#04

NOVIEMBRE 2019
EDICIÓN

ERES LIBRE DE COPIAR, DISTRIBUIR
Y COMPARTIR ESTE MATERIAL.
FREE!

DIGITAL MAGAZINE

La comunidad de Underc0de estará publicando mensualmente aportes sobre Software Libre, Hacking, Seguridad Informática, Programación y mucho más.

> ***La tecnología*** por sí sola no basta.
> También tenemos que poner ***el corazón.***
> *- Jane Goodall.*

UNDERC0DE.ORG

UNDERC0DE

UNDERDOCS #04

ACERCA DE UNDERDOCS

ES UNA REVISTA LIBRE QUE PUEDES COMPARTIR CON AMIGOS Y COLEGAS.
LA CUAL SE DISTRIBUYE MENSUALMENTE PARA TODOS LOS USUARIOS DE UNDERC0DE.

ENVÍA TU ARTÍCULO

FORMA PARTE DE NUESTRA REVISTA ENVIANDO TU ARTÍCULO A NUESTRO E-MAIL: REDACCIONES@UNDERC0DE.ORG CON EL ASUNTO **ARTICULO UNDERDOCS**

LLAVEROS, SEÑALADORES DE LIBROS Y CALCOS DE UNDERCODE (GRATIS)

OBTÉN GRATIS LOS MARCAPÁGINAS Y LAS PEGATINAS DE UNDERC0DE, BÚSCALAS EN TODAS LAS JUNTADAS DE LA COMUNIDAD, EN MENDOZA, ARGENTINA. *DONDE TAMBIÉN SE SORTEAN REMERAS Y TAZAS PARA LOS ASISTENTES.*

> ***La mayoría del software existe no para resolver un problema, sino para actuar de interfaz con otro software.***
> *– I. O. Angell.*

EN ESTA EDICIÓN

UNDERTOOLS DIY

EN ESTA SECCIÓN DESCUBRIRÁS **HACKING TOOLS** ÚTILES QUE PUEDES HACER TÚ MISMO, CON APOYO DE UN PEQUEÑO TALLER PRÁCTICO.

OFF TOPIC

ENCUENTRA AL FINAL DE CADA ENTREGA **NUESTRA SECCIÓN ESPECIAL CON**: DESAFÍOS, TEMAS VIRALES, MENSAJES/OPINIONES DE NUESTROS USUARIOS, Y MUCHO MÁS.

LAS DIFERENCIAS NOS ENRIQUECEN

Otra vez nos comunicamos por medio de este punto de encuentro que va en su **cuarta publicación**. Un proyecto que crece, aúna el empeño de muchos, **el trabajo de equipo** cobra forma en todo un crisol de temas donde se funde la informática y la tecnología.

Sin embargo, nada nuevo hay en el anuncio precedente, por eso en esta edición de **UnderDOCS** queremos destacar otros elementos. Por primera vez en nuestro **E-ZINE** aparece una publicación de un autor con capacidades diferentes, un chico invidente ejemplo de **superación y perseverancia**, nos aporta un artículo guía donde comparte su experiencia y cómo es que logra incorporarse a la vida digital, gracias a la tecnología informática.

Somos algo más que compartir conocimientos en forma solidaria y desinteresada. Nuestro proyecto comunitario implica también **una apuesta por la inclusión y la no discriminación de clase alguna**. En una sociedad fragmentada, atravesada por la violencia en sus más variopintas formas, la integración se transforma en un objetivo social al que todos debemos contribuir. **Underc0de** adhiere plenamente a estos principios. Qué sea este otro paso más en la apuesta por el humanismo.

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM:

@ANTRAX
@79137913
@GABRIELA
@BLACKDRAKE
@DENISSE
@DRAGORA
@GOLD MASTER
@DTXDF
@ENELPC
@PATTYB
@TREVANYAM
@MIJAILO_ARSCO
@DIEGOALTF4

DIFUSIÓN:

UNDERDOCS AGRADECE A LOS PORTALES QUE NOS AYUDAN CON LA DIFUSIÓN DEL PROYECTO:

sniferl4bs.com
securityhacklabs.net
tecnonucleous.com
redbyte.com.mx
antrax-labs.org
noxonsoftwares.blogspot.com
sombrero-blanco.com/blog

CONTACTO:

INFO@UNDERC0DE.ORG REDACCIONES@UNDERC0DE.ORG

VULNERABILIDAD
EN TARJETAS SIM

NOTICIAS INFORMÁTICAS

La mayoría disponemos de un dispositivo móvil, actualmente ya no es considerado un lujo sino una necesidad, para diversos usos, la tecnología acompañada con la evolución de los teléfonos móviles viene siendo ya casi una necesidad básica para cada uno de nosotros.

Escrito por: @**DRAGORA** | **MODERADOR GLOBAL** UNDERC0DE

Es Ingeniera en sistemas Computacionales, encantada por el mundo geek, Dedicada a Telecomunicaciones**,** y miembro muy activa de la comunidad Underc0de.

Contacto:
underc0de.org/foro/profile/Lily24

En los años 40 un de teléfono móvil[1] era un equipo que ocupaba todo el baúl de un coche muchos años más tarde aparece un aparato elegante de 800 gramos; el **DynaTAC 8000X** haya por los años 80's que costaba nada más y nada menos que $3,995.00 dólares...

[1] Wikipedia, Esta página se editó por última vez el 26 sep 2019 , Historia del teléfono móvil, es.wikipedia.org/wiki/Historia_del_teléfono_móvil, **Consultado:** 09/10/2019.

Lo que a la fecha ha ido evolucionando y apareciendo en versiones más livianas, con las últimas tecnologías multimedia, pantallas táctiles, colores, cantidad de cámaras, IA integradas y de ahí las innovaciones no paran cada día nos sorprenden con algo nuevo.

El problema acá es que los móviles van evolucionando constantemente, pero se olvidaron de algo muy importante "**El estándar de las tarjetas sim tiene 10 años sin actualizarse**", Lo que ha dado paso a diferentes ataques

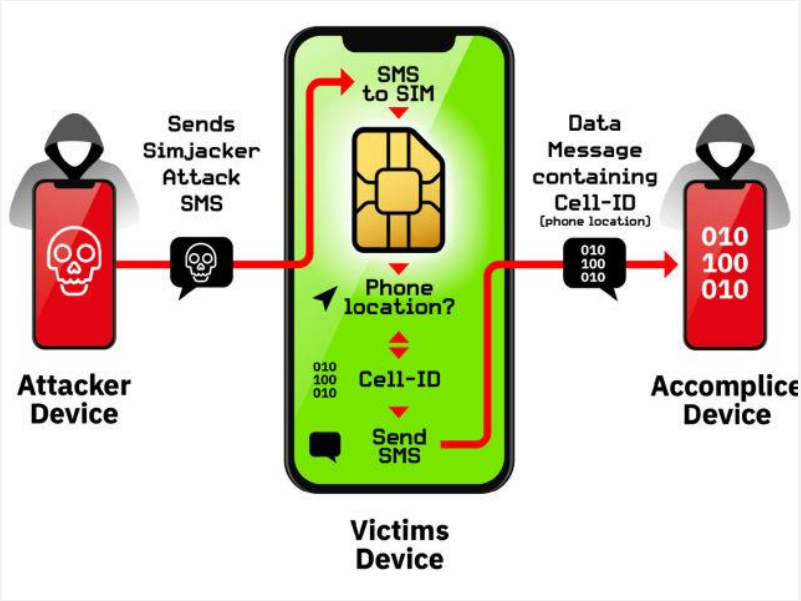
En el caso de la vulnerabilidad nombrada como **SimJacker** aprovechándose de que nuestra tarjeta SIM cuya seguridad debería ser primordial ya que permite a los operadores de telefonía darnos acceso a su red e identificarnos además de recopilar otros datos, un grupo de investigadores ha puesto en duda el tipo de seguridad que estas manejan ya que una vulnerabilidad crítica en nuestras tarjetas SIM[2] permite que un atacante remotamente pueda espiar a su víctima solo con enviar un **SMS**.

SimJacker vulnera parte del software S@T Browser (SIMalliance Toolbox Browser) herramienta aplicada por más de treinta países alrededor de todo el mundo.

¿Esta herramienta para que es utilizada?

- Pues es la que adhiere funcionalidades para los operadores
- Gestiona servicios, suscripciones
- Instrucciones para enviar un mensaje corto
- Establecer llamadas
- Lanzar el navegador
- Ejecutar comandos o enviar datos

Todo lo antes mencionado puede ser accionado enviando un simple SMS al dispositivo de la víctima, teniendo así el atacante a su disposición el área adecuada para ejecutar los respectivos comandos. También quedó descubierto y comprobado lo que desde hace mucho varios sospechaban, una entidad que labora con gobiernos de todo el mundo ha estado utilizando esta vulnerabilidad **para espiar y vigilar a usuarios**.

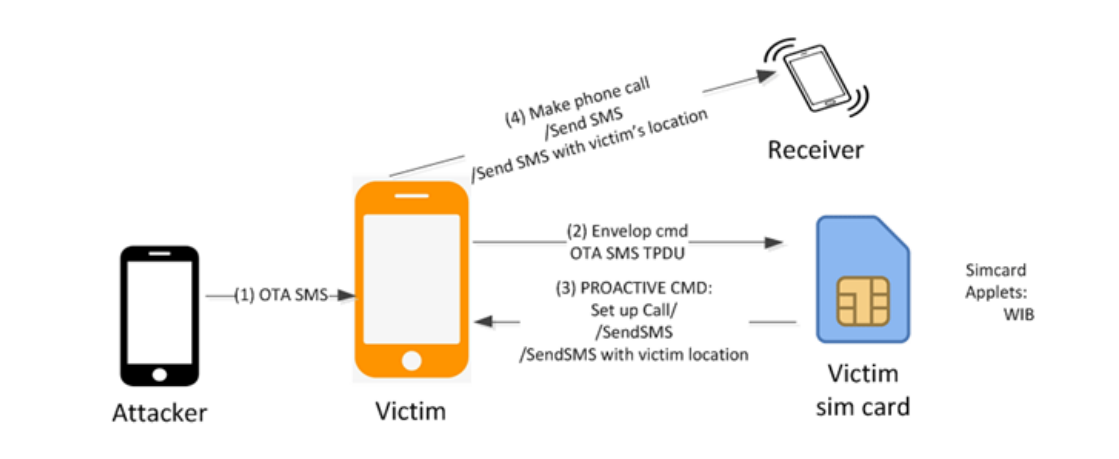


Los Materiales necesarios para explotar esta vulnerabilidad es un **modem GSM** con el cual se realiza el ataque obteniendo fácilmente del dispositivo IMEI, ubicación, suplantación de identidad, envío de fraudes de números Premium, hacer llamadas, abrir enlaces, perpetrar ataques **DDoS**, obtener información del móvil y cualquier cosa que pueda hacer cambios la tarjeta SIM.

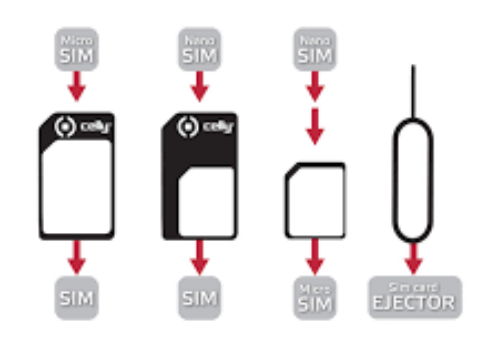
[2] Alberto García , 2019, Un fallo en tu tarjeta SIM puede hackearte el móvil sólo por un SMS, www.adslzone.net/2019/09/12/simjacker/, **Consultado:** 09/10/2019.

Otra variante de este tipo de ataques es **WIBATTACK**[3] descubierta por Ginno **Security Lab** que es un ataque desarrollado en el navegador de internet inalámbrico (WIB), basado en un kit de herramientas Sim diseñadas por Smart Trust. De la misma forma que S@T Browser se puede:

- Controlar WIB de manera remota con SMS Over the Air (OTA) utilizadas por las compañías telefónicas
- Modificar las configuraciones centrales
- Mostrar textos falsos
- Iconos falsos
- Acceder a diversas URL
- Recopilar datos
- Efectuar llamada



A causa de que las características de **WIB** no están documentadas es un poco difícil explotar **WIBAttack**. Uno de los especialistas en seguridad de apps web de Ginno Scurity afirma que estas falsas fueron encontradas hace 4 años lo cual ha estado en secreto razón por la que parchear este tipo de vulnerabilidad es bastante dificultoso.



Los descubrimientos han sido reportados a GSM Association (GSMA), que es un equipo de compañías operadoras de telefonía móvil y similares, hasta la fecha los investigadores están agrupados en buscar estrategias para proteger contra **Backdoors** en las tarjetas SIM, especialistas en seguridad de aplicaciones web del Instituto Internacional de Cibernética (IICS), GSMA está empleando medias para que los fabricantes y compañías operadoras atenúen el riesgo de la explotación de estas vulnerabilidades.

Aunque estos ataques no son tan populares como SS7 O SIM SWAP, el peligro está a la orden del día debido a que el estándar de las tarjetas SIM lleva 10 años sin actualizarse situación preocupante pues tanto como evolucionan los teléfonos también deberían de ir actualizando los estándares de las tarjetas SIM, porque esto desencadena que los usuarios se conviertan en víctimas y no puedan estar al tanto de que están siendo objetivos de un ataque, cabe resaltar que no importa el tamaño de la tarjeta SIM física pues todas son vulnerables pues la atribución está ahí desde 2009 sin la respectiva actualización. Lo único que pueden hacer los operadores es incorporar procesos para examinar y obstaculizar mensajes dudosos que manejen comandos S@T lo que nos e sabe es en qué momento empezaran a poner en marcha los cambios en corto lapso dejando así a los usuarios expuestos a que muchos hackers intenten explotarla.

[3] Alisa Esage, 2019, WIBATTACK: LA NUEVA FORMA DE HACKEAR TARJETAS SIM, noticiasseguridad.com/videos-noticias/wibattack-la-nueva-forma-de-hackear-tarjetas-sim/, **Consultado:** 10/10/2019.

BOTNETS: TAN PELIGROSOS COMO COMPARTIR CEPILLO DE DIENTES

HACKING

Ya hace mucho, pero que mucho tiempo se viene hablando sobre ellas, como crearlas, prevenirlas, defenderse, identificarlas y un sinfín de información que se habla de ellas una y otra vez.

Escrito por: **@DTXDF** | **MODERADOR GLOBAL** UNDERC0DE

Aficionado a la informática, apasionado por la seguridad informática y programación, sus lenguajes de programación favoritos son: Python, JavaScript, PHP y próximamente ASM y los demás lenguajes: SQL, bash, html y css.

Contacto:
underc0de.org/foro/profile/DtxdF

Tal vez ya hemos leído noticias sobre ataques informáticos relacionados con ellos, simplemente ignoramos esas noticias y preferimos no informamos correctamente de sus riesgos, **Botnet** es un término que hace referencia a un conjunto o red de robots **informáticos** o bots, "**IoT**" siglas del **Internet of Things.**

*Los **botnets** deberían hablarse tanto como los problemas y rumores de los famosos*

En pocas ocasiones, *podría decirse que casi nula*, escuchamos hablar de ataques por parte de **botnets** en televisión; Uno de los ataques informáticos más excepcionales que si hizo estragos en los noticieros fue el ***ransomware***, específicamente el **WannaCry**.

De ahí el dilema, ¿qué es más poderoso o peligroso el ransomware o los botnets?

Esta pregunta ya tiene una respuesta pegada en la frente, los **botnets**.

¿Porque?

Los **botnets** son eclipsados por los ataques de **ransomware**, suponiendo todas las diferencias que hay entre un **ransomware** y un **botnet**:

¿Qué hace un ransomware?:

- Cifrado los archivos (Algunos son tan efectivos, que ni con un simple formateo se puede restablecer)
- Pide un "**rescate**" para recuperarlos
- No se está totalmente seguro si después de pagar el rescate, los atacantes proporcionaran la clave para descifrar los archivos.

¿Qué hace un botnet?:

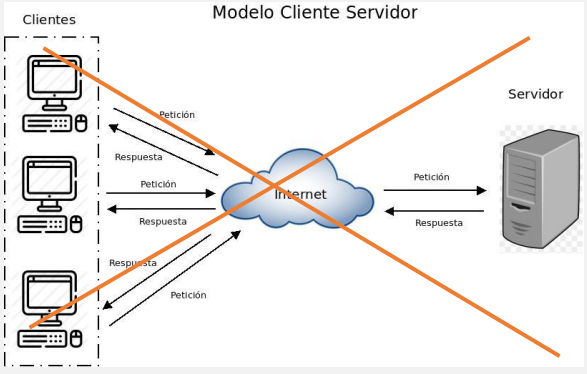
Es una red de dispositivos infectados (Mayormente llamados "*Zombies*"); Teniendo esto en cuenta básicamente tienen control sobre un dispositivo, pueden hacer lo que sea, *incluso*, integrarle más malware de otro tipo, si, también un **ransomware**; Aunque principalmente un **botnet** hace lo siguiente:

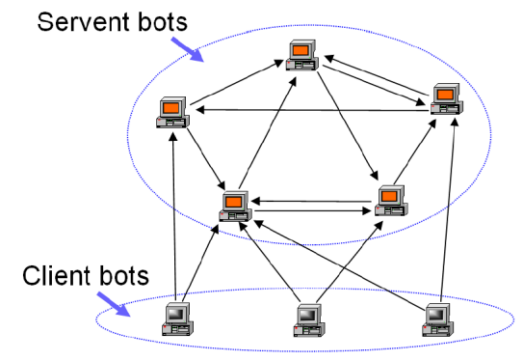
- Envío de spam
- Ataques de denegación de servicio distribuido (DDOS)
- Espiar a las victimas
- Incluir más malware

O básicamente, podríamos decir que puede ejecutar casi cualquier tarea que quisiese el atacante (**botmaster**) y dado que puede subir a los dispositivos infectados más malware de cualquier tipo, vuelve aún más peligroso al **botnet**, si el *botmaster* un día decidiera por subir una carga útil de **ransomware** a todas las máquinas de la red, podría infectar a todas ellas con un éxito cercano al 100% sin duda alguna.

modelo cliente-servidor

Ya no más modelo cliente-servidor por parte de una **botnet**, al menos en las más sofisticadas. Ahora usan las redes Punto a Punto (Peer to Peer – P2P, en inglés), lo que básicamente equivale a un riesgo aún mayor, ya que no dependerá de un servidor central, ahora un nodo (teniendo características necesarias) puede actuar como servidor o como cliente.





