#09

ABRIL 2020
EDICIÓN

DIGITAL MAGAZINE

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

> **Cualquier tecnología suficientemente avanzada es equivalente a la magía.**
> *-Arthur C. Clarke*

UNDERC0DE.ORG

UNDERC0DE

UNDERDOCS #09

"Algunos héroes nacen con superpoderes, otros usan la tecnología.

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.*

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.

LO MEJOR QUE PODEMOS HACER ES ESPERAR.

En la edición correspondiente al mes de abril, presentamos un repertorio de artículos comprometidos con nuestros **lectores**, como cada edición nuestros colaboradores desde donde se encuentran cumplen proporcionándonos parte de su conocimiento generando un contenido variado y de calidad, unidos aunque en diferentes países tomando en cuenta que no sólo afecta el mundo físico si no también virtual, en tiempos sin precedentes que nos exigen soluciones y comportamientos radicales e inéditos, nuestros mejores aliados en estos momentos son los dispositivos electrónicos y el internet.

Comienza donde estas, usa lo que tienes, haz lo que puedes

#YoMeQuedoEnCasa

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM

@ANTRAX
@DENISSE
@DRAGORA
@ANIMANEGRA

@ANDR0Z
@ISAAC_RODRIGUEZ
@ISRAEL_ABARCA
@OROMAN
@GENIOL

@ANDDREPAR
@LRAMOS
@MAXWELLNEWAGE
@HACKPLAYERS
@MAYASCTFTEAM

DIFUSIÓN:

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

hackplayers.com
mayas-ctf-team.blogspot.com
redbyte.com.mx
cerohacking.com

antrax-labs.org
sombrero-blanco.com/blog
diegoaltf4.com
grupos LinuxerOS

- t.me/Ubuntu_es
- t.me/Linuxeros_es
- t.me/DebianLatinoamerica
- t.me/SeguridadInformatica

CONTACTO:

INFO@UNDERC0DE.ORG REDACCIONES@UNDERC0DE.ORG

LA COMUNIDAD INFORMÁTICA QUE ESTÁ REALIZANDO PROTOTIPOS DE MASCARILLAS Y RESPIRADORES ARTIFICIALES

NOTICIAS INFORMÁTICAS

> 📣 JUNTOS DIFUNDAMOS 📣 Un enorme 👐 y agradecimiento a esta comunidad 👐👐. -*REVISTA_ANANDA*

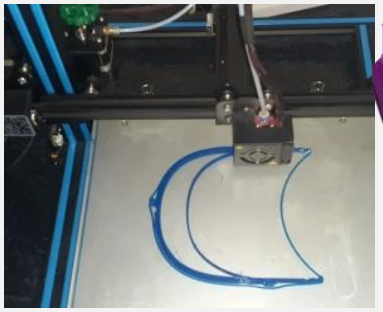
Underc0de es una comunidad informática que tiene más de 9 años de vigencia. Se trata de una plataforma online donde miembros de todo el mundo comparten material sobre infomática, programación, y seguridad entre otras cosas.

En comunicación con ***Ananda Revista de Cuyo*** Danilo Vezzoni, miembro de Underc0de en Mendoza contó que:

> *El principio de la comunidad es compartir lo que saben y aprender de los demás en todo momento y siempre colaborar o ayudar a quienes más lo necesiten»*

A raíz de la situación que está atravesando el país y el mundo entero con la propagación del COVID-19 es que los miembros de Underc0de decidieron unirse al grupo de «Resistencia Argentina» que se están encargando de hacer viseras, respiradores y mascarillas, entre otros elementos, con impresoras 3D, vale aclarar que esta comunidad cuenta con más de 75 mil usuarios en todo el mundo, en Mendoza se estima que son alrededor de 300 personas parte de ella.

anandarevista.com
***Ananda Revista de Cuyo*, Arg.**



Además de realizar dichos elementos con las impresoras 3D, este grupo de personas está colaborando con escuelas e institutos a levantar aulas online para que sus alumnos puedan seguir estudiando.

Ananda Revista de Cuyo

UnderTIPS del uso de internet

NO SATUREMOS LAS REDES

De preferencia:

- Fines informativos, laborales, educativos y de salud.
- Limitar el uso de videollamadas.
- Utilizar servicios de mensajería instantánea WhatsApp/Messenger o teléfono fijo.
- Realizar descargas de archivos pesados en horarios con menor tráfico de datos.
- Ver videos en calidad standard.

UNDERC0DE

vía IFT

UNDERC0DE.ORG

CRUZADA SOLIDARIA- PROTOTIPOS DE MASCARILLAS Y RESPIRADORES

NOTICIAS INFORMÁTICAS

"SOMOS UNA CADENA CON UN SOLO ESLABÓN. UNIDOS POR EL AMOR AL PRÓJIMO. -Elsa América Lugones.

La comunidad informática **Underc0de**, creada hace nueve años por **Danilo Vezzoni**, se sumó a una cruzada solidaria elaborando prototipos de **mascarillas** y **respiradores artificiales** en **impresoras 3D**, para las personas del área de salud y seguridad que están expuestas ante la pandemia del **coronavirus**.
Además, como iniciativa propia, apoyan a **institutos** y **escuelas** montando **aulas virtuales** para que estudiantes y docentes puedan continuar con el normal dictado de clases desde sus casas.

Se trata de una **comunidad abierta** de **habla hispana** "que se ha ido expandiendo y ahora hay personas no solamente de Argentina, sino que, de España, México, Perú, Chile, entre otros", explicó Vezzoni a ***Noticias d*** y agregó: "Los objetivos son **compartir lo que uno sabe y aprender de lo que saben los demás** y siempre **ayudar desinteresadamente**". En cuanto a los proyectos actuales de la comunidad, el **joven analista y programador en sistemas** explicó cómo se sumaron a la creación de prototipos.

*"Como hay faltantes o se estima que va a haber faltantes de vísceras, mascarillas y respiradores artificiales, empezaron a crear grupos en toda la Argentina con el fin de fabricarlas con las impresoras 3D que cada uno tenga en su casa. No es una iniciativa de **UndercOde** sino que la apoyamos, cuando nos enteramos nos **pusimos manos a la obra**, ya que somos muchos los integrantes con esas impresoras,*

www.noticiasd.com
***Noticias d* Godoy Cruz, Arg.**

"Con la propagación del virus creemos que no van a dar abasto con ciertos productos por eso decidimos imprimirlas nosotras con las impresiones 3D.
Hay mascarillas que cubren nariz y boca y vísceras para los doctores, policías y bomberos que van a estar atendiendo a las personas. Tenemos también válvulas de Venturi que se utilizan para los respiradores", especificó.
En solo dos días les solicitaron más de dos mil máscaras. Como no dan abasto con el material y personal, están buscando personas que tengan y sepan usar máquinas 3D, y solidarios que aporten materiales.

AULAS VIRTUALES

El proyecto de las aulas virtuales es una iniciativa de Underc0de, se basa en montar un aula virtual para cada curso, en donde los estudiantes y docentes tienen sus propios usuarios. Así, los jóvenes podrán acceder al foro de sus materias, con el material que carga cada profesor. Lo podrán descargar e incluso tienen la posibilidad de hacer exámenes online.

"Por suerte tenemos colaboradores en todo el país y en toda la provincia.

Noticias d

SCAVENGER- ENCONTRAR INFORMACIÓN SENSIBLE

PENTESTING

Durante un pentest interno, si tenemos suerte y/o la suficiente destreza, obtendremos acceso de nivel administrativo al dominio de Active Directory de Windows. Sin embargo, muchas veces tendremos el problema de tener acceso a demasiados sistemas con días limitados para pruebas. Necesitamos encontrar información valiosa lo antes posible...

Escrito por: **@VIS0R** EN **COLABORACIÓN CON** UNDERC0DE

Vicente Motos, Creador de Hackplayers, blogger y organizador del congreso h-c0n. Consultor de seguridad informática y hacker ético. Actualmente red teamer/threat hunter. Experiencia en arquitectura de sistemas y comunicaciones, investigación de vulnerabilidades, creador de varias herramientas, jugador de CTFs y amante del software libre.

Contacto:

Blog: Hackplayers.com

Redes Sociales:

Con: h-c0n.com

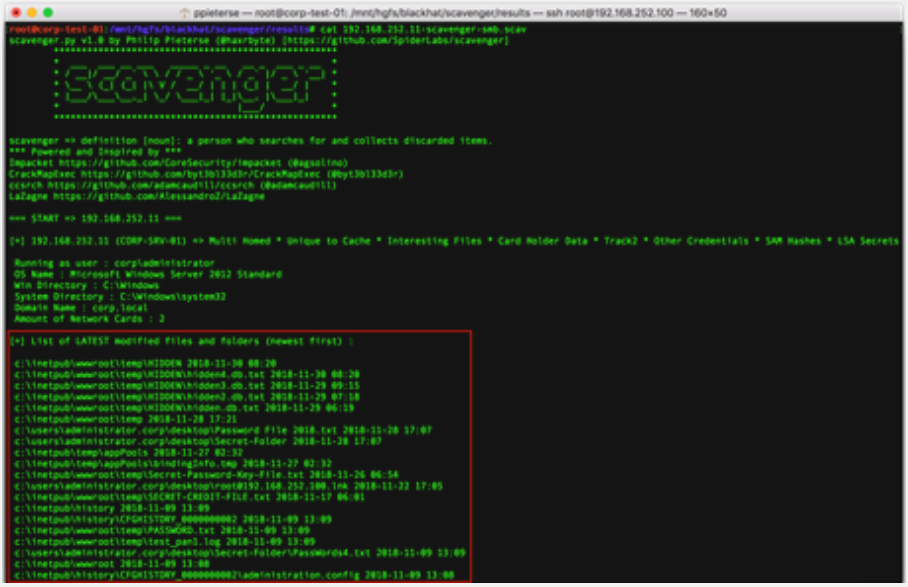
Twitter: @hackplayers

Scavenger es una herramienta creada por **Trustwave** que nos permitirá encontrar rápidamente esos archivos y carpetas "interesantes" una vez que hayamos obtenido credenciales (post-explotación). Es multi-hilo, permite escanear sistemas remotos (*nix, Windows y OSX) a través de los servicios SMB y SSH para analizar cada sistema en busca de información valiosa para luego almacenar en caché el resultado de forma ordenada en una base de datos.

La información confidencial puede tomar muchas formas dependiendo de lo que se busca, pero en el caso de un pentester, generalmente reside en contraseñas y nombres de usuario de otros sistemas o incluso de diferentes dominios de Windows.

Scavenger[1] busca y revisa proactivamente este tipo de información:

- Lista de los "últimos" archivos/carpetas accedidos/modificados/creados.
- Archivos que contengan palabras interesantes, por ejemplo, "password" o "secret". Una vez detectados, Scavenger los descargará a local.
- Archivos que contengan información de cuentas y tarjetas (PCI).
- Hashes de contraseñas del archivo SAM local o de la base de datos de Active Directory (ntds.dit).
- Contraseñas guardadas en algunas aplicaciones, por ejemplo, las contraseñas que se guardan en Chrome, también otras aplicaciones como WinSCP.



Además, Scavenger tiene la capacidad de comparar y contrastar la lista almacenada en caché de archivos, carpetas, previamente obtenidos con una lista recientemente escaneada y adquirida después de un período de tiempo no determinado (horas o días). Por ejemplo, si obtuvimos acceso de nivel de administrador de dominio el día inicial de la prueba de intrusión, el pentester puede esperar varios días y usar Scavenger para volver a escanear y comparar la lista "nueva" anterior de archivos encontrados con la última lista de archivos.

Dando al analista la capacidad de determinar rápidamente qué ha cambiado en ese período de tiempo, por ejemplo, si se han creado nuevos archivos y/o si se ha accedido o modificado los archivos antiguos de alguna manera. Por ejemplo, si vemos que el administrador accede con frecuencia a ciertas contraseñas o archivos, es seguro que lo que hay en esos archivos tiene un valor importante.

REQUISITOS

Instalar CrackMapExec - CrackMapExec Installation Page
Repo `git clone https://github.com/SpiderLabs/scavenger.git`

Ejemplos

```
$ python3 ./scavenger.py smb -t 10.0.0.10 -u administrator -p Password123 -d test.local

$ python3 ./scavenger.py smb --target iplist --username administrator --password Password123
--domain test.local --overwrite
```

[1] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/scavenger-post-exploitation-tool-for-collecting-vital-data/

BITCOIN VS COMPUTACIÓN CUÁNTICA

CRIPTOMONEDAS

Bitcoin nació alrededor del 2009 y ha tenido un auge importante por las bondades que ofrece, podríamos decir el sistema monetario digital más seguro y transparente de la actualidad. El precio de bitcoin se ha disparado hasta los 20 mil dólares en su máximo histórico, por obvias razones es una moneda que ha causado controversia en países como USA. Hace algunos años el caso de Silk Road fue muy sonado por haber utilizado bitcoin como forma de pago para las transacciones que se hacían de ventas ilícitas de drogas en internet.

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

Prometheo

Arquitecto de Seguridad de Aplicaciones y Desarrollador de Software Sr.
Auditor de seguridad en aplicaciones nube y escritorio, con conocimientos en las tecnologías de Blockchain públicas y privadas, desarrollador de contratos inteligentes en la red Hyperledger Fabric, Certificado con EC-Council como Ingeniero en Seguridad de aplicaciones.

Contacto:
www.prometheodevs.com

Bitcoin era ideal para este tipo de compra-venta por no depender de un banco central, además es una moneda que ofrece anonimato debido a que los usuarios no necesitan proporcionar información personal para utilizarla. Dicho lo anterior, es difícil para los gobiernos rastrear y cobrar impuestos sobre bitcoin.

Todas sus propiedades ponen a la criptomoneda en el ojo del huracán, pero... ¿Cómo Bitcoin logró todo esto?

¿A QUIÉN SE LE OCURRIÓ ESTA IDEA TAN INNOVADORA?

En el 2009 Satoshi Nakamoto quien aún permanece con entidad desconocida publicó el White Paper de bitcoin, en este documento Satoshi Nakamoto describe un conjunto de tecnologías y nuevo paradigma que denomina cadena de bloques o Blockchain. La tecnología de blockchain es lo que hace que bitcoin exista, podemos decir que bitcoin es el primer caso de uso de una blockchain. A la fecha de la publicación de este artículo un bitcoin cuesta 6,500 dólares aprox, esto nos indica que la tecnología aún se mantiene robusta y fuerte a pesar de los problemas que enfrentamos en la sociedad y en los mercados financieros.

En esta ocasión hablaremos de uno de los pilares más importantes de bitcoin, la **criptografía**. En una blockchain normalmente se utiliza la criptografía de llaves públicas y privadas. Con este tipo de criptografía los usuarios son capaces de realizar las transacciones de una manera muy segura. Para que alguien haga uso de bitcoin es necesario poseer una llave pública y privada, a esto se le denomina cartera o wallet en inglés. Con la llave privada se pueden realizar transacciones de envío de bitcoin donde el usuario debe firmar la transacción con su llave privada para que se realice el envío, la misma red valida que la llave privada sea correcta y tenga los fondos suficientes. Por otro lado, la llave publica se utiliza para recibir bitcoin, es como una dirección de correo y si el usuario desea que le depositen comparte su llave pública que es como la dirección de correo dentro de la red.

