6
Seguridad

En una red cableada tradicional, el control del acceso es muy sencillo: si una persona tiene acceso físico a una computadora o a un *hub* (concentrador) de la red, entonces pueden usar (o abusar) de los recursos de la red. Si bien los mecanismos a través de software son un componente importante de la seguridad de la red, el mecanismo decisivo es limitar el acceso físico a los dispositivos de la red. Es simple: si todas las terminales y los componentes de la red son accedidos sólo por personas de confianza, entonces la red puede ser considerada confiable.

Las reglas cambian significativamente en las redes inalámbricas. A pesar de que el alcance aparente de su punto de acceso puede ser de unos pocos cientos de metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso de su red aunque esté a varias manzanas de distancia. Aún cuando un usuario no autorizado sea detectado, es imposible "rastrear el cable" hasta el lugar donde está esa persona. Sin transmitir ni un sólo paquete, un usuario malintencionado puede registrar todos los datos de la red a un disco. Más adelante estos datos pueden utilizarse para lanzar un ataque más sofisticado contra la red. Nunca suponga que las ondas de radio simplemente "se detienen" en el límite de su propiedad.

Por supuesto, aún en las redes cableadas es casi imposible confiar por completo en todos los usuarios de la red. Un empleado descontento, un usuario con poca capacitación, así como una simple equivocación de un usuario honesto pueden causar daño significativo en las operaciones de la red. Como arquitecto de la red, su objetivo debe ser facilitar la comunicación privada entre los usuarios legítimos de la misma. Aunque en una red se necesita una cierta cantidad de control de acceso y de autenticación, habrá fallado en su función si a los usuarios legítimos de la red se les hace difícil utilizarla para comunicarse.

Según un viejo dicho, la única forma de mantener completamente segura una computadora es desenchufarla, ponerla dentro de una caja fuerte, destruir la llave y enterrarla bajo concreto. Si bien dicho sistema puede ser completamente "seguro", no es útil para la comunicación. Cuando tome decisiones de seguridad para su red, recuerde que por encima de todo, la red existe para que los usuarios puedan comunicarse unos con otros. Las consideraciones de seguridad son importantes, pero no deben interponerse en el camino de los usuarios.

Seguridad física

Cuando instala una red, usted está construyendo una infraestructura de la cual la gente dependerá y por lo tanto, la red debe ser confiable. Para la mayoría de los casos, las interrupciones en el servicio ocurren a menudo debido a alteraciones hechas por las personas, accidentalmente o no. Las redes son físicas, son cables y cajas, cosas que pueden ser modificadas fácilmente. En muchas instalaciones, puede ser que la gente no sepa qué tipo de equipamiento se ha instalado, o experimentan por pura curiosidad. Puede que no se den cuenta de la importancia de que un cable llegue a un puerto. Es posible que muevan un cable Ethernet para conectar su computadora portátil durante 5 minutos, o cambien de posición al conmutador porque les estorba. Un enchufe puede ser desconectado de una regleta porque alguien más necesita esa conexión. Asegurar la seguridad física de la instalación es un asunto prioritario. Las señales y las etiquetas le serán útiles a aquellos que saben leer, o que hablan su mismo idioma. Colocar el equipo fuera del camino, y limitar el acceso al mismo es el mejor medio para asegurarse de que no ocurran accidentes o se manipule el equipamiento.

En las economías menos desarrolladas no va a ser fácil encontrar los sujetadores, amarres o cajas apropiados. Sin embargo, podrá encontrar productos eléctricos equivalentes que funcionen igualmente bien. Los cerramientos a la medida también son sencillos de fabricar, y deben considerarse esenciales para cualquier instalación. A menudo es más económico pagar a un albañil para que haga las perforaciones e instale los conductos; a pesar de que ésta puede ser una opción cara en el mundo desarrollado, este tipo de actividad es accesible en los países del Sur. Se puede incrustar tubería de PVC en las paredes de cemento para pasar el cable de una habitación a otra, evitando hacer perforaciones cada vez que tenemos que pasar un cable. Para el aislamiento, se pueden rellenar los conductos alrededor del cable con bolsas de plástico.

El equipamiento pequeño debe montarse en la pared y el grande se debe colocar en un closet o en un armario.

Conmutadores (*switches*)

Los conmutadores, *hubs* o los puntos de acceso interiores pueden atornillarse directamente a la pared. Lo mejor es poner el equipo lo más alto posible para reducir las posibilidades de que alguien toque los dispositivos o sus cables.

Cables

Los cables deben esconderse y atarse. Es mejor enterrarlos que dejarlos colgando en un patio donde puedan ser usados para secar la ropa o simplemente enganchados con una escalera, etc. Para evitar alimañas o insectos consiga conductos plásticos para electricidad. El costo adicional le evitará molestias. Los conductos deben enterrarse aproximadamente a 30 cm de profundidad (o más abajo si el suelo se congela a mayor profundidad en climas extremos). También es recomendable comprar conductos de un calibre superior al mínimo necesario para que en el futuro otros cables que se requieran puedan pasarse por la misma tubería. Cuando se hacen instalaciones en edificios, también es posible encontrar conductos de plástico que pueden ser utilizados para pasar cables. De lo contrario, simplemente sujete los cables a la pared para asegurarse de que no queden expuestos en lugares donde puedan ser enganchados, pinchados o cortados.

Energía

Lo mejor es tener las zapatillas eléctricas (alargues, regletas, múltiples) dentro de un armario cerrado. Si esto no es posible colóquelas debajo de un escritorio o en la pared y utilice cinta adhesiva fuerte para asegurar el enchufe a la conexión de la pared. No deje espacios libres en la zapatilla eléctrica ni en la UPS, tápelas con cinta si es necesario. La gente va a tender a utilizar la conexión que esté más a su alcance, por lo tanto hágalas difíciles de usar. Si no lo hace, puede encontrarse con un ventilador o una lámpara enchufada en su UPS; aunque es bueno tener luz ¡es aún más importante mantener su servidor en funcionamiento!