Claro, esto es muy espeluznante, pero no todo es “magia sin un conejo”; Para que esto funcione, debe cumplir ciertas reglas para que un cliente se torne servidor, en el caso de los **botnets** punto a punto.

el firewall

Es un hecho que las victimas van a tenerlo activado, así no sea cierto esto, el atacante debe considerar que, si lo es, simplemente porque no será fácil.
Es cierto que podemos infectar a una víctima con facilidad, sin embargo, no podemos crear un servidor dentro de su computador y menos que funcione más allá de su red interna sin antes hacer un procedimiento; Cosa que facilita el ya tener infectada la máquina.

Ahí es donde entra (Nuestro conejo) ***UPnP*** *(Universal Plug and Play)...*

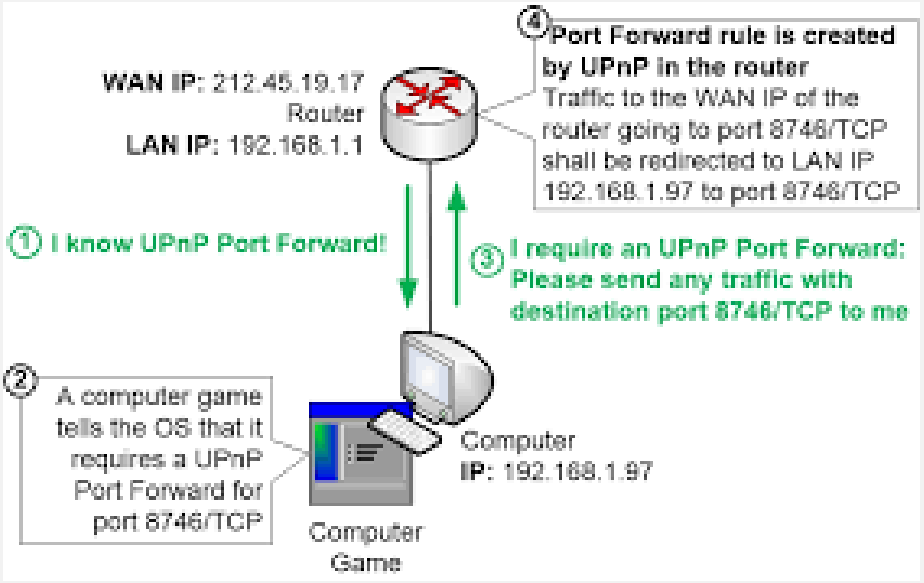
Universal Plug and Play (**UPnP**, sus siglas), nos muestra color de rosas aparentemente, una variedad de servicios entre computadoras y cientos de posibilidades de disfrutar entre familia compartiendo contenido multimedia, sintiéndose los súper sónicos...

Pues, *igual que la magia bella y hermosa*, donde se muestra *el conejo y todo el mundo se sorprende,* aplauden y miles de voces de felicidad, también existe la hechicería, es ahí, donde entramos nosotros los malvados genios de la maldad a descontrolar lo controlable.

Aparentemente **UPnP** no les ofrece nada más que facilitar la vida al ***usuario doméstico***, pues para hacerlo necesita de ciertos privilegios, como pueden ser uno de lo más importante: "**Port Forwarding**", exacto, así de sencillo, sin recurrir a ninguna otra aplicación de "hackeo" de la NSA, CIA, KGB o esas *simplezas interesantes*.

> *Tranquilos, no es que su **router** esté diseñado para que venga una persona y se conecte a espiarlos.*

En la imagen veremos una explicación sencilla de como funcionaria el "**Port Forwarding**" en **UPnP**, para configurar un simple juego de computadora en un puerto especifico.



Ahora resulta, que, en vez de un juego de computadora, no sea un juego ¿Y qué no sepan que esté instalado en su computadora?, con el único fin de que sean parte de una red.

Así, si su razonamiento deductivo no les falla al leer lo anterior, se darán cuenta que serán parte de un **botnet** y que su computadora será un servidor operando como un **atacante**.

DESTRIPANDO UNA BOTNET

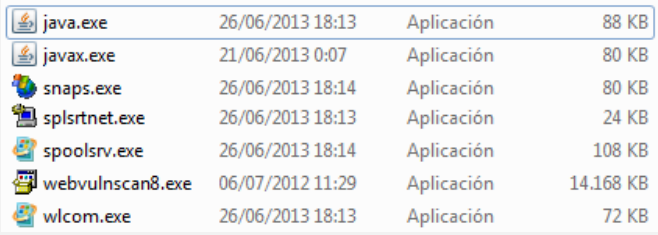
Una página que inspiraba total confianza para realizar la descarga e instalar una aplicación. Según el proceso de instalación iba marcando su barra de progreso, causando alarma por un error **Run-time 5**, *"de los de toda la vida"* ... o sea, en **Visual Basic**. Llegando a la deducción de que un malware ***bindeado*** al ejecutable de instalación saltaba en añicos, con lo que posiblemente se hubiese colado cualquier otra cosa.

Escrito por: **@ENELPC** | EN COLABORACIÓN CON **UNDERC0DE**

Analista de Malware, Consultor de Seguridad Informática, Docente en cursos de hacking ético/pentesting/malware, forense en Windows, ataques en redes de datos IPv4 e IPv6, VoIP, seguridad web, auditoría de código y temas relativos a la fortificación de sistemas, **Redactor del artículo** "Identification and Exploitation of the Most Common Vulnerabilities in Web Applications", para la revista **Hakin9 IT Security Magazine**, Pentesting con Kali - **OxWord** Computing20 de mayo de 2013.

Contacto:
Un Tal 4n0nym0us En El PC: www.enelpc.com
Redes Sociales: **TWITTER:** @enelpc

Con suerte en que el desarrollador del *supuesto malware*, pusiera el mismo nombre al ejecutable que al **título del proyecto**, y es que, en estas ventanas de error, se muestra el título del formulario principal de las aplicaciones. Dirigiéndo al administrador de tareas, botón derecho y "Abrir la ubicación del archivo", permitiendo llegar hasta una carpeta ubicada en **AppData** del **usuario actual**, donde son necesarios otros permisos para alertar al usuario. Mostrando el siguiente panorama...



java.exe	26/06/2013 18:13	Aplicación	88 KB
javax.exe	21/06/2013 0:07	Aplicación	80 KB
snaps.exe	26/06/2013 18:14	Aplicación	80 KB
splsrtnet.exe	26/06/2013 18:13	Aplicación	24 KB
spoolsrv.exe	26/06/2013 18:14	Aplicación	108 KB
webvulnscan8.exe	06/07/2012 11:29	Aplicación	14.168 KB
wlcom.exe	26/06/2013 18:13	Aplicación	72 KB

Network Analysis

Hosts Involved

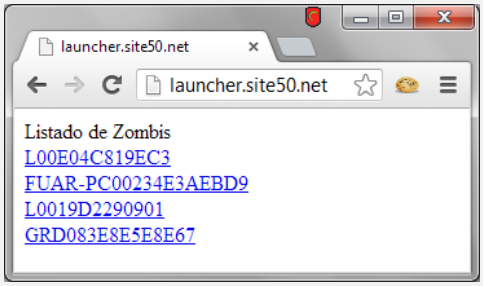
IP Address
192.168.1.101
192.168.1.255
8.8.8.8
31.170.162.243

DNS Requests

Domain	IP Address
launcher.site50.net	31.170.162.243

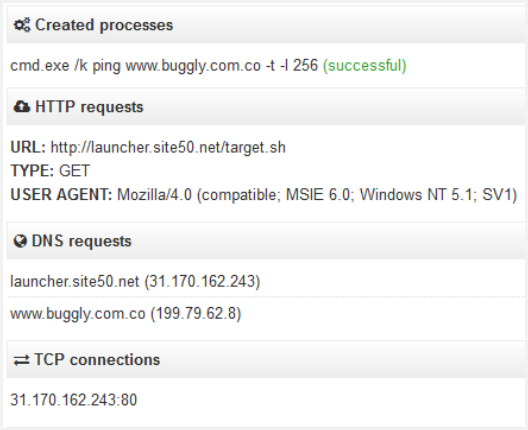
Sin **Cuckoo Sandbox** (en ese momento) hasta más tarde, obteniendo ayuda de ***Malwr.com***. Entre las cosas que más llamaron la atención al subir el instalador, fueron lógicamente las conexiones.

Nos dirigimos al navegador y tecleamos la URL que aparecía de vuelta del **Cuckoo**, Sin control de acceso.



Lo más gracioso es cuando vi el nombre de mi máquina en una de sus carpetas y una imagen de mi escritorio subida en su interior. Para más inri, soy el típico capullo que tiene una foto carnet en el escritorio jajajaj.

Una de las opciones era ***buscar la URL en Google***, para encontrar algún tipo de pista para obtener más de información. Por suerte un scanner en Virustotal mostraba que un malware de nombre **Project1.exe**, compilado en **Visual Basic 6** conectaba con ese mismo dominio. En este caso, el **malware** era totalmente diferente encontrarlo, además, de que se utilizaba para realizar denegaciones de servicio con una consola abierta en segundo plano sobre las víctimas, en este caso el ***tarjet*** era sobre el sitio de seguridad informática colombiano www.buggly.com.co.



Created processes

cmd.exe /k ping www.buggly.com.co -t -l 256 (successful)

HTTP requests

URL: http://launcher.site50.net/target.sh
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

DNS requests

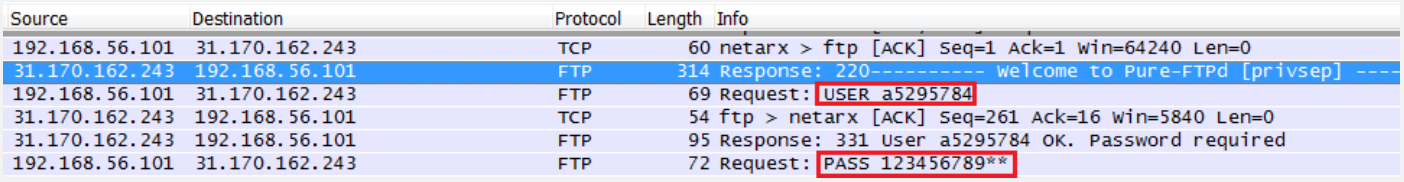
launcher.site50.net (31.170.162.243)
www.buggly.com.co (199.79.62.8)

TCP connections

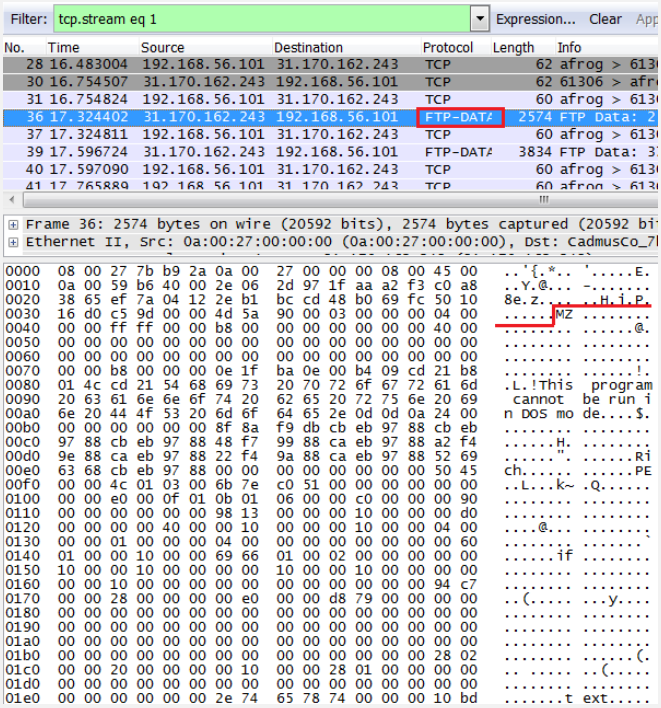
31.170.162.243:80

¿Qué Hacemos Aparte De Matar Los Procesos?

Cuckoo provee al auditor de la opción de realizar volcados de memoria, además de la posibilidad de guardar la captura de red sobre un fichero **pcap**. Así que echando un vistazo a todo lo que ocurría en la red mientras el malware se ejecutaba, resultando lo siguiente.



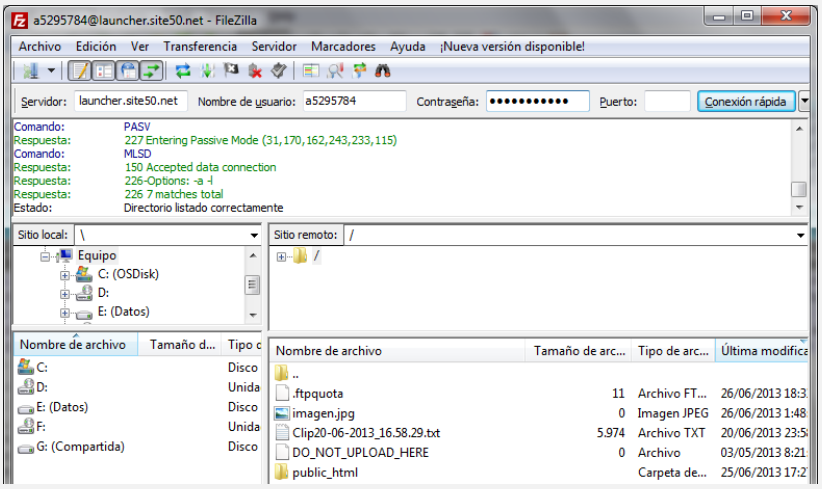
Source	Destination	Protocol	Length	Info
192.168.56.101	31.170.162.243	TCP	60	netarx > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
31.170.162.243	192.168.56.101	FTP	314	Response: 220---------- Welcome to Pure-FTPd [privsep] ----
192.168.56.101	31.170.162.243	FTP	69	Request: USER a5295784
31.170.162.243	192.168.56.101	TCP	54	ftp > netarx [ACK] Seq=261 Ack=16 Win=5840 Len=0
31.170.162.243	192.168.56.101	FTP	95	Response: 331 User a5295784 OK. Password required
192.168.56.101	31.170.162.243	FTP	72	Request: PASS 123456789**



Por otra parte, llamó mucho la atención el comportamiento del malware. Pues la gran mayoría de ejecutables eran descargados por **FTP** desde uno de ***los ejecutables bindeados al instalador***. Con lo que evitaban que el tamaño de la aplicación no fuese lo suficientemente grande.

> *Con toda esta información, tan solo quedaría eliminar mi captura de pantalla de su listado. Con lo que **Filezilla** y el usuario del **pcap** me abrieron la puerta.*

Otra de las cosas **destacables**, encontradas al revisar qué tipo de acciones realiza el malware sobre el FTP. *A parte de la captura de pantalla*, es la de captura de teclas a modo **Keylogger**, que desde la propia página no era posible la lectura del contenido de los ficheros de texto por prohibición del servidor... pero al tener acceso vía FTP ;)

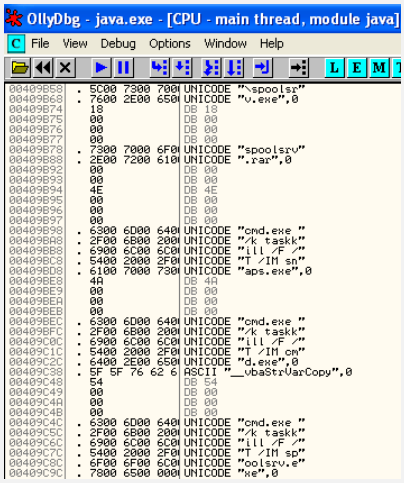


> *Me hizo recordar a mi entrada sobre Espionaje, cuerpos sexys y datos robados, pues el propio desarrollador de la botnet, se encontraba infectado a sí mismo...*

La siguiente imagen muestra como el sujeto realiza un **Control+V**, para pegar la contraseña de acceso sobre la aplicación **WinHTTrack Website Copier**, así logra descargar el contenido a su equipo personal. Además de tener el navegador de Firefox abierto para acceder desde el mismo.

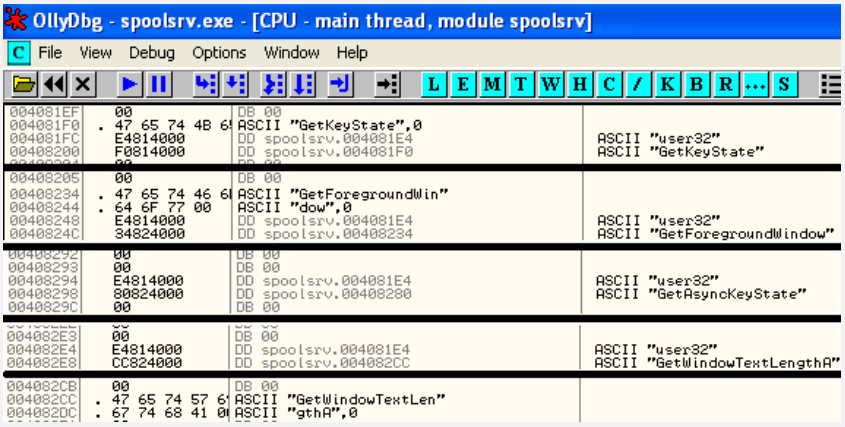
```
Insertar dirección URL
----------------------------------------
{ctrl}v123456789++{ctrl}{Left}{Left}{Left}{Left}{Left}{Left}{Left}{Left}{Left}{Left}{Left}WinHTTrack Website Copier - [aaa.whtt]
----------------------------------------
Índice de ftp://31.170.162.243/../../../../public_html/ - Mozilla Firefox
----------------------------------------
```

Revisando las capturas de su equipo en el FTP, para estudiar los ejecutables a los que logramos tener en nuestro poder. Por suposición se dedujo que el origen de que se trataran de Visual Basic 6, era debido a que utilizaría un **Crypter**, con lo que sería más tedioso ver de qué se trataban.

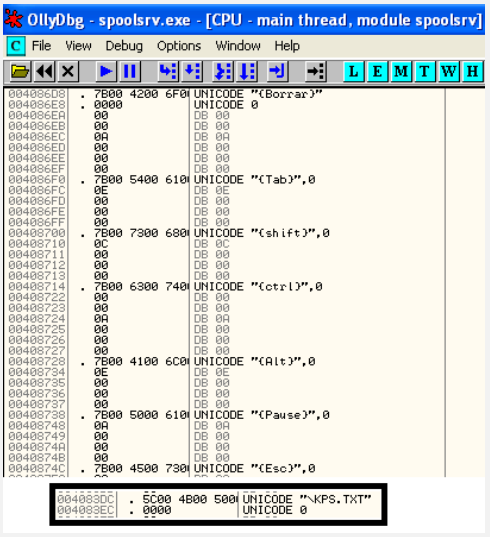


¡Pero no! El tipo no cifró ni lo más mínimo, y pude identificar de forma rápida, que realizaba cada uno de ellos.
*El ejecutable **Java.exe**, se encargaba de descargar el resto de ejecutables del FTP, ejecutarlos en el sistema y de matar sus procesos desde la consola.*

El ejecutable de **Javax.exe**, realizaba tareas muy similares, también realizando las ejecuciones del conjunto de aplicaciones de la **botnet**, que se encontraban en la carpeta **java** en **AppData** del usuario.

