Tema caliente

Network Defense

Victor Oppleman 

Grado de dificultad

Una técnica de seguridad poco conocida que ha demostrado ser uno de los medios de defensa más efectivos contra los ataques de denegación-de-servicio (denial-of-service).

Se ha utilizado globalmente por los proveedores de servicios de internet (ISP) como una manera de proteger a sus receptores. Como se explicará en este artículo la técnica, conocida como *sinkholing*, también puede usarse para proporcionar valiosa información con respecto a las amenazas a las que se enfrenta tu red. Con el empleo de la técnica de sinkhole (o sumidero) ganarás otros medios para defender tu red y obtener información valiosa sobre las amenazas y las configuraciones erróneas significativas que haya en esta.

Este artículo, escrito para usuarios conocedores de la red, os proporcionará lo siguiente:

- Los antecedentes y funcionamiento de la Sinkhole – breve reseña de los sinkholes en las IP y cómo varias organizaciones lo han puesto en práctica con éxito.
- La utilización de señuelos de red – cómo pueden usarse las técnicas de sinkhole aplicadas con el empleo de darknets y honeynets para atrapar y analizar los sondeos malintencionados, los intentos de infiltración, y otros eventos, junto a elementos de monitorización de la red, como la detección de intrusiones.
- La protección contra la denegación de Servicio – cómo las organizaciones y sus ascendentes proveedores de servicios de Internet han creado un medio de protección contra la denegación de servicio a través de la utilización extensiva, y puntual, de la técnica de sinkhole (o de sumidero).
- La dispersión inicial (Backscatter) y el rastreo de origen (Tracebacks) – explicación breve acerca de la dispersión inicial y cómo pueden usarse los rastreos de origen para identificar el punto de ingreso de un ataque

En este artículo aprenderás...

- Aprenderás a usar las técnicas del sinkholing y cómo protegerse de los ataques de denegación de servicio.

Lo que deberías saber...

- Debes tener conocimientos básicos sobre los ataques de denegación de Servicio
- Debes conocer los problemas del tráfico de red desde los ISP (Proveedores de Servicios de Internet)

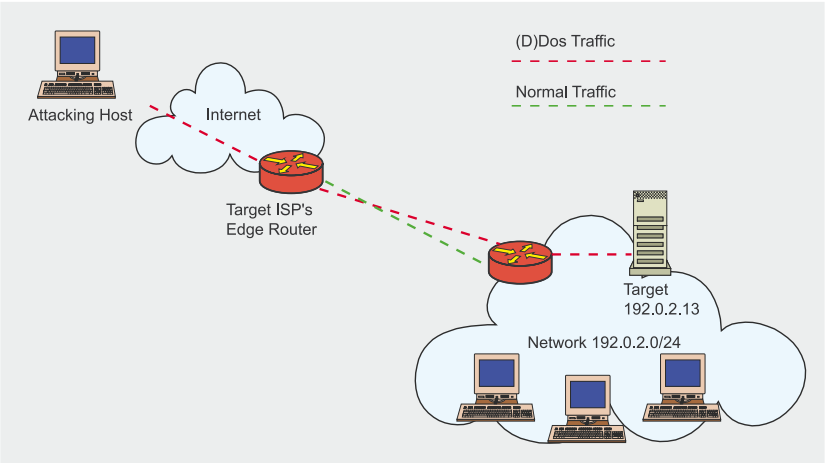

Figura 1. *Ataque a la dirección IP 192.0.2.13 (antes del sinkholing)*

de denegación-de-servicio en una red de gran tamaño.

Antecedentes y Funcionamiento

En este texto, el término *sinkhole* puede definirse como un medio generalizado de redireccionar el tráfico de red de un IP específico debido a diferentes razones relacionadas con la seguridad, dentro de las que se incluyen el análisis forense, la diversificación de ataques y la detección de actividades anómalas. Tier-1 ISPs fueron los primeros en poner en práctica estas tácticas, generalmente para proteger a sus receptores. Desde entonces, se han adaptado las técnicas para recoger información de interés relacionada con las amenazas en la red, a fin de realizar análisis de seguridad. Para visualizar la forma más simple de sinkhole, ten en cuenta lo siguiente:

Un tráfico malintencionado y perjudicial proveniente de diversas redes tiene como destino la red 192.0.2.13, como se muestra en la Figura 1. La organización que es objeto o blanco de este tráfico utiliza la 192.0.2.0/24 como su bloque de dirección de red que es enrutada por su flujo ISP ascendente. El ataque que se hace débil interrumpe las operaciones de negocio de la organización blanco e incrementa potencialmente sus costos debido al aumento del uso de la amplitud de banda y la necesidad de acción por parte del ISP debido a que la cantidad abrumadora de tráfico generado por el ataque perjudica a los clientes adyacentes, como una forma de daño colateral.

El ISP reacciona e inicia temporalmente un tipo de sinkhole en forma de agujero negro inyectando una ruta más específica para el objeto o blanco (192.0.2.13/32) dentro de su segmento principal, cuyo próximo salto es la interfaz de desechos en su router edge (también conocido como el *null0* o el *bit bucket*), como se muestra en la en Figura 2.

Esta táctica redirecciona el tráfico ofensivo hacia el sinkhole del ISP en lugar de permitirle llegar al blanco u objeto original. Lo beneficioso se manifiesta desde el mismo momento en que el sinkhole surte efecto, es muy probable que los clientes adyacentes del ISP (siempre que el ISP diseñe cuidadosamente sus defensas de sinkhole) queden libres de daños colaterales y que el blanco del ataque haya recuperado el uso de su conexión de Internet y el acceso local al dispositivo específico que fue objeto del ataque. Desgraciadamente, las direcciones de IP específicas (el dispositivo) que están siendo atacadas no podrán interactuar por Internet con los sistemas remotos hasta tanto no se elimine el sinkhole (probablemente después de que el ataque haya menguado). Obviamente, los servicios originalmente proporcionados por el dispositivo que ha sido atacado pueden ser desplazados a un dispositivo alternativo con una dirección IP diferente, pero habría que tener en cuenta otras consideraciones con respecto a la caducidad del DNS TTL, y así sucesivamente.

Este ejemplo refleja sólo uno de los tipos de sinkhole, conocido normalmente como ISP-induced blackhole route (ruta de agujero negro inducida por el ISP), no obstante, el mismo debería familiarizarte con el concepto para que así podamos explicar los diferentes usos del *sinkhole*.

