OSINT-Framework: Installation Guide

Version 1.0.0

Jorge Generelo

October 8, 2021

Contents

1 Introduction

This document describes the steps to install the OSINT-Framework OS distribution and the OSINT-Lab web application.

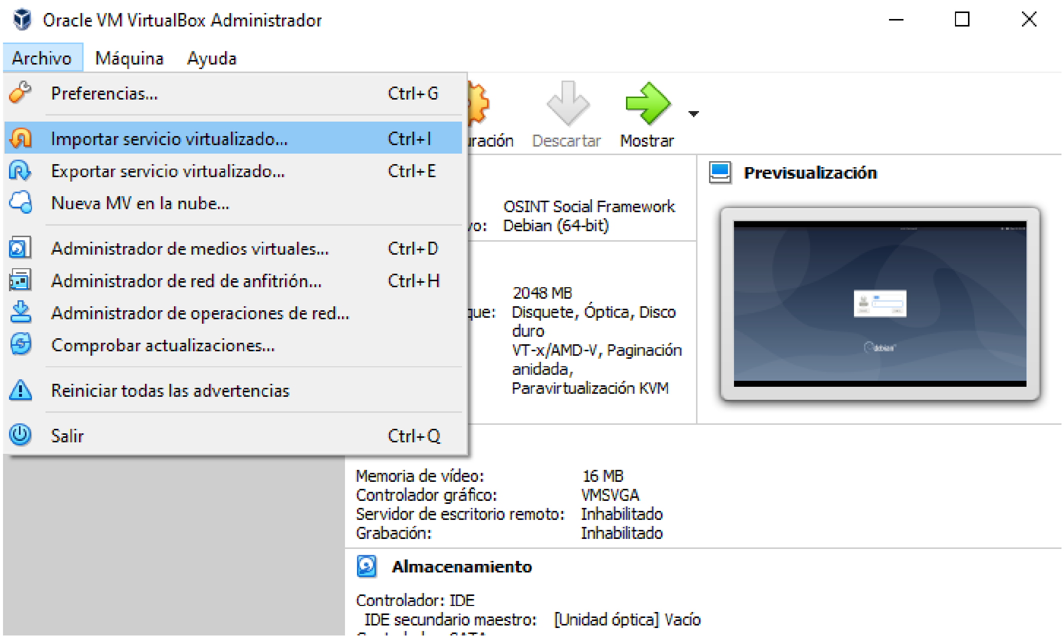
The OS distribution requires Virtual Box to run and the following specifications on the host system:

- 4GB RAM
- 40 GB Free Storage
- 2 Core CPUs

The web app needs Git, Docker and docker-compose installed in the system. Already installed in the OS distribution.

2 OSINT-Framework OS

To install the OS on Virtual Box you need the ”.ova” file that can be found in the GitHub repository. Once you have downloaded this VM image, go to Virtual Box and select the ”Import Appliance” option and search the ova file downloaded (Figure 1)


Oracle VM VirtualBox Administrador
Archivo
Máquina
Ayuda
Preferencias... Ctrl+G
Importar servicio virtualizado... Ctrl+I
Exportar servicio virtualizado... Ctrl+E
Nueva MV en la nube...
Administrador de medios virtuales... Ctrl+D
Administrador de red de anfitrión... Ctrl+H
Administrador de operaciones de red...
Comprobar actualizaciones...
Reiniciar todas las advertencias
Salir Ctrl+Q
ración
Descartar
Mostrar
Previsualización
Almacenamiento

OSINT Social Framework
o: Debian (64-bit)

2048 MB
ue: Disquete, Óptica, Disco duro
VT-x/AMD-V, Paginación anidada, Paravirtualización KVM

Memoria de vídeo: 16 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado

Controlador: IDE
IDE secundario maestro: [Unidad óptica] Vacío

Figure 1: Import Virtual Box ova.

Run the new VM and once it starts, log in using the default credentials that can be found in the project repository (Figure 2).

