Slide 1

Hi all,

This is Gunasekhar working in CIS DevSecOps Team as Security SME. At present, I'm working on AWS IAM scripting to generate list of users, list of roles and list of access keys.

Today I'm going to demo the access keys scripting and the plan of action to clean up all ineligible access keys in all the AWS accounts.

Slide 2

These are the objectives of this presentation

The main objective of this work is to list out all the access keys and cleaup in all CIS AWS accounts using boto3 scripting.

We have divided work into two phases:

In Phase 1:

We enumerate the access keys using account\_number, creationdate, and LastUsedDate.

From the list, first we extract Inactive and NeverUsed keys and then we will disable them.

Then we check LastUsedDate, to check whether the key was used in last 6 months, if it was not used then disable the key.

In Phase 2:

We consider the key age, if the key age is more than 365 days then we will rotate the key.

Finally, we will see the Q&A

Slide 3

This is the Workflow

1. Check the access keys in each account

2. Check the status of each access key, if it active then we check the LastUsedDate or else Inactive keys will be disabled.

3. If LastUsedDate is not available in access key, which states that key was never used since after its creation. So, we simply disable the key.

4. If LastUsedDate is available, then we check whether the key was used in last 6 months. If it's not used for a period of 6 months, disable the key.

This is the end of the Phase 1:

In Phase 2:

1. We check the access key age, if age is more than 365 days, then we rotate the key.

Slide 4

This is the access key script terminal/console output. and script will generate the report which consists of all the access keys.

Slide 5

This is report, where we can find the username, accesskeyID, CreationDate, Key Age, Not used period, Status, Account number and Account Name. By using Status, LastUsedDate and key age, we will disable the Inactive, NeverUsed and the key not for more than 6 months will be disabled.

Slide 6

Before this we didn't have automation instead, we did all the operation manually. It takes so much manpower and time.

To overcome this, we developed a script that can Automate and get the all access keys list at once and the Visibility will be high

We can eliminate the unused and never used access keys

Based on the key age, we will perform the rotation on access key.

With this we can understand the access key lifecycle in a better way.

Slide 7

Actions to be performed on each Phase:

Phase 1:

In Phase 1, We consider the Status and Lastuseddate and then disable the ineligible access keys

Slide 8

Phase 2:

In Phase 2, we check the access key age, if it is more than 365 days, then we will rotate the key.

Phase 3:

In Phase 3, we enumerate all AWS roles from all the CIS AWS accounts and review them. It's in progress.

Slide 9:

Any questions? I'm happy to answer!

Slide 10:

Thanks to my team and thank you all.