The #OpNewblood Super Secret Security Handbook

Si no has configurado el cliente IRC de chat
para tu sistema operativo, te recomendamos
que regreses y empieces allí.

Índice principal de contenidos:

1) Prólogo
2) Configurando Tor
3) Extensiones recomendadas para Firefox
4) Configurando i2p
  4.1) Instalación
  4.2) Configuración de Firefox
  4.3) Configuración del cliente IRC
  4.4) IRC i2p en Android vía irssi connectbot
5) IRC avanzado
  5.1) Comandos
  5.2) Navegando
6) Técnicas avanzadas de defensa
7) Soluciones portables
  8) Guía avanzada de hacking y vulnerabilidad de la seguridad

Sección 1: Prólogo

NOTA: Si en algún momento necesitas ayuda con cualquier tema de esta guía, no dudes en unirte a nosotros en http://goo.gl/8zxwO donde podrás encontrar a alguien dispuesto a ayudarte. Cabe señalar que esta guía contiene información que puede ser difícil de entender sin un conocimiento técnico amplio y funcional de los sistemas de información. Aunque esta guía pretende ponerlo en términos más simples, tú cómo usuario eres el último responsable de la la seguridad de tus propios sistemas.

Sección 2: Configurando Tor

Debido a abusos en el pasado, los usuarios que intentaban conectar a los servidores IRC de AnonOps usando Tor no eran capaces de conectarse. Esto no es nada personal, simplemente tuvimos problemas con el abuso del programa en el servidor IRC y por tanto, no recomendamos usarla para conectar al IRC y si como una herramienta fácil de usar para navegar por Internet de manera anónima. Tenlo en cuenta, para la mayoría de los usuarios es una conexión relativamente lenta.

Windows:

Descarga Tor desde aquí:
https://www.torproject.org/dist/torbrowser/tor-browser-2.2.35-4_es-ES.exe

Después de descargarlo:

1) Ejecuta el archivo .exe
2) Extráelo a tu PC.
3) Ahora tendrás TOR en la carpeta que hayas seleccionado. Deberás tener un icono de una cebolla llamado *"Star Tor"*, púlsalo para empezar (si quieres puedes crear un acceso directo haciendo clic con el botón derecho del ratón y arrastrándolo al escritorio, pero asegúrate que el original permanece en la misma carpeta).
4) Ya puedes empezar. Si tu proveedor de Internet te bloquea las conexiones a TOR y necesitas ayuda para configurar un 'puente', no dudes en preguntar sobre esto en el canal de IRC #OpNewBlood, al que de nuevo puedes acceder a través de tu navegador en este enlace: http://goo.gl/8zxwO

Linux:

1) Descarga TOR desde aquí: https://www.torproject.org/dist/torbrowser/linux/tor-browser-gnu-linux-i686-1.1.4-dev-en-US.tar.gz
2) Descomprímelo en el directorio que más rabia te dé.
3) Accede ahora al directorio y deberías poder hacer clic sobre el botón *"start"* para comenzar.

4) Para mayor facilidad de uso, prueba a instalar la extensión para el navegador web Firefox llamada "Tor button".
5) De nuevo, si tu ISP bloquea Tor, puedes obtener ayuda para crear un puente preguntando en el canal de IRC #OpNewBlood al que puedes acceder mediante el navegador web desde aquí: http://goo.gl/8zxwO

Mac OS X:

1) Descarga Tor desde aquí: https://www.torproject.org/dist/vidalia-bundles/vidalia-bundle-0.2.1.30-0.2.10-i386.dmg
2) Monta el archivo .dmg y búscalo en el escritorio.
3) Mueve Vidalia hasta tu carpeta de aplicaciones
4) Descarga la extensión para Firefox "Tor button" desde aquí: https://www.torproject.org/torbutton/index.html.en
5) Una vez tengas instalados ambos, ejecuta Vidalia y asegúrate que diga *"Connected to the Tor Network!"* luego ve la parte inferior derecha de tu navegador Firefox y haz clic derecho en *"Toggle Tor Status"*
6) Para más información sobre el funcionamiento de Tor puedes ir a: https://www.torproject.org/docs/tor-doc-osx.html
7) Una vez más, si tu ISP te bloquea Tor, puedes obtener ayuda para crear un puente preguntando en el canal de IRC #OpNewBlood si usas un cliente de IRC o vía tu navegador web: http://goo.gl/8zxwO

NOTA PARA TODOS LOS SISTEMAS OPERATIVOS:

1) Para comprobar en cualquier momento que TOR esta funcionando puedes ir a : https://check.torproject.org/ y te dirá si TOR está operativo.
2) Está altamente recomendado usar la extensión para Firefox "Tor button": https://addons.mozilla.org/en-us/firefox/addon/torbutton/ la cual permite habilitar y deshabilitar TOR así como comprobar su estado desde el navegador web.

Navegación anónima usando la extensión para Firefox "Tor Button".

Comienza por instalar TOR en tu ordenador y configúralo a tu gusto. Una vez realizado esto descarga la extensión para Firefox "Tor button" y utiliza sus opciones para configurarlo como quieras. Después, presiona "Tor Button" y dirígete a un sitio web de prueba https://check.torproject.org para asegurarte que funciona correctamente. Si el sitio web nos da como respuesta resultados anónimos apropiados eso significará que has configurado Firefox correctamente para la navegación a través de TOR. Otro punto importante, si seleccionas Herramientas>Comenzar navegación privada cuando navegas a través de TOR, el navegador dejará de registrar tu historial de navegación, de almacenar ficheros temporales, contraseñas, cookies e historial de descarga de manera que no tendrás que limpiar el histórico del navegador cada vez que lo utilices.

