El objetivo de este TFM consiste en crear una distribución linux orientada a la obtención de información en la red.

La distribución debe consistir en un fichero .ova virtualizado en el que se incluyan las herramientas vistas a lo largo de las diferentes actividades colaborativas realizadas en el módulo, tomando como base una distribución genérica limpia como Ubuntu o Debian.

Se deberá incluir una memoria de las herramientas incluidas en función de su área de utilidad, así como un script de instalación de las herramientas con los comandos a ejecutar seguidos.

Atajos del teclado

Accesos rápidos.

Añadir Konsole para poder abrir un terminal con Ctrl+Alt+T

**XUNIL TOOLS OSINT**

Luis Fernández Zuñiga

Campus Internacional - CIBERSEGURIDAD

**Resumen.** SDADADa FDSAFASDF asfdfasdf asfdasdfsadfsd fsadfsdfasf sfasdfsdfsdfasd fsda sd sadf dfsa sdf sadf asdf sadf sdf sdf sdsdfsad s sfsdf asd fsd

**Palabra Clave:** sda fasdf sdf

# Introducción

## Marco del proyecto

Este Trabajo de Fin de Master (TFM) consiste en la realización del diseño, XUNIL OSINT TOOLS, de una distribución orientada a la obtención de información en la red tomando como base una distribución GNU/Linux gratuita y de código abierto en este caso DEBIAN 12 [1] versión 12.4.0 para su posterior instalación en VMware® Workstation 15 Pro [2]. El escritorio elegido es KDE PLASMA por ser muy parecido al escritorio de Windows.

El sistema por defecto viene con la versión 3.11.2 de Python, así que todos los programas aquí instalados funcionan sobre dicha versión.

## Motivación

Mostrar los procesos a seguir para crear un entorno de trabajo personalizado, para que cualquiera pueda crear su propio entorno y mantenerlo a su gusto.

Existe numerosas distribuciones lista para su uso, pero ninguna muestra los pasos que hay que seguir para el resultado final.

Por lo que se propone no un sistema más, sino enseñar todos los procedimientos para que cada usuario pueda modificar e integrar las herramientas que más le guste.

## Objetivo

El principal objetivo es mostrar los pasos a seguir para configurar desde cero un sistema operativo básico en un entorno personalizado de trabajo, en nuestro caso con la instalación de los programas necesario para una investigación OSINT.

## Desarrollo del proyecto

El proyecto se divide en los siguientes apartados.

1. Descarga de los programas principales
2. Instalación del sistema operativo
3. Configuración del entorno
4. Descarga del repositorio
5. Creación del menú principal para la instalación de subprogramas
6. Configuración del escritorio
7. Creación del fichero de distribución

### Descarga de los programas principales



Se va a efectuar una instalación en un entorno virtual con VMware que se obtiene desde el repositorio GITHUB <https://github.com/laprise2023/Xunil-Osint-Tools/tree/main/VMware15>

El sistema operativo elegido es la versión de DEBIAN 12 versión 12.4.0 que se puede obtener en <https://www.debian.org/download>

### Instalación del sistema operativo



Tras la instalación de VMware se realiza la instalación del sistema operativo que se puede ver en el siguiente enlace <https://www.youtube.com/watch?v=2tnYtuiS01U>

### Configuración del entorno

La configuración del entorno consiste en personalizar la pantalla de inicio, el fondo de escritorio, los enlaces directos mostrado en el escritorio, asi como la barra de inicio, etc….

Lo primero que tenemos que hacer una vez finalizada la instalación del sistema operativo es ingresar nuestras credenciales para acceder a la pantalla principal

#### Acceso con usuarios

Existe en este primer momento dos usuarios. El primero es el usuario que hemos configurado durante la instalación, en nuestro caso “*xunil*” cuya clave de acceso es “linux” y el segundo el el superusuario -root- tiene como contraseña de acceso “12345” .

Se recomiendo siempre que se trabajo sobre un usuario y en pocas ocasión se utiliza el usuario -root-.

