

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 asdfasdf asfdasdfsadfsd fsadfsdfasf sfasdfsdfsdfasd fsda sd sadf dfsa
sdf sadf asdf sadf sdf sdf sdsdfsad s sfsdf asd fsd

Palabra Clave: sda fasdf sdf

1 Introducción

1.1 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.

1.2 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.

1.3 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.

1.4 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. Pantalla principal
6. Creación de script. Programación
7. Creación del fichero de distribución

2 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>

3 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>

4 Configuración del entorno

La configuración del entorno consiste en personalizar la pantalla de inicio, el fondo de escritorio, los enlaces directos mostrados en el escritorio, así 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

4.1 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 superusuario -root- tiene como contraseña de acceso “12345”.

Se recomienda siempre que se trabaje sobre un usuario y en pocas ocasiones se utiliza el usuario -root-.

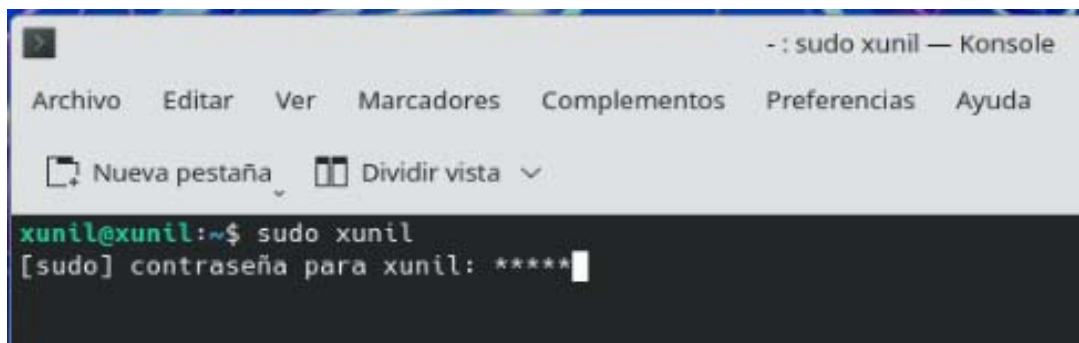
4.2 Configuración privilegios usuario

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

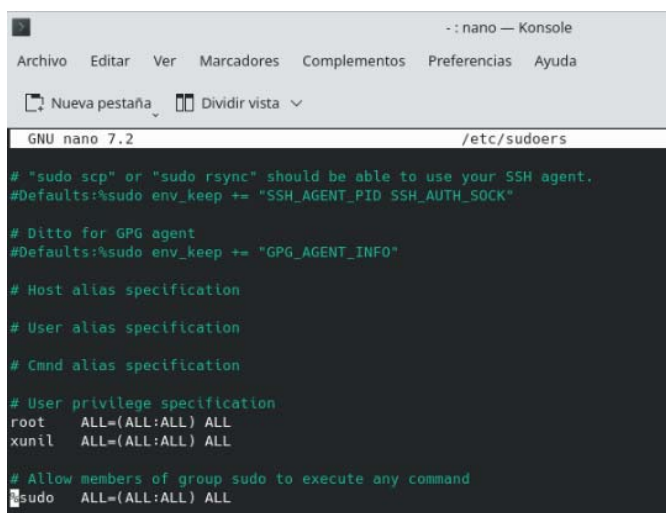
```
Su -l
```

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

A mí me gusta que cuando tecleo una contraseña me aparezca asteriscos. Si a continuación de “Defaults env_reset” escribimos “pwfeedback” lo

A screenshot of a Konsole terminal window. The title bar reads "- : sudo xunil — Konsole". The menu bar includes "Archivo", "Editar", "Ver", "Marcadores", "Complementos", "Preferencias", and "Ayuda". Below the menu bar are icons for "Nueva pestaña" and "Dividir vista". The terminal content shows a prompt "xunil@xunil:~\$" followed by the command "sudo xunil". The next line shows the prompt "[sudo] contraseña para xunil:" followed by five asterisks "*****" and a cursor.