Para resolución de problemas visita: www.torproject.org

Sección 3: Ad-ons recomendados para Firefox

Adblock-Plus: Este plugin bloquea alrededor del 90% de los servicios de Internet que intentan registrar tu actividad en Internet para enviarte publicidad personalizada. Es crucial usarlo mientras navegues por sitios web relacionados con anonymous.
http://goo.gl/fPmjm

NoScript: Es un plugin muy útil que deshabilita el javascript en los sitios web para proteger tu privacidad y para parar cualquier actividad maliciosa. Puedes establecer reglas para denegar la ejecución de scripts sólo en determinados sitios o denegar el permiso globalmente.
http://noscript.net/

BetterPrivacy: Es un plugin que identifica y borra cookies. También actúa como "opout" de publicidad y otras formas de seguimiento web.

FoxyProxy: Es un addon que permite gestionar una lista de servidores proxy.
El addon FoxyProxy te permitirá tener un acceso más fácil para habilitar sus túneles proxy, así como otras funciones avanzadas como la creación de una lista de dominios a los que siempre querrás conectar utilizando proxys de manera automatizada mientras mantienes otra conexión para los sitios que no has metido en la lista.
http://goo.gl/VRiHT

Ghostery: Se trata de otra herramienta para ayudar a gestionar y mitigar el seguimiento a través de cookies.
Las características de las herramientas Ghostery te alertarán cuando se detecte alguna clase de seguimiento de cookies en las páginas web que estés visitando en ese momento. También podrás ver información de cada "tracker" que esté intentando recolectar tus datos de navegación, e incluso ver el código fuente de dicho "tracker" y ver de que manera la cookie te está rastreando.

Greasemonkey (GM): Un buen addon para Firefox que te permite editar la forma en la que los sitios web te presentan la información, utilizando fragmentos pequeños de código javascript. Es más bien un "motor" o plataforma de desarrollo, que permite escribir y descargar scripts para hacer cosas variadas. http://goo.gl/atGk7

HTTPS Everywhere: Una extensión de firefox nacida de la colaboración entre "The Tor Project" y la "Electronic Frontier Foundation". Fuerza la conexión SSL en las webs principales siempre que sea posible. http://goo.gl/fsKV

Sección 4: Configurando i2p para IRC y navegación

Tabla de contenidos:

4.1 Instalación
- **a. Windows**
- **b. Linux**

4.2 Configuración de firefox
4.3 Configuración de cliente IRC
4.4 I2p IRC en android mediante IRSSI ConnectBot

4.1a) Instalación de i2p en Windows

1) Descarga:
Puedes descargar la ultima versión del software "I2p" en http://www.i2p2.de/download

2) Instalación:
En Windows, la instalación, como casi cualquier otro software de Windows, es relativamente sencilla. Haz doble clic sobre el archivo i2pinstall_(versión).exe que has descargado desde el enlace de arriba y sigue las instrucciones

3) Lanzando el router:
Después de que la instalación se haya completado puedes acceder a la consola de tu router (el panel de control del software de i2p, en forma de sitio web) incluso cuando no estás utilizando de forma activa el proxy, haciendo doble clic en el icono "Start i2p" o accediendo a http://127.0.0.1:7657 . Para los no versados en el funcionamiento de Internet, 127.0.0.1 es una dirección que conduce siempre a tu propia máquina. Si tienes en tu maquina un servidor web ejecutándose podrás acceder desde el navegador introduciendo esa IP para ver su contenido. No necesitas utilizar un software para anonimizar esta conexión ya que se trata de una conexión local con tu propia maquina.

4) Navegando con i2p:
Para acceder a sitios .i2p, o sitios epp, debes configurar i2p como un PROXY en el navegador web que tú elijas, las instrucciones pare realzar esto en Firefox están en el punto 4.2

4.1b) Instalación de i2p: Linux

1) La manera sencilla: Ubuntu Linux/Debian
Abre una terminal e introduce:
sudo apt-get install sun-java6-jdk
Obtén el último paquete instalable de i2p (sí, el maldito archivo .exe, no preguntes, es mierda java) desde http://www.i2p2.de/download. En tu terminal posicionate en el directorio donde esté el archivo .exe e introduce:
java -jar i2pinstall-*.exe
Sigue el prompt, no tiene pérdida

2) Otras distribuciones:
En los principales buscadores, encontrarás recetas de como instalar la Java Runtime Enviroment en tu distribución, habitualmente no es mucho más difícil que en Ubuntu, pero cada distribución tiene sus peculiaridades y su sistema de gestión de paquetes, además los comandos no son significativamente diferentes.
Una vez instalada la JRE, procedemos con el mismo comando que en ubuntu:
java -jar i2pinstall-*.exe

4.2) Configuración en Firefox

1) Comprobar que el invento funciona:
Una vez que hayas instalado el cliente i2p, puedes comprobar si está ejecutándose correctamente ejecutando un túnel por http:// abriendo la siguiente url en tu navegador: http://127.0.0.1:7657/i2ptunnel/

Bajo la sección "I2p Client Tunnels", la primera entrada debería ser "I2p HTTP Proxy". A la derecha, bajo la columna "Status", hay tres pequeñas estrellas; una roja, una amarilla y otra de color verde. Si la estrella roja está encendida, haz clic en el botón "start" a la derecha de la misma. Si es amarilla, es que no tiene suficientes conexiones de pares "peer", y deberías dejar primero que establezca una presencia en la red. Déjalo como está y tómate un bocadillo de jamón, debería de funcionar en una o dos horas.

