Made by Moeez Javed

Made by Moeez Javed

Shuffle SOAR Installation and Usage Manual

Created for SOC Analysts & Cybersecurity Enthusiasts

Introduction

In the modern cybersecurity landscape, the volume and velocity of threats have made manual response inefficient and error-prone. To address this, organizations are adopting SOAR (Security Orchestration, Automation, and Response) platforms. These tools empower Security Operations Centers (SOCs) to automate detection, investigation, and response workflows.

This manual guides you through the installation and usage of **Shuffle**, an open-source SOAR platform designed to automate repetitive tasks, integrate tools via APIs, and streamline security operations. Whether you're a beginner or a professional, this document will walk you step-by-step to build and execute automation flows.

Why is Shuffle Important in Cybersecurity?

✅ **Reduces Manual Workload**: Automates alert handling, threat enrichment, and response actions.

✅ **Increases Response Speed**: Detect and respond to threats in real time.

✅ **Improves Accuracy**: Reduces human error during repetitive security tasks.

✅ **Integrates with Multiple Tools**: Connects with tools like Splunk, VirusTotal, MISP, and more.

✅ **Cost-Effective**: Open-source and free to use.

What is SOAR? (Explained Simply)

SOAR stands for **Security Orchestration, Automation, and Response**.

Security Orchestration: It connects different tools together like a team, so they work as one.

Automation: It lets the system perform actions on its own, like blocking an IP or checking VirusTotal.

Response: It helps you quickly reply to security threats, either automatically or by guiding an analyst.

Made by Moeez Javed

Think of SOAR as a robot assistant for your cybersecurity team.

Installing Shuffle SOAR on Kali Linux

Step-by-Step Instructions:

Step 1
Clone the Repository

git clone https://github.com/frikky/Shuffle
cd Shuffle

Step 2
Start Shuffle Using Docker
docker-compose up -d

Step 3
Install and Configure Docker
sudo apt install docker.io -y
sudo systemctl start docker
sudo systemctl enable docker

Step 4
Check Docker Version:
docker --version

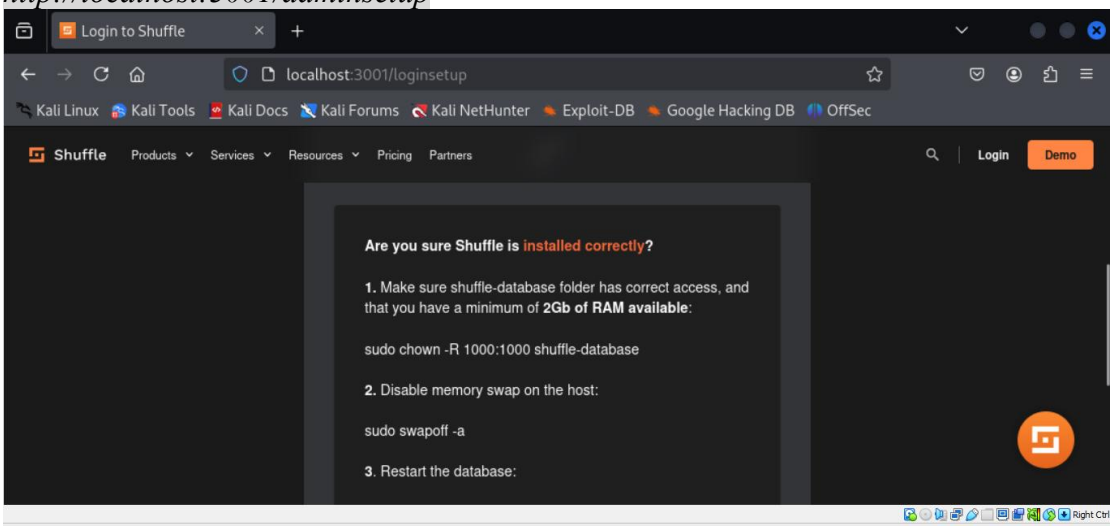
Step 5
Ensure Docker is Running
docker ps

Made by Moeez Javed

```
┌──(kali㉿kali)-[~/Shuffle]
└─$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED          STATUS          PORTS
                                                                                                                NAMES
86fd5b30226c   frikky/shuffle:http_1.4.0            "/bin/sh -c 'python …"   17 minutes ago   Up 17 minutes
                                                                                                                http_1-4-0.1.r4r33hgm9xzwc12g99ouyiovr
f13390c68c94   frikky/shuffle:shuffle-tools_1.2.0   "python app.py --log…"   17 minutes ago   Up 17 minutes
                                                                                                                shuffle-tools_1-2-0.1.j3xwibjmn958r1owmyh40g7nl
6a9a140f7819   frikky/shuffle:shuffle-subflow_1.1.0 "/bin/sh -c 'python …"   17 minutes ago   Up 17 minutes
                                                                                                                shuffle-subflow_1-1-0.1.cwtufvrgew3lsmd9xigwm5m5u
0c0b04f8dfcf   ghcr.io/shuffle/shuffle-worker:latest "./worker"              17 minutes ago   Up 17 minutes
                                                                                                                shuffle-workers.1.3lvf53k36oapcoq7atkistkcz
348949c195da   ghcr.io/shuffle/shuffle-frontend:latest "/entrypoint.sh ngin…"   30 minutes ago   Up 17 minutes   0.0.0.0:3001→80/
tcp, :::3001→80/tcp, 0.0.0.0:3443→443/tcp, :::3443→443/tcp   shuffle-frontend
4f6ab72dbf1b   ghcr.io/shuffle/shuffle-orborus:latest "./orborus"             30 minutes ago   Up 17 minutes
                                                                                                                shuffle-orborus
f1bb71517d26   opensearchproject/opensearch:3.0.0    "./opensearch-docker…"   30 minutes ago   Up 18 minutes   9300/tcp, 9600/tc
p, 9650/tcp, 0.0.0.0:9210→9200/tcp, :::9210→9200/tcp         shuffle-opensearch
16490e4eed16   ghcr.io/shuffle/shuffle-backend:latest "./webapp"              30 minutes ago   Up 17 minutes   0.0.0.0:5001→500
1/tcp, :::5001→5001/tcp                                      shuffle-backend
```

