

XUNIL TOOLS OSINT

Luis Fernández Zuñiga
Campus Internacional - CIBERSEGURIDAD

Resumen. Creación personalizada de una distribución Linux comentada paso a paso.

Palabra Clave: Linux, Osint

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.

1.3 Objetivo

El principal objetivo es exponer los pasos a seguir para configurar desde cero un sistema operativo Linux básico y convertirlo en un entorno personalizado de trabajo.

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. Configuración del escritorio

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 **superusuario -root-** tiene como contraseña de acceso “12345”. Se recomienda siempre que se trabaje sobre un usuario y en pocas se utilice el usuario -root-.

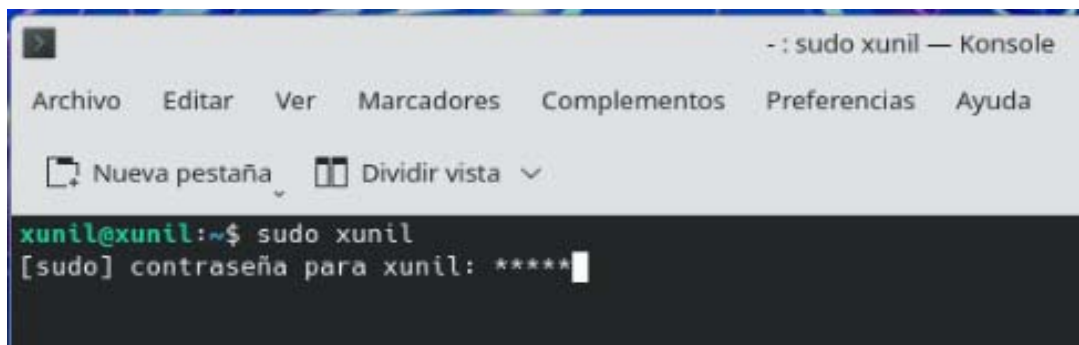
4.2 Configuración privilegios usuario

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
```

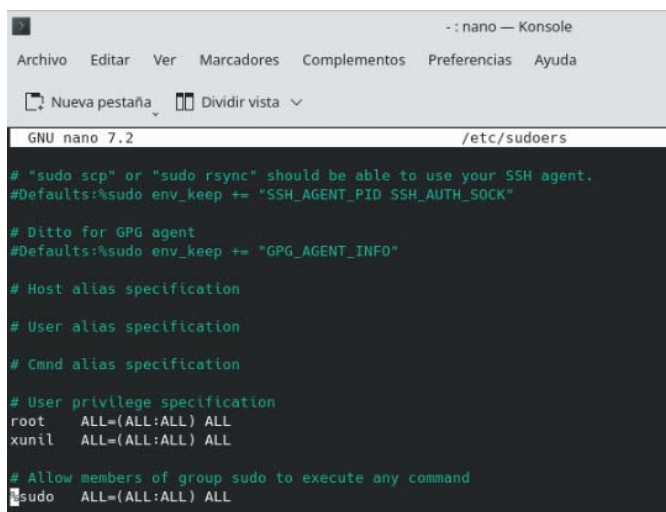
Introducimos la contraseña del Root -> 12345 y editamos el fichero “/etc/sudoers”

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



```
- : sudo xunil — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
Nueva pestaña  Dividir vista
xunil@xunil:~$ sudo xunil
[sudo] contraseña para xunil: *****
```

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



```
- : nano — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
Nueva pestaña  Dividir vista
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”.