La utilización de Sinkholes para Desplegar Redes de Señuelo

La utilización de varios tipos de redes de señuelo con el propósito

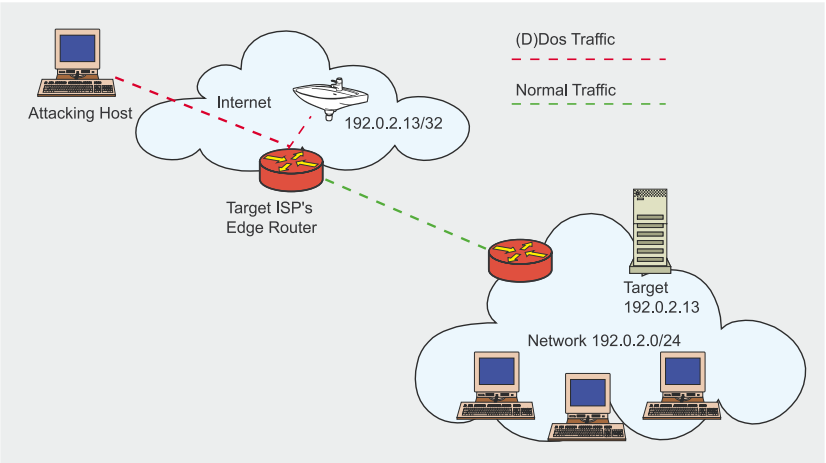

Figura 2. *Ataque a la dirección IP 192.0.2.13 (mientras se realiza el sinkhole)*

Listado 1. *Un ejemplo de la configuración del BGB*

```
router bgp XXX
redistribute static route-map static-to-bgp
# Route-map is a policy mechanism to
# allow modification of prefix attributes, or special
# filtering policies
route-map static-to-bgp permit 10
match tag 199
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
```