2) Establece localhost como proxy
Ir a Edición > Opciones
Ir a la pestaña "Avanzado"
En "Conexión", haz clic en el botón "Configuración..."
Selecciona "Configuración manual del proxy"
Escribe lo siguiente:
Proxy HTTP: 127.0.0.1 Puerto: 8118
Proxy SSL: 127.0.0.1 Puerto: 8118
Servidor SOCKS: 127.0.0.1 Puerto: 9050
SOCKS v5 marcado
No usar proxy para: 127.0.0.1

4.3) Varias configuraciones de clientes de IRC

Los clientes de IRC no necesitan ninguna configuración especial o proxy. Sólo tienes que visitar tu http://127.0.0.1:7657/i2ptunnel/ y asegurarte de que el proxy IRC está funcionando. Si es así, sólo tienes que conectar a 127.0.0.1 en el puerto 6668 como si fuera un servidor de IRC normal. Tu cliente enviará todos los datos al servidor proxy que se ejecuta en tu máquina a través del puerto 6668, que a su vez lo enviará, a través de i2p, de forma anónima y segura a los servidores i2p IRC.

Puedes añadir servidores irc .i2p adicionales haciendo clic en IRC Proxy en la página del gestor del túnel y pegar las direcciones en el campo *"Tunnel Destination"* (separados por comas). Echa un vistazo a la siguiente lista de clientes y escoge el que te parezca más adecuado para ti:

Windows: http://www.ircreviews.org/clients/platforms-windows.html
Linux: http://www.ircreviews.org/clients/platforms-unix-x.html

4.4) I2p IRC en android mediante IRSSI ConnectBot

1) Si tienes una maquina con Linux, puedes conectar a los servidores de IRC a través de I2P desde tu ordenador de casa y desde tu teléfono Android desde cualquier parte del mundo.
Lo que necesitas:
Ubuntu Linux: http://www.ubuntu.com
Irssi connectbot para android: https://market.android.com/details?id=org.woltage.irssiconnectbot
Openssh para ubuntu: *sudo apt-get install openssh-server*
Irssi para ubuntu: *sudo apt-get install irssi*

2) Abre irssi connectbot en tu android e introduce: *[tu nombre de usuario en linux]@tuip:puerto*
Ahora, desde que la mayoría de la gente está tras un firewall (cortafuegos), o un router, o algo,... probablemente tengas de mapear algunos puertos, pero por ahora, solo conecta a tu router wireless con tu android wifi. Esto es más seguro de todos modos.

3) La primera cosa que quieres hacer es iniciar sesión con tu contraseña (por eso es mejor hacerlo a nivel local antes que hacerlo en la web ... Por cierto, asegúrate de que tienes cifrado el wifi)
4) Una vez que tengas el símbolo del sistema (command prompt) en tu android, presiona el botón de atrás para regresar a la lista de hosts, a continuación el botón de menú para pulsar sobre *"Manage Pubkeys"* (administrar claves publicas), presion de nuevo el botón menú y selecciona *"generate"* (generar). Escribe tu clave, selecciona RSA y consigue al menos un hash de 1024 bits (yo iría a 2048 mejor). sin contraseña y pulsa en *"Generate"* (generar).

5) Ahora tendrás que hacer un poco el tonto con el touchpad para generar una aleatoriedad,
y crear tu clave publica (pubkey). Una vez estés de nuevo sobre la lista de claves publicas (pubkey list) tendrás que presionar sobre tu nueva clave publica y seleccionar "Copy Public Key" (copiar clave pública).

6) Ahora pulsa el botón atrás y haz clic sobre la conexión de tu host en la lista de hosts, esto te llevará de nuevo al símbolo de sistema (al command prompt). Introduce *cat "(presiona menu y selecciona paste para pegar tu clave publica sobre estas comillas)" >> .ssh/authorised.keys*

7) Ahora escribe exit para ir de vuelta a tu lista de servidores (server list), y desconectate.

Toca en el servidor para conectar de nuevo, y esta vez, el programa no debería preguntarte una contraseña. Esto significa que estas conectado usando una clave publica compartida de 1024 bits (al menos), que no esta nada mal.

8) Para conectar desde fuera a la red de tu casa necesitas unas cuantas cosas más:
Tu IP externa: http://www.whatismyip.com
Puerto redirigido al puerto 22 de tu maquina (si tienes, como la mayoría, un router y múltiples maquinas en la red de casa mírate el paso 9)

9) La mayoría de los routers están configurados con una interfaz webque permite cambiar su configuración.
Si tienes la seguridad wireless habilitada, entonces tu o quien sea que te configurase la red de casa web le puso una contraseña.
Necesitarás hacer login en la interfaz web, ir a la sección sobre "port forwarding" (mapeo de puertos) y redireccionar un puerto externo disponible (el 22) al puerto 22 de la IP local de tu maquina (normalmente 192.168.1.101 o algo así) y seleccionar tanto tcp como udp.
Esto lo dejo tan claro como puedo sin tener a mano las instrucciones especificas de un router determinado (habla con el proveedor de tu router o un geek cercano para obtener más ayuda sobre esto).