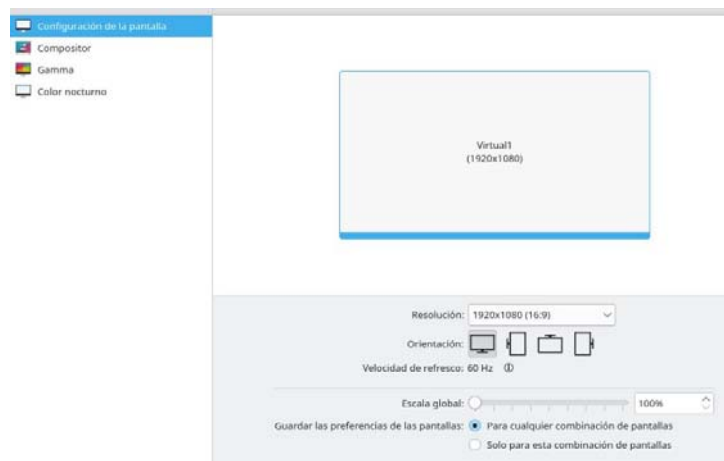
Para hacerlo nos dirigimos a modificar “Comportamiento del Arranque”



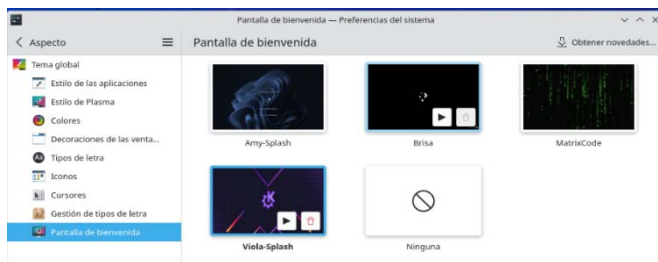
Donde seleccionamos y activamos la pestaña “*Iniciar sesión automáticamente*” se nos pedirá la contraseña para archivarla para su posterior uso del sistema.

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.



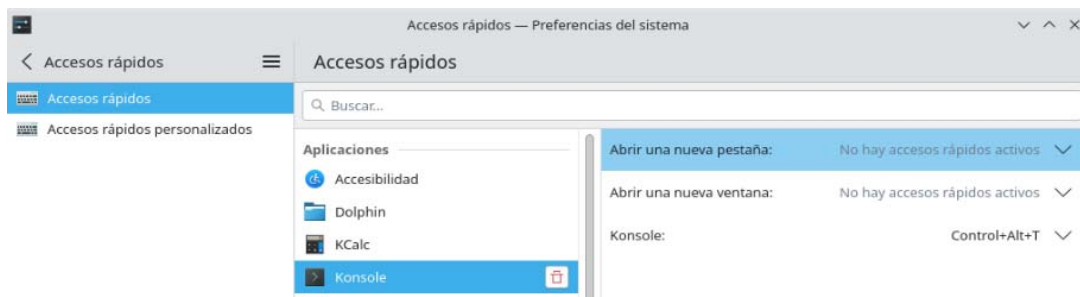
4.5 Personalizar pantalla de bienvenida



Se selecciona la pantalla que mas de adecue a nuestras necesidades

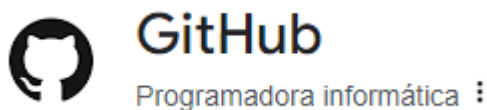
4.6 Configuración acceso rápidos

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
```

6 Programación. Creación de script

6.1 ¿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.

6.2 ¿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.

6.3 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.

6.3.1 Script de instalación de una aplicación

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

6.3.2 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
```