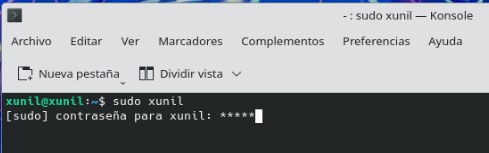
#### Configuración privilegios usuario

Por defecto nuestro usuario no tiene lo privilegios de un superusuario pero esto lo resolvemos de la siguiente manera. Abrimos una terminal (Konsole) y escribimos

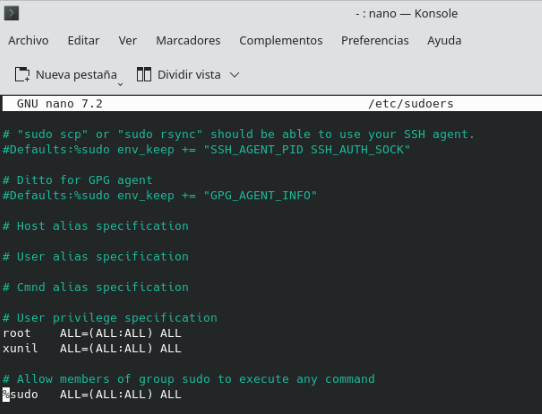
*Su -l*

Introducimos la contraseña del Root -> 12345 y editamos el fichero “/etc/sudoers”

A mi me gusta que cuando tecleo una contraseña me aparezca asteriscos. Si a continuación de “Defaults env\_reset” escribimos “,pwfeedback” lo



Pero lo importante es añadir a continuación de ”*root*” nuestro usuario con los mismo privilegios que el administrador.



No olvidar de grabar el fichero <Ctrl+O> y <Ctrl+x> para salir.

#### Acceso automático

Como la distribución de este sistema esta enfocado exclusivamente en OSINT, podemos si lo deseamos eliminar la pantalla de bloqueo/acceso principal y que el sistema arranque automáticamente en el entorno del usuario “*xunil*”.

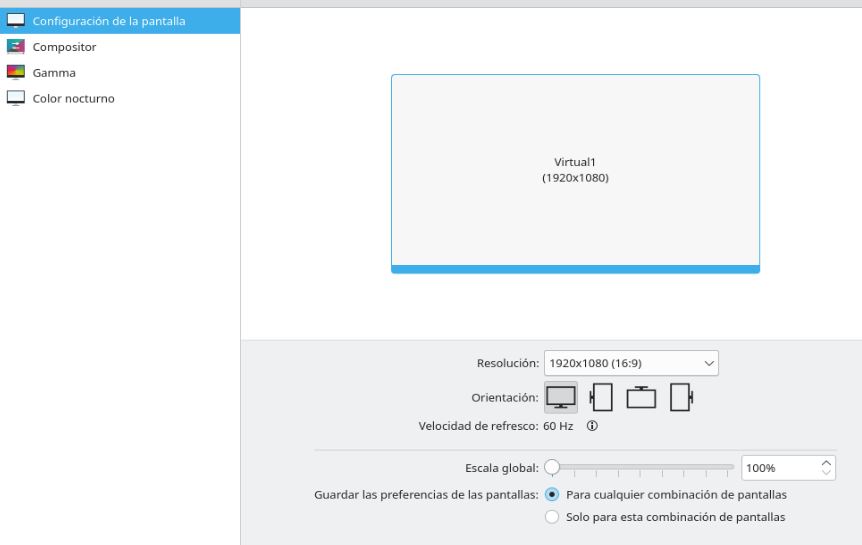
Para hacerlo nos dirigimos a modificar “Comportamiento del Arranque”



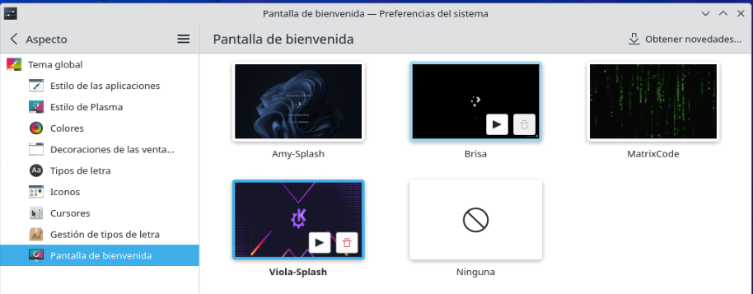
Donde seleccionamos y activamos la pestaña “*Iniciar sesión automáticamente*” se nos pedirá la contraseña para archivarla para su posterior uso del sistema.