Agua

Proteja su equipo del agua y de la humedad. En todos los casos asegúrese de que su equipo, incluida su UPS, está al menos a 30cm. del piso para evitar daños por posibles inundaciones. También intente tener una cubierta sobre su equipo, para que de esta forma el agua y la humedad no caigan sobre él. En los climas húmedos es importante que el equipamiento tenga la ventilación adecuada para asegurarse de que se va a eliminar la humedad. Los armarios pequeños deben tener ventilación, o de lo contrario la humedad y el calor pueden degradar o aún destruir su equipamiento.

Mástiles y torres

El equipo instalado en un mástil o torre a menudo está a salvo de los ladrones. No obstante, para disuadirlos y mantener su equipo a salvo del viento es bueno sobre-estructurar estos montajes. Los equipos que se monten sobre la torre o mástil deben pintarse de colores apagados, blanco o gris mate para reflejar el sol, así como para desviar la atención, haciéndolo lucir poco interesante. Las antenas tipo panel son mucho más sutiles que los platos y por eso debemos preferirlas. Todas las instalaciones en las paredes deberán estar a una altura tal, que se requiera de una escalera para alcanzarlas. Intente elegir lugares bien iluminados pero no muy prominentes para poner el equipo. También evite las antenas que se parezcan a las de televisión, porque esas pueden atraer el interés de los ladrones, mientras que una antena WiFi no va a ser de utilidad para la mayoría de ellos.

Amenazas a la red

Una diferencia esencial entre las redes Ehernet y las inalámbricas es que estas últimas se construyen en un ***medio compartido***. Se parecen más a los viejos concentradores de red que a los conmutadores modernos, en ellas cada computadora conectada a la red puede "ver" el tráfico de todos los otros usuarios. Para monitorear todo el tráfico de la red en un punto de acceso, uno puede simplemente sintonizar el canal que se está utilizando, colocar la tarjeta de red en el modo de monitoreo, y registrar cada paquete. Estos datos pueden ser de mucho valor para alguien que los escucha a escondidas (incluyendo datos como el correo electrónico, datos de voz o registros de conversaciones en línea). Esto también puede proveer contraseñas y otros datos de gran valor, posibilitando que la red se vea comprometida en el futuro. Como veremos más adelante en este capítulo, este problema puede mitigarse con el uso de la encriptación.

Otro problema serio de las redes inalámbricas es que los usuarios son relativamente ***anónimos***. Todos los dispositivos inalámbricos incluyen una dirección MAC única, la cual es asignada por el fabricante, pero esas direcciones a menudo pueden ser modificadas con ciertos programas. Aún teniendo la dirección MAC, puede ser muy difícil identificar donde está localizado físicamente un usuario inalámbrico. Los efectos del eco, las antenas de gran ganancia, y una amplia variedad de características de los transmisores de radio, pueden hacer que sea imposible determinar si un usuario malintencionado está en el cuarto de al lado o en un lujar muy alejado.

Si bien el espectro sin licenciamiento implica grandes ahorros económicos para el usuario, por otro lado tiene el desafortunado efecto colateral de que los ataques de ***denegación del servicio*** (***DoS*** *por su sigla en inglés*) son extremadamente simples. Simplemente con encender un punto de acceso

de alta potencia, un teléfono inalámbrico, un transmisor de video, o cualquier otro dispositivo de 2.4 GHz, una persona con malas intenciones puede causar problemas significativos a la red. Muchos dispositivos de red son vulnerables también a otras formas de ataques de denegación del servicio, tales como una avalancha de desasociaciones (*disassociation flooding*) y el desborde de las tablas ARP.

Les presentamos varias categorías de personas que pueden causar problemas a una red inalámbrica:

- ***Usuarios involuntarios.*** Como la mayoría de las redes inalámbricas están instaladas en áreas muy pobladas, es común que los usuarios de computadoras portátiles se asocien accidentalmente a la red equivocada. La mayoría de los clientes va a elegir cualquier red disponible si la de su preferencia no lo está. Los usuarios pueden hacer uso de esta red como lo hacen habitualmente, ignorando completamente que pueden estar transmitiendo datos importantes en la red de alguien más. Las personas malintencionadas pueden aprovechar esta situación instalando puntos de acceso en lugares estratégicos, para intentar atacar usuarios desprevenidos y capturar sus datos.

  El primer paso para evitar este problema es educar a sus usuarios, y subrayar la importancia de conectarse solamente a redes conocidas y de confianza. Muchos clientes inalámbricos pueden configurarse para conectarse solamente a redes confiables, o para pedir permiso antes de incorporarse a una nueva red. Como veremos más adelante en este capítulo los usuarios pueden conectarse de forma segura a redes públicas abiertas utilizando una encriptación fuerte.

- W***ar drivers.*** El fenómeno de los "*war drivers*" (buscadores de redes) basa su nombre en la famosa película sobre piratas informáticos de 1983, "Juegos de Guerra" (*War Games*). Ellos están interesados en encontrar la ubicación física de las redes inalámbricas. En general se mueven por la ciudad equipados con una computadora portátil, un GPS, y una antena omnidireccional, registrando el nombre y la ubicación de cada red que localizan. Luego se combinan esos registros con los de otros buscadores de redes transformándose en mapas gráficos describiendo las "huellas" inalámbricas de una ciudad.

