Sri Lanka Institute of Information Technology

Faculty of Computing

Department of Computer System Network Engineering

IE4040: Information Assurance & Auditing

Mid-Term Individual Assignment – 2020

Name : R.A.J.K.Rupasinghe

Index Number : IT 17059046

Group : CSNE

Submission Date : 08th May 2020

Auditing the security of an AWS cloud account

Introduction

Amazon Web Services is generally secure by default, but can be misconfigured and the initial setup lacks enforcement of some best practices. If you are running your IT infrastructure on Amazon Web Services or any other cloud platform, you need security audits on a periodic basis. While AWS comes with a range of in-built security features, there are a number of cloud security best practices that its users routinely overlook.

It is virtually impossible for companies focused on day-to-day business activities to also keep an eye on all minute moving parts of their cloud-hosted systems and databases. AWS Security Audit that mainly covers:

- AWS Security Groups
- Identity and Access Management (IAM)
- S3 Bucket permissions
- Root account Multi-Factor Authentication (MFA)
- Password Policy
- Amazon RDS Security Group Configurations
- CloudTrail logging
- CloudFront SSL Certificates
- IAM Access Keys
- Elastic Load Balancing (ELB) Security etc..

An example of best practices these tools check for is if MFA is on the root account. An example of potential security issues is if a Security Group is open to 0.0.0.0/0 (ie. it is open to network traffic from anywhere in the world) or an S3 bucket is world readable. In both of these cases there can be legitimate and safe reasons for doing this, so keep in mind that for your environment some of these issues identified could be false positives. These tools are just pointing out potential areas of concern.

There are three ways to gather information about an AWS account:

1. Make a bunch of AWS API calls to understand how an account currently exists.
2. Monitor CloudTrail logs and alert when potentially concerning changes are made.
3. Use AWS Config logs to understand how an account currently exists.

The following open-source tools can be used to do an audit for an aws cloud account.

- AWS Trusted Advisor
- AWS Config
- Scout2
- Prowler
- Security Monkey
- Cloud Custodian

In this article I am using **Scout2** for the audit. Scout2 is a security tool that lets AWS administrators assess their environment's security posture. Using the AWS API, Scout2 gathers configuration data for manual inspection and highlights high-risk areas automatically. Rather than pouring through dozens of pages on the web, Scout2 supplies a clear view of the attack surface automatically.

Installation

We can do the installation via pip:

$ pip install awsscout2

We can do the installation from the source also:

$ git clone https://github.com/nccgroup/Scout2

$ cd Scout2

$ pip install -r requirements.txt

$ python setup.py install

Requirements

Computing resources

Scout2 is a multi-threaded tool that fetches and stores your AWS account's configuration settings in memory during runtime. It is expected that the tool will run with no issues on any modern laptop or equivalent VM

Python

Scout2 is written in Python and supports the following versions:

- 2.7
- 3.3
- 3.4
- 3.5
- 3.6

AWS Credentials

To run Scout2, you will need valid AWS credentials (*e.g* Access Key ID and Secret Access Key). The role, or user account, associated with these credentials requires read-only access for all resources in a number of services, including but not limited to CloudTrail, EC2, IAM, RDS, Redshift, and S3.

The following AWS Managed Policies can be attached to the principal in order to grant necessary permissions:

- ReadOnlyAccess
- SecurityAudit

Usage

After performing a number of AWS API calls, Scout2 will create a local HTML report and open it in the default browser.

Using a computer already configured to use the AWS CLI, boto3, or another AWS SDK, you may use Scout2 using the following command:

$ Scout2

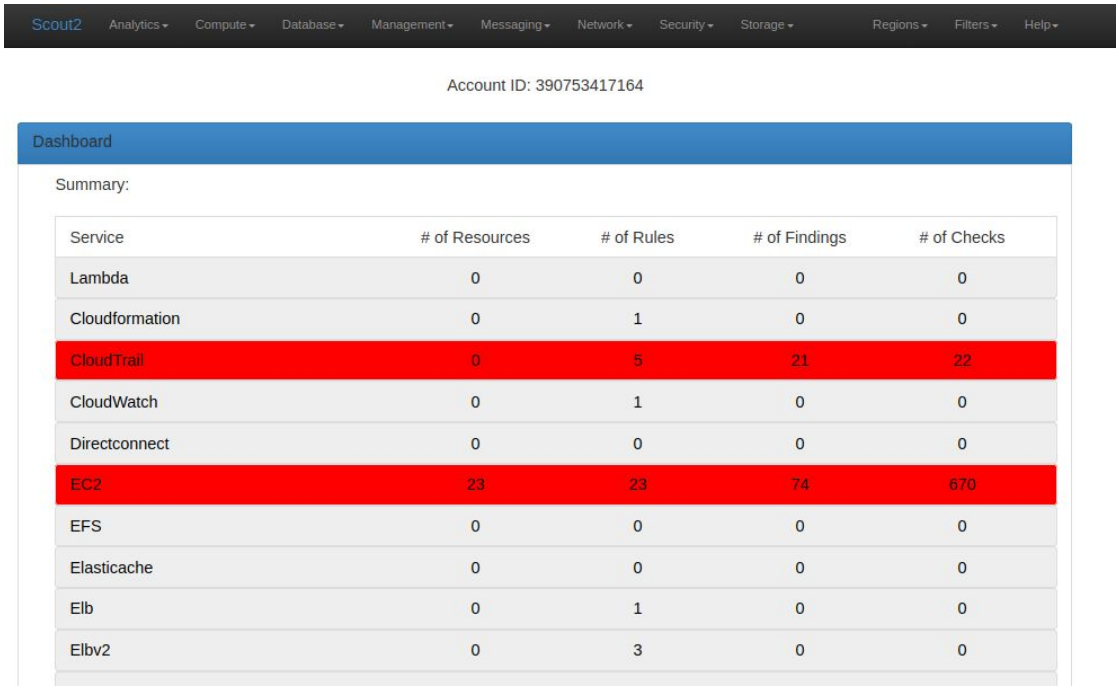
If you have a CSV file containing the API access key ID and secret, you may run Scout2 with the following command:

$ Scout2 --csv-credentials <CREDENTIALS.CSV>

When you run the Scout2 command, it generates a static web directory, allowing you to open the created report.html file in your browser.

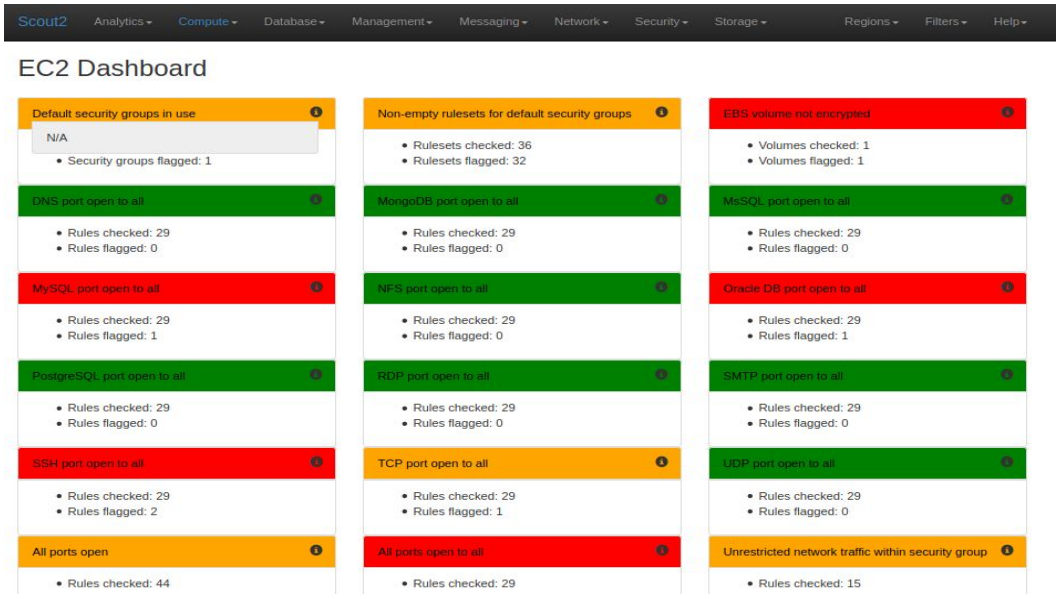
Audit Results

Here is the main screen.