10) Ahora todo lo que tienes que hacer es conectar a través del Irssi connectbot a *(tu nombre de usuario)@(tu IP externa):(El puerto que tienes redirigido a tu maquina)*

11) Una vez que estés conectado a un servidor ssh en el ordenador de casa (que por ahora debe estar ejecutando i2p) puedes lanzar irssi, un cliente IRC de línea de comandos y conectarte a los servidores i2p con irssi usando:

/connect 127.0.0.1 6668

¿Preguntas? ¿Comentarios? ¿Preocupaciones? Entra en #OpNewblood a través de tu navegador web aquí: http://goo.gl/8zxwO o puedes comunicarte a través de cred por i2pmail cred@mail.i2p o desde la web insegura (pero segura) en http://privacybox.de/cred.msg (no olvides incluir información dato de contacto para que la respuesta, ya que no almacena o transmite ningún dato de identificación)

Sección 5: Comandos IRC Avanzados

5.1) Comandos

1) /join
Se explica por sí mismo, se utiliza para unirse a un canal. Para entrar en #opnewblood, tendrías que escribir */join #opnewblood*
2) /me
En realidad, no es muy necesario, sino que se utiliza a veces, por ejemplo, si quieres saludar a alguien.. Para ello tendrías que escribir /me saluda que aparecería como *"anon saluda"*
3) /msg
Si quieres tener una charla con una persona específica fuera del canal lo mejor es mandarle un mensaje. Sólo tienes que escribir /msg username mensaje. Asegúrate de dejar un espacio entre el nombre del usuario y el mensaje.
4) /query
Lo mismo que /msg, excepto que éste abrirá una nueva ventana en la que mantener una conversación con la persona elegida. Por ejemplo */query username mensaje_opcional*
5) /nick
Este comando cambiará tu nick (nombre de usuario). Por ejemplo, si quieres pasar a llamarte gigapuddi deberías escribir */nick gigapuddi*. Recuerda que si haces eso dejarás de estar registrado a menos que vuelvas a registrarte con nickserv (consulta el tutorial de anon si no sabes lo que es nickserv, o si necesitas más ayuda)
6) /quit
Abandonas el chat.
7) /ignore
Hay mucho troll, y lo mejor es no alimentarlos, simplemente ignóralos. Para ignorar a alguien teclea /ignore nombredeusuario
8) /whois
Mostrará información sobre la persona seleccionada, como su vhost, canales en los que está etc. para usarlo escribe /whois username
9) /away
Puedes usar este comando para marcarte a ti mismo como no disponible, "estoy fuera". Por ejemplo si escribes "*/away preparando un bocata*" (sin las comillas) el resto de gente sabrá que estás fuera

del terminal preparándote un tentempié.
10) /ping
Esto es para ver la latencia del servidor, si sufres esperas este comando te podría dar más información, para hacer ping a un servidor sólo tienes que escribir */ping dirección_ip*
11) /notify on / off
Esto permite cambiar la opción que determina si recibirás una notificación (un pitido) cada vez que alguien escriba tu nombre. Para desactivarla */notify off* para activarla */notify on*
12) /topic
Permite cambiar el tema (topic) del canal. Ejemplo: */topic #canal Hoy hablamos de SOPA*
13) /list
Muestra la lista de los canales que están disponibles.

5.2) Navegando por IRC

NickServ
La primera vez que llegas al IRC, empezarás usando un nickname (nombre de usuario) sin registrar. Si vas a convertirte en un usuario habitual, es vital que registres tu nick. Es importante por varias razones:
Te asegura que nadie va a hacerse pasar por ti.
Te autoriza a diversas operaciones que no se permiten a los usuarios no registrados. La más importante es que puedes usar un vhost (esto oculta tu ubicación y la información de tu ISP a otros usuarios).

Para registrar tu nickname, consulta la guía de IRC para tu sistema operativo en la página original de #OpNewBlood
Cuando te conectes al servidor, teclea /msg nickserv IDENTIFY tu_password Esto informará a nickserv que eres el propietario real de tu nickname. Si no lo haces, no tendrás acceso a canales sólo para usuarios registrados ni a tu vhost. Por razones de seguridad, es recomendable que teclees el comando en tu ventana de estado, de este modo en caso de que cometas un error, no difundirás tu password a todo el canal.

Grupos
Si vas a usar más de un nickname (apodo), puedes agruparlos. Esto tiene varios usos, el principal es para decirle a la gente desde donde estas conectando o si por ejemplo estas "away" (fuera).
Por ejemplo: un usuario llamado "JohnDoe" podría estar fuera por un tiempo pero dejar su ordenador portátil encendido, en este caso podría cambiar su nick a "JohnDoe|Away" o "JohnDoe|AFK" para que otros usuarios sepan que no esta presente. Esto es importante para que, por ejemplo, la gente sepa el motivo por el que no está respondiendo a los mensajes. Podría usar también el nick "JohnDoe|Mobile" para que la gente sepa que está conectando desde un smartphone, y por tanto que sepan que no puede utilizar ciertas funciones como puede ser la posibilidad de recibir mensajes privados.

