#06

ENERO 2020
EDICIÓN

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

DIGITAL MAGAZINE

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

***Gracias** por hacer posible que **Underc0de** crezca y se fortaleza.*
Seguiremos aprendiendo, compartiendo y EVOLUCIONANDO.

UNDERC0DE.ORG

UNDERC0DE

UNDERDOCS #06

5/Enero/2020 - 9no aniversario de Underc0de.

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 UNDERC0DE (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.

CELEBRAMOS 9 AÑOS DEL INICIO DE NUESTRA COMUNIDAD.

Nos complace ser testigos de cómo **sigue creciendo nuestro foro día a día**, con altibajos como todos los proyectos, pero siempre con el **propósito de seguir adelante**, de no dejar morir underc0de y sobretodo de seguir evolucionando.
En estos 12 meses concentramos nuestras energías en atraer **nuevos Underc0ders**, interesarlos mediante **podcast, post, incluso dudas y nuestra E-ZINE UnderDOCS**, cada contribución así se considere pequeña son los responsables de mantener con vida esta gran comunidad.
Actualizamos la apariencia del foro con la intención de hacerlo responsivo y más atractivo, incorporando una nueva sección llamada **Hacking Tools** (Herramientas de Hacking, Documentación de tools que trae Kali-Linux y las distros de pentesting.) underc0de.org/foro/herramientas-hacking/, además nuestro blog.underc0de.org recibió una renovación, todo para **recibir el 2020 con prosperidad y frescura**.
Nos sentimos muy contentos por cumplir con nuestras metas y expectativas del año pasado, viendo nuestros proyectos realizados y ¡**vamos por más**!

Porque los desafíos continúan y sobre todo la ardua labor.
Somos una comunidad afortunada por seguir de pie y cada **usuario** que **consulta/publica** valiosa información, cada integrante del **staff** que **aporta contenido/ideas** y apoya en el mantenimiento de nuestro querido foro, todos los que **ayudan compartiendo nuestro contenido en redes sociales/blogs** por difundir les estamos muy agradecidos.
A la fecha tenemos **+71K de usuarios** aprendiendo y compartiendo desde el 2011, **pilares indispensables** para hacer posible que UNDERC0DE crezca y se fortalezca.

El Staff Oficial de Underc0de
@ANTRAX @79137913 @BLACKDRAKE @GABRIELA @DENISSE @AXCESS @HATI @DRAGORA @BARTZ @DTXDF @XYZ @SADFUD @DEBOBIPRO @KAIL @ANIMANEGRA.

De quienes estamos **muy orgullosos y agradecidos** de poder contar con un gran **>**Underc0de**team**< siempre activos y pendientes de lo que sucede.

CRÉDITOS

UNDERDOCS ES POSIBLE GRACIAS AL COMPROMISO DE

TEAM:

@ANTRAX
@DENISSE
@DRAGORA
@ANIMANEGRA
@ARDAARDA
@MR.EBOLA
@OROMAN
@EBOHUE
@MRXVS

DIFUSIÓN:

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

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

CONTACTO:

INFO@UNDERC0DE.ORG REDACCIONES@UNDERC0DE.ORG

BITCOIN: TECNOLOGÍA, ECONOMÍA Y FUTURO

CRIPTOMONEDAS /BLOCKCHAIN

Un Bitcoin ha sido un hito interesante en toda la década... ya sea por sus subidas o bajadas de precio, por su base en la que está montada llamada blockchain o por la rebeldía que ha causado al ser una moneda deflacionaria, **pseudo-anónima**, sin control central y lo más importante, **escasa**...

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

Prometheo

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

Bitcoin es el caso de uso **más relevante** de la tecnología que llamamos **blockchain**, un libro de contabilidad distribuido, que cuenta con 4 grandes propiedades:

1. Red P2P
2. Criptografía PKI
3. Inmutable
4. Utiliza un Ledger

La unión de estas cuatro partes la hace **tecnológicamente resistente**, por lo cual, en sus inicios, comenzó a tener su uso en los **mercados negros** ya que en ese momento (por ahí del año 2010) era muy complicado **rastrear las transacciones** que se hacían entre los *compradores y los vendedores*, haciendo su uso muy popular por su **anonimato**, comenzando a darle un valor en sí...

Ahora es posible comprar desde drogas, armas y muñecas inflables sin tener que hacer uso de una tarjeta de crédito o estar relacionados con alguna compra personal.

> *Considero que en eso pensaron en esos tiempos.*

Con el paso de los años, esta aplicación fue tomando una forma más real, no solo como una manera de comprar cosas ilegales o contratar hackers a sueldo y cosas por el estilo, que es lo que se rentaba bastante en aquellos tiempos sobre la red **TOR**, después de un tiempo, las personas comenzaron a notar, que este **activo digital** nacido de las sombras del internet profundo, tenía propiedades muy interesantes, que podrían ser utilizadas para propósitos más financieros.

Propiedades del Bitcoin en la economía

- **Portable**: Es posible tener un millón de bitcoin en un Ledger y moverlo por el mundo sin tener que hacerlo público.
- **Es fungible**: Todas las unidades son intercambiables.
- **Pseudo anónimo**: No se refleja la identidad real de su propietario y no es necesario identificarse para participar en la red bitcoin, aunque al contrario que una red anónima, permite generar una reputación y confianza entre los distintos usuarios.
- **Escaso**: Solo se pueden emitir 21,000,000 de estas **monedas digitales**.
- **Soberano**: la red de bitcoin no necesita alguien que la gobierne ya que se autoliquida con cada transacción.
- **Infalsificable:** Como tal, no es que sea infinitamente poderosa para que no sea falsificada, sino que, al ser una red P2P madura, esto la convierte en una red computacionalmente inviable de atacar para poder falsificar una sola transacción.

Y así podemos seguir con propiedades y características, pero el foco en todas sus propiedades, o en lo que consideramos el foco más relevante es: **SU ESCASEZ**.

Retomando un poco el tema financiero, se han puesto a pensar, ¿Por qué nuestro dinero tiene valor? ¿Es decir, final de cuentas, se imprime como loco... no tiene una base sustentada, no es escaso... Entonces ¿Por qué nuestro dinero, un billete de 200 por ejemplo puede adquirir algún bien o algún servicio?
La respuesta radica en el tipo de papel con el que los gobiernos cobran los impuestos y la gente como nosotros confía en él, así de simple.

A diferencia de los metales preciosos como el oro, la plata o el platino, que su valor radica en su escasez, su pureza y el costo que es extraerlos de la tierra, el dinero en papel no cuesta más, que el papel en el que este impreso.

El **Bitcoin**, llega a al mundo como un **tipo de cambio alternativo**, al igual que el oro, es escaso, y también su costo de fabricación es demasiado alto, y lo más importante, la gente comienza a confiar en él, al no tener un gobierno que pueda manipularlo se comienza a ser atractivo y las personas lo utilizan cada vez más. Convirtiéndose en un problema, ya que este nuevo activo de la última década, otorga poder a la gente y quitándole jurisdicción a los bancos, ya que al ser un **sistema Pseudo anónimo**, no hay manera exacta de cobrar impuestos, y como es evidente, al gobierno no le gusta eso.

También suelen llamarlo "**almacén de valor**" ya que los gobiernos devalúan su propia moneda para ser más competitivos en los mercados imprimiendo millones y millones de billetes, al contrario bitcoin se sigue minando y no habrá más de 21 millones de piezas en este juego, no se pueden falsificar, ni se pueden crear más de las escritas, al no poder emitir millones de bitcoin nuevos cada día, esto crea una sensación de necesidad, y la gente que lo tiene, generalmente lo almacena, vendiendo su dinero falso y comprar algo que tiene un propósito y una finalidad.

No puede ser congelado por ninguna entidad, eso genera una sensación de alivio para las personas que adquieren este tipo de bienes intangibles.

> *El **Bitcoin**, es la solución que viene a arreglar los problemas, que el dinero a creado en las últimas décadas.*
> *- Max Keiser un comentarista financiero y corredor de bolsa en Wall Street*

En el futuro podemos visualizar al bitcoin, como un método de pago alternativo a las monedas locales, no quiere decir que el bitcoin sea el reemplazo de las monedas utilizadas en el mundo, sino como un activo, una manera de poder enviar riqueza de un lado del mundo a otro, sin tener que pagar grandes cantidades de dinero por estas operaciones, realizándolas de manera segura, flexible y portable.

> *Como decía Max Keiser en uno de sus programas: "El bitcoin es el dinero interplanetario".*

Como ellos lo ven, con un par de satélites conectados a la red de bitcoin, se puede enviar valor de un planeta a otro, y eso mis amigos, no es algo tan descabellado, ya que las Telecom pueden hacer esto posible, que es algo que quizá no puedan ver nuestros ojos, es razonable, pero si existe en la teoría local, se puede aplicar a la teoría del futuro, por eso siempre es bueno tener algo de efectivo, algo de riqueza en metales y algo de bitcoin como patrimonio.

EVOLUCIÓN DEEPFAKES

NOTICIAS INFORMÁTICAS

Deepfakes **ayuda a editar videos falsos de personas reales en situaciones desconocidas,** ha avanzado en corto tiempo, dando como resultado ser cada vez más realistas y al alcance de todos.

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

Amante por la seguridad de la información, social y las buenas practicas. Le encanta la ciberseguridad, investigar para estar acorde al crecimiento de los ataques efectuados en cada momento.