#### Configuración pantalla

Para que todo se vea adecuadamente las imágenes están en una resolución de 1920x1080 pixeles, y por lo tanto tenemos que adecuar la resolución de la pantalla a esa resolución.



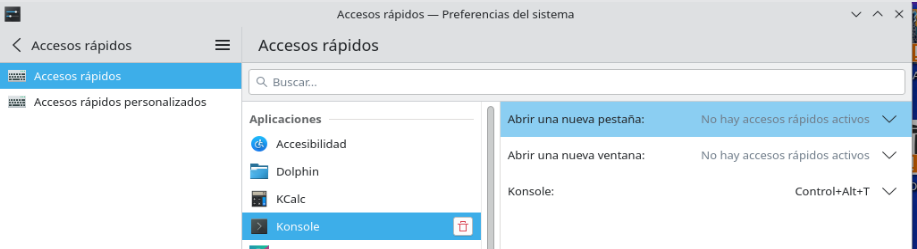
#### Personalizar pantalla de bienvenida



#### Se selecciona la pantalla que mas de adecue a nuestras necesidades

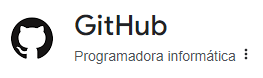
#### Configuración acceso rápidos

Como vamos a utilizar con mucha frecuencia el Terminal del sistema en nuestro caso “*Konsole”* vamos a configurar un acceso rápido por teclado, lo que resultara muy cómodo y rapido. Para eso no vamos al lanzador de aplicaciones seleccionamos “*Preferencias*” y en el apartado “Accesos rápidos” “*Añadir aplicación*” buscamos “*Konsole*” y comprobamos que el acceso es “Ctrl+Alt+T”



### Descarga del repositorio

En este proyecto he alojado en el portal



**El cual permite presentar y compartir nuestro proyecto, así como seguir y administra** los cambios en el código a lo largo del tiempo en la siguiente dirección <https://github.com/laprise2023/Xunil-Osint-Tools>

Para su descarga que se efectúa en una consola/terminal se ejecuta las siguientes instrucciones.



#### Estructura del árbol de directorio

Tras la descarga del repositorio en nuestro sistema se creará la siguiente estructura de fichero que parte desde el directorio principal:

**XunilTools**

En el encontramos dos ficheros que nos permitirá continuar con nuestro proceso de personalización.

* ConfigGrub.sh -> Este script está diseñado para personalizar el cargador de arranque múltiple GRUB
* Configuracion.sh - > Script que instala todos los programas y pone los iconos en el escritorio.

**aplicaciones**

Contiene todos los scripts para lanzar las aplicaciones

* la carpeta – **iconos -** contiene los iconos que serán utilizados durante la creación de los enlaces directos presentados en el escritorio.

**escritorio**

los ficheros de configuración de los enlaces directos para su uso en el escritorio.

**Imagenes**

Contiene las imágenes que son usadas para nuestra personalización

**instalación**

En esta la carpeta se aloja el script “InstalaPrg.sh” el cual nos permitirá instalar los programas que usaremos en nuestras investigaciones OSINT.

Así como el programa webapp-manager, el cual se usará para crear los accesos directos en nuestro escritorio con los enlaces a las paginas web de nuestra elección para personalizar mas el entorno de trabajo.

* herramientas

en el se aloja varios directorios con los scripts de instalación de las aplicaciones, cada una en su subdirectorio correspondiente según esta clasificación.

* coorp -> ejemplo “Instalar\_maltego.sh”
* otras -> ejemplo “Instalar\_Telegram.sh”
* Personas
* Recursos
* Redes

Y todas las subdivisiones que creamos necesarias para organizar nuestros scripts de instalación.

**manuales**

Contiene los manuales de diferentes aplicaciones y utilidades

**otros**

Ficheros utilizados durante el proceso de configuración de GRUB

## Correos electrónicos

Los siguientes correos electrónicos son usados en algún momento de la instalación