Para cambiar tu nick, escribe */nick nuevonick*. Sin embargo, cuando hagas ésto perderás tus niveles de acceso, tu vhost, y otras opciones asociadas a tu nick.
Para evitar ésto, cuando selecciones tu nuevo nick, cámbialo usando /nick nuevonick y a continuación escribe */msg nickserv GROUP nick password* (donde nick y password son tu nick y password principales). Ésto asegura que estos nicks compartan contraseñas y configuración.

Nicks fantasma
Aceptemoslo, a veces algo falla. Tu conexión a Internet puede caer inesperadamente, la batería de tu portátil se puede agotar, tu cliente de IRC se puede colgar, puedes cerrar una ventana por error... Hay muchos motivos que pueden hacer que te desconectes accidentalmente del IRC.

El problema es que a menos que uno se desconecte "como es debido", el servidor no se dará cuenta de que te has ido. Imagínatelo como si alguien abandonase el teléfono en mitad de una conversación, pero sin colgar. O como cuando tienes que forzar el apagado de tu ordenador porque no responde y no puedes apagarlo de forma normal. En estas circunstancias, el servidor IRC no se da cuenta de que te has ido, y asume que tu nick todavía sigue conectado. Esta situación se mantendrá hasta la próxima vez que el IRC haga un ping a tu nick y no obtenga respuesta (ping timeout). Ésto puede tardar un tiempo y muy a menudo la persona que se ha desconectado consigue volver a estar en línea antes de que el servidor haya tenido tiempo de darse cuenta de que había salido. Cuando ésto ocurre, el nick del usuario ya está en uso, de manera que el servidor le asigna uno nuevo (habitualmente simplemente añadiendo ` o _ al final, así si JohnDoe intenta conectarse cuando ya hay otro JonDoe conectado, se le registrará como JohnDoe_ or JohnDoe`)

El problema de ésto, por supuesto, es que al igual que un nick no registrado, estos nicks no tienen modos, ni vHosts, ni niveles de acceso, porque el "nick fantasma" los está ocupando.
Para forzar que la sesión caída se desconecte y reemplazar su nick por el tuyo, teclea /msg nickserv GHOST password, donde password es la contraseña del nick original. En este ejemplo ésto desconectaría el JohnDoe actual y cambiaría JohnDoe_ a JohnDoe automáticamente, identificando y configurando el nick de forma normal. Cuando ésto ocurra, probablemente verás algo así en el canal:

JohnDoe left the chat room (GHOST command used by JohnDoe_)
JohnDoe_ is now known as JohnDoe

Es muy importante que hagas ésto tan rápidamente como te sea posible después de reconectarte, porque hasta que lo hagas estarás bloqueado fuera de tu vHost.

vHosts
Obviamente una de las principales prioridades de cualquier Anonymous es permanecer, claro... anónimo.
Cuando te conectas a tu servidor IRC, el servidor automáticamente enmascara tu dirección IP (el *"número de teléfono"* de tu ordenador). Ésta es la capa de anonimato más importante, pero desgraciadamente hay un problema. La mayoría de las veces, NO ocultará automáticamente el nombre de tu ISP (Internet Service Provider - Proveedor de Servicios de Internet). Así por ejemplo podría quedar oculto el hecho de que tu IP es de cierta ciudad, pero que eres un cliente de Movistar, tal vez no.
Para remediar ésto, tenemos un vHostServ (un servidor virtual). Te proporciona un nombre de servidor falso, que enmascara el verdadero ISP a través del cual te estás conectando. Puede ser el que tu elijas, por ejemplo, si alguien intenta comprobar desde donde me conecto, verá en su lugar "que.te.den.morcilla" :D
Para conseguir un vHost, debes estar registrado e identificado. Es por eso que es CRUCIAL que te identifiques cuanto antes al conectarte, ya que tu vHost no estará activado hasta que lo hayas

hecho.

Cómo obtener un vHost:

1. Teclea /join #vhost en tu IRC.
2. Una vez estés en el canal vHost, teclea !vhost pon.un.nombre.inteligente.aquí

NOTA: Puedes, desde luego, usar lo que quieras como vHost (siempre que sea un nombre válido, por ejemplo sin espacios y que contenga al menos un punto ".") Lo más corriente es usar.los.puntos.como.espacios.en.tu.vHost.

Cuando lo hayas hecho, vHostServ automáticamente te expulsará y te negará la entrada (te baneará) al canal #vhost. Ésto es normal y es lo que debe ocurrir, simplemente significa que el vHost ha funcionado. Estarás baneado del canal #vhost durante cierto tiempo, después del cual volverás a ser capaz de cambiar tu vHost si quieres. Ahora que ya tienes un vHost, ya has configurado completamente el IRC para usarlo, cualquier otro ajuste que puedas hacer a tu nick es puramente opcional.

*NOTA: Si te unes a un #canal antes de establecer tu vHost, tu nueva información anonimizada no se actualizará automáticamente en ese canal. Después de que establezcas tu vHost asegúrate de salir y reconectarte de todos los canales en los que estuvieras, si no la información real de tu conexión todavía será visible.

**NOTA: Si utilizas Xchat con la opción para autounirse a canales, puedes decirle a Xchat que espere más antes de incorporarse a los canales al conectarse al servidor mediante el comando /set irc_join_delay X donde X es el número de segundos que XChat debe esperar antes de unirse a tus canales. Ajustar esta opción a unos 10 segundos ayuda si estás usando canales automáticos.