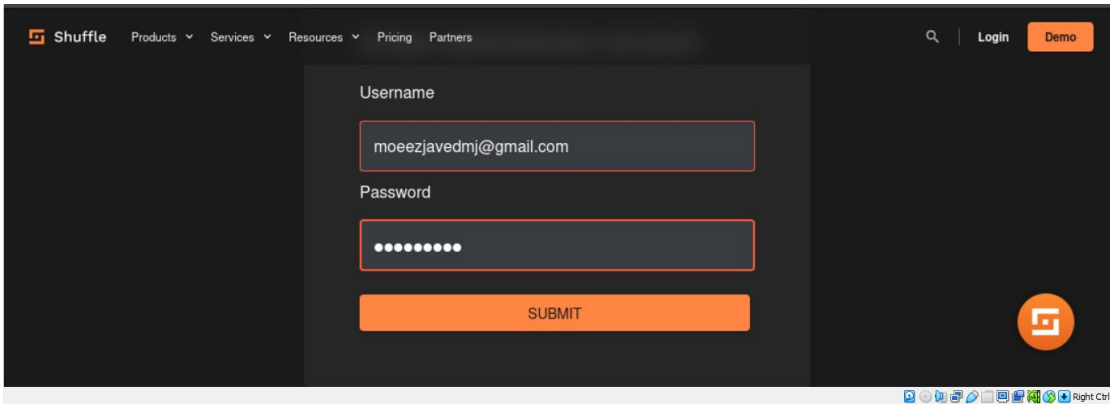
Step 6

Access Shuffle Web Interface
http://localhost:3001/adminsetup



Step 7

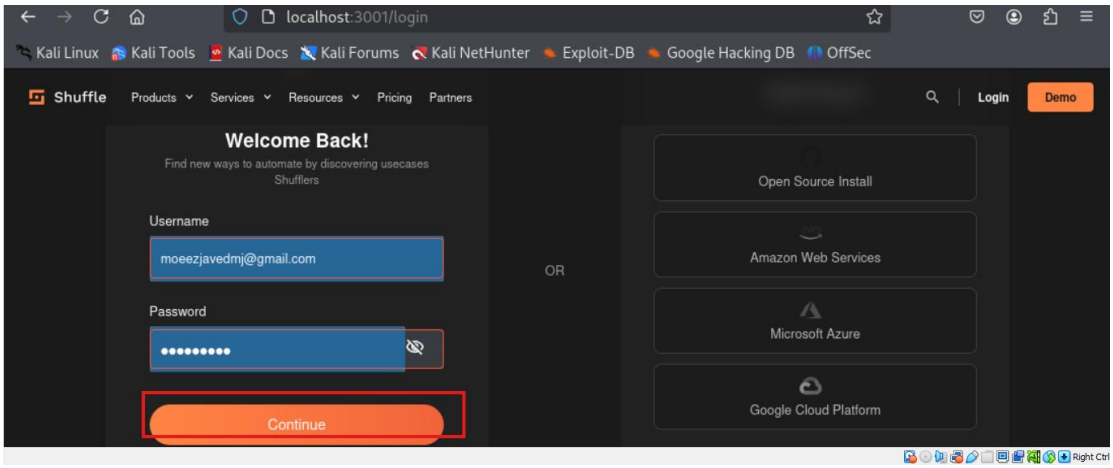
*Press the **Submit** button on the admin setup screen.*



Step 8

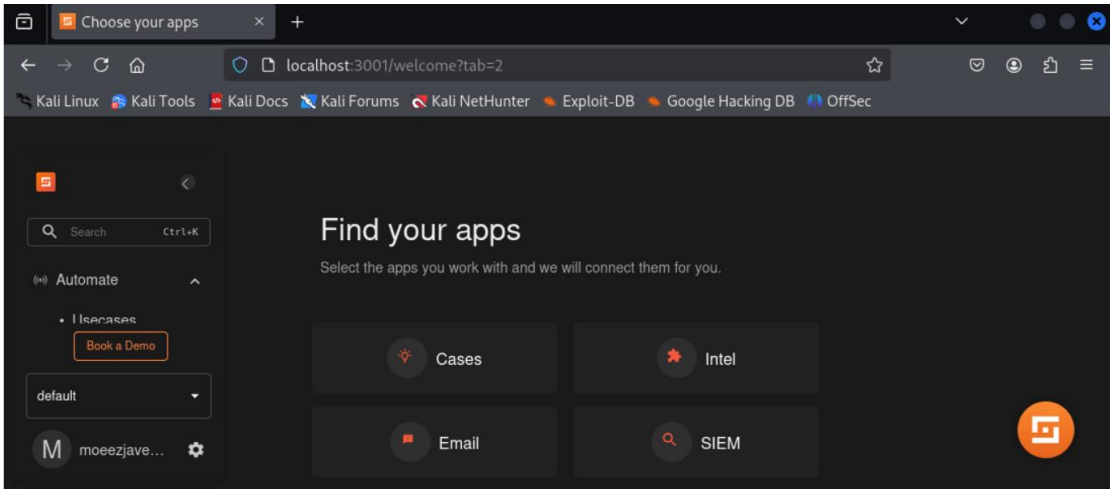
Press the Continue button on the admin setup screen.

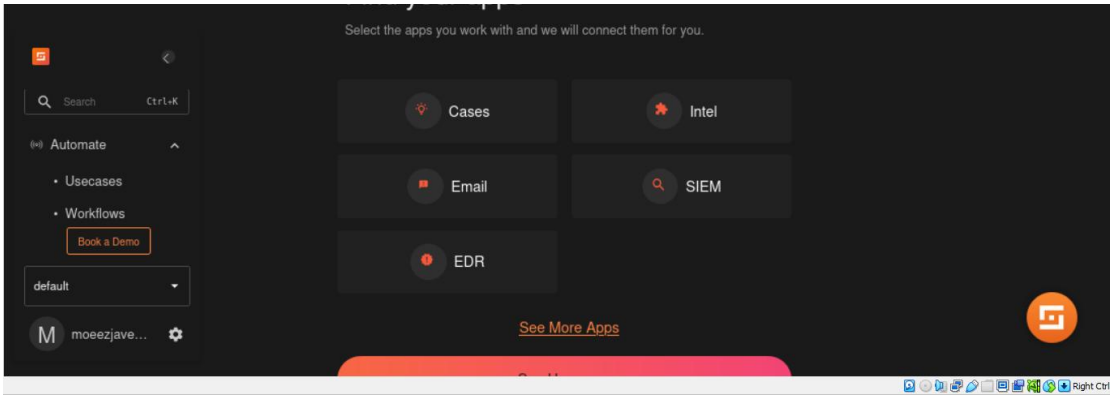
Made by Moeez Javed



Building a Security Automation Workflow

Once installed, let's begin automation for a SOC analyst.