  La amplia mayoría de los buscadores de redes no representa una amenaza directa a la red, pero los datos que recolectan pueden ser de interés para aquellos que se dedican a *atacar* redes. Por ejemplo, un punto de acceso desprotegido detectado de esta manera, puede estar ubicado en un edificio importante, como una oficina de gobierno o de una empresa. Una persona con malas intenciones puede utilizar esta información para acceder a esa red ilegalmente. La instalación de ese AP nunca debió haber sucedido en primer lugar, pero los buscadores de redes hacen más

urgente la solución de este problema. Como veremos más adelante en este capítulo, los buscadores de redes que utilizan el famoso programa NetStumbler pueden ser detectados con otros programas como el Kismet. Para más información acerca de los buscadores de redes, vea los sitios *http://www.wifimaps.com/*, *http://www.nodedb.com/*, o *http://www.netstumbler.com*.

- ***Puntos de acceso deshonestos.*** Hay dos clases generales de puntos de acceso deshonestos: aquellos instalados incorrectamente por usuarios legítimos, y los instalados por gente malintencionada que piensa en recolectar datos o dañar la red. En el caso más sencillo, un usuario legítimo de la red, puede querer una mejor cobertura inalámbrica en su oficina, o puede que encuentre demasiado difíciles de cumplir las restricciones de seguridad de la red inalámbrica corporativa. Al instalar un punto de acceso sin autorización, el usuario abre la red desde el interior de la misma a los ataques potenciales. Si bien existe la posibilidad de rastrear a través de la red puntos de acceso no autorizados, es muy importante tener una política clara que los prohíba.

  Puede que sea muy difícil lidiar con la segunda clase. Al instalar un AP de gran potencia que utilice el mismo ESSID de la red, una persona puede engañar a la gente para que use este equipo y registrar o manipular todos los datos que pasan por él. Repetimos, si sus usuarios están entrenados para usar una fuerte encriptación, este problema se va a reducir de forma significativa.

- ***Escuchas Subrepticias.*** Como mencionamos antes, este es un problema muy difícil de manejar en las redes inalámbricas. Utilizando una herramienta de monitoreo pasiva (como Kismet), un fisgón puede registrar todos los datos de la red desde lejos sin que ni siquiera se note su presencia. Los datos encriptados pobremente simplemente pueden registrarse y luego descifrarse, mientras que los datos sin encriptación se pueden leer fácilmente en tiempo real.

  Si a usted le es difícil convencer a otros de este problema, puede realizar una demostración con herramientas como Etherpeg o Driftnet (*http://www.etherpeg.org/* o *http://www.ex-parrot.com/~chris/driftnet/*). Estas herramientas buscan datos gráficos en redes inalámbricas, tales como archivos GIF y JPEG. Mientras que los usuarios están navegando en Internet, estas herramientas despliegan todos los gráficos encontrados en un collage. A menudo utilizo estas herramientas cuando estoy dando una charla de seguridad inalámbrica. Usted le puede decir a un usuario que su correo electrónico es vulnerable si no tiene encriptación, pero nada les hace llegar mejor el mensaje que mostrarles las imágenes que están buscando en su navegador web. Si bien no puede ser prevenido por completo, el uso de una fuerte encriptación va a desalentar las escuchas ***subrepticias***.

Esta introducción está pensada para darle una idea de los problemas a los que usted tiene que enfrentarse cuando diseña una red inalámbrica. Más adelante, vamos a presentarle herramientas y técnicas que lo ayudarán a mitigarlos.

Autenticación

Antes de tener acceso a los recursos de la red, los usuarios deben ser ***autenticados***. En un mundo ideal, cada usuario inalámbrico debería tener un identificador personal que fuera único, inmodificable e imposible de suplantar por otros usuarios. Este es un problema muy difícil de resolver en el mundo real.

Lo más cercano a tener un identificador único es la dirección MAC. Este es un número de 48-bits asignado por el fabricante a cada dispositivo inalámbrico y Ethernet. Empleando un ***filtro mac*** en nuestro punto de acceso, podemos autentificar a los usuarios mediante su dirección MAC. Con este método el punto de acceso, mantiene una tabla de direcciones MAC aprobadas. Cuando un usuario intenta asociarse a un punto de acceso, la dirección MAC del cliente debe estar en la lista aprobada, o de lo contrario la asociación va a ser rechazada. Como una alternativa, el AP puede tener una tabla de direcciones MAC "prohibidas", y habilitar a todos los dispositivos que no están en esa lista.

Desafortunadamente, este no es un mecanismo de seguridad ideal. Mantener las tablas MAC en cada dispositivo puede ser muy engorroso, requiriendo que todos los dispositivos cliente tengan su dirección MAC grabadas y cargadas en los AP. Además, las direcciones MAC a menudo pueden modificarse mediante software. Si un atacante determinado observa las direcciones MAC que están en uso en una red inalámbrica, él puede "suplantar" una dirección MAC aprobada y asociarse con éxito al AP. A pesar de que el filtro MAC va a evitar que los usuarios involuntarios y los curiosos accedan a la red, el filtro MAC por si solo no puede proteger su red de los atacantes empecinados.

Los filtros MAC son útiles para limitar temporalmente el acceso de usuarios que actúan de forma incorrecta. Por ejemplo, si una computadora portátil tiene un virus que envía grandes cantidades de tráfico no deseado, su dirección MAC puede agregarse a la tabla de filtrado para detener el tráfico de forma inmediata. Esto le dará tiempo para ubicar al usuario y arreglar el problema.

Otra forma popular de autenticación de las redes inalámbricas es la llamada ***red cerrada***. En una red común, los AP transmiten sus ESSID muchas veces por segundo, permitiéndoles a los clientes (así como a las herramientas

como NetStumbler) encontrar la red y mostrar su presencia al usuario. En una red cerrada, el AP no transmite el ESSID, y los usuarios deben conocer el nombre completo de la red antes de que el AP les permita asociarse. Esto evita que los usuarios casuales descubran la red y la seleccionen en su cliente de red inalámbrica.