En términos básicos las llaves están criptográficamente ligadas y se componen de números aleatorios muy largos. La longitud y la aleatoriedad hacen que con la computación actual sea casi imposible obtener las mismas llaves, esto las hace resistente a los ataques de fuerza bruta y evitar adivinar las llaves de algún usuario fácilmente.
En la red de bitcoin se generan llaves privadas de 32 bytes y se utiliza el algoritmo ECDSA o Curvas Elípticas, para las computadoras actuales tomaría miles de años en romper una llave de bitcoin. Pero si el romper una llave se trata de más poder de cómputo ¿qué pasa con la computación cuántica? ¿Es realmente una amenaza para los sistemas criptográficos como bitcoin y el internet?

COMPUTACIÓN CUÁNTICA

Un término que cada vez se vuelve más popular, si ya es complejo entender la computación tradicional imaginen ahora tener que entender la física y mecánica cuántica para comprender la computación cuántica. No es algo muy sencillo, pero partamos de lo más básico.

En una computadora convencional todo se basa en un fenómeno de circuitos eléctricos que se encuentran en un solo estado, encendido o apagado. La información se maneja en términos de bit la cual se basa en voltaje o carga de 0 y 1 en donde los circuitos son gobernados por la física clásica. El procesamiento se realiza en CPU o Unidad de Procesamiento Central el cual consiste en una unidad de aritmética y lógica. Una computadora cuántica por lo contrario se basa en la mecánica cuántica, donde existe un principio de la superposición el fenómeno donde es posible estar en más de un estado a la misma vez.

La información y el almacenamiento se basa en quantum bit o qubit que quiere decir 0 o 1 o 0 y 1 a la misma vez, estos se basan en la polarización de un fotón. Por esta razón, el circuito está gobernado por la física o mecánica cuántica. Finalmente, en la computación cuántica el procesamiento se realiza a través de Unidades de Procesamiento Cuánticos, los cuales consisten en qubits interconectados.

Ahora bien, después de entender un poco sobre cómo funciona la computación cuántica la pregunta es ¿Qué puede hacer exactamente la computación cuántica? Para darnos una idea, pongamos un ejemplo: en la computación convencional si existen 4 bytes, la combinación para representar estos 4 bytes se puede representar como 2^4 = 16 combinaciones de un valor en un instante. En un concepto de computación cuántica la combinación de 4 qubits hace posible tener las 16 combinaciones a la misma vez. Esto le permite a la computación cuántica realizar operaciones o cálculos matemáticos en minutos que tomarían a las computadoras convencionales hasta miles de años en realizar. Respondiendo a la pregunta anterior, las computadoras cuánticas son excelentes en resolver problemas de optimización y ciertamente también pueden fácilmente romper algoritmos de cifrado, pero no necesariamente todos los algoritmos.

Actualmente el Instituto Nacional de Estándares y Tecnología (NIST) está llevando una convocatoria sobre la criptografía post-cuántica, en donde miles de participantes principalmente matemáticos y criptógrafos envían sus propuestas para ser evaluadas y puedan ser tomadas como un estándar global que mitigue las amenazas de la computación cuántica a los sistemas criptográficos. Recordemos que las computadoras cuánticas pueden hacer ciertas operaciones de manera muy eficiente pero no necesariamente cualquier operación, los participantes se enfocan en diseñar algoritmos post-cuánticos para que a una computadora cuántica le resulte casi imposible romper el algoritmo.

No se sabe con certeza cuando se estarán implementando estos algoritmos, la fecha de selección está programada para el año 2024. Lo que es cierto, es que ya estamos preparándonos para esta transición. En las computadoras convencionales la ley de Moore expone que el poder de procesamiento tiende a duplicarse cada dos años creando lo que conocemos como el crecimiento exponencial. En la computación cuántica esto cambia, por el hecho de no regirse bajo las mimas leyes convencionales. Aquí es donde nace la ley de Neven, en la cual se estipula que el procesamiento cuántico crece al doble exponencialmente a diferencia del procesamiento convencional.

En los siguientes años tenemos que hacer modificaciones en nuestros sistemas que usan criptografía convencional, recientemente han salido varios proyectos que buscan mitigar la computación cuántica. Quantum Resistant Ledger (QRL) es un proyecto de Blockchain que ya está enfocado en implementar mecanismos resistentes a la computación cuántica desde su implementación. Así como estos, habrá muchos otros que se implementaran a lo largo del tiempo.

Bitcoin es un sistema al final del día, y como la mayoría de los sistemas informáticos, tiene la capacidad de hacer actualizaciones cuando lo requiere. Los sistemas cuánticos no representan una amenaza a corto plazo para la criptomoneda. Con los algoritmos actuales se especula que las computadoras cuánticas puedan romper la seguridad en el año 2027 aproximadamente, obviamente esto depende del avance del procesamiento cuántico en los próximos años. Lo que es un hecho, es que la comunidad tiene que agregar una capa de seguridad y preparase para este cambio, bitcoin ha tenido varias actualizaciones en el pasado y no sería la primera vez que tengan que implementar un cambio a la red.

A pesar de muchas críticas fuertes a bitcoin, esta criptomoneda ha demostrado tener un valor intrínseco por su robustez y las propiedades mencionadas anteriormente en este artículo. Queda claro que es un sistema bien diseñado y que hasta ahora no se ha demostrado lo contrario. Podemos comparar bitcoin con el internet, mientras exista la electricidad y las comunicaciones de red bitcoin seguirá dando mucho de qué hablar.

EN CONCLUSIÓN

Si poseemos bitcoin podemos estar confiados en que estamos del lado seguro, que hasta el día de hoy la computación cuántica no será un problema, seguramente en el futuro se implementará una solución cuando la necesidad de hacerlo llegue.

SOBREVIVIENDO CON BITCOIN

CRIPTOMONEDAS

La aventura que se convirtió en una Odisea.

Todo comienza cuando le comunican a Isaac Rodríguez vía correo qué fue seleccionado por parte del Gobierno de Jalisco, China campus Network y la Universidad de Gongshang en la provincia de Zhejiang para estudiar la **Maestría de Big Data E-Commerce**, una oportunidad única que detonaría una serie de eventos inesperados.

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

Entusiasta Ing. Industrial, apasionado por la tecnología, fundador de la comunidad Mr.Coin,
Bussines development de WaltonChain, Co-Founder de la Startup Prometheo, apasionado por las criptomonedas y Blockchain.

Contacto:
www.prometheodevs.com

Las siguientes semanas transcurrieron de forma natural en México, preparando documentos, cazando el mejor vuelo ($), organizando los últimos eventos de Bitcoin y cursos prácticos de blockchain... quién iba a pensar que estos conocimientos facilitarían su estadía en China al ser la mejor opción para poder adquirir bienes y servicios.

Después de 36 horas de traslado, que si de por si fue cansado el primer obstáculo en Beijin fue su equipaje roto por "*el excelente servició que caracteriza a las aerolíneas*", nunca se imaginó que al ir a reclamar a la aerolínea le propusieran el reembolso del valor del equipaje o entregarle uno nuevo. Eligiendo ambas opciones ya que en Beijin recibió el dinero y en Hangzhou al reclamar nuevamente a la aerolínea en esa ocasión tomaría la maleta. (La importancia de una buena gestión de bases de datos en las empresas).

A transcurrir los días de haber llegado al país asiático se dirigió al banco con sus compañeros de maestría, para realizar los trámites del banco, igual que en cualquier país el proceso es tardado y fastidioso, pero es lo que hay.

Para poder tener tarjeta de débito del banco chino es necesario contar con la documentación que valide como estudiante o empresario, la cual se vinculará con el mayor número de aplicaciones para comprar en línea y hacer pagos. Es sumamente importante ya que, si no se tiene esto, posiblemente la versatilidad en adquirir bienes y servicios no sea tan placentera.

OPERACIÓN QUE LA MAYORÍA DE LOS ESTUDIANTES REALIZAN PARA DISPONER DE SU DINERO EN CHINA

En este caso en específico y con esto se podrán dar una idea general sobre los demás. Lo primero es fondear la cuenta de banco del país de origen y usando dicha tarjeta se puede retirar desde un cajero automático chino el dinero, este movimiento cobra una comisión por parte del cajero y solo se permite retirar 2000 yuanes por operación.
Una vez teniendo el efectivo se utiliza el mismo cajero automático para ingresar el dinero y cargar la tarjeta de débito que previamente se vinculó con las apps ***como wechat y alipay***, por este movimiento no hay cobro de comisión.

¿QUÉ HACER SI EL CAJERO NO DEVOLVIÓ LA TARJETA?

La tarjeta que "se comió" el cajero, automáticamente se cancela y si queremos recibir una tarjeta nueva es necesario pedirla al banco el cual desafortunadamente pide un código de confirmación que solo llega al número telefónico del país de origen, que desafortunadamente no tiene señal en china.

Después de varios días de búsqueda en línea solicitan que se comunique con el banco vía teléfono. ¡Claro! En este caso solo son 14 horas de diferencia, y ahí comienza el estrés… fueron largas horas donde no se pudo solucionar mucho por no decir que nada.

Como sabrán los bancos son especialistas en solucionar los problemas de sus usuarios inmediatamente (léase con sarcasmo).

> *Así de rápido así de sencillo me di cuenta de lo absurdo de la situación y les pregunto, ¿Qué hubieran hecho ustedes? Todo mi dinero estaba en la cuenta del banco que afortunadamente pude seguir moviendo con la app del banco en mi celular, pero de que me sirve tenerla en mi banco si no puedo usarlo…*

¿Y SI UTILIZAMOS BITCOIN?

Pues bueno como saben o quizás no, Bitcoin es ilegal en China, pero es preferible arriesgarse a morir de hambre. Parecía una idea descabellada ya que al preguntar a las personas sobre si aceptaban Bitcoin solo unas pocas sabían que era, pero no aceptaban pagos con ella por lo que volvemos a la misma problemática. Por fortuna todos aceptan ***Alipay y Wechat pay*** entonces lo más obvió sería conseguir alguna persona en el internet que esté interesado en intercambiar el créditos o dinero de estas aplicaciones por Bitcoin.

> *En México ya había tenido la experiencia de cambiar tarjetas de iTunes por Bitcoin usando Paxful, plataforma que conecta compradores y vendedores P2P.*

Al explorar las opciones había un par de usuarios que aceptarían los Bitcoin como intercambio y cargar la cuenta de ***Alipay***.

*Primera compra con **alipay** cargado con Bitcoin.*

El proceso es sencillo, se manda el Bitcoin a la cartera de **Paxful** para después comunicarse con el usuario que continua la conversación por el chat de alipay validando que todo vaya en orden al realizar el intercambio, una vez ejecutada la plataforma libera los fondos y ambos se califican para futuros tratos.

La plataforma y el usuario se quedan con una comisión por la venta. (Excelente opción si se busca generar una utilidad desde el celular).

Después de un tiempo y hacer cálculos sobre las comisiones se descubrió **coincola**, plataforma que tiene XRP para hacer intercambio, esto fue una ventaja ya que las comisiones de envió del **wallet** o **exchange** tenían que absorberse en Bitcoin.

> *De igual manera que en la primera plataforma todo funcionó de manera fluida y ambas tienen su app por lo que no presenta problemas, con esto mi supervivencia en Asia estuvo cubierta sin la necesidad de pedir apoyo a mi banco.*

Hasta aquí todo bien, pero... ahora que hacer con el Bitcoin, si no interesa hacer trading la mejor opción es prestarlo a ***OKEx*** en su producto de ***Piggybank***. La mejor decisión ya que solo era cambiado de Bitcoin a otras **cryptos** o **stablecoins**, esta plataforma proporciona rendimientos todos los días al dejar los activos en la plataforma.

> *Cabe hacer mención que tener tu dinero en una casa de cambio no es la mejor idea del mundo ya que puede desaparecer con tu dinero y no sabrás nada del nunca más, como ocurrió con Mt.Gox.*

TRAVESÍA EN EL INICIO DE LA PANDEMIA

Cuando las cosas comenzaron a complicarse y los países cerraban sus fronteras, los vuelos cada día eran más difíciles de conseguir, sabía que debía salir pronto del país; cosa complicada cuando la mayoría de las agencias solo aceptan pagos con tarjetas de crédito, afortunadamente ya existen algunas agencias que aceptan pagos con Bitcoin, un proceso sencillo y nada complicado.

El paso por España, donde las cosas seguían tranquilas, aunque la mayoría no les agradaba ver a los asiáticos o personas que tenían cubre bocas llegar a su país, el personal del aeropuerto nunca se preocupó por tener las medidas de seguridad que hoy vemos por todos lados como algo básico.

Al viajar por el mundo, en ocasiones no se prevé que al comprar necesidades básicas debe ser en la moneda nacional o en dólares y si solo se cuenta con yuanes (en este caso), entonces al convertir la moneda se vuele al mismo problema de las comisiones, pero por la situación, ya no era tan relevante; la idea era poder pagar alimento, bebida y alojamiento.

Lo primero es buscar un lugar cerca del aeropuerto para descansar y cajeros de Bitcoin que fue posible localizar gracias a la página de cryptoatm.
Una vez que cambiado el Bitcoin a euros, lo siguiente es comprar boletos de transporte para desplazarse por la ciudad y comprar lo necesario.

EN CONCLUSIÓN:

Bitcoin, aunque no es la moneda de uso global sin duda ayuda mucho más que cualquier banco internacional. No es la reserva de valor o póliza de garantía ante la crisis financiera lo que lo hace llamativo; es volverlo líquido.
Y eso justamente es lo que debemos ver como valioso en este activo digital, el poder disponer del valor en cualquier momento, en cualquier parte del mundo para intercambiarlo por bienes o servicios sin problemas de horarios o consentimiento de alguien más.

Tips:

1. Tener más de una cuenta de banco para retirar dinero en el extranjero.
2. Tener todas sus tarjetas con su nombre grabado por si se la traga el cajero. (Algo que pasa más seguido de lo que uno desearía.)
3. Dos dispositivos celulares para tener varios chips.
4. Olvidar todo lo que sabemos y adaptarnos rápidamente.

"Be Water My Friend"
-Bruce Lee

CRIPTOMONEDAS - COMO REFUGIO DE CRISIS

Durante el 2020 algo nos hemos percatado de los problemas que ha tenido la sociedad en general, en cuestiones de salud y económicas. Por ejemplo, nos hemos cuenta de que el peso mexicano (MXN) se ha estado devaluando desde que inició la contingencia.

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

Ingeniero en tecnologías de la información, en el área de seguridad informática y seguridad de la información desde hace 5 años.
Curioso de las nuevas tecnologías emergentes y la economía digital.
Co-Fundador de la Startup Prometheo, dedicada a desarrollo de aplicaciones con tecnologías emergentes.

