

MOBILE PENETRATION TESTING MANUAL



MOEEZ JAVED

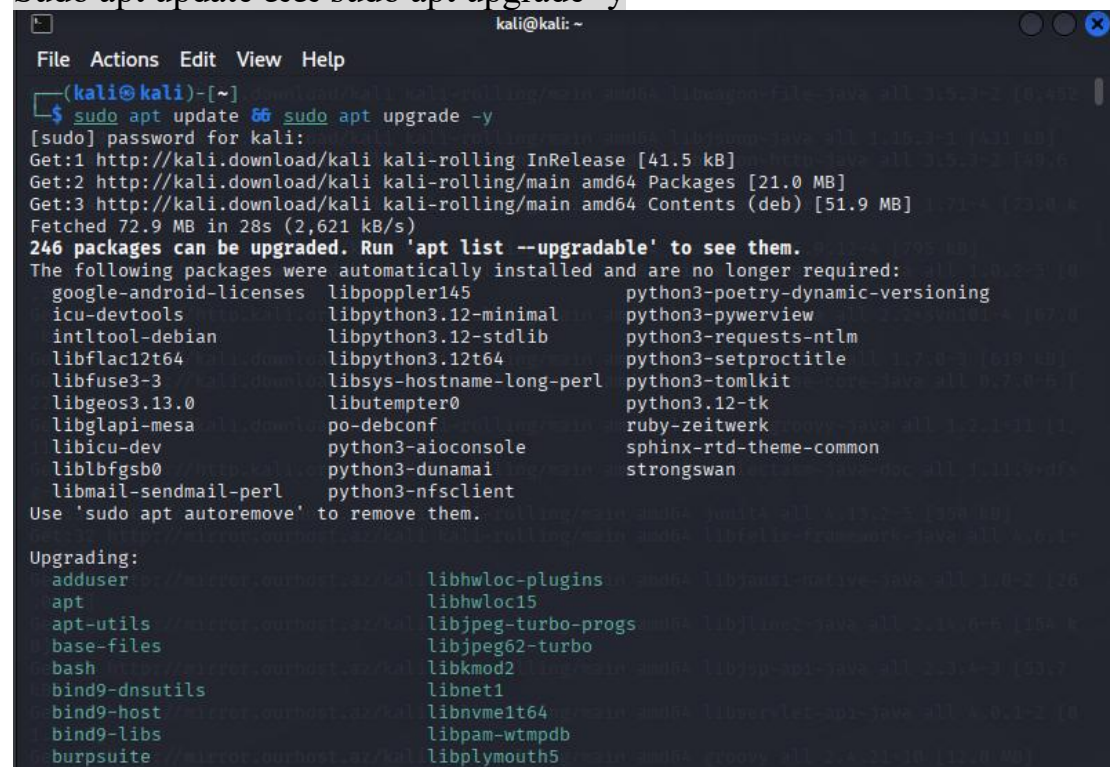
Android Penetration Testing with MobSF — Professional Manual

Prerequisites

- ✓ OS: Kali Linux (latest rolling release recommended)
- ✓ Permissions: sudo access
- ✓ Internet connection

This command updates the package list and upgrades all installed packages to their latest versions — **best practice before any installation.**

`Sudo apt update && sudo apt upgrade -y`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt update && sudo apt upgrade -y  
[sudo] password for kali:  
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.9 MB]  
Fetched 72.9 MB in 28s (2,621 kB/s)  
246 packages can be upgraded. Run 'apt list --upgradable' to see them.  
The following packages were automatically installed and are no longer required:  
  google-android-licenses libpoppler145 python3-poetry-dynamic-versioning  
  icu-devtools libpython3.12-minimal python3-pywerview  
  intltool-debian libpython3.12-stdlib python3-requests-ntlm  
  libflac12t64 libpython3.12t64 python3-setproctitle  
  libfuse3-3 libsys-hostname-long-perl python3-tomlkit  
  libgeos3.13.0 libutempter0 python3.12-tk  
  libglapi-mesa po-debconf ruby-zeitwerk  
  libicu-dev python3-aioconsole sphinx-rtd-theme-common  
  libbfgsb0 python3-dunamai strongswan  
  libmail-sendmail-perl python3-nfsclient  
Use 'sudo apt autoremove' to remove them.  
Upgrading:  
  adduser libhwloc-plugins libaudi-native-java  
  apt libhwloc15  
  apt-utils libjpeg-turbo-progs  
  base-files libjpeg62-turbo  
  bash libkmod2  
  bind9-dnsutils libnet1  
  bind9-host libnvme1t64  
  bind9-libs libpam-wtmpdb  
  burpsuite libplymouth5
```

This installs the official docker.io package from Kali's repositories.

`sudo apt install docker.io -y`

