My Secure AWS DevOps Project

About This Project

This project is about setting up a cloud server, installing all the tools needed, running a web app using Docker, and then check it for security problems using Trivy.
I did this completely from scratch on an AWS EC2 server running Amazon Linux 2023.

Why I Made This

I wanted to practice DevOps and cloud security skills in a real environment instead of just watching tutorials.
This project helped me learn:

- How to work on AWS EC2 servers.
- How to install Python, Docker, and other tools.
- How to run an app inside a Docker container.
- How to scan that app for vulnerabilities.

What I Used

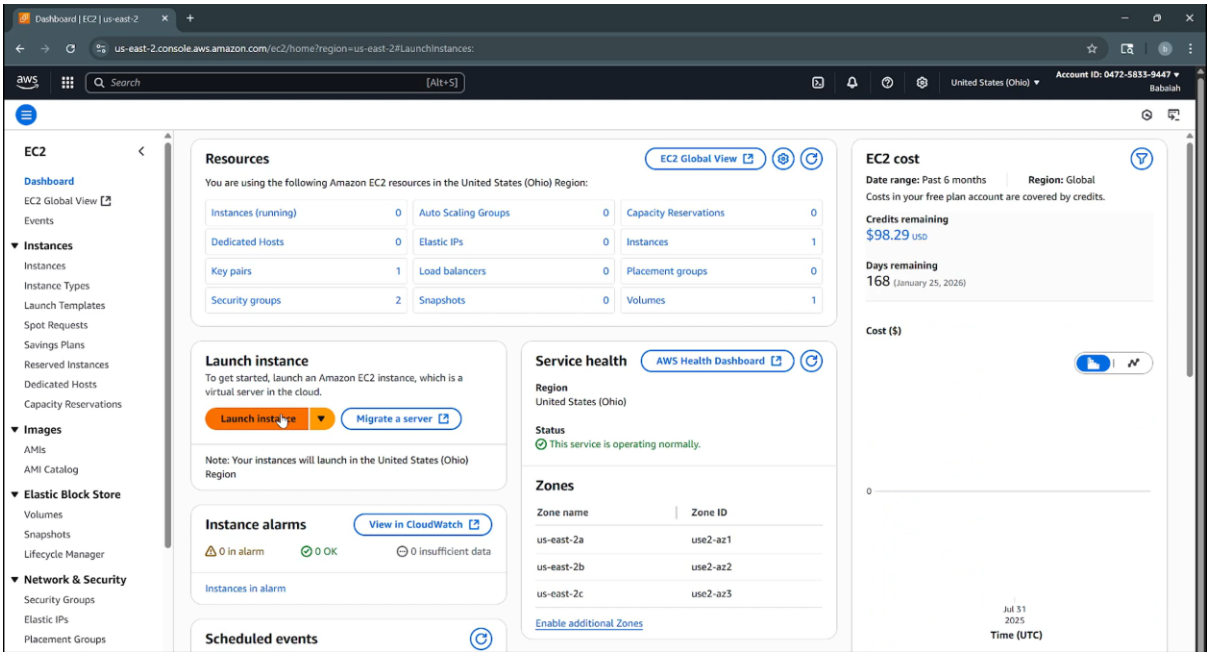
- **AWS EC2** (Amazon Linux 2023)
- **Python 3**
- **Docker**
- **Trivy** (for security scanning)
- **Git**
- **AWS CLI**

