Desarrollo Seguro de Aplicaciones Web con OWASP

Lab: Preparación del Laboratorio para el Análisis de Vulnerabilidades en Aplicaciones Móviles

Objetivo

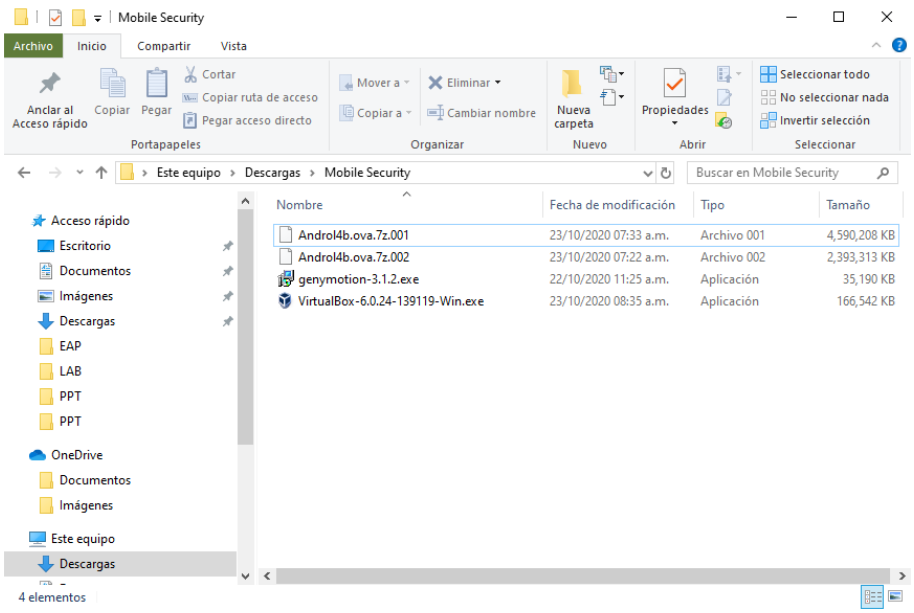
- Preparar las herramientas necesarias para analizar vulnerabilidades en aplicación móviles desarrolladas en Android.

Procedimiento

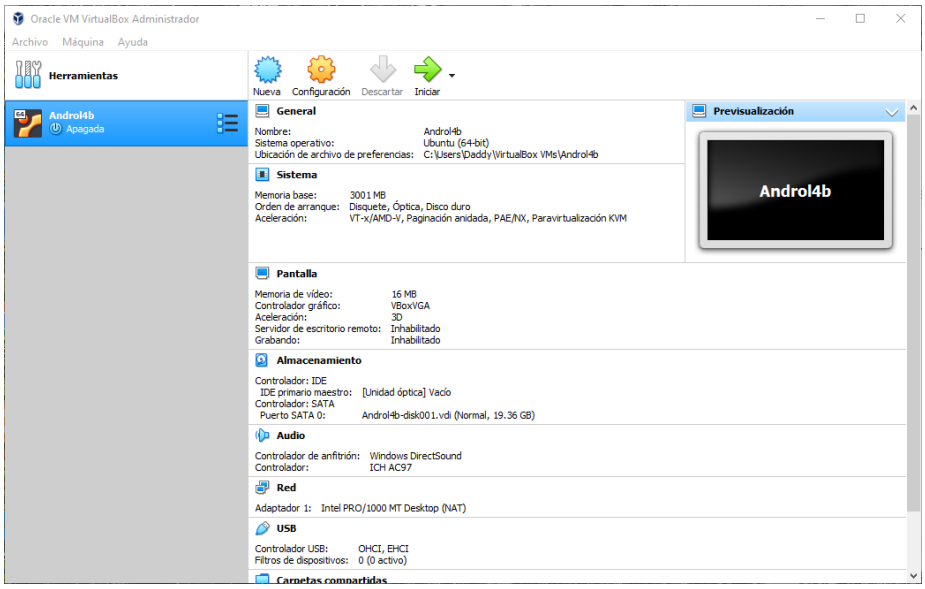
1. Descargar el software necesario para preparar las máquinas virtuales del laboratorio.