Contacto:
www.prometheodevs.com

Estamos viviendo momentos cruciales que hacen notar que nuestra mejor aliada en este momento es una computadora, pero con toda la información que se está generando (y vídeos nefastos de tiktok) la información importante está siendo sepultada por millones y millones de personas que hablan sin tener nada que decir. Las personas están haciendo su mayor esfuerzo para seguir operando por medio de Internet luchando por gastar menos dinero, eso es normal, ya que el problema está causando una crisis económica.

Entonces si me pongo a pensar que en este momento mis ahorros, los había estado almacenado en la criptomoneda BTC para protegerme contra la inflación, entonces durante 2019, procure hacer algunos ahorros en criptomonedas específicamente BTC y LTC, me percate que cuando se declaró estado de emergencia por la pandemia fue la rapidez con la que el peso se devaluó con respecto al dólar, esto estaba causando que mis ahorros incrementaran un poco (ya que las criptomonedas pueden ser cotizadas en dólares) digamos que cuando el peso mexicano (MXN) costo alrededor de $25.50 por dólar, mi cartera donde almaceno mis BTC tuvo un rendimiento positivo, a pesar de que el precio de las criptomonedas estaba estático, esto indicaba que a pesar de que mi moneda local se estuviera devaluando, tenían una alta probabilidad de que las monedas digitales, estaban generándome rendimientos, ya que se cotizan contra el dólar u otro tipo de divisas, en estos momentos estaba teniendo una especie de refugio ante la devaluación de mi propia moneda.

Algo realmente interesante, por lo que estamos viviendo en perspectiva el **Bitcoin** resulta una reserva o almacén de valor en esta contingencia.

El dólar está subiendo de precio, los productos están experimentado subidas irracionales de precio a escondidas, algunas organizaciones están dejando de operar, las líneas de producción están deteniéndose poco a poco y no nos queda más que ver como los productos comienzan a escasear.

En teoría los gobiernos están tratando de apoyar a los locatarios emitiendo moneda y solicitando prestamos, aquí lo irónico es salir a la calle con dinero en mano, pero no hay nada que comprar, ya que muchos negocios se vieron obligados a cerrar.
Esta ayuda no fue gratis, esta ayuda causa devaluación, las cosas que en este momento siguen circulando como la canasta básica, aumenta su precio. También los bancos centrales están emitiendo billones de dólares mágicos, para rescatar las bolsas de valores que se desplomaron desde inicios de febrero, lo que implica que mucha gente está perdiendo mucho dinero, situación que los bancos centrales están aprovechando para comprar las acciones de estos grupos a precios bajos.

Ya que las monedas locales están sufriendo por la gran devaluación, los inversionistas están regresando sus pesos (MXN) para poder resguardarlos en monedas más fuertes como el dólar.

Otros optan más por temas tecnológicos, apostando a las criptomonedas como un refugio de valor, y en efecto, lo está haciendo de manera considerable ya que, con la devaluación del peso, las criptomonedas están encareciendo su costo, esto lo podemos ver claramente en Argentina donde el 1 de febrero del 2019 el costo de tener un B**itcoin** era de:

$128,837 pesos argentinos para el día de la redacción de este post el precio es de $445,666 pesos argentinos

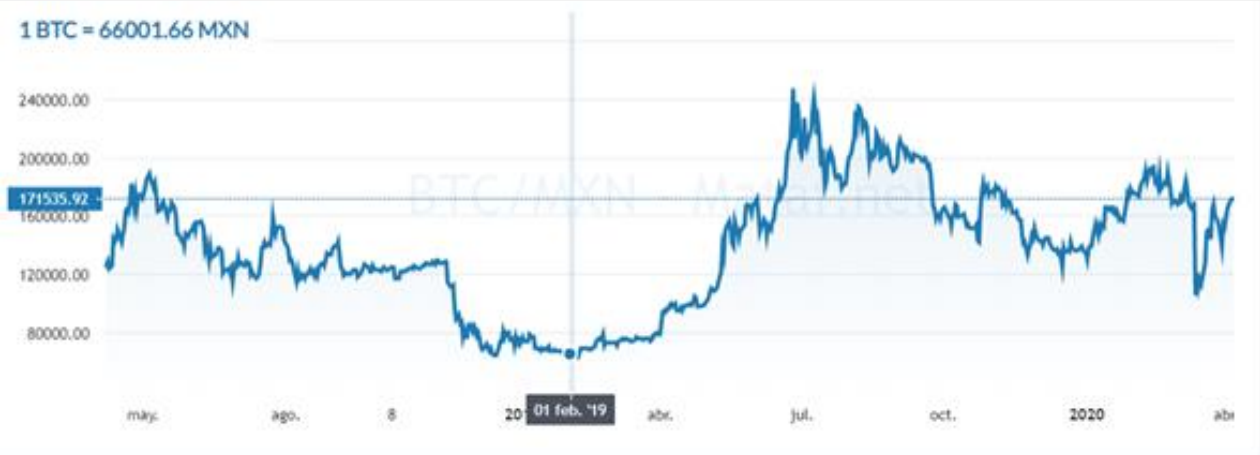
Es decir, quien tenía 1 Bitcoin en su poder en 2019, ahora no está sufriendo por el desplome de su moneda, ya que Bitcoin le permitió mantener su poder adquisitivo.

1 **Bitcoin** 1 de **febrero** del 2019: **$128,378 ARS**

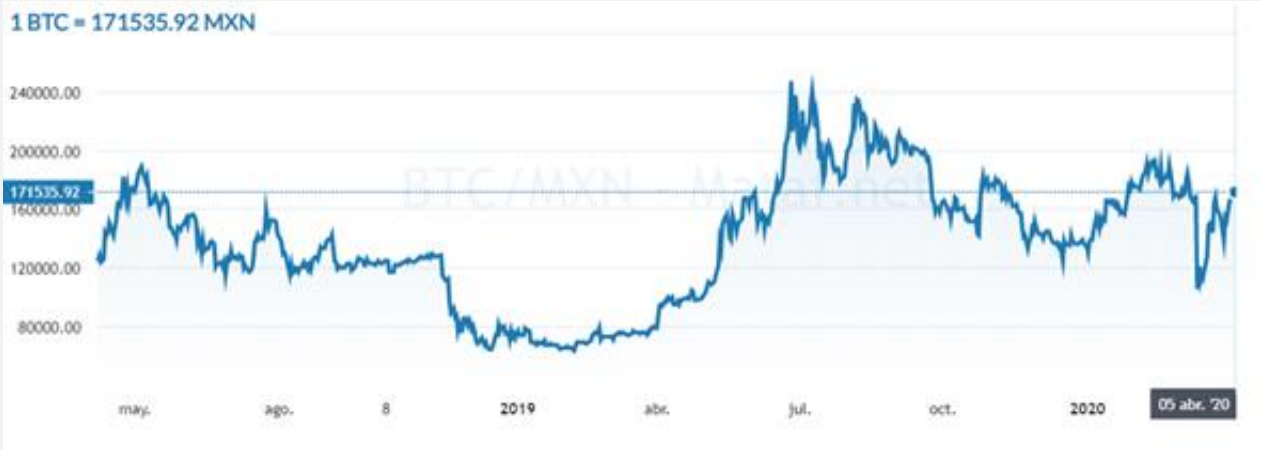
1 **Bitcoin** 5 de **abril** del 2020: **$445,666 ARS**

Con respecto al peso mexicano sucedió algo muy similar, en las mismas fechas, el costo de un **Bitcoin** era de apenas **$66,001** pesos mexicano... pero si observamos hoy, su costo es de **$171,535** pesos.

1 **Bitcoin** 1 de **febrero** del 2019: **$66,001 MXN**



1 **Bitcoin** 5 de **abril** del 2020: **$171,535 MXN**



Con esta información podemos considerar que es muy importante validar los números, ya que en los números están las claves.

Sin embargo, existen otros refugios de valor como los **metales**, ya que su precio Spot (venta de mercados) se está desacoplando de su venta física, ya que el Oro en precio spot es basura, ¿cómo así? si, es la misma práctica que hacen los dueños del dinero, compran una onza de 400 USD de oro, y emiten millones de papeles diciendo que contiene 1 gramo de oro ese papel, lo cual es falso.

Y a esto se le conoce como una gran estafa, ya que el dinero que se mueve en los mercados financieros como los Spot y los Margin trading, están haciendo comercio con papel que no tienen ningún valor, esto les permite seguir emitiendo papel, y gente que lo siga comprando, hasta que se dan cuenta, de que el precio para el metal físico oscila entre 1720–1813 USD cuando el precio spot esta por los 1612 USD.

Y lo podemos consultar en las siguientes gráficas

Precio Spot mercado basura: **$1618 USD — Oz**

Precio del Oro físico: 1798–1808 **USD — Oz**

La pregunta del millón, entonces es...

¿EL BITCOIN FUNCIONA COMO VALOR REFUGIO ANTE LA CRISIS QUE ESTAMOS VIVIENDO?

Las gráficas los dicen todo.

HACKEANDO

REDES WIFI EN 2 MINUTOS

HACKING

En una juntada de todos los miembros de Underc0de de Mendoza-Argentina, entre pizzas y cervezas, uno de los miembros notó que el lugar en donde estábamos, tenía una red Wireless de **DirecTV** y apostó una jarra de cerveza que podía hackearla en menos de 2 minutos... Algunos miraron sorprendidos, y uno de los chicos aceptó la apuesta.

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.

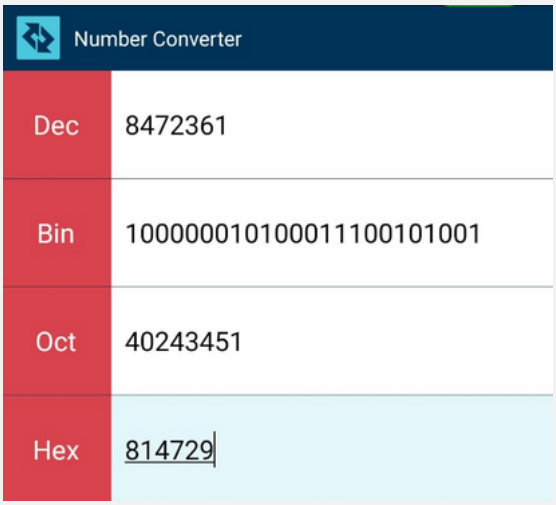
Contacto:
underc0de.org/foro/profile/ANTRAX

Cabe aclarar que **solo sirve para routers de DirecTV** que tienen la password que viene por default.

Para sorpresa de todos, logró hacerlo y en este artículo veremos como lo hizo.

La red en cuestión se llama **DTV_08472361**

Los pasos son muy simples, consiste en tomar el número que aparece en la red **«08472361»** y debemos convertirlo de DECIMAL a HEXADECIMAL

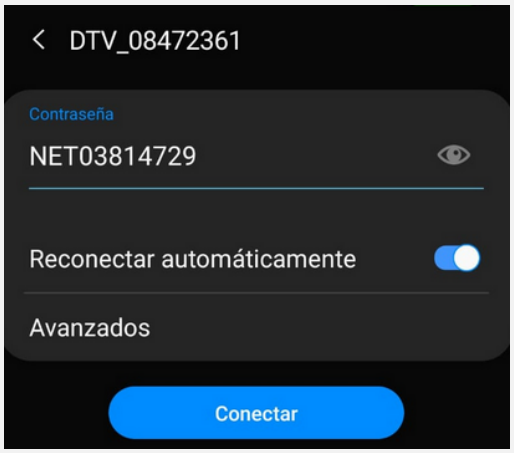


Como resultado obtuvimos «**814729**«. Lo que debemos hacer ahora, es usar ese número para armar la contraseña.

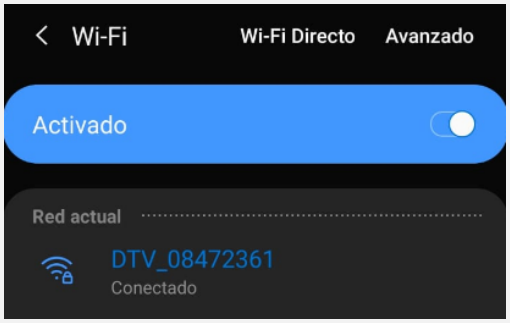
Las contraseñas de los routers de DirecTV tienen el siguiente formato:

NET03**814729**

Es decir: la palabra NET (en mayúsculas) + 03 + número hexadecimal que generamos



Colocamos la password, damos a conectar y...



INTERNET GRATIS!!!!


<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

U2F: BLINDAJE PARA LA SEGURIDAD DE LA INFORMACIÓN

PRIVACIDAD

¿A cuántos no nos preocupa la seguridad de la información que introducimos en algún Website o dispositivo conectado a internet (i.e., posnets, laptops, etc.)? ¿Cuántos de nosotros no estamos aprensivos al introducir datos personales y/o sensibles durante el proceso de completado de algún proceso en internet, como el login? ¿Cuán seguros estamos de que nuestros datos están realmente protegidos o fuera del alcance los hackers de la internet?

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

Ingeniero de Sistemas, enfocado en las áreas de IT, Seguridad y Ciencias de la comunicación. Interesado en el desarrollo y supervisión de la seguridad digital, enfocado en el diseño e implementación de metodologías y estándares estructurados sobre proyectos de seguridad en plataformas IT, actualmente desarrollándose como Security Risk & Compliance Manager - LATAM.

Fiel defensor de espacios tecnológicos contextualizados en la seguridad de la información que cubran las necesidades de los usuarios y fomenten/difundan nuevos hallazgos en este campo.

Contacto:
www.security-sense.com

Pues bien, las nuevas tecnologías, como la **U2F**, vienen a darnos más tranquilidad ante estas inquietudes al ofrecernos un dispositivo que ***nos ayuda a blindar nuestros procesos de autenticación y accesibilidad de usuario***: **YubiKey**.

U2F: blindaje para la seguridad de la información

En un mundo tan competitivo, complejo y cada vez más dependiente de la tecnología, el asunto de la seguridad de la información se vuelve más y más preponderante. Hacerse de herramientas actualizadas que "pongan en jaque" la susceptibilidad y vulneración de elementos que necesiten mantenerse privados es una actividad laboriosa, además de ser también una tarea de todos los días.

Mucho se ha invertido a nivel tecnológico, monetario e intelectual para lograr conseguir las maneras de mantener privada la información sensible ante riesgos de ser hackeada. Las áreas relacionadas con el tema y sus desarrolladores, se mantienen en constante actualización para combatir a los que desean apoderarse de la privacidad de otros, o de los que busquen cometer fraude a través del "phishing".

Es así entonces cuando recientemente se ha desarrollado una tecnología que se denomina Universal 2nd Factor, o U2F según sus siglas en inglés. Por algún tiempo, el requerimiento de seguridad 2FA (2-Factor Authentication) ha sido una buena manera de mantener a los usuarios seguros de que la accesibilidad de sus plataformas, aplicaciones y/o códigos de acceso se mantengan privados, y aun así los hackers siguen actualizando sus maneras al mismo paso para lograr sus objetivos.

