National College of Ireland

Configuration Manual

MSc Industrial Internship
MSc. Cybersecurity

Muskan Mangla
Student ID: X21162697

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Muskan Mangla
Student ID:	X21162697
Programme:	MSc. Cybersecurity **Year:** 2022-2023
Module:	MSc Industrial Internship
Lecturer:	Vikas Sahni
Submission Due Date:	06th January 2023
Project Title:	Securing CI/CD Pipeline: Automating the detection of misconfigurations and integrating security tools
Word Count:	603 **Page Count:** 5

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Muskan

Date: 04th January 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Muskan Mangla
Student ID: X21162697

1 AWSGoat Application Setup

To install and configure the AWSGoat application on AWS Cloud, the following are requirements

Prerequisites

- An AWS Account
- AWS Access and Secret keys with administrative privileges

Installation

The following are the steps for ease of installation and deployment on AWS Cloud.

Step 1: Forked the AWSGoat from INE-labs GitHub repository[1] in the *su-muskan* GitHub Repository
Step 2: Set up the GitHub Action Secrets by adding the AWS access credentials under the settings of the forked repository.

```
AWS_ACCESS_KEY
AWS_SECRET_ACCESS_KEY
```

Step 3: Utilized the in-built terraform code to deploy the application by running the **Terraform Apply** workflow.

After this workflow run, the application URL is displayed in the output and the application was accessed and hosted on the cloud.

2 Integrated security tools in CI/CD Pipeline

- **Semgrep**

Configuration: The following are the steps taken to install and configure Semgrep
Step1: Inside the repository, Go to Security ->Code Scanning -> Add scanning tool-> search Semgrep
Step 2: Then, Sign in to the Semgrep application[2].

[1]https://github.com/ine-labs/AWSGoat
[2]https://semgrep.dev/orgs/-/

Step 3: Configure the displayed secret token on the Semgrep application under the GitHub Secrets in the setting of the repository

```
SEMGREP_DEPLOYMENT_ID
GREP_APP_TOKEN
```

Step 4: Commit the configuration file
Step 5: Push some code to your repository or create a pull request to trigger the Semgrep GitHub Action.
Step 6: Detected misconfiguration alerts

- **tfsec**

Configuration: The following are the steps taken to install and configure tfsec
Step 1: Select Go to Security ->Code Scanning -> Add scanning tool-> search tfsec
Step 2: Configured the GitHub Action workflow inside the su-muskan/AWSGoat repository. that can be found at 'https://github.com/su-muskan/AWSGoat/tree/master/.github/workflows'
Step 3: The name of the configuration file was tfsec.yml
Step 4: Committed the configuration file and modify/ add /delete the code to trigger the tfsec GitHub Action.
Step 5: Detected code security issues

After integrating both of these tools before deployment using GitHub Actions workflows, the misconfigurations were detected and identified. The workflows created for the Continuous Integrity, Continuous Security, and Continuous Deployment are shown in Figure 1.

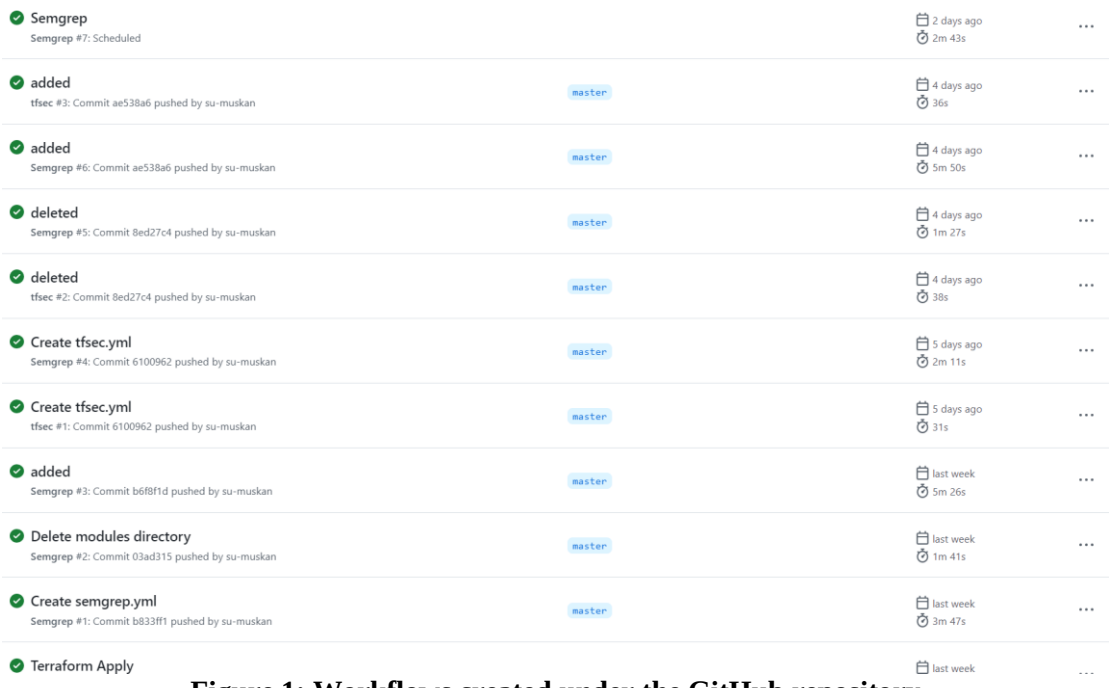

Figure 1: Workflows created under the GitHub repository

Integrating Prowler, Scout Suite, and Security Hub post deployment of the AWSGoat application on AWS EC2 instance.