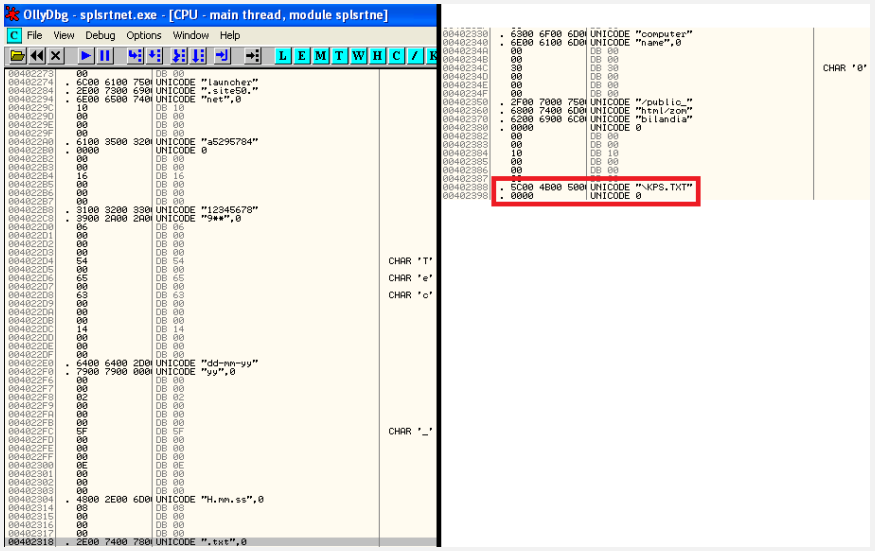


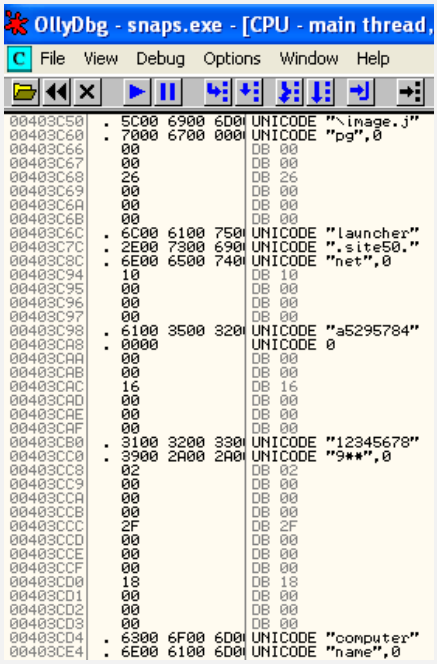
El ejecutable de **Spoolsrv.exe**, tenía tan solo la acción de captura de teclas y eventos para la funcionalidad de ***Keylogger***. La siguiente imagen muestra las declaraciones de las Apis más comunes para estas capturas.



Por otro lado, aparecían en el mismo ejecutable todo el listado de caracteres que era capaz de capturar y cuál era el archivo de texto destinado al almacenamiento de los mismos.

Separada la acción de subida al **FTP** de las capturas de teclas, se encontraba bajo el ejecutable **splsrtnet.exe**, encargado de generar un **nombre único** a la captura basado en la fecha y hora de subida.

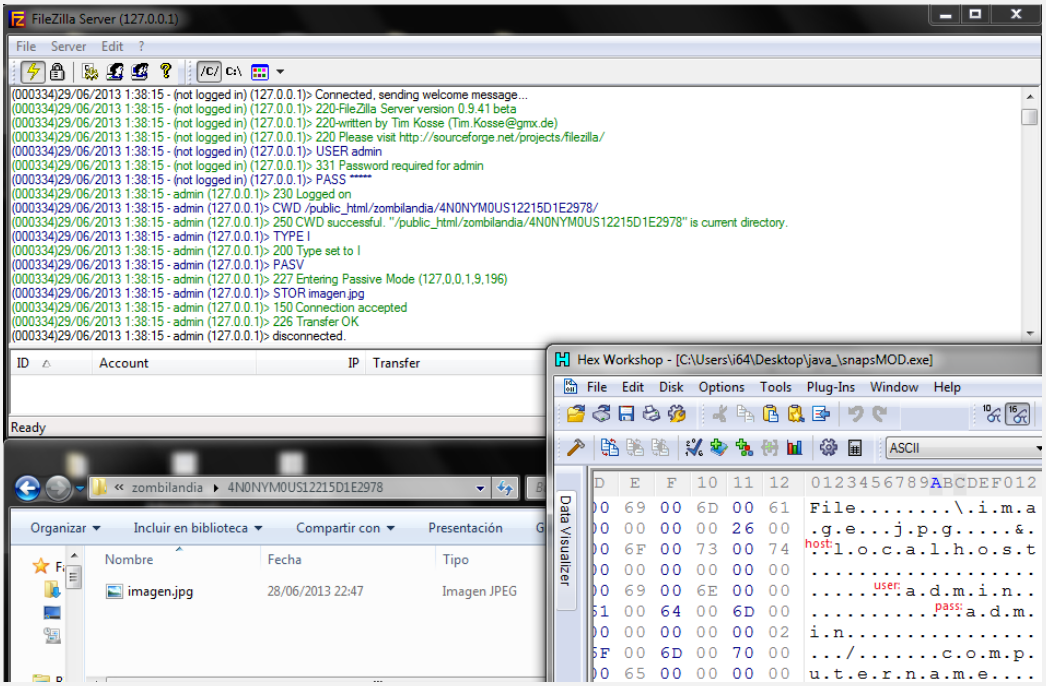




El otro ejecutable llamado **Snaps.exe**, se encarga de **generar las capturas de pantalla** y de subirlas al FTP.

*Así que, con toda esta información en plano, se me ocurrió la idea de parchear los ejecutables y hacerme con la **botnet** para mi uso personal...*

La imagen muestra como el **malware**, se conecta y sube una imagen del escritorio personal a la FTP en **localhost** con usuario **admin** y contraseña **admin**.



JOK3R - PENTEST AUTOMATION FRAMEWORK

PENTESTING Y SEGURIDAD WEB

Jok3r es un framework cuyo entorno nos ayuda a la hora de realizar un pentesting tanto a nivel de infraestructura como a nivel de aplicaciones web. Éste framework utiliza muchas herramientas, ahorrándonos mucho tiempo a la hora de realizar un análisis.

Escrito por: **@BLACKDRAKE** | **CO-ADMIN** UNDERC0DE

Co-Fundador de Red4Sec, dónde actualmente realiza auditorías de seguridad. Apasionado de la seguridad web y blockchain. Además de que posee las certificaciones OSCP y OSWP.

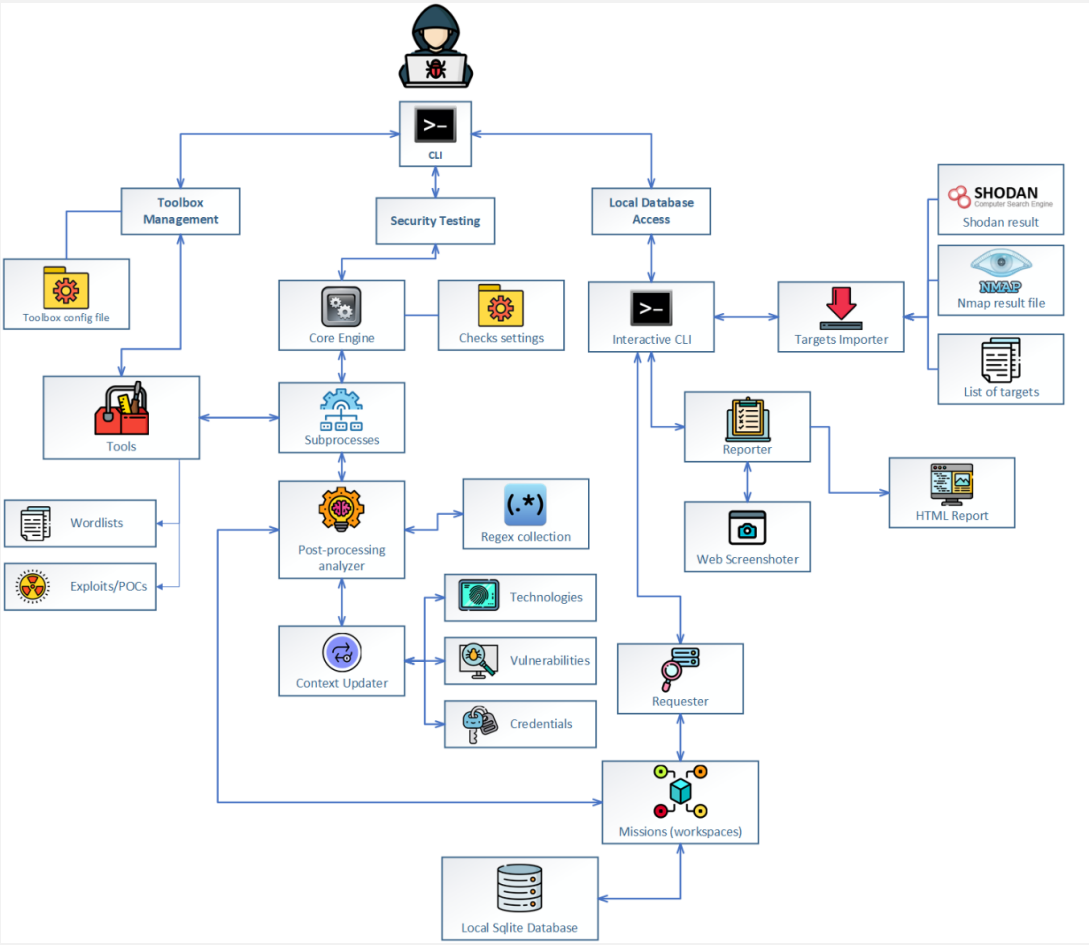
Contacto:
underc0de.org/foro/profile/blackdrake
Redes sociales:
Twitter: @alvarodh5

Jok3r un **framework** que ayuda a los **pentesters** a la hora de realizar un *test* de intrusión desde infraestructura de red hasta la propia seguridad web.

El principal objetivo de Jok3r es automatizar la mayor cantidad de tareas posible, ahorrando tiempo en el análisis del objetivo. Además, nos permite identificar y explotar rápidamente todo tipo de vulnerabilidades en los servicios (TCP/UDP) y tecnologías web más comunes (servidores, CMS...).

arquitectura de jok3r

La arquitectura actual del framework es la siguiente:



desplegando jok3r

Hay varias formas de desplegar **jok3r**, no obstante, la más rápida sin lugar a dudas es utilizar docker, además, de que probablemente nos ahorrará problemas con alguna dependencia.

- `sudo docker pull koutto/jok3r`

```
[12:54:33] alvaro ~ : docker images
REPOSITORY                  TAG                 IMAGE ID            CREATED             SIZE
koutto/jok3r                latest              a42b47c33347        2 months ago        16.4GB
```

- `sudo docker run koutto/jok3r`

```
[12:58:19] alvaro ~ : docker ps -a
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS                      PORTS               NAMES
a859ea77b9ac        koutto/jok3r        "bash"              2 weeks ago         Exited (0) 10 days ago                          jok3r
```

- `sudo docker start -i jok3r`

```
[13:01:12] alvaro ~ : docker ps -a
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS               NAMES
a859ea77b9ac        koutto/jok3r        "bash"              2 weeks ago         Up About a minute                       jok3r
```

- `sudo docker exec -it jok3r bash`

```
[13:02:47] alvaro ~ : sudo docker exec -it jok3r bash
root@jok3r-docker:~/jok3r#
```

***Nota**: Si no queremos utilizar **Docker**, podemos descargar el proyecto desde su repositorio oficial e instalarlo de la siguiente forma:*

1. Descargamos el proyecto github.com/koutto/jok3r
2. Instalamos las dependencias necesarias:
   - pip install -r requirements.txt
   - install-all.sh
   - install-dependencies.sh
3. Una vez instaladas todas las dependencias, podremos ejecutar jok3r de la siguiente forma: python3 jok3r.py –help

Jugando con Jok3r

Para comenzar podemos listar todas las herramientas que utiliza jok3r a través del siguiente comando: `python3 jok3r.py toolbox --show-all`

La herramienta permite elegir el lugar dónde queremos guardar los resultados de los escaneos. Para ello, antes debemos crear una base de datos:

`python3 jok3r.py db`

En ese instante, podremos comprobar que el **prompt** ha cambiado. A continuación, podemos utilizar **help** para visualizar todas las opciones que contempla la herramienta.

```
jok3rdb[default]> help

Documented commands (type help <topic>):

Attacks results
================================================================================
results             Attacks results
vulns               Vulnerabilities in the current mission scope

Import
================================================================================
file                Import a list of targets from a file
                    One target per line, with the following syntax:
                    - For any service: <IP/HOST>:<PORT>,<SERVICE>
                    - For HTTP service: <URL> (must begin with http(s)://)
nmap                Import Nmap results (XML)

Missions data
================================================================================
creds               Credentials in the current mission scope
hosts               Hosts in the current mission scope
mission             Manage missions
options             Specific Options in the current mission scope
products            Products in the current mission scope
services            Services in the current mission scope

Reporting
================================================================================
report              Generate an HTML Report with all data and checks outputs from
                    the current mission

Other
================================================================================
alias               Manage aliases
help                Display this help message
history             View, run, edit, save, or clear previously entered commands
macro               Manage macros
quit                Exit this application
set                 Set a settable parameter or show current settings of parameters
shell               Execute a command as if at the OS prompt
```

Llegados a este punto es importante mencionar que todos los comandos poseen ayuda personalizada, podemos obtenerla de la siguiente forma: nombre_comando --help

```
jok3rdb[default]> mission --help
usage: mission [-h] [-a <name>] [-c <name> <comment>] [-d <name>] [-D]
               [-r <old> <new>] [-S <string>]
               [<name>]

Manage missions

positional arguments:
  <name>                          Switch mission

optional arguments:
  -h, --help                      show this help message and exit
  -a, --add <name>                Add mission
  -c, --comment <name> <comment>  Change the comment of a mission
  -d, --del <name>                Delete mission
  -D, --reset                     Delete all missions
  -r, --rename <old> <new>        Rename mission
  -S, --search <string>           Search string to filter by
```

En primer lugar, debemos crear una misión, utilizando el comando: `mission -a nombre_mision`

```
jok3rdb[default]> mission -a test

[+] Mission "test" successfully added
[*] Selected mission is now test
```

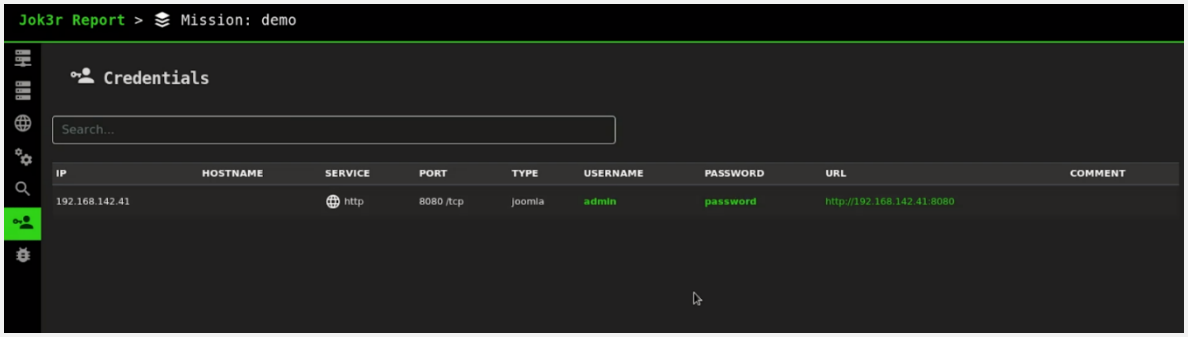
Con nuestra misión creada, podemos salir de la db utilizando `quit`.

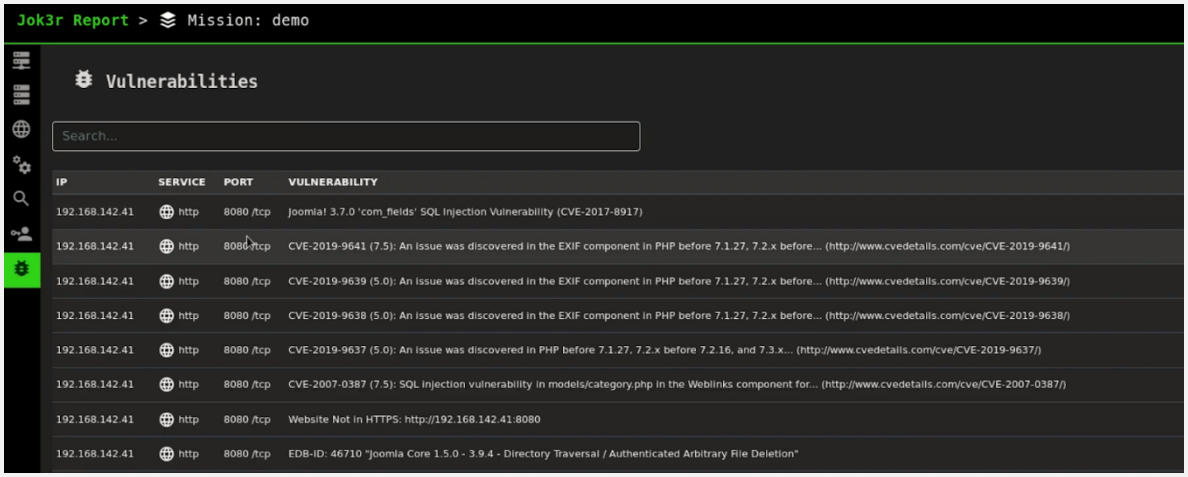
Acto seguido, iniciaremos el ataque sobre el scope en concreto y guardando los resultados en la db de la siguiente forma:

```
python3 jok3r.py attack -t http://127.0.0.1 --add test
```

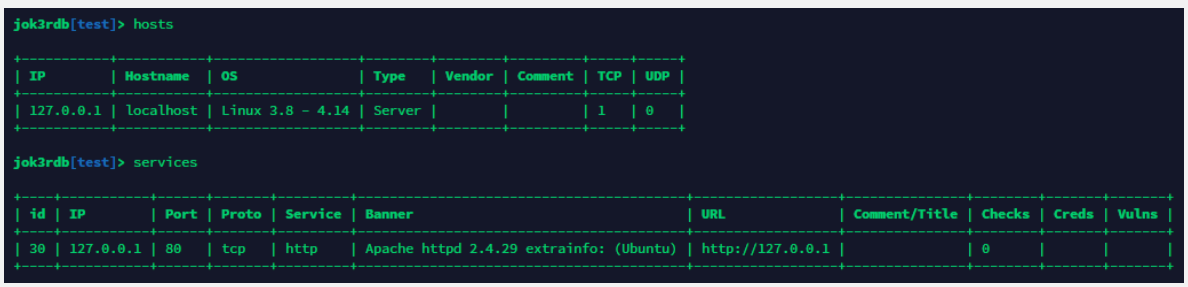
```
[*] URL given as target, targeted service is HTTP
[*] Reverse DNS lookup for 127.0.0.1...
[*] 127.0.0.1 -> localhost
[*] Check if service is reachable...
[*] Grab service info for [host 127.0.0.1 | port 80/tcp | service http] via Nmap...
[*] Banner = Apache httpd 2.4.29 extrainfo: (Ubuntu)
[*] Detected OS = Linux 3.8 - 4.14
[*] Web technologies detection using Wappalyzer...
+--------+---------+
| Name   | Version |
+--------+---------+
| Apache | 2.4.29  |
| Ubuntu |         |
+--------+---------+
[+] Target URL http://127.0.0.1 is reachable
[*] Results from this attack will be saved under mission "test" in database
[+] Added: host 127.0.0.1 | port 80/tcp | service http


+----+-----------+-----------+------+-------+---------+----------------------------------------+------------------+
| id | IP/       | Hostname  | Port | Proto | Service | Banner                                 | URL              |
+----+-----------+-----------+------+-------+---------+----------------------------------------+------------------+
| >1 | 127.0.0.1 | localhost | 80   | tcp   | http    | Apache httpd 2.4.29 extrainfo: (Ubuntu) | http://127.0.0.1 |
+----+-----------+-----------+------+-------+---------+----------------------------------------+------------------+

[?] Start attack ? [Y/n] n
[X] Attack canceled !
```

Durante el ataque la herramienta nos irá devolviendo todo tipo de información, no obstante, al finalizar, se generará un informe en html con toda la información descubierta:





Además, si accedemos a la db y utilizamos los diferentes comandos, podremos observar los hosts, servicios... descubiertos durante el análisis.