Listado 2. *La configuración básica por parte del ISP*

```
router bgp XXX
# Route-map is simply a policy mechanism
# to massage routing information such
# as setting the next hop
neighbor < customer-ip >
 route-map customer-in in
# prefix-list is a static list of customer
#prefixes and mask length that
# are allowed.
#Customer should be allowed to
# announce down to a single host
# in their prefix(es) such as 172.16.0.1/32
neighbor < customer-ip > prefix-list 10 in
# ebgp-multihop is necessary to prevent
# continuous prefix announcement and
# withdrawal
neighbor < customer-ip > ebgp-multihop 2
# Now we define the
#route-map for policy match
# and setting the blackhole
# next hop
route-map in-customer permit 5
# the customer sets
#this community on their side,
# and the ISP matches on its
# side.  XXXX  would likely be
#the customer ASN,
# and NNNN is an arbitrary number agreed
# on by the ISP and the customer
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

de entrampar, exponer, y acopiar información valiosa constituye una forma más novedosa de emplear los sinkholes.

Un señuelo es algo que conduce a una trampa, un cebo que engaña y conduce al peligro, al poder del enemigo, actuando como carnada.

Los dos tipos de redes de señuelo que analizaremos en detalle son la darknet (red oscura) y la honeynet (red de miel). Ambas son útiles para recopilar información valiosa relacionada con asuntos de seguridad, pero una de ellas es particularmente útil en el campo de la ingeniería de redes seguras.

El Despliegue de las Darknets

En general, una darknet (red oscura) es una porción de un espacio IP asignado y enrutado donde no reside ningún servicio sensible. Tales redes se clasifican de *oscuras* porque aparentemente no hay nada *encendido* en ellas. Sin embargo, una red oscura (darknet) de hecho incluye por lo menos un servidor, diseñado para actuar como un vacío de paquete. Este servidor recoge y organiza los paquetes que entran en la red oscura, y son útiles para los análisis a tiempo real o para el análisis forense de la red posterior al evento.

Cualquier paquete que entra en una red oscura es inesperado. Puesto que ningún paquete legítimo debe aparecer dentro de una red oscura, aquellos que llegan lo hacen debido a algún error de configuración, o por la causa más frecuente, que es que haya sido enviado por software maligno. Este software maligno, en su búsqueda de dispositivos vulnerables, enviará paquetes hacia el interior de la red oscura, y por tanto, se expondrá a las revisiones de seguridad administrativas. Hay un enfoque ingenioso en este método para encontrar gusanos y otros softwares malignos de propagación. Sin falsos positivos, y sin firmas o instrumentos complicados de análisis estadísticos, un administrador de seguridad con redes oscuras empleadas correctamente puede detectar las exploraciones (intentos llevados a cabo por softwares malignos con el fin de descubrir receptores adyacentes convenientes para la propagación) en redes de cualquier tamaño. Ésa es una herramienta de seguridad poderosa. Además, los paquetes que llegan a la darknet revelan configuraciones erróneas de redes que son inofensivas y cuya eliminación agradecerán los administradores de redes. Por supuesto, las darknets tienen usos múltiples en el terreno de la seguridad. Pueden usarse para albergar a los recaudadores de flujo, a los detectores de backscatter (o dispersión inicial), a los rastreadores de paquetes y a los sistemas de detección de intrusión. La elegancia de la darknet o red oscura es que reduce considerablemente los positivos falsos de cualquier dispositivo o tecnología mediante una simple reducción del tráfico.

La puesta en funcionamiento de un darknet o red oscura es relati-

prenumerata

hakin9

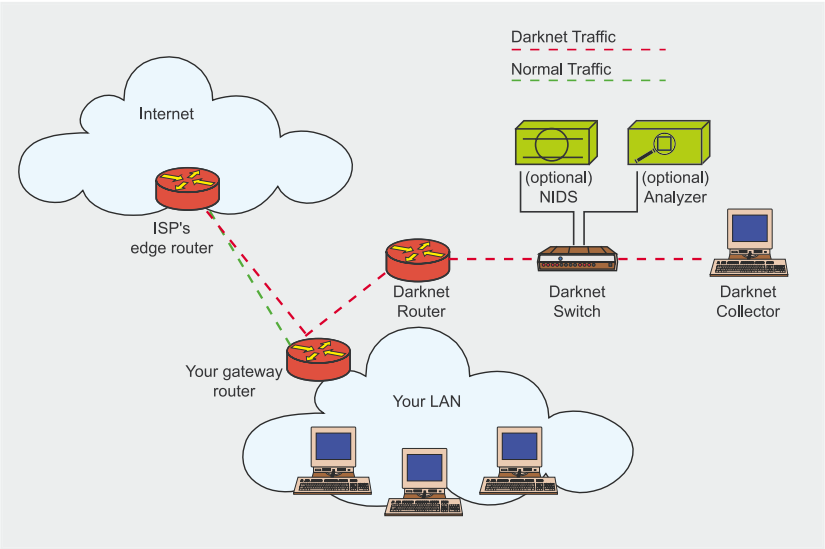

Figura 3. *Topología física de referencia para las redes oscuras o darknets*

vamente sencilla. De hecho, aquí tienes cinco pasos fáciles.

Seleccione una o más regiones inutilizadas en los espacios de las direcciones IP de su red, que enrutarás con su red oscura o darknet. Esta podría ser un prefijo /16 o mayor de las direcciones, o por lo contrario reducirse a una dirección única (/32). Una mayor cantidad de direcciones propiciará una percepción más exacta desde el punto de vista estadístico de la actividad de red no solicitada. Yo recomiendo seleccionar, por ejemplo, varios segmentos de direcciones, tales como un /29 de cada una de las diferentes redes internas, y un /25 de su asignación de red pública (externa). No existe razón alguna por la que no puedas hacer una darknet en una región de su espacio interno de dirección privada (por ejemplo, espacio RFC 1918, 10.0.0.0/8). De hecho, si seleccionas regiones de tu red interna para convertirlas en darknet o redes oscuras, podrás observar sondeos o exploraciones internas que podrían dejarse de ver si solamente creas redes oscuras en los segmentos de redes externas (públicas). Otra estrategia que puede tenerse en cuenta en las organizaciones que utilizan un enrutado específico para sus redes internas, es apoyarse en la regla de enrutamiento que plantea que *la ruta más específica es la vencedora* (usualmente se distribuye a través de algún tipo de protocolo de pasarela interior). Esto quiere decir que si utilizo las redes 10.1.1.0/24 y 10.2.1.0/24 internamente, puedo enrutar sencillamente la red 10.0.0.0/8 por completo hacia mi darknet. Entonces sé que si mi red está configurada adecuadamente, la darknet recibirá todo el tráfico de la 10.0.0.0/8, salvo las redes dentro de esta que estoy enrutando/utilizando de manera específica (las cuales probablemente tienen entradas de enrutamiento estáticas en mi infraestructura de red).

El próximo paso sería la configuración de la topología física. Necesitarás un enrutador o conmutador (layer-3) que remitirá el tráfico a tu darknet, un servidor con una amplia capacidad de almacenamiento para servir como recolector de datos, y un conmutador de Ethernet que usarás en el futuro para conectar estos componentes y los componentes opcionales, tales como un sensor de IDS o un analizador de protocolo. Como enrutador puedes elegir el uso de un dispositivo de pasarela existente, ya sea interno o externo (o ambos, aunque no es recomendable) – La mayoría de las redes oscuras de las empresas, a diferencia de las darknets de los soportes de telecom, se localizan dentro de uno de los DMZs de la organización y se encuentran separadas del resto de la red. Por consiguiente, podrías tener en cuenta para realizar este trabajo el uso de un firewall en lugar de uno de tus enrutadores. No obstante, nuestra recomendación es que utilices su enrutador de pasarela externo para las darknets o redes oscuras externas, y un conmutador interno layer-3 para tus darknets internas. En cualquier caso, lo más importante a tener en cuenta es que configurarás este dispositivo de enrutamiento para remitir el tráfico destinado a la darknet que este recibe desde fuera de una interfaz ethernet dedicada a la darknet (a través del conmutador), hacia el servidor recolector que configurarás para que acepte dichos paquetes. El servidor recolector también debe tener una interfaz dedicada a la darknet que recibirá esos paquetes. Para la administración, el servidor recolector también necesitará por lo menos una interfaz de Ethernet adicional (que será ubicada en una LAN de administración separada). Asegúrese de emplear sus propias y mejores prácticas para la seguridad de los dispositivos de red, pues le garantizamos que muy pronto todo tipo de cosas desagradables fluirán por este segmento de red. Controla el impulso de utilizar rápidamente un conmutador DMZ existente con el propósito de conectar estos componentes, a menos que puedas configurar adecuadamente la VLAN de manera que ningún paquete de transmisión logre llegar a la red oscura o darknet. —recuerda que la darknet es sólo para el trafico ilegítimo, por tanto no es conveniente que las trasmisiones correctas provenientes de tus otras LAN invadan el territorio de la red oscura. La Figura 3 ilustra un ejemplo de esta configuración. En nuestros ejemplos empleamos un enrutador o conmutador ejecutando el Cisco IOS con una licencia de programa layer-3, un servidor FreeBSD-based, y un interruptor layer-2 no administrado para conectar los dispositivos.

A fin de que nuestro servidor recolector evite el protocolo de resolución de direcciones (ARP) para cada dirección en el espacio de la darknet, configuraremos el enrutador para

que remita el tráfico destinado a la darknet hacia una única dirección IP final en la interfaz de Ethernet del servidor para la red oscura. Para lograr esto, sugerimos dedicar un /30 de red como el 192.0.2.0/30 para el recorrido entre el enrutador y la interfaz de la darknet. Esto haría que la interfaz Ethernet de su enrutador fuese la 192.0.2.1/30 y podría llegarse al servidor recolector vía la 192.0.2.2/30. La configuración de la interfaz depende en gran medida de las plataformas que has seleccionado, por tanto nosotros asumiremos que estás en condiciones de hacerlo por tu cuenta. En nuestros ejemplos, estamos usando el Cisco IOS con la licencia de software del layer-3. Una vez se haya realizado esto, simplemente introducirás las declaraciones de enrutamiento adecuadas en el conmutador para que remita todo el tráfico de su red oscura o darknet a la 192.0.2.2 en el servidor colector, y ya estás fuera de peligro:

```
router#conf t
router(config)# ip route 10.0.0.0 ←
255.0.0.0 192.0.2.2
router(config)# ^Z
router# wr
```

Ya debes estar recibiendo el tráfico de la red oscura o darknet. Un ejemplo de la topología lógica se muestra en la Figura 4.

Qué hacer con el tráfico una vez que este llegue allí es otra historia. El servidor debe configurarse para que no responda a ningún dato que reciba en su interfaz de red oscura. Por supuesto, llevará a cabo un protocolo de resolución de direcciones (ARP) para tu dirección configurada (solamente la 192.0.2.2/30) con el fin de establecer comunicación con el enrutador, no obstante, todos los otros paquetes deben ser desechados por algún tipo de firewall en el dispositivo local. Como decía con anterioridad, no debe existir ningún tipo de administración en la interfaz de la darknet, deberás configurar otra interfaz de Ethernet en la que llevarás a cabo las funciones de administración y gestión. La ruta predeterminada para el sistema debe ser la pasarela de la interfaz de administración. En cuanto al firewall necesario, tu selección de plataforma del servidor tendrá que ver con la selección del firewall, pero recomendamos que emplee un sistema basado en BSD y en pf, o un ipfw2 como firewall. Si debe habilitarse o no un loggin para su firewall dependerá en gran medida del uso que le vayas a dar. Nosotros utilizamos herramientas de análisis de archivos de registro que exigen un loggin para activarse (de manera que los registros puedan ser analizados sintácticamente y se generen las alertas) Sin embargo, en dependencia de las diferentes elecciones de software y hardware, y del tamaño de su red oscura o darknet, este logging puede degradar seriamente la eficacia de la darknet. Como medida de seguridad adicional (los firewalls pueden dañarse o apagarse accidentalmente) sería buena idea anular la ruta del tráfico de la darknet en caso de que accidentalmente este no sea filtrado. Un ejemplo de anulación de ruta según FreeBSD podría ser este:

```
route add -net 10.0.0.0/8 ←
127.0.0.1-blackhole
```

Ahora que tu darknet está funcionando y ya has protegido su servidor recolector de la darknet, necesitas guardar los datos en un formato útil para el análisis y las herramientas forenses. La opción más obvia serían los archivos binarios formateados para pcap (capturar paquetes) pues son prácticamente ubicuos y la mayoría de las aplicaciones de análisis de red pueden operar en ellos. La manera más fácil de hacerlo de forma continuada es mediante el uso de la opción de rotación incorporada del programa tcddump. El programa tcpdump es proporcionado por el Grupo de Investigación de Red del Lawrence Berkeley National laboratory. Según nuestra opinión el siguiente es un ejemplo de la fórmula del comando del tcddump para lograr la rotación del registro:

```
tcpdump -i en0 -n -w darknet_dump -C125
```

En este ejemplo, se le ordena al tcpdump escuchar en la interfaz en0, la resolución (DNS) número-a-nombre se desactiva, y un archivo nombrado darknet_dumpN se escribe por cada 125 millones de bytes asignados, donde N se incrementa para que los nombres de los archivos sean únicos. Repetimos, esto proporcionará un archivo binario formateado para pcap que contiene el tráfico de la red. Luego podrás usar este archivo como entrada en tus softwares favoritos de análisis de red. La idea aquí es guardar una copia de los datos

Listado 3. *La configuración básica del cliente*