    - Oracle Virtual Box 6.0.24
    - Genymotion 3.1.2
    - Androl4b

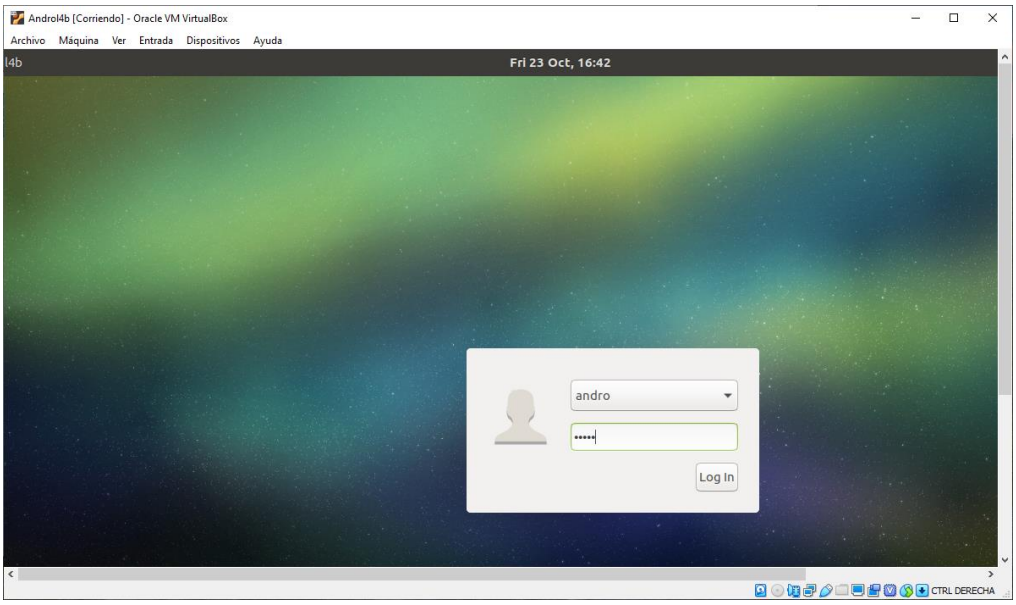
    Androl4b es una máquina virtual de seguridad de Android basada en ubuntu-mate que incluye la colección del último framework, tutoriales y laboratorios de diferentes expertos en seguridad e investigadores para la ingeniería inversa y el análisis de malware. Funciona bien en Oracle Virtual Box 6.0.24 (Julio,2020) pero tiene algunos problemas en VMWare y en las ultimas versión de Virtual Box. Descarga Androl4b desde: https://github.com/sh4hin/Androl4b



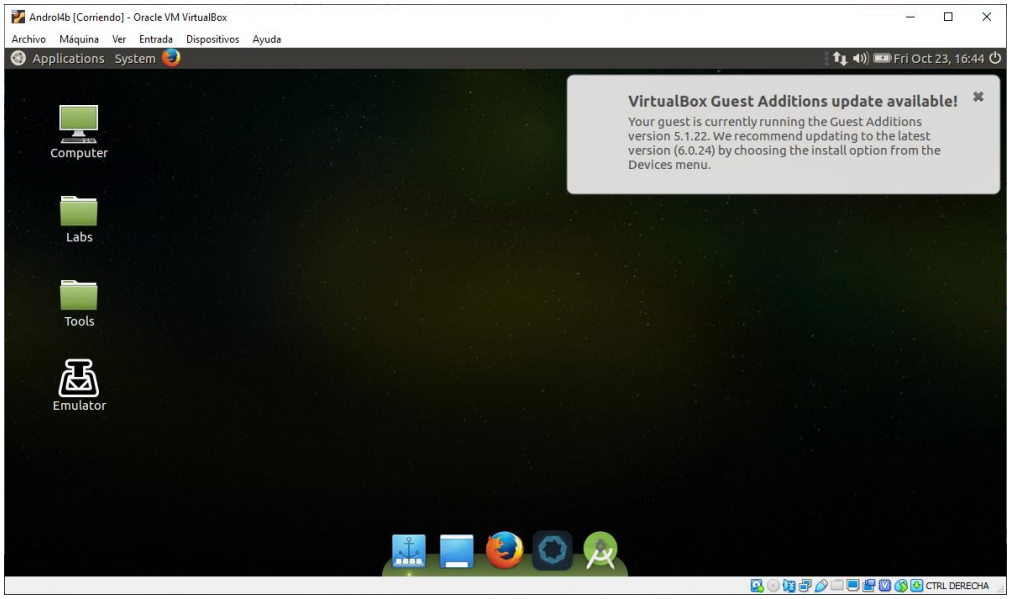
2. Importa la máquina virtual Androl4b en Virtual Box



