The deep web; los suburbios de Internet

Cuando hablamos de la Internet profunda, hablamos a vez de un espacio mas libre, mas abierto pero no tan neutral como la Internet comercial que todas conocemos. Dicen las malas lenguas que en este espacio podremos encontrar sicarios a sueldo, venta directa de drogas, armas..., todo lo que la común mente podría tachar de deleznable. Aunque la teoria conspiraoíca suene a ciencia ficción, hay veces en que las malas lenguas no están demasiado alejadas de la realidad.

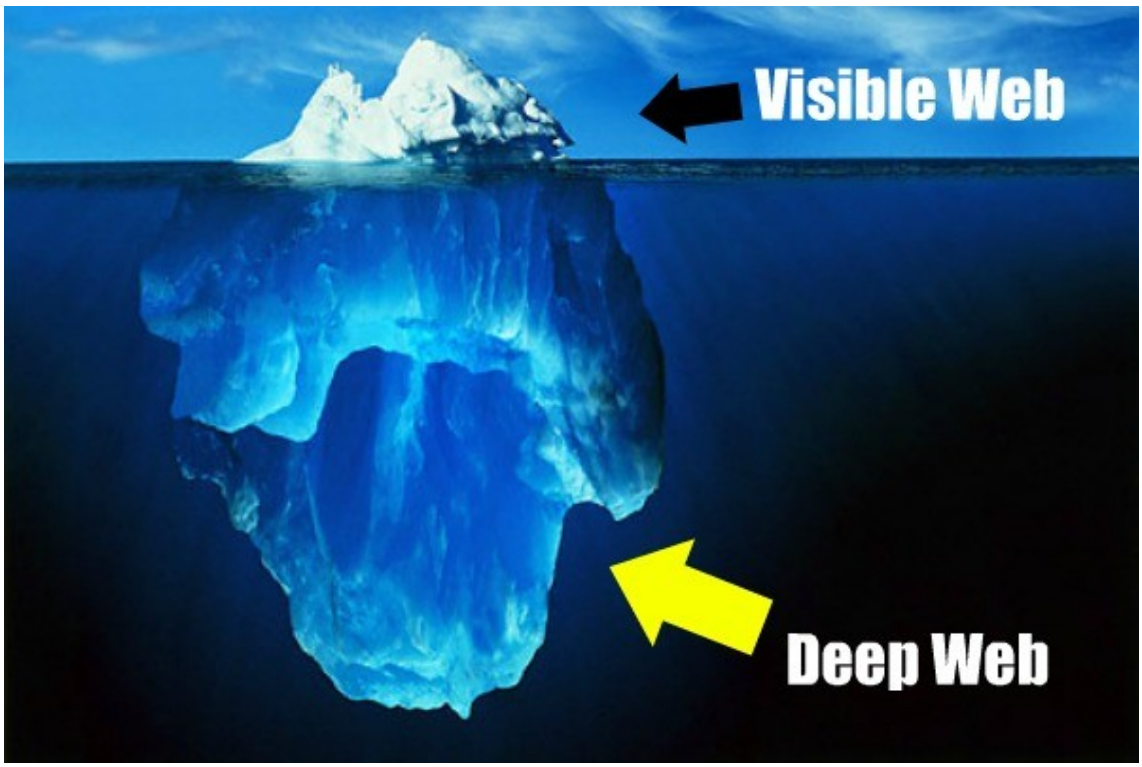
> *Cuando miras al abismo, el abismo también te mira a ti.*
>
> *Nietzsche*

Deep Web, ¿mito o realidad?

Lejos de las posibles conspiraciones cibernéticas, centrarmos el artículo en las posibilidades reales y positivas de la *Deep Web*.

La *deep web* o Internet profunda son redes que escapan a los buscadores mas conocidos de la superficie, de ahí su nombre. Sus paginas, manuales, documentos..., no estan indexados y necesitamos usar programas específicos para poder acceder a ellas. Son las bases de datos no indexadas, son redes que no quieren mantener comunicación con la Internet común, son las entrañas de la red, los suburbios. No se trata de un dogma de fe, algo supuesto e intangible; ¡en el 2000 se hablaba de 7.500 TeraBytes de información! ¿Impresionados? Bien. Pues sabed que la Universidad de Berkeley, California, estima que actualmente la Internet Profunda debe tener unos 91.000 TeraBytes.

Tal vez la forma más sencilla, aunque poco original de explicar este fenómeno, sea el iceberg. Es un excelente símil; claro y conciso.