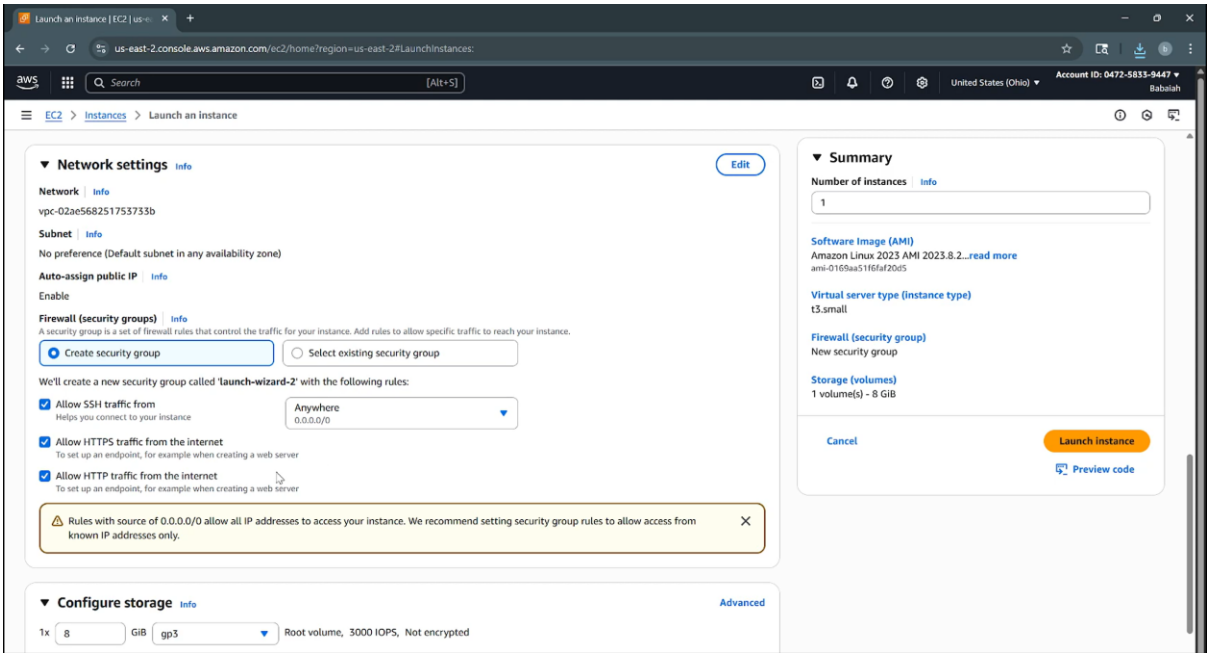
Steps I Followed

Here's exactly what I did from start to finish.

1. Launching the EC2 server

- I logged into my AWS account.
- I launched a new EC2 instance with **Amazon Linux 2023**.
- I selected a **t2.micro** instance type (free tier).
- I added my .pem key so I could SSH into it.





2. Connecting to the server

On my computer, I opened the terminal and went to where my PEM file was:

cd ~/Downloads

chmod 400 my-key.pem

ssh -i "my-key.pem" ec2-user@<my-ec2-public-ip>

Now I am inside my EC2 terminal.

```
PS C:\Users\gbaba\Downloads> ssh -i  "<0aws-1.pem>" ec2-user@3.143.245.5
Warning: Identity file <0aws-1.pem> not accessible: No such file or directory.
ec2-user@3.143.245.5: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
PS C:\Users\gbaba\Downloads> ssh -i  "<aws-1.pem>" ec2-user@3.143.245.5
Warning: Identity file <aws-1.pem> not accessible: No such file or directory.
ec2-user@3.143.245.5: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
PS C:\Users\gbaba\Downloads> ssh -i  aws-1.pem ec2-user@3.143.245.5
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-37-253 ~]$ sudo apt-get update -y
sudo: apt-get: command not found
[ec2-user@ip-172-31-37-253 ~]$
```

---

3. Updating the system

First thing I did was update the server so it has the latest packages:

bash

sudo dnf update -y

---

4. Installing basic tools

I installed the tools that I would need later:

bash

sudo dnf install -y git curl unzip wget jq make gcc gcc-c++ openssl-devel bzip2 libffi-devel