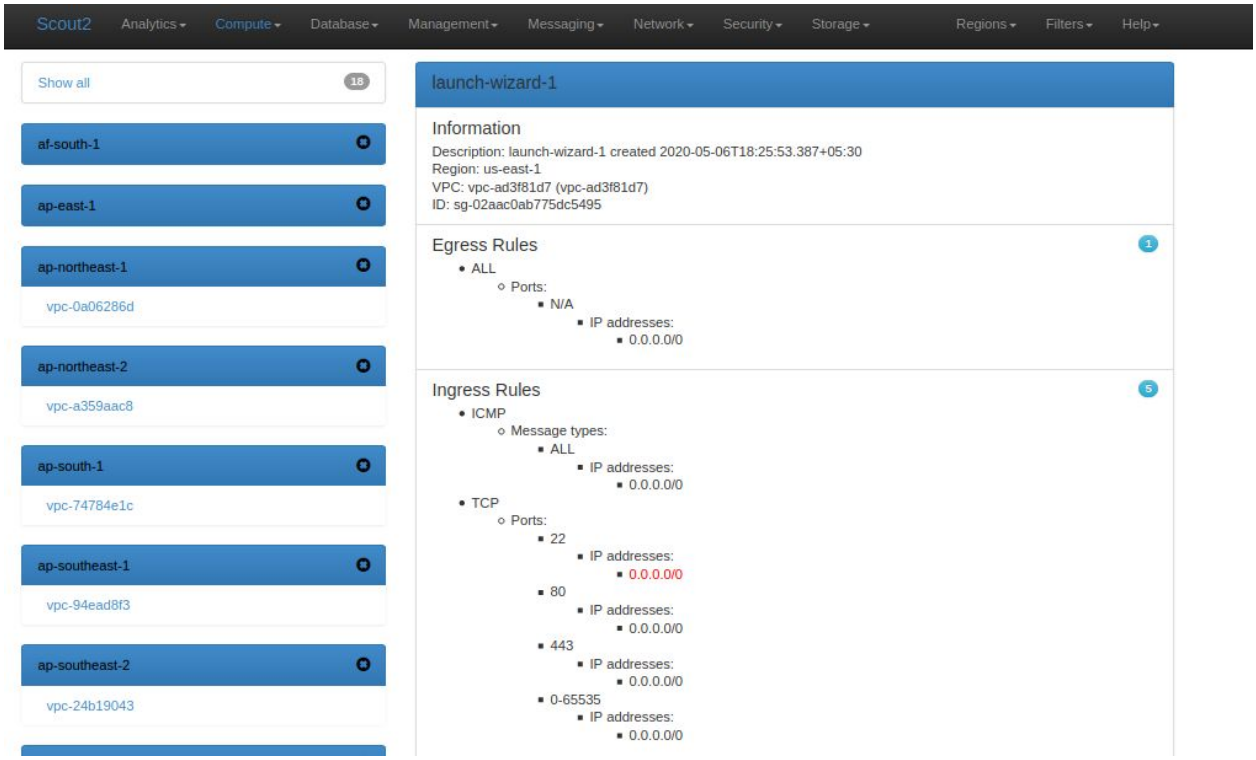


Service	# of Resources	# of Rules	# of Findings	# of Checks
Lambda	0	0	0	0
Cloudformation	0	1	0	0
CloudTrail	0	5	21	22
CloudWatch	0	1	0	0
Directconnect	0	0	0	0
EC2	23	23	74	670
EFS	0	0	0	0
Elasticache	0	0	0	0
Elb	0	1	0	0
Elbv2	0	3	0	0

Clicking over to the EC2 Dashboard gives us a summary of all the issues for that service.



Looking at the “SSH port open to all” in red, we can see all the security groups open to 0.0.0.0/0.



References

1. https://summitroute.com/blog/2017/05/30/free_tools_for_auditing_the_security_of_an_aws_account/
2. https://medium.com/@devopslearning/100-days-of-devops-day-42-audit-your-aws-environment-50237fc3b3
3. https://github.com/nccgroup/Scout2
4. https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html