Despliegue de Onion Services

En nuestra guía sobre la red Tor explicamos que era una muy buena herramienta para asegurar el anonimato de las comunicaciones sobre redes. Más imporante es, aún, en un mundo donde los gobiernos y las empresas vigilan por activa y por pasiva nuestros movimientos y acciones en Internet.

La red Tor, además de de proveer anonimato a sus usuarios, también permite exponer servicios a través de ella, de tal forma que los servicios sean teóricamente anónimos. A estos servicios se les llama Onion Services y son muy útiles para el despliegue de servicios o servidores anónimos.

¿Qué es un Onion Service?

Un Onion Service o Hidden Service es un servicio accesible a través de la red Tor. Esto significa que para acceder al servicio hay que hacerlo desde la red Tor y que al acceder no se sale de esta misma red.

Un Onion Service es identificado por una dirección *.onion*, que es un nombre de dominio que solo se resuelve dentro de la red Tor. La resolución del dominio no devuelve la dirección IP real del servicio, sino que ayuda a enrutar la conexión para llegar a ese servicio. Por ejemplo, la dirección *.onion* de la página oficial del proyecto Tor es:

2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion

A esta dirección solo se puede acceder usando el Navegador Tor o pasando las conexiones del sistema por la red Tor. Cuando se accede a esa dirección, no se está saliendo en ningún momento de la red Tor.

Ahora bien, el proyecto Tor también tiene una página en el Internet convencional: www.torproject.org. Por tanto, se ve que un mismo servidor puede exponerse tanto a la red Tor como al Internet convencional o *clear web*. En este caso, el servidor no es anónimo, pero permite a los usuarios que acceden a él a través de la red Tor no salir nunca de esta red cuando acceden a través de la dirección *.onion*, mientras que si acceden a través de la red Tor a *www.torproject.org*, el último salto de la ruta lo estarán dando desde el último nodo de la red Tor al servidor del proyecto Tor, es decir, el último salto se dará desde el margen de la red Tor a la *clear web*, mientras que usando la dirección *.onion* este último salto fuera de la red Tor no se daría.

Utilizar un Onion Service sirve principalmente para levantar servidores anónimos, únicamente accesibles por la red Tor, aunque hemos visto con el ejemplo de la página web del proyecto Tor que pueden usarse para exponer un servidor a la red Tor, sin necesidad de ser anónimo. Nosotros nos vamos a centrar en la primera funcionalidad, porque ofrece varias ventajas importantes:

1. Desplegar servicios anónimos: el funcionamiento **teórico** de la red Tor impide revelar la dirección IP del servidor.

2. Desplegar servicios sin necesidad de exponer la dirección IP, comprar un nombre de dominio ni exponer el servidor directamente a Internet: cuando configuramos un Onion Service, la red Tor nos asigna gratuitamente un nombre de dominio *.onion* y si la máquina tiene esos puertos abiertos y con servicios corriendo, normalmente no hace falta configurar nada más para que sea accesible a través de la red Tor.
3. Desplegar servicios ocultos en gran medida: los nombres *.onion* son aleatorios y lo suficientemente largos para que sea muy dificil encontrar un servicio por casualidad o haciendo fuerza bruta.
4. Exponer, apagar o trasladar servicios de forma rápida: un Onion Service puede exponerse o eliminarse simplemente modificando la configuración o apagando el servicio Tor en la máquina. También puede asignarse un nuevo *.onion* a un servicio cambiando el archivo de configuración, en caso de que haya sido descubierto o se quiera ocultar a usuarios que ya conocen el servicio.

Con todas estas caracterísiticas, los Onion Service son una herramienta muy útil no solo para preservar el anonimato, sino también para facilitar el despliegue de herramientas propias para la militancia, incluso de forma totalmente gratuita.

Cómo desplegar un Onion Service

Edición del archivo de configuración

El primer paso es instalar **tor** en una máquina, normalmente la misma en la que ejecutamos el servicio a exponer. Una vez instalado, hay que editar el archivo de configuración, que en sistemas operativos tipo Unix suele estar en la ruta */etc/tor/torrc*. El archivo *torrc* es el archivo de configuración. Según el sistema operativo en el que estemos, puede que ese archivo se cree en la instalación, pero no tiene por qué. Si no se ha creado, habrá que crearlo. Si se ha creado en la instalación, normalmente suele venir ya escrito con ejemplos, de los cuales nos interesan los de la sección inmediatamente debajo de la línea en la que aparece `This section is just for location-hidden services`. De todas formas, puede que en otras versiones o configuraciones de ejemplo esto no sea así.

