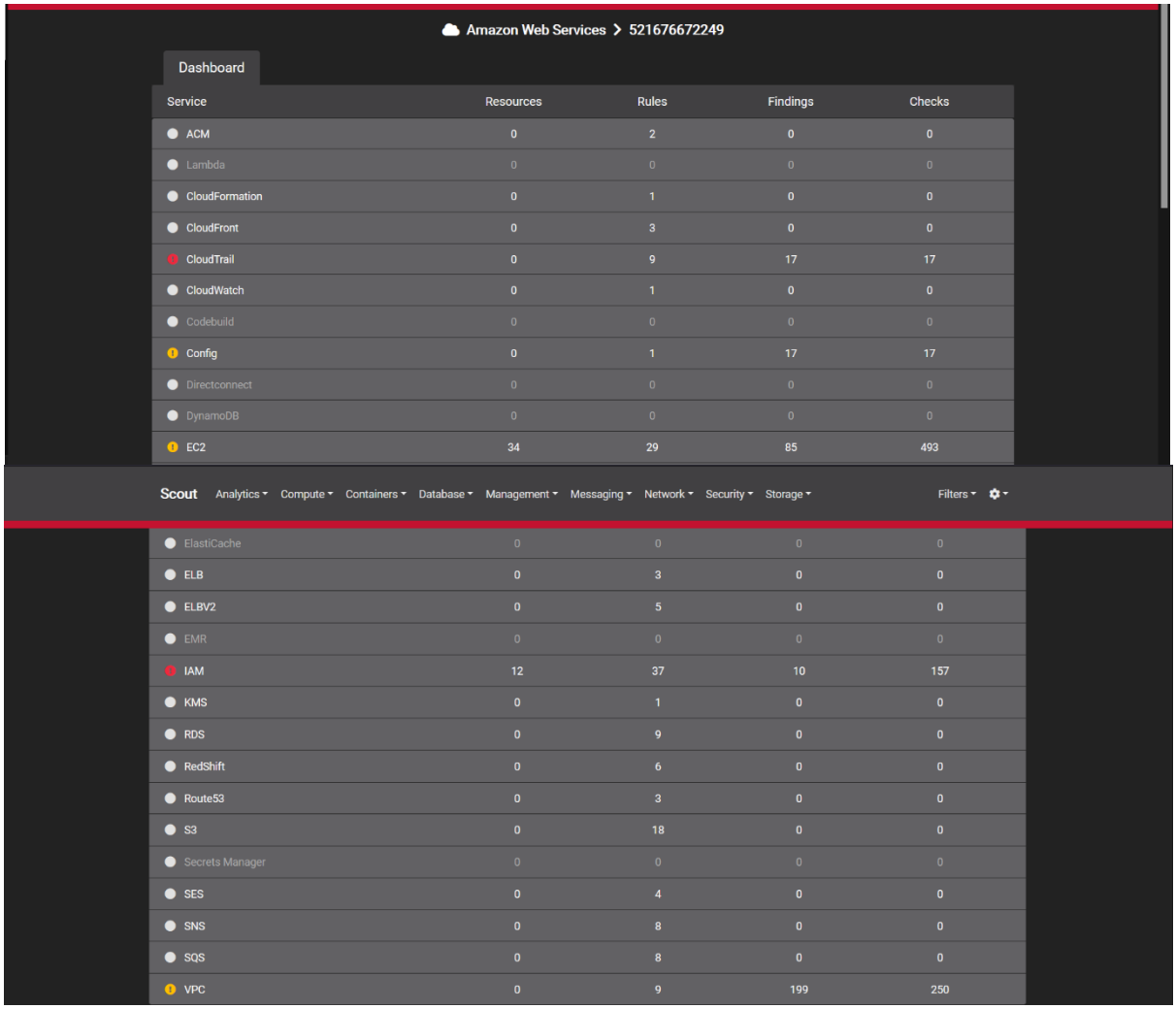
Or we can run a stateless check (entering the access keys each time) to generate the report by updating and using the following code template: (Meuller, 2023)

