Mobile Security Framework (MobSF)

Introduction

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis. Mobile Security Framework (MobSF) is an automated, open-source, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic, and malware analysis. It is suggested by OWASP MSTG for static analysis of security in mobile applications. It can be used for effective and fast security analysis of Android, iOS, and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code. MobSF can do dynamic application testing at runtime for Android apps and has Web API fuzzing capabilities powered by CapFuzz, a Web API-specific security scanner. MobSF is designed to make your CI/CD or DevSecOps pipeline integration seamless. It has a graphic UI in the form of a web service. Web service consists of a dashboard that presents the results of the analysis, its own documentation site, an integrated emulator & an API that allows users to trigger the analysis automatically. It is hosted in a local environment, so sensitive data never interacts with the cloud.

Static Analysis

In static analysis, the application is tested from the inside out. It analyzes the source code or binary without executing the application. It does not rely on a runtime environment. It can be used to test code during development and cache vulnerabilities early on. Static analysis security testing tools must be run on the application on a regular basis, such as during daily/monthly builds, every time code is checked in, or during a code release.

Features

The following are the features of the MobSF:

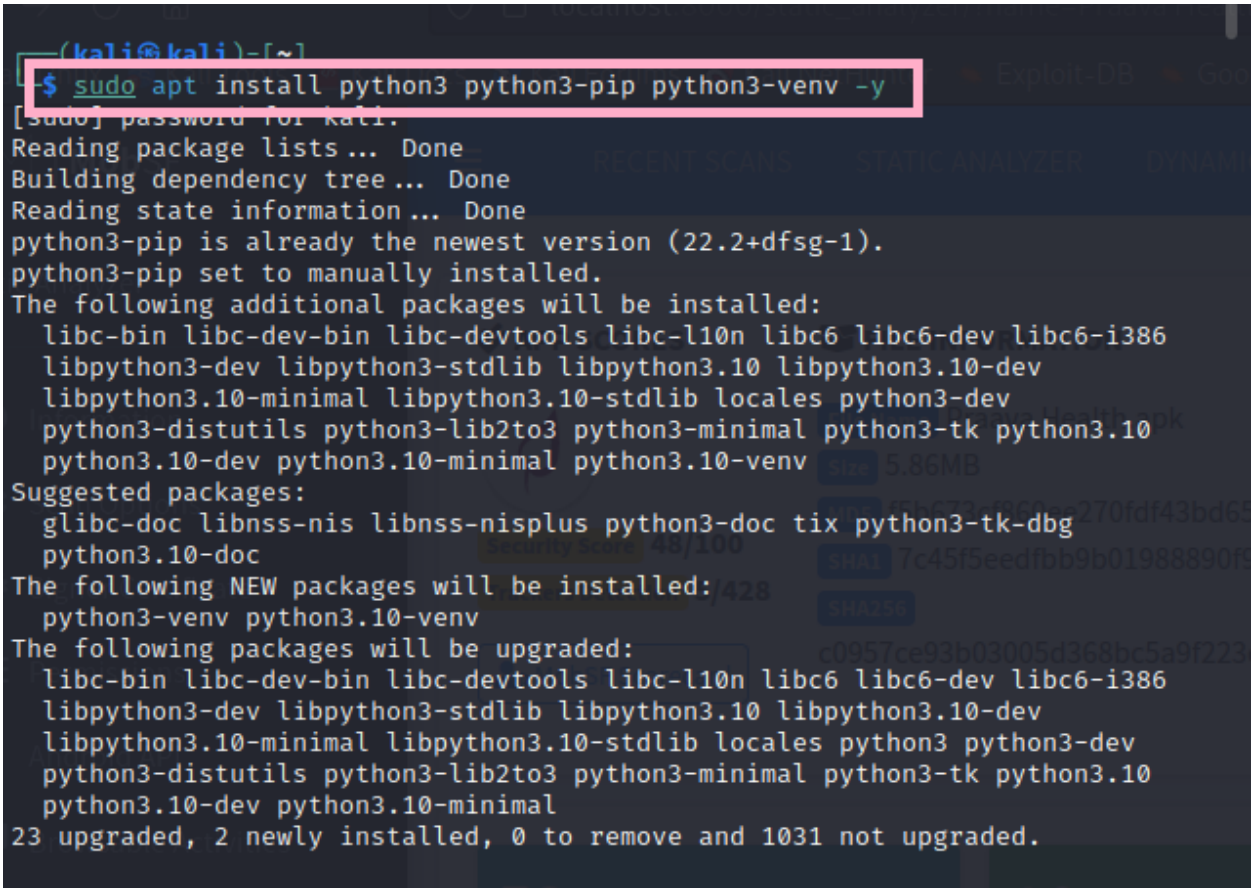
- False Positive Triaging / Suppression Triaging Support for critical Android and iOS Security Analysis features.
- Android Binary & Source - Supports Code Analysis and Manifest Analysis
- iOS Binary - Supports Binary Code Analysis
- iOS Source - Supports Code Analysis
- New REST APIs for Suppression Support
- Android Certificate Analysis improvements
- Remove RELRO check from android binary analysis due to false positives
- iOS Bundle ID extraction improvements
- Feature parity - Allow IPA downloads from reports view
- Code QA: Reduce False positives in identified secrets