Nos vamos a centrar únicamente la sección de los Onion Services. Si ya has configurado alguna otra funcionalidad en el archivo *torrc*, seguramente este tutorial no te haga falta.

Por simplicidad, vamos a borrar todo el archivo **torrc** y escribir las líneas que necesitamos.

Empezaremos por definir un directorio para el Onion Service. Por ejemplo, lo llamaremos “servidor_tor”:

```
HiddenServiceDir /var/lib/tor/servidor_tor/
```

Después, expondremos los puertos, mediante la opción *HiddenServicePort*. Esta opción va seguida del puerto en el que se expondrá y de la dirección IP del puerto

donde está expuesto el servicio. Por ejemplo, para exponer en el puerto 1234 un servicio corriendo en nuestra misma máquina (127.0.0.1) en el puerto 80:

```
HiddenServicePort 1234 127.0.0.1:80
```

La configuración completa quedaría así:

```
HiddenServiceDir /var/lib/tor/servidor_tor/
HiddenServicePort 1234 127.0.0.1:80
```

Un archivo de configuración *torrc* con estas dos líneas es suficiente para exponer ese servicio como Onion Service. Para que se genere el Onion Service, es necesario iniciar o reiniciar el servicio *tor* en el sistema. Una vez iniciado, la dirección *.onion* podremos obtenerla en el archivo *hostname* dentro del directorio del Onion Service. En el caso del ejemplo anterior, estará en */var/lib/tor/servidor_tor/hostname*. Para acceder al Onion Service, solo necesitamos estar conectados a la red Tor y usar la dirección *.onion* como destino.

Si quisiéramos abrir más puertos en esa misma dirección, añadiríamos otra línea con la opción *HiddenServicePort* apuntando al puerto de ese otro servicio. Además, el archivo de configuración no está limitado a un solo Onion Service, por lo que si creamos otra línea con otro *HiddenServiceDir* (el directorio debe ser diferente) y abrimos otros puertos, tendremos dos Onion Service en la misma máquina.

Para más información sobre cómo configurar Tor, consultar el manual de Tor, especialmente bajo la sección “HIDDEN SERVICE OPTIONS”.

Un ejemplo

Veamos el despliegue de unos Onion Service mediante un ejemplo algo más complejo. Pongamos que tenemos un ordenador viejo con Alpine Linux instalado y con acceso a Internet. Queremos exponer a través de la red Tor una página web informativa sobre nuestra organización, un foro y un servidor de chat XMPP para los integrantes de la misma. El servidor web está ejecutándose en el puerto 8080 del ordenador, expuesto en la interfaz local (127.0.0.1). El foro se ejecuta en una máquina virtual en la dirección IP 10.10.200.20 y en el puerto 3000. El servidor de chat XMPP se ejecuta en un contenedor Docker en la dirección 10.10.100.15 y en el puerto 5222. Queremos exponer la página web y el foro en el mismo *.onion*, la web en el puerto 80 y el foro en el puerto 5000. En otro *.onion* expondremos el servidor XMPP, ya que este será solo para uso interno de los militantes y solo queremos que conozcan su dirección los integrantes de la organización.

Una vez instalado el paquete *tor* a través del gestor de paquetes (`apk add tor` en Alpine Linux), crearemos/borraremos y editaremos el archivo */etc/torrc*, quedando de la siguiente manera:

```
HiddenServiceDir /var/lib/tor/web_y_foro/
```

```
HiddenServicePort 80 127.0.0.1:8080
HiddenServicePort 5000 10.10.200.20:3000

HiddenServiceDir /var/lib/tor/xmpp/
HiddenServicePort 5222 10.10.100.15:5222
```

Ahora reiniciamos el servicio *tor* y encontraremos el *.onion* de la página web y del foro en el archivo */var/lib/tor/webyforo/hostname* y el *.onion* el servidor XMPP en el archivo */var/lib/tor/xmpp/hostname*. Para acceder a ellos apuntaremos el navegador Tor o el cliente de chat XMPP a las direcciones *.onion* y puertos correspondientes.

Colectivo 406