```
router bgp XXXX (customer's ASN)
# the customer will install a static route,
# which is redistributed into BGP
# hereredistribute static route-map
# static-to-bgp
# just like the ISP, use a
# route-map to set
# and match specific prefix
# attributes
route-map static-to-bgp permit 5
# match the arbitrary tag,
# agreed on by the customer and the ISP
match tag NNNN
set community additive
# XXX:NNNN
# NNNN is the tag, agreed on
# by the customer and the ISP
ip route 192.168.0.1 255.255.255.255
Null0 tag NNNN
```

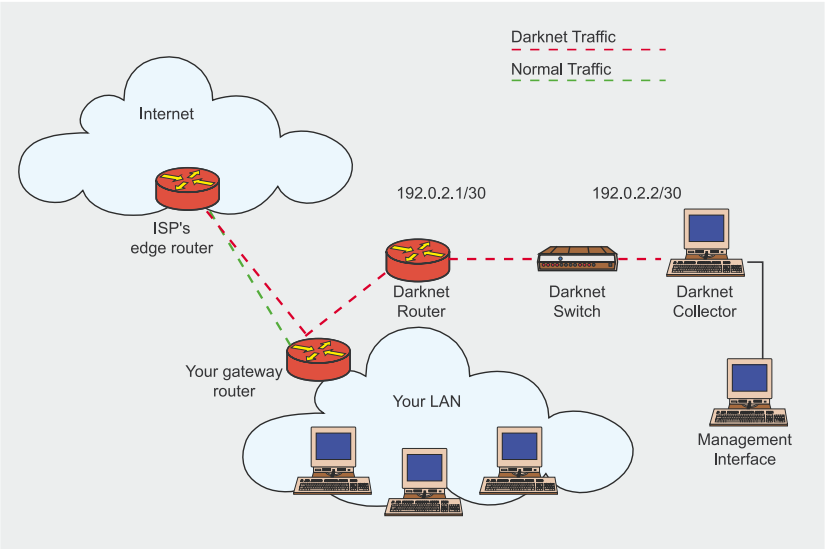

Figure 4. *Una referencia de topología lógica para las redes oscuras*

y utilizar abundantes herramientas diferentes para reproducir los archivos posteriormente, en busca de características interesantes del tráfico. En condiciones normales, emplearías un programa como el tcpdump con una expresión especifica de BPF (filtro de paquete Berkeley) para buscar cosas dentro de estos archivos. A pesar de que esto puede hacerse en tiempo real (tiempo de captura), si guardas un registro de todo el trafico, podrás utilizar diferentes herramientas con posterioridad sin correr el riesgo de perder algo importante.

Otras herramientas útiles que facilitan la visualización de flujos de tráfico son el Argus, la red *Audit Record Generation* (Generación de datos de auditoria) y el Sistema de Utilización, creadas por QoSient. Aunque su configuración es demasiado compleja para explicarla aquí, nosotros utilizamos normalmente el Argus para observar flujos interesantes en nuestras redes oscuras o darknets. El Argus proporciona una aguda interfaz de resumen basada en el flujo que debe ayudarlo a entender con exactitud lo que sucede con respecto a los flujos de tráfico maligno.

Para visualizar el volumen de tráfico que entra en tu darknet, podrías apoyarte en herramientas de interfaz basadas en un contador, tales como el MRTG (vea *http://www.mrtg.org /*) de Tobias Oetiker. El MRTG puede ayudarle a crear bonitos gráficos desde un tráfico de darknet no tan bello. Existen también docenas de herramientas accesibles útiles para analizar los registros del firewall que pueden constituir alternativas rápidas y fáciles a las herramientas de análisis más complicadas como las basadas en pcap o el Argus. Ten presente los problemas de funcionamiento que afrontarás con el logging basado en el texto del filtro del paquete y subsecuentemente con el análisis de dichos archivos.

Literalmente existen docenas de herramientas que se pueden utilizar en tu red oscura. Para comenzar, esto es lo que encontrarías en alguna de las nuestras:

- Un sensor IDS (Bro, Snort, et al.)
- Un rastreador del paquete (el tcpdump descrito con anterioridad)
- Un analizador de flujo (argus, exportador de flujo de red desde el enrutador, SiLK, herramientas de flujo)
- Un analizador sintáctico de archivos de registro del firewall que puebla las bases de datos RRD para los gráficos
- El MRTG y los contadores de tráfico de gráficos
- El p0f (de Michal Zalewski) para categorizar plataformas de dispositivos infectados/contaminadores.

El Despliegue de las Honeynets

Al igual que las redes oscuras o darknets, la honeynet es en general una porción de un espacio enrutado con una IP designada. Ahora bien, en lugar de proporcionar un destino donde los paquetes van a morir, este destino imita un servicio real (o muchos servicios), y por tanto permite que ocurra la conexión (el apretón de manos) y se establezca un diálogo bidireccional completo. Una honeypot, o esta imitación del sistema de un servicio real, debe ser un recurso bien sostenido y cons-

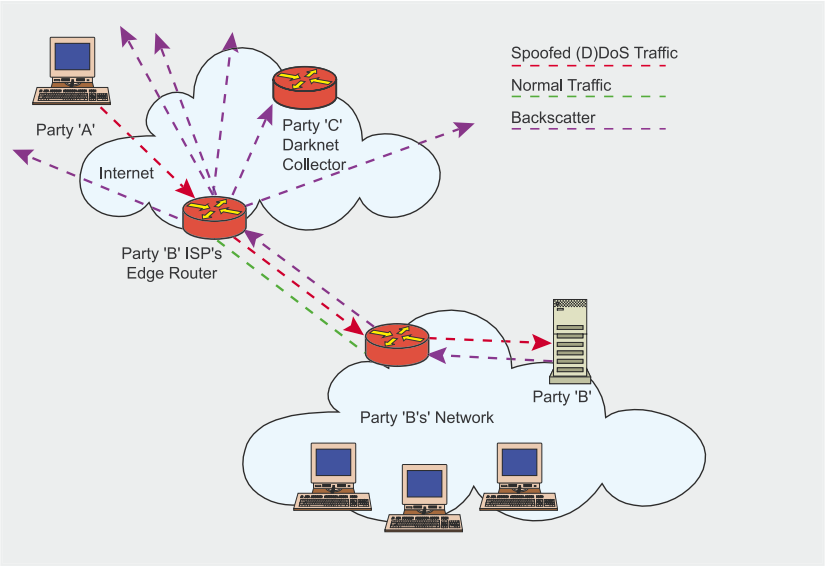

Figura 5. *Un ejemplo de backscatter durante un ataque de DDoS*

tantemente monitoreado que tenga como objetivo atraer atacantes para sondearlos y/o infiltrarlos. A pesar de que existen varios tipos de honeypots, todos persiguen la misma meta: aprender las tácticas del atacante y obtener la mayor cantidad de información posible sobre este.

Las Honeypots Físicas

Las honeypots físicas son máquinas completas dentro de la honeynet o red de miel con su propia dirección IP, con un sistema operativo y herramientas de imitación de servicios.

Las Honeypots Virtuales

Las honeypots virtuales son sistemas de programas de honeypots simulados dentro de la red de miel o honeynet que simulan condiciones de entorno tales como el sistema operativo, la pila de red, y los servicios brindados como señuelos. Un servidor físico puede proporcionar una red de miles de honeypots virtuales.

Las Honeypots de Baja Interacción

Las honeypots de interacción baja (las que más se utilizan en la actualidad) se diseñan para atraer a un atacante con una o más vulnerabilidades aparentemente explotables, establecer el diálogo, y capturar los primeros paquetes de comunicación con el atacante. Obviamente, el atacante o el software maligno autónomo que está conversando con la honeypot en algún momento se dará cuenta de que su blanco u objetivo es imposible de explotar, no obstante, antes de que eso ocurra puede quedar expuesta alguna información valiosa, léase la táctica de explotación o la firma del software maligno. Estas honeypots de baja interacción se emplean en la actualidad como modelo para las tácticas de contaminadores (spammers) (por ejemplo, el intento de derivar las heurísticas tales como las características de temporización de las transacciones SMTP de los contaminadores).

En general, existen muy pocas aplicaciones comerciales de la tecnología de la honeynet, pero la aplicación más popular se encuentra en el proyecto de fuente abierta, honeyd, de Niels Provos. Puede encontrarse más información sobre la adquisición y la instalación del honeyd en *http://www.honeyd.org*.