Contacto:
underc0de.org/foro/profile/Ebohue

Función

Se selecciona un video base, luego se cargan las fotos de la cara donde muestra diferentes miradas, gestos o perspectivas de la víctima, para dañar su imagen o jugar una mala pasada, posteriormente entra IA para que cada imagen pueda adaptarse al ciclo del video.

La **veracidad de un video expuesto** es cada vez más complicada de comprobar porque la autenticidad del video engaña a la vista habitual de cada persona.

El **96%** de los deepfakes[1] que circulan en las redes son *pornográficos* y las víctimas son mujeres, este estudio ha elaborado **Deeptrace**, el cual recibe más de 134 millones de visitas en todo el mundo.

Paul Barret, profesor adjunto de derecho en la Universidad de New York, explica que los deepfakes son videos falsos hechos con aprendizaje profundo. El ***aprendizaje profundo*** no es más que una pata de la **Inteligencia Artificial** y se refiere a un set de algoritmos que pueden aprender y ejecutar tareas complejas por sí mismos.

En el futuro se deberán crear mecanismos para la detección de estos videos, ya que se pueden realizar en tiempo real y son utilizados en programas de televisión. El uso de los deepfakes será utilizado como **arma,** dando como resultados el desconcierto y guerras dirigidas.

Un deepfake con la información mal intencionada puede causar una conmoción social activando una división social. Los especialistas en el tema, están creando softwares de detección con ayuda de IA para eliminar cada video subido en la web, es posible tener una idea general de cómo esta evolucionado de forma rápida y comprender como los atacantes utilizan esta herramienta para beneficios de terceros.

¿qué sucederá en el 2020?

Después de la divulgación de información realizada en meses pasados, en el 2020 se pronostica que pueden realizar un ataque más específico como es a los **datos biométricos** de cada usuario expuesto, dando como resultado la incrementación la **ilegalidad de la información personal con IA**.

Debemos prepararnos para cambiar nuestra ideología digital, ya que se presentarán más falsificaciones en cualquier ambiente o situación que se pueda mostrar la imagen o el video.

¿Podemos tener claro la realidad en la que vivimos vs la información que presenta las redes sociales?

[1] Open Democracy, cómo usar el porder de blockchain para combatir videos deepfake www.opendemocracy.net/es/democraciaabierta-es/c%C3%B3mo-usar-el-poder-de-blockchain-para-combatir-videos-deepfake/

NOTICIAS INFORMÁTICAS

GOOGLE Y XIAOMI SUSPENDEN INTEGRACIÓN DE SUS ASISTENTES

Dadas las vulnerabilidades de seguridad que están a la orden del día en este caso hablaremos de los problemas de seguridad entre las cámaras Xiaomi y los dispositivos de Google Nest.

Un usuario de Reddit Dio-V informó que al momento que él intentaba ver el vídeo captado desde su cámara **Xiaomi Mijia 1080p por medio de su Google Nest Hub** quedó sorprendido al ver imágenes que no eran de su domicilio.

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

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

Contacto:
underc0de.org/foro/profile/Lily24

El usuario, declaró que **adquirió su** cámara nueva mediante **AliExpress** y, así mismo horas después de salir a luz este suceso.

> ***Google informó:***
> *"Somos conscientes del problema y estamos en contacto con Xiaomi para trabajar en una solución. Mientras tanto, estamos deshabilitando[2] las integraciones de Xiaomi en nuestros dispositivos."*

> ***Xiaomi**: "Pedimos disculpas por las molestias."*

En un inicio y **como medida de seguridad, Google decidió poner un alto a la integración de los productos de Xiaomi** con el Asistente de Google y dispositivos compatibles.

Actualmente, **el Asistente no permite controlar los dispositivos domóticos de Xiaomi Mi Home ni es posible vincular nuevas cuentas**. Xiaomi, por su lado, ha emitido en un comunicado, "Xiaomi siempre ha priorizado la privacidad y la seguridad de la información de nuestros usuarios. Somos conscientes de que hubo un problema de recepción de imágenes fijas mientras se conectaba Mi Home Security Camera Basic 1080p al Google Home Hub. Pedimos disculpas por las molestias que esto ha causado a nuestros usuarios."

Fallo de seguridad

La falla de seguridad afecta a la cámara de seguridad **IP inteligente Xiaomi Mijia 1080p** que para su funcionamiento también es vinculada a una cuenta de Google para ser utilizada a con dispositivos Nest a través de la aplicación My Home de Xiaomi.

Xiaomi afirma que "su equipo ha actuado de inmediato para resolver el problema" y afirman que actualmente "ya está solucionado". Haciendo énfasis en que **este fallo de seguridad fue causado por una actualización de la caché el 26 de diciembre de 2019**, diseñada para perfeccionar calidad en transmisión de la cámara.

Informando que este fallo "sólo ha ocurrido en condiciones extremadamente raras" y que **"sólo" han encontrado a 1044 usuarios con este tipo de integraciones**. De esos 1044, sólo se vieron afectados los que tenían "una conexión pobre".

Xiaomi se ha comunicado y ha solucionado este problema con Google, y también ha suspendido este servicio hasta que la causa principal se haya resuelto completamente, para asegurar que estos problemas no vuelvan a ocurrir.

Cabe resaltar que ya son varias veces en las que cámaras de seguridad para el hogar dan este tipo de problema por lo cual debemos de tener el debido cuidado y mantener actualizado el firmware, cambiar las claves por defecto que traen los dispositivos y estar pendientes constantemente de cualquier anomalía que veamos para que la situación no llegue a salirse de control.

[2] SANTI ARAÚJO 3 Enero 2020 Google suspende la integración de Xiaomi con su asistente y Google Home tras un fallo que permitía ver casas ajenas, www.genbeta.com/actualidad/google-suspende-integracion-xiaomi-su-asistente-google-home-fallo-que-permitia-ver-casas-ajenas **Consultado**: 04/01/2020

CORS - PARTE I

HACKING/
PENTESTING

CORS (Cross Origin Resource Sharing) es un mecanismo que permite que una página web realice solicitudes a otro dominio que no sea el que sirvió la página.
Surge derivado de la necesidad de invocar recursos de otros dominios.

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

Apasionado de la seguridad informática y hacking ético, actualmente enfocado en Gestión de Seguridad Informática.

Contacto:
underc0de.org/foro/profile/yov4n

Same-origin policy

Esta política limita la capacidad de un sitio web de interactuar con recursos fuera del dominio origen, en respuesta a interacciones entre dominios potencialmente maliciosos.
En muchas ocasiones los sitios web interactúan con subdominios o sitios de terceros de tal forma que requieren un acceso completo de origen cruzado.

El protocolo implementa un conjunto de encabezados HTTP que permiten identificar orígenes web confiables.

vulnerabilidad de cors.

Muchos sitios webs requieren ***permitir el acceso a sus recursos desde subdominios*** u otros sitios web de terceros. La implementación de CORS puede ser demasiado permisiva o contener errores en su configuración.

explotación

La mala configuración de esta política podría permitirle a un atacante acceder a recursos sensibles del portal, la explotación de estas fallas en la configuración son del tipo **CSRF**.
El ataque es trasparente para la victima ya que se incluye código JavaScript en un portal controlado por el atacante, una vez que la víctima ingresa este envía la petición a la página vulnerable obteniendo información sensible como cookie de sesión, API Key, CSRF token, etc...

La forma de verificar si existe esta vulnerabilidad en una página es la siguiente:
Se envía una solicitud al portal **target.domain** intentando utilizar el archivo file.php desde el origen foo.bar

```
GET http://target.domain/file.php HTTP/1.1
Host: target.domain
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8;)
Gecko/20100101 Firefox/24.0
Accept: text/html
Accept-Language: en-US
Referer: http://foo.bar/
Origin: http://foo.bar/
Connection: keep-alive
```

Obteniendo la siguiente respuesta.

```
HTTP/1.1 200 OK
Date: Fri, 23 NOV 2018 18:57:53 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.4-14+deb7u3
Access-Control-Allow-Origin: *
Content-Length: 44
Keep-Alive: timeout=18, max=89
Connection: Keep-Alive
Content-Type: application/xml

[Response Body]
```

Se observa la cabecera Access-Control la cual contiene un '*' esto significa que desde cualquier dominio se puede acceder al archivo **file.php**, si este en la respuesta contiene información sensible pude ser utilizada por un atacante.

Esperen en la próxima edición

la segunda parte de este artículo.

CÓMO DEFENDERSE DE LA GEOLOCALIZACIÓN IP

SEGURIDAD INFORMÁTICA

La geolocalización IP es una de las formas más prolíficas de rastrear individuos. Geolocalización IP. Es la forma del siglo XXI de decirle a las empresas si conduces o cocinas espaguetis en el piso 14 de tu complejo de apartamentos. Parecería una broma, pero no lo es.

En el mundo de hoy, **las compañías de publicidad y redes sociales** más grandes utilizan esta función todos los días. La mayoría no te dice cómo evitarlo o cómo defenderte ante esto.

Escrito por: @MR.EBOLA | EN COLABORACIÓN CON **UNDERC0DE**

Cesar gusta de compartir sus conocimientos sobre Hacking ético y Blockchain, además de Tecnología y Emprendimiento, mediante su canal llamado HackWise con más de 168k suscriptores en YouTube.

Contacto:
Hackwise.mx
Redes Sociales:
TWITTER | INSTAGRAM | TELEGRAM: @mr.ebola

Incluso desactivando el servicio de ubicación en el teléfono no es suficiente. Por ello en este artículo les diremos como protegerse. Recientemente *The New York Times* investigó cuán detallado es el seguimiento de personas normales.