Con esta característica hay varios inconvenientes. Forzar a los usuarios a escribir el ESSID completo antes de conectarse a la red, amplía las posibilidades de error y a menudo resulta en solicitudes de soporte y quejas. La red no será detectada por herramientas como NetStumbler, y esto puede prevenir que la misma aparezca en los mapas de los *war drivers*. Pero esto también significa que otros instaladores de redes tampoco pueden encontrar su red con facilidad, y no van a saber que usted está usando un canal dado. Un vecino podría realizar un estudio del lugar, y al no detectar redes cercanas podría instalar su propia red en el mismo canal que usted está utilizando, lo cual va a provocarle problemas de interferencia tanto a usted como a su vecino.

Finalmente, utilizar redes cerradas ofrece poca seguridad adicional a su red. Utilizando herramientas de monitoreo pasivas (como Kismet), un usuario experimentado puede detectar paquetes enviados desde sus clientes legítimos al AP. Esos paquetes necesariamente contienen el nombre de la red. Y por lo tanto, un malintencionado puede usarlo luego para asociarse, al igual que lo haría un usuario normal.

Probablemente la encriptación sea la mejor herramienta que tenemos para autenticar a los usuarios de la red. Mediante una fuerte encriptación, podemos identificar a un usuario de una forma única difícil de suplantar, y usar esa identidad para determinar accesos futuros a la red. La encriptación también tiene el beneficio de ofrecer una capa de privacidad adicional ya que evita que los fisgones tengan un acceso fácil al tráfico de la red.

El método de encriptación más utilizado en las redes inalámbricas es el llamado ***encriptación WEP***. WEP ***significa privacidad equivalente*** a la cableada (*del inglés Wired Equivalent Privacy*), y es soportada por casi todo el equipamiento 802.11a/b/g. WEP utiliza una clave compartida de 40-bits para encriptar los datos entre el punto de acceso y el cliente. La clave debe ingresarse en los AP así como en cada uno de los clientes. Cuando se habilita WEP, los clientes no pueden asociarse con el AP hasta que utilicen la clave correcta. Un fisgón oyendo una red con WEP igual puede ver el tráfico y las direcciones MAC, pero los mensajes de los datos de cada paquete están encriptados. Esto provee a la red de un buen mecanismo de autenticación, además de darle un poco de privacidad.

WEP definitivamente no es la mejor solución de encriptación que haya disponible. Por un lado, la clave WEP se comparte entre todos los usuarios, y si

la misma está comprometida (es decir, si un usuario le dice a un amigo la contraseña, o se va un empleado) entonces cambiar la contraseña puede ser extremadamente difícil, ya que todos los AP y los dispositivos cliente deben cambiarla. Esto también significa que los usuarios legítimos de la red pueden escuchar el tráfico de los demás, ya que todos conocen la clave.

A menudo la clave es seleccionada sin mucho cuidado, haciendo posibles los intentos de ataques fuera de línea. Aún peor, varias versiones de WEP son vulnerables mediante técnicas conocidas, haciendo aún más fácil atacar algunas redes. Algunos fabricantes han implementado varias extensiones a WEP (como claves más largas y esquemas rápidos de rotación), pero esas extensiones no son parte del estándar, de tal manera que no van a funcionar correctamente entre equipamientos de diferentes fabricantes. Actualizando al *firmware* más reciente en todos sus dispositivos inalámbricos, puede prevenir alguno de los primeros ataques conocidos a WEP.

Pese a lo anterior, WEP puede ser una herramienta útil de autenticación. Confiando en que sus usuarios no van a difundir la contraseña, puede estar casi seguro de que sus clientes de red inalámbrica son legítimos. Los ataques a WEP están fuera del alcance de la mayoría de los usuarios. WEP es extremadamente útil para asegurar enlaces punto a punto a larga distancia, aún en redes abiertas. Si utiliza WEP en dicho enlace, desalentará que otras personas se asocien al enlace, y probablemente escojan otro AP. Definitivamente WEP es una señal de "manténgase afuera" para su red. Cualquiera que detecte la red va a ver que se requiere una clave, dejándole claro que no es bienvenido.

La mayor fortaleza de WEP es su interoperabilidad. Para cumplir con los estándares, todos los dispositivos inalámbricos soportan un WEP básico. Si bien no es el método más fuerte disponible, ciertamente es la característica implementada más comúnmente. Más adelante vamos a ver otras técnicas de encriptación más avanzadas.

Para obtener más detalles sobre el estado de la encriptación WEP, vea estos artículos:

- *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- *http://www.cs.umd.edu/~waa/wireless.pdf*
- *http://www.crypto.com/papers/others/rc4_ksaproc.ps*

Otro protocolo de autenticación en la capa de enlace de datos es el **Acceso Protegido Wi-Fi**, o ***WPA*** (***Wi-Fi Protected Access*** *por su sigla en inglés*). WPA se creó específicamente para lidiar con los problemas de WEP que mencionamos antes. Provee un esquema de encriptación significativamente más fuerte, y puede utilizar una clave privada compartida, claves únicas

asignadas a cada usuario, o inclusive un certificado SSL para autenticar el punto de acceso y el cliente. Las credenciales de autenticación se chequean usando el protocolo 802.1X, el cual puede consultar una base de datos externa como RADIUS. Mediante el uso de un Protocolo de Integridad Temporal de la Clave (*TKIP –Temporal Key Integrity Protocol*), las claves se pueden rotar rápidamente, reduciendo la posibilidad de que una sesión en particular sea descifrada. En general, WPA provee una autenticación y privacidad significativamente mejor que el estándar WEP.