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

A screenshot of a nano editor window editing the file "/etc/sudoers". The title bar reads "- : nano — Konsole". The menu bar includes "Archivo", "Editar", "Ver", "Marcadores", "Complementos", "Preferencias", and "Ayuda". Below the menu bar are icons for "Nueva pestaña" and "Dividir vista". The terminal content shows the following text:

```
GNU nano 7.2 /etc/sudoers

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
xunil    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

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

4.3 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”.

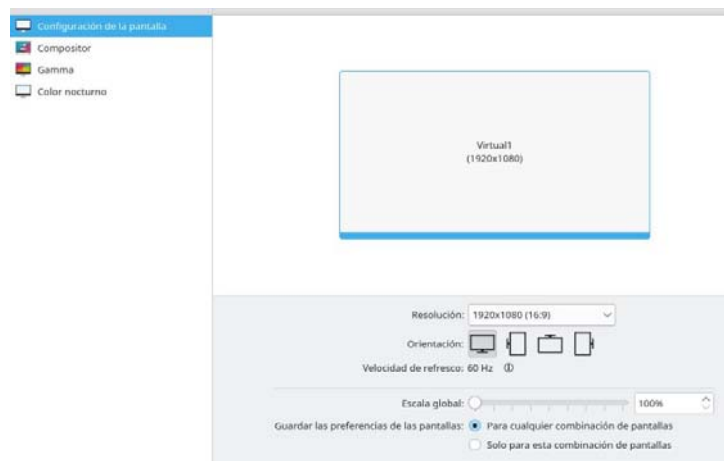
Para hacerlo nos dirigimos a modificar “Comportamiento del Arranque”



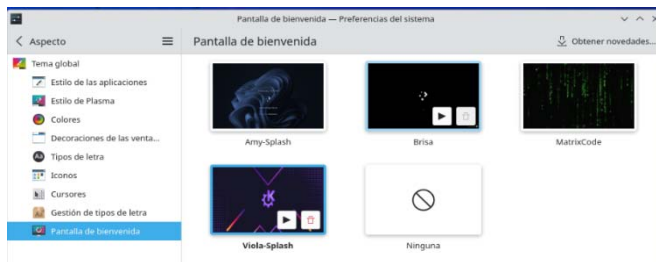