SOLUCIONES PARA EJERCER EL DERECHO AL OLVIDO EN INTERNET

SEGURIDAD

El derecho a ser olvidado en el mundo digital no es de fácil ejercicio. Puede ser un proceso largo y hasta llegar a judicializarse. En este artículo hablamos de **Forget.me**, un servicio gratuito que acerca e intermedia al usuario con los grandes buscadores (**Google** y **Bing**) para facilitar la gestión de la eliminación del pasado digital.

Escrito por: **@GABRIELA** | **CO-ADMIN** UNDERC0DE

Entusiasta de la seguridad informática, la ingeniería social y las buenas prácticas de protección cibernética del usuario común.

Contacto:
underc0de.org/foro/profile/Gabriela

Aspectos judiciales del derecho al olvido

Recientemente se anunció que Google había ganado una importante batalla legal referente al famoso “derecho al olvido”, esto es, la obligación de suprimir contenidos indexados por el buscador quedaría **limitada a la Unión Europea**. Si hacemos un poco de historia, en el año 2014, los tribunales europeos habían exigido al gigante informático eliminar aquellos enlaces perjudiciales (por falsos o dañosos) para los internautas a petición de éstos últimos. Se reconoció así, el “derecho al olvido” frente a Google sin circunscribirse a ningún área geográfica en especial.

No obstante, un **nuevo** fallo del Tribunal de Justicia de la Unión Europea, con fecha 24/09/19, sentenció que Google **no está obligado a nivel mundial** a aplicar el "derecho al olvido" sobre aquellos contenidos que afectan negativamente a los navegantes, sino que lo acotó al territorio de la Unión Europea. El máximo Tribunal expresó: "(...) el Derecho de la Unión obliga al gestor de un motor de búsqueda a retirar los enlaces en las versiones de su motor que corresponden al conjunto de la UE" (El Espectador, 2019)[4].

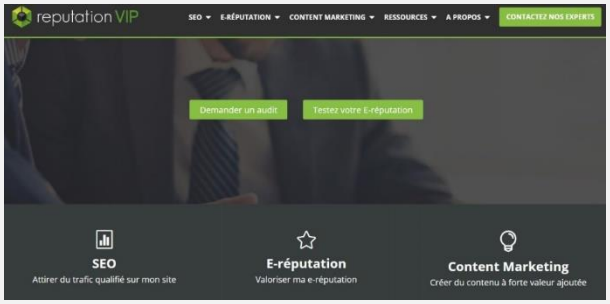
Uno de los argumentos más sólidos esgrimidos por Google es que de aplicarse el "derecho al olvido" sin restricción alguna (es decir, a nivel mundial), éste podría ser empleado por gobiernos autoritarios para intentar solapar trasgresiones o abusos a los Derechos Humanos fuera del viejo continente o incluso limitar la información en internet.

De esta forma, el Supremo Europeo determina las fronteras donde operará el derecho a borrar toda la información o datos agraviantes que vulneren la dignidad de las personas. Se pondera o se equilibra de esta manera el derecho al olvido con el derecho a la información y la libertad de prensa/expresión, que no pocas veces coloca en evidencia regímenes totalitarios e irrespetuosos de los valores democráticos. Los jueces entendieron que antes de retirar un enlace "deben ponderarse los derechos fundamentales de la persona que [lo] solicita... y los de los internautas potencialmente interesados en la información de estos"[5].

Soluciones para ser olvidados por Google o Bing

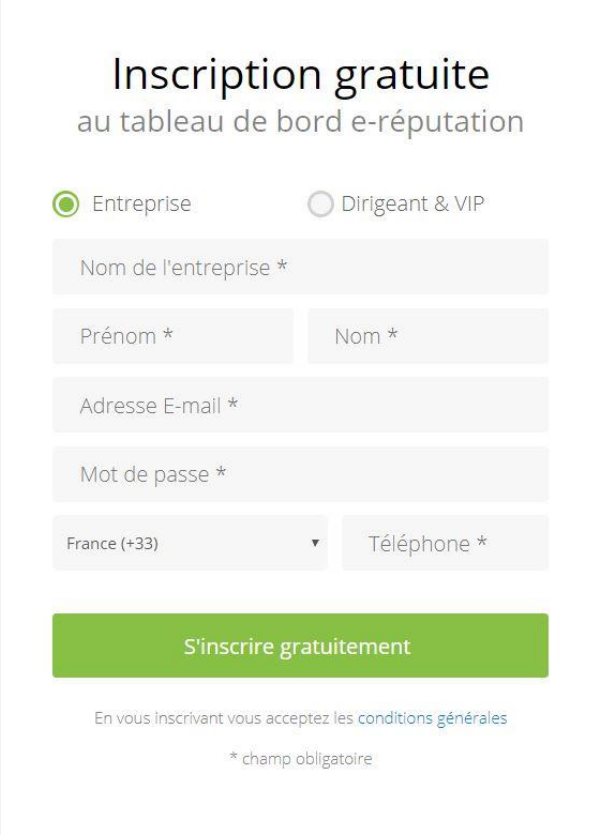
Restringido a la Unión Europea, nos planteamos la pregunta ¿qué podemos hacer si necesitamos que Google (o Bing) elimine una entrada que nos perjudica negativamente?
Independientemente del lugar en que se localice el usuario interesado en borrar información personal ofensiva, y sin acudir a un largo y arduo proceso judicial, **forget.me** ofrece a los usuarios un servicio que opera como intermediario entre los internautas y Google (o Bing, el motor de búsqueda de Microsoft) para la gestión del ejercicio del derecho al olvido. El servicio de **forget.me** funciona desde el 2014, pero luego de la sentencia última, su difusión se ha ampliado.

¿Qué es Forget.me?



Forget.me es un sitio web administrado por la compañía francesa **Reputation VIP**, y como su nombre lo indica gestiona la reputación digital, esto es, "la **imagen digital** que devuelve internet a una persona"[6]. Cuenta con un equipo de expertos en **SEO** y de personal especializado en materia legal que orienta el usuario en la desaparición del pasado digital. Su **objetivo** es facilitar la búsqueda de aquellos enlaces que aparecen en los resultados de Google (o Bing) donde se visiona información de un internauta y que éste no quiere que figure por serle perjudicial para su reputación.

[4] **El Espectador (2019).** Internet Of Things: La Justicia Europea Limita El "Derecho Al Olvido" En Internet. www.america-retail.com/internet-of-things/internet-of-things-la-justicia-europea-limita-el-derecho-al-olvido-en-internet, **Consultado**: 30/09/2019.
[5] *Ibídem.*
[6] Reputation VIP (2019) www.reputationvip.com/fr/suppression-contenu-google **Consultado**: 05/10/2019.



Así, por medio del llenado de un formulario web se va guiando al usuario a través de un proceso, organizado en distintas etapas, que permite la identificación de dichos resultados hasta culminar con la solicitud de eliminación de las huellas digitales. El único requisito que se exige es ser mayor de 18 años. Es destacable que no hay necesidad de expresar un motivo de la solicitud de borrado ya que el mismo sistema lo asocia automáticamente a una razón legal. Se puede acceder al formulario desde **este enlace.**

Una vez registrados y completado el formulario de la imagen precedente, el siguiente paso es la creación de una "solicitud de eliminación" con el objetivo de identificar la "información inapropiada". Para ello, se selecciona la información a suprimir y del menú que se despliega se elige la categoría a que pertenece cada solicitud. Si la información es removida, **Forget.me** avisa al usuario.

Hay que advertir al lector que el contenido solo se suprime de las indexaciones de los motores de búsqueda -Google y Bing- y que éstos podrán oponerse a la petición si consideran que la información es de interés general o público. Tampoco **Reputation VIP** se hace responsable de las decisiones de los buscadores en mérito que se trata de un servicio independiente.

Por último, no queremos cerrar el artículo sin mencionar que tanto Google como Bing, cuya decisión depende de un largo análisis y valoración, tienen sus propios formularios para borrar las huellas digitales cuyos enlaces facilitamos:

- **Olvídame Google**
- **Olvídame Bing**

A modo de cierre

Lo ideal es no compartir información que en el día de mañana nos pueda perjudicar o afectar en nuestra reputación o imagen digital. Sin embargo, no siempre es posible cuando esa información proviene de terceros. Un error en la vida juvenil puede arrastrar consecuencias por años, principalmente, en materia laboral.

Entendemos que el derecho al olvido, como uno de los derechos fundamentales del ser humano, cuyo ejercicio permite a las personas no ser juzgados múltiples veces por los mismos hechos a través de la infinita circulación en línea de situaciones superadas; y que, al día de hoy, posiblemente ya no se correspondan con la identidad digital de la persona.


<Zerpens>
HAZ CRECER TU NEGOCIO
TE HACEMOS
TU TIENDA ONLINE
Ideal para negocios interesados
en mostrar sus productos o
vender por internet.
ZERPENS.COM@GMAIL.COM
CONTACTAR

HACKEANDO EL CUERPO HUMANO

BIOHACKIING

Existe una nueva tendencia de modificar biológicamente el cuerpo humano, de ahí el término **Biohacking** (**Biología** + **Hacking**).

Escrito por: **@ANTRAX** | **ADMINISTRADOR** UNDERC0DE

Trabaja actualmente como QA en dos empresas de software, controlando la calidad de los desarrollos que realizan, sometiéndolos a distintas pruebas, como lo es la seguridad. Participa activamente en la comunidad de Underc0de como administrador.

Disfruta investigar temas nuevos y redactar papers de lo que va aprendiendo para que después más gente pueda aprender de ellos.

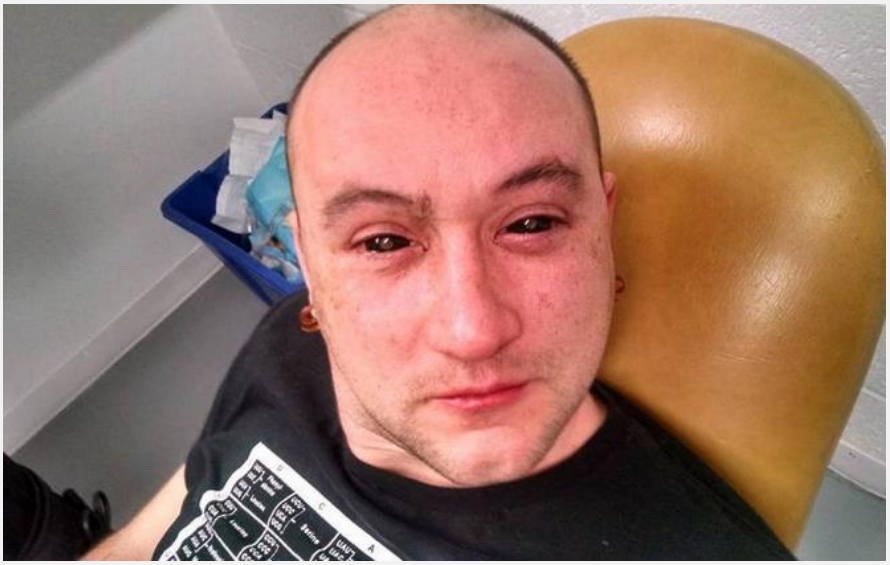
Contacto:

underc0de.org/foro/profile/ANTRAX

Consiste en insertarse dispositivos dentro del cuerpo para obtener cualidades para las cuales el cuerpo no fue creado genéticamente.

Este movimiento nace a través de algo llamado ***transhumanismo*** y buscan otorgarle al cuerpo capacidades que actualmente no tiene.

Uno de los casos más conocidos, es el de un grupo de **Biohackers** de *Los Ángeles*, quienes se implantaron en los **ojos** algo que les otorga una **visión nocturna**.



*Hay **Biohackers** que aseguran que en el **futuro** los humanos seremos **100% artificiales**.*

Uno de los ***Biohackers*** o ***Cyborgs*** más reconocidos es **Tim Cannon**, quien experimenta desde hace años esta materia. Uno de sus implantes más impactantes, lo tiene en el brazo.

Este **dispositivo** en su brazo le indica:

- Su temperatura corporal
- Sus pulsaciones
- Entre otros datos de su cuerpo.

Además, tiene *otro implante* en su mano, que **le permite abrir la puerta de su laboratorio** y varios más.

Otro de los casos es el de **Liviu Babitz**, *de Londres*, quien lleva incrustado en su pecho un **chip Bluetooth**. Este dispositivo tiene la función de realizar ***una vibración*** cada vez que su cuerpo gira al norte

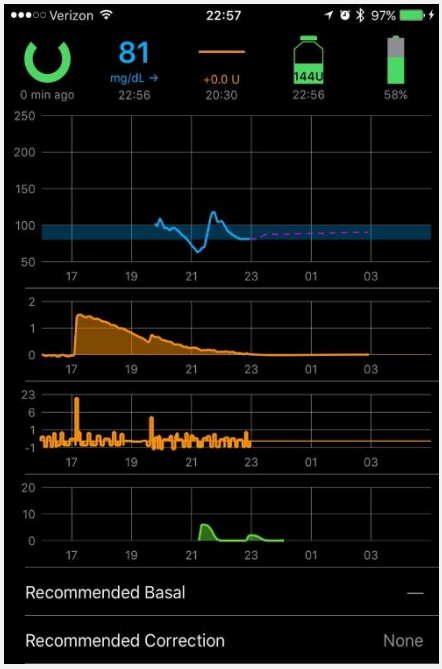
Cada vez son más las personas que experimentan con este tipo de cosas.

Por último, veremos el caso de **John Costik**, es un ingeniero que en realidad experimenta con su propio hijo.

El pequeño tiene *diabetes*, y su padre cuenta que, desde los 4 años, debía pincharle las yemas de sus dedos a diario para poder medir sus niveles de glucosa.

Su padre al ser ingeniero, pensó que esto era muy primitivo, y por eso **creó un implante para evitar los pinchazos.**

En sus primeras versiones, el implante enviaba información a una aplicación web, pero con el tiempo fue evolucionando. Actualmente la **información** queda almacenada en la **nube** y puede **monitorearlo** desde el teléfono móvil o desde su apple watch.



Si bien **no es de código abierto** por obvias razones, esto abre las puertas a una infinidad de cosas que se pueden hacer y mejorar.

CLAVES PARA ASEGURAR EVIDENCIA DIGITAL DE MANERA EXITOSA

INFORMÁTICA FORENSE

Actualmente el valor de los datos e información sensible tanto de gobiernos como empresas o personales, va aumentando cada vez más, por lo que es imprescindible protegerla al máximo, la **informática forense** se ha convertido en uno de los más sólidos aliados para lograrlo, es recomendable la realización de auditorías en los sistemas de forma periódica.

Escrito por: **@PATYB** & **@TREVANYAM** | **USER** UNDERC0DE

Ingeniera en sistemas, especialista en Seguridad de la Información, apasionada por la ciberseguridad.

Contacto:
underc0de.org/foro/profile/PatyB

Ingeniero en Sistemas, especialista en ingeniería de software, apasionado por el Ethical Hacking y el Desarrollo de Software.

Contacto:
underc0de.org/foro/profile/trevanyam

El **análisis forense digital** es el encargado de cumplir la misión **de encontrar rastros digitales**, aunque estén aparentemente escondidos o hayan sido eliminados, analizar datos residuales, recuperar información, restaurar conversaciones perdidas, detectar intrusiones/vulnerabilidades/ataques informáticos en equipos y redes. **La computación forense** también llamada así, es la rama de la informática de la policía científica y de los médicos forenses que hemos visto **en libros, series o películas**.

La informática es pieza fundamental de nuestro día a día en el ámbito personal y profesional, las funciones del aspecto forense son bastante extensas, tanto en el ámbito legal como en las empresas y aquí les presentamos las claves para llevar a cabo un proceso de informática forense exitoso:

Conocer y aplicar la legislación acorde al país aplicado en Materia de manejo de evidencia digital.

Fortalecer el perfil profesional capacitándose en temas de **informática forense** que permitan demostrar una adecuada idoneidad para el desarrollo de la labor.
Algunas certificaciones son:

- CHFI (EC-Council),
- GCFA (SANS)
- CCFP (ISC2)

Realizar un adecuado proceso de Adquisición tomando como base los siguientes lineamientos:

- ***Identificar la Evidencia Digital:*** Esta evidencia puede estar contenida en:
  - ✓ Discos duros
  - ✓ Servidores
  - ✓ Celulares
  - ✓ Tabletas
  - ✓ Consolas
  - ✓ USB
  - ✓ IOT
  - ✓ Internet u otros.

Estas evidencias se deben manejar con la rigurosidad necesaria, como si fuera un arma de fuego en la escena de un crimen.

- ***Aseguramiento fotográfico:*** fijar la escena del crimen tecnológico por medio de fotografías o videos en el que se muestre los registros y seriales de los dispositivos y estado físico de los mismos. (usa guantes de látex para manipular la evidencia y manillas antiestáticas)
- ***Realizar una imagen forense:*** ya que no debe trabajarse sobre la evidencia original, genera una imagen forense garantizando que no se sobrescriban los datos en el disco evidencia.