```
(kali@kali)-[~]
$ sudo apt install docker.io -y

[sudo] password for kali:
docker.io is already the newest version (26.1.5+dfsg1-9+b6).
The following packages were automatically installed and are no longer required:
  google-android-licenses libpoppler145 python3-poetry-dynamic-versioning
  icu-devtools libpython3.12-minimal python3-pywebview
  intltool-debian libpython3.12-stdlib python3-requests-ntlm
  libflac12t64 libpython3.12t64 python3-setproctitle
  libfuse3-3 libsys-hostname-long-perl python3-tomlkit
  libgeos3.13.0 libutempter0 python3.12-tk
  libglapi-mesa po-debconf ruby-zeitwerk
  libicu-dev python3-aiococonsole sphinx-rtd-theme-common
  liblbfgsb0 python3-dunamai strongswan
  libmail-sendmail-perl python3-nfsclient
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 7
```

enable: ensures Docker starts on system boot.

start: launches Docker service for immediate use

`sudo systemctl enable docker`

`sudo systemctl start docker`

```
(kali@kali)-[~]
$ sudo systemctl enable docker
$ sudo systemctl start docker

Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sy
sv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
```

Confirms Docker is installed correctly.

`docker --version`

```
(kali@kali)-[~]
$ docker --version

Docker version 26.1.5+dfsg1, build a72d7cd
```

Downloads the latest **official MobSF** image from DockerHub.

`sudo docker pull opensecurity/mobile-security-framework-mobsf:latest`

```
(kali@kali)-[~]
$ sudo docker pull opensecurity/mobile-security-framework-mobsf:latest

latest: Pulling from opensecurity/mobile-security-framework-mobsf
Digest: sha256:7dccc98e0c036ba751270edd3dcc81a30b21a7fb20f834d6198078b54265992
Status: Image is up to date for opensecurity/mobile-security-framework-mobsf:latest
docker.io/opensecurity/mobile-security-framework-mobsf:latest
```

✓ **Corrected Explanation:**

-it: interactive terminal

--rm: auto-remove container after exit

-p 8000:8000: maps MobSF's port 8000 to localhost

This starts MobSF **temporarily**. Close the terminal = stops MobSF.

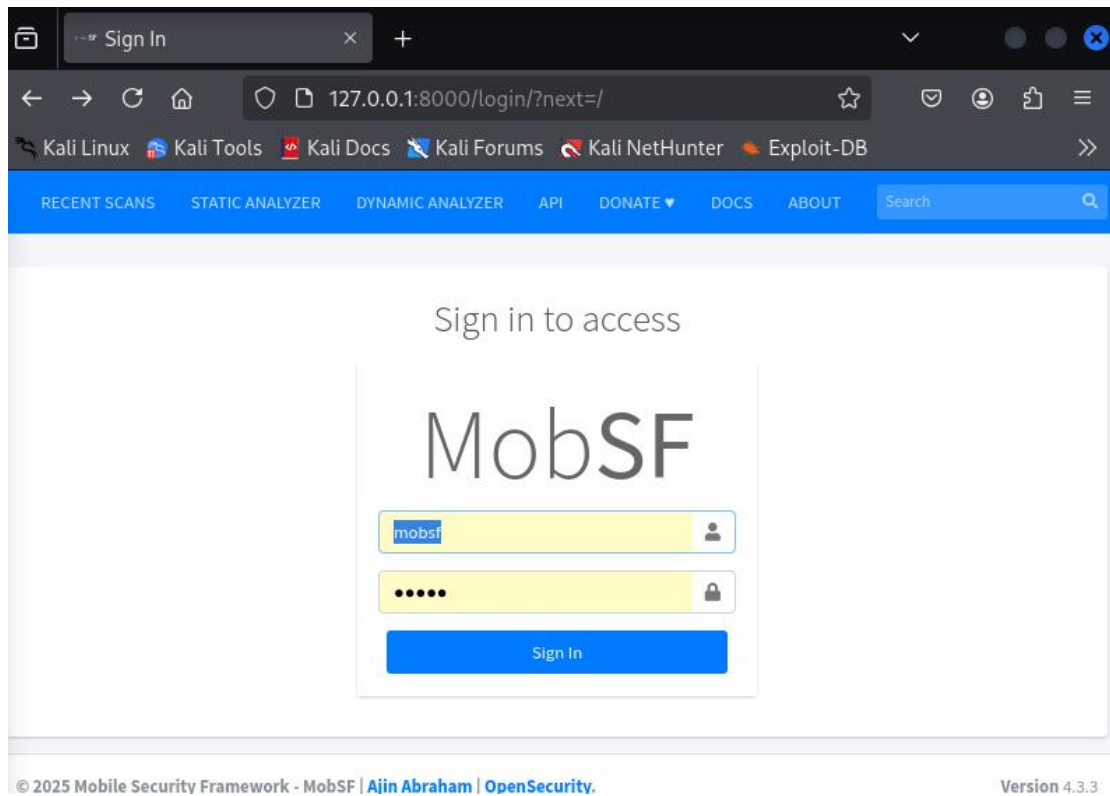
```
sudo docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
```