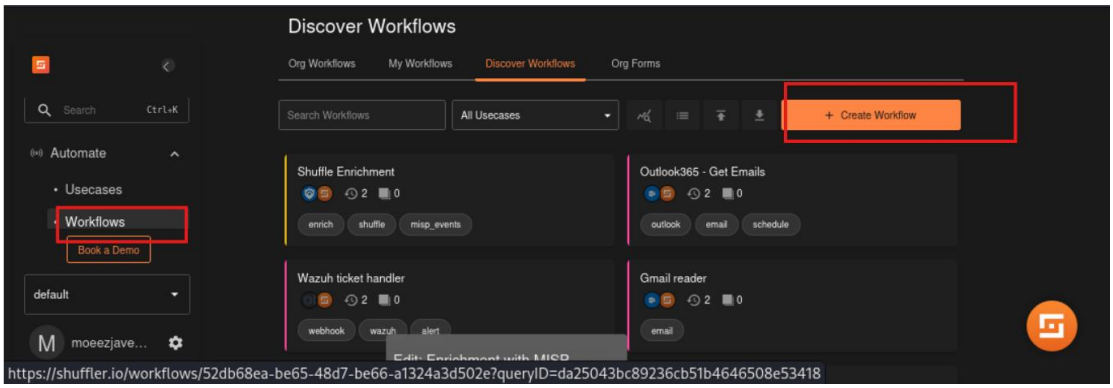


Step-by-Step: Creating a Security Workflow in Shuffle

<u>Step 1</u>

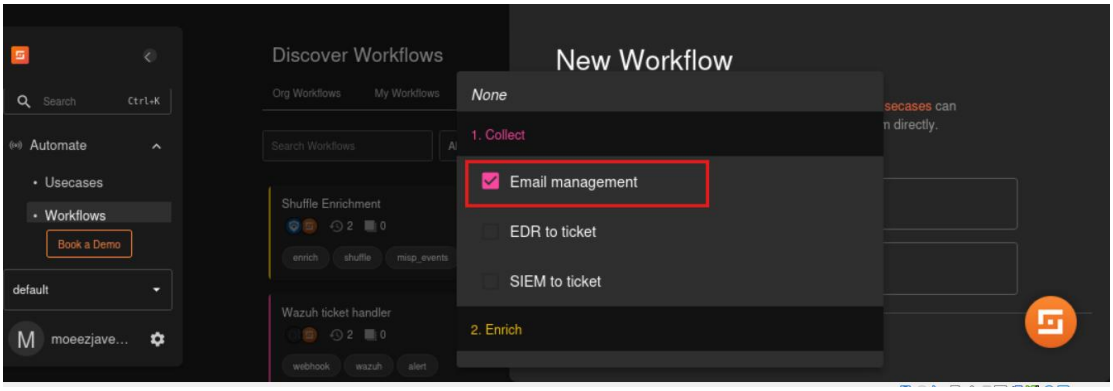
Click "Create New Workflow"

Made by Moeez Javed

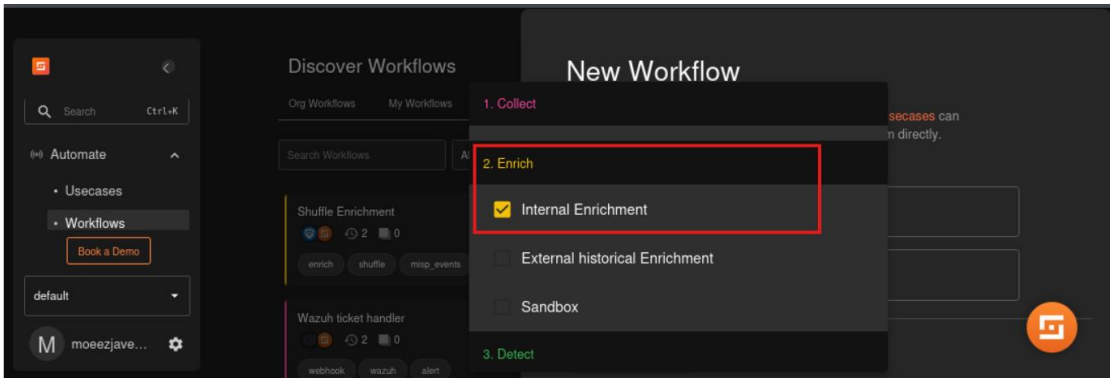


Step 2

Add a Trigger (e.g., Scheduled Task)