Siguiendo la vida de varias personas, descubrieron que las compañías de publicidad (gracias a su ID de anuncio) pudieron rastrear a una maestra. La rastrearon desde su casa, al trabajo, al almuerzo, yendo de clase en clase y cuánto tiempo estuvo atascada en el tráfico.

Sin embargo, con la Geolocalización de IP eso es solo la punta del iceberg. No mucha gente sabe, que si alguien obtiene **tu dirección IP.** En el peor de los casos, de tu computadora de escritorio o portátil, puede averiguar exactamente dónde vives. Independientemente de si tu IP está designada como "privada" o no. Estos servicios están disponibles para el público y absolutamente cualquier persona puede usarlos.

Formas de protegerte contra el seguimiento de la Geolocalización de IP personal

1. **Dejar de usar las redes sociales:** Esta es la mejor forma de salir casi de la red. Si nos damos cuenta de cuánto nos siguen las empresas de redes sociales y nuestra actividad, probablemente nos volveríamos paranoicos, caminando con un casco de papel de aluminio.
   Las redes sociales son las principales culpables del seguimiento y la mayoría de las empresas tienen lo que se llama un **período de retención**. Incluso Snapchat, sus imágenes no desaparecen inmediatamente de sus servidores.
   En el caso de que las fuerzas del orden público o las **agencias estatales o federales** necesiten información una persona, pueden obtener una orden judicial para conseguirla de dichas compañías, pero hay una trampa en eso:
   Cuando utilizan **Snapchat, Facebook y Gmail**, solo para nombrar algunos, de buena gana proporcionan la información solicitada a la empresa. Lo que significa: todo lo que la policía realmente necesita es... **preguntar**.
   Así es, al proporcionar dicha información a la compañía, en realidad, una orden es la forma correcta pero no es del todo necesaria, ya que la policía realmente la necesita de la compañía y no del usuario.

Se puede ver esto en la entrevista de Joe Rogan con Edward Snowden aquí: www.youtube.com/watch?v=KU-C0ImoIZc

2. **Jaulas de Faraday:** Para aquellos que son ingenieros eléctricos, ya saben de qué se trata. Una jaula de Faraday es una jaula de malla de alambre que repele la electricidad si llegase a golpear dicho dispositivo. Sin embargo, **en la actualidad, una jaula de Faraday es una bolsa**, funda o maletín que bloqueará completamente todas las señales hacia y desde un teléfono inteligente, computadora portátil, iPad o cualquier dispositivo.
   Cada señal, llámese **GPS, RFID, WiFi, Bluetooth, NFC**. Incluso la peor pesadilla de los Estados Unidos, EMP (*Pulso electromagnético*) estarán bloqueados siempre que el dispositivo esté en dicha bolsa.

Dentro de los próximos treinta segundos de haber puesto un teléfono en esta bolsa o funda, literalmente se *aísla del mundo*. Ahora debe tenerse en cuenta que por ejemplo los auriculares Bluetooth no funcionarán y no recibirá ninguna llamada. Sin embargo, se tiene la tranquilidad de no estar siendo rastreado.

3. **VPN:** Las Redes Privadas Virtuales, son una forma de ocultar anónimamente la dirección IP de sitios web y diferentes servicios que recopilan estos datos. Las VPN en realidad pueden hacer que parezca que se está navegando desde Alemania cuando en realidad estás en San Luis Potosí.
   Una de las VPN que tiene la mejor reputación en este momento es **NordVPN**. Permite ver Netflix con su servicio habilitado, esto no lo permiten otras VPN's o evadir la censura de Internet de un país.
   Probablemente surjan preguntas de: por qué deberíamos usar una VPN. Si consideran que el WiFi de restaurante o cafetería es seguro para iniciar sesión en sitios con su información personal, entonces probablemente necesites una VPN. Las VPN lo que hacen es proporcionar una **capa de seguridad cada vez** que usen una ***red Wi-Fi pública no segura***. La cantidad de puertas y exploits que un atacante puede usar cuando alguien está conectado a una red no segura es atroz.
   Por ejemplo, **MITM** (Man In The Middle), **Evil Twin** (Rogue Access Point), **Honeypot** (Red que parece legítima o hackeable pero es realmente utilizado para monitorear a la víctima).
   Asimismo, pueden ver/inyectar paquetes (inundando la computadora con "paquetes" para explotar las vulnerabilidades del sistema en un dispositivo). Las VPN también proporcionarán cierta privacidad adicional cuando se esté navegando por Internet. Agregando una capa de seguridad que a su vez ocultará el historial de navegación. No obstante, si un **analista forense** o estado-nación quisiera establecer la ubicación de un individuo, también podrían hacerlo, pero será mucho más difícil de obtener.

4. **Practicando COMSEC (comunicaciones seguras):** Es un método militar para estar y permanecer literalmente fuera de la red lo más humanamente posible. Estas son personas que, en lugar de usar iPhones y Samsung Galaxy, usan iPod Touch con Signal y WhatsApp para llamadas WiFi y solo las usan mientras están conectadas a redes Wifi a su alrededor. En el caso de aquellas personas que necesitan desaparecer. A menudo son periodistas de investigación, soldados de SPECOPS o personas que se supone que no existen. Suelen comprar cosas solo en efectivo para ocultar las compras de dispositivos, son completamente anónimas e imposibles de rastrear. Ahora, vivir una vida moderna mientras se practica *COMSEC* es extremadamente difícil de hacer y practicar; No es ideal para la mayoría de las personas. Sin embargo, si logran hacerlo con éxito, la Geolocalización de IP será un chiste para ellos. El COMSEC adecuado significa que no pueden ser rastreado … en absoluto.

conclusión

Para terminar, la Geolocalización de IP es una pesadilla e invade nuestras vidas todos los días. Si pueden desactivarla, apagarla y eliminarla. Pero, si no pueden y disfrutan de las redes sociales y compartir el estilo de vida, entonces es algo que nunca podrán lograr.

EASYTOTP 2FA PARA SERVIDORES DE SSH

SEGURIDAD INFORMÁTICA

Aprenderemos a desarrollar **un sistema de segundo factor de autenticación** para los servidores **SSH** que permita generar un One Time Password basado en tiempo.

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.

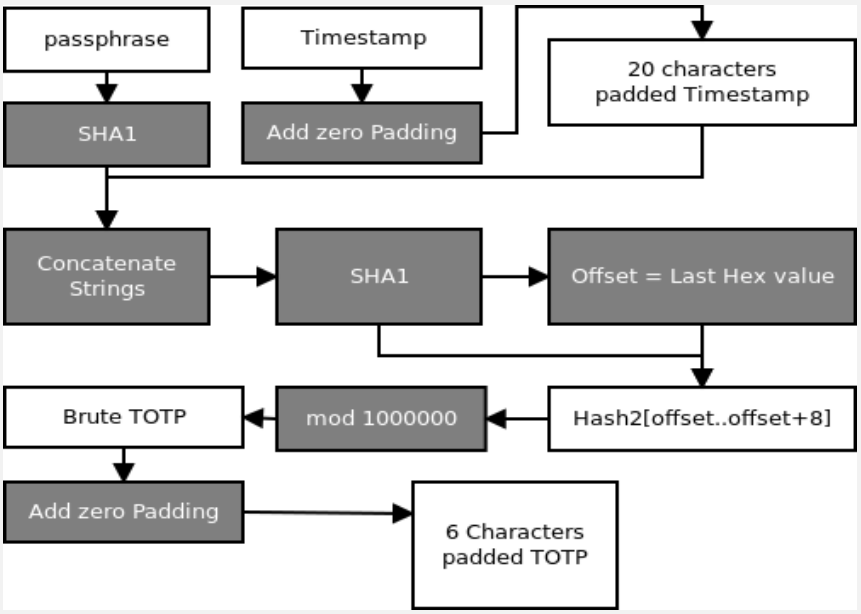
Contacto: underc0de.org/foro/profile/animanegra

Redes Sociales:

Github: github.com/4nimanegra

Trataremos un diseño sencillo de un *Time-based One Time Password* (***TOTP***) para la implantación de un segundo factor de autenticación en servidores de ***SSH***. Ofreciendo un algoritmo más sencillo, el diseño está basado en hashes de tipo ***SHA1*** en lugar del diseño original basado en una estructura basada en ***HMAC*** con la utilización interna de distintos hashes, (El más extendido es el ***SHA1***). Generando un sistema de ***TOTP*** fácil de implementar en cualquier lenguaje sin necesidad normalmente de librerías adicionales (En ***PHP***, ***BASH***, y otros lenguajes parecidos el hashing mediante ***SHA1*** son incluidos).

Para habilitar la autenticación de segundo factor en ***SSH*** utilizando una vía más sencilla por lo que una implementación de las librerías de ***PAM*** probablemente sea más segura. El algoritmo maneja (como en el caso original) dos entradas, una **passphrase** y un **timestamp**. El proceso queda completamente definido en la figura siguiente:



Realizando dos implementaciones, una dirigida al proceso de verificación programada en código ***C***, del lado del servidor ***SSH***. Esta implementación

- La primera deberá pedir el ***TOTP*** y verificar que el ***TOTP*** es correcto.
- La segunda basada en ***HTML/Javascript*** orientada a ejecutarse por parte del usuario que desea acceder al servidor ***SSH***.