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

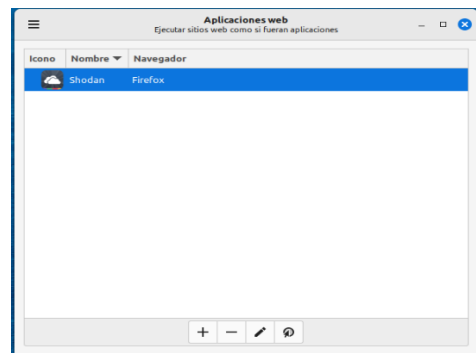
Un archivo DESKTOP es un acceso directo de la aplicación (entrada de escritorio) que se usa en entornos de escritorio. Este archivo se aloja en el siguiente directorio “/home/xunil/Escritorio” y contiene texto que define el tipo de acceso directo, el nombre, la ruta del archivo de iconos, las acciones, 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
```

6.4 Enlace a una URL desde el escritorio

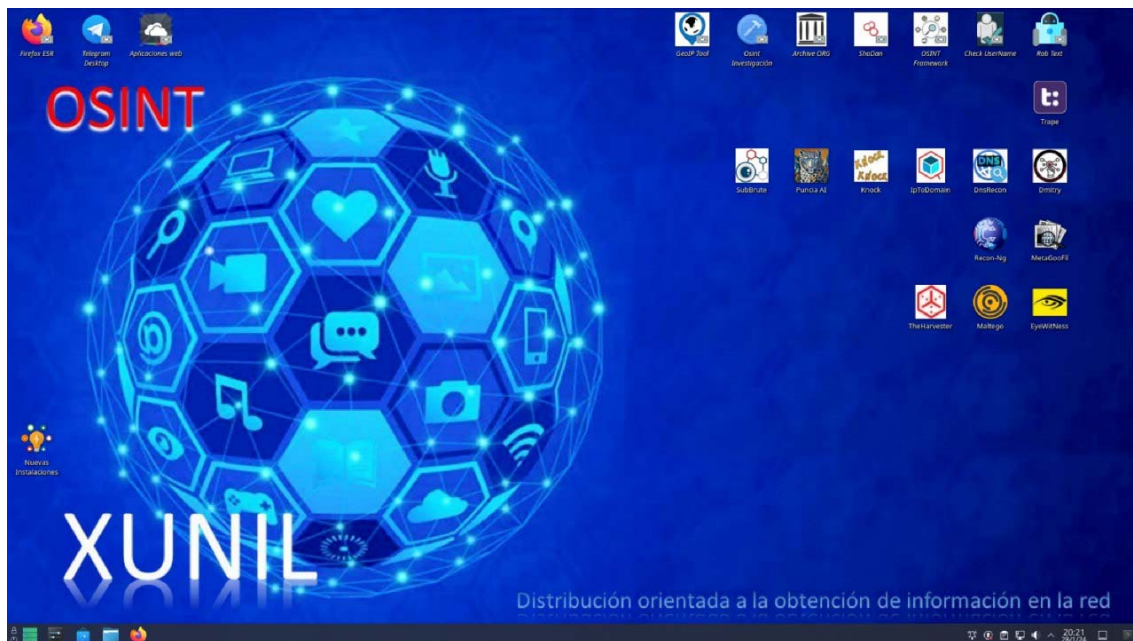
Se utiliza un programa WebApp Manager [3] cuyo repositorio se encuentra en [GitHub - linuxmint/webapp-manager](https://github.com/linuxmint/webapp-manager).

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 más nos interese



Esta aplicación nos permite generar enlaces director que se integra en el sistema operativo y que posteriormente enviarlo como en el apartado 5.2 al escritorio principal.

7 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.

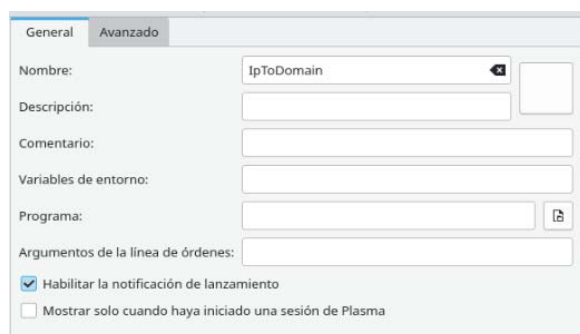
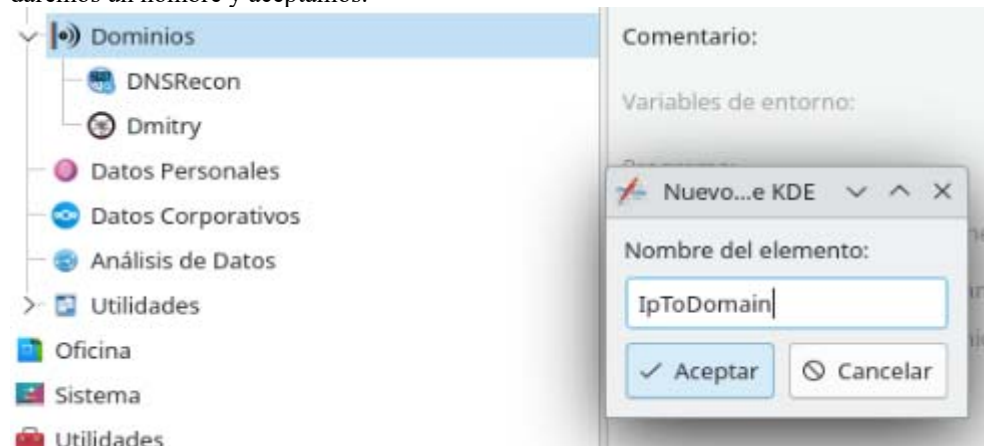
1. Enlaces directos de programas instalados por el sistema operativo. Por ejemplo, el navegador Firefox.
2. Enlaces directos creados por nosotros, por ejemplo, Trape.
3. Enlaces directos a páginas WEB creado a través de la aplicación WebApp Manager, por ejemplo, Archive Org.

8 Configuración del escritorio

8.1 Editor de menús

Con el editor de menús de KDE configuramos el menú según nuestras necesidades.

Creamos un “*Nuevo submenú*” en el cual crearemos submenú y elementos hasta configurar todo a nuestro gusto. Para crear un nuevo elemento nos posicionamos sobre el submenú elegido y solicitamos nuevo elemento, le daremos un nombre y aceptamos.