Canales que requieren invitación (modo +i)
Algunos canales, por razones diversas, sólo son accesibles mediante invitación. Habitualmente eso es porque el canal tiene un propósito muy específico y sólo quienes se dediquen a un trabajo determinado pueden acceder a él. Por ejemplo, hay canales privados para operadores y hackers. A veces, un canal se configurará como +i si está siendo invadido o inundado por bots o por trolls.
Si un canal es +i, no serás capaz de unirte a él utilizando /join. Simplemente recibirás un mensaje de error diciéndote que el canal sólo es accesible mediante invitación. Sin embargo, si eres un operador, o si estás en una lista de excepciones de invitación, puedes forzar al servidor para que te permita entrar.

Para hacer éso, debes mandar un mensaje a otro bot llamado ChanServ, que no trataremos en esta guía ya que en general sólo usuarios más avanzados van a necesitarlo alguna vez. De todos modos, para solicitar una invitación, teclea /msg chanserv INVITE #canal, donde #canal es el canal al que intentas conectarte. Es importante incluir el # al principio del nombre del canal, o ChanServ no lo reconocerá. Si estás en la lista, recibirás un mensaje preguntándote si te gustaría incorporarte al canal. En otro caso, ChanServ te contestará que no tienes permiso.

Si no estás en la lista de invitados o de operadores de un canal, pero de todos modos crees que deberías poder acceder, puedes teclear /knock #canal mensaje, donde mensaje es lo que quieras decir a los administradores del canal. Así por ejemplo, si te encuentras con un canal llamado

#mallorquins pensado solamente para gente de Mallorca, y tú siendo de la isla no tienes acceso, puedes escribir */knock #mallorquins Uep! Som mallorquí, que puc entrar?*

Este comando mandará un mensaje a los administradores del canal y hará que tu mensaje aparezca en el canal. Los administradores entonces (si deciden dejarte entrar) te mandarán una invitación igual que las que hace ChanServ. Recibirás el mismo mensaje que recibirías de ChanServ preguntándote si te gustaría unirte al canal.

NOTA: Llamar a la puerta de un canal insistentemente 10 veces no hará gracia a nadie. Lo más probable es que consigas que definitivamente decidan no invitarte al canal. Si no recibes ninguna invitación puede significar que o bien los administradores no están activos en ese momento, o que por alguna razón han decidido no invitarte. Si estás en esta situación, puedes volver a intentarlo más tarde, pero no insistas 10 veces en un minuto, así lo más seguro es que seas vetado en ese canal.

Si nadie contesta tu petición de entrar, otra opción que tienes es escribir /msg chanserv INFO #canal, donde #canal es el nombre del canal (de nuevo, tienes que incluir # delante del nombre del canal porque si no ChanServ ignorará tu mensaje). Este comando te informará del propósito del canal y quién lo ha creado. Entonces podrías mandar un mensaje al fundador del canal y solicitarle que te deje acceder, aunque ésto no es recomendable a menos que sea extremadamente urgente.

Sección 6: Técnicas de Defensa Avanzada

Usando Máquinas Virtuales

Es altamente recomendable que consideres hacer una Máquina Virtual (VM) para separar la instancia de tu sistema operativo personal con el sistema operativo para tu actividad como anónimo. Ésto te asegura que tus datos personales no se filtrarán mientras ves medios sociales relacionados con Anonymous en sitios como Twitter o Facebook.
Esto tiene otras ventajas como permitirte borrar rápidamente toda tu actividad como anónimo de tu ordenador simplemente borrando la propia máquina virtual.

Software de Máquinas Virtuales
VirtualBox - x86 and x64
VMWare Workstation 7 - x86 and x64
Windows Virtual PC - x86
etc. (haz una búsqueda en google con "máquina virtual")

Cifrado de disco

El cifrado de disco es otra forma de protegerte a ti mismo. El software de cifrado de disco hará prácticamente imposible que cualquiera aparte de ti mismo acceda a los datos de cualquier disco físico.

Software de Cifrado de Disco
TrueCrypt - http://www.truecrypt.org/
Bitlocker - (Win 7 Ultimate only)
Cifrado de Ficheros de Email y Validación (añadido por cred)
Usando el estándar openPGP, el software crea un "llavero" para ti, asociado a tu nombre y dirección de correo (ninguno de los cuales necesita ser real, pudiendo crear dos o más, uno para tu identidad en la "vida real" y otro para tu actividad como anónimo).
La llave privada es una llave protegida por contraseña que necesitarás en cualquier sistema en el que pretendas DESCIFRAR información; tu ordenador personal, y si eres valiente, por ejemplo en tu teléfono Android. La llave pública es utilizada para CIFRAR información o ficheros, y está

disponible para cualquiera. De esta forma, si tú quieres mandarme información cifrada, tendrías que buscar mi llave pública, cifrar los datos, y enviármelos. A partir de este momento, lo único que puede recuperar los datos es mi llave privada junto a mi contraseña.

PGP es el estándar industrial para correo cifrado de alta seguridad.
PGP (Windows) http://gpg4win.org/download.html
PGP (Linux) http://www.gnupg.org/
APG (Android) https://market.android.com/details?id=org.thialfihar.android.apg

Listas de proxies

- http://www.freeproxies.org
- http://www.socks24.org
- http://www.samair.ru/proxy

Máquinas virtuales Linux con Tor.