[tfmosint2023@gmx.com](mailto:tfmosint2023@gmx.com) -> C@di72023

[laprise.adrien@mail.com](mailto:laprise.adrien@mail.com) -> C@di72023

[laprise.adrien2023@gmail.com](mailto:laprise.adrien2023@gmail.com) -> C@diz2023

## Twitter (X)

@LapriseAdr72086 -> C@di72023

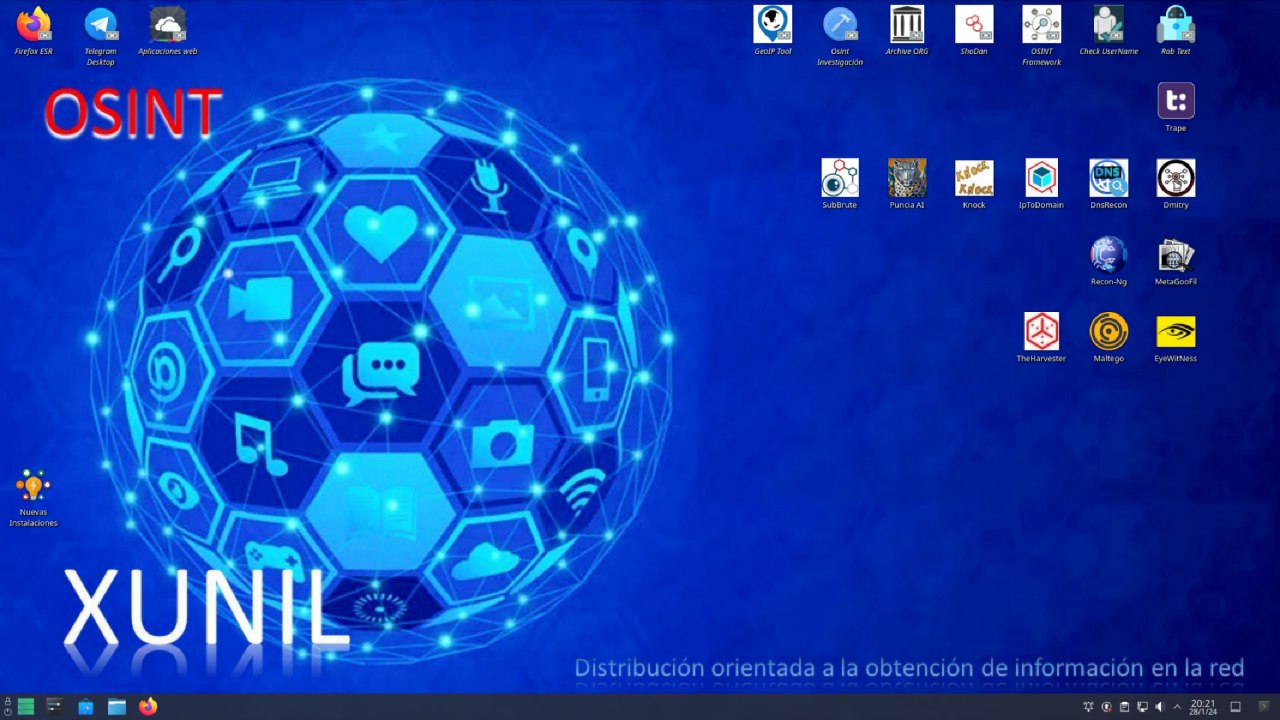
## Obtención de API’S

### Virustotal

Usurario: [laprise.adrien@mail.com](mailto:laprise.adrien@mail.com) -> C@diz2023

API: 8e4c76dd148a6bd06592b2deb97d1b3c6da59525cd3f6217c31824f58e42b31c

## Pantalla principal



# Programación

## ¿Qué es BASH?

Bash (Bourne again Shell) es el intérprete de comandos (shell) por defecto de los sistemas operativos basados en el kernel Linux y su función es proporcionar una interfaz en la cual el usuario introduce comandos que la shell interpreta y envía al núcleo (kernel) para que este ejecute las operaciones.

## ¿Qué es un Script?

Se le suele llamar script a una pieza de software que no necesita ser compilado para ser ejecutado. La mayor ventaja de los lenguajes interpretados es que pueden ser modificados en cualquier momento sin tener que pasar por procesos de compilación para probar los cambios, lo que nos permite testear nuestros programas rápidamente, facilitando la experimentación y el aprendizaje a través de una metodología de ensayo y error.

## Script para nuevas instalaciones

Este script “InstalaPrg.sh” permite seleccionar el programa que se desea instalar. El siguiente código permite ver como se realiza las operaciones, la cuales pueden ser modificada para añadir o suprimir cualquier programa que en un futuro se necesite.