Donde seleccionamos y activamos la pestaña “Iniciar sesión automáticamente” se nos pedirá la contraseña para archivarla para su posterior uso del sistema.

4.4 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.



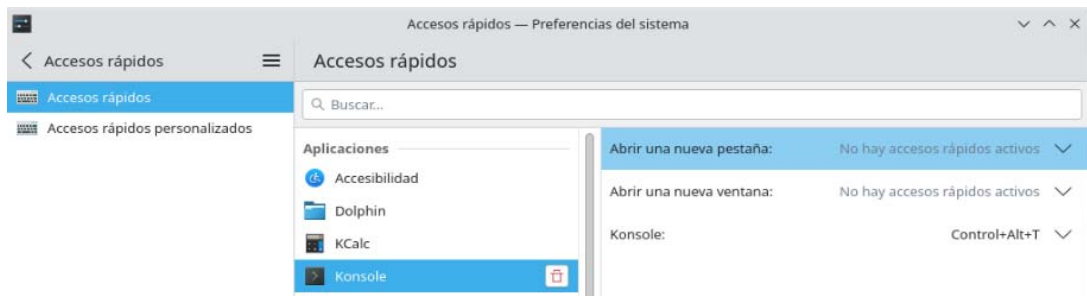
4.5 Personalizar pantalla de bienvenida



Se selecciona la pantalla que mas de adecue a nuestras necesidades

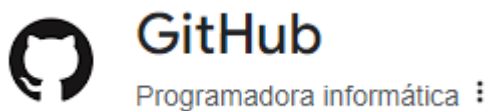
4.6 Configuración acceso rápidos

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*”



5 Descarga del repositorio

En este proyecto he alojado en el portal

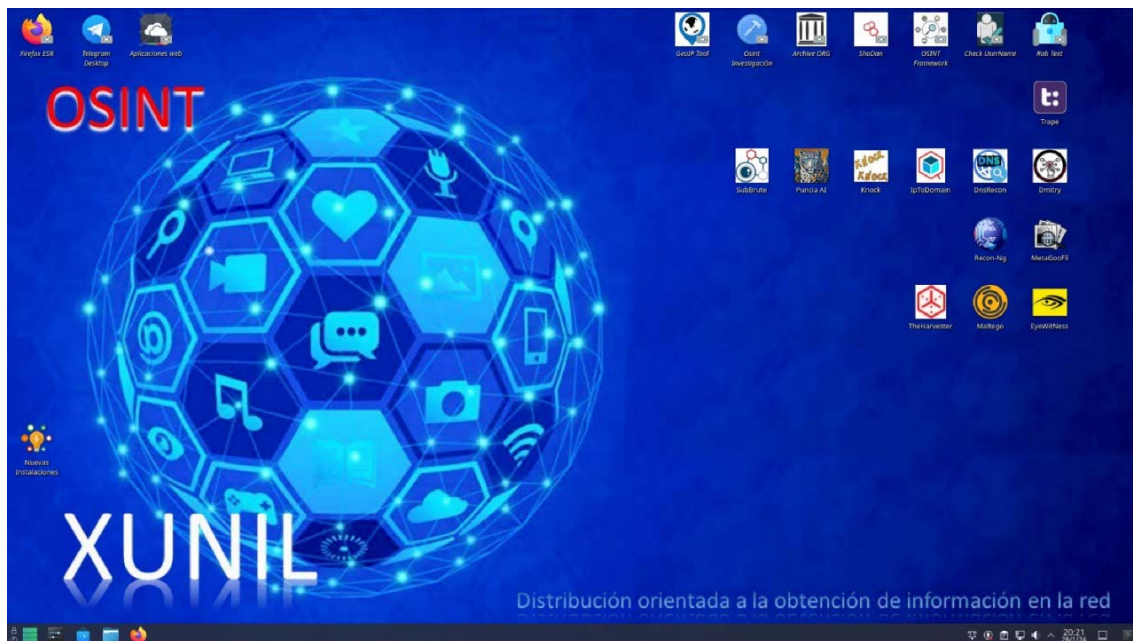


El cual permite presentar y compartir nuestro proyecto, así como seguir y administra los cambios en el código a lo largo del tiempo en la siguiente dirección <https://github.com/laprise2023/Xunil-Osint-Tools>

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