Datos de interés: el honeyd está diseñado para ser un honeypot/ honeynet virtual que puede simular varios sistemas operativos diferentes y componentes de software convenientes para atraer a los atacantes. Otra forma de honeypot de baja interacción que merece ser mencionada es un concepto novedoso de Tom Liston llamado LaBrea. LaBrea (llamado así por el hoyo de alquitrán) es un software demonio (servicio) que es capaz de generar respuestas autónomas a las solicitudes de conexión a través de bloques potencialmente enormes de direcciones IP. Para abreviar, crea un ambiente atractivo para el software maligno de contaminación/ propagación, pero cuenta con un truco sucio. En cuanto dicho software intenta conectarse, LaBrea retrasa, en ocasiones considerablemente, la pila de la red del remitente. Hablando en sentido figurado, la pila de la red del sistema infectado por el software maligno se queda atascada en un hoyo de alquitrán. Por tanto, no existe ninguna interacción en la capa o en el nivel de la aplicación, pero sí existe una interacción significativa en la capa 4 cuando la conexión (TCP) intenta producirse. LaBrea incluso es capaz de llevar a cabo el ARP para todas las direcciones IP virtuales que hay en su configuración sin asignarlas a las interfaces del sistema anfitrión, lo que facilita extremadamente su instalación. Puede encontrar más información sobre LaBrea en *http://labrea.sourceforge.net/labrea-info.html*.

Nota: varias agencias de investigación han llegado a la conclusión de que las honeypots de baja interacción son una táctica viable contra los gusanos de alta propagación retardándolos con el fin de proteger la infraestructura de la red. Nosotros postulamos que la configuración necesaria para lograr este beneficio es cuanto menos obtusa. No obstante, tanto LaBrea como el honeyd pueden configurarse para crear este tipo de entorno hostil para el gusano.

Las Honeypots de Interacción Alta

Las honeypots de interacción alta son menos utilizadas, pero son sumamente valiosas. El honeypot de interacción alta está diseñado para permitir que el ataque se infiltre completamente en el sistema en que reside en lugar de capturar únicamente las primeras transacciones en el diálogo entre el atacante y el honeypot. En este caso, la información que se recoge no solo incluye las técnicas de sondeo y de explotación empleadas sino que también permitirá al administrador de seguridad observar al atacante una que vez que este gane acceso al sistema y exponga de manera inconsciente sus intenciones y herramientas.

Existe una organización sin fines lucrativos conocida como The Honeynet Project (vea *http://www.honeynet.org/*) que proporciona bastante información y algunas herramientas fáciles de poner en práctica, diseñadas para permitirle al usuario la utilización de los honeypots de interacción alta. También ofrece excelentes herramientas de tipo forense para analizar los datos recogidos durante las infiltraciones en los honeypots.

Datos de interés: The Honeynet Project (*http://www.honeynet.org/*) publica varias herramientas fantásticas que puedes emplear en la utilización de tus propias honeynets. Recomendamos que prestes especial atención a las herramientas Honeywall, Termlog, y Sebek. Igualmente, el equipo del proyecto también ha escrito un libro excelente sobre la psicología, las tácticas, y las herramientas usadas por los atacantes de la manera en que se observan a través de las tecnologías de la honeynet. El libro titulado Know Your Enemy (Conoce a Tu Enemigo) que en este momento está en su segunda edición, se encuentra disponible en el sitio web de *honeynet.org*,

Tabla 1. *Los Paquetes ICMP*

Paquetes ICMP	Descripción
3.0	Red inalcanzable
3.1	Host inalcanzable
3.3	Puerto inalcanzable
3.4	Se requiere fragmentación
3.5	Fallo en la ruta de origen
3.6	Error desconocido de la red de destino
3.7	Error desconocido del host de destino
3.10	Prohibición administrativa del Host
3.11	Tipo de servicio de red inalcanzable
3.12	Tipo de servicio de host inalcanzable
3.13	Prohibición administrativa de comunicación
11.0	TTL expiró durante el tránsito
11.1	Se excedió el tiempo de desfragmentación

Paquetes de TCP	Descripción
RST bit set	Restablecimiento de TCP

y los beneficios que se obtienen de su venta se usan como parte de los fondos para las investigaciones del honeynet.

Recomendaciones para la utilización de las Honeynets

Para aquellas organizaciones, o aquellos que dispongan de dinero y tiempo de sobra (¿conoces a alguien?), las honeypots pueden ser una herramienta inestimable, no obstante, nosotros no recomendamos el uso de las honeypots de manera cotidiana dentro de la empresa. Sin embargo, a pesar de que no es conveniente para el uso cotidiano, cuando un software malintencionado, aparentemente inofensivo, muestra sus garras y ninguna herramienta olfateadora o forense contribuye a identificar el problema de manera que su administrador pueda resolverlo, puede utilizarse el honeynet de manera puntual con el fin de establecer la comunicación mostrándose como un blanco para este software, y por consiguiente se expondrá la información suficiente para identificar el ataque adecuadamente. Otro uso puntual que se le puede dar es como un medio para verificar una infiltración sospechosa. Por tanto, la honeynet debe ser otra flecha en la aljaba del administrador de seguridad.

Una de las puestas en práctica del honeynet que vale la pena mencionar está en uno de los principales productores de chips del mundo. Ellos tienen, en toda su red, servidores de Linux que usan VMWare, encima de los que se ejecutan cuatro máquinas virtuales, una máquina para cada una de las variedades de OS de Windows comunes en la empresa —NT, 2000, 2003, y XP. Cada una se mantiene actualizada según los niveles de ajuste estándares de la corporación. El Linux OS monitorea el tráfico y los cambios a fin de detectar gusanos nuevos (u otras amenazas) que podrían circular en la compañía. Fundamentalmente usan este entorno como una combinación de honeynet e IDS para los gusanos. Podrás encontrar más información sobre esta aplicación en *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*

La puesta en práctica de los Sinkholes para defenderse contra los ataques DDoS (Blackhole Routing)