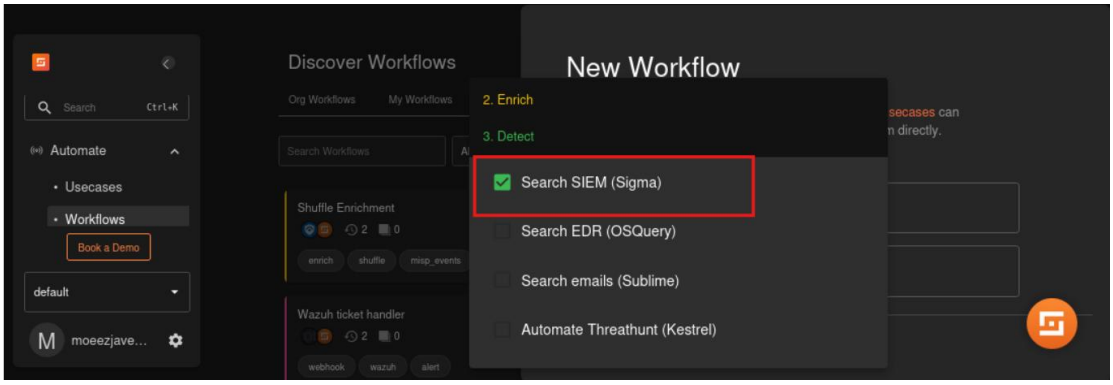


Step 3

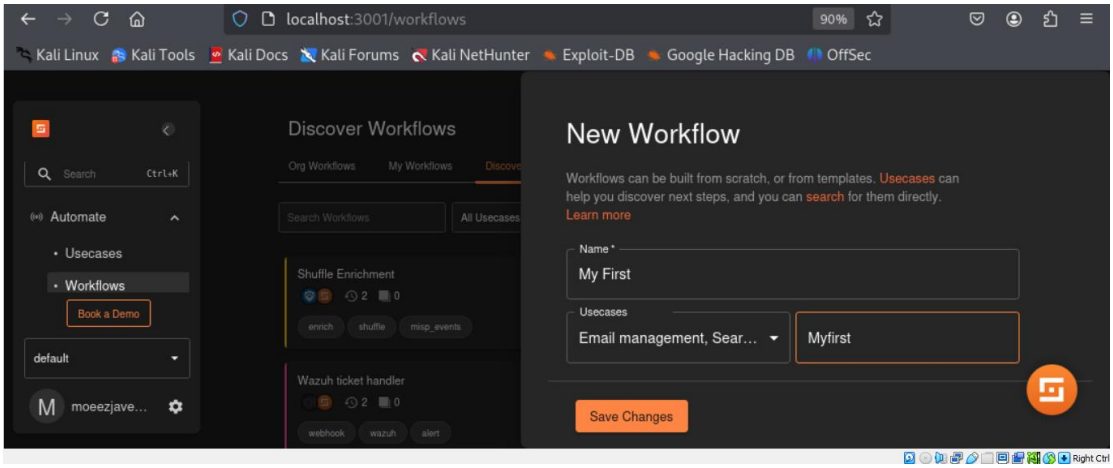


Step 4

Made by Moeez Javed



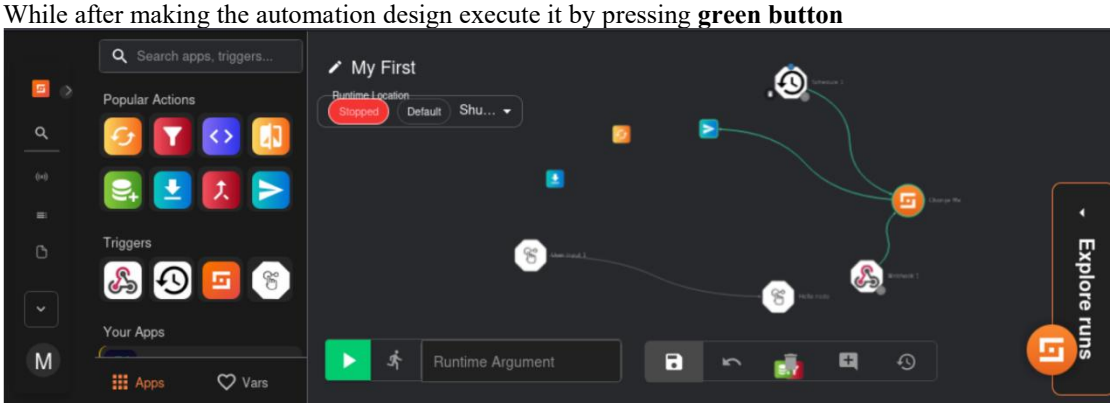
Step 5



Add Apps and Actions

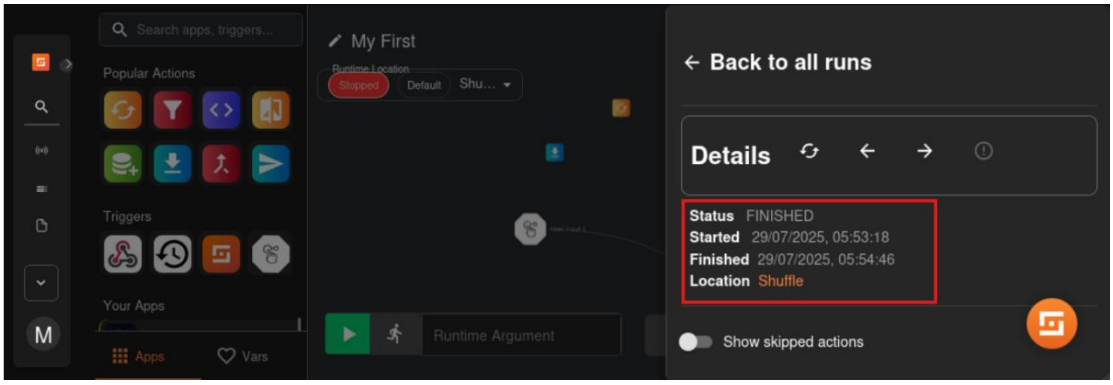
Step 1

While after making the automation design execute it by pressing **green button**

