3. (AWS specific) Python script to find the security group that is open to the external world.  
Hint: If the security group has entry like "0.0.0.0/0", it is open to external world.  
Please provide the solution in such a way that it can be executed via AWS Lambda.

**1) Create an SNS topic and configure subscription.**

Once you create SNS topic, you get an end point that you need to configure in scripts.

**2) Configure IAM User / Role with required policy.**

import sys

import boto

from boto import ec2

from boto import sns

connection=ec2.connect\_to\_region("region-name")

connSNS = boto.sns.connect\_to\_region("region-name")

sg=connection.get\_all\_security\_groups()

listOfInstances=""

messages="Following Instances have port 22 open"

def getTag(instanceId):

    reservations=connection.get\_all\_instances(filters={'instance\_id':instanceId})

    for r in reservations:

        for i in r.instances:

            return i.tags['Name']

try:

    for securityGroup in sg:

        for rule in securityGroup.rules:

            global instanceId;

            if (rule.from\_port=='22' and rule.to\_port == '22') and '0.0.0.0/0' in str(rule.grants):

                for instanceid in securityGroup.instances():

                    instanceId=str(instanceid)

                    listOfInstances += "Instance Name : " + getTag(instanceId.split(':')[1]) + "\t State:" + instanceid.state + "\t SecurityGroup:" +securityGroup.name + "\n"

                    connSNS.publish(topic='SNS-topic-arn-endpoint',message = messages + "\n" + listOfInstances, subject='ProjectName : Server List with Port 22 Open')

except :

    print 'Some Error occurred : '

    print sys.exc\_info()

    connSNS.publish(topic='SNS-topic-arn-endpoint',message = sys.exc\_info(), subject='script ended with error')

You can schedule this script as a cron on a daily basis to get the report over the email

<https://www.tothenew.com/blog/continuing-with-boto-find-security-group-having-port-22-open-for-all/>