Como se sabe, uno de los mecanismos de acceso basados en 2FA, consiste en acceder a una aplicación o alguna cuenta digital de un sitio web introduciendo usuario y contraseña. Al momento de acceder, el sistema genera un código que es recibido en un email o número telefónico que el usuario haya suministrado para tal fin, entonces con la información regular más el nuevo código generado instantáneamente, se puede acceder a la cuenta.

Precisamente, esta tecnología U2F supera las expectativas del 2FA, al sacar del tráfico evidente y hackeable; elementos como números telefónicos y direcciones de correos electrónicos que puedan poner en riesgo la seguridad de la información del usuario en cualquiera de sus dispositivos. Es tan sencillo como que el "segundo factor" o "código", que es generado y enviado al usuario pasa a ser sustituido por esta "llave de seguridad".

EL FUNCIONAMIENTO ES EL SIGUIENTE:

- El usuario aplica esta llave
- El sistema la reconoce
- Le da acceso al usuario

LU2 VERDE DE LOS GRANDES DE LA INFORMACIÓN PARA EL U2F

La vanguardia en U2F ha sido ampliamente desarrollada por YUBICO, en trabajo conjunto con Microsoft y Google, crearon este artefacto que denominan "YubiKey", que en ingles tiene una analogía con "your ubiqitous key", como presencia natural de la tecnología en cualquier lugar, y por otro lado también funciona con una referencia en japonés, en donde "yubi" significa dedo, con ello al tener la llave en sus dedos, el usuario puede hacerle notar a la máquina de su presencia humana.

Compañías como Dropbox, Amazon, Facebook, Apple, Samsung, entre otras, se unen también a esta tecnología, además de dar su aval en lo positivo que esto significa para los miles de usuarios de estas plataformas, también garantizan que las conexiones que se establezcan con estos portales y servicios se den de manera segura y bajo estándares más estructurados.

Del YubiKey / U2F se han desarrollado varias modalidades, que incluyen desde el USB nano, pasando por USB-A, USB-C, hasta los "hard-tokens" con disponibilidad NFC para los aparatos que puedan soportar y sean compatibles con esta tecnología.
Ante las ventajas que han derivado de esta llave de seguridad, Google tomó el paso al frente en relación a su uso y esparcimiento en el mercado. Los trabajadores del coloso de la internet fueron animados a usar activamente el YubiKey para acceder a sus cuentas.

Según Brian Krebs, quien fuera el primer periodista en el área de seguridad que informara acerca del éxito de Google contra los intentos de phishing, la compañía empezó a pedirle a sus numerosos empleados que usaran estas llaves de seguridad físicas a principios del año 2017. Que haya sido un éxito para Google es un gran paso ante la aceptación de esta pequeña llave cuyo costo ronda los 20USD. Desde entonces, para Google no ha habido ningún reporte de fraude o hackeo de cuentas para sus empleados con el uso del YubiKey.

"Google no ha reportado a ninguno de sus más de 85.000 empleados con algún caso exitoso de 'phishing' en sus cuentas laborales desde principios de 2017, cuando comenzó a requerir que todos los empleados usaran la Lleve de Seguridad física en lugar de claves de acceso o 'contraseñas de un solo uso'", según la compañía al portal KrebsOnSecurity.
De hecho, la publicación de Google '*Security Keys: Practical Cryptographic Second Factors for the Modern Web*' (Lang, Czeskis, Balfanz, Schilder y Srinivas, 2016), afirma que el acceso basado en 2FA, con las llamadas "One-time password", genera un fallo aproximadamente en el 3% de los casos, cuando por otro lado, el U2F obtuvo 0% de fallos en cualquiera de sus intentos.

SEGURIDAD DIGITAL:
SINCRONÍA ENTRE EL USUARIO Y LA HERRAMIENTA TECNOLÓGICA

Ahora bien, aunque no necesariamente sean detractores, muchos son los que le ven puntos débiles al requerimiento de seguridad U2F. Por un lado, mucho se dice sobre la necesidad de tener un dispositivo de "**backup**" ante la eventualidad de perder el de uso principal. También se genera discusión acerca de la necesidad de conectar/desconectar la llave al momento de cambiar de equipo y lo tedioso que eso se pueda tornar.

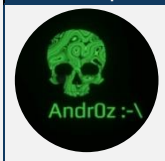
Finalmente, y como punto débil que el avance natural de la tecnología muy probablemente minimice, tenemos la compatibilidad plena con todas las plataformas o aplicaciones en las que sea necesario.
Desde luego, y ante esta u otra novedad en el mundo de la tecnología, siempre habrá defensores y detractores, todo depende del tipo de usuario y el manejo que se le dé a la herramienta tecnológica en cuestión. Lo cierto es que para continuar avanzando protegidos de hackers y las técnicas de phishing, YubiKey es una **buena manera de mantener la accesibilidad y privacidad** tan seguras como puedan estar. Entendiendo que siempre habrá una "siguiente herramienta" disponible en cualquier espacio tecnológico, analicemos ésta a ver los beneficios que, por ahora, nos puede aportar.

ALGORITMOS GENÉTICOS: FUNCIONAMIENTO Y APLICACIONES

PROGRAMACIÓN

Los algoritmos genéticos son meta heurística cuya principal inspiración es el principio de la teoría de la evolución de Darwin, siendo así, una de las ideas más intuitivas dentro del campo de la IA. Este tipo de técnicas reflejan el proceso de selección natural, donde los individuos más aptos son los seleccionados para reproducirse, dando inicio a una nueva generación "mejor adaptada".

Escrito por: @**ANDR0X** | **COLABORADOR** UNDERC0DE



Ingeniero en aeronáutica, amante de las ciencias físico-matemáticas y gran gusto por la programación, arte y tecnología.

Contacto:
underc0de.org/foro/profile/androz

En principio parecería una explotación inteligente de búsqueda aleatoria para resolver problemas en optimización, pero, aunque son aleatorios, ésta técnica explota información histórica para dirigir la búsqueda a la región de mejor desempeño dentro del espacio de búsqueda.

¿CÓMO FUNCIONA UN ALGORITMO GENÉTICO?

Recurriremos a un ejemplo ilustrativo para ver su funcionamiento, supongamos que se necesita recrear el siguiente vector de valores binarios:

Para hacerlo, el algoritmo genético generará propuestas de solución (*individuos*) de forma aleatoria, a las que en conjunto se llamaran "generación 1", estás serán previamente evaluadas para obtener las mejores soluciones de la población y con esta información crear una segunda generación "mejor adaptada" y así sucesivamente hasta cumplir con el objetivo propuesto (*gen N*), esto se vería de la siguiente manera:

Para llevar cabo el procedimiento anteriormente ilustrado se definen 5 pasos principales, estos son:

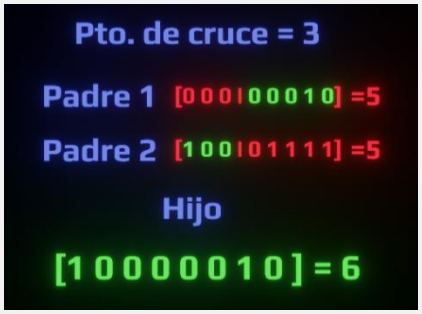
1. **Inicialización:** Se genera una población *aleatoria* inicial con una cantidad de individuos lo suficiente mente grande y diversa para garantizar la obtención de diferentes cantidades de aptitud así tener diferentes individuos de los cuales seleccionar a los mejores.

2. **Evaluación de función de aptitud (Fitness):** De acuerdo al objetivo del problema, se define la "función objetivo ", que servirá para evaluar a todos y cada uno de los individuos de la población y de esta manera que se les asigne un valor numérico que indicará que tan bueno o malo es según el problema a solucionar. Como ejemplo, si se toma a toda la población de la generación número 1 para evaluarse, quedarían de la siguiente manera:

Donde en este caso la aptitud está dada por la similitud de los elementos de cada individuo y el objetivo del problema.

3. **Selección:** Para llevar a cabo la selección se tendrá una preferencia por los individuos más aptos. Existen varios tipos de selección en AG, algunos de ellos son:
   - **Por ruleta:** una forma de selección proporcional a la aptitud en la que la probabilidad de que un individuo sea seleccionado es proporcional a la diferencia entre su aptitud y la de sus competidores.
   - **Por torneo:** elección de subgrupos de individuos de la población, y los miembros de cada subgrupo compiten entre ellos. Sólo se elige a un individuo de cada subgrupo para la reproducción.
   - **Proporcional:** en esta selección, cuanto más apto es el individuo mayor es su probabilidad para ser seleccionado.
   - **Por rango:** los individuos se ordenan según su aptitud, y por tanto la probabilidad de ser seleccionado va acompañada de la posición en la que se encuentra ordenado.

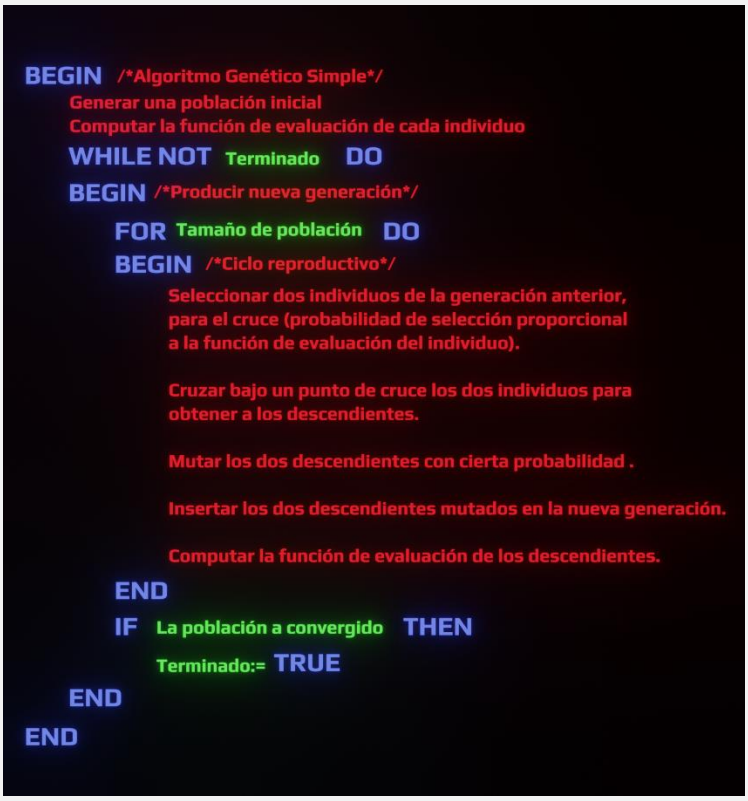
4. **Reproducción y cruzamiento(Crossover):** Seleccionados los mejores individuos de la población se procede a cruzar su información para obtener una nueva generación que en este caso serán los hijos de la generación anterior. Para hacer la operación de cruzamiento se define primero de forma aleatoria un punto de cruce que servirá para saber desde que posición del vector de valores del individuo intercambiará información con el otro individuo. El cruzamiento se vería de la siguiente manera:



5. **Mutación y reemplazo:** Modifica al azar parte de la información de los individuos, y permite alcanzar zonas del espacio de búsqueda que no estaban cubiertas por los individuos de la población actual. Una vez pasados por la mutación, los nuevos individuos remplazan a los anteriores para conformar una nueva generación.

Eso sería todo por parte de la forma en que funciona un algoritmo genético básico. Como se pudo observar, los algoritmos genéticos sirven esencialmente para optimización en general ya que tienden a seleccionar las mejores soluciones generación tras generación.

En conclusión, el algoritmo que describiría a un AG básico quedaría de la siguiente manera:



APLICACIONES:

Debido a que los algoritmos genéticos tienen como función principal optimizar, la aplicación de los mismos es muy grande, a continuación, se enuncian algunas de sus aplicaciones en distintas áreas de las ciencias:

- Hallazgo de errores en programas.
- Aprendizaje de comportamiento de robots.
- Aprendizaje de reglas de lógica difusa.
- Optimización de sistemas de compresión de datos, por ejemplo, usando wavelets.
- Ingeniería de software
- Optimización de producción y distribución de energía eléctrica.
- Diseño de redes geodésicas (problemas de diseño).
- Calibración y detección de daños en estructuras civiles.
- Cálculo de poblaciones estelares en sistemas estelares complejos
- Diseño de sistemas de distribución de aguas.
- Diseño de topologías de circuitos impresos.
- Diseño de topologías de redes computacionales.
- En teoría de juegos, resolución de equilibrio

Se puede seguir con infinidad de aplicaciones de estos algoritmos en la ciencia. Como ha quedado en evidencia, con los AG hay un mundo inmenso por delante que descubrir.

Para ver un ejemplo básico de un algoritmo genético en C#

CRIPTOMONEDAS CON PYTHON - LLAMADAS A APIS

PROGRAMACIÓN

Lo interesante de las criptomonedas y las API es que permiten poner a prueba algoritmos automatizados (algorithmic trading) de manera bastante sencilla, como captar pequeñas variaciones en los precios.

Escrito por: @**GENIOL** | **USER** UNDERC0DE

Desarrollador web, Big Data, Programador Python, Relaciones Publicas de Uncerc0de Mendoza, Argentina. Profesor de kung-fu whushu y de Tai chi chuan. Hobbie: Edición de publicidad para radios FM e instructor de GYM.

Contacto:
underc0de.org/foro/profile/GENIOL

Abordaremos los casos que, para la resolución de problemas, es necesario ejecutar un grupo de instrucciones más de una vez, pero en diferentes partes de los algoritmos. Existen varias formas de solventar esta situación, dependiendo si sólo se necesita ejecutar las instrucciones, si necesitamos que a partir de esa ejecución se obtiene uno o más valores o si se requiere pasar uno/más valores a esas instrucciones para que puedan ser ejecutadas y así obtener los resultados esperados.

En este sentido podemos definir/utilizar Funciones y Procedimientos. Estos mecanismos facilitan la estructuración y reutilización de instrucciones, evitando la duplicación/redundancia en nuestros algoritmos, promoviendo la reutilización de código.
Una vez que se definen las funciones o procedimientos, pueden ser invocados desde cualquier parte del algoritmo a través de su nombre, permitiéndonos crear algoritmos más legibles, por tanto, mejor estructurados. Ahora vamos a explicar con más detalle la definición y uso de funciones.

Una función es un grupo de sentencias que forman una expresión, recibiendo uno o más valores denominados ***argumentos***, para producir un único valor que se denomina resultado. Este concepto se fundamenta en el concepto de función matemática; es decir, una función es una relación que asocia elementos de entrada pertenecientes a un dominio con un solo elemento del condominio representado en su valor de retorno.

Las funciones se usan cuando existen dos o más porciones de algoritmo dentro de un código que son iguales o muy similares, cuya ejecución, retorna un único valor. Esa porción se define como una función, se le asigna un nombre, para luego invocarla mediante ese nombre en cualquier parte del algoritmo y hasta dentro de la misma función u otras funciones. El tipo del valor de retorno de una función puede ser: numérico, una cadena de caracteres y booleano.