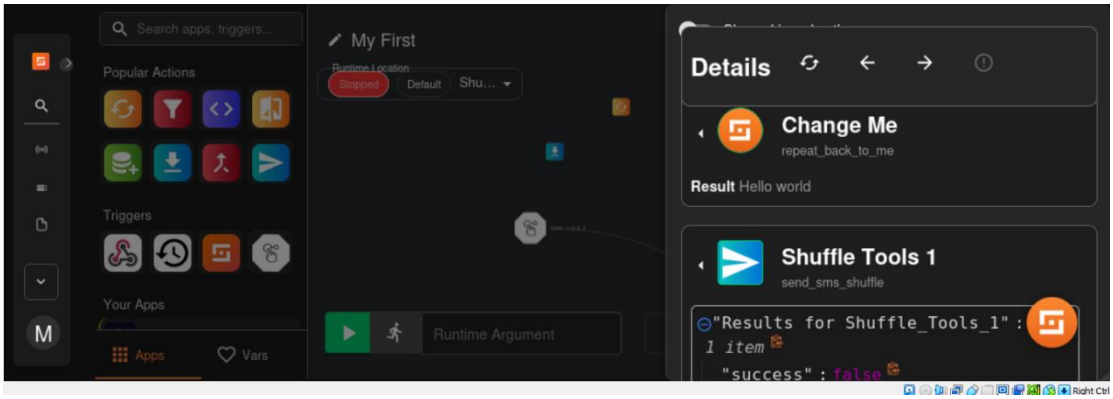


Step 2

Made by Moeez Javed



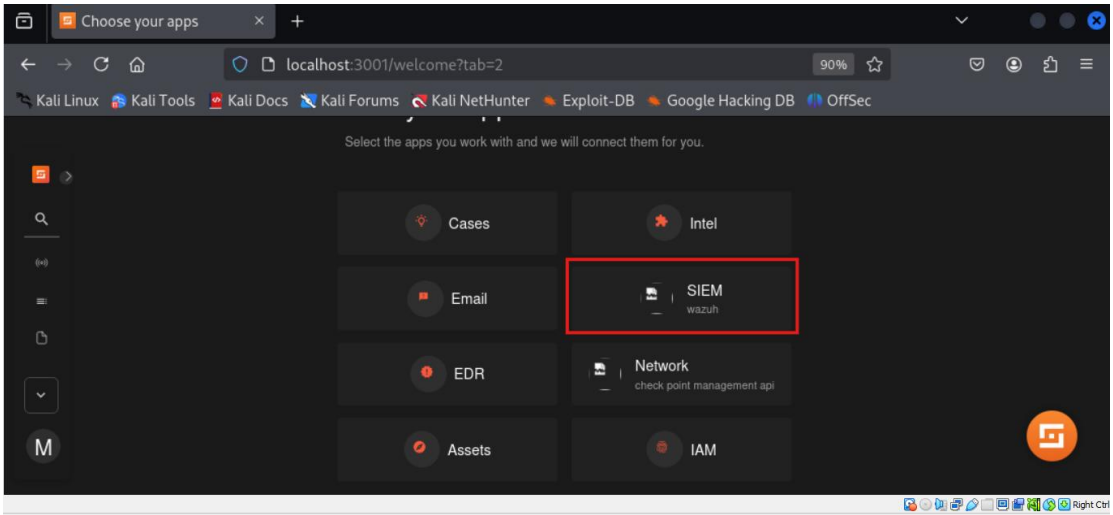
Step 3



Creating and Handling Cases

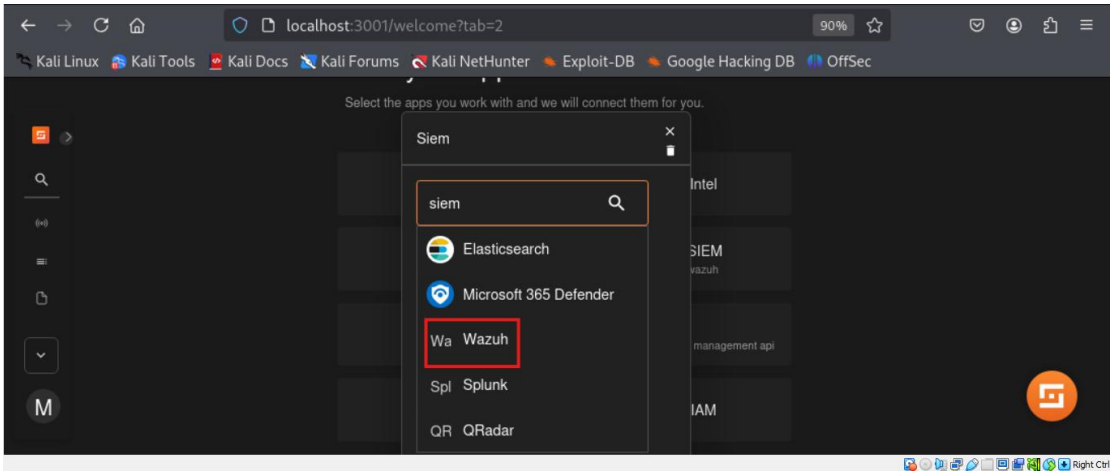
This feature allows you to manually or automatically create incident cases based on workflow output.