#!/bin/bash

#Luis Fernández

# Con \e[ comienzas la secuencia

# x;y;zm definen el formato, color de texto y color de fondo.

# \e[m define el final de la secuencia.

# Así, la definición de colores se corresponde con la siguiente tabla,

# Texto Color texto Color fondo

# 0 – normal 30 – Negro 40 – Negro

# 1 – negrita 31 – Rojo 41 – Rojo

# 4 – subrayado 32 – Verde 42 – Verde

# 33 – Amarillo 43 – Amarillo

# 34 – Azul 44 – Azul

# 35 – Púrpura 45 – Púrpura

# 36 – Turquesa 46 – Turquesa

# 37 – Blanco 47 – Blanco

# Ahora ya es cuestión que pruebes todas las combinaciones que tu consideres, para personalizar y colorear la línea de comandos. Una observación, cada vez que comienzas una secuencia, utilizando \e[, sobrescribes el formato anterior. Y cuando terminas con \e[m, simplemente vuelves al estado por defecto. En mi caso, ese estado por defecto es texto en blanco y fondo negro. Y el formato de texto es normal.

## Script de instalación de una aplicación

Cada programa que se desea instalar dispone de un script que contiene los comandos necesarios para su instalación. Por ejemplo.

### Instalar\_puncia.sh

|  |
| --- |
| #!/bin/bash  #Luis Fernández  cd $HOME/XunilTools/  sudo git clone https://github.com/ARPSyndicate/puncia.git  cd puncia  sudo pip3 install --break-system-packages puncia  #puncia  cd $HOME/XunilTools/instalacion/ |

Una vez realizada la instalación se tiene que presentar un acceso directo en el escritorio para ello se tiene que escribir un script que lanzara dicha aplicación

## Script para lanzar una aplicación

Por ejemplo “puncia.sh” esta alojada en /home/xunil/XunilTools/aplicaciones/ contiene tres órdenes de ejecución

cambia al directorio donde se encuentra la aplicación

ejecuta el programa

mantiene la consola/terminal abierta

|  |
| --- |
| #!/bin/bash  #Luis Fernández  cd $HOME/XunilTools/puncia  puncia  $SHELL |

## Script para crear un enlace en el escritorio

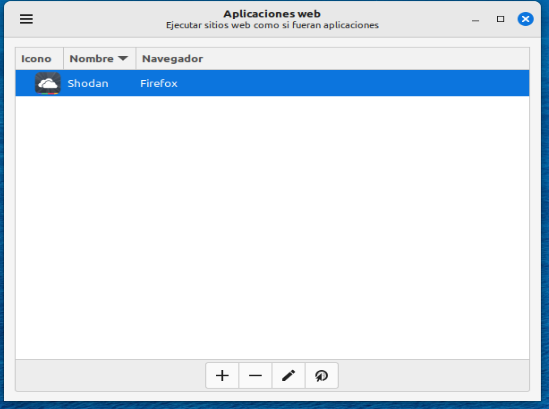
Los ficheros .desktop tiene una estructura especial con la cual se crea un icono en el escritorio para poder ejecutar el script del programa seleccionado

|  |
| --- |
| #!/usr/bin/env xdg-open  [Desktop Entry]  Comment[es\_ES]=Ejecutar Script puncia.sh  Exec=sh /home/xunil/XunilTools/aplicaciones/puncia.sh  GenericName[es\_ES]=  Icon=/home/xunil/XunilTools/aplicaciones/iconos/Puncia.png  MimeType=  Name[es\_ES]=Puncia AI  Path=/home/xunil/XunilTools/aplicaciones  StartupNotify=true  Terminal=true  TerminalOptions=  Type=Application  X-KDE-SubstituteUID=false  X-KDE-Username= |