En el pseudo-lenguaje una función se declara de la siguiente manera:

```
funcion <nombre>(<listaParámetrosFormales>): <tipoResultado>
   <declaraciones>
inicio
   <instrucciones>
retorna <expresión>
finfuncion
```

Donde:

- **<nombre>**: nombre de la función por el cual será invocada.
- **<listaParámetrosFormales>:** contiene nombre y tipo de las variables que pasan alguna información necesaria para que la función ejecute el conjunto de instrucciones.
- **<tipoResultado>:** indica el tipo de dato que devuelve la función.
- **<declaraciones**>: representa el conjunto de variables definidas para la función (diferentes a los parámetros).
- <**instrucciones>:** representa el conjunto de instrucciones que realiza la función.
- **<expresión>:** representa el valor que retorna la función.

Una vez que se ejecuta la función, se devuelve el control del programa al lugar donde se ha llamado a la función. Dentro del contexto del proyecto que estamos desarrollando. Se requiere tener instalado Python 2.7 o superior y configurado el intérprete.

APIS

Trabajaremos con APIs, que son aplicaciones alojadas en webs, podremos utilizar para obtener datos y realizar acciones. Las páginas que trabajan con ***criptomonedas*** proporcionan su propia API para que podamos automatizar toda clase de acciones. Para empezar, vamos a la documentación de la API de **Coinmarketcap**[2]. Para

[2] coinmarketcap.com/api/

acceder a los datos que nos brinda **coinmarketcap** vamos a realizar llamadas HTTP api.coinmarketcap.com/v2/ticker/ Para manipular esta información accederemos a ellos a través de un lenguaje de programación.

ACCEDIENDO A LAS APIS CON PYTHON

Iniciaremos abriendo un editor de código que interprete **Python**, después colocando simplemente las URL's que hemos visto antes nos va a dar error. Para abrir HTTPs en Python es necesaria la librería **request**. Cuando tengamos instalada el módulo requests, podremos enviar peticiones fácilmente. Ahora sí, vamos a nuestro editor y escribimos:

`import requests` para importar este módulo en nuestro script.

Cabe destacar que siempre usaremos **`import`** al principio de nuestros scripts para cargar módulos en ellos.

Ahora crearemos un **`input`** para indicar *"el nombre de la moneda a obtener el precio:"*, una condición que verifique si el nombre de la **criptomoneda** es válida, si no se imprimirá en pantalla ***"Moneda Invalida"***

Nuestro código quedaría así:

Código: Python

```
1. import requests
2.
3. def esmoneda(cripto):
4.     return cripto in monedas
5.
6. monedas=()
7. monedas_dic={}
8.
9. data = requests.get("/api/v3/ticker/price?symbol=").json()
10.for id in data["data"]:
11.    monedas_dic[data["data"][id]["symbol"]]=data["data"][id]["quotes"]["USD"]["price"]
12.monedas=monedas_dic.keys()
13.moneda=input("Indique el nombre de la moneda a obtener el precio: ")
14.while not esmoneda(moneda):
15.        print("Moneda Invalida.")
16.        moneda=input("Ingrese el nombre de la moneda: ")
17.else:
18.    print("La moneda con symbol:",moneda,
19."Tiene un precio de: ", mondenas_dic.get(moneda,"USD")
```

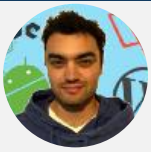
Con estas pocas líneas de código ya estamos accediendo a la API de coinmarketcap, y podemos ver el precio de la moneda en "USD".

ANDROID: GUÍA PARA FUTUROS DESARROLLADORES

PROGRAMACIÓN

En un mundo gobernado por React y la idea de lanzar tu aplicación a múltiples plataformas, ¿por qué aprender Android nativo?
Si se trata de una empresa chica o quizá de un emprendedor, contratar un programador android y otro de Swift es caro. La salida más rápida es usar un framework como React Native que simplifica desarrollar una sola vez y salir a todas las plataformas.

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



Desarrollador Android Nativo con Kotlin y Java. Maratonero de series en Netflix y arduas horas en Steam. Le gusta leer, especialmente fantasía. Disfruta de hacer caminatas y explorar lugares nuevos donde nadie más se atreve a llegar.

Contacto:
https://medium.com/@maxwellnewage

Sin embargo, nos estamos olvidando de una cuestión fundamental: Si bien React es muy distinto al viejo Phonegap o Cordova, no deja de ser un puente hacia lo nativo.
React tiene que generar código para representar lo que estamos escribiendo en Javascript o Typescript. Eso nos quita algo de control sobre cómo queremos desarrollar nuestra aplicación.

Y luego está el problema de la compatibilidad. Android saca una nueva versión cada año. En la mayoría de los casos, implica un cambio en el hardware (como una versión nueva de la cámara que maneje una perspectiva 3D).
Cuando Google saca una nueva versión de su sistema operativo, lanza un SDK (Software Development Kit). Esto es un conjunto de herramientas que nos permite trabajar con las nuevas funcionalidades de ese sistema.

React, conjunto de los demás **frameworks**, tiene que lanzar un soporte específico para cada nuevo SDK. En el caso de los programadores nativos, trabajen directamente con el que nos provee Google.
No malinterpretemos: React es muy bueno, su soporte también. Si el objetivo es trabajar independiente en aplicaciones que no involucren un manejo de hardware muy específico, va a funcionar sin problemas.
Programar Android nativo nos pone al frente de todo lo nuevo que vaya saliendo. Y no nos limitemos a móviles, también tenemos Android TV, Android Wear, Android Auto, entre otros. Otro punto interesante es que nativamente podemos trabajar con Java o Kotlin. En el caso de React, desarrollamos con Javascript o Typescript.

Programar en una tecnología requiere entender los fundamentos.

Herramientas indispensables

Estas son las herramientas de software que vamos a necesitar para iniciar en el desarrollo de Android:

- Intellij: este IDE permite correr aplicaciones en Java. Con la versión Community es suficiente.
- Android Studio: Es fundamental. permite correr aplicaciones en Android. La instalación ya viene con el SDK incluido.
- JDK: (Java Development Kit): Es el kit de desarrollo de Java. Cualquier versión de la 8 o superior sirve.
- Visual Studio Code: puede ser opcional. Se trata de un editor de código creado por Microsoft. El más famoso hasta la fecha. A veces puede ser necesario editar un archivo puntual y no queramos abrir un IDE.
- Windows, Linux o Mac: Android se puede desarrollar en cualquiera de estos sistemas operativos. Aunque la instalación en Linux puede ser un poco más compleja.
- Disco SSD: Un disco sólido, indispensable. Android Studio accede al disco constantemente, por lo que tener una velocidad buena te va a beneficiar en muchos aspectos, especialmente en la compilación.
- 8GB de RAM: Es lo recomendable. Lo mínimo sería cuatro.
- Café, Mate o Té: Cualquier cosa que nos mantenga despierto por muchas horas. Probablemente el requisito más importante.

Aprender Java

Muchos por ahí andan diciendo que el futuro esta con **Kotlin**. El desarrollo en Java puede resultar muy cómodo, si leen por ahí que Java está muriendo, no se preocupen: No es así. Podemos tener la seguridad porque Java es un lenguaje multiplataforma. Hoy día muchos bancos confían su sistema a **Java Spring** (un framework de desarrollo web y APIs).
Minecraft está desarrollado en Java y siguen lanzando actualizaciones, aunque muchos estamos de acuerdo que la optimización es un tema complejo de tratar.
También se han desarrollado muchas aplicaciones para escritorio, aunque en este caso podemos sugerir más, usar Electron, una librería de interfaces visuales usando Javascript.
Es fundamental entender que **Java** corre en una **JVM** (Java Virtual Machine), que viene a ser una máquina virtual con su propio entorno para correr sus aplicaciones. Esto aplica a cualquier tecnología que utilicemos con este lenguaje.
Otra particularidad es que Java soporta el paradigma de programación orientada a objetos, estructurada, funcional y reactiva. Por lo tanto, es un lenguaje *multiparadigma* que se va a adecuar a nuestras necesidades. Los recursos para aprender Java son miles. Si no les atraen los cursos de hispanohablantes, también pueden encontrar alternativas en inglés. Aunque si lo suyo son los libros, les recomendamos los libros de **O'Reilly**. Muchos rechazan la idea de un escrito, dado que el contenido tiende a desactualizarse. Pero en el caso de los fundamentos en Java, eso nunca cambia. Son bases y se van a mantener por mucho tiempo.

Continuamos en la siguiente edición

CYPRESS

REVIEWS

El ámbito del Testing está hablando de Cypress y de sus maravillas; incluso muchos se preguntan si es este el fin de Selenium como rey del testing automatizado. Vamos a aclarar algunas dudas y malentendidos que rodean a Cypress hoy por hoy, para que puedas elegir la mejor herramienta para realizar las pruebas en tu proyecto.

Escrito por: @**ANDDREPAR** | **USER** UNDERC0DE

Aficionada a la informática desde siempre, programadora de oficio, QA de vocación.

Contacto:
underc0de.org/foro/profile/Anddre/
Redes Sociales
linkedin.com/andreaparlanti

Cypress es una herramienta de automatización de pruebas. Está dando que hablar porque es diferente a todo lo anteriormente conocido.

¿Cypress llegó a reemplazar a Selenium?

La respuesta es incierta, no es el fin inmediato de la era Selenium ni de su WebDriver. Mucho menos será el fin de todas las aplicaciones que han sido construidas usando Selenium como base. Por lo menos por ahora, en el corto plazo.

Porque, como bien sabemos, todas estas herramientas comparten los mismos inconvenientes, es por eso que Cypress[3] construye su propia arquitectura desde los cimientos, y soluciona así inconvenientes y errores que existen de forma horizontal en todos los demás frameworks.

¿Es una herramienta de automatización?

Cypress no es una herramienta de automatización, es una herramienta de testeo automatizable. No se pueden correr scripts de cualquier tipo y automatizar cosas, está hecha para automatizar pruebas.

Al estar instalada localmente en cada máquina, Cypress tiene la capacidad de acceder al sistema operativo y automatizar algunas tareas, como tomar capturas de pantalla, grabar videos, realizar operaciones de sistema y operaciones sobre la red, pero todo esto dentro de un caso de prueba.

¿En qué se diferencia con todas las herramientas anteriores?

Además de no usar a Selenium como base, Cypress no es un framework de automatización generalizada, tampoco realiza pruebas unitarias contra los servicios del backend. Para eso existen otras herramientas que funcionan de maravilla.

Está creada por desarrolladores frontend, para desarrolladores frontend. Teniendo en cuenta esto, cabe mencionar que Cypress está diseñada para trabajar solo con Mocha como test runner; no puede usarse contra diferentes navegadores ya que es exclusiva para Chrome; sus pruebas se escriben en JavaScript únicamente. Por otro lado, incluye la posibilidad de realizar mocking, una buena cantidad de reglas de validación muy útiles para cualquier programador de front.

Cypress conoce y entiende todo lo que sucede en la aplicación de forma asíncrona; es imposible que no encuentre objetos al momento de disparar sus eventos; incluso conoce los tiempos de animación de los elementos, esperará pacientemente a que terminen. Adicionalmente, espera de forma automática que los elementos se vuelvan visibles, que estén habilitados, y que dejen de estar cubiertos.

[3] Tayar, G. (n.d.). Introduction to Cypress. testautomationu.applitools.com/cypress-tutorial/
End to End Testing Framework. (n.d.) .www.cypress.io/how-it-works/
Kinsbruner, E. (n.d.). Cypress vs. Selenium: What's the Right Cross-Browser Testing Solution for You?: by Perforce. www.perfecto.io/blog/cypress-vs-selenium-whats-right-cross-browser-testing-solution-you

¿Cuáles son sus diferencias principales con Selenium?

Por lo que ya hemos visto, son varias las diferencias que existen entre ambas. A continuación, veremos un cuadro comparativo del sitio perfecto.io, donde se pueden ver con claridad las más importantes.

Framework	Lenguajes de desarrollo soportados	Navegadores soportados	Frameworks de pruebas soportados	Configuración para uso	Integraciones	Rango de opciones de Testing	Madurez Documentación Soporte
Selenium WebDriver	Java, C#, Java Script, Python, Ruby, Objective-C	Chrome, Safari, Firefox, Edge, IE	Mocha JS, Jest, otros supersets sobre Selenium (Protractor, WebDriverIO, etc.	Descargar el driver correspondiente, configurar una red, la red y la ubicación impactan en la velocidad de la ejecución.	Múltiples integraciones (CI, CD, reportes,pruebas visuales, cloud vendors)	Extremo a extremo, seguridad, unitario.	Comunidad robusta, variedad de conexiones, mejores prácticas.
Cypress.io	JavaScript	Chrome, Electron	Mocha JS	Comes with bundled Chrome browser, no complex environment setup.	Integraciones limitadas	Extremo a extremo	Buena documentación y ejemplos de código, comunidad en crecimiento.

¿Es más rápida que Selenium?

Sí, es mucho más rápida que Selenium, esto se debe a que su estructura es muy diferente a la de Selenium. Mientras que la mayoría de las herramientas que existen -incluyendo Selenium- operan corriendo por fuera del navegador, ejecutando comandos remotos a través de la red, Cypress corre a la misma altura que el código de la aplicación, en el mismo run-loop.

¿Es mejor que Selenium?

No es mejor, es distinta. Al tener acceso tanto al front como al back, las respuestas a los eventos de la aplicación son en tiempo real; mientras al mismo tiempo se atienden tareas más prioritarias por fuera del navegador.

Además, al operar en el mismo run-loop que la aplicación, tiene acceso nativo a todos los objetos; llámese la ventana, el documento, algún elemento DOM, la instancia de la aplicación, una función, un timer, un service worker, o cualquier otro objeto. Con Cypress desaparece por completo la serialización de objetos.