```
sudo apt install git
git clone https://github.com/laprise2023/Xunil-Osint-Tools.git ~/XunilTools
```

5.1 Pantalla principal



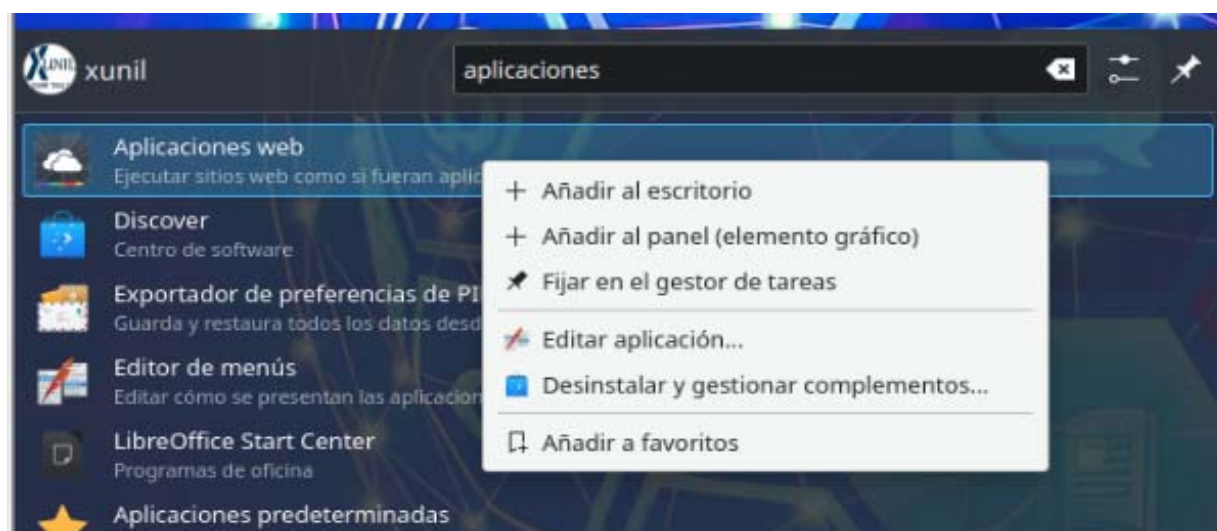
Nuestra pantalla principal presenta una imagen de fondo personalizada con sus iconos de enlaces directos a nuestras aplicaciones preferidas.

Nuestro escritorio presenta tres tipos diferente de enlaces directos.

1. Enlaces directos de programas instalados por el sistema operativo. Por ejemplo, el navegador Firefox.
2. Enlaces directos creados por nosotros, por ejemplo, Trape.
3. Enlaces directos a páginas WEB creado a través de la aplicación WebApp Manager, por ejemplo, Archive Org.

5.2 Enlace directo creado por el sistema operativo.

Es la forma más común de crear los iconos en el escritorio.



Se selecciona el fichero que deseamos agregar al escritorio y pulsamos sobre “+ *Añadir al escritorio*”. De esta forma se creara un fichero .desktop conteniendo las instrucciones e icono por defecto de la aplicación.

5.3 Programación. Creación de script

5.3.1 ¿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. En el directorio “/home/xunil/XunilTools/manuales/” dispone de varios manuales.

5.3.2 ¿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.

5.3.3 Script para nuevas instalaciones

El script “/home/xunil/XunilTools/instalacion/InstalaPrg.sh” nos muestra un menú principal donde seleccionar el programa que se desea instalar, el cual puede ser modificado para añadir o suprimir los programas para adecuarse a las necesidades de cada usuario.

5.3.4 Script de instalación de una aplicación

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

5.3.4.1 Ejemplo de instalación

En el directorio “/home/xunil/XunilTools/instalacion/herramientas/recursos/” se encuentra el script “Instalar_puncia.sh” que contiene las instrucciones para una instalación automatizada del programa.