Es necesario recordar que una herramienta forense adecuada debe generar al finalizar el proceso los códigos Hash tipo MD5 y/o SHA1 que garantizan la integridad de la información contenida en la evidencia.

Algunas herramientas para crear imagen forense son:

- ✓ Línea de comando de Linux
- ✓ FTK Imager
- ✓ Entre otras

- **Embalar, Rotular y generar la cadena de custodia:** La evidencia digital original debe ser embalada y rotulada para evitar su manipulación física y/o alteración de los datos que contiene. Un adecuado proceso de embalaje debe contar con elementos tales como bolsa de burbujas, bolsa antiestática y bolsa de manila; mientras que el rotulado debe incluir Identificadores como lo son un código único de la evidencia, el color, la marca, seriales, códigos hash, fechas, horas de recolección y datos de la persona que realiza el embalaje.

Sellar el embalaje con el rotulo y diligencia los formatos de cadena de custodia de acuerdo a la legislación del país en cuestión.

Realizar el Análisis Forense apoyándose en Herramientas especializadas que permitan analizar la información contenida en la imagen adquirida. Aunque las herramientas pueden ser de software libre o licenciadas, asegurarse que estas cuenten con acreditación y aceptación en los estrados judiciales del país.

Algunas herramientas para Análisis forense son:

- ✓ Caine
- ✓ DEFT
- ✓ Autopsy
- ✓ Encase
- ✓ FTK
- ✓ Entre otros

Generar dos tipos de informes: Debe generarse un ***informe técnico*** con todo el detalle técnico de la labor realizada, este informe está dirigido para la contraparte que debe tener el mismo **perfil técnico;** debe ser muy detallado y cuidadoso. El segundo es un ***informe gerencial*** en el cual se presenta el resumen de las actividades realizadas y las conclusiones.

Para la sustentación en Juicio de la labor realizada, se debe tener en cuenta los siguientes lineamientos:

- ✓ Preparar ayudas audiovisuales
- ✓ Revisar el informe técnico presentado, en especial las conclusiones
- ✓ De ser posible preparar con el abogado del cliente el cuestionario a desarrollar.

TOP DISTROS PARA INICIARSE EN EL MUNDO LINUXERO

GNU/LINUX

En el mundo de los Sistemas Operativos hay quienes aún se resisten a probar distribuciones libres, por la que aparentan ser Sistemas Operativos complejos.

Escrito por: @**DENISSE** | **CO-ADMIN** UNDERC0DE

Informática de profesión, adicta al mundo de la tecnología, involucrada en el gremio educativo con énfasis informático, participante en el desarrollo de un proyecto educativo que fomenta la lectura en niños, llamado GoGoReaders. Moderadora de los subforos Debates y Diseño Gráfico, partidaria de redactar temas que causen distintas opiniones y que sean de interés de la comunidad, gusta del Diseño, aunque no por profesión, pero si por afición, y ferviente colaboradora en el foro Underc0de, participando por pasión a la comunidad.

Contacto:
underc0de.org/foro/profile/Denisse

Aunque la **comunidad Linuxera** va en aumento para distintos ámbitos laborales, algunos no terminan de adaptarse y algunos se quedan en el intento, lo cierto es que Linux, nos presenta decenas de opciones para familiarizarse con el mundo del software libre.

Y aquí tenemos el siguiente top 4:

Ubuntu

Sin duda es la distro más popular de Linux, basada en **Debian** (otro de los favoritos por excelencia), su presencia en el mundo de Sistemas Operativos desde hace mucho tiempo, por lo tanto, cuenta con una comunidad enorme, actualizaciones continuas.

Ubuntu[7] cuenta con una interfaz gráfica demasiado intuitiva y a nivel de escritorio llega con Gnome.

Para probar esta distribución de Linux sin instalarla o sin configurar una máquina virtual, es posible hacerlo mediante **OnWorks**[8]**.**

Linux Mint[9]

Distro basada en Ubuntu, con un entorno totalmente amigable, con paquetes incorporados que simplifican la configuración, cuenta con varias ediciones, teniendo **Cinnamon Edition** la versión más amigable, con XFCE un gestor de ventanas fluido y bonito con un buen funcionamiento.

elementary OS[10]

Basado en **Ubuntu** resultando estable e intuitivo, una distro que es considerada para los usuarios que vienen de Apple, con una interfaz que hace referencia a las versiones de macOS, desde los botones y aplicaciones como AppCenter que es parecido al de Apple.

Para probar esta distribución de Linux sin instalarla o sin configurar una máquina virtual, es posible hacerlo mediante **OnWorks.**

Manjaro

Una distribución basada en **ArchLinux** (Destacada por su estabilidad y robustez), si bien tiene excelentes características, mediante Manjaro[11] es posible facilitar la instalación y tener ArchLinux con una interfaz gráfica amigable con la que es posible adaptarse pronto a su entorno.

---

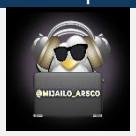
[7] ubuntu.com/#download-content
[8] underc0de.org/foro/gnulinux/experimentar-con-sistemas-operativos-alternativos-desde-el-navegador/
[9] blog.linuxmint.com/?p=3669
[10] elementary.io
[11] manjaro.org

UNA EXPERIENCIA INFORMÁTICA CON: ORCA

GNU/LINUX

Un concepto que poco comentamos es la **Brecha Digital**, utilizado para hacer referencia a la diferencia tecnológica para quiénes tienen acceso a las **TIC** (Tecnologías de la Información y Comunicación) y quiénes no, nos referimos a Smartphone, ordenador, Internet y software. Los posibles generadores de estas diferencias son desde nivel socioeconómico hasta la capacidad de usar la Tecnología de forma eficaz, ya que existen distintos grados de alfabetización y capacidades diferentes.

Escrito por: **@MIJAILO_ARSCO** EN COLABORACIÓN CON **UNDERC0DE**



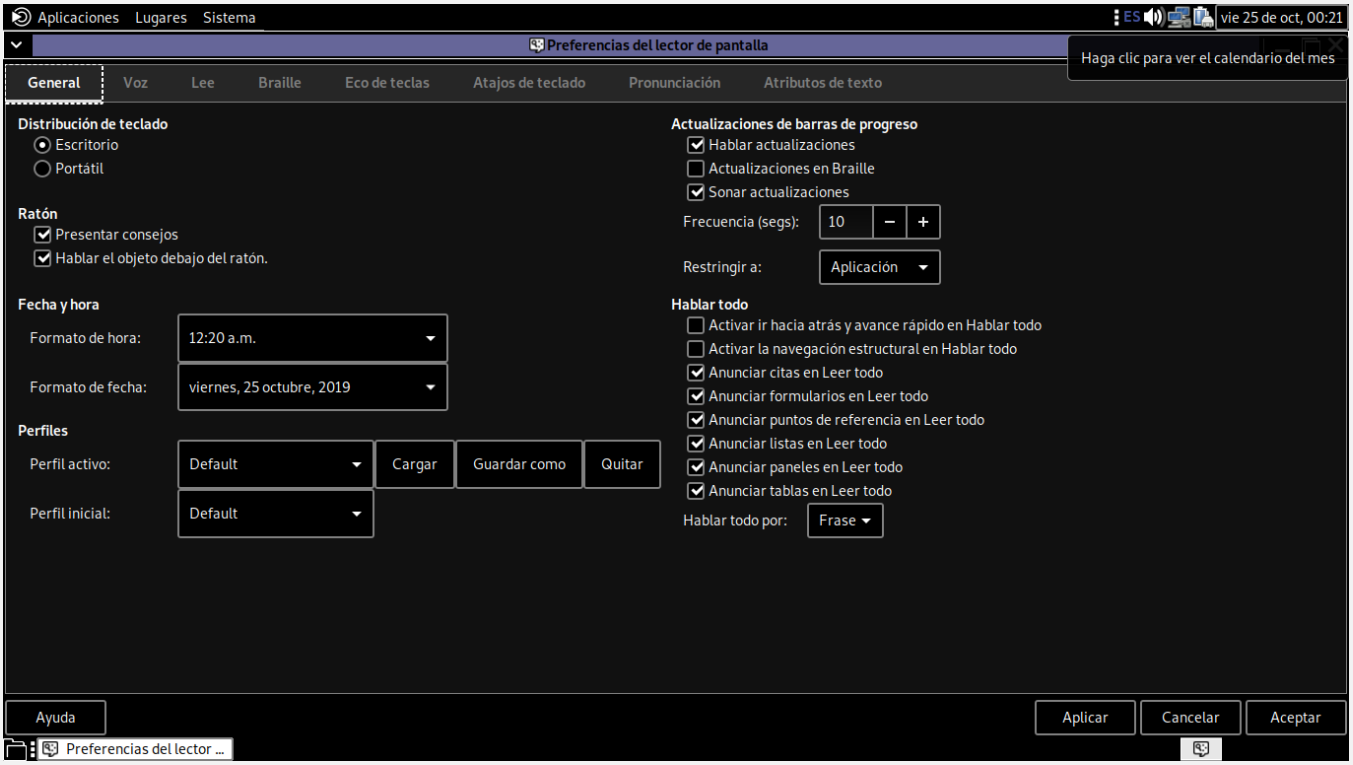
Entusiasta del área informática, dispuesto a brindar apoyo a quien lo necesite ofreciendo guía para interactuar en el medio digital con apoyo de herramientas. Antes dedicado a desarrollo de software en el área de accesibilidad, su principal interés en personas con capacidades diferentes. Quien se desenvuelve en un mundo virtual gracias a herramientas que le permiten interactuar y desarrollar sus habilidades.

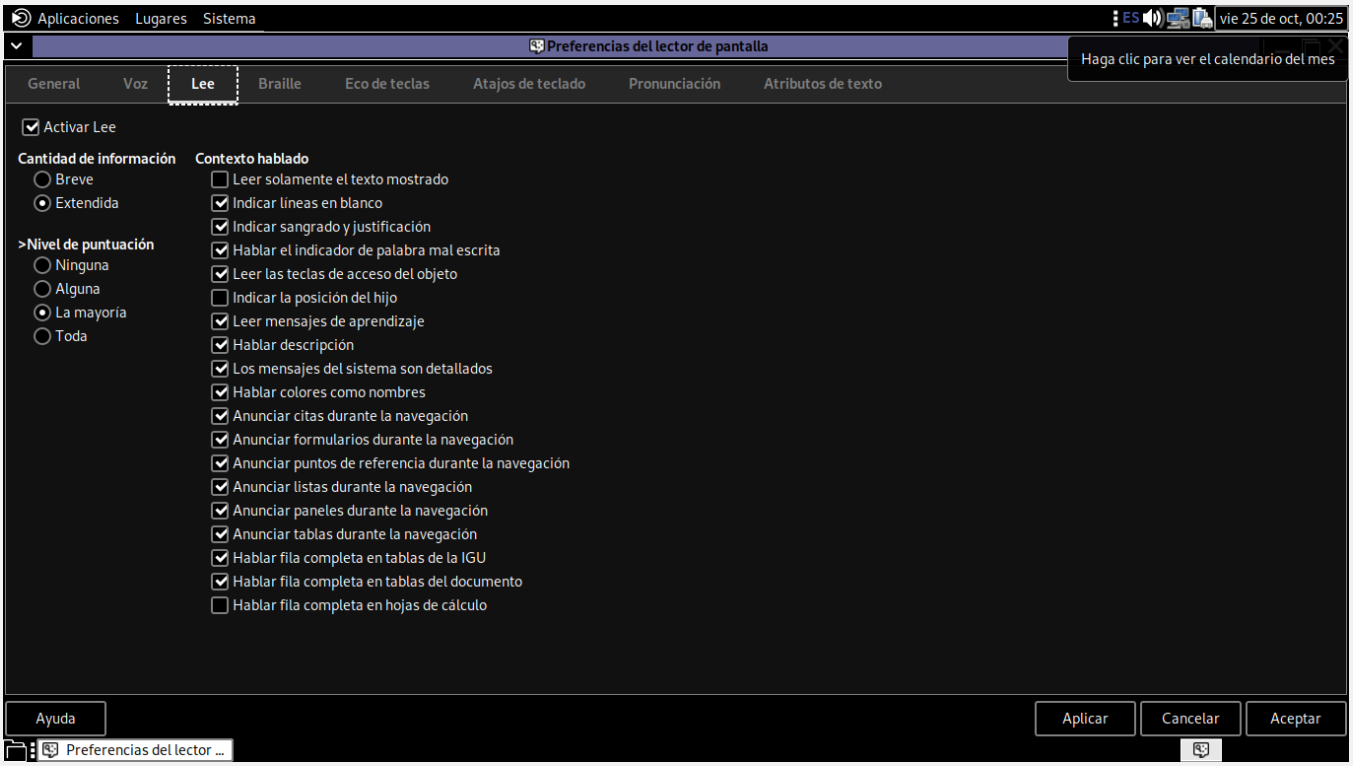
Contacto:
underc0de.org/foro/profile/Mijailo_Arsco/
Redes Sociales:
Telegram @Mijailo_Arsco
UnderDOCS agradece contacto con el autor a: @elhada3d

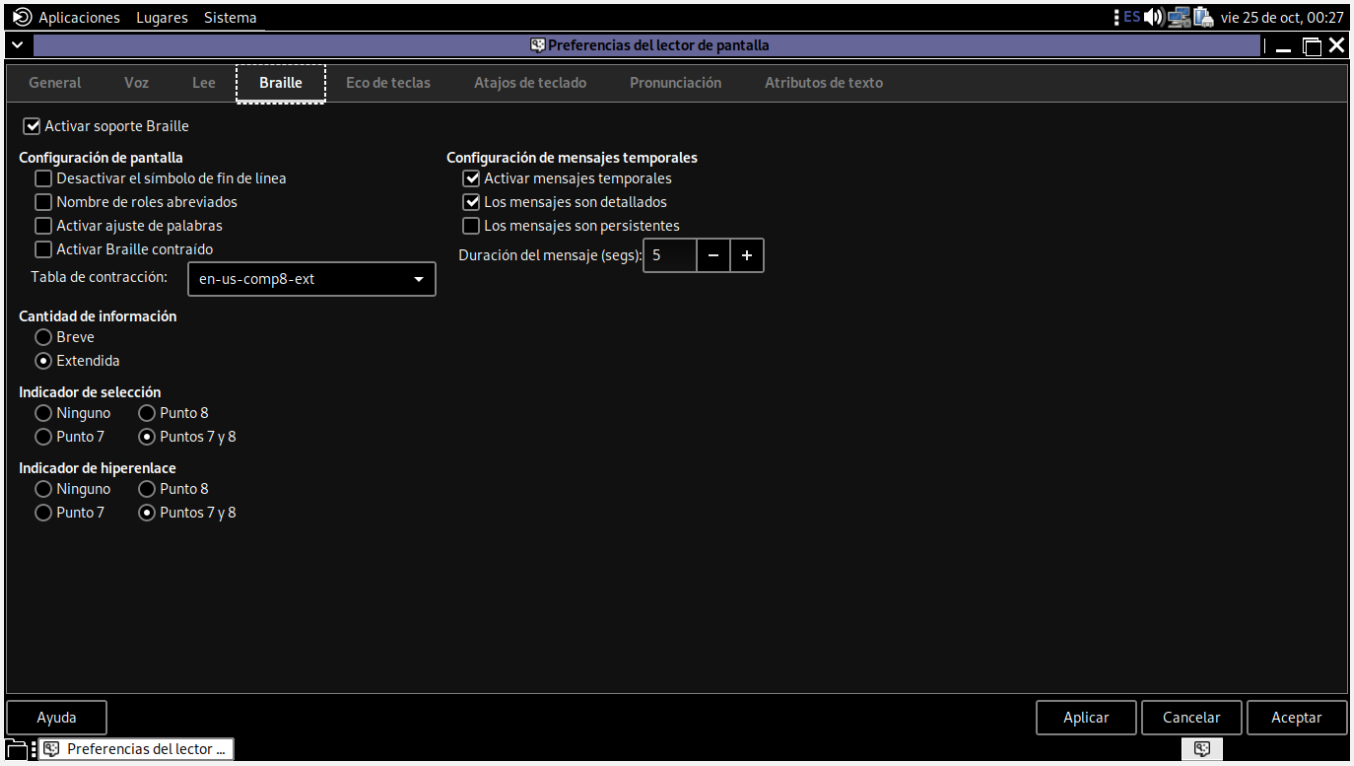
El mundo **GNU/Linux** ha desarrollado herramientas para asistir a las personas con discapacidad visual o motriz; y uno de ellos son los lectores de pantalla, por ejemplo, **ORCA**, cuya función es facilitar la experiencia de uso para personas con discapacidad visual, una solución gratuita e integrada en sistemas compatibles con plataformas **Solaris y GNU/Linux**.

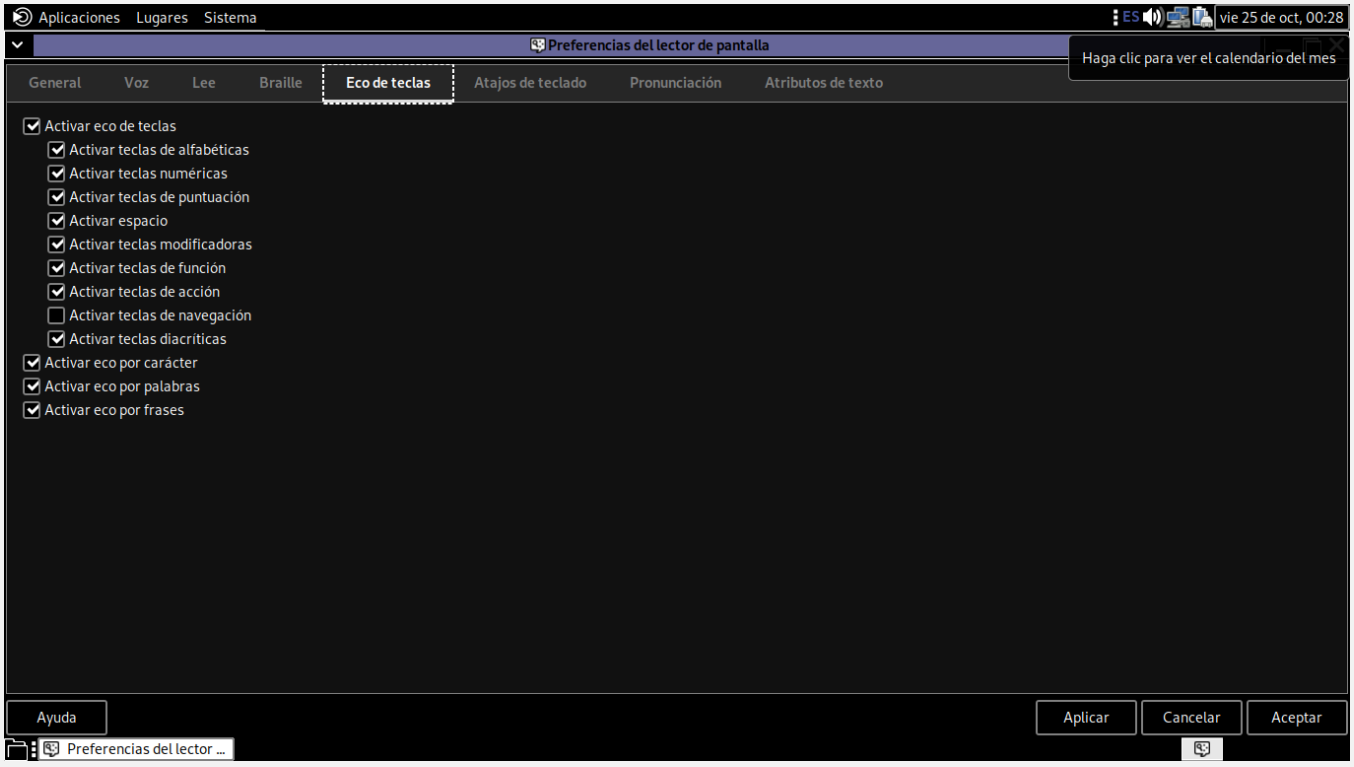
El lector de pantalla **ORCA**, permite al usuario invidente interactuar con su sistema mediante la utilización de la interfaz de audio (parlantes), con la posibilidad de trabajar magnificación de pantalla y Braille, un dispositivo especial para invidentes, conectado al puerto USB.