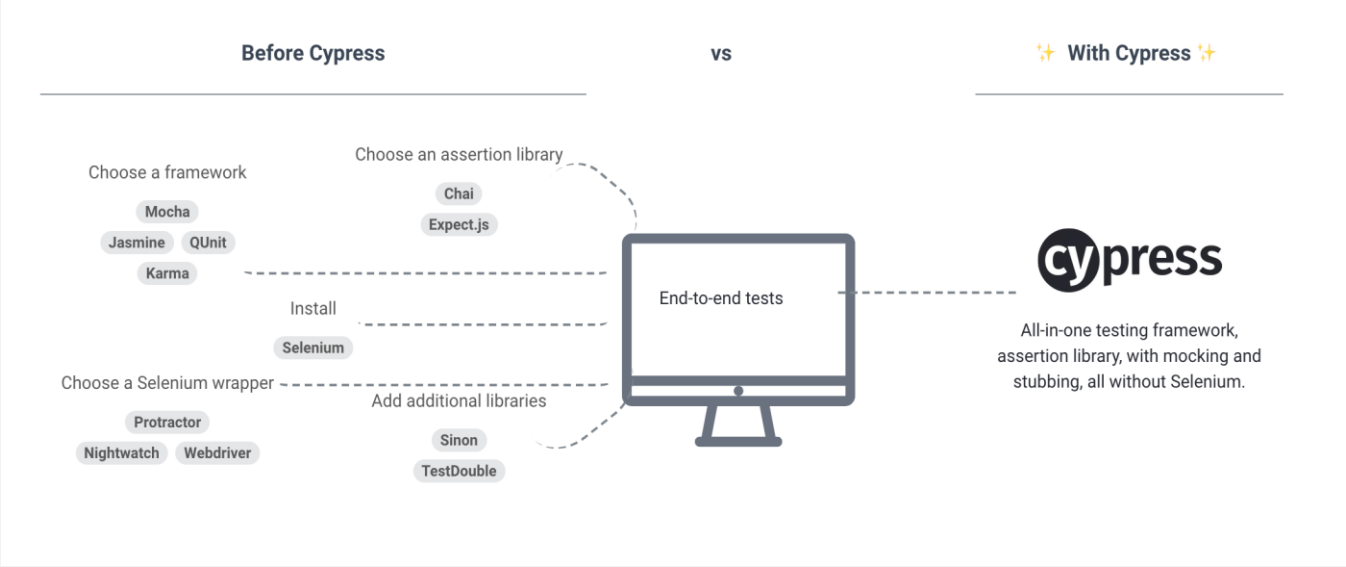
Entonces, ¿cuál es el objetivo de Cypress?

La especialidad de Cypress es mejorar la experiencia de escribir pruebas de extremo a extremo para nuestras aplicaciones web.

Si bien Cypress fue creado pensando en aquellos que programan la parte frontal de las aplicaciones, su innovación más importante es hacer posible el Desarrollo Dirigido por Tests junto con pruebas de extremo a extremo (TDD + E2E). El mejor momento para usar Cypress es mientras se construye la aplicación, ya que está diseñado de modo tal que el desarrollo y el testing puedan suceder de forma simultánea.

Todo en uno

Para poder escribir pruebas E2E, las demás tecnologías necesitan una buena cantidad de herramientas coordinadas entre sí. Con Cypress, no es necesario instalar múltiples frameworks y librerías para poner a funcionar nuestros test suites. Y es que el mismo Cypress cuenta con una compilación de las mejores utilidades que ya conocemos, trabajando en equipo para hacer nuestra labor más llevadera.



¿Cómo funciona?

Pues, detrás de Cypress hay un proceso corriendo un servidor de Node.js. Cypress y el proceso de Node.js se comunican constantemente, se sincronizan, e incluso intercambian tareas entre ellos.

Una vez que el código de las pruebas está corriendo en el navegador, Cypress puede automatizar cosas como hacer click, encontrar objetos, y obtener el texto de un elemento, entre otras.

Cypress también hace operaciones en la capa de la red, teniendo la capacidad de leer y alterar el tráfico sobre la marcha, lo que le permite no solamente modificar todo lo que entra y sale del navegador, sino

también cambiar el código que pueda llegar a interferir con las tareas de automatización sobre el navegador.

Finalmente, Cypress tiene control sobre el proceso completo de automatización, de principio a fin, lo que le da el privilegio de entender absolutamente todo lo que suceda dentro y fuera del navegador. Esto se traduce en resultados y reportes mucho más concisos que los que otras herramientas pueden ofrecer.

Atajos de Cypress

Cypress evita tener que comportarnos como un usuario para poder generar el estado previo a la ejecución de ciertas pruebas; nos habilita controlar la aplicación de forma programática para poder alcanzar las precondiciones que sean necesarias; quita el requerimiento de interactuar con la Interfaz del Usuario para poder probar nuestros escenarios.

Todo esto se traduce en que ya no tendremos que visitar una página de login, ingresar un nombre de usuario y una contraseña, y esperar a que la página cargue o haga el redireccionamiento típico. Tampoco es necesario preocuparse por los CORS; ni por acceder a esos lugares recónditos de la aplicación; ni por tener que correr de forma repetida esas pruebas eternamente lentas que todos bien conocemos.

El poder de elegir cuándo testear la aplicación como un usuario, cuándo saltearse las partes lentas y repetitivas, es nuestra decisión.

¿Con cuál herramienta me quedo?

Si bien Cypress fue creada para hacer posible por primera vez que los desarrolladores frontend puedan realizar pruebas de extremo a extremo en un enfoque de desarrollo dirigido por tests, eso no significa que su uso esté limitado a ellos únicamente.

Los QA Engineers pueden sacarle provecho, y deberían hacerlo, ya que es una herramienta poderosa, muy rápida, que mejora la experiencia de cualquiera que necesite realizar pruebas contra una aplicación web.

Para aprovechar su potencial, es necesario tener claro cuáles son sus puntos fuertes, cuáles son sus limitaciones. Por ejemplo, en algunos proyectos será una delicia ocuparla en momentos en los que necesitemos realizar pruebas E2E; habrá otros proyectos que necesiten un enfoque más integral, para lo cual podremos elegir alguno de los frameworks que ya conocemos.

Los invitamos a que la pruebes con un **simple npm install cypress** y saquen sus propias conclusiones.

UNDERC0DE APP

Hacking y Seguridad Informática

PRÓXIMAMENTE

GET IT ON Google Play

iOS

UNDERC0DE.ORG

CORONA-AI: INVESTIGACIONES DEL COVID-19

Evidentemente en estos tiempos sin precedentes mundial está saliendo a relucir lo mejor de algunos, en este caso es válido mencionar del esfuerzo que están haciendo algunas fundaciones que desean apoyar en las investigaciones del Coronavirus, Imperial College de Londres han unido fuerzas con Fundación Vodafone para lanzar Corona-AI.

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. 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

Es algo que hemos visto en el trascurso de esta pandemia, lo toman humorísticamente dentro de lo que cabe, mencionando “Voy a dormir que mi país me necesita para salvar al mundo”, frases similares podemos leer muy frecuentemente en redes sociales...

¿Qué pensarían si les dijéramos que pueden ayudar a combatir el Coronavirus mientras duermen?

Pues esta iniciativa invita a los usuarios de Smartphone a ser partícipes en este proyecto de investigación, mediante la aplicación gratuita **DreamLab**[4] basada en la nube, que fue creada con el propósito de ayudar en la lucha contra el cáncer ahora habilitada en las investigaciones del COVID-19.

FUNCIONAMIENTO

Mientras cargamos nuestro dispositivo por la noche, de tal manera mientras no se, usa activar la aplicación para compartir los recursos, aprovechando la gran capacidad de procesamiento de los teléfonos celulares, uniendo estos para crear una supercomputadora virtualmente y así procesar millones de datos complejos. En el momento que se desconecta, deja de funcionar. Así, es posible contribuir a la investigación contra esta enfermedad.

El proyecto **Corona-AI**[5] consta de dos fases:

1. La primera se enfocará en el descubrimiento de moléculas basadas en fármacos ya disponibles y alimentos.
2. La segunda implicará combinar candidatos de fármacos, moléculas para crear tratamientos y proporcionar asesoramiento nutricional.

Si bien la investigación experimental y métodos de investigación tradicionales podrían tardar años en desarrollarse, la orientación de procesamiento móvil que propone **DreamLab** puede reducir considerablemente el tiempo para analizar gran cantidad de datos.

Mientras que a un ordenador convencional con un procesador de ocho núcleos funcionando las 24 horas le tomaría décadas procesar millones de datos, contrario a una red de unos 100.000 Smartphone funcionando por 6 horas nocturnas podrían hacer el trabajo en solo unos meses. DreamLab utiliza el aprendizaje automático en una red de supercomputación móvil para analizar miles de millones de combinaciones de medicamentos existentes, moléculas basadas en alimentos e interacciones genéticas, reduciendo fundamentalmente el tiempo necesario para hacer descubrimientos puntuales.

[4] **iOS** apps.apple.com/app/dreamlab/id1273619275?ls=1
Android play.google.com/store/apps/details?id=au.com.vodafone.dreamlabapp&pcampaignid=MKT-Other-global-all-co-prtnr-py-PartBadge-Mar2515-1

[5] www.imperial.ac.uk/news/196733/new-covid-19-project-will-power-smartphones/

DEFEATING UNITY GAME WITH DNSPY, BASIC REVERSING ENGINEERING

CAPTURE THE FLAG / RETOS

Un CTF (Capture The Flag/Captura la bandera). Son competencias que permiten poner a prueba nuestras habilidades sobre hacking por medio de retos de diferentes modalidades que tendremos que resolver para conseguir la famosa **flag** que es un código (Por ejemplo: *fl4g<W3lc0m3_t0_CTF}* que permite confirmar a la plataforma del desafío que hemos sido capaces de resolver el reto y normalmente, va acompañada de una compensación con puntos o premio. La cantidad de puntos irá relacionada con la complejidad del reto y/o tiempo/personas en resolverlo. Por ejemplo, si el reto principalmente vale 100 puntos y hemos sido los 2º en resolverlo, pues el 1º habrá ganado 100 puntos, nosotros (2º) 99 puntos, el 3º 98 puntos, etc.

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

Integrante del Mayas CTF Team equipo orgullosamente mexicano con una meta en común, poner el nombre de México en lo más alto en competiciones tipo CTF a nivel mundial,

Contacto:

Blog: mayas-ctf-team.blogspot.com

Redes Sociales:

Twitter: @chucho_domz

Agradecemos a @ArdaArda **por el contacto**

Los CTFs tienen un tiempo límite para resolver el mayor número de retos posibles y sirven para:

- Adquirir conocimientos y experiencia en el entorno de la seguridad informática.
- Poner a prueba nuestras habilidades de hacking de forma legal y controlada.
- Mejorar nuestro currículum vitae.
- Lo más importante.... ¡Para divertirnos!

Reto de la categoría de *'reverse engineering'* del X-MAS CTF 2019

CHALLENGE

X-MAS: Lapland Mission

I have been trying to win at this game for a while now, but whatever I do there's always a robot that shoots me dead :(
Can you help me win please? **(Game)**
File recognition
Una vez descargado el archivo vemos que es un .exe, procederemos a ejecutarlo en una máquina virtual y veremos de que va.

Al ejecutar el archivo vemos que nos dice **made with unity**, por lo que confirmamos que es un juego hecho en unity.

Al entrar al juego nos dan unas instrucciones del modo de juego y unas recomendaciones.

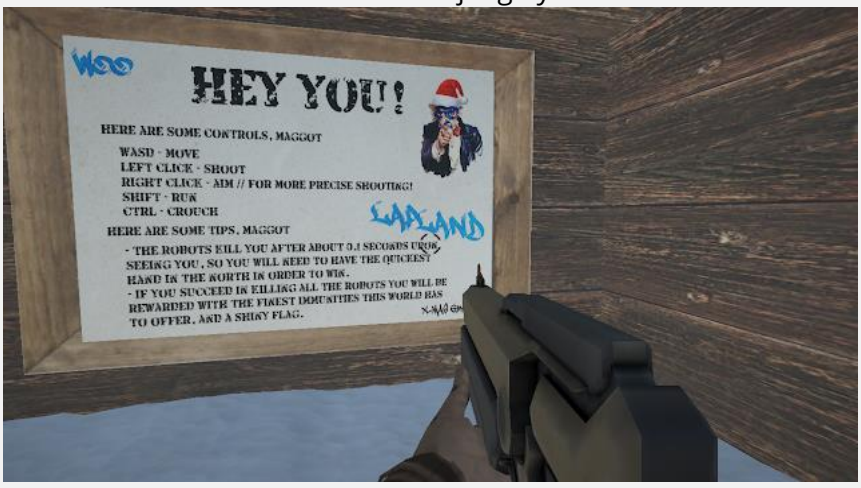


Fig2

Vemos que la parte de recomendaciones hay 2 cosas por notar, la primera es que hay unos robots que apenas te vean te mataran y la segunda es que para conseguir la **flag** hay que matarlos a todos.

Vamos a jugar a ver qué pasa.

Como vemos empezamos en una cabaña y al apenas salir nos disparan los robots.

Fig4

Se intentó ver si se podían ver por las paredes como pasa en algunos juegos, para intentar ver el mapa completo y tampoco se obtuvo resultado.

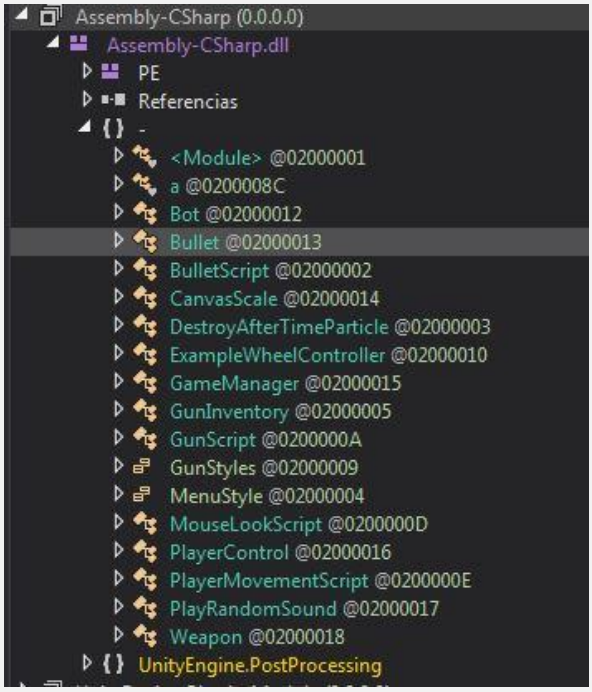
Fig5

Unity es un motor de video juegos multiplataforma que mayormente utiliza el lenguaje del alto nivel **C#** para su programación, aunque también soporta de forma nativa **UnityScript** y **Boo**, siendo estos dos últimos menos populares que el primero.

Hay que recordar que tanto unity como .NET, usan algo llamado **AOT**, **compilación anticipada**, los cuales generan a partir de un lenguaje de alto nivel un lenguaje intermedio (**CIL** en caso de .NET), para posteriormente generan el código ensamblador.
Teniendo en cuenta lo anterior usaremos una herramienta que ya nos ha salvado cuando hemos hecho reversing a .NET, esta es **dnSpy**, que como la documentación dice sirve para debuggear y editar ensamblados de Unity y .NET, una herramienta similar es **ILSpy**.

Ahora bien, el compilado que unity genera lo tenemos en la carpeta \X-MAS_Data\Managed y es el archivo Assembly-CSharp.dll, que es donde unity compilo toda la programación en C#.

Al abrir la DLL vemos todas las clases que el juego tiene programadas, así que vamos a empezar a explorar para ver la forma de ganar.