Es posible usar Tor como VPN usando algunas máquinas virtuales linux preconfiguradas. Una vez que se inicializan estas máquinas virtuales, es posible crear una conexión de Red Privada Virtual (VPN) a la Máquina Virtual Tor.

Estas máquinas virtuales incluyen paquetes extras de privacidad como Squid y Privoxy Software Linux Tor
JanusVM - http://janusvm.com/
TAILS - https://amnesia.boum.org/

Sección 7: Soluciones portables

Portable se refiere a por ejemplo un sistema operativo y paquetes de software que puedes ejecutar desde un CD, DVD o dispositivo USB. Esto te permite llevar tu anon OS en el bolsillo, conectarlo o insertarlo en otro ordenador y estar listo para acceder a recursos anon de una forma segura.
Algunas distribuciones linux live recomendables:

The Amnesic Incognito Live System: https://amnesia.boum.org/download/index.en.html
Una distribución live de linux centrada en seguridad y privacidad. Básicamente con todo lo que hablamos en esta guía en una sola descarga

Gnacktrack: http://www.gnacktrack.co.uk/
Para las anónimas, una distribución live con todas sus herramientas, es todo lo que se necesita para controlar el destino del mundo desde un portátil en una cafetería

Ubuntu Privacy Remix: https://www.privacy-cd.org/
Arranque desatendido, no se requiere instalación en el disco duro, y no se guarda ningún dato generado.

Sección 8: Guía de hacking avanzado y vulnerabilidades en la seguridad

La información contenida en esta sección puede ser extremadamente confusa para los nuevos usuarios que no cuenten con los conocimientos técnicos adecuados para entenderlos, pero no te preocupes, todos tuvimos una primera vez.
Sé cuidadoso cuando trates con sistemas que no comprendes en su totalidad, puedes terminar obteniendo resultados indeseables, detecciones, y en casos extremos, fallos en el sistema o problemas con la justicia.
Para todos aquellos interesados, existe una buena guía sobre los ataques de denegación de servicio distribuidos, puedes encontrarla aquí: http://insurgen.cc/index.php?title=DDOS

Como ciudadano de pleno derecho, deberías poder entrar en los sistemas a voluntad de formas diversas. Hay muchas maneras de acceder a una web y de protegerte a ti mismo en términos de anonimato y de minimización de la vulnerabilidad

Tabla de contenidos

1. Usando Putty para configurar un túnel SSH
2. Manual de Openvpn para GNU/Linux
3. Utilizando proxies SOCKS4/5 con Firefox
4. Cambiando los servicios locales de DNS
5. Cambiando hostnames permanentemente en Windows
6. Capturar paquetes diversos
7. TCP / IP y la Internet en general
8. Hack en un saco: El Framework Metasploit

1. Usando Putty para configurar un túnel SSH
http://oldsite.precedence.co.uk/nc/putty.html
A menos que se use SSL, las conexiones normales a Internet típicamente son transmisiones no encriptadas divididas en paquetes de datos. Mediante el uso de un packetsniffer, es posible capturar la mayoría de los paquetes y examinar su carga en forma de texto plano. Ésto puede incluir nombres de usuario, emails, mensajes instantáneos y a veces incluso contraseñas e información sensible. Cuando configuras un túnel de forma segura, te estás conectando a una conexión segura, encriptada a la máquina receptora, contribuyendo a prevenir que se usen packetsniffers para robarte información.

Esto no sólo es útil para mantener segura tu conexión local a Internet, también es una de las formas básicas en las que puedes ocultar la dirección IP desde la cual te conectas a Internet desde casa. Cuando estás usando un túnel para tus transmisiones, todos tus paquetes, en la sección dedicada a la dirección de origen, tendrán la dirección IP de la máquina de destino, en lugar de la tuya. De nuevo, como se ha tratado anteriormente, no puedes confiar en una VPN (SSH) que se ofrezca a coste cero. Te interesa especialmente utilizar un proveedor de pago.

2. Manual de Openvpn para GNU/Linux
Puedes encontrar información acerca de cómo configurar un sistema GNU/Linux para que use VPN aquí: http://openvpn.net/howto.html (OpenVPN sólo te asegura entre tú y tu servidor, no entre tu servidor e Internet. Tu servidor será el intermediario y es identificable a menos que se apliquen técnicas adicionales de ofuscación)

3. Utilizando proxies SOCKS4/5 con Firefox
Si estás interesada en utilizar proxies SOCKS 4/5 con el navegador Firefox, puedes encontrar instrucciones aquí: http://uniqueinternetservices.com/configure-proxy-para-firefox.html

4. Cambiando los servicios locales de DNS
Esta sección explica cómo cambiar el servidor de nombres que traduce nombres de dominio en direcciones IP, que es usado a veces como un medio ideal para rastrearte por tu ISP, incluso si los datos que usaste estaban encriptados vía RSA o por una encriptación triple DES robusta, alguien sigue llevando a cabo la solicitud de traduccion de un nombre de dominio a una IP, asegúrate que eres tu o alguien amistoso.
Si eres "súperparanoico" las solicitudes de DNS es la situación ideal que debería ser encriptada. Algunos proxies lo ofrecen. No puedo hacer una lista de cabeza, lo siento.
http://dnscurve.org/in-benefits.html

5.Cambiando hostnames permanentemente en Windows
Este truco hacker es un buen camino para asociar una IP mirror permanente a tu red social favorita como Facebook, Twitter, etc, etc.
Si estas interesado en esto, puedes encontrar más información aquí:
http://www.ehow.com/how_5225562_edit-windows-hosts-file.html

Si quieres que cannabis.com vaya a 4.2.1, entonces puedes ponerlo como la entrada localhost 127.0.0.1 que encontraras en tu configuración de windows.
Esto pasa por alto el nombre del servidor pedido en la mayoría de navegadores (Compruébalo con un sniffador de paquetes para estar seguro).