Iremos rellenando los campos necesarios para su correcta ejecución.

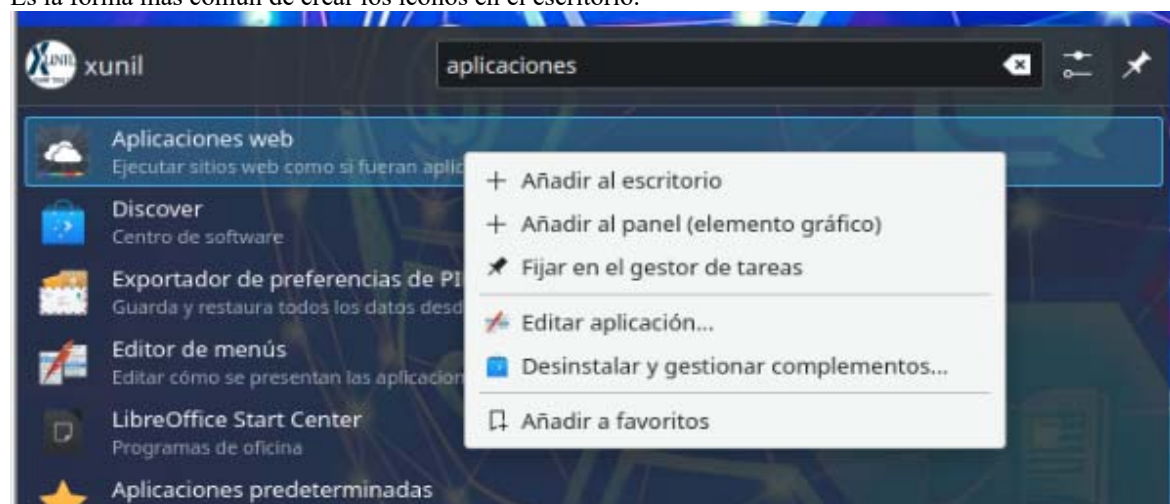
En nuestro caso debemos de rellenar “*Variables de entorno*” con la variable `$SHELL` para identificar que el programa se va a ejecutar sobre una ventana *Terminal*. Introducimos la dirección donde se encuentra el script “`/home/xunil/XunilTools/aplicaciones/iptodomain.sh`” y en la pestaña *Avanzado* marcaremos la casilla de activación de “*Ejecutar en una terminal*”

Y ya tenemos configurar nuestro nuevo elemento en el menú.

8.2 Tipo de aplicaciones

8.2.1 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.

8.2.2 Programas que se lanza sobre una terminal

Son script que contiene las instrucciones sobre su ejecución, por ejemplo, “*Sherlock.sh*”

8.2.3 Enlaces directos a una URL

Son aquellos que son gestionado a través de la aplicación WebApp, solo hay que copiar la línea de Argumentos y el programa que lo ejecuta.

9 Accesos a aplicaciones

Relación de usuarios y contraseñas utilizados en este proyecto.

9.1 Acceso a NGROK

Usuario: laprise
Email address: laprise.adrien@mail.com
Current Password: [C@diz2023](#)

9.2 Acceso a MALTEGO

¿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.

Usuario: tfmosint2023@gmx.com
Contraseña: C@diz2023

9.2.1 Activar Servicio Alien Vault OTx

Usuario: laprise.adrien@mail.com
Contraseña: C@diz2023
Api: 1f42b5bd8548e282da50a2a99dc9e522d134172e56ccfd4425795bd26b35988a

9.2.2 Activar Virustotal

Usuario: laprise.adrien@mail.com
Contraseña: C@diz2023
API: 8e4c76dd148a6bd06592b2deb97d1b3c6da59525cd3f6217c31824f58e42b31c