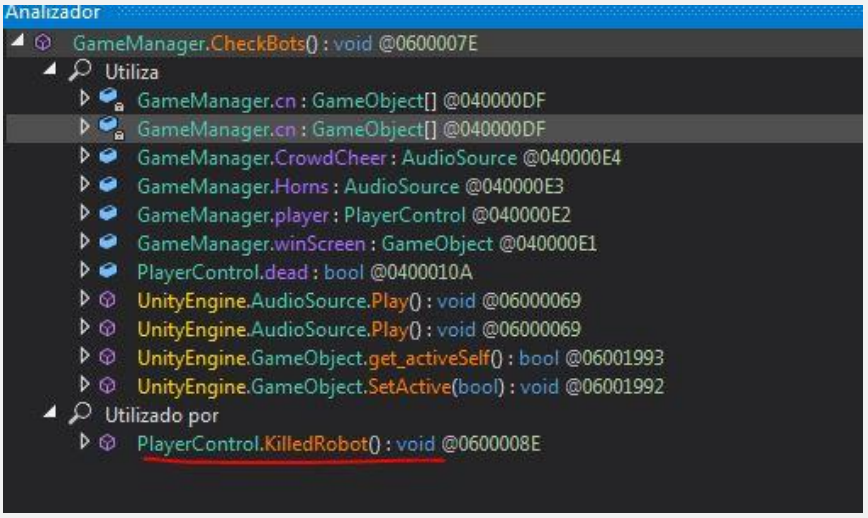


Explorando un rato las clases vemos que la clase **GamerManager**, tiene un método llamado **CheckBots**, el cual revisa que los bots estén activos, en caso de que todos los Robots del juego lo estén, muestra la pantalla de ganador con el método **winscreen.SetActive()**, por lo cual ganaríamos el juego.

```
// Token: 0x0600007E RID: 126 RVA: 0x00005490 File Offset: 0x00003690
public void CheckBots()
{
    bool flag = true;
    for (int i = 0; i < this.cn.Length; i++)
    {
        if (this.cn[i].activeSelf)
        {
            flag = false;
        }
    }
    if (flag)
    {
        this.winScreen.SetActive(true);
        this.player.dead = true;
        this.Horns.Play();
        this.CrowdCheer.Play();
    }
}
```

Fig.7

Vamos a analizar el método para ver donde es llamado este.
Vemos que es llamado en el método **KilledRobot**, de la clase **PlayerControl**.



Con esto confirmamos que tenemos que matarlos a todos para ganar.

La siguiente clase que nos llama la atención es la de **Bot**, donde tenemos varios métodos, uno es el método **Shoot**, que es usado para dispararnos. (Fig9)

```
// Token: 0x06000072 RID: 114 RVA: 0x000023C4 File Offset: 0x000005C4
private void Shoot()
{
    if (!base.gameObject.activeSelf)
    {
        return;
    }
    this.weapon.Shoot();
    if (this.seesPlayer)
    {
        this.player.Die();
    }
}
```

Vemos que dentro de la misma clase en el método **Update**, es llamado mediante el método **IsInvoke**. En la documentación de unity vemos que, el método Update es heredado de **MonoBehavoir**, y este se invocado en cada frame del vídeo juego.

Llegamos a la conclusión que en este método se usa para dispararnos, en concreto en las siguientes condiciones.

```
private void Update()
{
    if (this.player.dead)
    {
        return;
    }
    base.transform.LookAt(this.playerHead);
    base.transform.rotation = Quaternion.Euler(0f, base.transform.rotation.eulerAngles.y, 0f);
    RaycastHit raycastHit;
    if (!Physics.Raycast(this.head.position, (this.playerHead.position -
      this.head.position).normalized, out raycastHit, float.PositiveInfinity))
    {
        this.bl();
        return;
    }
    if (raycastHit.transform.tag == "Player")
    {
        if (!this.seesPlayer)
        {
            this.seesPlayer = true;
            this.robotWake.Play();
            this.laserSound.PlayRandom();
        }
        if (!base.IsInvoking("Shoot"))
        {
            base.Invoke("Shoot", 0.1f);
        }
        this.cg.SetPosition(0, this.gunSight.transform.position);
        this.cg.SetPosition(1, this.playerHead.position + new Vector3(0f, -0.12f, 0f));
        return;
    }
    this.bl();
}
```

Fig10

El **seesPlayer** se inicializa en **FALSE**, así que el robot nos disparara en cuanto nos vea. En la siguiente condición **IsInvoking** retorna **FALSE** por lo que entra a la condición llamando a la función **Shoot** con 0.1(Fig9).
Quitaremos los operadores **NOT** de las condiciones para que aunque se muestre la animación donde nos disparan, seamos inmunes al no invocarse el método **Shoot** (Fig9) y podamos ganar. (Fig11)

```
}
if (raycastHit.transform.tag == "Player")
{
    if (this.seesPlayer)
    {
        this.seesPlayer = true;
        this.robotWake.Play();
        this.laserSound.PlayRandom();
    }
    if (base.IsInvoking("Shoot"))
    {
        base.Invoke("Shoot", 0.8f);
    }
    this.cg.SetPosition(0, this.gunSight.transform.position);
    this.cg.SetPosition(1, this.playerHead.position + new Vector3(0f, -0.12f, 0f));
    return;
}
```

Fig11

Con esto hecho recompilamos la DLL y sustituimos la original.

Abrimos el juego y probamos. Y si todo correcto a pesar de que la animación se muestra la función **Shoot** no es invocada por lo tanto no entra el método **Die** de la clase **Player** (Fig9) y no morimos. (Fig12)

Fig12

Funciono, la animación se muestra, pero no morimos.
Acabaremos con los robots para ganar el juego.

Eliminamos al último.

¡Ganamos y obtenemos la flag!

Fig14

Flag
X-MAS{G3T_GOOD_G3T_LM4O_BOX}

CHEAT-SHEET: C#

C Sharp es un lenguaje de programación orientado a objetos desarrollado y estandarizado por Microsoft como parte de su plataforma.NET, que después fue aprobado como un estándar por la ECMA e ISO. Su sintaxis básica deriva de C/C++ y utiliza el modelo de objetos de la plataforma.NET el cual es similar al de Java aunque incluye mejoras derivadas de otros lenguajes (entre ellos Delphi).

TIPOS DE DATOS

C# contiene dos categorías generales de tipos de datos integrados: tipos de valor y tipos de referencia. El término tipo de valor indica que esos tipos contienen directamente sus valores.

byte Entero sin signo de 8 bits
sbyte Entero con signo de 8 bits
short Entero corto
ushort Entero corto sin signo
int Entero medio
uint Entero medio sin signo
long Entero largo
ulong Entero largo sin signo
float Punto flotante corto
double Punto flotante largo
decimal Punto flotante monetario

No existen conversiones automáticas de tipo entero a char.
char Carácter 16 bit unicode
string Cadena de carácteres

bool true or false
No existe una conversión definida entre bool y los valores enteros (1 no se convierte a verdadero ni 0 se convierte a falso).

CONSTANTES

se denominan literales. Todas las constantes tienen un tipo de dato, en caso de ser una constante entera se usa la de menor tamaño que pueda alojarla, empezando por int. En caso de punto flotante se considera como un double. Sin embargo se puede especificar explícitamente el tipo de dato que una constante deberá usar, por medio de los sufijos:

SUFIJO	TIPO DE DATO	EJEMPLO
L	long	12L
UL	ulong	68687UL
F	float	10,19F
M	decimal	9,95M

VARIABLES

Toda variable se debe declarar antes de ser utilizada.

```
tipo nombre_variable;
```

Asignar un valor a una variable:

```
nombre_variable = valor
```

OPERADORES

OPERADOR	SIGNIFICADO	TIPO
+	Suma	Aritmético
-	Resta	""
*	Producto	""
/	División	""
%	Módulo	""
++	Incremento	""
--	Decremento	""
==	Igual que	Relacional
!=	Distinto que	""
>	Mayor que	""
<	Menor que	""
>=	Mayor o igual que	""
<=	Menor o igual que	""
&	AND	Lógico
|	OR	""
^	XOR	""
||	OR	""
&&	AND	""
!	NOT	""
	A NIVEL DE BITS	
~	Complemento a uno	
<<	Desplazamiento a la izquierda	
>>	Desplazamiento a la derecha	

INSTRUCCIONES DE CONTROL

if-else básicamente como C, C++ y Java.
switch a diferencia con la versión de C, C++ y Java es que todo cuerpo que pertenciente a un case debe de toparse con un break o un goto antes de toparse con otro case, a menos que dicho cuerpo esté vacío.
for básicamente igual que en C, C++ y Java.
while es básicamente como C, C++ y Java.
do-while como en C, C++ y Java.
foreach realiza un ciclo a través de los elementos de una colección (grupo de objetos). El formato de esta instrucción es:

```
foreach(tipo variable in coleccion)
```

En este ciclo se recorre la colección y la variable recibe un respectivo elemento de dicha colección en cada iteración.

Las siguientes instrucciones como C++ y C
break permite forzar la salida de un ciclo omitiendo el código restante en el cuerpo del ciclo.
continue permite forzar la repetición temprana de un ciclo omitiendo el código restante en el cuerpo del ciclo.
return devuelve un valor de un método.
goto se sigue utilizando en C# a pesar de toda la polémica que esto conlleva.

MÉTODOS

Todo método debe de ser parte de una clase, no existen métodos globales. De forma predeterminada, los parámetros se pasan por valor (se copia dicho valor).
ref forza a pasar los parámetros por referencia en vez de pasarlos por valor.
out es similar al modificador ref con una excepción: sólo se puede utilizar para pasar un valor fuera de un método. El método debe de asignar un valor al parámetro antes de que el método finalice. Cuando ref y out modifican un parámetro de referencia, la propia referencia se pasa por referencia.
params define un número variable de argumentos los cuales se implementan como una matriz.
Ejemplo: `public int maxVal(params int[] nums){...}, esta función se podría llamar así: maxVal(23,3,a,-12);.`
Un método debe tener como máximo un único parámetro params y éste debe de ser el último, puede devolver cualquier tipo de datos, incluyendo tipos de clase. Las matrices se implementan como objetos, un método también puede devolver una matriz (algo que se diferencia de C++ en que las matrices no son válidas como tipos de valores devueltos).
C# implementa sobrecarga de métodos, dos o más métodos pueden tener el mismo nombre siempre y cuando se diferencien por sus parámetros.
Main es un método especial al cual se refiere el punto de partida del programa.
Sintaxis:

```
public static int Main(string[] args){...}.
```

MATRICES

Se implementan como objetos.

```
tipo[] nombre_matriz = new tipo[tamaño];
```

Para inicializar:

```
tipo[] nombre_matriz = { val1 , val2 , val3 , ... , valN };
```

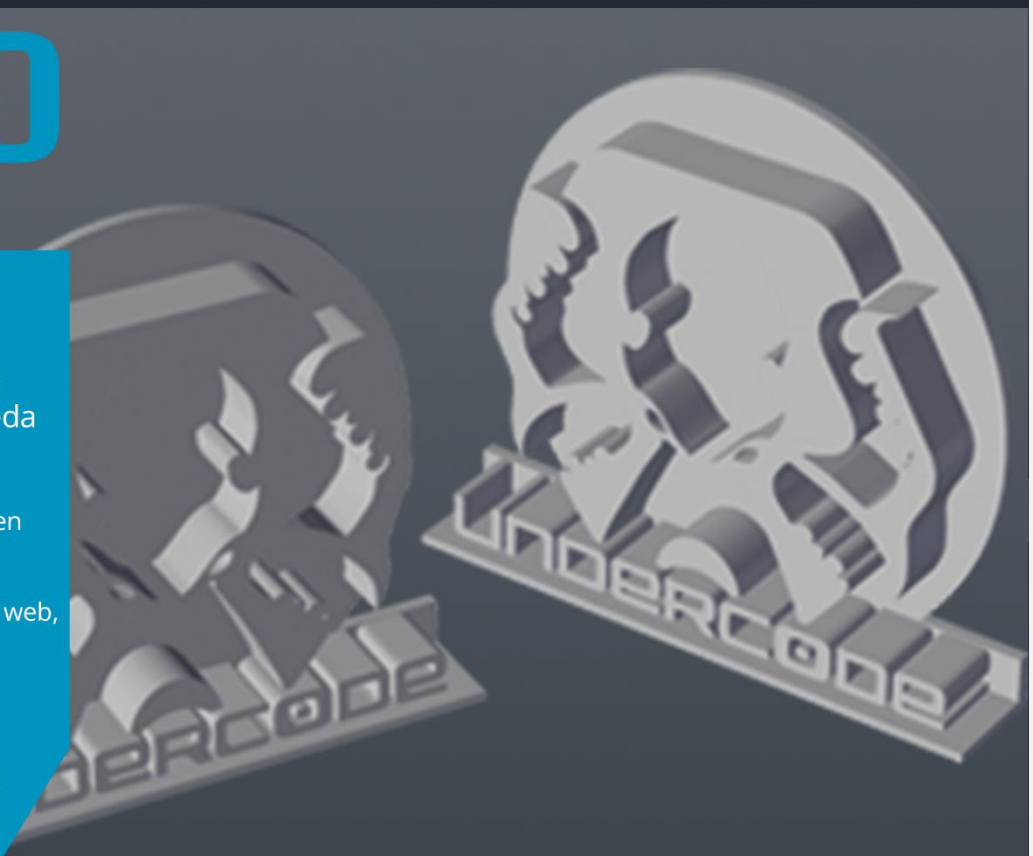
Los índices de las matrices comienzan en 0.
Matriz bidimensional:

```
tipo[,] nombre_matriz = new tipo[filas,columnas]
```

Un elemento de una matriz bidimensional no se usa la forma matriz[fila][columna] (la cual usa C++), si no matriz[fila,columna].
Ya que C# implementa matrices como objetos, cada matriz tiene asociada una propiedad Length que contiene el número de elementos que puede alojar cada matriz.

ABRIL

2020



uDork

Script hecho en Python, utiliza técnicas avanzadas de búsqueda de Google para:

- Obtener información confidencial en archivos o directorios
- Encontrar dispositivos IoT
- Detectar versiones de aplicaciones web, etc.

SOURCE:
github.com/m3n0sd0n4ld/uDork

TOOLBOXUC

SOURCE UNDERC0DE.ORG/FORO/IMPRESIONES-3D/ADORNO-PULPO-UNDERC0DE-3D

DO	LU	MA	MI	JU	VI	SA
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

UNDERC0DE.ORG

EASYPHPCRACKER

UNDERTOOLS DIY

En esta ocasión en **Undertools DIY** realizando un diseño sencillo de un crackeador de **hashes** escrito en **PHP**. Este lenguaje de programación está muy extendido y como lenguaje docente resulta un lenguaje bastante accesible y probablemente no dé tanto miedo como otros lenguajes como puede ser C.

Escrito por: **@ANIMANEGRA** | **COLABORADOR** UNDERC0DE

Siempre pensando en que la comprensión y creación de la tecnología es un arte agrario y que esta tiene una vinculación consustancial con la sociedad, entiende que la mejor forma de que se prospere es regar y cuidar con mesura los conocimientos que en ella se portan. y ver como poco a poco crece el conocimiento y destreza, gracias a la información, con ayuda de explicaciones poder conformar una sociedad tecnológica que vaya de la mano de la ética humana. Ampliamente ligado al espíritu investigador, educador, social y ético intenta formar parte de la gente que ofrece una pequeña ayuda a que la tecnología se convierta en una herramienta de unión y no en un muro a saltar, otorgando comprensión en un mundo que para muchos resulta mágico y por ende, aterrador en muchos de sus aspectos.