6.Capturar paquetes diversos
Todo esto necesita tener instalados los drivers PCap, y están incluidos en estan incluidos en las descargas de cada uno...
Entender los paquetes lleva tiempo y práctica.
Para iniciarse instala una copia de wireshark (http://www.wireshark.org/); o MS Network Monitor 3.4, los dos son gratuitos.
Si no ves ninguna interfaz con la capacidad de capturar en la lista, entonces debes ejecutarlo como administrador.

Para identificar que interfaz está viendo tu trafico, clica en el primer icono (arriba-izquierda) "list availabe interfaces" ("lista de interfaces disponibles") y busca una con los números creciendo.
Iniciala y mira el flujo de paquetes.

Debes ver mucho tráfico, empieza cerrando esa mierda de que estas descargando o lo que estés viendo streaming.
Tendrás ahora un desplazamiento más lento de tráfico ARP y NetBios, la ocasional explosión UPNP y otras cosas.
Si estás en una VPN segura, o algo asi, veras todos los paquetes SSL/TTS coloreados de gris o todos los paquetes UDP de azul, en algunos casos.
Intenta activar otra interfaz (como una interfaz TAP) para ver los buenos.

Captura en tu red doméstica y juega; mira como son los DHCP, las peticiones y respuestas DNS, navega a una carpeta compartida y mira que te muestra, cosas como estas.
Si sabes cómo, haz un escaneado nmap y mira cuán obvio y ruidoso es, y aprende técnicas para usarlas en más encubiertas.

http://www.wireshark.org/docs/ <- lee y mira los vídeo. Hay muchos, pero una vez lo cojas, es muy fácil de entender.

TCPDump(Linux)/WinDump(Windows) - Capturador de paquetes por linea de comandos para almacenar y analizar mas tarde. http://www.tcpdump.org/ y http://www.winpcap.org/windump/

NetworkMiner (http://networkminer.sourceforge.net) es una alternativa que te permite acortar los paquetes recogidos como quieras (por ejemplo, filtrando por host) para facilitar la excavación.

7. TCP / IP y la Internet en general
Cambiar la configuración del servidor DNS en windows XP:
http://www.mediacollege.com/computer/network/dns.html

Capas de red y modelo OSI:

Para que un experto en seguridad llegue realmente a entender el funcionamiento de un software o hardware conectado a una red o sistema de seguridad debe ser capaz de entender la relación y concebir las implicaciones de los cambios que se realizan en una instalación.
Lo que se haga en cualquier nivel de la capa de red estará interactuando en otros niveles también.
Por ejemplo la capa de enlace de datos (capa 2 OSI) debe hacer uso de la capa física (capa 1 OSI), y así sucesivamente.

Capa 1: Capa física
Se refiere a las especificaciones eléctricas y físicas de los dispositivos. En particular se refiere a los pins, voltajes, repetidores, hubs, adaptadores de red, ... Normas como el RS-232C para el estándar del puerto serie, popular en los años 90, usa cables físicos para acceder al medio.
Un medio popular como llegaría después a ser Internet al principio se conectaba mediante modems.

Capa 2: Capa de enlace de datos
La capa de enlace de datos proporciona los medios funcionales y de procedimiento para transferir datos entre las entidades de la red usando capas físicas (o cables, adaptadores, routers, repetidores, ...).
Al principio la capa 2 fue ideada para transferencia punto a punto solamente. LAN y multi-broadcast fueron desarrollados independientemente a la norma ISO IEEE 802.
WAN y LAN son servicios sobre la capa de enlace de datos que organizan los bits en secuencias lógicas desde la capa física.

Estas secuencias contienen información importante relativa a tu protocolo de transmisión, y incluye información como por ejemplo tu dirección IP.
Esta dirección es pasa a traves de niveles de servicio mediante el protocolo TCP de la capa de transporte.

8. Hack en un saco: El Framework Metasploit
Metaesploit es una suite de software creada para test de penetración, y esta incluida en ambos liveCDs, Gnacktrack y Backtrack, mencionadas en la sección de soluciones portables.
Esta suite tiene una interfaz de linea de comandos, una GUI (interfaz gráfica de usuario) y una interfaz web. Metasploit es, en la realidad, el primer software de hacking point-and-clic.
Contiene una enorme base de datos constantemente actualizada de explotis que puedes utilizar para acceder remotamente a sistemas vulnerables: http://www.metasploit.com/

Sign off
Gracias por leer este documento colaborativo, ¿crees que lo hicimos bien? por favor, haz preguntas en el canal de IRC #OpNewblood (al que, una vez más, puedes acceder también vía navegador web desde aquí: http://goo.gl/8zxwO) refiriéndote a este documento y recuerda como mantenerse a salvo.

Proteger tu anonimato es la parte más importante de ser anónimo.
En nuestro mundo la mejor defensa es un buen ataque.