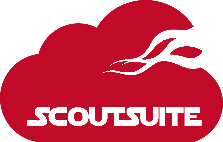
**ScoutSuite** 

## **Description**

## Scout Suite is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments. Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas. Rather than going through dozens of pages on the web consoles, Scout Suite presents a clear view of the attack surface automatically.

The following cloud providers are currently supported/planned:

* Amazon Web Services
* Microsoft Azure
* Google Cloud Platform

### **Compliance**

#### **AWS**

Use of Scout Suite does not require AWS users to complete and submit the AWS Vulnerability / Penetration Testing Request Form. Scout Suite only performs API calls to fetch configuration data and identify security gaps, which is not considered security scanning as it does not impact AWS' network and applications.

### **Requirements**

### **Computing resources**

Scout Suite is a multi-threaded tool that fetches and stores your cloud 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. **Note** that running Scout Suite in a VM with limited computing resources such as an AWS t2.micro instance is not intended and may result in the process being killed.

In our setup we have launched our Kali Linux AMI on t2. medium machine and installed ScoutSuit tool using commands mentioned below in document.

**Python**

Scout Suite is written in Python and supports the following versions:

* 3.5
* 3.6
* 3.7

### **AWS CLI**

Install AWS CLI on your machine using following commands

To install or upgrade the AWS CLI on Amazon Linux (user)

1. Use pip3 install to install the latest version of the AWS CLI. We recommend that if you have Python version 3+ installed that you use pip3. If you run the command from within a Python virtual environment (venv), then you don't need to use the --user option.

$ pip3 install --upgrade --user awscli

1. Add the install location to the beginning of your PATH variable.

$ export PATH=/home/ec2-user/.local/bin:$PATH

Add this command to the end of your profile's start-up script (for example, ~/.bashrc) to persist the change between command line sessions.

1. Verify that you're running new version with aws --version.

$ aws –version

**AWS User**

Create an AWS user with programmatic access with the following AWS Managed Policies.

* ReadOnlyAccess
* SecurityAudit

These policies are used to run Scout in order to grant the necessary permissions.

## **Installation**

Install via pip (we recommend using a virtual environment):

$ virtualenv -p python3 venv

$ source venv/bin/activate

$ pip install scoutsuite

$ scout --help

Or install from source:

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

$ cd ScoutSuite

$ virtualenv -p python3 venv

$ source venv/bin/activate

$ pip install -r requirements.txt

$ python scout.py --help

### **Usage**

1. Login on AWS cli using ScoutSuit user’s access key and secret access key which you have created in previous step.
2. The following command will provide the list of available command line options:

*$ python scout.py –help*

1. List the available regions

*$ aws ec2 describe-regions --query "Regions[].{Name:RegionName}" --output text*

1. Run Scout Suite by using the following command

*$ python scout.py aws --regions “regions”*

Note: Please mention the regions which we have got in step 3

Ex: *python scout.py aws --regions eu-north-1 ap-south-1 eu-west-3 eu-west-2 eu-west-1 ap-northeast-2 ap-northeast-1 sa-east-1 ca-central-1 ap-southeast-1 ap-southeast-2 eu-central-1 us-east-1 us-east-2 us-west-1 us-west-2*

1. After successful completion of scan, report will be automatically opened on browser.
2. Report can be found in scoutsuit-report directory under ScoutSuit Folder.

**Note**

If you restarted the VM in which you have installed the Scout suit tool. You must activate venv using following command before proceeding with the scan

$ source venv/bin/activate

**Issues faced**

Some buckets related to Bentley and Mindsphere were inaccessible due to policies and those were out of our scope and giving access denied error. Hence, we have ignored those errors/buckets after the discussion with Architect.

**Links**

<https://github.com/nccgroup/ScoutSuite>

<https://github.com/nccgroup/ScoutSuite/wiki>