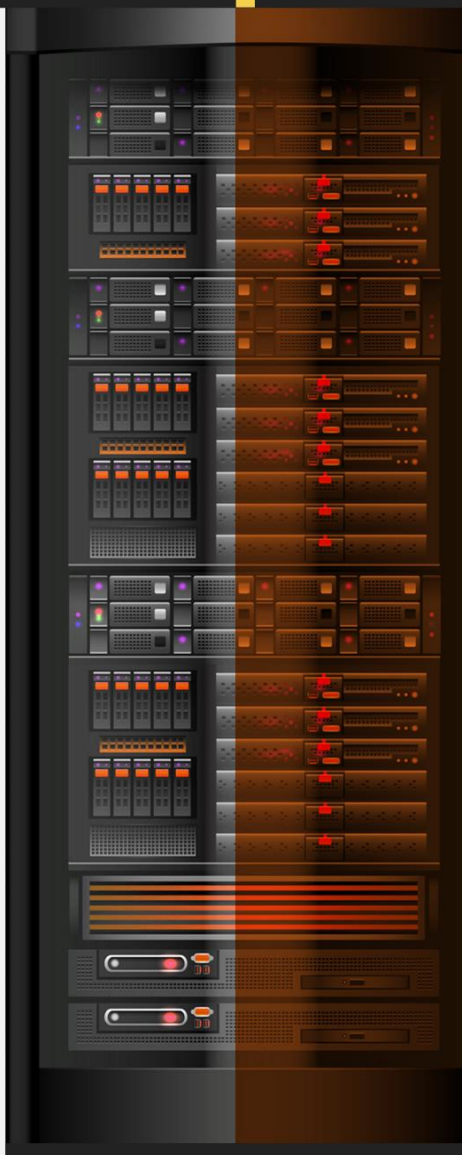
Contacto: underc0de.org/foro/profile/animanegra

Redes Sociales:

Github: github.com/4nimanegra

taller

Los **hashes** se refieren al resultado de unas funciones de una sola dirección que se utilizan ampliamente en los sistemas de autenticación. Cuando se guarda un dato para poder autenticar a alguien no interesa que sea la contraseña directamente ya que, ante cualquier eventual hackeo, el hacker dispondría de las contraseñas en limpio de todos los usuarios del sistema.



Como los **hashes** son el resultado de dichas funciones unidireccionales es sencillo realizar la operación de obtener el **hash** pero resulta imposible matemáticamente realizar la inversa de la función. Esto implica que no existe función matemática a partir de la cual, desde el **hash** se obtenga el contenido original que se había introducido dentro la función. Hay distintas operaciones de **hashing** entre ellas se incluyen las más famosas **MD5, SHA1, SHA256** y **SHA512**. Cuando tenemos un **hash** del que se desea saber qué palabra original lo obtiene como resultado, la única forma que disponemos para obtenerla es realizar pruebas de distintas entradas para intentar obtener el mismo resultado. A dicha acción se le suele denominar **crackeo** de contraseñas.

Para el **crackeo** de contraseñas disponemos de dos opciones, generar todas las palabras posibles de distintas longitudes hasta dar con el **hash** o utilizar un diccionario de palabras.

- La primera opción tarde o temprano dará con el resultado, dependiendo del tamaño de la contraseña puede que no vivamos para verla.
- La segunda opción es muy útil porque el número de pruebas totales se reduce por contra, si la contraseña no está incluida en el diccionario, no se obtendrá la contraseña.

En este documento se explicará cómo programar una herramienta que automatice el cálculo de la contraseña utilizando ambas formas. Para la realización del cálculo de los **hashes** se utilizarán las librerías de **openssl**.
Generaremos una función llamada **testHash** que será la encargada de realizar el **hash** de una palabra. En caso de que el **hash** sea el mismo que el **hash** que se está buscando dicha función terminará el programa mostrando por pantalla la palabra original que se corresponde con el **hash**.

Además, la función permitirá seleccionar entre utilizar **MD5, SHA1, SHA256** y **SHA512** pasándoselo en los parámetros. El código correspondiente a la función es el siguiente:

Código: PHP

```php
function testHash($HASH,$palabra,$CRACKTHIS){
        switch($HASH){
          case "MD5":
          case "SHA1":
          case "SHA256":
          case "SHA512":
             $TESTHASH=openssl_digest($palabra,$HASH);
              break;
           default:
                  die();
                  break;
      }
```

Al inicio del programa se definirán unas variables que permitirán determinar entre que caracteres se aplicarán el método que realiza las pruebas para todas las posibles combinaciones. También determinarán la longitud inicial y la longitud final para este caso concreto de búsqueda de **hashes**. Se definirá de forma fija que los caracteres irán desde el **0** hasta el carácter **z**, que mayormente incluye todos los caracteres habituales imprimibles que se utilizan para las contraseñas. La longitud inicial será de **1** y la longitud máxima será de **6** por defecto:

Código: PHP

```php
<?php
    $FIRSTCHAR='0';
    $LASTCHAR='z';
    $maxleng=6;
    $leng=1;
    $hash=”MD5”;
```

Además, se desea que el usuario de la herramienta pueda definir dichas variables o de definir un archivo de contraseña para realizar el **cracking**. Se tomará la variable **$_SERVER['argv']** que es el vector de argumentos que se le pasan al programa para ver si el usuario ha introducido algún modificador, en nuestro caso estos incluirán **-l, -i, -h** y **-d** para definir la longitud máxima, la longitud inicial, el **hash** a utilizar o si se desea utilizar un archivo de diccionario respectivamente.
Cada modificador requerirá que el siguiente argumento defina o bien la longitud en el caso de **-l** o **-i**, un nombre de **hash** en el caso de **-h** y un nombre de archivo en el caso de **-d**. También deberemos introducir seguido del comando el **hash** que deseamos romper.
El código encargado de hacer esto simplemente da un paseo por los argumentos introducidos por el usuario y si se encuentra un modificador, obtendrá el valor correspondiente del siguiente argumento como valor para la variable que lo define.

Es un código relativamente sencillo con un bucle **while** que va avanzando y comprobando los argumentos. En caso de encontrar alguno de los modificadores, aquellos cuyo primer carácter es **-**, cambiará el valor de la variable correspondiente. En caso de no ser un modificador o su respectivo valor, se decide que ese argumento debería de ser el **hash** a comprobar. Si no se introduce ningún argumento en la herramienta, esta simplemente no ejecutará nada:

Código: PHP

```php
$I=1;
    while($I < count($_SERVER['argv'])){
       if($_SERVER['argv'][$I][0] != "-"){
          if(isset($CRACKTHIS)){die();}
          $CRACKTHIS=$_SERVER['argv'][$I];
       } else {
          if($_SERVER['argv'][$I][1] == "l"){
             $I=$I+1;
             $maxleng=$_SERVER['argv'][$I];
          } else if($_SERVER['argv'][$I][1] == "i"){
             $I=$I+1;
             $leng=$_SERVER['argv'][$I];
          } else if($_SERVER['argv'][$I][1] == "h"){
             $I=$I+1;
             $HASH=strtoupper($_SERVER['argv'][$I]);
          } else if($_SERVER['argv'][$I][1] == "d"){
             $I=$I+1;
             $DICTIONARY=$_SERVER['argv'][$I];
          }
```

La ejecución dependerá de si se ha seleccionado el uso de diccionario o no. En caso negativo deberemos de realizar todas las posibles palabras utilizando los caracteres que van desde **$FIRSTCHAR** hasta **$LASTCHAR**. La forma de realizar esto es definir primero la longitud de un **array** o tabla. Dicha longitud empezará por **$leng** e iremos incrementando en **1** hasta que lleguemos a la longitud definida en **$maxleng**. Cada vez que incrementamos en **1** la longitud del **array** se inicializa en todas las posiciones el carácter definido en **$FIRSTCHAR** y después se irá iterando hasta que todas las posiciones de la tabla tengan el valor **$LASTCHAR** en ellas.

La forma de iterar se parece bastante a la forma de realizar las sumas cuando estábamos en el colegio, pero sumando al número siempre **1**. En el colegio cuando tenemos un número determinado si le sumamos **1** pueden pasar dos cosas, que en su último dígito lleguemos al **10** o que no lleguemos a él. Si llegamos al **10** entonces se vuelve a poner **0** en el último dígito y al penúltimo dígito se le sumará **1** siguiendo el mismo proceso. Si no llegamos a **10** se pondrá en esa posición el resultado de la suma, si no pondremos un **0** y a la siguiente posición aplicaremos la misma norma. Cuando se llega a que todos los números son **9**, si se le suma uno lo que se hace es ampliar el número de dígitos poniendo un espacio numérico más. En nuestro caso ejecutaremos la misma idea, solo que los dígitos en lugar de comprender del **0** al **9**, compondrán del **0** a la **z**. En formato **ASCII,** en realidad tendremos en cada posición números que comprenden desde el **48** al **122**.

En el **array $palabra_arr** mantendremos la representación numérica del **ASCII** y en $**palabra** se compondrá en cada iteración el **string** en formato **ASCII**, conformado por todas las letras que representan los números incluidos en el **array $palabras_arr**. Mayormente, se forma un **string** para poder después realizar su **hash** y poder comprobar si este, es el **hash** que buscábamos. El código de dicha funcionalidad, que va probando las palabras de distinta longitud es el siguiente:

Código: PHP

```
1.  if(!isset($DICTIONARY)){
2.        while($leng <= $maxleng){
3.           $I=0;
4.           while($I < $leng){
5.              $palabra_arr[$I]=ord($FIRSTCHAR);
6.              $I=$I+1;
7.           }
8.           while($palabra_arr[$leng-1] < ord($LASTCHAR)){
9.              $I=0;
10.             $palabra="";
11.             while($I < $leng){
12.                $palabra=$palabra.chr($palabra_arr[$I]);
13.                $I=$I+1;
14.             }
15.             testHash($HASH,$palabra,$CRACKTHIS);
16.             $I=0;
17.             while($I < $leng && $palabra_arr[$I]==ord($LASTCHAR)){
18.                $palabra_arr[$I]=ord($FIRSTCHAR);
19.                $I=$I+1;
```

Por último, si el usuario ha deseado utilizar un diccionario, simplemente abriremos el archivo e iremos calculando el **hash** de cada una de las líneas de dicho archivo.
El código responsable de esto es notablemente más sencillo que el anterior, ya que simplemente se deberá abrir el archivo especificado por el usuario mediante **fopen** e iremos leyendo cada una de las líneas mediante **fgets**. Hay que tener en cuenta que **fgets** obtiene cada una de las líneas con el salto de línea deberemos eliminar mediante la función **trim** para después realizar el cálculo del **hash**. El código de este apartado será el siguiente:

Código: PHP

```
1.  } else {
2.        $f = fopen($DICTIONARY,"r");
3.        if(isset($f)){
4.           while($palabra = fgets($f)){
5.              $palabra=trim($palabra);
6.              testHash($HASH,$palabra,$CRACKTHIS);}}}
7.  ?>
```

De frente a la ejecución del programa realizado simplemente se deberemos llamar desde la línea de comando el comando **php** seguido del nombre del programa que se ha generado y los argumentos requeridos.
Ejemplo: si deseamos calcular qué palabra hay detrás del **md5 4d186321c1a7f0f354b297e8914ab240** se ejecutará el siguiente comando:

Código: PHP

```
1. animanegra@host:~/$ php ./EasyPhpCracker.php 4d186321c1a7f0f354b297e8914ab240
2. hola
3. animanegra@host:~/$
```

Se puede ejecutar la herramienta con los modificadores definidos. Por ejemplo, para obtener la contraseña que se corresponde con el valor **sha1 81fe8bfe87576c3ecb22426f8e57847382917acf** alternativamente ejecutaremos también el programa de la siguiente forma:

Código: PHP

```
1. animanegra@host:~/$ php ./EasyPhpCracker.php 81fe8bfe87576c3ecb22426f8e57847382917acf -h sha1
2. abcd
3. animanegra@host:~/$
```

Los códigos **PHP** podemos ejecutarlas como **scripts** de forma directa incluyendo en la primera línea del código la ruta al intérprete que se utiliza para ejecutarlo. En este aspecto es bastante análogo a los **scripts** programados en **bash**.
De forma que si la ruta al binario del intérprete **PHP** fuese **/usr/bin/php** podemos incluir en la primera línea lo siguiente:

Código: PHP

```
1. #!/usr/bin/php
```

Debemos tener en cuenta que debemos dar al **script** permisos de ejecución de esta forma:

Código: PHP

```
1. animanegra@host:~/$ chmod +x ./EasyPhpCracker.php
```

Una vez hecho esto se puede ejecutar el programa directamente mediante la siguiente instrucción:

Código: PHP

```
1. animanegra@host:~/$ ./EasyPhpCracker.php 81fe8bfe87576c3ecb22426f8e57847382917acf -h sha1
2. abcd
3. animanegra@host:~/$
```

mensajes / opiniones de nuestros usuarios

"La revista quedó Hermosa...

Simplemente hermosa. Siento una atracción por esta revista cómo ninguna otra, es cómo un positivismo que quedó impregnado, dotándola de un cerebro constituido por millones de usuarios que invirtieron amor en algo que no muchos pueden ver un camino de rosas.
Apenas me he leído cuatro artículos y he quedado maravillado, creo que es una de las mejores revistas que se ha dedicado con tanto esfuerzo y amor a toda la comunidad fuera y dentro de Underc0de.

DTXDF
VÍA FORO UNDERC0DE

"Excelente material... gracias!

ALGONCA00
VÍA FORO UNDERC0DE

"Muchas gracias a todos los que hacéis esto posible, staff, colaboradores y usuarios. A por 9 años más que estos han pasado muy rápido Saludo.

BLACKDRAKE
VÍA FORO UNDERC0DE

"¡Gracias Denisse, me gustó mucho tu mensaje y el post en sí! Toda "orgullosa" de ser parte del staff Oficial, un grupo y equipo de excelencia.

GABRIELA
VÍA FORO UNDERC0DE

"Felicidades al equipo que hace posible UnderDOCS, agradezco por el esfuerzo y tiempo dedicado. Y agregar que estoy al tanto cada 10 del mes para ver la revista. ¡Sigan adelante!!!

GH0STSNIP3R
VÍA FORO UNDERC0DE

"Gracias por todo el trabajo que te tomas en sacar las revistas. Están geniales

ANIMANEGRA
VÍA FORO UNDERC0DE

"Thanks, cada mes lo espero.

LAUTI
VÍA GRUPO DE TELEGRAM UNDERC0DE

"Excelente revista e información!

MARLON ESCOBAR
VÍA GRUPO TELEGRAM UBUNTU EN ESPAÑOL

"Felicitaciones al equipo Underc0de en su (9°) |\|oveno aniversario. Que vengan ya nuevos retos. Gracias Underc0de.

BENGALA
VÍA FORO 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.