```
#!/bin/bash
#Luis Fernández

# Cambio al directorio principal
cd $HOME/XunilTools/

#Clonar el repositorio alojado en github del programa en cuestion
sudo git clone https://github.com/ARPSyndicate/puncia.git

# Se posiciona sobre el directorio creado conteniendo el programa
cd puncia

# instruccion para su instalación
sudo pip3 install --break-system-packages puncia

# información como se puede ejecutar el programa
#puncia

# Vuelta al menu de instalación para poder continuar con la
# instalación de nuevo programas
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

5.3.4.2 Script para lanzar una aplicación

En el directorio “/home/xunil/XunilTools/aplicaciones/” se aloja el programa *puncia.sh* que contiene las instrucciones para poder ser lanzado el programa.


```
#!/bin/bash
#Luis Fernández

# Se posciona sobre el directorio donde se encuentra el programa
# que deseamos ejecutar
cd $HOME/XunilTools/puncia

# Orden de ejecución del programa
puncia

# Mantener la ventana Terminal abierta
$SHELL
```

5.3.4.3 Script para crear un icono con el enlace directo en el escritorio

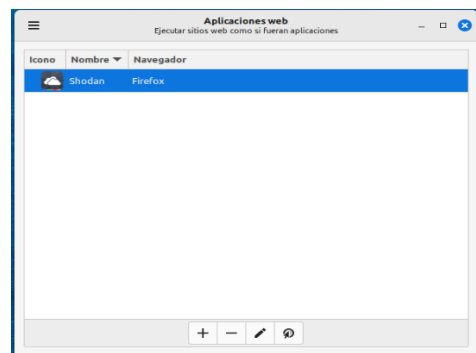
Un archivo DESKTOP es un acceso directo de la aplicación (entrada de escritorio) que se usa en entornos de escritorio. Este archivo se aloja en el siguiente directorio “/home/xunil/Escritorio” y contiene texto que define el tipo de acceso directo, el nombre, la ruta del archivo de iconos, las acciones, la versión de la aplicación y una ruta al ejecutable real, etc. Este archivo ejecuta una aplicación cuando un usuario hace doble clic en él. Hay que crear tanto acceso como sea necesario para tener un escritorio personalizado.

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

5.4 Enlace a una URL desde el escritorio

Se utiliza un programa WebApp Manager [3] cuyo repositorio se encuentra en [GitHub - linuxmint/webapp-manager](https://github.com/linuxmint/webapp-manager).

Para su instalación se realiza la descarga desde el enlace “<http://packages.linuxmint.com/pool/main/w/webapp-manager/>” donde se puede elegir la versión que mas nos interese



Con esta aplicación se genera un fichero que se integra en el sistema operativo y que como tal hay que enviarlo como en el apartado 5.2 al escritorio principal. Y de esta forma crear tantos enlaces como sean necesarios para tener en el escritorio todas las herramientas que mas nos guste.

6 Aplicaciones con necesidad de identificación

6.1 Análisis de Redes sociales

6.1.1 Trape

NGROK

Usuario: laprise

Email address: laprise.adrien@mail.com

Current Password: [C@diz2023](#)

6.1.2 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.

6.2 Análisis de datos corporativos

6.2.1 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.

6.2.2 Acceso Maltego Free

Usuario: 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 -> C@diz2023

Api: 1f42b5bd8548e282da50a2a99dc9e522d134172e56ccfd4425795bd26b35988a

6.2.3 SHODAN


Usuario: Laprise -> C@diz2023

7 Utilidades en la Red

7.1 GENIALLY

Iniciar sesión

 Inicia sesión con Google

Otros 

o con tu email y contraseña:



☐ Recuérdame [¿Has olvidado tu contraseña?](#)

Entrar

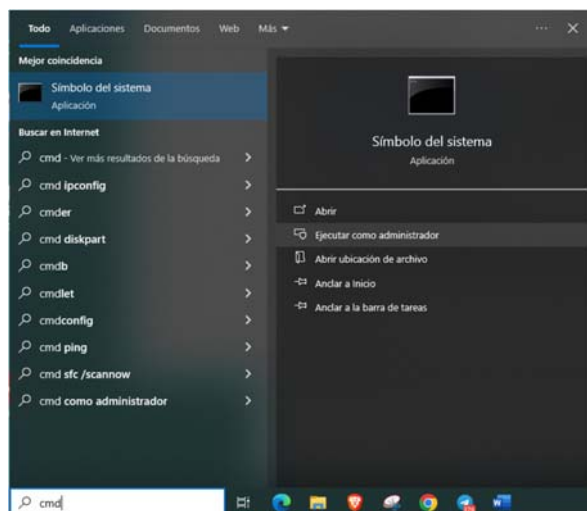
[¿Aún no tienes cuenta? Regístrate](#)