Interfaz de Lector de Pantalla Orca









ORCA, *es un lector de pantalla flexible*, integrado en algunos escritorios e instalable en otros, con los que tiene compatibilidad. En la actualidad, generalmente, lo podemos encontrar en el escritorio **Gnome** y mate; también se encuentra en algunos derivados del escritorio Gnome, sus creadores aseguran que hay compatibilidad con los *escritorios XFCE y LXDE*.

Iniciar el Lector ORCA[12]

- Mediante la combinación de las teclas **Alt + super (Windows) S**
- Otra forma de iniciarlo es oprimiendo la **tecla Alt + F2,** después escribiendo la palabra **ORCA** y oprimiendo la **tecla Enter**

Por defecto el lector de pantalla nos indicará que se ha activado, mediante ***una voz sintetizada.*** A partir de éste momento la navegación por pantallas y sus diferentes elementos será asistida mediante la voz que nos indicará los **textos, controles y demás objetos que integran el sistema y sus aplicaciones**; ahora podemos utilizar el computador tal cual lo hace un vidente mediante la descripción y orientación de lo que se muestra en pantalla.

Una vez activado el *lector de pantalla* en la instalación realizada, la voz se iniciará con el sistema obteniendo la **accesibilidad** hasta el momento en que se apaga el computador.

En el caso de **algunos sistemas de escritorio como Cinnamon y Budgie**, existe compatibilidad con ORCA, pero no del todo y no siempre se encuentra instalado; en el caso de las distribuciones con **escritorio XFCE y LXDE** es posible instalar esta herramienta que facilita el uso de computadoras:

- Buscando la palabra ORCA en la tienda de software
- O bien mediante el terminal **instalando el paquete gnome-ORCA** y sus dependencias.

> *Claro está, con la ayuda de un vidente.*

Cabe señalar, que la **voz sintética** por defecto es algo robótica, pero se puede instalar una voz llamada **PicoTTSs** algo más humana pero monótona.

> *Esperemos que en un futuro cercano haya muchas más opciones con tonos de voz mucho más humanas, en los repositorios de cada distribución.*
> *Siendo **usuario actual de ORCA**, este lector es comparable a las opciones comerciales de plataformas exclusivas, el aprendizaje, adaptación y manejo del software no insume demasiado tiempo. Los resultados se ven pronto de forma simple y eficaz.*

Algo importante, es indicar que **el uso de los lectores de pantalla**, no está únicamente confinado a las personas **ciegas o baja visión**, sino que también algunas personas que no saben leer pueden aprovechar la función de lectura en textos y de los elementos propios de las pantallas del sistema y así poder utilizar un computador que por su carencia educativa antes no podría hacerlo. En éstos casos también les permitiría aprender a leer, observando el texto leído y escuchando su correspondiente pronunciación.

[12] **Página oficial Lector de Pantalla y Magnificador Orca:** wiki.gnome.org/Projects/Orca

Además, la población vidente se puede beneficiar con la incorporación de los lectores de pantalla en los sistemas informáticos, pues les permite utilizar la función de lectura continua en la lectura de páginas web o documentos extensos permitiendo escuchar el texto deseado al tiempo que realizan otras actividades lejos de la pantalla del computador, incluso pudiendo descansar la vista, **ayudando a la protección de la salud visual.**

Nociones básicas del trabajo del lector de pantalla.

A continuación, hablaremos cómo funciona el lector en la interfaz gráfica del sistema operativo.

- **Recorrido**: La manera en que **ORCA lee los textos** en la pantalla es en **orden secuencial,** de izquierda a derecha, luego avanzando a la siguiente línea.
- **Imágenes**: Donde encuentra una imagen incrustada leerá el nombre de la imagen y su descripción, si esta la posee.
- **Pantallas**: En el caso de las pantallas en general, primero se anunciará el nombre de la ventana, los elementos dentro de ella se podrán acceder presionando la tecla tabulador o flechas, esto dependerá del elemento o el área en la pantalla seleccionada, para retroceder al elemento anterior es necesario presionar las **teclas shift + tabulador**; los **menús** se leerán en forma de lista con los métodos de teclado según cada función del menú, *esto último si está activado en la configuración de ORCA.*
- **Navegación de las ventanas del explorador de archivos:** Dependerá de cuál explorador está instalado.
- **Barras de progreso de una tarea:** Se verbalizará el porcentaje de la acción realizada, cada cierto tiempo y se escuchará un sonido de grave a agudo según el avance del porcentaje de la acción, *esto si así se configuró en el ORCA*.
- **Administrador de ventanas:** Permitirá escuchar las ventanas entre las que se puede cambiar, presionando la combinación de teclas **Alt + Tabulador.**
- **Notificaciones de sistema:** Serán leídas y reproducidas por ORCA.
- **Reproductores multimedia:** Se utilizarán mediante los métodos de teclas abreviados, o bien; con los botones de la interfaz gráfica, los cuales se verbalizarán, **además del nombre del archivo de multimedia reproducido**.
- **Editores de texto:** Los principales del sistema permiten la lectura y edición de textos de forma accesible con ORCA, lo recomendable es utilizar los menús para acceder a las funciones.
- **Terminal o ventana de comandos:** Es completamente accesible y verbalizados todos sus contenidos.
- **Botones:** Se activarán mediante las **teclas Enter o Espaciadora**.
- **Cajas de marca o activación:** Se utilizará la tecla Espaciadora.
- **Cajas con menús desplegables:** Se elegirá con flechas direccionales arriba y abajo.
- **Ventanas:** se cerrarán con Alt + F4.

El lector de pantalla verbalizará desde el momento que se enciende y carga el sistema hasta que se apague el computador.

Aunque el área de Accesibilidad en términos de Inclusión Digital va avanzando, una de las comunidades un tanto olvidadas y menos consideradas por los programadores es la discapacidad. La accesibilidad debería incorporar aplicaciones personalizables, permitiendo la adaptación de acuerdo sus necesidades.

Lectura del Artículo en voz de: @79137913 | YouTube youtu.be/EmXuDrQj8wI

SERVIDOR IIS EN WINDOWS: INSTALAR Y CONFIGURAR

SERVIDORES

La red cliente-servidor es aquella en la cual los clientes están conectados a un servidor, en el que se centralizan los diversos recursos y aplicaciones con que se cuenta; poniendo a disposición de los clientes cada vez que estos son solicitados.

Escrito por: **@GOLD MASTER** | **USER** UNDERC0DE

Su área favorita es la parte técnica ya que considera que es un tema fundamental en donde se puede ayudar bastante a usuarios de diferentes regiones. Le gusta estar constantemente actualizado en la tecnología para poder brindar siempre un mayor apoyo a quien lo necesite. Como especialidad le apasiona el hardware y temas en general de la parte técnica en equipos con Windows, Linux entre otros.

Contacto:
underc0de.org/foro/profile/Gold%20Master/

Significa que todas las gestiones que se realizan se concentran en el servidor, de manera que en él se disponen los requerimientos provenientes de los clientes que tienen prioridad, los archivos de uso público, uso restringido, archivos que son de solo lectura y los que, por el contrario, pueden ser modificados, etc.

Diseño y configuraciones

- **Equipo cliente:** Es aquel equipo (ordenador) utilizado por los usuarios de una red solicitando información y servicios a los equipos Servidores.

- **Equipo Servidor:** Un servidor dedicado puede ser exclusivamente de archivos, impresoras, bases de datos, correo electrónico, páginas web, etc.

El equipo servidor funciona como sistema de administración inteligente que procesa las tareas más complejas.

1. Instalaremos el IIS, y para ello deberemos de realizar las instrucciones del video:
   www.youtube.com/watch?v=0InB6f0DIBY

2. Crearemos un acceso directo en el escritorio:

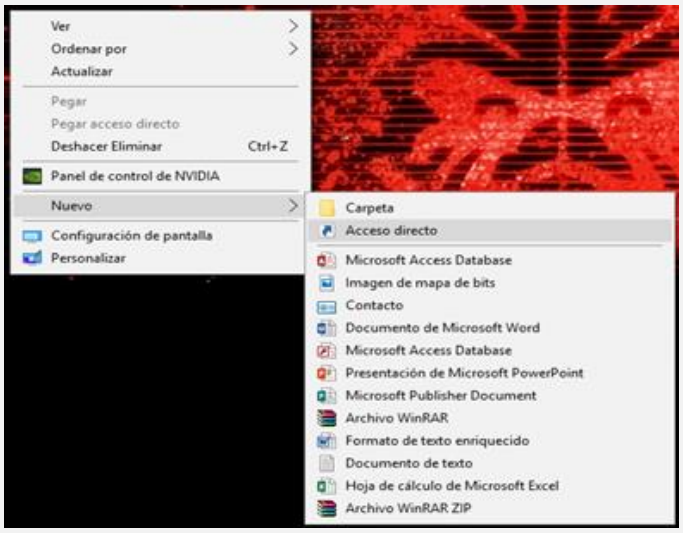


Figura 1. Creación de un Acceso directo en el escritorio.

Se colocó la dirección: **C:\Windows\System32\inetsrv\InetMgr.exe /**

3. Clic en **Siguiente.**

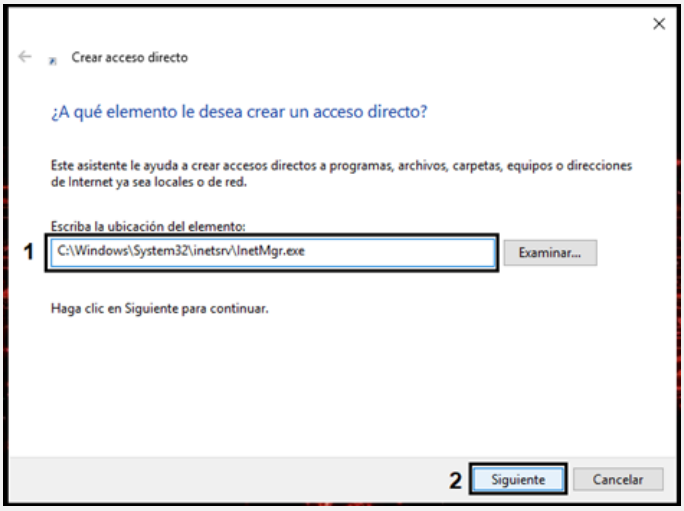


Figura 2. Ruta / ubicación.

4. Únicamente damos clic en **Finalizar**.

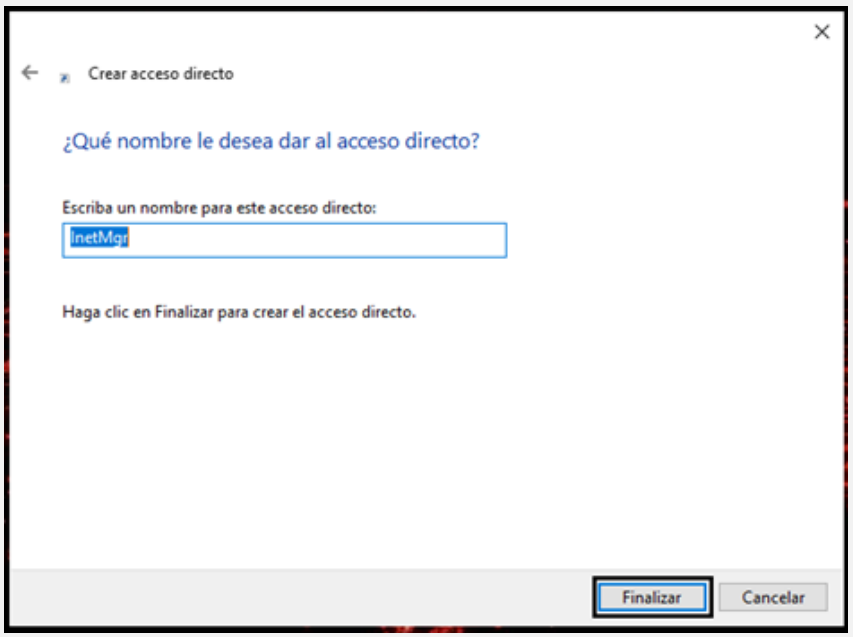


Figura 3. Creación del acceso.

- Desde el **cmd**, estableceremos una carpeta llamada **pruebas** con los comandos mostrados en la imagen, como podemos observar se guardó en la ruta C:\

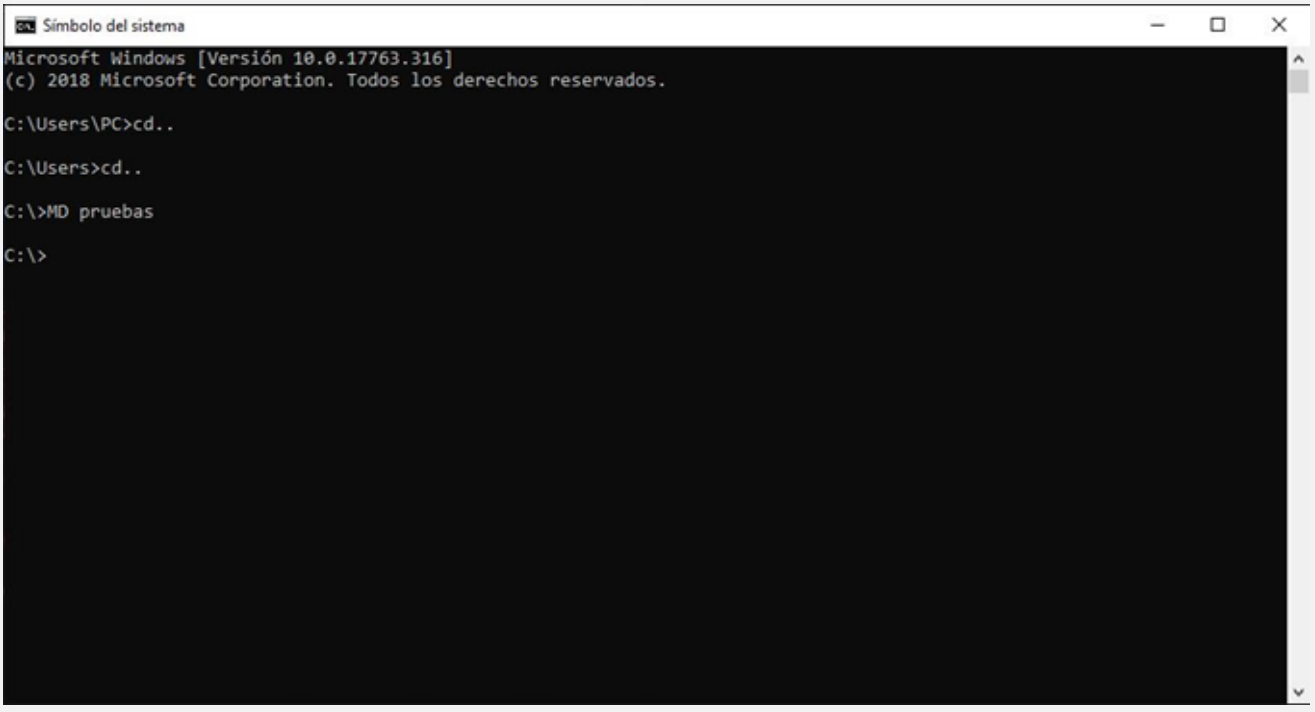


Figura 4. Creación de carpeta en cmd.

El servidor fue el equipo **\\DESKTOP-L04TRAR** y el cliente **\\LAPTOP-P4DJPA0Q**.

- En la ruta **C:** damos clic derecho sobre la carpeta creada "**pruebas**" seleccionamos la opción **Propiedades**.

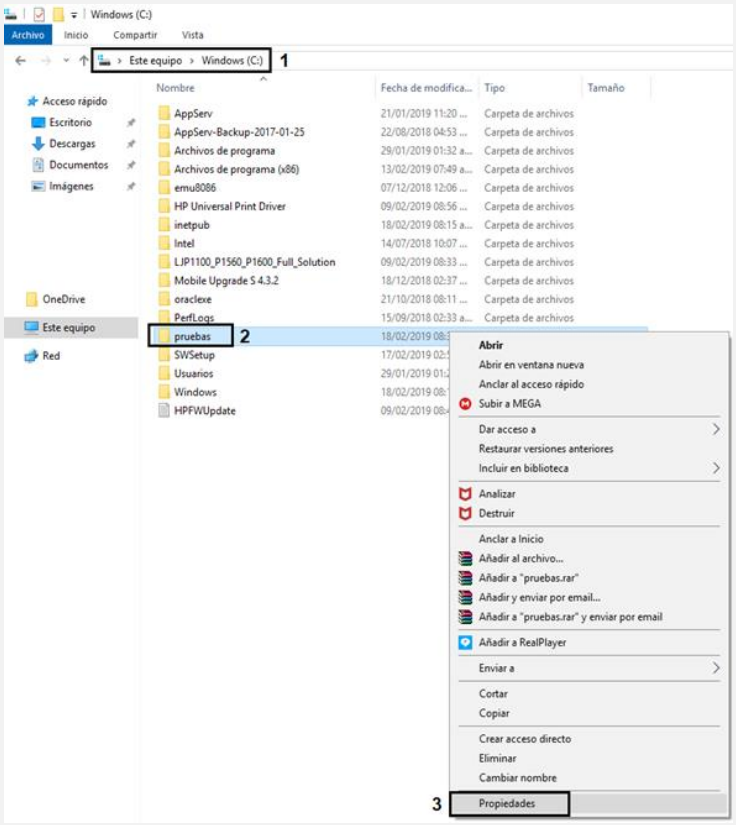


Figura 5. Opciones de la carpeta.