## Script para lanzar una URL desde el escritorio

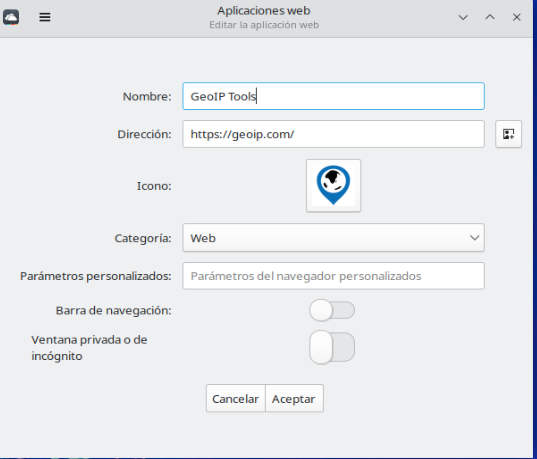
Se utiliza un programa WebApp Manager [3] el código fuente se encuentra en [GitHub - linuxmint/webapp-manager](https://github.com/linuxmint/webapp-manager). Fichero para su instalación se descarga desde <http://packages.linuxmint.com/pool/main/w/webapp-manager/>



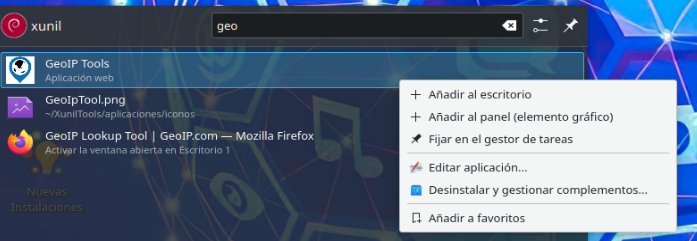


Esta aplicación genera una aplicación que desde el lanzador de programas se envía al escritorio

Vamos a realizar una instalación, por ejemplo



Tras seleccionar el icono poner la direccion WWW y el nombre damos a Aceptar.



A

ñadir al escritorio

# Aplicaciones con necesidad de identificación

## Análisis de Redes sociales

### Trape

NGROK

Usuario: laprise

Email address: laprise.adrien@mail.com

Current Password: C@diz2023

### Que es Trape

Trape fue creado con el objetivo de enseñar al mundo cómo las grandes empresas de Internet pueden obtener **información confidencial**, como el estado de las sesiones de sus sitios web, fue creado con el objetivo de enseñar al mundo cómo las grandes empresas de Internet pueden obtener información confidencial, como el estado de las sesiones de sus sitios web o servicios y el control sobre sus usuarios a través del navegador, sin que ellos lo sepan.

## Análisis de datos corporativos

### MALTEGO.sh

¿Qué es Maltego y cómo funciona?. Maltego es un servicio que tiene el poteNcial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc.

Por ejemplo, a la hora de buscar establecer contacto con una empresa, esta herramienta puede proporcionarnos datos muy útiles que nos facilitaría el contacto con esta empresa o persona, como la dirección de correo electrónico de recursos humanos, del departamento de ventas, de soporte técnico o el número telefónico. También ofrece la capacidad de encontrar distintos tipos de artículos, como son autos, motos, aviones, entre otros.

### Acceso Maltego Free

Usuario: [tfmosint2023@gmx.com](mailto:tfmosint2023@gmx.com) -> C@diz2023

<https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/d>

Activar aplicaciones dentro de Maltego

* Servicio Alien Vault OTx

Usuario: [laprise.adrien@mail.com](mailto:laprise.adrien@mail.com) -> C@diz2023

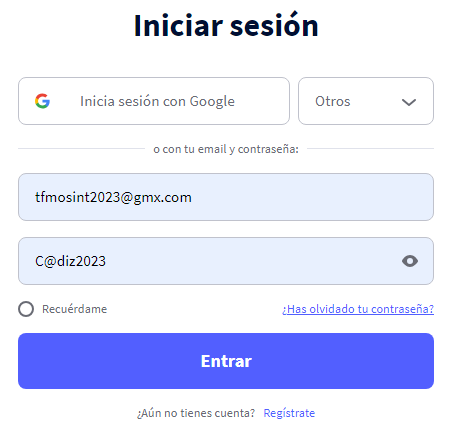
Api: 1f42b5bd8548e282da50a2a99dc9e522d134172e56ccfd4425795bd26b35988a

### SHODAN

Usuario: Laprise -> C@diz2023

# Utilidades en la Red

## GENIALLY



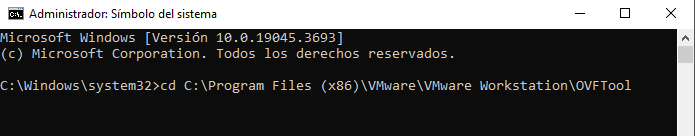
# Utilidades para crear .OVA

En el directorio C:\Program Files (x86)\VMware\VMware Workstation\OVFTool hay un programa ovftool.exe que sirve para transformar los ficheros de VmWare (.vmx) a ficheros (.ova)

Se abre una consola como administrador.