Se dice que la *deep web* no se navega, se bucea, y es común sentirse perdido las primeras veces; se trata de un ejercicio nuevo en un elemento conocido, y eso genera cierta confusión y tendencia a abandonar el intento. Los principales problemas con los que tropezamos son los siguientes: No sabemos cuales son los enlaces de interés ni sabemos como llegar a ellos. Tambien es común que al intentar acceder a un servicio de la *deep web,* este se encuentre caído, perdido o muerto. Hay que tener en cuenta que el mantenimiento de estas paginas, foros, chat, servicios..., no es tan habitual como el de una pagina web comercial, la de un periódico de éxito o la de un blog conocido en la Internet común, pero como todo en esta vida, no tenemos mas que seguir buscando, curioseando e incluso fisgando para poder encontrar cuales son esos buenos enlaces.

Ya sabemos navegar; comencemos a bucear

Cuando nos adentramos en los suburbios de nuestras ciudades, acostumbramos ha hacerlo con cautela, paseamos con alguien que conozca el terreno, por ejemplo, o al menos, buscamos información de primera mano sobre lo que pretendemos explorar. Lo mismo deberiamos hacer al entrar a la *deep web*.

Son muchos los servicios y programas que nos permiten bucear por ella y aunque TOR es una de los mas conocidos y es sobre el que haré hincapié en este articulo, tambien es cierto que existen algunos otros y que funcionan ingual de bien, o incluso mejor que TOR. Cabe mencionar también dos grandes redes que aunque menos conocidas son igual de importantes: FreeNet o i2p. Tenemos que hacer la elección correcta en base a nuestras necesidades ya que todas han sido desarrolladas con diferentes propositos.

Es común pensar, de hecho así lo hago yo, que la idea romántica y hacker del anonimato es una de las mas importantes convicciones a la hora de acceder a este tipo de redes.

TOR (The Onion Router and The onion web)

The Onion Router, en su forma abreviada Tor, es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet en la que no se revele la identidad de los usuarios (anonimato a nivel de red) además de mantener la integridad y el secreto de la información mientras esta viaja a través de ella. Por este motivo se dice que esta tecnología pertenece a la llamada *deep web*.

El uso de este tipo de herramientas esta bastante extendido en las activistas políticas. El uso de los proxyes camufla tu rastro en Internet y ademas te permite saltarte algunas de las restricciones que, como es bien conocido, algunos gobiernos imponen sobre la red y su uso. TOR permite preservar tu privacidad dentro de las web que visitas, permite ocultar los destinos en linea de nuestros ISPs y por ultimo y no por ello menos importante nos permite saltarnos filtros de censura en Internet. Pero es importante saber que TOR fue diseñado para preservar tu privacidad en una capa de red pero no lo fue para preservarla en tus comunicaciones en linea. Por lo que no debería ser utilizado para enviar información a servicios web que usen una canal de comunicación inseguro (http).

TOR ofrece un software para conectarnos a los diferentes proxyes de su red. Para ello es necesario acceder a su web en la Internet comercial y descargarnos el software en forma de bundle o instalarlo en GNU/Linux usando el gestor de paquetes de nuestra distribución favorita. En los dos casos se recomienda la instalación del Vidalia, su panel de administración, así como Polipo, nuestro propio PROXY. Y en caso de que elijamos la segunda forma de instalación tendremos que instalar el plugin ProxyFoxy para Firefox, en el primer caso el navegador en formato de Bundle ya dispone de la gestión de proxy necesaria para red TOR usando la extensión de Firefox TOR Buttom.

```
aptitude install tor tor-geoipdb vidalia polipo
```