- Nos dirigimos a **Uso compartido** / **Compartir**.

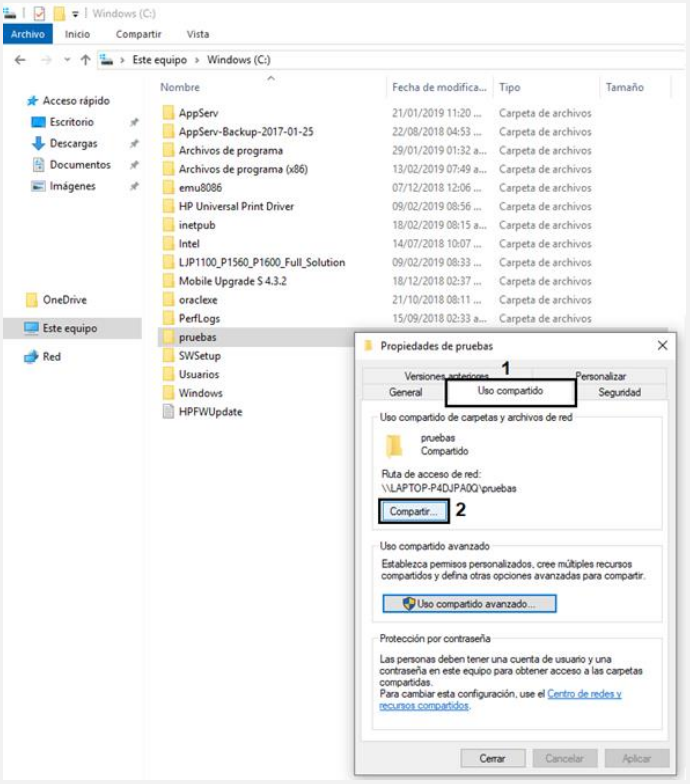


Figura 6. Propiedades de la carpeta pruebas.

- Desplegamos las opciones y seleccionamos **Everyone** / **Agregar** / **Compartir**.

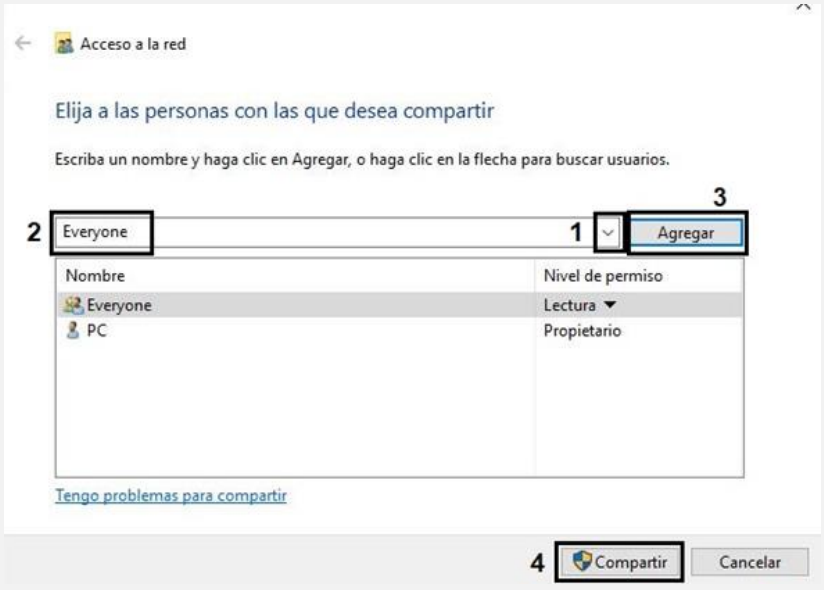


Figura 7. Acceso a la red.

***Nota**: Lo que está subrayado en color azul es la ruta de acceso del pc.*

CREANDO BOTS PARA TELEGRAM

PROGRAMACIÓN

Aprenderemos a crear un **bot** en **Telegram** y programarlo en **Python** para darle funcionalidad. ***Telegram*** es una aplicación de mensajería multiplataforma, disponible en: **Android**, **IOs**, **Windows**, **MacOS** y **Linux,** con una arquitectura basada en la nube optimizada para cualquier dispositivo. Desarrollada por los hermanos **Nikolái y Pável Dúrov**. Ofreciendo grandes posibilidades que en otras aplicaciones de mensajería no existen como: abrir **mega-grupos de hasta 200.000 miembros** o la **creación de bots** gracias a su **API abierta.**

Escrito por: **@DIEGOALTF4** | EN COLABORACIÓN CON **UNDERC0DE**

Entusiasta de la seguridad informática y de la programación. “Si se puede imaginar se puede programar”

Contacto:
diegoaltf4.com

Github: Diegoaltf4coder

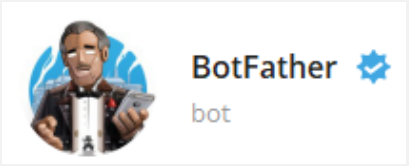
Redes Sociales:
Telegram | **instagram**: diegoaltf4

Lo primero que necesitamos es lógicamente disponer de **Telegram**. Para quienes no lo tengan instalado ingresamos a la página oficial para descargarlo:

telegram.org

creando el bot

Una vez instalado Telegram iniciaremos una conversación con **BotFather**, para ello buscaremos **@BotFather.**

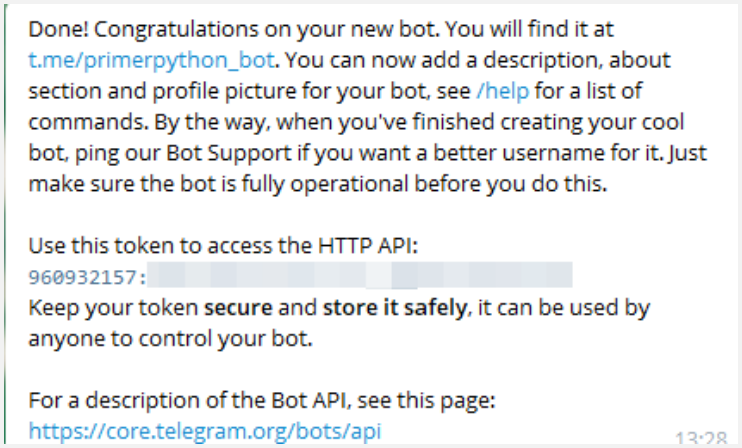


Bot Father es el padre de todos los **bots** y lo necesitamos para crear el nuestro. Iniciamos una conversación con él escribiendo **/start** acción que nos ofrece una serie de posibilidades. Entre ellas destacan:

- /**newbot** - crear un nuevo bot
- /mybots - edita tus bots[beta]
- /setname - cambia el nombre de un bot
- /setdescription - cambiar la descripción del bot
- /setuserpic - cambiar la foto de perfil del bot
- /setcommands - cambia la lista de comandos
- /deletebot - borrar un bot
- /token - genera un token de autorización
- /revoke - revocar el token de acceso al bot

Utilizaremos la función /**newbot**. Nos preguntará el nombre que deseamos asignar a nuestro bot, en este caso "**Hola mundo**". Es necesario seleccionar el **nombre de usuario** el cual debe finalizar con "**_bot**". Nos desplazaremos a la opción para elegir **primerpython_bot**.

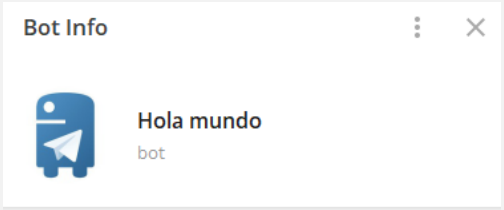
Al momento de crear nuestro bot, nos enviarán el siguiente mensaje:



En el anterior mensaje se nos indica el **token**. Esto es lo **más importante para poder programar el bot**.

Antes de empezar a programarlo, **personalizaremos el bot**, añadiendo ***descripción y foto de perfil*** de la siguiente manera:

- Usando el comando **/setdescription** para la foto de perfil **/setuserpic**.



Si ahora buscamos el **username** de nuestro bot, veremos esa información.

Programación del bot

1. Crearemos un **virtualenv** de **Python**, donde iniciaremos el proyecto.

```
$ apt-get install python3-venv
$ python3 -m venv telegram_bot
$ cd telegram_bot
$ . ./bin/activate
```

2. A continuación, podemos *clonar* el repositorio de GitHub con el ejemplo del bot en:
   github.com/Diegoaltf4coder/Telegram-Bot-Example

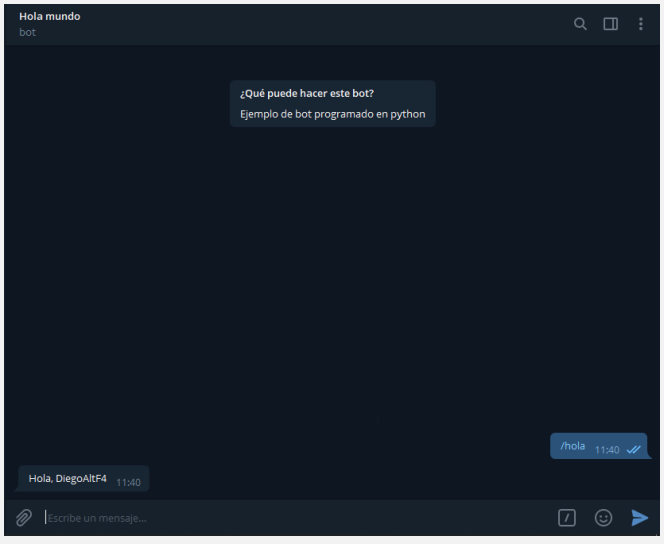
Código: Python

```
1.  #!/usr/bin/env Python
2.  # -*- coding: utf-8 -*-
3.  from telegram.ext import Updater, CommandHandler
4.  TOKEN = 'Pon tu TOKEN aqui'
5.  def hola(update, context):
6.  user_name = update.message.from_user.first_name
7.  context.bot.send_message(chat_id=update.message.chat_id, text="Hola, " + user_name)
8.  def main():
9.  updater = Updater(TOKEN, use_context=True)
10. updater.dispatcher.add_handler(CommandHandler('hola', hola))
11. updater.start_polling()
12. updater.idle()
13. if __name__ == '__main__':
14. main()
```

Básicamente, lo que hace el **bot** es responder al comando "**/hola**", definido en la línea 10 y gestionado en la función de la línea 5.

Para que funcione solo hay que **ejecutar el bot**, y posteriormente abrir una conversación con nuestro respectivo **bot**.

```
root@Diego:~/telegram_bot# python3 holamundo.py
```



No se pierdan en las próximas ediciones **Creación de Bots más avanzados aplicados a la Seguridad Informática.**

CHEAT-SHEET 1: JAVASCRIPT

JavaScript está influenciado sobre todo por la sintaxis de Java, pero también de Awk, Perl y Python.
JavaScript es case-sensitive (distingue mayúsculas y minúsculas) y utiliza el conjunto de caracteres Unicode. Por ejemplo, la palabra Früh (que significa "temprano" en Alemán) puede ser usada como el nombre de una variable.

```
var Früh = "foobar";
```

Pero, la variable **früh** no es la misma que **Früh** porque JavaScript distingue mayúsculas y minúsculas (case-sensitive).
En JavaScript las **Sentencias** y son separadas por un punto y coma (;).

COMENTARIOS

La sintaxis de comentarios es igual a C++ y muchos otros lenguajes:

```
// comentario en una sola línea

/* este es un comentario
   multilínea
 */

/* no puedes, sin embargo, /* anidar comentarios */ SyntaxError */
```

DECLARACIONES

Hay tres tipos de declaraciones en JavaScript.
`var` Declara una variable, inicializándola opcionalmente a un valor.
`let` Declara una variable local en un bloque de ámbito, inicializándola opcionalmente a un valor.
`const` Declara una constante de sólo lectura en un bloque de ámbito.

VARIABLES

Las variables se usan como nombres simbólicos para valores en tu aplicación. Los nombres de las variables, llamados identificadores, se rigen por ciertas reglas.
Un identificador en JavaScript tiene que empezar con una letra, un guión bajo (_) o un símbolo de dólar ($); los valores subsiguientes pueden ser números. Debido a que JavaScript diferencia entre mayúsculas y minúsculas, las letras incluyen tanto desde la "A" hasta la "Z" (mayúsculas) como de la "a" hasta la "z".
Puedes usar la **ISO 8859-1** o letras **Unicode** tales como å y ü en un identificador.

Con la palabra clave `var`.

```
var x = 42
```

Esta sintaxis puede ser usada para declarar tanto v**ariables locales como globales.** Simplemente asignándole un valor. Por ejemplo, x = 42.
Esto siempre declara una **variable globa**l y no puede ser cambiada a nivel local. Esto genera una **advertencia strict de JavaScript**.
Con la palabra clave **let.**

```
let y = 13
```

Esta variable puede ser usada para declarar una **variable local** en un bloque de ámbito.

Se puede usar **undefined** para determinar si una variable tiene un valor. En el siguiente código a la variable input no se le asigna ningún valor y la sentencia de control **if** la evalúa como **true.**

```
var input;
if(input === undefined){
  hazEsto();
} else {
  hazEso();
}
```

El valor **undefined** se comporta como un ***false*** cuando se utiliza en un contexto **booleano**. Por ejemplo, el siguiente código ejecuta la función myFunction porque el elemento **myArray** no ha sido definido:

```
var myArray = new Array();
if (!myArray[0]) myFunction();
```

El valor **undefined** se convierte en **NaN**, ***no numérico***, cuando se usa en una operación aritmética.

```
var a;
a + 2; // Se evalua a NaN
```

Cuando se evalúa una variable nula, el valor null se comporta como el 0 en operaciones aritméticas y como false en operaciones lógicas.
Por ejemplo:

```
var n = null;
console.log(n * 32); // Va a lanzar 0 a la consola
```

ÁMBITO DE VARIABLE

Cuando se declara una variable fuera de una función, se le denomina **variable global**, porque está disponible para cualquier otro código en el documento actual. Cuando se declara una variable dentro de una función, se le denomina **variable local**, porque está disponible solo dentro de esa función donde fué creada.

Antes de **ECMAScript 6 Javascript** no tiene ámbito de sentencias de bloque; más bien, una variable declarada dentro de un bloque es local para la función (o ámbito global) en la que reside el bloque. Por ejemplo, el siguiente código registrará 5, porque el ámbito de x es la función (o contexto global) dentro del cual se declara x, no el bloque, que en este caso es la **sentencia if**.

```
if (true) {
  var x = 5;
}
console.log(x); // x vale 5
```

Este comportamiento cambia, cuando usamos la declaración let introducida en ECMAScript 2015.

```
if (true) {
  let y = 5;
}
console.log(y);  // ReferenceError: y no está definida
```

CONSTANTES

Puede crear una de solo lectura, llamada constante con la palabra **clave const**. La sintaxis del identificador de la constante es el mismo como para un indentificador de variable: debe de empezar con una letra, guión bajo(_) o símbolo de dollar($) y puede contener alfabéticos, numéricos o guiones bajos.

```
const PI = 3.14;
```

Una constante no puede cambiar de valor mediante la asignación o volver a declararse mientras se ejecuta el script.
Las **reglas de ámbito** para las constantes son las mismas que las de las variables let en un ámbito de bloque. Si la palabra clave const es omitida, el identificador se asume que representa una variable.
No puedes declarar una constante con el mismo nombre que una función o una variable en el mismo ámbito.

TIPOS DE DATOS

El último estándar **ECMAScript** define ocho tipos de datos
Siete tipos de datos que son primitivos:

- **Boolean:** `true y false.`
- **null:** Una palabra clave especial que denota un valor nulo. Como JavaScript es case-sensitive, null no es lo mismo que Null, NULL, o cualquier otra variante.
- **undefined:** Una propiedad de alto nivel cuyo valor no es definido.
- **Number:** Un número entero o un número con coma flotante. Por ejemplo: 42 o 3.14159.
- **BigInt:** Un número entero con precisión arbitraria. Por ejemplo: 9007199254740992n
- **String:** Una secuencia de caracteres que representan un valor "Hola"
- **Symbol (nuevo en ECMAScript 6):** Un tipo de dato cuyas casos son únicos e inmutables
- **y Object.**

Aunque estos **tipos de datos** son pocos, permiten realizar funciones útiles con las aplicaciones. Los otros elementos fundamentales en el lenguaje son los **Objects** y las **funciones**. Es posible tener objetos como contenedores con nombre para los valores, y las funciones como procedimientos que puede realizar la aplicación.

OFF TOPIC

Gracias a todos los que participaron en:

underc0de.org/foro/underc0de/2tb-de-almacenamiento-gratis!/msg136691/#msg136691

¡FELICITACIONES!

AL GANADOR:

@DHAXOK

PARTICIPANTES:

- **CHOJUN**
- **TRAFIK**
- **DHAXOK**
- **J4G**
- **DANHIEL98**
- **ZAVITAR**
- **SH4DWZ**
- **ZENTRAEDI**
- **BOICOTREFRITO**
- **NOXONSOFTWARES**
- **MRV0LK0VX**
- **BARTZ**
- **ELHADA3D**
- **FORTECKGIRL**
- **DUBETO**
- **MIGUEL ALONSO**
- **SANTER**
- **K A I L**
- **CR4$HCR4CK**
- **BOLIVARNELSO**
- **BRUTSLOM**
- **VIRTUALSHOOT**
- DR__NESTO
- **MIJAILO_ARSCO**

Agradecimientos especiales a **@rommel360** por donar el premio!

TIPOS DE LENGUAJES

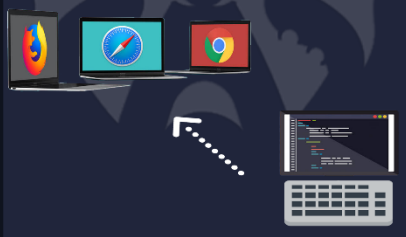
UNDERC0DE

COMPILADO

Convierte el código a binarios que lee el Sistema Operativo.

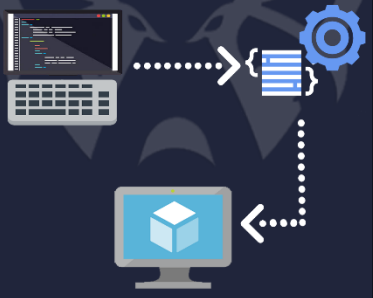
INTERPRETADO

Requieren de un programa que lea la instrucción del código en tiempo real, y la ejecute.



INTERMEDIO

Se compila el código fuente a un lenguaje intermedio y este último se ejecuta en una máquina virtual.



@DENISSE

UNDERTOOLS DIY

CREANDO UN GENERADOR DE CONTRASEÑAS SEGURAS CON VBNET

En esta ocasión **Undertools DIY**, aprenderemos cómo crear un generador de contraseñas seguras con VB.NET en solo 3 pasos.