scout aws
--report-dir ./aws-scan-<DATE>
--report-name aws-report-<DATE>
--result-format json --access-key-id <ACCESS_KEY_ID>
--secret-access-key <SECRET_KEY>

```
PS C:\Users\mayur> scout aws --report-dir ./aws-scan-2024-9-4 --report-name aws-report-2024-9-4 --result-format json
 --access-key-id AKIAXS5S2JT4Y5B4VHPP --secret-access-key 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
2024-09-04 20:11:07 LLamaL0rd21 scout[19448]      Launching Scout
2024-09-04 20:11:07 LLamaL0rd21 scout[19448]      Authenticating to cloud provider
2024-09-04 20:11:14 LLamaL0rd21 scout[19448]      Gathering data from APIs
2024-09-04 20:11:14 LLamaL0rd21 scout[19448]      Fetching resources for the ACM service
2024-09-04 20:11:15 LLamaL0rd21 scout[19448]      Fetching resources for the Lambda service
2024-09-04 20:11:17 LLamaL0rd21 scout[19448]      Fetching resources for the CloudFormation service
2024-09-04 20:11:18 LLamaL0rd21 scout[19448]      Fetching resources for the CloudTrail service
2024-09-04 20:11:19 LLamaL0rd21 scout[19448]      Fetching resources for the CloudWatch service
2024-09-04 20:11:21 LLamaL0rd21 scout[19448]      Fetching resources for the CloudFront service
2024-09-04 20:11:22 LLamaL0rd21 scout[19448]      Fetching resources for the CodeBuild service
2024-09-04 20:11:23 LLamaL0rd21 scout[19448]      Fetching resources for the Config service
2024-09-04 20:11:24 LLamaL0rd21 scout[19448]      Fetching resources for the Direct Connect service
2024-09-04 20:11:26 LLamaL0rd21 scout[19448]      Fetching resources for the DynamoDB service
2024-09-04 20:11:27 LLamaL0rd21 scout[19448]      Fetching resources for the EC2 service
2024-09-04 20:11:28 LLamaL0rd21 scout[19448]      Fetching resources for the EFS service
2024-09-04 20:11:29 LLamaL0rd21 scout[19448]      Fetching resources for the ElastiCache service
2024-09-04 20:11:31 LLamaL0rd21 scout[19448]      Fetching resources for the ELB service
2024-09-04 20:11:32 LLamaL0rd21 scout[19448]      Fetching resources for the ELBv2 service
2024-09-04 20:11:33 LLamaL0rd21 scout[19448]      Fetching resources for the EMR service
2024-09-04 20:11:34 LLamaL0rd21 scout[19448]      Fetching resources for the IAM service
2024-09-04 20:11:34 LLamaL0rd21 scout[19448]      Fetching resources for the KMS service
2024-09-04 20:11:36 LLamaL0rd21 scout[19448]      Fetching resources for the RDS service
2024-09-04 20:11:37 LLamaL0rd21 scout[19448]      Fetching resources for the RedShift service
```

ScouteSuite Report:

This creates a report that looks as below:



ScouteSuite highlighted the following security issues:

CloudTrail not enabled:
CloudTrail allows you to log, monitor, and retain account activity across your AWS infrastructure (Amazon, 2024). This should be turned on for monitoring and logging security.

AWS Config not enabled:
AWS Config monitors and records resource configurations, tracking their changes.
It should be turned on to improve auditing security.

EC2 Yellow Warnings:
The issues found in EC2 category are related to EBS encryption, security group configurations, and unrestricted traffic.
These issues include EBS volumes not being encrypted by default, security groups allowing open ports and unrestricted internal traffic, and the presence of non-empty rules in default security groups. These misconfigurations could lead to data breaches, unauthorized access, and increased attack potential if not attended to. (Amazon, 2024).

IAM Red Warnings:
The IAM warnings indicate critical issues in the Identity and Access Management policies These include extra permissive policies, weak password settings, and a lack of multi factor authentication on user accounts.
These weaknesses can lead to compromised accounts, unauthorized access, and data theft, making it necessary for stricter security policies such as multi factor authentication and least-privilege access. (Amazon, 2024).

VPC Yellow Warnings:
The VPC-related flags are concerns about network access control lists (ACLs) allowing all inbound and outbound traffic and the lack of monitoring in the logs.
These configurations create risks of unauthorized access, data exfiltration, and a lack of visibility into network traffic, potentially leaving the network exposed to attacks. (Amazon, 2024).

References

Amazon, 2024. What Is AWS CloudTrail?. Amazon Documentation [Online]. Available at: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html [Accessed 9 September 2024].

Amazon 2024. What is Amazon EC2?. Amazon Documentation [Online]. Available at: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html [Accessed 9 September 2024].

Amazon, 2024. AWS Identity and Access Management. Amazon Documentation [Online]. Available at: https://aws.amazon.com/iam/ [Accessed 9 September 2024].

Amazon, 2024. How Amazon VPC works. Amazon Documentation [Online]. Available at: https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html [Accessed 9 September 2024].

Meuller, J. 2023. Scanning Your AWS Environment for Vulnerabilities With ScoutSuite. SimpleThread. 19 December 2023. . [Online]. Available at: https://www.simplethread.com/scanning-your-aws-environment-for-vulnerabilities-with-scoutsuite/ [Accessed 9 September 2024].

ScoutSuite. 2024. ScouteSuite Documentation. [Online]. Available at: https://github.com/nccgroup/ScoutSuite [Accessed 9 September 2024].