El siguiente código es el encargado de efectuar la verificación devolviendo al sistema operativo una salida de error con valor 0 en caso de que la verificación sea correcta u otra salida de error en cualquier otro caso:

Código: C

```c
#include <stdint.h>
#include <stdio.h>
#include <openssl/sha.h>
#include <string.h>
#include <sys/time.h>
#include <stdlib.h>
#include <sys/mman.h>
#define LONG 1000000
#define TIME 30
int main(int argc, char *argv[]){
   mlockall(MCL_FUTURE|MCL_CURRENT); // prevent swapping memory
   FILE *f; // to disk
   uint8_t userpass[61], sha1[21], sha1aux[61], offset;
   uint8_t mytime[21], user[7], otpstring[7], i, ii;
   struct timeval timestamp;
   uint32_t otp=0;
   long int timeotp;
   if(argc == 2){
```

Tras compilar el código el binario debe moverse a la carpeta home del usuario o usuarios en los que se desee habilitar el **2FA** mediante **TOTP**:

```
gcc -o totp totp.c -lcrypto

cp totp ~/
```

También se deberá incorporar en un archivo llamado ***mysecrettotpfile.txt*** la passphrase que se desee utilizar para el ***TOTP*** y almacenarlo en la carpeta home del mismo usuario.
De cara a habilitar el ***TOTP*** en el ***SSH*** cada vez que se autentique el usuario se deberá generar un archivo llamado ***totp.sh*** con el siguiente contenido:

```
1.  if [ "$SSH_CONNECTION" != "" ]; then
2.     if [ "$SSH_ORIGINAL_COMMAND" == "" ]; then
3.        SSH_ORIGINAL_COMMAND=/bin/bash;
4.     fi;
5.     AUX=`echo $SSH_ORIGINAL_COMMAND | cut -f "1" -d " "`;
6.     if [ "$AUX" != "scp" ]; then
7.        ~/totp ~/mysecretotpfile.txt;
8.        if [ $? == 0 ]; then $SSH_ORIGINAL_COMMAND; fi;
9.        else if [ -e ~/scpenable ]; then
10.          $SSH_ORIGINAL_COMMAND; rm ~/scpenable;
11.    fi;fi;
12. fi;
```

Es necesario añadir las siguientes líneas al final del archivo de configuración del servidor ***SSH***, normalmente localizado en el archivo ***/etc/ssh/sshd_config***:

```
th User username

   AllowTcpForwarding no

   X11Forwarding no

   ForceCommand /home/username/totp.sh
```

Nótese que el **script** deshabilitará la posibilidad de realizar port forwarding utilizando este usuario y si se desea realizar alguna copia vía ***SCP*** se deberá generar en cada ocasión un archivo llamado ***scpenable*** en el directorio home del usuario dejará tener una verificación en dos pasos también cuando se realizan copias de archivos. Tras realizar el cambio en la configuración del servidor ***SSH*** será necesario su reseteo para que la configuración sea efectiva.
La implementación de programa de usuario que genera la password de un solo uso, se ha optado por una implementación mediante ***HTML/Javascript***. Este tipo de implementación permitirá una fácil importación del sistema a aplicación móvil mediante la utilización de ***Cordova*** o ***PhoneGap***.

Haciendo uso de la librería ***javascript Crypto-JS*** para el cálculo del ***SHA1*** disponible para su descarga mediante el repositorio ***NPM***.

Es de vital importancia para tener un ***2FA*** proporcionar una vía paralela de autenticación, que el programa cliente basado en ***HTML/Javascript*** se utilice en un dispositivo diferente al que se utilice para realizar el login en ***SSH***.

El código de implementación del sistema cliente es el siguiente:

Código: HTML5

```
<html>
   <script src="sha1-min.js"></script>
   <script>
      var data = localStorage.getItem("mypass");
      function newpass(){
      localStorage.setItem("mypass",userpass.value);
      data = localStorage.getItem("mypass");
      newotppass.style.visibility="hidden";
      otppass.style.visibility="";}
      function hideMe(){newotppass.style.visibility="";
      otppass.style.visibility="hidden";}
   </script>
   <body>
      <center>
         <div id="otppass">
            <div id="pass" size="64"></div><br>
            <button onClick="hideMe();">
            New Password</button>
         </div>
         <div id="newotppass">
            <input name="userpass" id="userpass"></input>
            <button onClick="newpass();">OK</button><br>
         </div>
      </center>
   </body>
   <script>
      if(data == null){
         newotppass.style.visibility="";
         otppass.style.visibility="hidden";
      }else{
         newotppass.style.visibility="hidden";
         otppass.style.visibility="";
      }
      function generate(){
         if(data != null){
            date = new Date();
            mypass=""+CryptoJS.SHA1(data);
            aux=""+Math.floor((date.getTime())/30000);
            while(aux.length < 20){aux="0"+aux;};
           mypass=""+CryptoJS.SHA1(mypass+aux);
           offset = parseInt(mypass[mypass.length-1],16)*2;
           otp="";
           for(i=0;i<8;i++){
              otp=otp+mypass[(offset+i)%mypass.length];}
           otp=""+(parseInt(otp,16)%Math.pow(10,6));
           while(otp.length < 6){otp="0"+otp;};
           pass.innerHTML=otp;}
        setTimeout(generate, 1000);}
     generate();</script></html>
```

Este código es exportable directamente a una aplicación móvil mediante ***Cordova*** o ***PhoneGAP***. De cara a realizar la exportación de la aplicación, por ejemplo, un ***APK*** de android.
El proceso empezaría por vincular el ***SDK*** de ***Android*** a ***Cordova***:

```
export PATH=$PATH:/home/user/Android/Sdk/platform-tools/

export PATH=$PATH:/home/user/Android/Sdk/tools/
```

Después generamos una aplicación de ***Cordova*** vacía para colocar nuestro código ***HTML/Javascript*** en ella:

```
cordova create TOTP com.TOTP TOTP

cd TOTP

cordova platform add android
```

Como vemos estamos dentro del directorio creado por ***Cordova*** para nuestra aplicación. Se borrará el contenido original del directorio ***www*** generado por ***Cordova*** y copiamos lo el archivo ***totp.html*** y ***sha1-min.js*** al directorio ***www*** con los nombres ***index.html*** y ***sha1-min.js*** respectivamente:

```
rm -fr ./www/*

cp /home/user/easyTOTP/src/totp.html ./www/index.html

cp /home/user/easyTOTP/src/min-sha1.js ./www/
```

Por último, le indicaremos a ***Cordova*** que genere el ***APK*** de la aplicación:

```
cordova build android
```

Una vez terminado el proceso de generación la aplicación ***APK*** se encuentra en el directorio:

```
platforms/android/app/build/outputs/apk/debug/app-debug.apk
```

Se copiará el ***APK*** en el móvil y se podrá utilizar la aplicación ***WEB*** como una aplicación ***stand-alone***.

RAMSOMWARE: EL MALWARE DE LA DÉCADA

SEGURIDAD INFORMÁTICA

El ransomware dejó de ser un **malware ignorado** gracias a **WannaCry,** provocando un cambio absoluto en **mayo del 2017** con una tasa de más de **300.000** ordenadores afectados en todo el mundo, acabado en los titulares por aniquilar instituciones tan importantes como el Sistema Nacional de Salud del Reino Unido.

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

Estudiante de Desarrollo de Software, apasionado por la seguridad informática y uso de herramientas OSINT.

Contacto:
underc0de.org/foro/profile/mrxvs
Redes Sociales:
Twitter: twitter.com/Elvis7Huerta

El ransomware[3] es un software malicioso, o malware, diseñado para negar el acceso a un sistema informático o datos hasta que se pague un rescate.

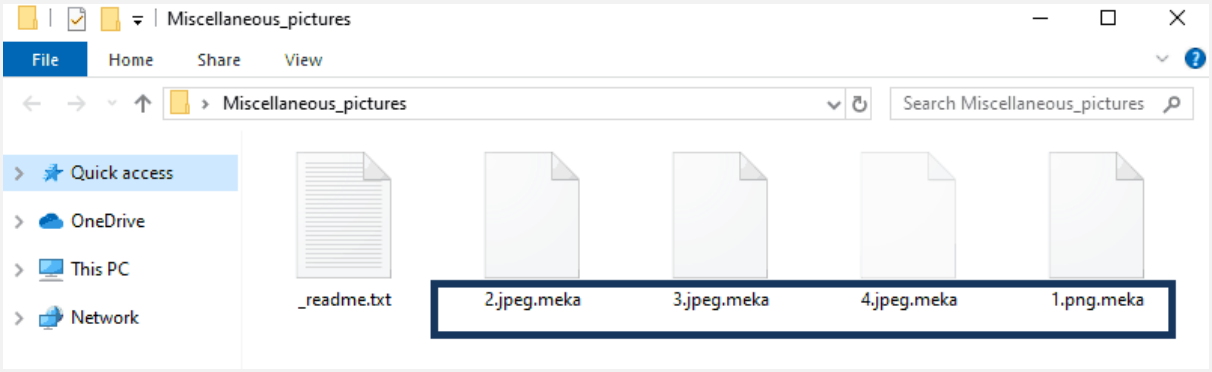
[3] **Departamento de Seguridad Nacional (CISA)** Ransomware, www.us-cert.gov/Ransomware, **Consultado:**26/11/2019

Tipos de Ransomware

- **Cifrado de archivos**

  Características

  - ✓ El malware elimina los archivos originales, después de cifrarlos.
  - ✓ Deja nota de rescate o en ocasiones muestra una pantalla de bloqueo.
  - ✓ Permite uso del dispositivo, es decir, uso del reproductor de música, video, navegación web.
  - ✓ Elimina los **shadow copy**, lo que dificulta la capacidad de recuperar los archivos.