Otra utilización novedosa de la tecnología de los *Sinkholes* es como una táctica de defensa contra los ataques de denegación de servicio (distribuidos). En la sección anterior de este artículo sobre *Antecedentes y Funcionamiento*, el primer ejemplo que se dio fue la manera más sencilla que adopta esta técnica de enrutado de black-hole (agujero negro). Una vez identificado el blanco de un ataque, la dirección IP objeto del ataque era desviada hacia la interfaz de desecho hacia el límite de la red, antes de cruzar el vínculo final hacia el blanco. Esto liberaba a la red objeto o blanco de una ruptura total por saturación de vínculos, pero aún así probablemente impactaba en el funcionamiento de toda la red, especialmente de los clientes adyacentes que compartían algunas de las topologías de soporte edge con la red atacada. En la actualidad, los principales soportes de telecom han diseñado sus redes y han incluido versiones sofisticadas de este medida de defensa como parte de su filosofía de diseño para la red en general. En muchos casos, los soportes pueden utilizar una técnica de rastreo para localizar los puntos de ingreso del ataque y emplear el blakhole para los paquetes malignos allí (justo en los puntos de ingreso) en lugar de permitir que el ataque obstruya la columna vertebral del soporte y la recorra hasta llegar al vínculo de red objeto del ataque. Esta técnica de rastreo es en gran parte innecesaria puesto que las rutas de blackhole de los soportes suelen anunciarse habitualmente en toda la red entre sus enrutadores edge mediante una comunidad BGP; de ese modo, envían al blackhole el tráfico maligno en cada punto de ingreso, lo que les permite conducir los ataques al blackhole en la medida en que estos penetran y en muchos casos evitar la congestión de la columna vertebral y del edge al mismo tiempo. Algunos han ampliado incluso el control y la automatización de esta capacidad hacia el cliente final mediante lo que se conoce como blackholes a tiempo real activados por el cliente (customer-triggered real-time blackholes).

Tabla 2. *Gráfico de Resumen*

Pasos	Descripción
Comprende cómo tu ISP puede ayudarte durante un ataque de DDoS	Traza un plan de acción para enfrentar ataques de DDoS con estrategias que incrementen la capacidas de de tu IP en el área de enrutados de blackhole a tiempo real. Establece un diálogo entre tu organización y tu ISP a fin de que este le permita crear blackholes a tiempo real activados por el cliente para que se proteja, sin tener que desperdiciar tiempo valioso en sus procedimientos de escalado.
Ten en cuenta la puesta en práctica de una darknet interna	Recuerda que una darknet interna te facilita atrapar los gusanos con mayor prontitud que tu antivirus. Igualmente, esto expone configuraciones de red erróneas que te gustaría conocer
Ten en cuenta la puesta en práctica de una darknet externa	Las darknets externas pueden proporcionarte información sobre lo que está atacando tu red desde el exterior y la herramientas que se emplean pueden resultarte más fácil a la vista que las de un registro de firewall estándar. El backscatter que se recoge de una darknet externa puede proporcionarte información sobre el momento en que tu red está siendo implicada en un ataque a una tercera parte.
Explora la posibilidad de poner en práctica los honeypots con fines investigadores si dispones de tiempo y recursos.	Aunque la mayoría de las organizaciones no aprecian la implementación de una honeynet como un beneficio importante (más allá de la alerta), ésta es inestimable para los investigadores de la seguridad de la información. Considere lo que implica poner en práctica una honeynet en su organización. Al hacerlo, incluya la exploración de las leyes estatales que pueden influenciar en su determinación.

El Enrutado de Blackhole Activado

Como se ha dicho con anterioridad, la mayoría de los ISPs principales han puesto en práctica un sistema distribuido automatizado para *activar* los enrutados de blackhole en las direcciones IP que son blanco de ataques. Esta activación puede ser iniciada por el ISP o por el cliente, de forma manual o mecánica. El enrutado de blackhole activado utiliza el sinkhole sencillo que se describió con anterioridad en la sección *Antecedentes y Funcionamiento*. El sinkhole puede configurarse en todos los enrutadores de ingreso (edge) dentro de la red ISP, en la que el ISP intercambia tráfico con otros proveedores o clientes. Cuando se identifica un ataque contra un blanco de la red, el ISP o el cliente pueden anunciar el prefijo *atacado* (o un prefijo más específico) en la mesa de enrutado del BGP. El prefijo atacado se rotula con un next-hop que se enruta estáticamente hacia la interfaz de desecho de todos los enrutadores edge, y se propaga dentro de la red ISP a través de un BGP interno (iBGP). Por tanto, siempre que los paquetes destinados para el prefijo atacado penetran la red ISP (el punto del ingreso), se les envían inmediatamente a la interfaz de desecho en el enrutador más cercano anunciando el prefijo atacado.

Para que el ISP ponga en práctica el mecanismo de blackhole distribuido deben seguirse los siguientes pasos:

- Selecciona un prefijo que no esté enrutado globalmente, como el Test-Net (RFC 3330) 192.0.2.0/24, para que se utilice como next hop de cualquier prefijo atacado, que será enviado al blackhole. El uso de un prefijo de longitud 24 te permite utilizar muchas direcciones IP diferentes para tipos específicos de enrutado de blackhole. Tal vez quieras diferenciar las rutas de blackhole que utilizas para el cliente, de las internas y de las externas.
- Configura una ruta estática en cada enrutador de ingreso/escutrinio para la 192.0.2.0/24, que señale a la interfaz de desecho. Por ejemplo: ruta ip192.0.2.0 255.255.255.0 Null0
- Configure el BGP y las políticas de los mapas de ruta para que anuncien el prefijo que debe ser enviado al blackhole como se indica en el Listado 1

En la configuración del ejemplo, estamos redistribuyendo las rutas estáticas en el BGP que se corresponden o igualan al *código199* (ver más adelante), estableciendo el next hop en una dirección IP que está enrutada hacia la interfaz de desecho, estableciendo la preferencia local en 50 (el menos preferido), y asegurándonos así de que estas rutas no se infiltrarán en ninguno de nuestros pares externos (sin exportar).

Una vez realizada esta configuración básica, el ISP puede iniciar la activación estableciendo una ruta estática para que el prefijo atacado (o host) sea conducido al blackhole, por ejemplo:

```
ip route 172.16.0.1 255.255.255.255
192.0.2.1 Null0 tag 199
```

La ruta estática mostrada con anterioridad es el *activador* que inicia el proceso de enrutamiento del blackhole. El router en el que se configura esta ruta le anunciará la misma a todos los enrutadores internos, incluidos los enrutadores edge, a través de un iBGP. Cualquier router con una ruta estática hacia la interfaz de desecho para la 172.16.0.1/32, inmediatamente hará desaparecer el trafico local.

Así mismo, el ISP podría establecer una activación automática a través del BGP, de manera que un cliente de BGP pueda activar la ruta del blackhole, independientemente de la intervención del ISP. Este es el rasgo más poderoso del enrutado activado del blackhole. La configuración del lado del ISP es ligeramente diferente en esas comunidades y se emplea un ebgp-multihop para recibir y etiquetar adecuadamente las rutas que aprenden los clientes. La configuración básica por parte del ISP aparece en el Listado 2.

El ISP ya tiene el <blackhole-ip> enrutado estáticamente para las interfaz de desecho a lo largo de la red, por tanto, tan pronto como el cliente anuncia el prefijo que debe ser conducido al blackhole, el ISP lo redistribuye internamente y el tráfico que viene a este prefijo se conduce al blackhole en el límite de la red ISP.

La configuración básica del cliente aparece en el Listado 3.

Una vez se configure el BGP, el cliente sólo necesita instalar una ruta estática para el prefijo # blanco del ataque. Con alguna configuración muy básica en el BGP, y con la ayuda de su ISP, ahora cuentas con un método muy rápido para responder a los ataques de denegación de servicio contra un host solamente, o contra un prefijo entero.

Nota: Asegúrate de verificar con el servicio técnico de tu ISP antes de llevar a cabo su solución de activación del blackhole, ya que la puesta en práctica de este concepto por parte de los diferentes ISP puede diferir ligeramente.

Los Backscatter y Tracebacks

En esta sección exploraremos algunos usos creativos de las redes de señuelo para detectar ataques y falsificaciones, así como para contribuir a localizar al autor de estos perjuicios.

El Backscatter

Después de todo lo que se ha hablado sobre las redes de señuelo y los ataques DDoS resulta propicio mencionar el concepto de backscatter o dispersión inicial. Durante un semestre entero de mi primer año de universidad, le escribí cartas (sí, de las convencionales) a varios amigos que se mudaban con frecuencia. Como soy muy despistado, a menudo escribía la dirección de devolución equivocada en el sobre. Se me olvidaba poner el número de mi habitación en la beca o lo escribía totalmente ininteligible (ya había descubierto la cerveza). De vez en cuando, alguno de mis amigos a los que había escrito se mudaba y la carta que le había enviado retornaba con una notificación de correo que decía *devolver al remitente*. Pero como mi dirección de devolución era incorrecta la carta no llegaba a mí sino a la oficina de residentes en el piso de abajo. Desde allí me llamaban (identificando mi nombre) para hacerme saber que nuevamente había escrito mal mi dirección y que tenían una carta allí en espera de que la recogiera para reenviarla. Ese *devolver al remitente* es una forma de backscatter o dispersión inicial. Claro, el backscatter indicaba a la oficina de residentes que yo había estado enviando correos (y a quien).

En Internet, cuando una parte A piensa realizar un ataque de denegación-de-servicio contra la parte B, pero la parte A quiere ocultar su identidad, normalmente escribe la dirección de la fuente equivocada en sus paquetes de ataque (los encabezamientos IP se falsifican para que parezca que salieron de las partes A-Z, por ejemplo, sólo de la A-Z en la IPv4 es de 2^{32} permutaciones). Durante tales ataques, los routers y otros dispositivos de red a lo largo del trayecto envían inevitablemente una serie de mensajes que van desde el restablecimiento de la conexión para satisfacer la solicitud hasta las notificaciones inalcanzables. Puesto que estos mensajes son *devueltos al remitente*, y ya que el remitente es falsificado, todas las partes de la A a la Z los reciben, y por tanto conocen del ataque a la parte B, de la misma manera en que la oficina de residentes supo de los correos que yo enviaba. Esto se muestra en la Figura 5.

En la actualidad cuando se trata de filtrar paquetes, la mayoría de estos mensajes del backscatter son desechados silenciosamente por los firewalls porque son vistos como respuestas a mensajes no enviados. No obstante, con una red de darknet externa puesta en práctica de la manera en que explicamos con anterioridad, podemos buscar estos paquetes de backscatter y determinar cuando nuestro espacio de dirección ha sido implicado en un ataque a otra parte. Los siguientes tipos de paquetes que aparezcan en la darknet pueden clasificarse como backscatters e indicar que su (darknet) espacio de dirección está implicándose en un ataque (ver Tabla 1).

El Traceback

Ahora que ya tenemos conocimientos sobre el backscatter explicaremos cómo utilizarlo. Dentro de una red con pasarelas múltiples de tránsito de Internet, resultaría útil localizar los puntos de ingreso de los *paquetes defectuosos* durante un ataque debilitado. Esta técnica, conocida como traceback (rastreo), es válida puesto que una vez que identifiquemos el punto específico de

En la Red

- Extreme Exploits: Advanced Defenses against Hardcore Hacks, publicado por McGraw-Hill/Osborne. Derecho de autor 2005 *http://www.amazon.com/gp/product/0072259558/*
- Internet RFCs 3330 (Special-use IPv4 Addresses) and 3882 (La configuración del BGP para bloquear ataques de denegación de servicio)
- The Team Cymru Darknet Project *http://www.cymru.com/Darknet/*
- The home of tcpdump and libpcap *http://www.tcpdump.org/*
- The home of ARGUS *http://www.qosient.com/argus/flow.htm*
- The home of Honeyd *http://www.honeyd.org*
- The home HoneyNet Project *http://www.honeynet.org*
- The home of the p0f tool *http://lcamtuf.coredump.cx/p0f.shtml*
- Artículo de Chris Morrow y Brian Gemberling sobre el proceso de blackhole del ISP y el análisis del backscatter: *http://www.secsup.org/Tracking/*
- Presentación de Dan Hawrylkiw sobre las honeynets. *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*
- Preguntas más frecuentes acerca del filtro del paquete OpenBSD *http://www.openbsd.org/faq/pf/*

Sobre el autor

Victor Oppleman es un autor consumado, orador y maestro en el campo de la seguridad de las redes y es también asesor de algunas de las compañías más admiradas del mundo. El software de fuente abierta de Oppleman se ha distribuido a centenares de miles de computadoras en todo el mundo y posee las patentes estadounidenses de propiedad intelectual de enrutado adaptativo distribuido y de las aplicaciones inalámbricas del consumidor. La mayoría del contenido de este artículo ha sido extraído del libro del Sr. Oppleman, Extreme Exploits: Advanced Defenses Against Hardcore Hacks, publicado por McGraw-Hill/Osborne (Derechos de autor 2005) que seguramente está disponible en tu librería favorita.

ingreso en nuestra red (o en nuestro ISP), podemos estar en condiciones de disminuir el tráfico allí y reducir la carga en nuestros vínculos, e incluso podemos potencialmente permitir que *el tráfico válido* fluya (a través de pasarelas alternas); a diferencia de la táctica de protección contra el DDoS de blackhole que es más sencilla y que discutimos con anterioridad. El rastreo o Traceback nos permite utilizar el backscatter que recogemos en nuestro(s) darknet(s) como un medio para encontrar el punto donde el ataque está penetrando en la red. Desgraciadamente, esto sólo es viable para ISPs o redes de datos de largo alcance con muchas pasarelas de Internet. Algunas dependencias que van más allá de esta descripción incluyen la utilización del mecanismo de defensa del blackhole en cada pasarela de Internet. Dado que los principales ISPs hacen esto junto a un grupo de redes de compañías globales, resulta adecuado al menos explicar el proceso.

Si asumimos que tu red está configurada en correspondencia a lo anteriormente expuesto, puedes realizar un rastreo (traceback) en medio de un ataque de denegación de servicio en tres pasos fáciles:

- Identifica el blanco y verifica que el tráfico del ataque está siendo falsificado (si no es así, está táctica de rastreo será inútil).
- Establece un blackhole para la ruta de los hosts específicos (probablemente los /32s) que son atacados en cada una de sus pasarelas. Se cauteloso y usa las mejores prácticas con respecto a la utilidad de remitir hacia la interfaz de desecho en lugar de usar un filtro de paquetes para reducir los paquetes de ataque. Esta operación de blackhole hará que este router de pasarela comience a generar mensajes de ICPM inalcanzable, los cuales son (intentan ser) devueltos a las fuentes falsificadas de los paquetes de ataque.
- Dentro de tus darknets, utiliza las herramientas de darknet que has colocado para buscar el tráfico de backscatter (probablemente en forma de ICPM inalcanzables) con la dirección IP de tus routers de pasarela en su interior. Cualquier dirección IP de tu pasarela que veas como la fuente de estos paquetes de backscatter confirma que tales pasarelas son realmente el punto de ingreso del tráfico de ataque. Voilá, ha encontrado el lugar donde el ataque está penetrando la red. Aun cuando no tenga configuradas sus herramientas sofisticadas de darknet, una simple lista de acceso aplicada a la interfaz del enrutador puede funcionar, como se describe a continuación:

```
access-list 105 permit icmp any any unreachables log; access-list 105 permit ip any any
```

Por tanto, si accedes al modo de monitoreo terminal en esta lista de acceso (o si simplemente reduces el registro), conseguirás un informe pobre del backscatter, el que podrás estudiar para encontrar las direcciones IP de sus pasarelas. La táctica de traceback o rastreo y la defensa de blackhole contra los ataques de DDoS son útiles en situaciones donde las inundaciones de tráfico maligno han falsificado los encabezados. Ahora bien, con la proliferación de máquinas zombis y botnets, muchos atacantes han dejado de falsificar los paquetes DDoS completamente – no existe razón para falsificar encabezados si su ejercito de sistemas atacantes está por todos lados. De igual manera, los ataques DDoS falsificados han disminuido considerablemente como resultado de una mayor utilización del filtrado de ingreso y de uRPF. ●