3. Inicia la máquina virtual Androl4b, ingresa con la cuenta **andro** password **andro**.

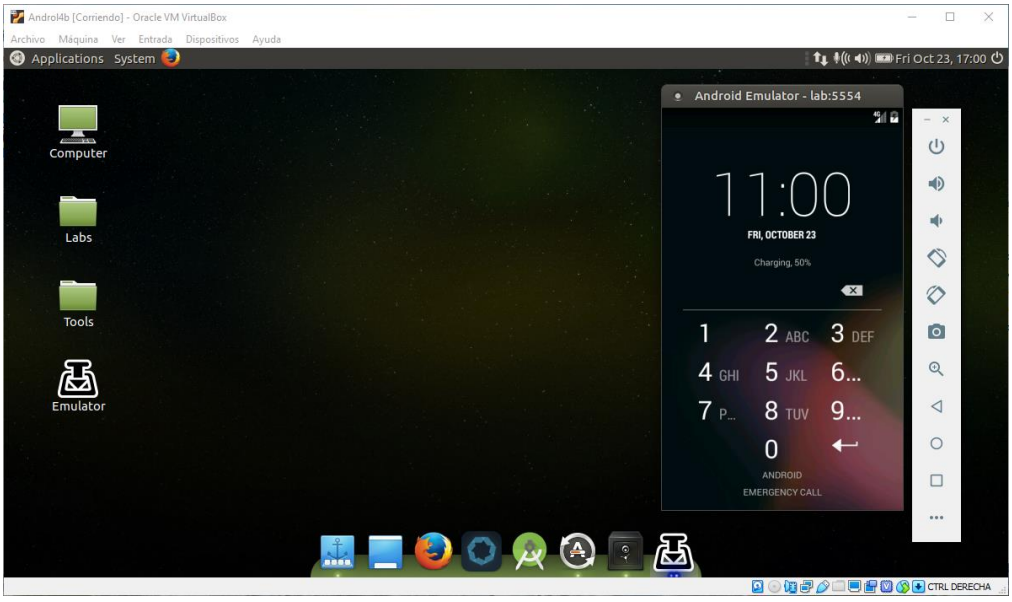


Clic en Login

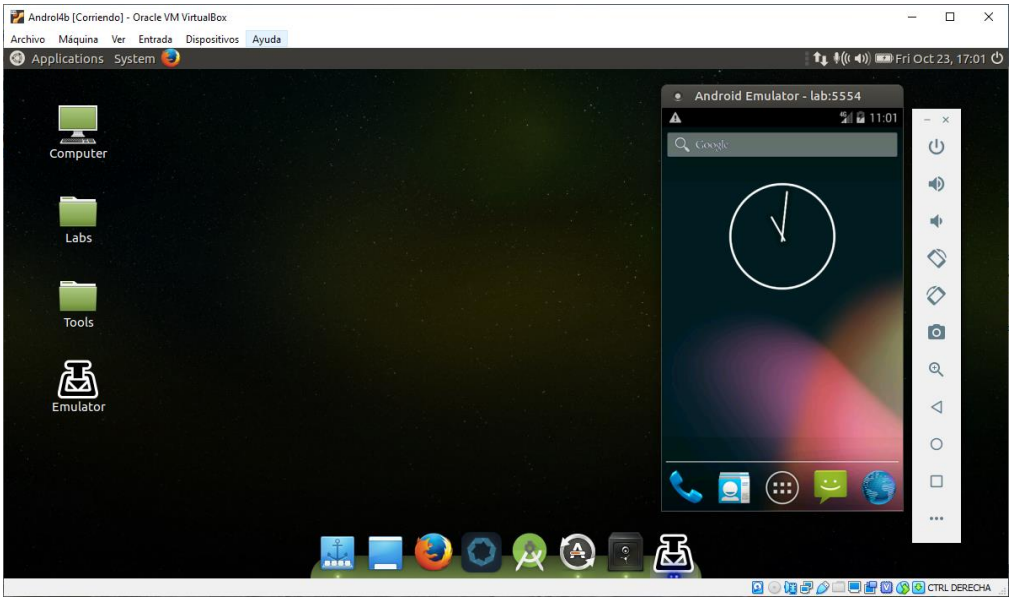


En este punto ya estamos casi listos.