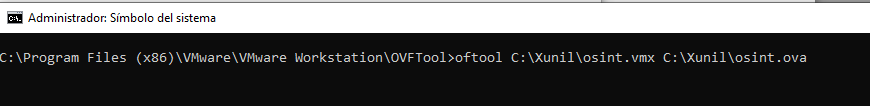


Se cambia de directorio a donde está el fichero OVTOOL



Se ejecuta el programa

* Ovftool <directorio seguido del nombre del fichero.vmx> <directorio de salida y el nombre del fichero.ova>

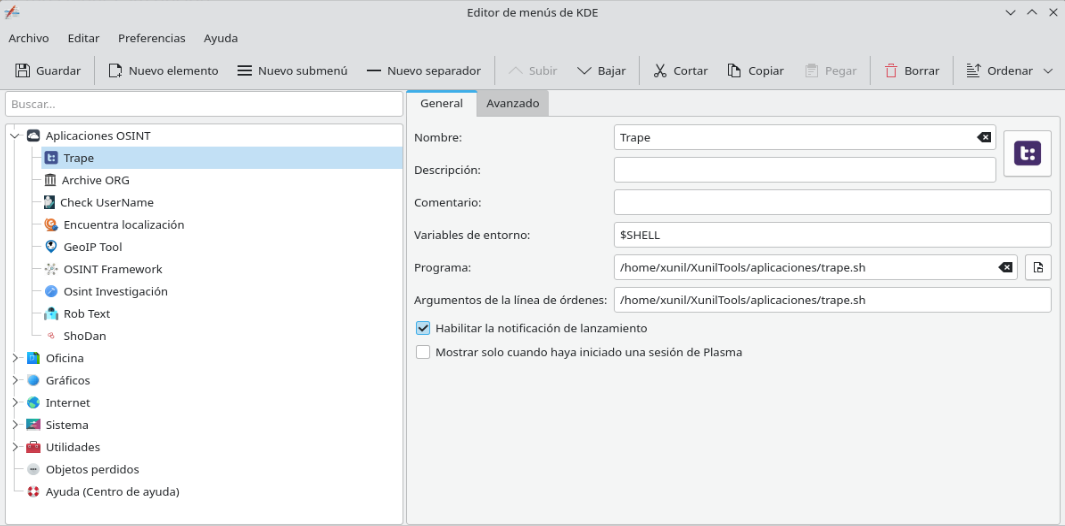


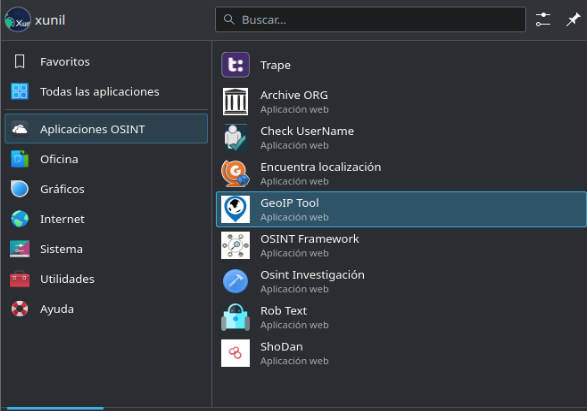
Fichero guardado en MEGA.nz

Usuario: [laprise.adrien@mail.com](mailto:laprise.adrien@mail.com) -> C@di72023

Clave recuperación: zbrMEUlwDEoTj5uEubvxOA

Editar lanzador de aplicaciones





# Referencias

|  |  |
| --- | --- |
| [1] | «Debian 12, codenamed bookworm,» para PC de 64 bits (amd64) debian-12.5.0-amd64-netinst.iso, [En línea]. Available: https://www.debian.org/download. |
| [2] | «VMware® Workstation 15 Pro,» [En línea]. Available: https://customerconnect.vmware.com/en/downloads/details?downloadGroup=PLAYER-1510&productId=800&rPId=55787. |
| [3] | «Descargar WebApp Manager,» [En línea]. Available: http://packages.linuxmint.com/pool/main/w/webapp-manager/. |