El problema con WPA, a la fecha de publicación de este libro, es que la interoperabilidad entre los vendedores es aún muy baja. WPA requiere equipamiento de última generación para los puntos de acceso, y *firmware* actualizado en todos los clientes inalámbricos, así como una configuración laboriosa. Si usted controla la totalidad de la plataforma de equipamiento del lugar donde está realizando la instalación, WPA puede ser ideal. La autenticación de los clientes y de los AP, resuelve los problemas de puntos de acceso deshonestos y provee muchas más ventajas que WEP. Pero en la mayoría de las instalaciones de red donde el equipamiento es variado y el conocimiento de los usuarios es limitado, instalar WPA puede ser una pesadilla. Por esta razón es que la mayoría continua utilizando WEP, si es que usa algún tipo de encriptación.

Portales cautivos

Una herramienta común de autenticación utilizada en las redes inalámbricas es el ***portal cautivo***. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet.

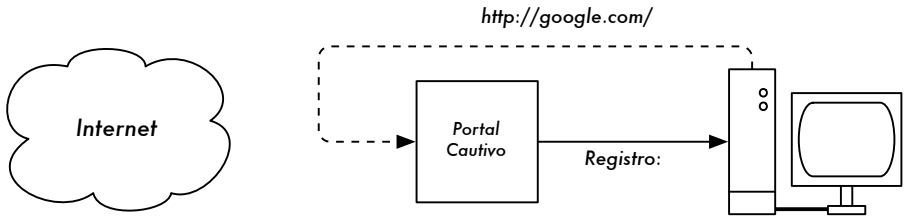

Figura 6.1: El usuario solicita una página web y es redireccionado.

En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de "registro"(*login*), escribe los números de una tarjeta prepago, o ingresa cualquier otra credencial que solicite el administrador de red. El punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales.

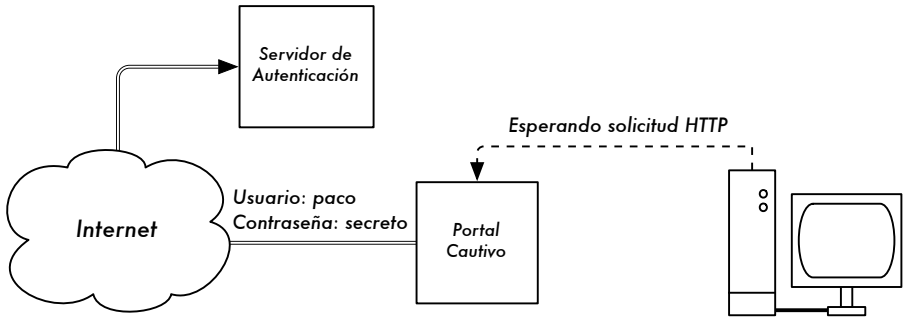

Figura 6.2: Las credenciales se verifican antes de brindar acceso al resto de la red. El servidor de autenticación puede ser el punto de acceso mismo, otra computadora en la red local, o un servidor en cualquier lugar del Internet.

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es redireccionado al sitio web que solicitó originalmente.

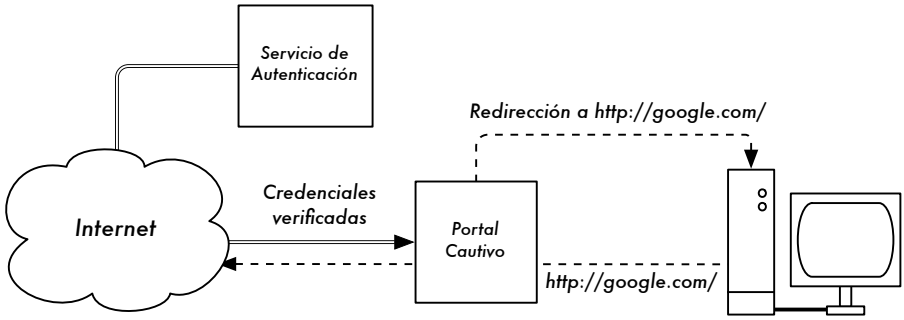

Figura 6.3: Después de que el usuario es autenticado, se le permite el acceso al resto de la red.

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicos. Si bien esto no es necesariamente muy seguro, muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente. Esto puede hacerse automáticamente, minimizando una ventana emergente (*pop-up*) del navegador, cuando el usuario se registra por primera vez.

Debido a que no proveen una fuerte encriptación, los portales cautivos no son una buena elección para aquellas redes que requieren una protección fuerte y limiten el acceso solamente a usuarios confiables. En realidad se adaptan mejor para cafés, hoteles y otros lugares de acceso público donde se esperan usuarios casuales de la red.

En redes públicas o semipúblicas, las técnicas de encriptación como WEP y WPA son realmente inútiles. Simplemente no hay forma de distribuir claves públicas o compartidas para el público en general sin comprometer la seguridad de esas claves. En esas instalaciones, una simple aplicación como un portal cautivo provee un nivel de servicio intermedio entre completamente abierto y completamente cerrado.

Dos implementaciones de portales cautivos de fuente abierta son NoCatSplash y Chillispot.

NoCatSplash

Si usted simplemente necesita proveer a los usuarios de una red abierta con información y la política de uso aceptable, preste atención a NoCatSplash. El mismo está disponible en *http://nocat.net/download/NoCatSplash/*.

NoCatSplash provee una página de ingreso modificable, solicitándoles a sus usuarios presionar el botón de “registro” antes de utilizar la red. Esto es útil

para identificar los operadores de la red y mostrar las reglas de acceso a la misma.

NoCatSplash está escrito en C, y va a correr en casi cualquier sistema operativo tipo Unix incluidos Linux, BSD, y también plataformas embebidas como OpenWRT. Tiene un archivo de configuración muy simple y puede usar cualquier archivo HTML personalizado como la página de ingreso. En general se corre directamente en un punto de acceso, pero también funciona en un enrutador o un servidor *proxy*. Para más información, vea la página *http://nocat.net/*.