```
(kali@kali)-[~]
└─$ sudo docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest

[INFO] 28/May/2025 12:55:27 - JADX is already installed at /home/mobsf/.MobSF/tools/jadx/jadx-1.5.0
[INFO] 28/May/2025 12:55:27 - Loading User config from: /home/mobsf/.MobSF/config.py
[INFO] 28/May/2025 12:55:31 -
[INFO] 28/May/2025 12:55:31 - Author: Ajin Abraham | opensecurity.in
[INFO] 28/May/2025 12:55:31 - Mobile Security Framework v4.3.3
REST API Key: 21215d4206d36c0015b3a2df304e57d72fefebee01ab74ff2d53b67948333db3
Default Credentials: mobsf/mobsf
[INFO] 28/May/2025 12:55:31 - OS Environment: Linux (debian 12 bookworm) Linux-6.12.25-amd64-x86_64-with-glibc2.36
[INFO] 28/May/2025 12:55:31 - CPU Cores: 2, Threads: 2, RAM: 5.10 GB
[INFO] 28/May/2025 12:55:31 - MobSF Basic Environment Check
No changes detected
[INFO] 28/May/2025 12:55:33 - Checking for Update.
[INFO] 28/May/2025 12:55:33 - No updates available.
[INFO] 28/May/2025 12:55:38 - Loading User config from: /home/mobsf/.MobSF/config.py
[INFO] 28/May/2025 12:55:40 -
```

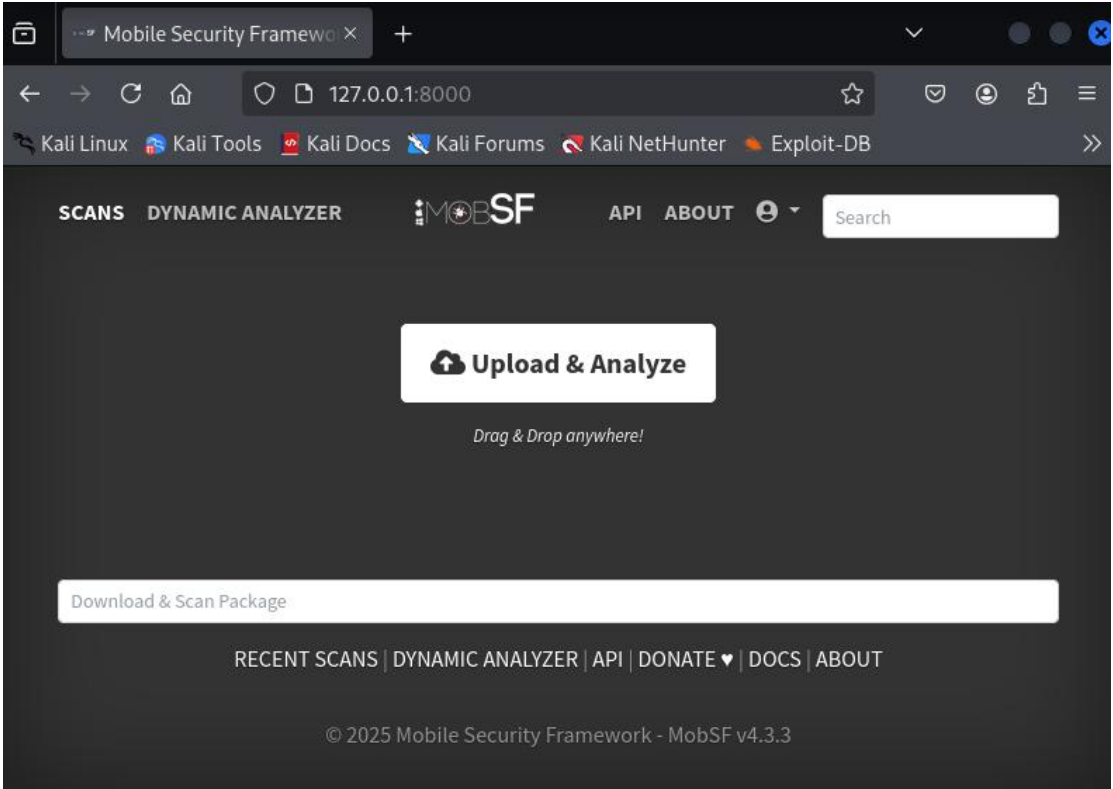
In browser

<http://127.0.0.1:8000/>

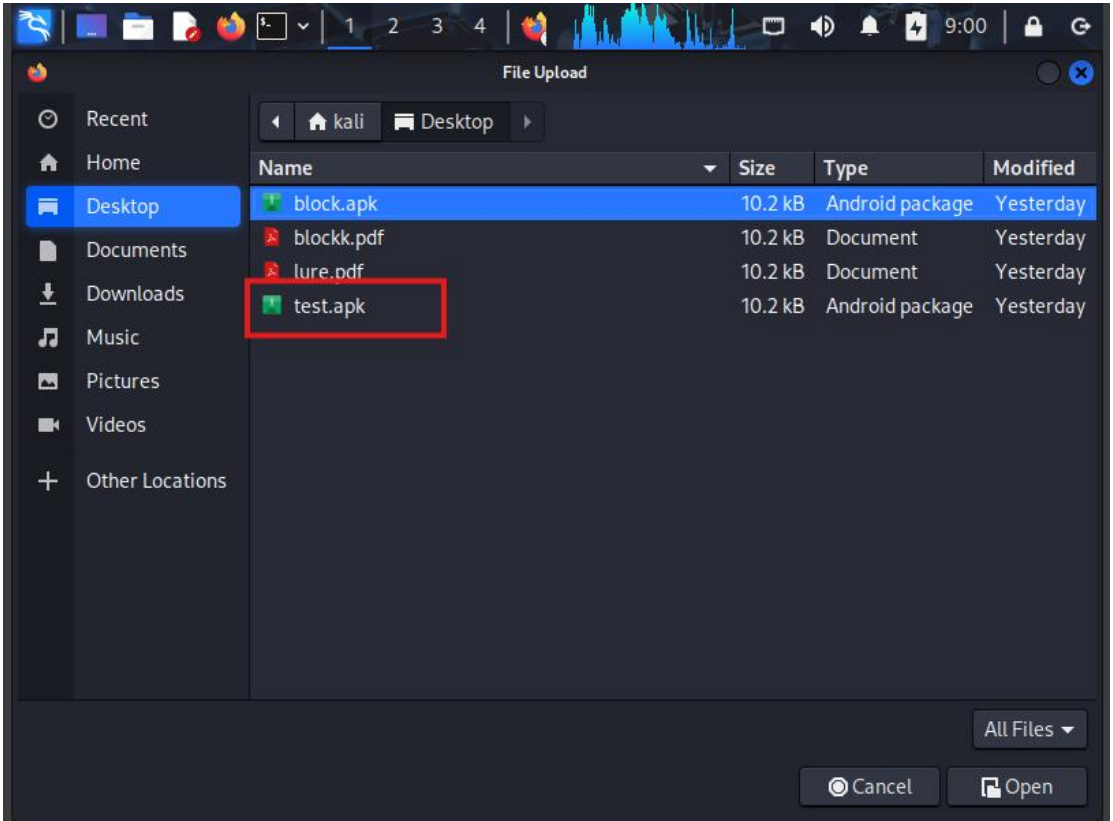


username: mobsf
password: mobsf

Explain what the APK is, what risks were found, and what each tab in the results means.



Now upload any apk file to scan



Made by Moez Javed

After scanning it give me detailed information.