---

5. Installing Docker

I wanted to run my app in a Docker container, so I installed Docker:

bash

sudo dnf install -y docker

sudo systemctl enable --now docker

sudo usermod -aG docker $USER

newgrp docker

docker --version

---

6. Installing Python 3 and pip

My app is in Python, so I installed Python and pip:

bash

sudo dnf install -y python3 python3-pip python3-devel

python3 --version

pip3 --version

---

7. Installing AWS CLI (for AWS commands)

bash

curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"

unzip awscliv2.zip

sudo ./aws/install

aws --version

---

8. Installing Trivy (security scanner)

This is to check my Docker images for known vulnerabilities:

bash

curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/main/contrib/install.sh | sudo sh -s -- -b /usr/local/bin

trivy --version

---

9. Cloning my project

I pulled my project from GitHub:

bash

git clone https://github.com/yourusername/yourproject.git

cd project-location

---

10. Setting up Python environment

I created a virtual environment for Python:

bash

python3 -m venv .venv

source .venv/bin/activate

pip install --upgrade pip

pip install -r requirements.txt

---

11. Building the Docker image

bash

docker build -t myapp .

---

12. Running the app in Docker

Bash

docker run -d -p 8000:8000 myapp

I then opened my browser and went to:

perl

http://<my-ec2-public-ip>:8000

I saw my app running there.

---

13. Running security scan with Trivy

Performed container image security scans using Trivy on AWS-hosted Python/Flask applications, identified and classified vulnerabilities (Debian base image + Python dependencies), and documented remediation steps for high/critical issues.

To check if my Docker image had vulnerabilities:

bash

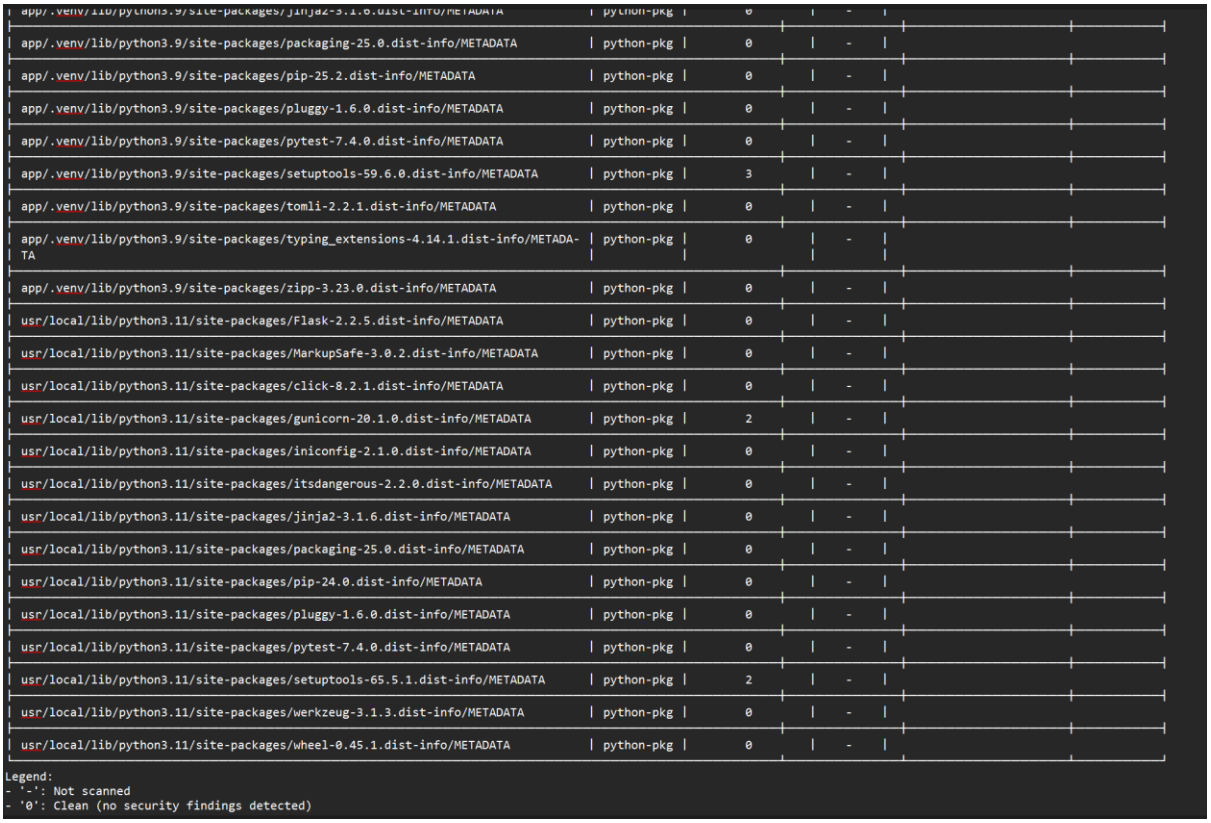
trivy image myapp

This gave me a list of security issues and their severity levels.

```
(.venv) [ec2-user@ip-172-31-37-253 terraform]$ cd aws-1
bash: cd: aws-1: No such file or directory
(.venv) [ec2-user@ip-172-31-37-253 terraform]$ pwd
/home/ec2-user/aws-1/terraform
(.venv) [ec2-user@ip-172-31-37-253 terraform]$ cd /home/ec2-user/aws-1/
(.venv) [ec2-user@ip-172-31-37-253 aws-1]$ trivy image myapp
2025-08-10T21:54:47Z    INFO    [vulndb] Need to update DB
2025-08-10T21:54:47Z    INFO    [vulndb] Downloading vulnerability DB...
2025-08-10T21:54:47Z    INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
68.34 MiB / 68.34 MiB [---------------------------------------------------------------] 100.00% 18.51 MiB p/s 3.9s
2025-08-10T21:54:52Z    INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-08-10T21:54:52Z    INFO    [vuln] Vulnerability scanning is enabled
2025-08-10T21:54:52Z    INFO    [secret] Secret scanning is enabled
2025-08-10T21:54:52Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-08-10T21:54:52Z    INFO    [secret] Please see also https://trivy.dev/v0.65/docs/scanner/secret#recommendation for faster secret detection
2025-08-10T21:55:03Z    INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all affected packages.
2025-08-10T21:55:10Z    INFO    Detected OS     family="debian" version="12.11"
2025-08-10T21:55:10Z    INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=105
2025-08-10T21:55:10Z    INFO    Number of language-specific files       num=1
2025-08-10T21:55:10Z    INFO    [python-pkg] Detecting vulnerabilities...
2025-08-10T21:55:10Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.65/docs/scanner/vulnerability#severity-selection for details.
2025-08-10T21:55:10Z    INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

Report Summary

┌──────────────────────────────────────────────────────────────────────────────────────────────────────┬────────────┬─────────────────┬─────────┐
│                                                Target                                                │    Type    │ Vulnerabilities │ Secrets │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ myapp (debian 12.11)                                                                                 │   debian   │       106       │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/Flask-2.2.5.dist-info/METADATA                                 │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/MarkupSafe-3.0.2.dist-info/METADATA                            │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/Werkzeug-2.2.3.dist-info/METADATA                              │ python-pkg │        4        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/click-8.1.8.dist-info/METADATA                                 │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/exceptiongroup-1.3.0.dist-info/METADATA                        │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/gunicorn-20.1.0.dist-info/METADATA                             │ python-pkg │        2        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/importlib_metadata-8.7.0.dist-info/METADA-                     │ python-pkg │        0        │    -    │
│ TA                                                                                                   │            │                 │         │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/iniconfig-2.1.0.dist-info/METADATA                             │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/itsdangerous-2.2.0.dist-info/METADATA                          │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/jinja2-3.1.6.dist-info/METADATA                                │ python-pkg │        0        │    -    │
├──────────────────────────────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ app/.venv/lib/python3.9/site-packages/packaging-25.0.dist-info/METADATA                              │ python-pkg │        0        │    -    │
└──────────────────────────────────────────────────────────────────────────────────────────────────────┴────────────┴─────────────────┴─────────┘
```



What I Learned

- How to set up an AWS EC2 instance from scratch.
- How to install all required DevOps tools on Amazon Linux.
- How to containerize a Python app with Docker.

- How to run security scans on Docker images.
- How to connect all these steps into a mini DevOps workflow.