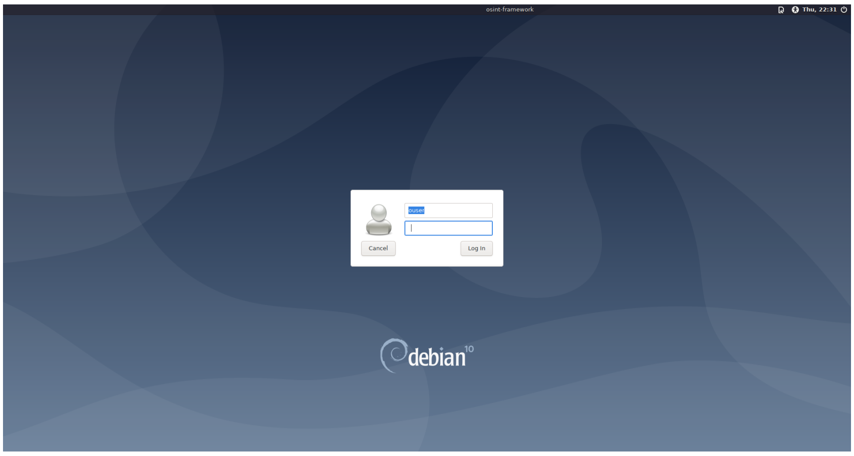


Figure 2: Login screen.

After logging in the desktop will be displayed and the VM is ready to start a new investigation (Figure 3).

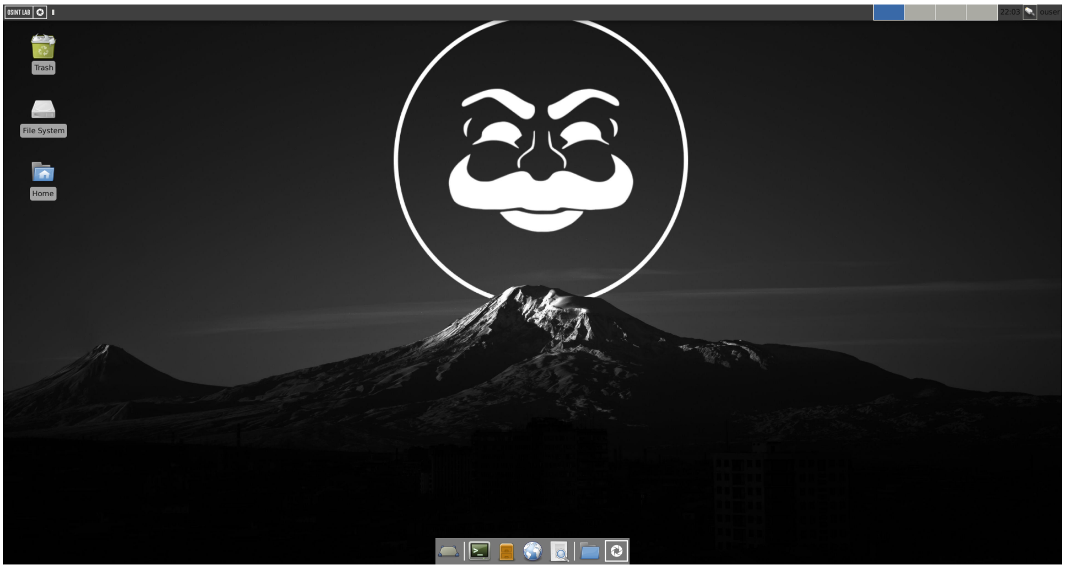


Figure 3: Desktop screen.

3 OSINT-Lab Web App

First step to install the Web App in our system is to download the repository using git and access the downloaded directory.

```
$ git pull https://github.com/jorgegene/OSINT-Framework.git
$ cd OSINT-Framework
```

Once we are in the project folder there a few things we have to configure after installing the application.

3.1 Facebook Cookie

First of all we have to add a Facebook session cookie in order to allow the framework using our profile to do the searches (It is highly recommended not to use your personal profile). To get the cookie we can use the Firefox extension Cookie Quick Manager[1]. Install the extension in your browser and log in to your Facebook account then select ”Search cookies for facebook.com” (Figure 4).