Repositorio del ransomware de código abierto Hidden Tear
github.com/goliate/hidden-tear

- **Lock screen cryptowall (Virus de la policía)**

  Características

  - ✓ Bloquea el dispositivo y demanda un rescate mediante una imagen a pantalla completa.
  - ✓ Los archivos personales no son cifrados.
  - ✓ En algunos casos hacen uso de recursos del dispositivo como: micrófono, cámara web.
  - ✓ Aplicación de ingeniería social para obtener la dirección ip, datos personales e incluso fotografía de la víctima.

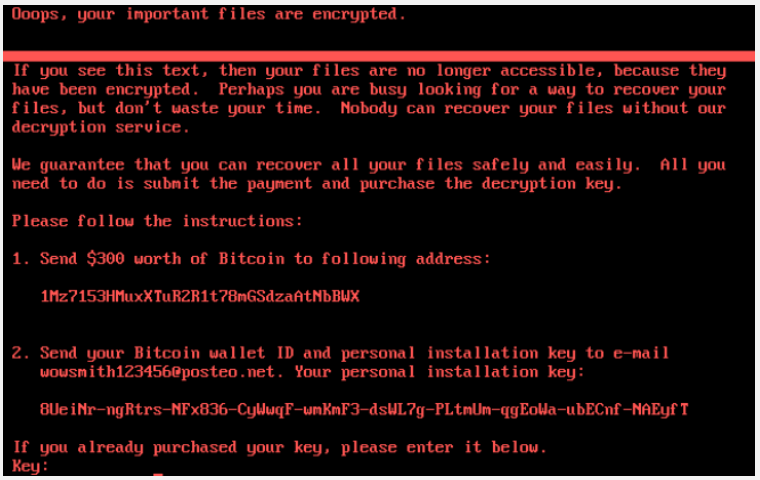
- **Master Boot record (MBR)**

El MBR es la parte del disco duro que permite al equipo que el sistema operativo arranque.

Características

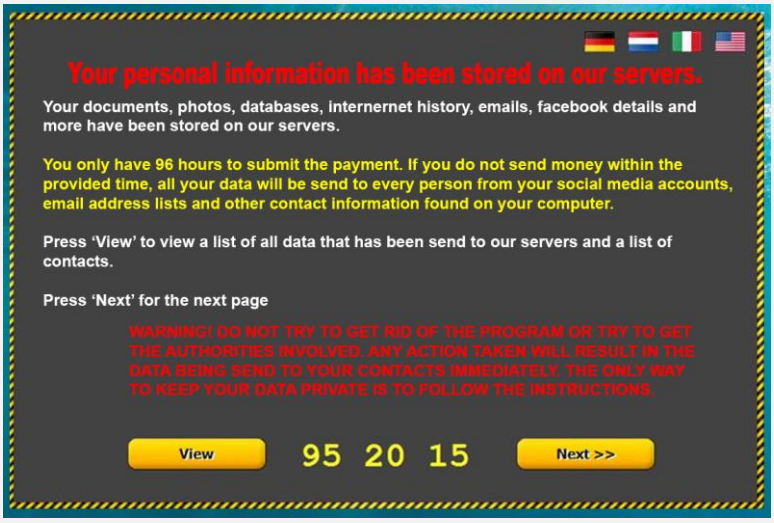
- ✓ Cifra los archivos mientras destruye los archivos originales.
- ✓ Cambia el sistema de arranque para que se interrumpa y en vez de arrancar el sistema operativo se visualice una demanda de rescate.

Los ransomware Petya y su versión mejorada NotPetya explotaba la vulnerabilidad CVE-2017-0145, su primera versión cifraba únicamente el sistema de arranque, pero debido a que fue solucionado rápidamente su sucesor comenzó a cifrar los archivos y el sistema de arranque.



- **Doxware**

Este realiza una copia de archivos personales y amenaza con liberarlos al público si el usuario no realiza un pago en determinado tiempo.



El ransomware busca tomar posesión de:

- Servidores
- Sitios web
- Dispositivos móviles
- Computadores
- Dispositivos IoT

Es decir, todos los dispositivos físicos que estén conectados a Internet, recolectando y compartiendo datos.

Por medio de diversos vectores de infección como son:

- Phishing
- Archivos Adjuntos
- Enlaces incrustados
- Descargas maliciosas
- Exploit kits.

Medidas de prevención[4]

- Realizar/Mantener copias de seguridad periódicas.
- Actualizaciones del Sistema con los últimos parches de seguridad.
- Activar firewall/cortafuegos correctamente configurado.
- Filtro anti spam a nivel del correo electrónico.
- Utilizar bloqueadores de JavaScript para el navegador.
- Mostrar las extensiones para tipos de ficheros conocidos.

[4] **Instituto de Ciberseguridad** Ransomware: Prevención y respuesta a incidentes, www.iciberseguridad.io, **Consultado:** 27/11/2019

SCRUM – METODOLOGÍA ÁGIL

QA ANALITICA WEB

Antes de mencionar las tareas de un QA, repasaremos que es Scrum. Existen muchas metodologías ágiles, **Scrum** es la más utilizada hoy en día.

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

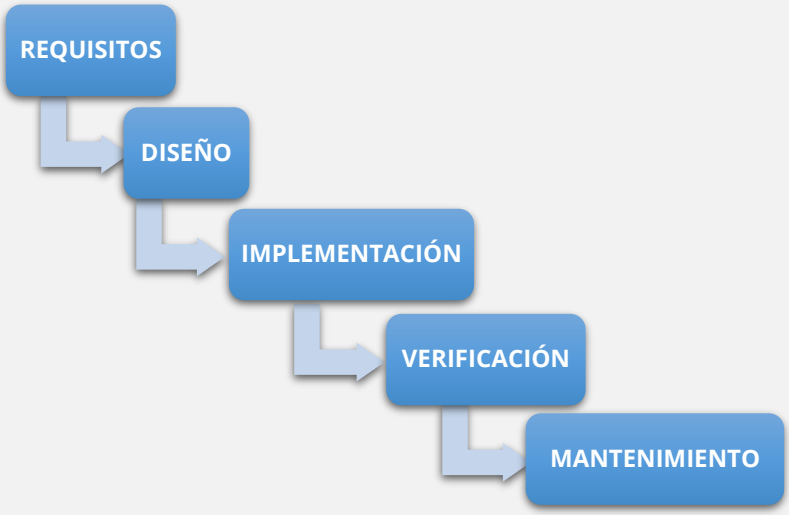
Trabaja actualmente como QA en dos empresas de software, controlando la calidad de los desarrollos que realizan, sometiéndolos a distintas pruebas, como lo es la seguridad. Participa activamente en la comunidad de Underc0de como administrador.

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

Las metodologías ágiles, son la evolución de las metodologías tradicionales, tales como la de cascada.

Para aquellos que no sepan lo que es, les dejo un gráfico representativo



Supongamos que un cliente llamado Carlos, tiene una tienda de computadoras y vende insumos informáticos. Carlos nos llama al teléfono y pide reunirse para que le desarrollemos un sistema de stock. En esta reunión, nos explica que necesita llevar un inventario de todos los insumos, clientes, proveedores y ventas de su negocio.

Con esta información, ya tenemos los **Requisitos** del sistema, que es el primer paso del gráfico anterior.

Llegamos a nuestra casa, y diseñamos en papel como debería ser el sistema. En el papel escribimos que será un sistema web, en donde al ingresar a la URL de su negocio se topará con un panel de login, podrá visualizar un menú con cada uno de los módulos. En el módulo de productos podrá dar de alta sus insumos y al realizar una venta, descontará automáticamente el stock... Y así con cada una de los módulos a desarrollar **(Etapa de diseño)**

Una vez que ya tenemos en mente cómo será la plataforma, comenzamos a desarrollarla... **(Etapa de implementación).**

Después de 3 largos meses de desarrollo, logramos tener todo lo que nuestro cliente Carlos nos pidió **(Etapa de verificación)**.

Regresamos victoriosos a su tienda, ansiosos de cobrar el dinero por la plataforma y al enseñar el sistema, Carlos comenta que es muy distinto a lo que él quería realmente.

Pues se imaginaba otros colores distintos a los que pusimos en su sistema, al formulario del inventario le faltan campos como el del código de producto, el precio de costo y que automáticamente calcule un precio de venta, entre varias otras cosas más.