Otros proyectos populares relacionados con *hotspots*

NoCatSplash es una implementación simple de portal cautivo. Existen muchas otras implementaciones gratuitas que soportan diversos rangos de funcionalidad. Algunas de ellas incluyen:

- Chillispot (*http://www.chillispot.org/*). Chillispot es un portal cautivo diseñado para autenticar verificando los datos contra una base de datos de credenciales de usuarios, tal como RADIUS. Si lo combinamos con la aplicación phpMyPrePaid, se puede implementar fácilmente un sistema de autenticación basado en pre-pago. phpMyPrePaid se puede descargar desde *http://sourceforge.net/projects/phpmyprepaid/*.
- WiFi Dog (*http://www.wifidog.org/*). WiFi Dog provee un paquete muy completo de autenticación vía portal cautivo, en muy poco espacio (generalmente menos de 30kB). Desde la perspectiva del usuario, no requiere de una ventana emergente (*pop-up*) ni de soporte javascript, permitiéndole trabajar en una amplia variedad de dispositivos inalámbricos.
- m0n0wall (*http://m0n0.ch/wall/*). Como mencionamos en el capítulo cinco, m0n0wall es un sistema operativo embebido completo basado en FreeBSD. Este incluye un portal cautivo con soporte RADIUS, así como un servidor web PHP.

Privacidad

La mayoría de los usuarios son dichosamente ignorantes de que su correo electrónico privado, conversaciones en línea, y aún sus contraseñas a menudo son enviados “al descubierto” por docenas de redes inseguras antes de llegar a su destino en Internet. No obstante lo errados que pueden estar, en general, los usuarios tienen expectativas de un poco de privacidad cuando usan redes de computadoras.

La privacidad se puede lograr, aún en redes inseguras como los puntos de acceso público e Internet. El único método efectivo probado para proteger la privacidad es el uso de una ***encriptación*** fuerte ***de extremo a extremo***.

Las técnicas de encriptación como WEP y WPA intentan mantener la privacidad en la capa dos, la capa de enlace de datos. Aunque éstas nos protegen de los fisgones en la conexión inalámbrica, la protección termina en el punto de acceso. Si el cliente inalámbrico usa protocolos inseguros (como POP o SMTP para recibir y enviar correos electrónicos), entonces los usuarios que están más allá del AP pueden registrar la sesión y ver los datos importantes. Como mencionamos antes, WEP también tiene la debilidad de utilizar claves privadas compartidas. Esto significa que los usuarios legítimos de la red pueden escucharse unos a otros, ya que todos conocen la clave privada.

Utilizando encriptación en el extremo remoto de la conexión, los usuarios pueden eludir completamente el problema. Estas técnicas funcionan muy bien aún en redes públicas, donde los fisgones están oyendo y posiblemente manipulando los datos que vienen del punto de acceso.

Para asegurar la privacidad de los datos, una buena encriptación de extremo a extremo debe ofrecer las siguientes características:

- ***Autenticación verificada del extremo remoto.*** El usuario debe ser capaz de conocer sin ninguna duda que el extremo remoto es el que dice ser. Sin autenticación, un usuario puede darle datos importantes a cualquiera que afirme ser el servicio legítimo.
- ***Métodos fuertes de encriptación.*** El algoritmo de encriptación debe ser puesto al escrutinio del público, y no debe ser fácil de descifrar por un tercero. El uso de métodos de encriptación no publicados no ofrece seguridad, y una encriptación fuerte lo es aún más si el algoritmo es ampliamente conocido y sujeto a la revisión de los pares. Un buen algoritmo con una clave larga y adecuadamente protegida, puede ofrecer encriptación imposible de romper aunque hagamos cualquier esfuerzo utilizando la tecnología actual.
- ***Criptografía de clave pública.*** Aunque no es un requerimiento absoluto para la encriptación de extremo a extremo, el uso de criptografía de clave pública en lugar de una clave compartida, puede asegurar que los datos personales de los usuarios se mantengan privados, aún si la clave de otro usuario del servicio se ve comprometida. Esto también resuelve ciertos problemas con la distribución de las claves a los usuarios a través de una red insegura.
- ***Encapsulación de datos.*** Un buen mecanismo de encriptación de extremo a extremo protege tantos datos como sea posible. Esto puede ir

desde encriptar una sencilla transacción de correo electrónico, a encapsular todo el tráfico IP, incluyendo búsquedas en servidores DNS y otros protocolos de soporte. Algunas herramientas de encriptación proveen un canal seguro que también pueden utilizar otras aplicaciones. Esto permite que los usuarios corran cualquier programa que ellos quieran y aún tengan la protección de una fuerte encriptación, aunque los programas no la soporten directamente.

Note que la legislación sobre el uso de encriptación varía ampliamente de lugar en lugar. Algunos países pueden llegar a equiparar el uso de encriptación con el uso de armamento o municiones, y pueden requerir un permiso, exigir la custodia de las claves privadas o prohibir su uso por completo. Antes de implementar cualquier solución que implique encriptación verifique que el uso de esta tecnología esté permitido en su comunidad.

En las siguientes secciones vamos a examinar algunas herramientas específicas que proveen una buena protección para los datos de sus usuarios.

SSL

La tecnología de encriptación de extremo a extremo más accesible es ***Secure Socket Layer*** conocida simplemente como ***SSL*** *por su sigla en inglés*. Incluida en casi todos los navegadores web, SSL utiliza criptografía de clave pública e ***infraestructura de clave pública confiable*** (***PKI*** *por su sigla en inglés*), para asegurar las comunicaciones de datos en la web. Cada vez que visita la URL de una web que comienza con https, está usando SSL.