Escrito por: @**79137913** | **CO-ADMIN** UNDERC0DE

79137913

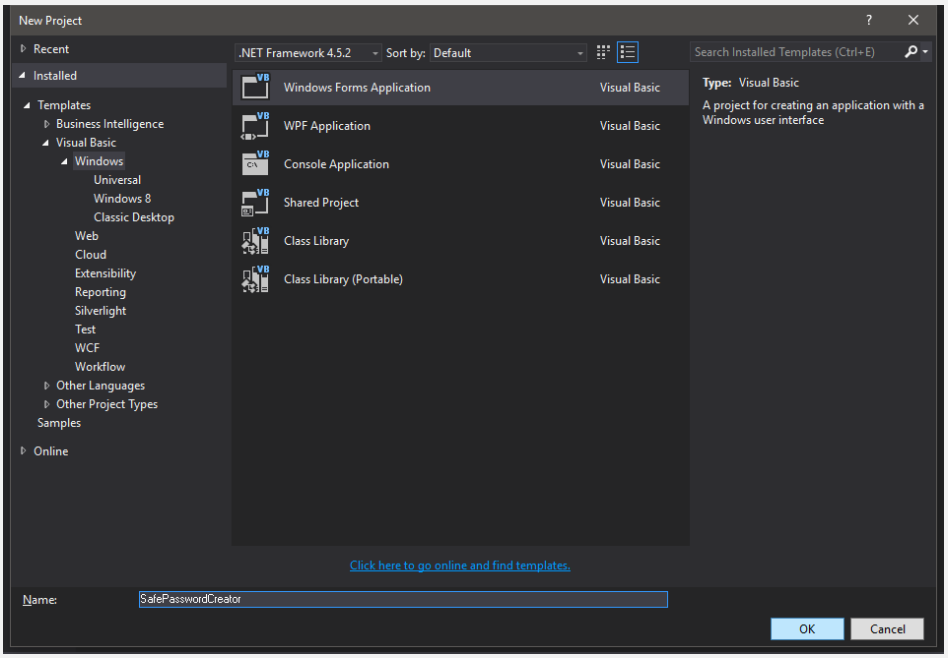
Hello my name is 79137913, I'm a lonely bot with an advanced artificial intelligence, at your service.

Contacto:
underc0de.org/foro/profile/79137913

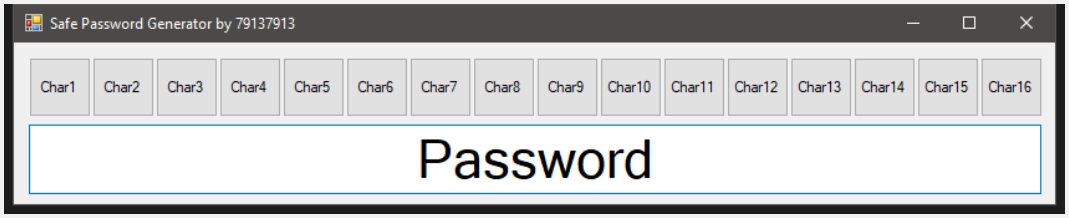
taller

Aunque no tengan conocimientos de programación verán que leer el código y hacer pequeñas modificaciones será muy simple, y quien sabe, por ahí estos sean sus primeros pasos para convertirse en **Developer.**

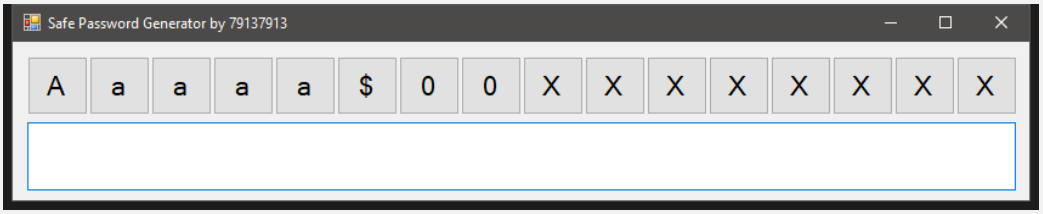
1. Crearemos el proyecto



2. Luego en el Form1 Realizar la siguiente interfaz (respetando los nombres de los controles):



3. Y luego poner las **propiedades .Text** de la siguiente forma:



4. Vamos a la sección de código del formulario y pegamos lo siguiente:

Código: vb.net

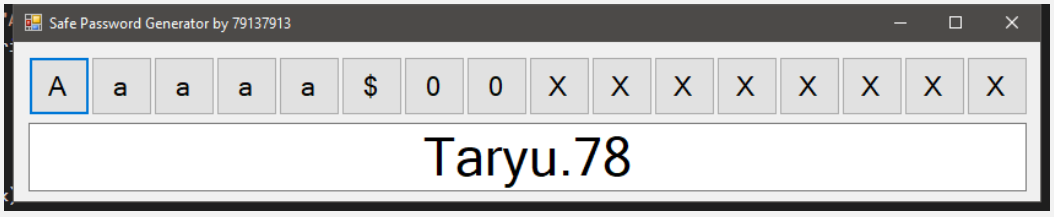
```
1.  'By 79137913 for http://underc0de.org
2.  Module ControlArray
3.      'creamos un Array de controles con los botones asi es mas facil manejarlos.
4.      Public Chars() As Button = {Form1.Char1, Form1.Char2, Form1.Char3, Form1.Char4,
    Form1.Char5, Form1.Char6, Form1.Char7, Form1.Char8, Form1.Char9, Form1.Char10,
    Form1.Char11, Form1.Char12, Form1.Char13, Form1.Char14, Form1.Char15, Form1.Char16}
5.  End Module
6.  Public Class Form1
```

```
7.      Dim Sym() As String = Split("/ \ ! · $ % & / ( ) = ' "" ¡ ¿ ? < > . , : ; - _ * +")
    'Simbolos
8.      Private Function PalabrasPronunciables7913(Letras As Long) As String
9.          Dim Aux As Long 'Caracteres restantes
10.         Dim Act As Long 'Variable para hacer aleatorio el select
11.         Dim Ret As String = "" 'Variable de retorno
12.         Dim Uno() As String : Dim Dos() As String 'Variables de almacenamiento de silabas
13.         Dim Tre() As String : Dim Tr2() As String : Dim Tr3() As String 'Variables de
    almacenamiento de silabas
14.         Dim Cua() As String : Dim Cu2() As String : Dim Cin() As String 'Variables de
    almacenamiento de silabas
15.         Randomize() 'Utilizado para que las combinaciones siempre sean diferentes
16.         Uno = Split("a e i o u")
17.         Dos = Split("ab ad ak al am an ar as az ba be bi bo bs bu da de di do du ed ef ek
    el em en er es fa fe fi fo fu ga ge gi go gu ia id ie im in ir is iz ja je ji jo ju ka
    que ki ko ku la le li lo lu ma me mi mo mu na ne ni nn no nu ña ñe ñi ño ñu ob oi ok ol
    on op or os pa pe pi po pu qa ra re ri ro ru sa se si so ss su ta te ti to tu ud ue ui uk
    ul um un ur us xa xe xi xo xu ya ye yi yo yu za ze zi zo")
18.         Tre = Split("abs bad bal ban bar bas bea bed bel ben ber bes bia bid bie bik bil
    bin bir bis bla ble bli blo boa boi bol bom bor bos boz bra bre bri bro bru bue bui bul
    bur bus cha che chi cho chu dad dak dam dan dar das dea ded del den der des dez dia did
    die dir dis doa doi don dop dor dos dra dre dri dro dru dua due duk dum duo dur duz eks
    fad fak fal fan far fas fek fen fer fes fia fid fie fil fin fir fis fla flo flu fon for
    fra fre fri fue fui fun gad gal gan gar gas gem gen ger ges gia gid gie gil gir gis gla
    gle glo gol gon gor gos gra gre gri gro gru gua gue güi gun guo gus ian ias ier ils ins
    jad jak jal jan jar jas jaz jed jem jen jer jes jia jid jie jir jis jon jor jos jue")
19.         Tr2 = Split("jun jus juz kad kal kam kan kar kas kea kel ken kes kez kia kie kin
    kis kla kle kli klo klu koe kol kom kon kor kos kot kra kre kri kro kru kua kue kui kul
    kum kun kuo kur lad lan lar las lea led lek len ler les lez lia lie lim lin lir lis lla
    lle lli llo lom lon lor los lua lud lue lum lun lus lus mad mak mal man mar mas mea med
    mek men mer mes mez mia mid mie mil min mir mis miz mon mor mos mue mui mul mun nad nal
    nan nar nas naz nea ned nen ner nes net nez nia nid nie nin nir nis nom nor nos noz nua
    nue nui nun nuo ñad ñak ñan ñar ñas ñed ñen ñes ñia ñir ñis ñol ñor ños oia oid oim oir
    ois pad pak pal pan par pas paz pea pek pel pen per pes pez pia pie pin pis pla ple")
20.         Tr3 = Split("pli plo pon por pos pra pre pri pro pru pue pul pun pur pus rad rak
    ral ran rar ras raz rea red rek ren res rez ria rid rie rir ris roa roe ron ros rra rre
    rri rro rru run sad sak sal san sar sas saz sea sed sek sem sen sep ser ses sia sie sig
    sil sim sin sir sis soi sol son sor sos sua sub sul sun sur sus tad tal tam tan tar tas
    tea ted tek tem ten ter tes tia tid tie tin tir tis toi ton tor tos tra tre tri tro tru
    tua tud tue tui tum tun tuo tur tus tut ueb uel ues uia uid uin uir uis xak xan xar xas
    xed xen xer xes xia xid xie xir xis xue xun yad yan yar yas yek yen yer yes yor yos yun
    zad zad zam zan zar zas zea zed zen zep zer zes zia zid zie zin zir zis zit zon zos")
21.         Cua = Split("bean beas biad bian biar bias biem bien bier bies blad blan blar
    blas blen bles blos brad bran brar bras bren bres bria brid brie bril brin brir bris bron
    bros buel buen buia buid buir buis chad chan char chas chen ches chis chos deas diad dial
    dian diar dias dien dies diez doem doin drad dran drar dras dren dres dria drid dron duad
    duan duar duas duen duer dues fiad fian fiar fias fien fies flek flik flui fran fras fren
    fres fria frie frir fron fuel fuen fuer fuis giad giar gias gien gies glad glan glar glas
    glen gles grad gran grar gras gren gres gris gros guad gual guan guar guas guen gues guez
    jiad jian jiar jias jien jies joan juez kear kers kiad kian kiar kief kien kier kies king
    klad klan klar klas klea klen kles klos klui koin kons krea kred kren krer kres krez kria
    krie kruz kuad kual kuam kuan kuar kuas kuel kuen kuer kues kuns lead")
22.         Cu2 = Split("lean lear leas lian liar lias lien lies llad llan llar llas llen
    lles llon llos luar mean mear meas mian mias miem mien mier muer mues neas nian nias nien
    nuad nuan nuar nuas nuen nues nuia nuid nuir nuis nuks ñias oian oias pers piad pian piar
    pias pien pier pies plan plas plea plen ples plid plie plir plis plus prad prak pran prar
    pras pren prer pres prie prin proe proi prok prue puer pues reas riad rial rian riar rias
    rien ries rins rrad rran rrar rras rrea rred rrek rren rrer rres rria rrid rrie rrin rrir
    rris rrom rrue sead sean sear seas sian sias siem sien soft sual tead tean tear teas teks
    ters tial tian tias tiem tien tlan trad tral tram tran trar tras tren tres trol tros tros
    trui truk tuad tual tuan tuar tuas tuen tuer tues tuia tuid tuir tuis uian uias xian xias
    xien zead zean zear zeas ziad zial zian ziar zias ziem zien zier zies")
23.         Cin = Split("brean brian brias buian buias drian drias fluen fluia fluid fluir
    fluis frian frias frien fries kluia kluid kluir kluis kread krean krear kreas kriad krian
    kriar krias krien kries nuian nuias plead plean plear pleas plian plias plien rreak rreal
    rrian rriar rrias rrien rries trans truia truid truir truis tuian tuias fluian fluias
    kluian kluias truian truias")
24.         Do
25.             Aux = Letras - Ret.Length
26.             If Aux <= 0 Then Return Ret
27.             If Aux > 5 Then
28.                 Act = Int(Rnd() * 5) + 1
29.             Else
30.                 Act = Int(Rnd() * Aux) + 1
31.             End If
```

```
            Select Case Act
                Case 1
                    Ret = Ret & Uno(Int(Rnd() * 5))
                Case 2
                    Ret = Ret & Dos(Int(Rnd() * 130))
                Case 3
                    Select Case Int(Rnd() * 3)
                        Case 0
                            Ret = Ret & Tre(Int(Rnd() * 170))
                        Case 1
                            Ret = Ret & Tr2(Int(Rnd() * 170))
                        Case 2
                            Ret = Ret & Tr3(Int(Rnd() * 170))
                    End Select
                Case 4
                    Select Case Int(Rnd() * 2)
                        Case 0
                            Ret = Ret & Cua(Int(Rnd() * 171))
                        Case 1
                            Ret = Ret & Cu2(Int(Rnd() * 171))
                    End Select
                Case 5
                    Ret = Ret & Cin(Int(Rnd() * 59))
            End Select
        Loop
    End Function
    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        For Each bt As Button In Me.Controls.OfType(Of Button)()
            'Poner los event handlers de cada boton en el mismo sub.
            AddHandler bt.Click, AddressOf ButtonChar_Click
        Next
        Password.Text = MakePass()
    End Sub
    Private Sub ButtonChar_Click(sender As Object, e As EventArgs)
        Dim bt = DirectCast(sender, Button)
        'Cambiamos el Texto del boton
        Select Case bt.Text
            Case "A"
                bt.Text = "a"
            Case "a"
                bt.Text = "Aa"
            Case "Aa"
                bt.Text = "0"
            Case "0"
                bt.Text = "$"
            Case "$"
                bt.Text = "X"
            Case "X"
                bt.Text = "A"
        End Select
        Password.Text = MakePass() 'Creamos una contraseña
    End Sub
    Private Function MakePass() As String
        Dim AuxString As String = ""
        Dim AuxPass As String = "xxxxxxxxxxxxxxxx"
        Dim FlagProcesar As Boolean = False
        For x = 0 To 15
            'Armar Pass
            Select Case Chars(x).Text
                Case "A"
                    AuxString = AuxString & Chars(x).Text
                Case "a"
                    AuxString = AuxString & Chars(x).Text
                Case "Aa"
                    'Elegir aleatoriamente mayuscula o minuscula
                    If Int(Rnd() * 2) Then
                        AuxString = AuxString & "A"
                    Else
                                AuxString = AuxString & "a"
                        End If
                   Case "0"
                        'Elegimos aleatoriamente el numero
                        Mid(AuxPass, x + 1, 1) = Int(Rnd() * 10)
                        FlagProcesar = True
                   Case "$"
```

```
107.                            'Elegimos aleatoriamente el simbolo
108.                            Mid(AuxPass, x + 1, 1) = Sym(Int(Rnd() * 26))
109.                            FlagProcesar = True
110.                        Case "X"
111.                            FlagProcesar = True
112.                    End Select
113.                    If FlagProcesar Then
114.                        Mid(AuxPass, x + 1 - AuxString.Length, AuxString.Length) =
    PalabrasPronunciables7913(AuxString.Length)
115.                        For y = 1 To AuxPass.Length
116.                            If Mid(AuxString, y, 1) = "A" Then
117.                                Mid(AuxPass, x - AuxString.Length + y, 1) =
    UCase(Mid(AuxPass, x - AuxString.Length + y, 1))
118.                            End If
119.                        Next
120.                        AuxString = ""
121.                        FlagProcesar = False
122.                        If Chars(x).Text = "X" Then
123.                            AuxPass = Mid(AuxPass, 1, x)
124.                            Exit For
125.                        End If
126.                    End If
127.                Next
128.                Return AuxPass
129.            End Function
130.        End Class
```

Cuando ya colocamos el código solo queda iniciar (presionar F5) y empezar a usarlo solo clickeamos los botones para elegir el patrón de texto que queremos para nuestra contraseña y la magia comienza:



Para descargar el proyecto completo ingresa a:

Para los curiosos:

En esta edición tenemos 2 cosas muy interesantes, la primera, cómo crear arrays de controles y cómo unir los handlers a un solo sub y la segunda es la función PalabrasPronunciables7913 que permite obtener palabras pronunciables de cualquier largo, puede ser muy útil si son creativos.

mensajes / opiniones de nuestros usuarios

"Hola Felicitaciones por la comunidad y la revista acabo de leer la edición #2 y estoy leyendo la #1 Soy de Mendoza y de la informática. Saludos a todos

@RENZO_ONTIVERO
VÍA GRUPO DE TELEGRAM UNDERC0DE OFICIAL

"Muy buena información.

FREDDY RÍOS CUNNINGHAM
VÍA PÁGINA DE FACEBOOK UNDERC0DE

"Excelente trabajo están haciendo chicos, muchas felicitaciones para ustedes!

KAIRO BARILLAS
VÍA PÁGINA FACEBOOK UNDERC0DE

"Esto sigue siendo increíble

FUENTES URIEL
VÍA PÁGINA FACEBOOK UNDERC0DE

"Muchas gracias Underc0de por el PDF de mucha ayuda.

BETO LOPEZ
VÍA PÁGINA DE FACEBOOK UNDERC0DE

"Muy buena la info...

TEODORO SUELDO
VÍA PÁGINA FACEBOOK UNDERC0DE

"Muchas felicidades continúen así éxito c: buena revista

OSMA ARTE-DIGITAL
VÍA PÁGINA FACEBOOK UNDERC0DE

EXPRESÁTE Y HAZ LLEGAR TU MENSAJE / OPINIÓN
REDACCIONES@UNDERC0DE.ORG

Acerca de UNDERC0DE...

Underc0de nació en 2011, con la visión de ser una comunidad dedicada al Hacking y a la Seguridad Informática, ***comprendiendo la libre divulgación del conocimiento, compartir saberes, intercambiar aportes e interactuar día a día*** para potenciar las capacidades y habilidades de cada uno en un ambiente cordial. Para ello, se desarrollan **talleres, tutoriales, guías de aprendizaje, papers de variados temas, herramientas y actualizaciones informáticas.**

Con un foro nutrido de ***muchas secciones y posts relacionados al hacking y la seguridad informática.*** A diario los usuarios se conectan y comparten sus dudas y conocimientos con el resto de la comunidad.
En una búsqueda constante por mantener online la comunidad y seguir creciendo cada día un poquito más.

Los invitamos a que se **registren** en caso de que no lo estén, y si ya tienen una cuenta, **ingresen**.

¡MIL GRACIAS A TODOS POR LEERNOS Y COMPARTIR!

PRODUCIDO EN LA COMUNIDAD UNDERC0DE, POR HACKERS DE TODO EL MUNDO, PARA PROFESIONALES DE TODO EL PLANETA.