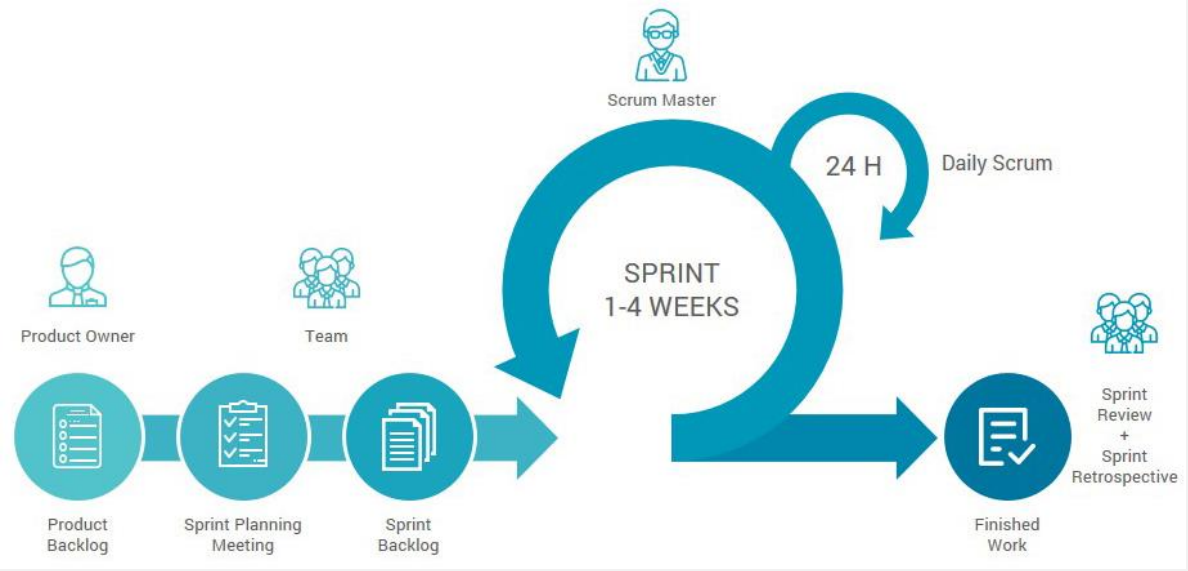
Teniendo estos nuevos requisitos, volvemos a nuestra casa y nos situamos nuevamente encima de la cascada para volver a comenzar. Y esto no quiere decir que la próxima presentación quede todo solucionado, sino que corremos riesgos de que vuelva a pasar lo mismo.

Seguramente dirán... ¿Qué tiene que ver todo esto con SCRUM?

La respuesta es fácil. Hubiésemos utilizado alguna metodología ágil como lo es SCRUM, nos ahorrábamos esas ida y vuelta.

Pero… ¿cómo funciona Scrum?

Para entenderlo de forma fácil, lo veremos mediante una imagen característica de esta metodología.



Una imagen en inglés a propósito, ya que son los términos que se suelen utilizar en las empresas de software.

Otra cosa a tener en cuenta, es que esta metodología se usa cuando trabajamos con equipos de trabajos y ahora veremos por qué.

Product Owner (Dueño del producto) nos da los requerimientos del sistema que debemos realizar (Product Backlog).

Seguido a esto, separamos las tareas que podemos realizar en un lapso de 1 a 4 semanas. (Este ciclo se define antes de arrancar el proyecto). Supongamos que los ciclos o sprints son de 2 semanas, entonces en la **Planning Meeting** debemos tomar tareas que nos lleven 2 semanas o menos y esas tareas son colocadas en el **Sprint Backlog**.

Por ejemplo, en el primer sprint (primeras 2 semanas), haremos el Login y el módulo de productos. Al siguiente sprint (sprint 2), haremos el módulo de clientes, y así con todos los módulos. El orden de desarrollo, suele ser por prioridad. Esto quiere decir que, si desarrollamos primero el login y el módulo de productos, el dueño del negocio podrá utilizar la plataforma mientras desarrollamos el resto de los módulos.

Una vez que ya está todo definido en el **Sprint Backlog** (3er forma en la imagen), comienza el ciclo de desarrollo. Si prestan atención, por fuera del círculo del sprint, hay otro más chico que dice «**Daily Scrum**», también conocido como «**Daily Meeting**» o «**Stand Up Meeting**», esto es una reunión diaria que se tiene con todos los miembros del equipo, y debe ser sumamente corta, lo suficiente como para poderla tener de pie, de ahí viene el «Stand Up Meeting». En esta reunión, que suele ser al principio de cada día, debemos responden las siguientes preguntas:

1. **¿Qué hice ayer?**
2. **¿Qué estoy haciendo ahora?**
3. **¿Estoy bloqueado con algo?**

Ejemplo:

- Ayer comencé con el diseño del login.
- Hoy voy a finalizar toda la interface del login.
- Estoy bloqueado para hacer el backend porque mi compañero aún no termina de crear las tablas en la base de datos del login.

Si prestamos atención, sale una figura en la imagen llamada **Scrum Master**, esta persona es la encargada de solucionar los problemas o bloqueos que podamos tener. En este caso, hablaría con esa persona que está atrasada y vería cual es el motivo, o intentaría ayudarlo para que avance más rápido y así desbloquear a su compañero. De no tener ningún problema, solo mencionar que no está bloqueado con nada y le pasan la voz a su compañero para que informe su status.

Una vez finalizadas las 2 semanas de desarrollo, se presenta una **DEMO** al cliente para que vea lo desarrollado. Lo bueno de esto, es que si tiene algún comentario, ejemplo colores, formas, posiciones, etc. Las puede mencionar y no solo se arregla en lo que ya está hecho, sino que se tiene en cuenta para el resto de los módulos.

Por último, podemos ver 2 figuras más en la imagen como el Sprint Review y Retrospective, básicamente en estas reuniones se suelen mencionar que cosas salieron bien y que cosas salieron mal durante ese sprint para aplicarlo o corregirlo en el siguiente.

Ya sabemos que es Scrum, ¿En dónde entran los QA?

Podemos decir que en el QA está presente en todo el proceso del desarrollo. Cuando el cliente define el backlog, debemos ayudarlo a pasar todos los requerimientos a un issue tracker y asegurarnos de que quede todo lo suficientemente claro como para que luego los desarrolladores puedan leerlos y comenzar a programar sin problemas.

Mientras los programadores se encuentran en fase de desarrollo, los QA tenemos que comenzar a escribir los casos de prueba y a organizar nuestras suites para luego someter a esa plataforma a los diferentes tests que preparemos.

> *Aunque hay que aclarar que todo esto que he redactado es en base a mi experiencia personal.*

SCRUM es una metodología **muy flexible**, puede que tenga más reuniones que solo son necesarias en ciertos proyectos. El gráfico visto en este artículo, es lo más común de ver en las empresas de software factory.


<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

¿POR DONDÉ COMENZAR?, PARA SER UN QA

QA ANALITICA WEB

Siguiendo la temática orientada a quienes desean iniciarse como **QAs**, este articulo ayudara a responder esta pregunta que suelen hacer bastante seguido.

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

Para comenzar...

Vamos a empezar explicando lo que es un **BUG**, que puede ser nuestro aliado o enemigo.

Un **bug**, es básicamente un error (comportamiento no esperado, error visual, entre otros)

¿Cómo distinguir si es un enemigo o un aliado?

Una de las formas de saber si estamos haciendo bien nuestro trabajo, es porque estamos encontrando errores en una plataforma. Y se puede decir que se trata de un enemigo, porque mientras más errores tenga una plataforma, más tiempo tardaremos en salir a producción.

Para entender mejor el tema, vamos a poner el siguiente ejemplo.

Tenemos un sistema de **Stock**, en dicho sistema, tenemos un CRUD de productos, en donde podemos crear, editar, eliminar y ver los items cargados.

Nuestra tarea como **QAs**, es probar cada campo, cada función, de hecho, hasta todo lo visual que podamos llegar a notar en la pantalla que estamos testeando.

Supongamos que estamos dando de alta un producto y que los campos son:

- **Título**
- **Cantidad**
- **Precio**

Podemos probar cosas como:

- **Título:** Caracteres especiales, colocar más de 500 caracteres, dejarlo vacío, etc.
- **Cantidad:** Colocar un número muy grande, número negativo, número con decimales, letras, etc.
- **Precio:** Ingresar letras, números negativos, caracteres especiales, etc.

La idea, es intentar romper la aplicación como sea, si el campo es de cantidad, no tiene sentido que se ingresen letras.

> *Parece un poco obvio, pero no se dan idea de la cantidad de errores así que se encuentran en las aplicaciones.*
> *Muchas veces por apurarse, los desarrolladores olvidan poner validaciones en los campos.*

Bien... ya sabemos que es un bug... ¿y ahora qué hacemos?

Esto varía mucho dependiendo del proyecto en el que estemos trabajando, los tiempos que tengamos y demás. Pero suponiendo que es un mundo feliz, en donde el **testing** inicia junto con el proyecto, es decir, que el desarrollo este comenzando junto con nuestro testing, entonces se comienza creando un **plan de pruebas (test plan)** con **casos de pruebas (test cases)**. Esto tiene como ventaja generar una documentación de que alcance tiene el testing y sobre qué cosas se prueban y que no.

En caso de que el proyecto ya esté desarrollado y necesitan un test en un corto lapso de tiempo, se puede optar por otras estrategias de testing, como por ejemplo un testing exploratorio. Que consiste en navegar la aplicación en busca de errores. La desventaja aquí, es que no tenemos como documentar lo que hemos probado y lo que no.

¡Encontramos un bug!

¿Con qué se come?