8 Utilidades para crear .OVA

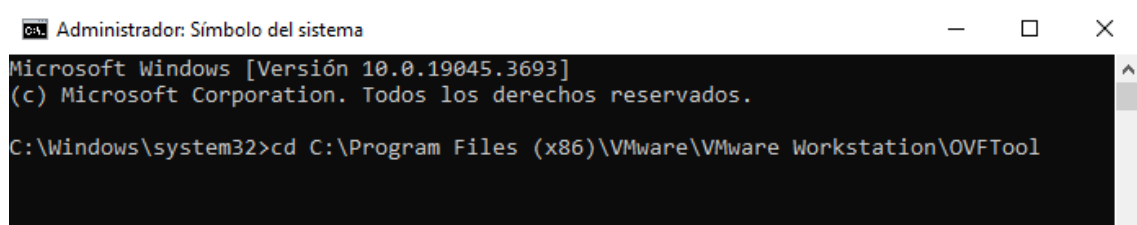
En el directorio C:\Program Files (x86)\VMware\VMware Workstation\OVFTool hay un programa ovftool.exe que sirve para transformar los ficheros de VmWare (.vmx) a ficheros (.ova)

Se abre una consola como administrador.

Se cambia
fichero OVTOOL

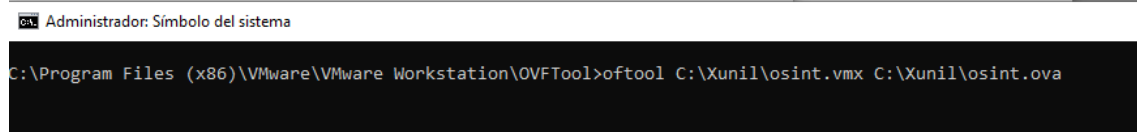


de directorio a donde está el



Se ejecuta el programa

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

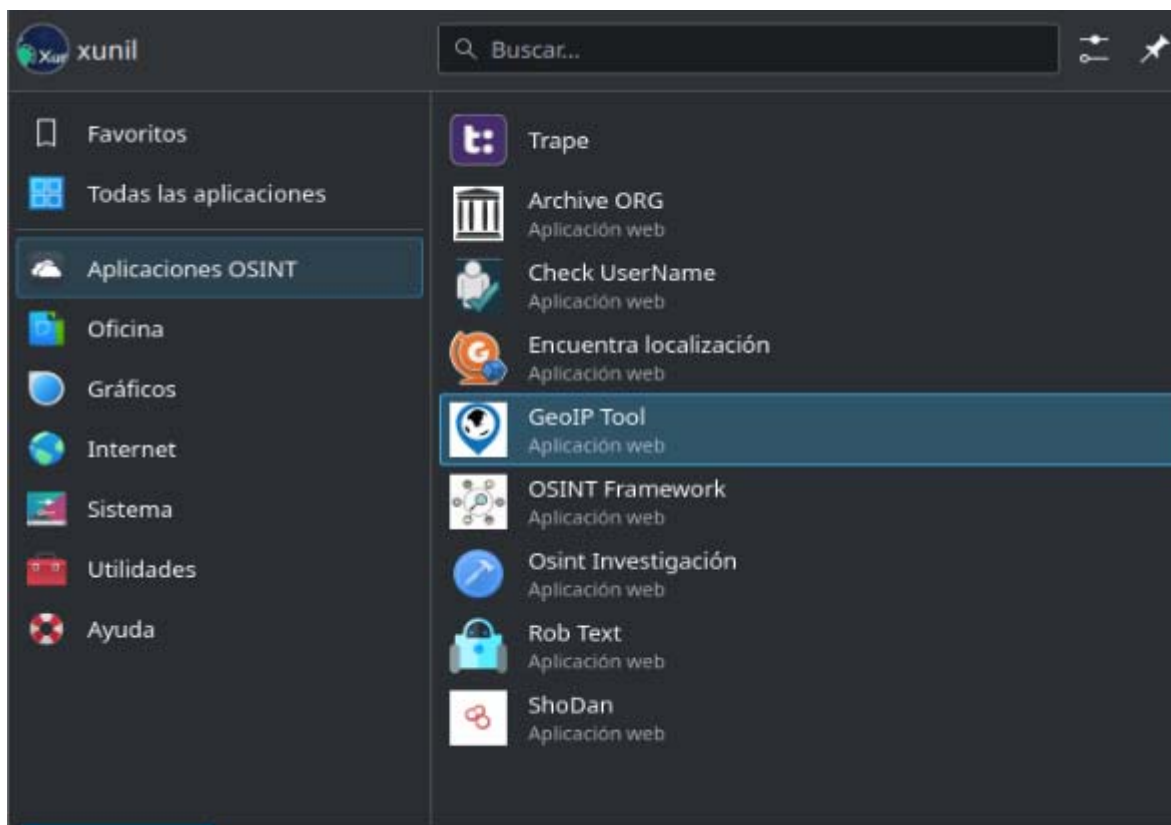
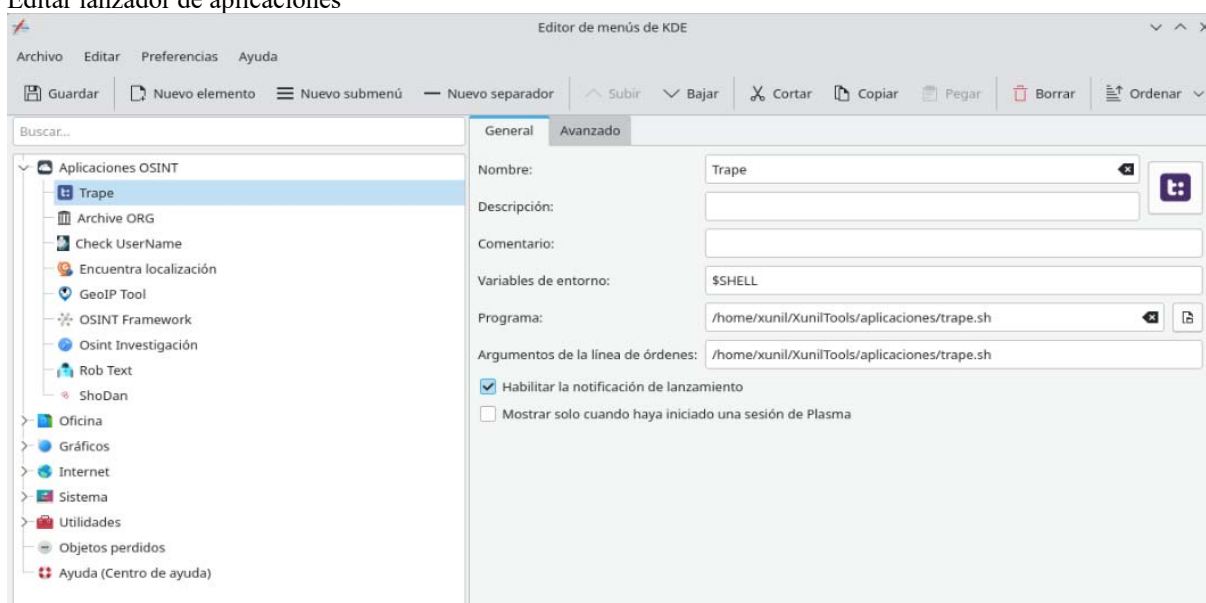


Fichero guardado en MEGA.nz

Usuario: laprise.adrien@mail.com -> C@di72023

Clave recuperación: zbrMEUlwDEoTj5uEubvxOA

Editar lanzador de aplicaciones



8.1 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.

Imágenes

Contiene las imágenes necesarias para configurar el entorno personal.

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, creara los accesos directos de los enlaces a las páginas web de nuestra elección.

- herramientas
Se divide varios directorios conteniendo los scripts de instalación de las aplicaciones.
 - coop -> 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

8.2 Correos electrónicos

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

tfmosint2023@gmx.com -> C@di72023

laprise.adrien@mail.com -> C@di72023

laprise.adrien2023@gmail.com -> C@diz2023

8.3 Twitter (X)

@LapriseAdr72086 -> C@di72023

8.4 Obtención de API'S

8.4.1 Virustotal

Usuario: laprise.adrien@mail.com -> C@diz2023

API: 8e4c76dd148a6bd06592b2deb97d1b3c6da59525cd3f6217c31824f58e42b31c

9 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/>.