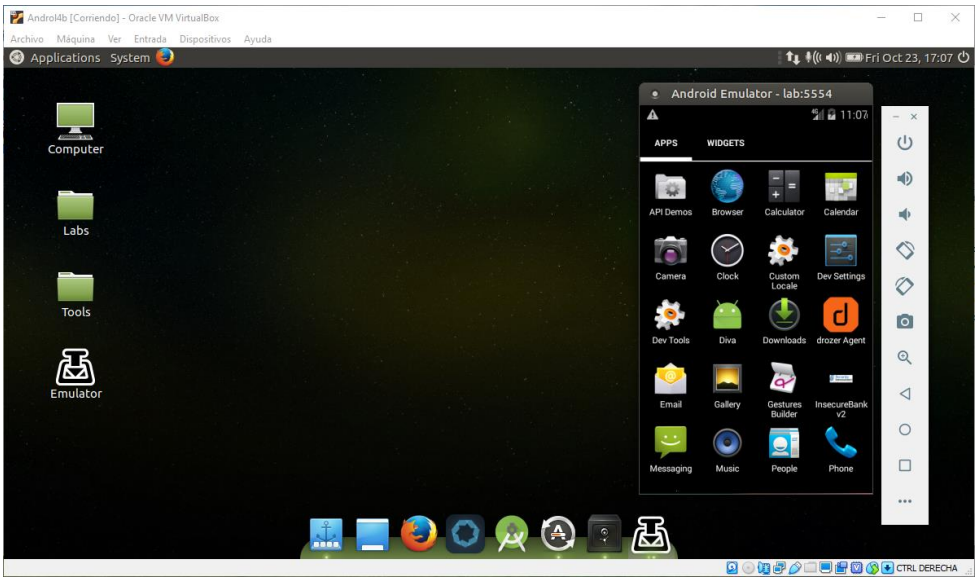
4. Inicia el emulador, haz clic en el icono del escritorio “Emulator”



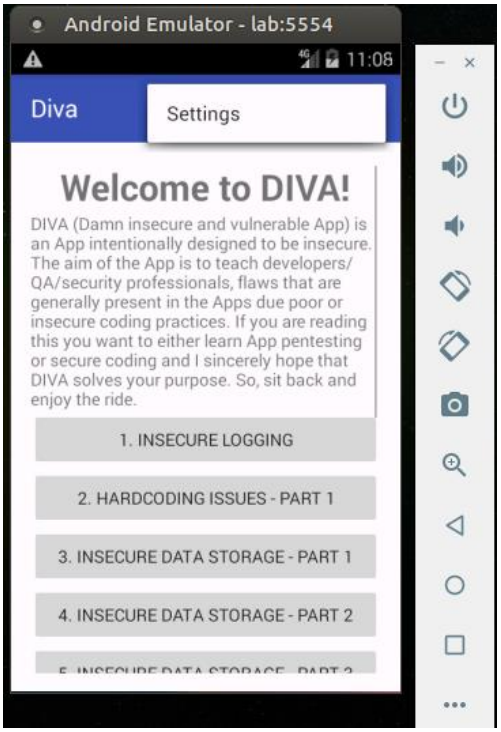
Ingresa el pin del dispositivo es 1234.



5. Abre la aplicacion DIVA (“Damm Insecure and Vulnerable App”) en el dispositivo. La aplicación DIVA es una aplicación demo que tiene un conjunto de vulnerabilidades que descubriremos.



Haz clic en Diva, para ver la interface de la aplicación.



6. Accediendo a las fuentes de la aplicación DIVA. Abre un terminal y activa el directorio que contiene el código fuente de la aplicación.