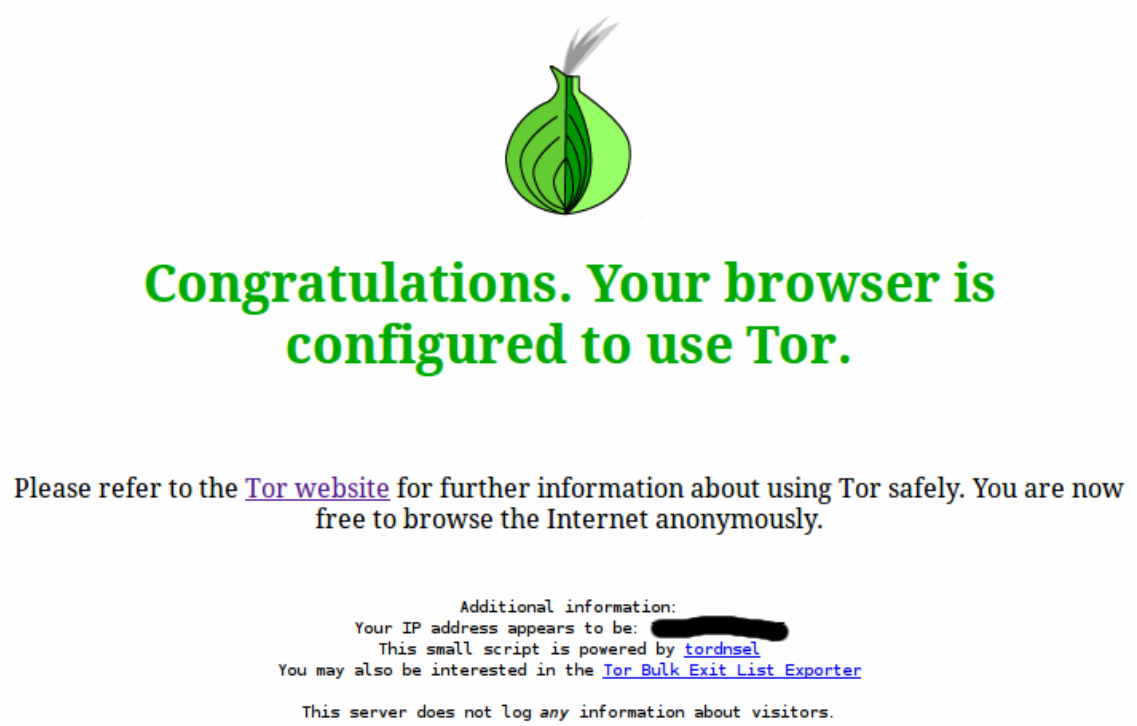
Nos descargamos la configuración de Polipo, para que no la tengamos que hacer nosotras mismas:

```
wget
https://gitweb.torproject.org/torbrowser.git/blob_plain/ae4aa49ad9100a50eec
049d0a419fac63a84d874:/build-scripts/config/polipo.conf
cp /etc/polipo/config{,.original}
mv polipo.conf /etc/polipo/config
service polipo restart
```

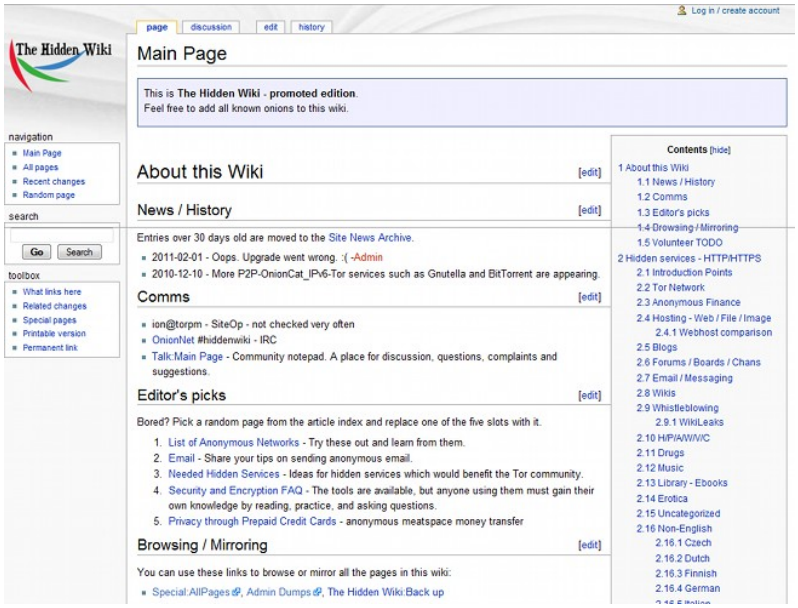
Y por último reiniciamos TOR:

```
service tor restart
Los parámetros de configuración de FoxyProxy son los siguientes:
localhost PUERTO Socket 5
```

Si todo ha ido bien podremos ir a la web que nos permite mirar si nuestro TOR esta bien configurado. En caso de que todo este correcto ya podremos hacer nuestra primera inmersión a UNO de los suburbios de Internet, The Onion Web.



The hidden services I: que podemos encontrar para garantizar nuestro anonimato



Los servicios que podremos encontrar en la *deep web* son comúnmente conocido con *Hidden Services* o servicios ocultos y no van mucho mas alla de los servicios que podemos encontrar en la Internet común, pero tienen el añadido de la privacidad: foros, comercio electrónico (donde aseguran el anonimato), bibliotecas de documentos en PDF o TXT, servidores de correo..., y sobre todo muchas cosas que tacharíamos de menos interesantes en la internet común, pero que aquí adquieren el valor añadido de gestionar correctamente nuestra privacidad.