La implementación SSL provista en los navegadores web incluye un conjunto de certificados de fuentes confiables, denominados ***autoridades certificadoras*** (***CA***). Estos certificados son claves criptográficas que se utilizan para verificar la autenticidad de los sitios web. Cuando usted navega en un sitio que utiliza SSL, el navegador y el servidor primero intercambian certificados. Luego el navegador verifica que el certificado brindado por el servidor concuerde con el nombre en su servidor DNS, que no haya expirado, y que esté firmado por una autoridad certificadora confiable. Opcionalmente el servidor verifica la identidad del certificado del navegador. Si los certificados son aprobados, el navegador y el servidor negocian la clave de sesión maestra utilizando los certificados intercambiados anteriormente para protegerla. Dicha clave se usa para encriptar todas las comunicaciones hasta que el navegador se desconecte. Este tipo de encapsulamiento de datos es conocido como ***túnel***.

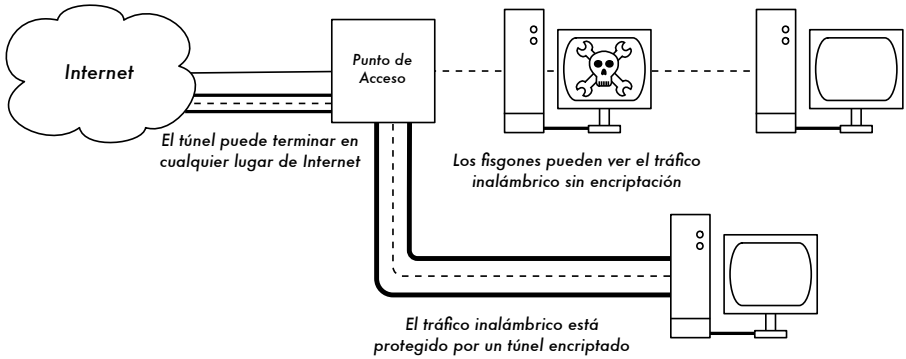

Figura 6.4: Los fisgones deben romper la encriptación para monitorear el tráfico dentro de un túnel encriptado. La conversación dentro del túnel es igual a cualquier otra conversación sin encriptar.

El uso de certificados con una PKI no solo protege a la comunicación de los fisgones, sino que también evita los ataques del llamado ***hombre en el medio*** (***MITM*** *por su sigla en inglés*). En un ataque del hombre en el medio, un usuario mal intencionado intercepta una comunicación entre el navegador y el servidor. Presentándoles certificados falsos a ambos, puede mantener dos sesiones encriptadas al mismo tiempo. Puesto que este usuario conoce el secreto de ambas conexiones, es trivial observar y manipular los datos que están pasando entre el servidor y el navegador.

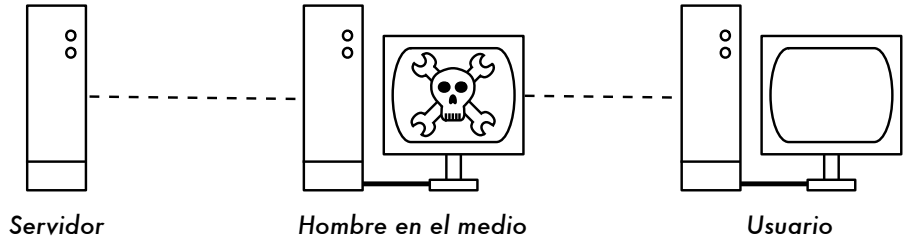

Figura 6.5: El hombre en el medio controla de forma efectiva todo lo que el usuario ve, y puede grabar y manipular todo el tráfico. Sin una infraestructura de clave pública para verificar la autenticidad de las claves, la encriptación fuerte por si sola no podría protegernos de este tipo de ataque.

El uso de una buena PKI previene este tipo de ataque. Para tener éxito el usuario con malas intenciones debería presentar un certificado al cliente, que estuviera firmado por una autoridad certificadora. A menos que la CA haya sido comprometida (muy poco probable) o que el usuario pueda ser engañado para aceptar el certificado falso, este tipo de ataque es infructuoso. Es por esto que es de vital importancia que los usuarios comprendan que ignorar los avisos sobre los certificados vencidos o falsos es muy peligroso, especialmente cuando usamos redes inalámbricas. Pulsando el

botón "ignorar" cuando son avisados por su navegador, los usuarios se abren a una cantidad de ataques potenciales.

SSL no sólo se utiliza para navegar en la web. Los protocolos de correo electrónico como IMAP, POP, y SMTP (que son bastante inseguros) pueden asegurarse envolviéndolos en un túnel SSL. La mayoría de los clientes de correo electrónico actuales soportan IMAPS y POPS (IMAP y POP seguros), así como SMTP protegido con SSL/TLS. Si su servidor de correo no provee soporte SSL, de todas formas puede asegurarlo con SSL utilizando un paquete como Stunnel (*http://www.stunnel.org/*). SSL puede utilizarse para asegurar de forma efectiva casi cualquier servicio que corra sobre TCP.

SSH

La mayoría de la gente considera SSH como un sustituto para **`telnet`** que provee seguridad, porque **`scp`** y **`sftp`** son los equivalentes seguros de rcp y ftp. Pero SSH es mucho más que un acceso remoto a consola encriptado. Al igual que SSL, utiliza una fuerte criptografía de clave pública para verificar el servidor remoto y encriptar los datos. En lugar de PKI, utiliza una clave de impresión digital almacenada que se chequea antes de permitir la conexión. Puede usar contraseñas, claves públicas u otros métodos de autenticación de usuarios.

Mucha gente no sabe que SSH también puede actuar como un túnel de encriptación general o como un servidor proxy de encriptación. Estableciendo una conexión SSH en un lugar confiable cerca de (o en) un servidor remoto, los protocolos inseguros pueden protegerse de los fisgones y los ataques.

Esta técnica puede resultar algo avanzada para muchos usuarios, pero los desarrolladores de redes pueden utilizar SSH para encriptar el tráfico en enlaces inseguros, como los enlaces inalámbricos punto a punto. Como las herramientas son gratuitas y funcionan sobre el estándar TCP, los usuarios avanzados pueden implementar conexiones SSH por sí mismos, obteniendo su propia encriptación de extremo a extremo sin la intervención del administrador.