- Check for updates from GitHub releases
- M1 Mac support
- Disabled by default feature to support hotspots in AppSec Scorecard
- Dependency updates
- Added CodeQL scan on MobSF python code base
- Bug Fixes
- Fixes #1999, #1917, #2042 #1981 #2014 #2043
- Fixed a bug in JSON response REST API
- iOS URL view fix
- Code fixes to address minor security issues in third-party libraries.
- Handle JADX timeouts

Installation

We can install MOBSF using apt-get by running the following command:

sudo apt install python3 python3-pip python3-venv –y

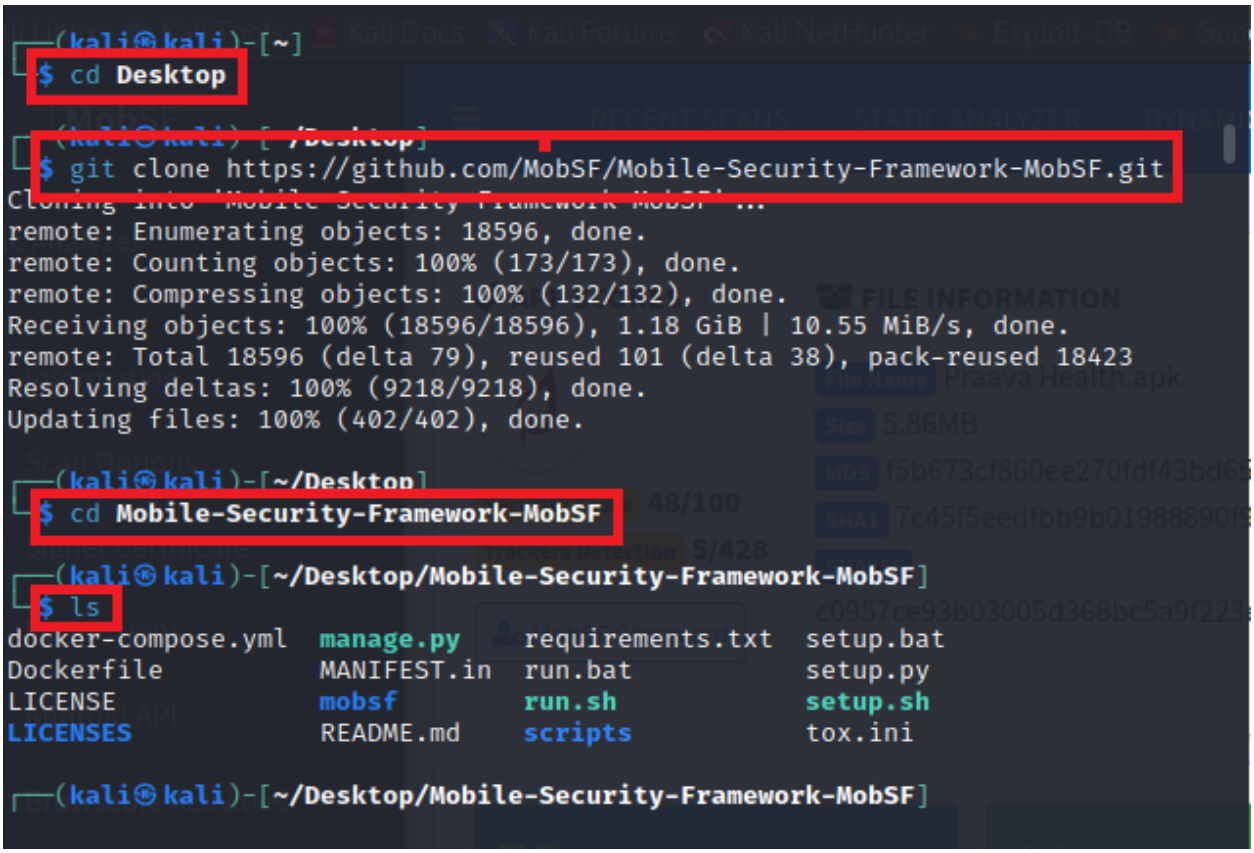


cd Desktop

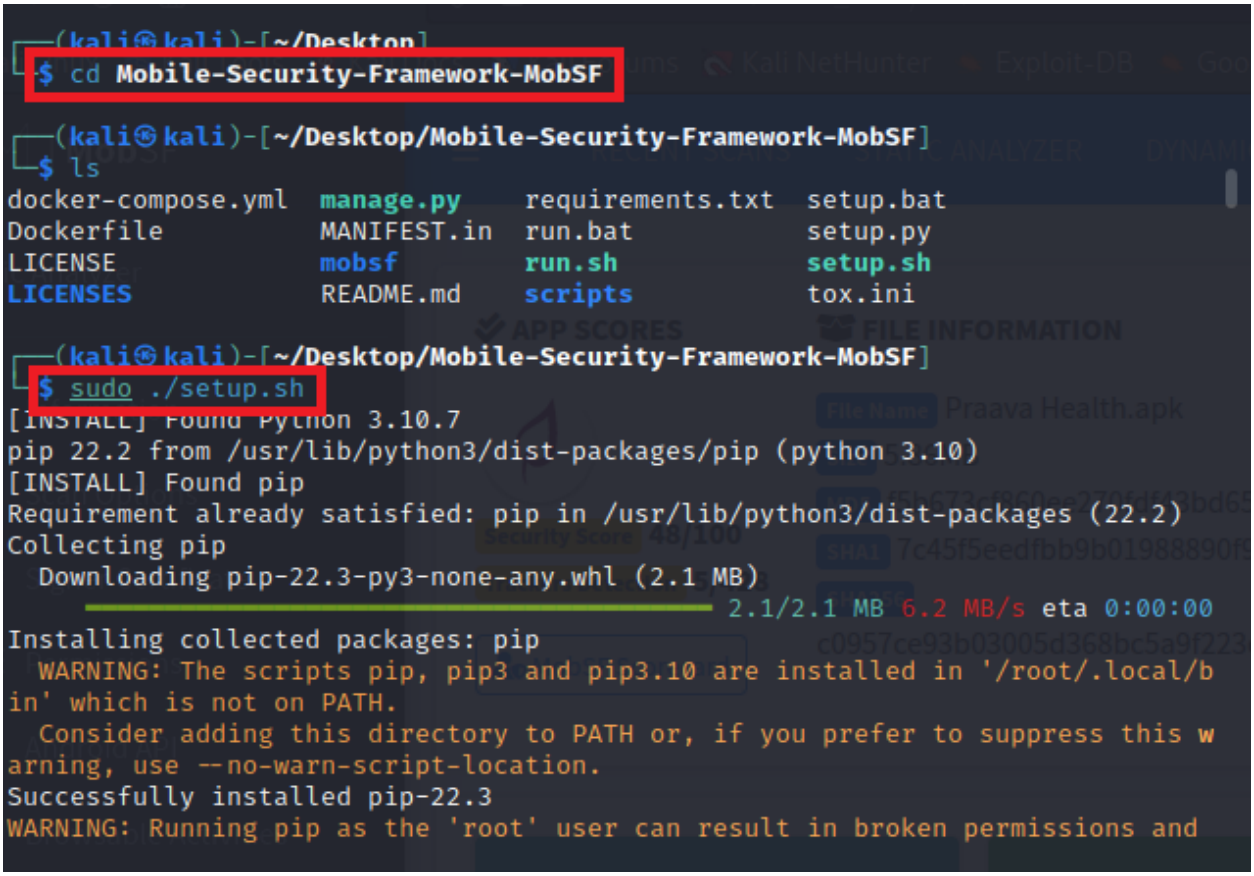
git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git