[1] https://addons.mozilla.org/es/firefox/addon/cookie-quick-manager/

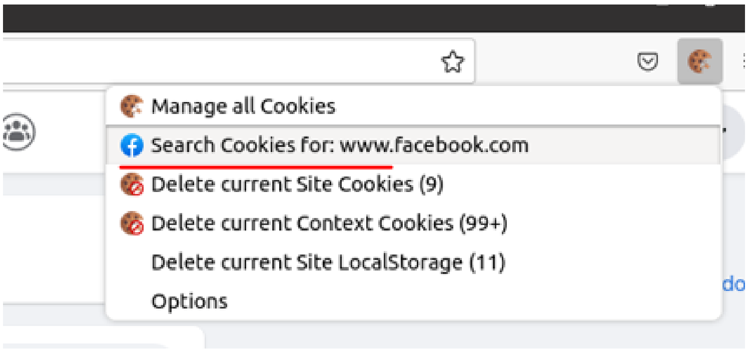
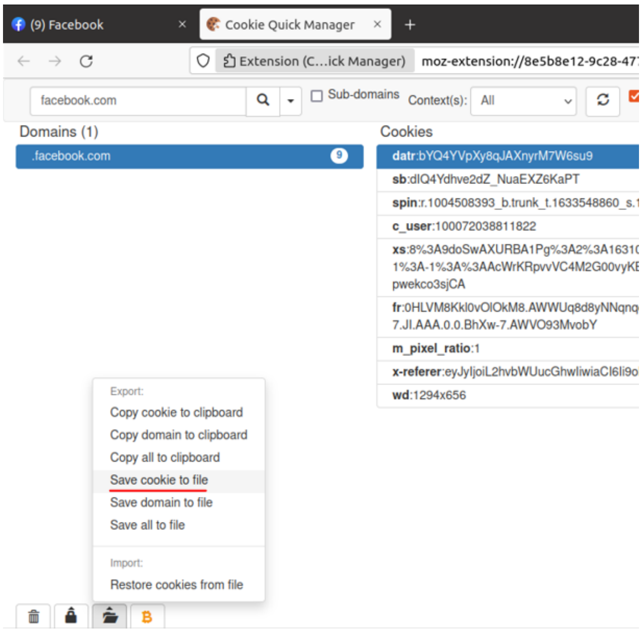

Manage all Cookies
Search Cookies for: www.facebook.com
Delete current Site Cookies (9)
Delete current Context Cookies (99+)
Delete current Site LocalStorage (11)
Options

Figure 4: Search Facebook cookie.

Once we select the Facebook cookie we want to use download it using the export option and save it to a file named ”cookie.json”(Figure 5).



datr:bYQ4YVpXy8qJAXnyrM7W6su9
sb:dlQ4Ydhve2dZ_NuaEXZ6KaPT
spin:r.1004508393_b.trunk_t.1633548860_s.1
c_user:100072038811822
xs:8%3A9doSwAXURBA1Pg%3A2%3A1631(
1%3A-1%3A%3AAcWrKRpvvVC4M2G00vyKE
pwekco3sjCA
fr:0HLVM8Kkl0vOlOkM8.AWWUq8d8yNNqnq
7.JI.AAA.0.0.BhXw-7.AWVO93MvobY
m_pixel_ratio:1
x-referer:eyJyljoiL2hvbWUucGhwliwiaCl6li9o
wd:1294x656

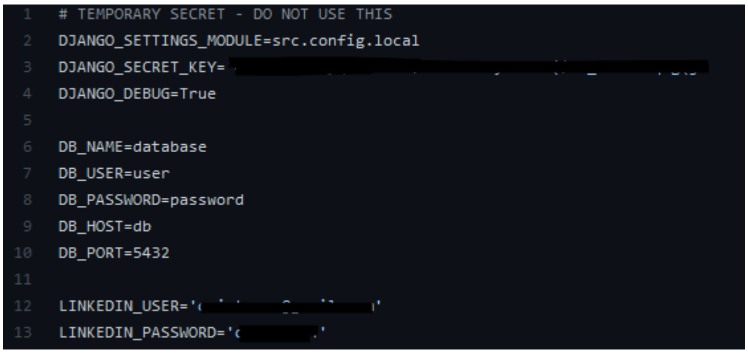
Figure 5: Export Facebook cookie.

Final step is to move the ”cookie.json” file to the project root folder (an empty file with the same name can be found there).

3.2 LinkedIN Credentials

In order to allow LinkedIN search for profiles, we have to add the credentials of an existing account.

In this case just editing the ”.env” file in the root folder adding your own credentials will make it work (Figure 6).



```
# TEMPORARY SECRET - DO NOT USE THIS
DJANGO_SETTINGS_MODULE=src.config.local
DJANGO_SECRET_KEY=[redacted]
DJANGO_DEBUG=True

DB_NAME=database
DB_USER=user
DB_PASSWORD=password
DB_HOST=db
DB_PORT=5432

LINKEDIN_USER='[redacted]'
LINKEDIN_PASSWORD='[redacted]'
```

Figure 6: LinkedIN credentials.

3.3 Docker Installation

Once everything is ready run docker-compose up to deploy the containers and docker-compose up to run the containers. The build process just has to be done once.

```
$ sudo docker-compose build
$ sudo docker-compose up
```

After deploying the environment access to the ”api” docker container in order to create a new user on the framework using docker exec. The ”api” container ID can be checked using docker ps.

```
$ sudo docker exec -it <container_ID> /bin/bash
```

In the container, use manage.py script to create a super user.

```
$ ./manage.py createsuperuser
```

Finally access to ”http://127.0.0.1:9084/” using a web browser and log in the web application.