Step 1

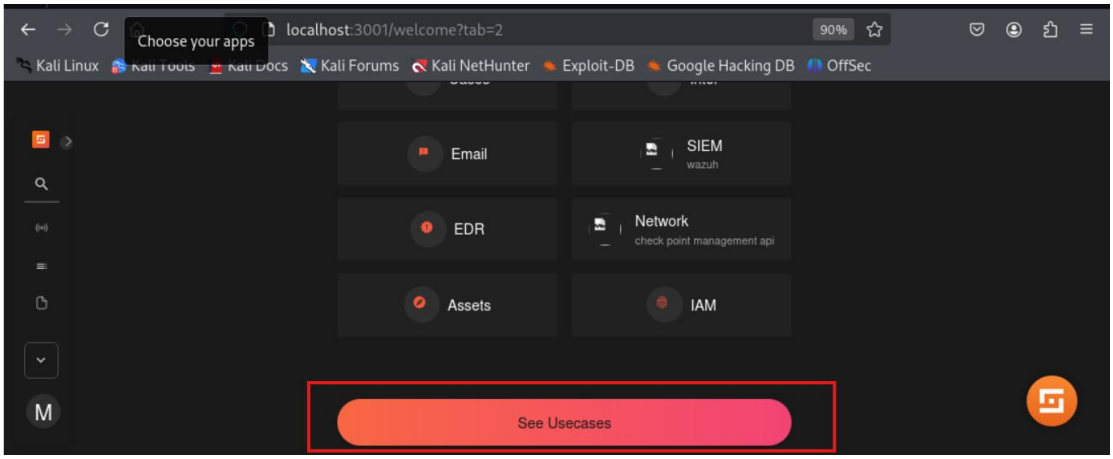


Step 2

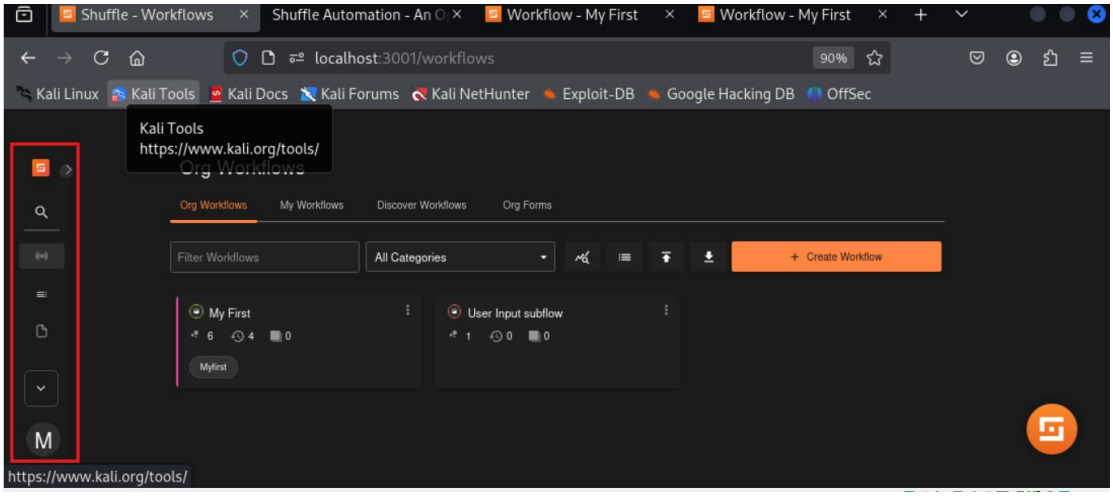
Made by Moeez Javed



Step 3

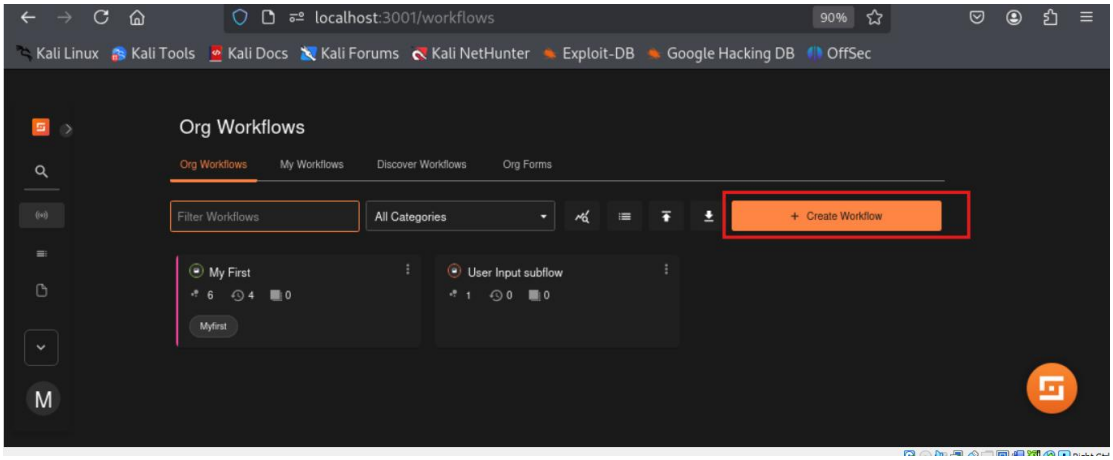


Step 4

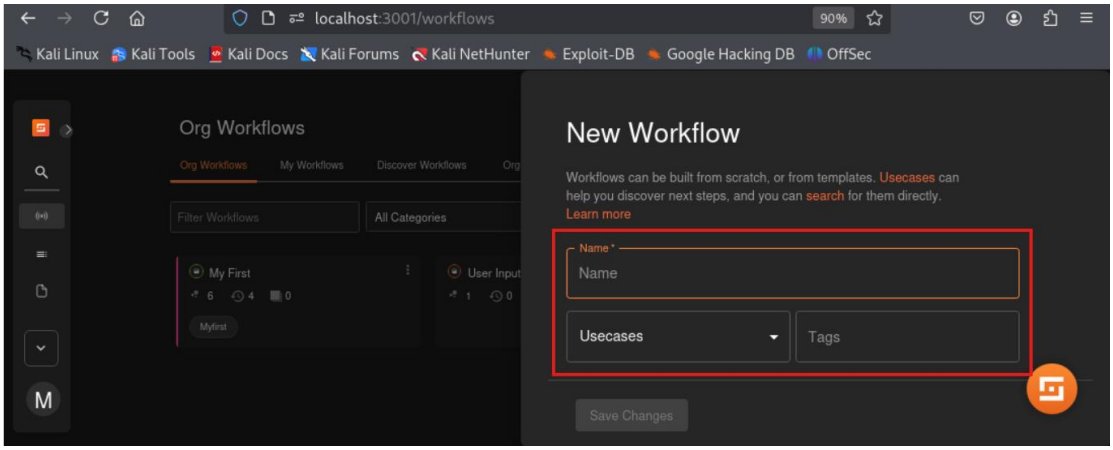


Step 5

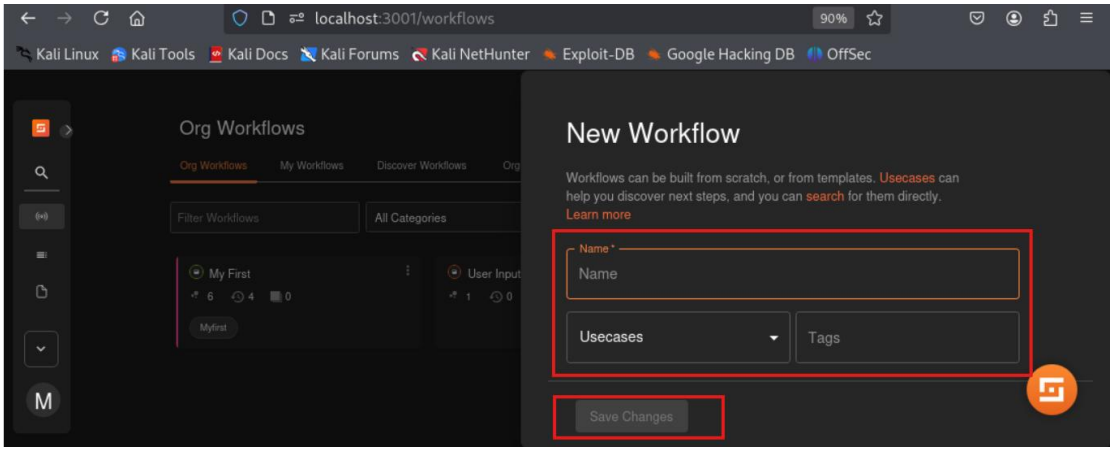
Made by Moeez Javed



Step 6

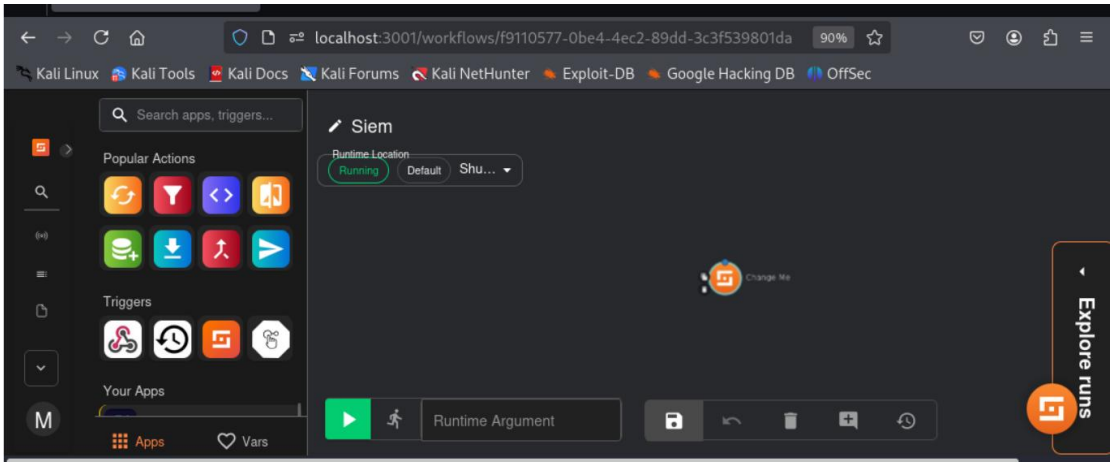


Step 7

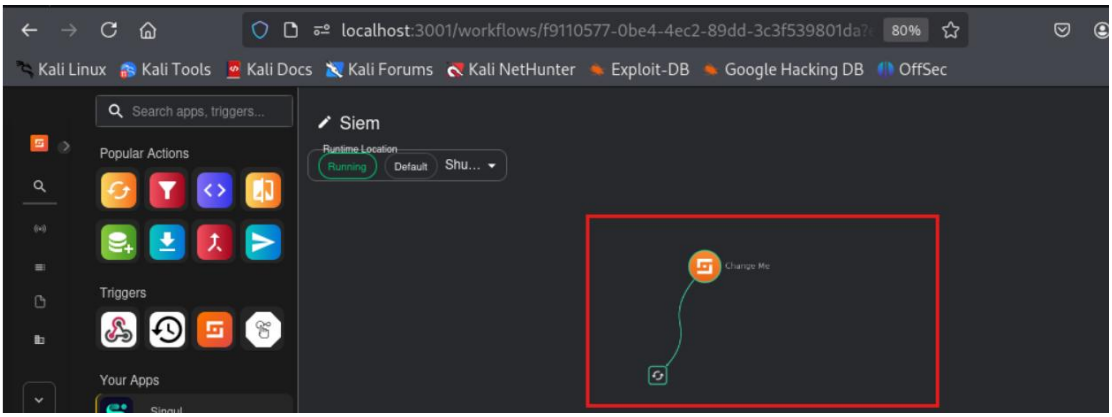


Step 8

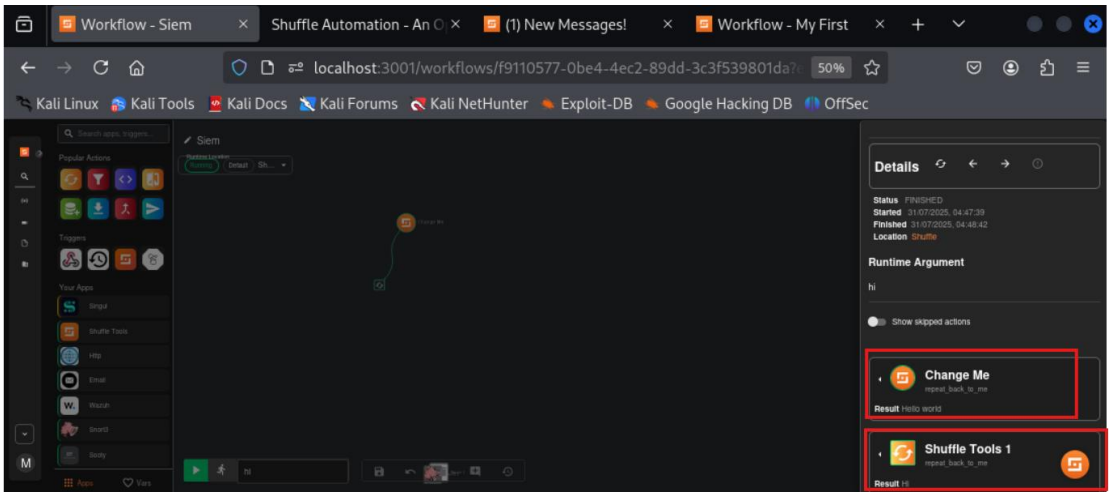
Made by Moeez Javed



Step 9

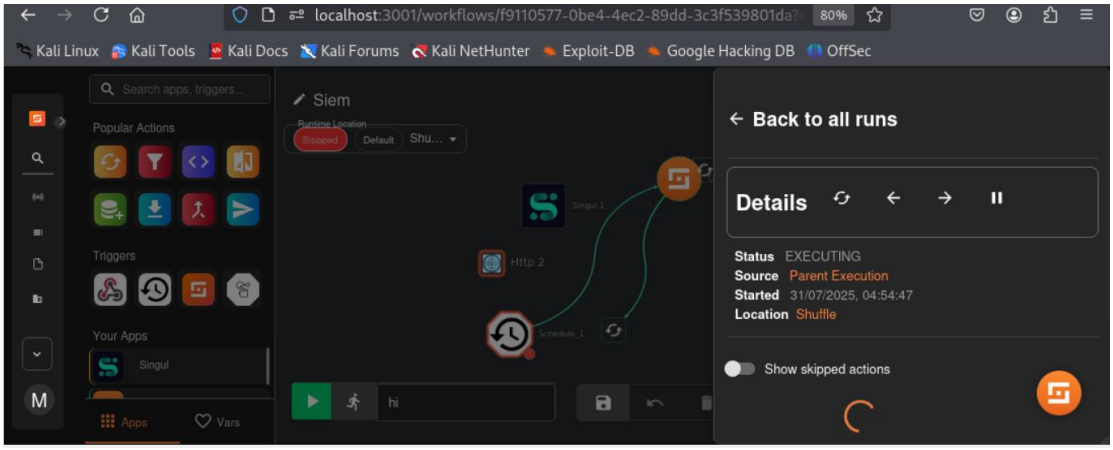


Step 10



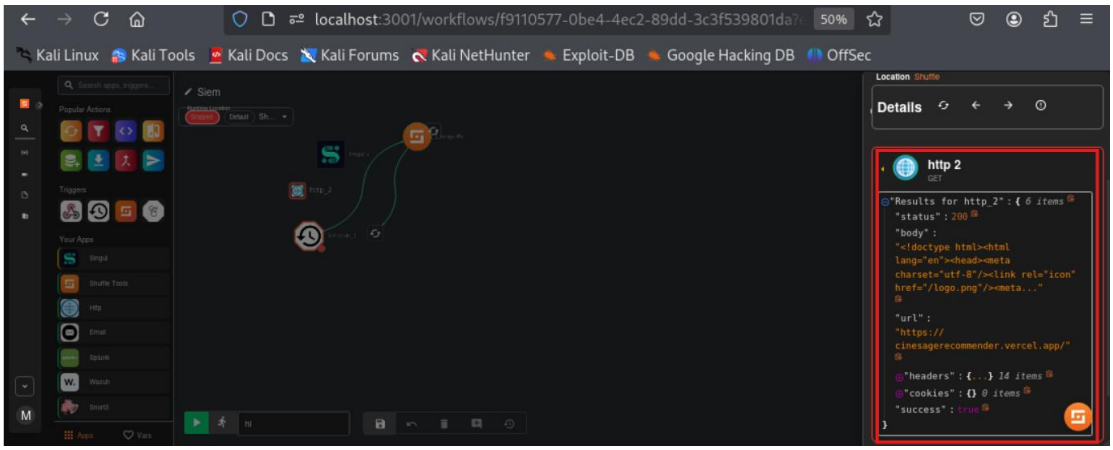
Made by Moeez Javed

Step 11



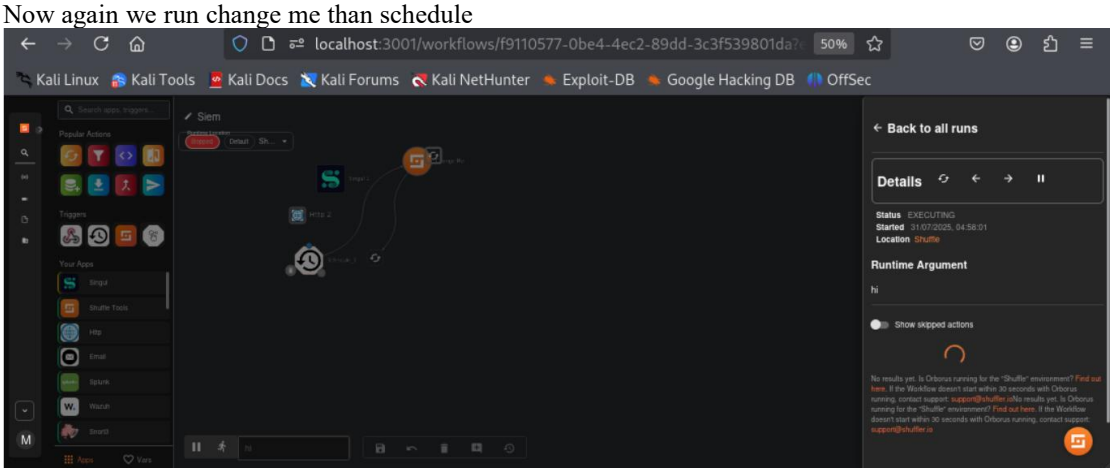
Step 12

View Output of Workflow