9.3 Acceso a SHODAN

Usuario: Laprise
Contraseña: C@diz2023

9.4 Acceso a MEGA

Usuario: laprise.adrien@mail.com -> C@di72023
Clave recuperación: zbrMEUlwDEoTj5uEubvxOA

9.5 Acceso a Twitter (X)

Usuario: @LapriseAdr72086
Contraseña: C@di72023

10 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

Tabla de contenido

1	Introducción.....	1
1.1	Marco del proyecto.....	1
1.2	Motivación.....	1
1.3	Objetivo	1
1.4	Desarrollo del proyecto	2
2	Descarga de los programas principales.....	2
3	Instalación del sistema operativo.....	2
4	Configuración del entorno	3
4.1	Acceso con usuarios	3
4.2	Configuración privilegios usuario	3
4.3	Acceso automático.....	4
4.4	Configuración pantalla	4
4.5	Personalizar pantalla de bienvenida.....	5
4.6	Configuración acceso rápidos.....	5
5	Descarga del repositorio	5
6	Programación. Creación de script.....	6
6.1	¿Qué es BASH?.....	6
6.2	¿Qué es un Script?	6
6.3	Script para nuevas instalaciones	6
6.3.1	Script de instalación de una aplicación	6
6.3.2	Script para lanzar una aplicación	6
6.3.3	Script para crear un icono con el enlace directo en el escritorio	7
6.4	Enlace a una URL desde el escritorio	7
7	Pantalla principal	8
8	Configuración del escritorio	9
8.1	Editor de menús.....	9
8.2	Tipo de aplicaciones	9
8.2.1	Enlace directo creado por el sistema operativo.....	9
8.2.2	Programas que se lanza sobre una terminal	10
8.2.3	Enlaces directos a una URL	10
9	Accesos a aplicaciones	11
9.1	Acceso a NGROK	11
9.2	Acceso a MALTEGO	11
9.2.1	Activar Servicio Alien Vault OTx.....	11
9.2.2	Activar Virustotal.....	11
9.3	Acceso a SHODAN	11
9.4	Acceso a MEGA.....	11
9.5	Acceso a Twitter (X).....	11
10	Correos electrónicos	11

