Scout Suite – Multi-Cloud Security Auditing Tool

STAR Method Project Summary

Situation
Cloud environments often grow rapidly, and misconfigurations in IAM, S3, VPC, and other AWS services can lead to serious security risks. Organizations need a way to audit these environments efficiently.

Task
I set up and ran **Scout Suite**, an open-source multi-cloud auditing tool, to scan my AWS environment for misconfigurations, security gaps, and compliance risks. The goal was to generate a security assessment report for my portfolio.

Action

- Installed and configured **Scout Suite** in a controlled AWS account.
- Authenticated using my AWS CLI credentials.

Executed the Scout Suite command:

```
scout aws --report-dir scoutsuite-report
```

-
- Waited while Scout Suite fetched resources across services like IAM, EC2, VPC, S3, KMS, CloudTrail, and more.
- Allowed Scout Suite to run its **pre-processing, rule engine, and post-processing**.

Generated an **HTML report** at:

```
scoutsuite-report/aws-default.html
```

-
- Explored the dashboard findings for IAM, S3, CloudTrail, VPC, and others.

Result

- **IAM**: 44 resources analyzed → 14 findings → 37 rules → 492 checks.
- **S3**: Misconfigured buckets detected, highlighting risks of public access.
- **CloudTrail**: Showed multiple enabled trails (good practice for auditing).
- **VPC**: Identified open security groups that could expose resources.
- Delivered a **visual HTML security report** showing risks by service category.
- Successfully added to my **cloud security portfolio** as proof of hands-on AWS security auditing experience.

Technical Appendix

1. Installation

```
pip install scoutsuite
```

Check installation:

```
scout --help
```

2. Running Scout Suite (AWS Example)

```
scout aws --report-dir scoutsuite-report
```

3. Report Output

- `scoutsuite-report/aws-default.html` → Interactive dashboard.
- `scoutsuite-report/scoutsuite-results/` → Raw JSON & JS data for automation.

4. Key AWS Services Audited

- IAM (users, roles, policies, MFA)
- S3 (bucket access, encryption, public exposure)
- VPC (security groups, NACLs, networking risks)
- EC2 (instance exposure, SSH/RDP access)
- KMS (encryption keys & rotation)
- CloudTrail (logging & auditing configuration)

5. Example Findings

- IAM users without MFA.
- Public S3 buckets.
- Security groups open to `0.0.0.0/0`.
- Missing CloudTrail in some regions.

📊 Why This Project Matters

- Demonstrates **hands-on experience with a real-world security tool**.
- Shows ability to **analyze cloud configurations** against security best practices.
- Provides a **portfolio case study** useful for interviews and GitHub.

Tools Used

Scout Suite (security auditing)

AWS CLI (authentication)

Python venv (virtual
environment)

GitHub (portfolio hosting)