cd Mobile-Security-Framework-MobSF

ls



sudo ./setup.sh

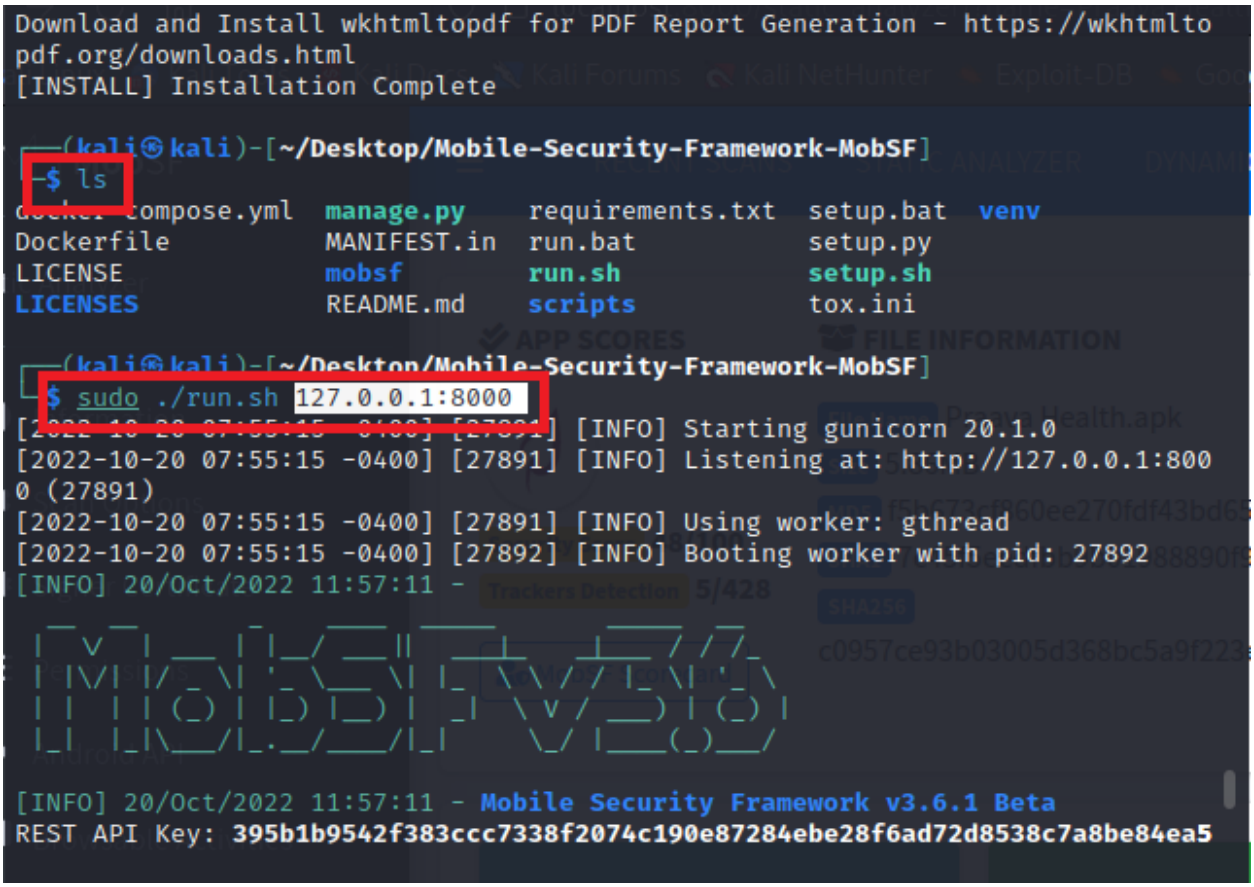


Usage

To check or scan the “localhost:8000” server and open the MobSF tool we can execute the following command:

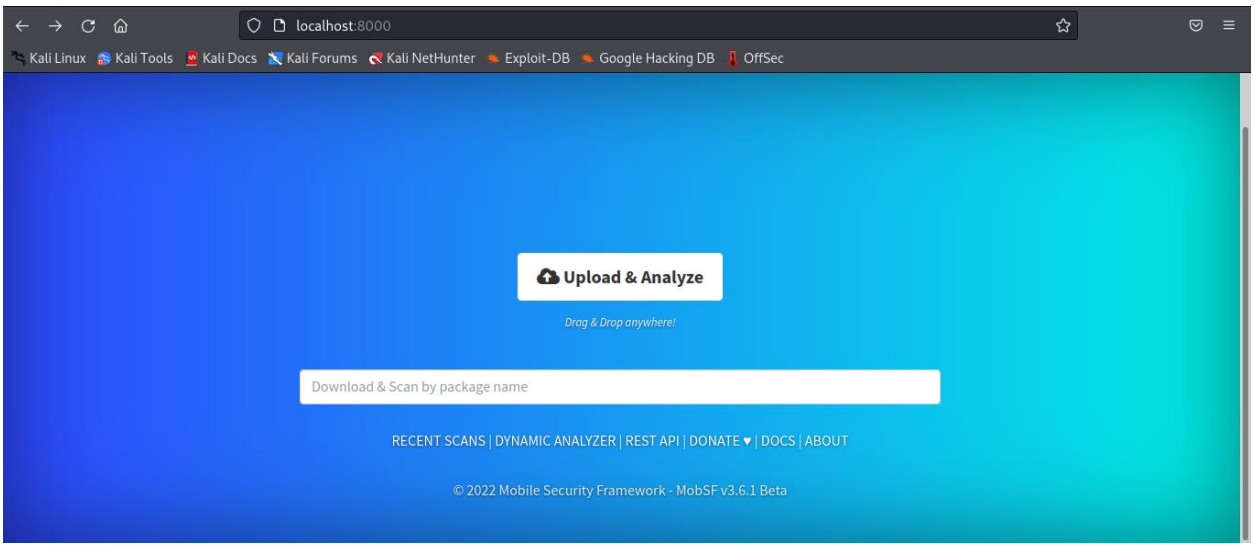
ls

sudo ./run.sh 127.0.0.1:8000

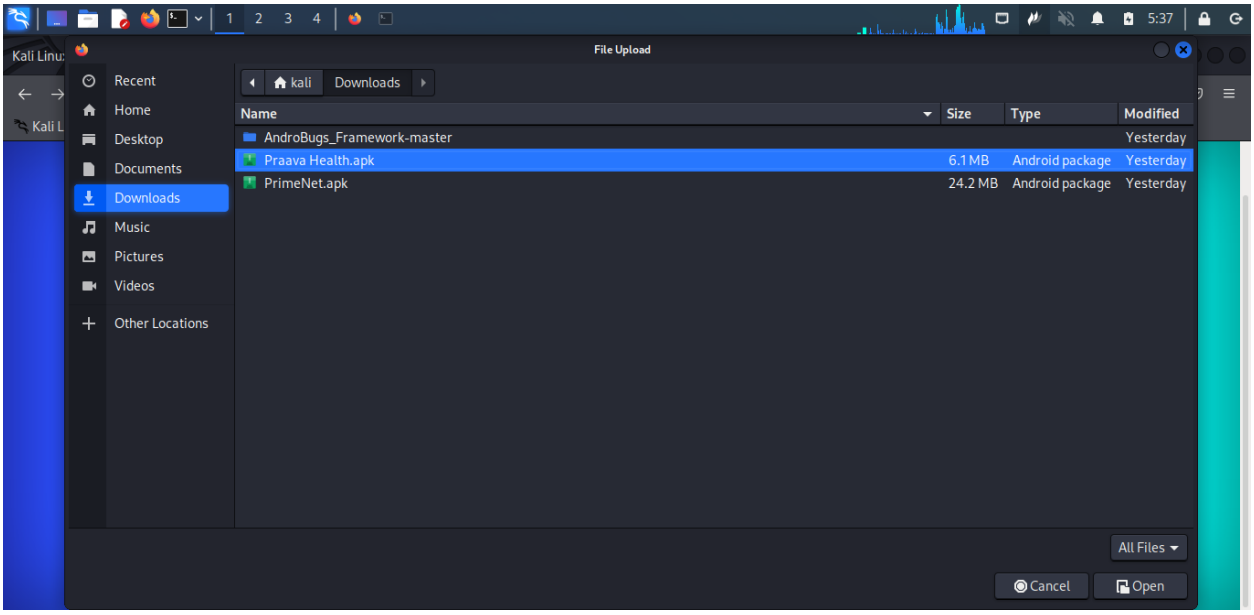


Write this in the browser URL in kali linux:

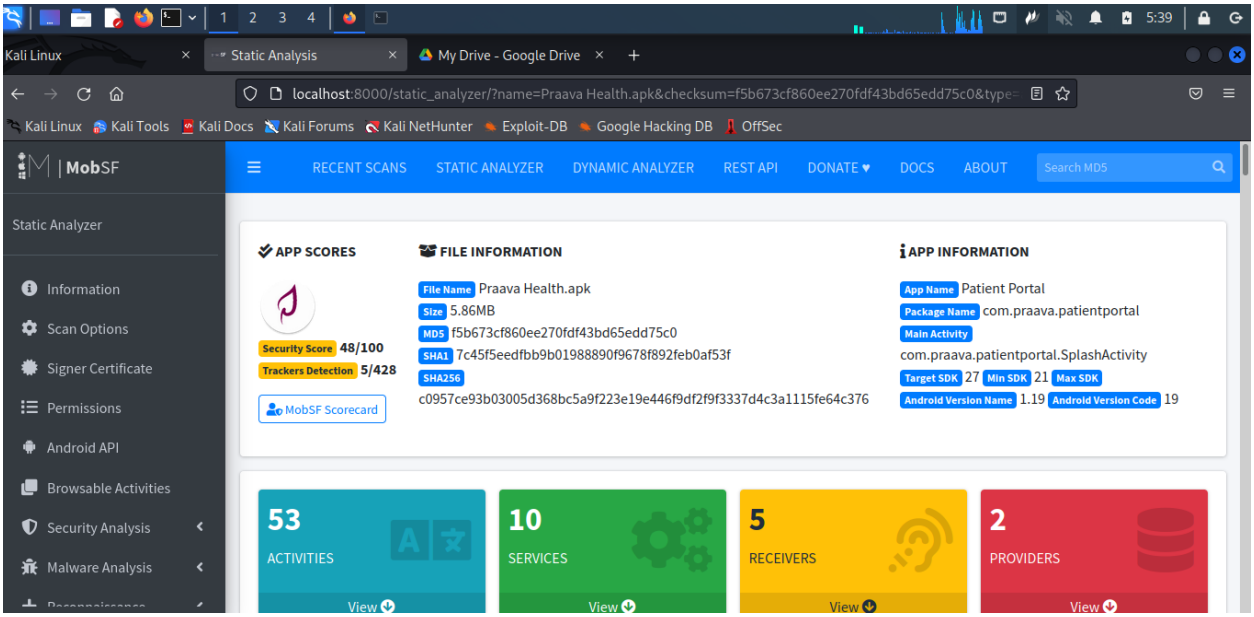
http://localhost:8000/



Upload your APK file:



Here is the Static Analysis:



The “Praava Health.apk” PDF report link is given below:

Drive link: https://drive.google.com/drive/folders/1h37dhMVCHMxbC41jcKY0qXOe9OfTn7wO

References

1. https://mobsf.github.io/docs/#/
2. https://medium.com/@kshitishirke/mobile-security-framework-mobsf-static-analysis-df22fcdae46e
3. https://mobsf.github.io/Mobile-Security-Framework-MobSF/changelog.html