The screenshot displays the MobSF (Mobile Security Framework) web interface. The top navigation bar includes links for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, API, DONATE, DOCS, and ABOUT, along with a search bar. The main content area is divided into three sections: APP SCORES, FILE INFORMATION, and APP INFORMATION.

APP SCORES: Shows a 'No Icon' placeholder, a Security Score of 44/100, and Trackers Detection of 0/432. A 'MobSF Scorecard' link is also present.

FILE INFORMATION: Lists file details for 'test.apk':
- File Name: test.apk
- Size: 0.01MB
- MD5: d3b04ce6cda8af90d8f3ae581e1c2ff4
- SHA1: 7fa51cae85649b45e2a2db22ea3bed4b8e0cbb50
- SHA256: 3e9296eee11db3dc78f394cfc369c67da0997b59dec3bdec672fd6e588d3474

APP INFORMATION: Lists app details:
- App Name: MainActivity
- Package Name: com.metasploit.stage
- Main Activity: .MainActivity
- Target SDK: 17, Min SDK: 10, Max SDK: 10
- Android Version Name: 1.0, Android Version Code: 1

Below these sections are four colored cards representing exported components:
- **EXPORTED ACTIVITIES:** 0/1 (Blue card)
- **EXPORTED SERVICES:** 1/1 (Green card)
- **EXPORTED RECEIVERS:** 1/1 (Yellow card)
- **EXPORTED PROVIDERS:** 0/0 (Red card)
Each card has a 'View All' link with a download icon.

Stop MobSF::

```
sudo docker stop mobsf
```

Start Mobsf

```
sudo docker start mobsf
```