Step 13

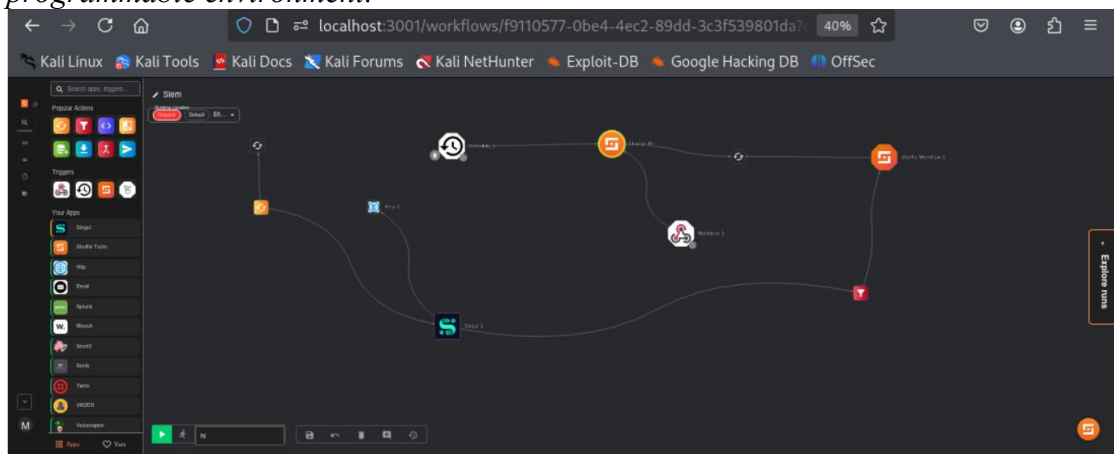
Now again we run change me than schedule



Step 14

Made by Moeez Javed

*This image shows a security automation workflow built in **Shuffle**, a SOAR (Security Orchestration, Automation, and Response) platform, running locally on Kali Linux. The workflow, named "SIEM," is designed to automate tasks such as fetching security alerts (possibly from a SIEM like QRadar), enriching them with external threat intelligence (via tools like MISP and VirusTotal), and applying logic-based actions based on the data. It includes a scheduler trigger, API calls, enrichment steps, and conditional logic to handle security events efficiently. The goal is to reduce manual effort in threat detection and response by automating key processes in a visually programmable environment.*



Conclusion

Shuffle SOAR provides a user-friendly, visual, and code-optional way to automate repetitive and time-consuming security operations. This tool is highly recommended for SOC analysts, penetration testers, and cybersecurity engineers who wish to boost their efficiency and incident response capability.

Appendix – Useful Links

***Shuffle GitHub**: https://github.com/frikky/Shuffle*

***Documentation**: https://shuffler.io/docs*

***Docker Installation**: https://docs.docker.com/engine/install/*