Una de las webs de referencia en TOR es *The hiden Wiki*, La wiki oculta, allí con mucha frecuencia se cambian los enlaces a las webs mas comunes dentro de TOR, buscadores internos, repositorios de documentación importante, enlaces a foros de interés..., incluso enlaces a cosas que no nos gustaría tener que ver, lo dicho, los suburbios.

Es muy conocido el mundo de los *BitCoin* en estos lares del ciber espacio, todo se paga con una moneda digital, global, anónima y P2P. Esta moneda tiene buena fama dentro de todos los usuarios de este tipo de servicios y cada vez estamos viendo que llega mas arriba ya que hoy por hoy es bastante común encontrarnos con *BitCoin* en la Internet

comercial. Sin entrar en mucho detalle, ya que no es el objeto del artículo, diré que *BitCoin* es una sistema de pago en la que todos los pares validan todas las transacciones que se efectúan en esa red (TODOS los pares TODAS las tansacciones), incluso las que se hayan efectuado antes de que nuestra usuaria entrara en la red de *BitCoin,* por lo tanto tiene carácter retroactivo. Por ello es habitual que al arrancar por primera vez el *Wallet* de *BitCoin* tarde en dejarte hacer operaciones, ya que actualmente se descarga y valida unos 3 GB de datos.

The hidden services II: como poner en marcha nuestros propios servicios ocultos.

La gente que busca preservar el anonimato de su identidad en la red (tanto si es en la onion web como en la Internet comercial) usa servicios que estan en la red TOR. Todas y cada una de nosotras tenemos la posibilidad de desplegar servicios ocultos en nuestros servidores con una relativa facilidad.

A la hora de instalar un *Hidden Service* web tenemos que hacer una configuraciones muy simples en los ficheros de configuración de TOR. En este ejemplo solo explicare como montar un servidor web básico para poder servir HTML dentro de la red TOR, pero podéis usar las guías de vuestros sistemas operativos libres favoritos para poner servicios tales como blogs, (s)FTP, wikis..., o cualquier otra cosa que se os pueda ocurrir.

Lo primero que tenemos que hacer, antes de ponernos con TOR es instalar un servidor web, en mi caso *Apache2*:

```
# aptitude install apache2
```

Una vez hecho esto y comprado que "*It's works*", podemos ponernos manos a la obra con TOR, si lo tenemos arrancado lo primero es parar tanto Vidalia, el panel de administración de TOR, como el servicio TOR:

```
# /etc/init.d/tor stop
```

Una vez hecho esto tenemos que editar el archivo, buscaremos la linea #HiddenServicie y la dejaremos de la siguiente forma, donde /var/www es el directorio donde querremos poner el Hidden Service:

```
# vim /etc/tor/torrc
# Hidden Service
HiddenServiceDir /var/www
HiddenServicePort 80 127.0.0.1:80
```

Una vez realizada esta simple configuración arrancamos de nuevo TOR, así como Vidalia y miramos que en sección *error_logs* de Vidalia todo esta OK, en caso de tener algún error el log nos ayudara a descubrir que es lo que tenemos mal configurado.

Si todo va OK, TOR habrá creado dos ficheros en el directorio del *Hiden Service* (en el caso de este ejemplo /var/www), serán *hostname* y *private_key*, si abrís el fichero hostaname (que contiene la dirección .onion de nuestro *Hidden Service*) veréis que si accedéis a esa URL "torificada" podréis acceder a vuestro servidor web sin tener que hacer NINGÚN cambio en el router. Si les pasáis el fichero a vuestras compañeras ya podréis disfrutar del servicio :-)

La guerra se activa en la deep web: #opDarknet

> *Solamente aquel que construye el futuro tiene derecho a juzgar el pasado.*
>
> *Nietzsche*

Aunque los suburbios y el anonimato pueden ser un excelente caldo de cultivo de acciones deleznables, también se gestionan contraacciones por parte de los usuarios de estos "bajos fondos". Así pues, cuando *Freedom Hosting* permitía que redes de pederastas montaran sus servicios dentro de sus servidores, Anonymous, al igual que otros muchos, penso que eso no se podía permitir y se lanzó uno de los mayores ataques colectivos que se han dado en la Internet oculta: *#opDarknet*

Dicha acción fue un éxito y cayeron servicios importante de pederastia como lo fue *TORpedo.* Los integrantes de Anonymous lo comunicaron tanto en *The house of anonymous* como en la Internet comercial.

Con esto no quiero decir que todo lo que se hace en los suburbios sea bueno o sea malo, quiero decir que el anonimato y sus posibilidades son una herramienta más, no un modo moderno de ser impune. Nietzsche lo sabía.