En todo proceso de desarrollo de software, es necesario contar con **un issue tracker (Redmine, Jira, etc)**

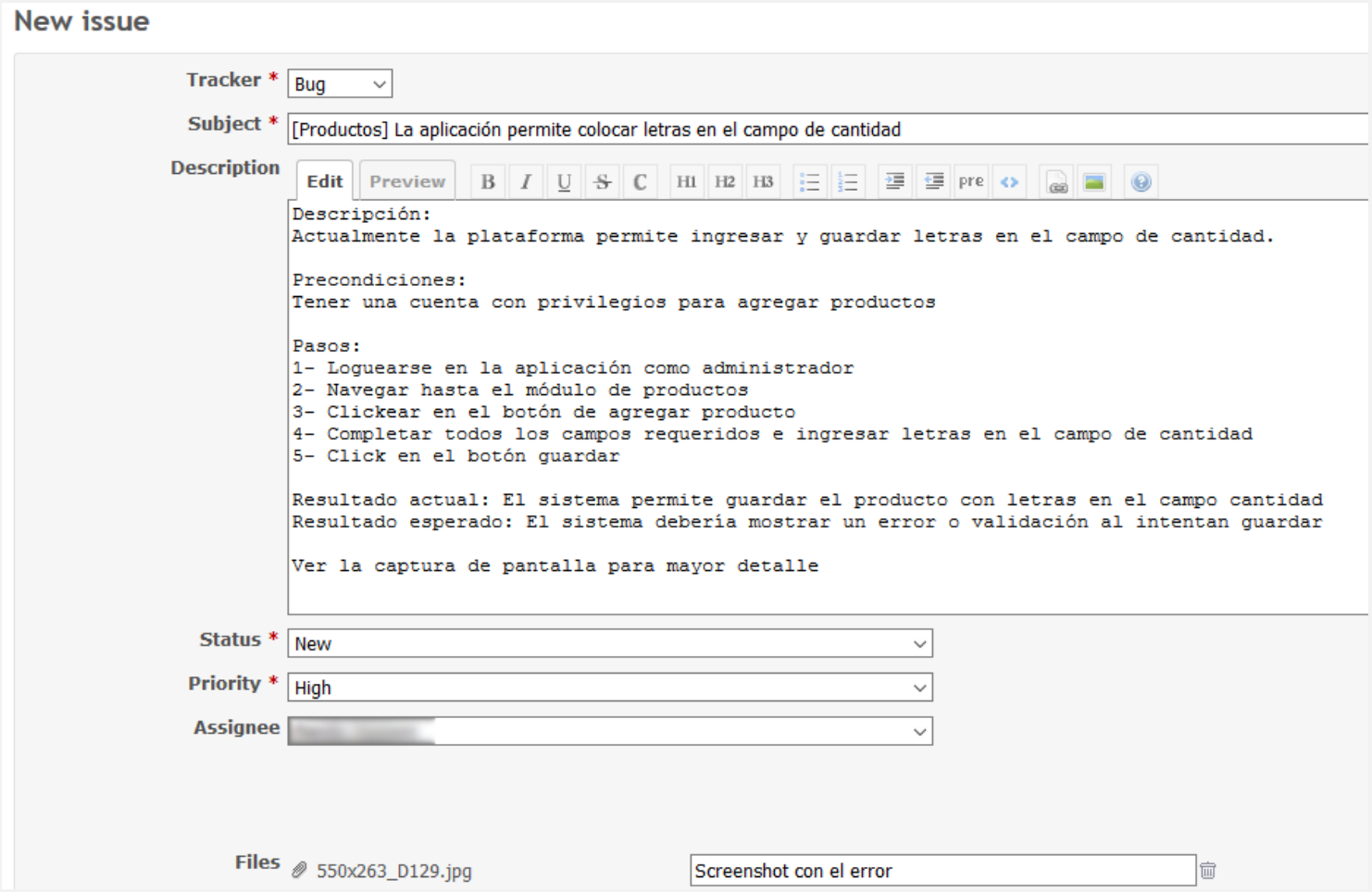
Los issues trackers no solo sirven para documentar las funcionalidades de la aplicación, sino también para reportar cada bug que encontremos.

Al reportar un error, debemos ser lo más claros posibles a la hora de reportarlo, es decir, debemos documentar bien qué tipo de bug es, pasos para reproducirlo, etc.

A continuación, compartiremos una plantilla para utilizar a la hora de reportar un bug:

- **ID #:** ID único de cada bug. Los issue tracker los colocan de forma automática
- **Título:** Título descriptivo. Es recomendable colocarlo entre corchetes el nombre del módulo que posee el error
- **Descripción:** Una breve descripción sobre el error encontrado
- **Precondiciones:** Si es necesario tener ciertos accesos o permisos para poder reproducir el bug
- **Pasos para reproducirlo:** Detalle paso a paso de que acciones deben realizar para reproducir el bug
- **Resultado Actual:** Explicar que está pasando actualmente
- **Resultado Esperado:** Explicar cómo debería funcionar
- **Screenshot/Video:** Alguna captura de pantalla o video mostrando el error
- **Prioridad:** Que tipo de prioridad tiene este issue
- **Asignación:** Asignarle el issue al desarrollador que hizo esa funcionalidad

ejemplo con redmine:



Esto es todo lo que necesitan saber por ahora sobre bugs y como reportarlos. Esperen un próximo artículo sobre más ***metodologías o estrategias de testing*** *y poco a poco iremos encadenando los conceptos.*

CAMINO A UN FUTURO SIN CONTRASEÑAS

PRIVACIDAD

Evidentemente las **contraseñas** un elemento imprescindible en nuestra vida digital, es decir casi todas las plataformas requieren de crear una cuenta para poder hacer uso de dicho servicio y de esta manera proteger mediante contraseñas nuestros datos registrados en ella.

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

Cuando internet estaba en sus comienzos, resultaba útil la protección mediante claves sencillas, pero ahora la información se ha convertido en un **activo muy valioso**, por lo que la seguridad convencional ya no es suficiente. Ahora es necesario recurrir a otros métodos para lograr hacer frente a la situación actual.

Si hacemos el recuento de ¿En cuántos sitios/servicios estamos registrados?, es difícil recordar con claridad cuál fue el correo y contraseña de dicha plataforma, es decir en más de 1 sitio tenemos que utilizar la opción "He olvidado mi contraseña" y de esta manera realizar la acción para recibir un código vía e-mail o SMS, así cambiar la contraseña o recuperarla, en otras ocasiones cuesta recordar el e-mail que se utilizó, volviéndose un verdadero dolor de cabeza recuperar nuestra cuenta, aquí es donde muchos usuarios prefieren reutilizar contraseñas en sus distintos servicios o crear contraseñas débiles pero sencillas de recordar.

O sea, todo esto ciertamente rompe con la función para qué fue creado el uso de contraseñas, al ser vulnerables/débiles, perdiendo el propósito de proteger a los usuarios contra ciber amenazas.
Han surgido alternativas como:

- **Autenticación de múltiples factores:** la cual exige verificación de dos modos distintos, notificando que alguien está tratando de ingresar a una cuenta, solicitando confirmar si se trata del dueño de la cuenta, constando de 3 elementos:
  1. Datos registrados (contraseñas, preguntas de seguridad)
  2. Alternativas para confirmar (correo, aplicación, dispositivos)
  3. Identificación (biométrico o voz)

Suponiendo que uno de los elementos del punto 2 cae en manos equivocadas, en cuestión de tiempo para que el ciberdelincuente puede lograr obtener el punto 1, por tal razón muchas iniciativas están trabajando por diseñar sitios que funcionen o pidan también el punto 3, es decir, que soliciten confirmar identidad, asegurando la exclusividad del registro/uso de cuentas.

Passwordless

Es un movimiento donde se han unido una gran cantidad de iniciativas, con el objetivo de hacer que el futuro de la tecnología no dependa de las contraseñas. Dándose a la tarea de crear nuevos métodos para mantener la comodidad de las cuentas/suscripciones, sin tener que crear una nueva contraseña.
Los sistemas ***passwordless***[5] se basan en el uso de **criptografía asimétrica** o de **clave pública** similar al utilizado en la firma digital. El usuario tendrá dos claves, una **pública** y otra **privada**, las cuales serán usadas para realizar la autenticación en el servicio.

La clave privada será almacenada en el dispositivo de forma segura junto a varios identificadores necesarios para saber a qué servicio pertenece. La clave privada únicamente será accesible si se está en posesión del mecanismo de seguridad elegido en el proceso de registro que puede ser un código PIN, biometría como huella dactilar o reconocimiento facial, voz, *token* físico, etc. **La clave pública** será enviada al servidor y vinculada con la cuenta del usuario**.**

Actualmente existen tecnologías que permiten prescindir de las contraseñas, aunque algunos consideran que hacer esos cambios resultará demasiado costoso.

Saliendo a relucir si es muy tedioso el ingresar a un sitio/servicio, habrá usuarios que dejarán de visitar o acceder, lo contrario sucedería utilizando sistemas de identificación sin contraseñas, logrando un acceso más sencillo y rápido.

[5] Passwordless el comienzo del fin de las contraseñas www.incibe.es/protege-tu-empresa/blog/passwordless-el-comienzo-del-fin-las-contrasenas, **Consultado:** 28/12/2019.

webauthn[6]

En mayo 2019 el World Wide Web Consortium (W3C) aprobó el **WebAuthn**, un estándar de autenticación que busca reemplazar el uso de contraseñas en un futuro cercano. Ya es soportado por los navegadores más importantes **como Chrome, Firefox, Edge y Safari**, el hecho de que ahora sea aceptado como un estándar de red permitirá una mayor adopción entre los diversos sitios de internet.

La **API** de **WebAuthn** aprueba a los sitios web comunicarse con algún dispositivo de seguridad FIDO para permitir/denegar el acceso, mediante dispositivos USB keys o algunos más avanzados en combinación con un lector biométrico, haciendo el acceso técnicamente más complejo, pero de uso más sencillo para los usuarios. Otro paso importante en la adopción de este estándar es que Android anunció que todos sus dispositivos capaces de correr su sistema operativo en la versión 7.0 o superior, estarán certificados con FIDO2, lo cual hace más sencillo el uso de **WebAuthn** al no ser necesaria la adopción de más hardware para poder utilizarlo, simplemente se requerirá de un celular certificado. Algunos portales que ya soportan esta tecnología son:

- Google
- Microsoft
- Dropbox

Cómo con toda nueva tecnología, un cambio a veces resulta un tanto complicado de realizar, existirá una gran cantidad de retos durante su adopción, después de todo es más sencillo cambiar una contraseña que cambiar la identidad física en la eventualidad de que un sistema biométrico logre ser hackeado.

