# CLOUD GUARD SENTINEL

## 1.Setting the environment

```
# Install Python virtual environment
sudo apt-get update
sudo apt-get install python3-venv -y

# Create and activate a virtual environment
python3 -m venv cloud_security_env
source cloud_security_env/bin/activate

# Install necessary Python packages
pip install requests

# Install Terrascan
curl -L https://raw.githubusercontent.com/accurics/terrascan/master/scripts/install.sh | sh

# Install Nmap and OpenVAS
sudo apt-get install nmap -y
sudo apt-get install openvas -y
```

## 2.Python Code

```
import os
import subprocess

def run_terrascan(directory):
    try:
        print(f"Scanning directory: {directory}")
        result = subprocess.run(['terrascan', 'scan', '-d', directory], capture_output=True,
text=True)
        return result.stdout
    except Exception as e:
        return str(e)

def run_nmap_scan(target):
    try:
        print(f"Running Nmap scan on: {target}")
        result = subprocess.run(['nmap', '-sV', target], capture_output=True, text=True)
        return result.stdout
    except Exception as e:
        return str(e)

def run_openvas_scan(target):
    try:
        print(f"Running OpenVAS scan on: {target}")
        # Example command, adjust as needed for your OpenVAS setup
        result = subprocess.run(['openvas', '--scan', target], capture_output=True, text=True)
        return result.stdout
    except Exception as e:
        return str(e)

if __name__ == "__main__":
    # Path to the infrastructure as code directory
    iac_directory = "/path/to/your/iac"
    # Cloud environment target (IP or domain)
    cloud_target = "your-cloud-target.com"

    # Run Terrascan
    scan_result = run_terrascan(iac_directory)
    print("Terrascan Result:\n", scan_result)

    # Run Nmap vulnerability scan
    nmap_result = run_nmap_scan(cloud_target)
    print("Nmap Scan Result:\n", nmap_result)

    # Run OpenVAS vulnerability scan
    openvas_result = run_openvas_scan(cloud_target)
    print("OpenVAS Scan Result:\n", openvas_result)
```

3.Running the code

```
python3 cloud_guard_sentinel.py
```

**Expected output**

For AWS

```
Terrascan Result:
----------------------------------------
Scanning directory: /path/to/your/iac
Found 3 total violations in 2 files.
+------------------------------------------+------------------------------------------+------------------------
-------+
|              FILE PATH               |               RULE ID               |         DESCRIPTION
|
+------------------------------------------+------------------------------------------+------------------------
-------+
|    /path/to/your/iac/main.tf              |               AWS_RDS_PUBLIC_ACCESS        |
AWS RDS Instance allows     |
|                                   |                                   |    public access.            |
+------------------------------------------+------------------------------------------+------------------------
-------+
|    /path/to/your/iac/ecs.tf              |               AWS_ECS_EXECUTION_ROLE_MISSING
|    AWS ECS Task Definition     |
|                                   |                                   |    requires an execution role.  |
+--------------------------------------------+--------------------------------------------+------------------------
-------+

Nmap Scan Result:

----------------------------------------
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-10 15:30 UTC
Nmap scan report for your-cloud-target.com (10.0.0.1)
Host is up (0.021s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
443/tcp  open  https    Apache httpd 2.4.38 ((Debian))

OpenVAS Scan Result:
----------------------------------------
Running OpenVAS scan on: your-cloud-target.com
Target: your-cloud-target.com
Scan started at: 2024-06-10 15:35:00 UTC
Scan completed at: 2024-06-10 15:45:00 UTC
Results:
- High Severity Vulnerabilities: 2
- Medium Severity Vulnerabilities: 5
- Low Severity Vulnerabilities: 3
```

For MS Azure

```
Terrascan Result:
----------------------------------------
Scanning directory: /path/to/your/iac
Found 2 total violations in 1 file.
+--------------------------------------------+--------------------------------------------+------------------------
-------+
|                FILE PATH                |                RULE ID                |         DESCRIPTION
|
+--------------------------------------------+--------------------------------------------+------------------------
-------+
|        /path/to/your/iac/main.tf           |                AZURE_STORAGE_NO_HTTPS        |
Azure Storage account       |
|                                    |                                    |     allows unencrypted HTTP
|
|                                    |                                    |     access.                 |
+--------------------------------------------+--------------------------------------------+------------------------
-------+

Nmap Scan Result:
----------------------------------------
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-10 15:30 UTC
Nmap scan report for your-cloud-target.com (10.0.0.1)
Host is up (0.021s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
443/tcp  open  https    Apache httpd 2.4.38 ((Debian))

OpenVAS Scan Result:
----------------------------------------
Running OpenVAS scan on: your-cloud-target.com
Target: your-cloud-target.com
Scan started at: 2024-06-10 15:35:00 UTC
Scan completed at: 2024-06-10 15:45:00 UTC
Results:
- High Severity Vulnerabilities: 1
- Medium Severity Vulnerabilities: 3
- Low Severity Vulnerabilities: 2
```