- **Prowler**

Configuration: Prowler was installed using AWS CLI on Kali Linux machine and configured

Step 1: For Prowler to be installed, AWS CLI was set up using the below command:

```
pip install awscli
```

Step 2: Once the AWS CLI is installed, you need to configure your AWS credentials using the below command:

```
AWS configure
```

Step 3: After configuring the AWS CLI, Prowler was installed by cloning the Prowler repository from GitHub and running the install script:

```
git clone https://github.com/toniblyx/prowler
cd prowler
./install.sh
```

After Prowler was installed, Prowler was executed using the following command:

```
prowler aws --profile custom-profile -f us-east-1
```

Scout Suite for AWS was installed on the Kali Linux machine by cloning the GitHub repository[3]. Scout Suite was installed and executed using the following commands:

```
$ 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
```

In addition, Security Hub and CloudTrail were enabled using the AWS console.

3 Components of Secure CI/CD Pipeline

Table 1: Components, tools, and their versions

Component	Tools	Version
Repository	GitHub	2.35.1
CI/CD	GitHub Action, terraform(hashicorp)	NA, 3.27
Security	Semgrep, tfsec, Security Hub, Scout Suite, Prowler	NA
Dependencies		
Scout Suite	Python	3.10.8

References

Decan, A., Mens, T., Mazrae, P.R. and Golzadeh, M., 2022, October. On the Use of GitHub Actions in Software Development Repositories. In 2022 IEEE International Conference on Software Maintenance and Evolution (ICSME) (pp. 235-245). IEEE.

[3]https://github.com/nccgroup/ScoutSuite

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Muskan Mangla Student number: X21162697

Company: The SecOps Group Month Commencing: September

- Researched various research subjects including Cloud Security, IoT security, andNetwork security.
- Finalized the research project topic on DevSecOps
- Performed application security testing using various security tools and manually.
- Gaining knowledge of common security vulnerabilities and how to identify themin applications.
- Gaining knowledge of common security vulnerabilities and how to identify themin applications.

Employer comments

Muskan was hardworking and completed her given responsibilities

Student Signature: Muskan Date: 29th December 2022

Industry Supervisor Signature:_____Date: 30/12/2022

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Muskan Mangla Student number: X21162697

Company: The SecOps Group Month Commencing: October

- Written the abstract and Introduction of my research topic "Securing DevOps Pipeline: Automating the detection of misconfigurations and integrating securitytools" in the report
- Researched various previous works by multiple researchers using the string "DevSecOps" or "Misconfigurations in Infrastructure as code" on IEEE Journal articles or others.
- Alongside, initiated the work on Vulnmachines platform; technical writing w.r.tvarious latest CVEs, its detection techniques, and payloads.
- Developed vulnerable source code for other cyber security enthusiastic personnel to practice upon source code review part and identify vulnerabilities
- Learned coding, security testing, code review, and modern attacks and their analysis.

Employer comments

Muskan was able to execute and manage the projects. She was able to carry out the research

Student Signature: Muskan Date: 29th December 2022

Industry Supervisor Signature: Date: 30/12/2022

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The InternshipActivity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Muskan Mangla Student number: X21162697

Company: The SecOps Group Month Commencing: November

- Completed the Literature Review on a research topic and provided the ResearchNiche that included the strength and limitations of Related Work(s)
- Executed penetration testing on multiple network hosts and exploitation of vulnerabilities was conducted
- Started with Research Methodology and described the methods to implementthe proposed solution.
- Implemented the DevOps Pipeline using GitHub Actions

Employer comments

Muskan has completed the designing and implementation phase of a research project and has successfully addressed any technical challenges that were encountered during this phase.

Student Signature: Muskan Date: 29th December 2022

Industry Supervisor Signature: Date: 30/12/2022

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The InternshipActivity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Muskan Mangla Student number: X21162697

Company: The SecOps Group Month Commencing: December

- Integrated continuous security to detect major misconfiguration in AWS Infrastructure or services and in every stage of the CI/CD pipeline.
- Reviewed identified security misconfigurations and completed research methodology, and implementation of the research project.
- Evaluated CI/CD pipeline without security and with security.
- Learned how to add security in the DevOps pipeline and various challenges while integrating security tools.
- Formulated the Industrial Internship report and successfully completed

Employer comments

Muskan has improvised a lot on her technical writing asepcts as well. She got opportunities to document processes with manager. Muskan was able to detect misconfigurations in CI/CD pipeline andcompleted her research objective and reporting.

Student Signature: Muskan Date: 29th December 2022

Industry Supervisor Signature: Date: 30/12/2022