Los beneficios no solo resultan ser para los usuarios, sino también las empresas ya que contarán con sistemas de seguridad más complejos, previniendo futuros problemas de robo de datos, aunque el proceso aún está en sus primeros pasos, existen plataformas y desarrolladores que desean implementar esta alternativa, por lo que dentro de poco las contraseñas estarán pasando al baúl de los recuerdos de mundo tecnológico donde la única constante es el cambio.

Camino a un futuro sin contraseñas, es momento de abrir nuestra mentalidad hacia la ***era del passwordless***, un nuevo sistema de autenticación más ágil, seguro y eficiente.

[6] **DEMO WebAuthn** https://webauthn.org/

CHEAT-SHEET 1: GNU/LINUX

Comandos fundamentales para la operación del sistema operativo Liinux. Hay desde comandos simples hasta aquellos que ejecutan funciones más complejas.
Linux incluye una gran cantidad de comandos, aquí los más importantes y habituales.

LS
Este comando lista los ficheros y directorios (Recordemos que en GNU/Linux todo es un fichero).
Ejemplo:
```
ls /home
```
Si queremos que nos muestre la información ampliada y en columnas, utilizaremos el parámetro '-l', y si además queremos que nos muestre los elementos ocultos, usaremos 'ls -la /home'

CD
Con este comando nos desplazarémos entre diferentes directorios. Si nos queremos ir a un directorio el particular:
Ejemplo:
```
cd /var/cache
```
Si en cambio nos encontramos en un directorio, y queremos pasar al inmediatamente superior:
```
cd ..
```
O ir directamente a otro directorio que esta al mismo nivel que el nuestro:
```
cd ../log
```

MKDIR
Hablando de directorios, con este comando podemos crear los que deseemos, como si no hubiera un mañana.
Ejemplo:
```
mkdir LaLigaDeLaJusticia
mkdir LaLigaDeLaJusticia/Batman
```

RMDIR
Podemos borrar del mapa un directorio.
Ejemplo:
```
rmdir /LaLigaDeLaJustica/GreenLantern
#(Ejecutando ese comando se ha eliminando ese directorio)
```

TOUCH
Con este comando es posible crear ficheros.
Ejemplo:
```
touch fichero1 fichero2 fichero3
```

RM
Al igual que con touch podemos crear nuevos ficheros, con rm, su contrario, podemos eliminarlos por completo.
Es primo hermano del comando 'rmdir', pero en este caso borra ficheros en vez de directorios.
Ejemplo:
```
rm lunes.txt
```
Un comando un poco preguntón, si se desea se dedique a eliminar sin mala conciencia, sólo debemos añadir el parámetro '-f', y si además se desea que elimine ficheros y subdirectorios, con '-r', será más que suficiente. Un "rm -rf"
Nota: Utilizar este comando con esos parámetros son bajo su responsabilidad.

MV
Sirve para mover un fichero o un directorio de lugar,para cambiar el nombre de un fichero.
Ejemplo:
```
mv /facturas/porpagar/factura1.pdf /facturas/yapagadas/
```
O bien:
```
mv /Avengers/PeterParker.jpg /Avengers/Spider-Man.jpg
```

RENAME: Cambia el nombre de un fichero o conjunto de ficheros. Tiene muchos parámetros interesantes.
Ejemplo:
```
rename 's/.jpeg/.jpg/' *
```
De esta manera indicamos que en la ubicación se cambiarán todas los ficheros con extensión "jpeg" por "jpg".

MAN: Podemos consultar el manual, de ahí que se llame "man". Si lo utilizamos seguido del comando a consultar, nos mostrará su entrada en el manual.
Ejemplo: `man touch`

INFO: Es un comando similar al de 'man' con información ampliada sobre el comando a consultar.
Ejemplo: `info touch`

WHATIS: Un comando poco conocido, muy útil. Se encarga de buscar el contenido de la palabra indicada, en una BD propia, que contiene breves descripciones de los comandos.
Ejemplo:
```
[jorge@servcentos1 ~]$ whatis man
man (1)              - una interfaz de los manuales de referencia electrónicos
```

CLEAR: Se encarga de borrar la pantalla. No hace mucho más. Para utilizar solo debemos de escribir '`clear`'.

SUDO: Con este comando nos podemos otorgar los poderes de **super usuario**, siempre que tengamos permisos para ello.
Ejemplo:
```
# make install pastel
¡No tienes permisos!
#sudo make install pastel
¡No te olvides apagar el horno!
```

HISTORY: Uno de los comandos, que sobre todo al principio, se utilizará más a menudo. Se encarga de mostrar un historial de todos los comandos que han sido utilizado.

PWD: Nos muestra el nombre del directorio de trabajo actual.
Ejemplo:
```
[jorge@servcentos1 ~]$ pwd
/home/jorge
```

CAT: Muestra el contenido de un fichero dado. Si se utiliza con varios ficheros a la vez, mostrará su contenido de manera secuencial.
Ejemplo:
```
cat GuiaDelAutoestopistaGalactico-CopiaLegal-eh.txt
```

CHMOD: Se encarga de cambiar los permisos de acceso a los ficheros.

CHOWN: Cambia el usuario y grupo propietarios de ficheros.
Ejemplo:
```
chown jorge:familia fotos-de-vacaciones.tar.gz
```

FIND: Busca un directorio o ficheros específico en el sistema de ficheros. Tiene un larga lista de opciones.

LOCATE: Similar al comando '`find`', se encarga de buscar en el todo el sistema, ficheros o directorios que coincidan con una consulta. Por default busca únicamente en los ficheros que tiene permisos. A diferencia de 'find' tiene su propia BD de consulta.

WGET: Descarga el fichero o página web dada, indicando la URL.
Ejemplo:
```
wget http://ejemplo.com/programa.tar.gz
```

Reto 9no. aniversario

Estamos muy contentos y agradecidos con todos los que interactúan, rompen el hielo y se animan a participar en nuestros retos, con la única intención de investigar, poner a prueba sus conocimientos y desafiarse a ustedes mismos yendo más allá de una competencia, la motivación de crear retos en la comunidad es animarlos a probar y seguir buscando más desafíos.

Sin más que agradecimiento infinito hacia toda la comunidad por ayudar a que sigamos creciendo, aprendiendo, compartiendo y evolucionando juntos.

PARTICIPANTES:

- MIGUEL ALONSO
- LIO54
- BENGALA
- OSCAR
- GODWITHUS
- ANIMANEGRA

niveles de desarrolladores

JUNIOR

- Necesita supervisión.
- Conocimientos básicos.
- Colabora en la planificación del proyecto.
- Trabaja en funciones y herramientas internas de software.

SEMI - JR

- Capacidad técnica de realizar tareas con menos supervisión.
- Conoce las etapas del desarrollo (análisis, desarrollo, prueba, implementación, documentación, etc.)
- Configura un ambiente de desarrollo.
- Detecta errores de código, haciéndolo más eficiente.
- Crea y escribe pruebas unitarias simples.

SENIOR

- Es capaz de supervisar y dirigir equipos.
- Comprende el alcance de un proyecto y plantea métodos para desarrollar, probar, implementar y mantener el proyecto.
- Asesora a desarrolladores junior y semi junior.
- Hace revisiones periódicas de código.
- Mejora la calidad y estructura del código.

@DENISSE

ENERO 2020

WireSpy

Automatiza varios ataques WiFi Man-In-The-Middle, mediante la configuración rápida de Honeypots para llevarlos a cabo.
Entre sus funciones se encuentran monitoreo y registro de las actividades de las víctimas.
Permite la integración de otras herramientas para realizar ataques más avanzados.

SOURCE:
GITHUB.COM/ARESS31/WIRESPY

TOOLBOXUC

01 HACKING NEW YEAR.
05 NOVENO ANIVERSARIO DE NUESTRA COMUNIDAD.

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	31	

UNDERC0DE.ORG

mensajes / opiniones de nuestros usuarios

"A por muchos años más...

SADFUD
VÍA FORO UNDERC0DE

"Con gran alegría un año más, un gran honor pertenecer al Staff y ser parte de esta hermosa comunidad. A cada uno infinitas gracias por el empeño y dedicación. ¡Hail Underc0de!

DRAGORA
VÍA GRUPO 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

"Por muchos más años. Y que la comunidad siga creciendo. Salud.

NOXONSOFTWARES
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

"Felicitaciones por el tremendo trabajo Staff y por la grata comunidad en la cual nos permiten desarrollarnos. Feliz aniversario #9 Underc0de.

DEBOBIPRO
VÍA GRUPO UNDERC0DE

"Felicidades al equipo en realidad me hacen el día, son muy buenos chicos con proyectos increíbles, espero cuando ya esté más experimentado pueda ayudarles.

ARTURO CHAVOOLLA
VÍA PÁGINA DE FACEBOOK UNDERC0DE

"Enhorabuena, no es fácil aguantar tantos años on-line.

KIKE RAMÓN
VÍA PÁGINA DE FACEBOOK UNDERC0DE

"Muchas Felicidades Underc0de!!! por su 9no aniversario, es un gran foro de mucha ayuda y apoyo en los temas de la seguridad informática. Así mismo igualmente a todos los integrantes que tengan felices fiestas. happy Hacking!

LIO54
VÍA FORO UNDERC0DE

"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.