Probablemente OpenSSH (*http://openssh.org/*) sea la implementación más popular en las plataformas tipo Unix. Para Windows tenemos disponibles implementaciones gratuitas como Putty (*http://www.putty.nl/*) y WinSCP (*http://winscp.net/*). OpenSSH también corre en Windows bajo el paquete Cygwin (*http://www.cygwin.com/*). Los ejemplos a continuación suponen que usted está utilizando una versión reciente de OpenSSH.

Para establecer un túnel encriptado desde un puerto en la computadora local hasta un puerto en el extremo remoto se debe utilizar el parámetro **-L**. Por ejemplo, supongamos que usted quiere reenviar el tráfico del *proxy* web en

un enlace encriptado al servidor squid en *squid.example.net*. El puerto de reenvío 3128 (el puerto *proxy* por omisión) utiliza este comando:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

Las opciones **-fN** le ordenan a ssh que permanezca abierto en segundo plano después de conectarse. La opción **-g** permite a otros usuarios en su segmento local que se conecten a la computadora local, y la utilicen para la encriptación sobre el enlace inseguro. OpenSSH utilizará una clave pública para la autenticación si usted ya ha configurado una, o va a solicitarle su contraseña para conectarse al extremo remoto. Luego usted puede configurar su navegador web para conectarse al servidor local puerto 3128 como su servicio de proxy. Todo el tráfico web será encriptado antes de la transmisión al sitio remoto.

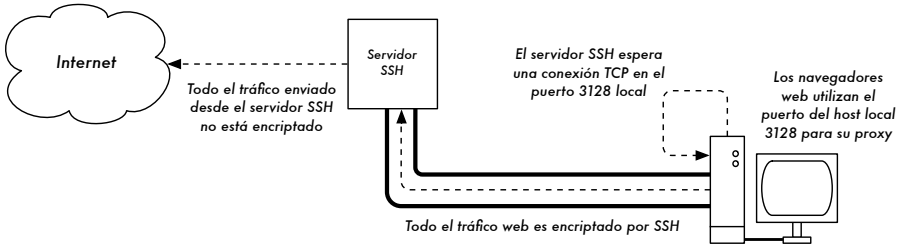

Figura 6.6: El túnel SSH protege el tráfico web hasta llegar al servidor SSH remoto.

SSH también puede funcionar como un proxy dinámico SOCKS4 o SOCKS5. Esto le permite crear un proxy web encriptador sin la necesidad de instalar squid. Tenga en cuenta que éste no será un proxy con memoria intermedia (cache), simplemente encripta todo el tráfico.

```
ssh -fN -D 8080 remote.example.net
```

Configure su navegador web para utilizar SOCKS4 o SOCKS5 en el puerto local 8080, y listo.

SSH puede encriptar datos en cualquier puerto TCP, incluyendo puertos utilizados para el correo electrónico. También puede comprimir los datos, lo que puede hacer disminuir el tiempo de recuperación de datos (latencia) en enlaces de baja capacidad.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

La opción **-C** habilita la compresión. Especificando múltiples veces la opción **-L** se pueden agregar tantas reglas de redirección de puertos como quiera. Tenga en cuenta que para vincularse a un puerto local inferior a 1024, debe tener privilegios de administrador (root) en la máquina local.

Estos son solo algunos ejemplos de la flexibilidad de SSH. Al implementar claves públicas y utilizar el agente de reenvío ssh, puede automatizarse la creación de túneles encriptados a través de la red inalámbrica, y proteger nuestras comunicaciones con una fuerte encriptación y autenticación.

OpenVPN

OpenVPN es una implementación VPN gratuita de fuente abierta construida con encriptación SSL. Existen versiones para un amplio rango de sistemas operativos, incluyendo Linux, Windows 2000/XP y superiores, OpenBSD, FreeBSD, NetBSD, Mac OS X, y Solaris. Una VPN encapsula todo el tráfico (incluyendo DNS y todos los otros protocolos) en un túnel encriptado, no un solo puerto TCP. La mayoría de la gente lo encuentra considerablemente más sencillo de comprender y configurar que IPSEC.

OpenVPN también tiene algunas desventajas, como por ejemplo una latencia bastante alta. Cierta cantidad de latencia no se puede evitar porque toda la encriptación/desencriptación se hace en el entorno de usuario, pero si se utilizan computadoras relativamente nuevas en cada extremo del túnel puede minimizarla. Si bien puede usar las tradicionales claves compartidas, OpenVPN se destaca realmente cuando se usa con certificados SSL y una autoridad certificadora confiable. OpenVPN tiene algunas ventajas que lo hace una buena opción para proveer seguridad de extremo a extremo.

- Se basa en un protocolo de encriptación robusto y probado (SSL y RSA)
- Es relativamente fácil de configurar
- Funciona en muchas plataformas diferentes
- Está bien documentado
- Es gratuito y de fuente abierta

Al igual que SSH y SSL, OpenVPN necesita conectarse a un puerto TCP único en el extremo remoto. Una vez establecido, puede encapsular todos los datos en la capa de red, o en la capa de enlace de datos, según sus requerimientos. Lo puede utilizar para crear conexiones VPN robustas entre máquinas individuales o simplemente utilizarlo para conectar enrutadores en redes inalámbricas inseguras.

La tecnología VPN es un campo complejo, y está un poco más allá del alcance de esta sección. Es importante comprender dónde encajan las VPN en la estructura de su red, para proveer la mejor protección posible sin exponer a su organización a problemas involuntarios. Existen varios recursos en línea que se dedican a la instalación de OpenVPN en un servidor y un cliente, personalmente recomiendo este artículo del Linux Journal:

http://www.linuxjournal.com/article/7949, así como el sitio oficial de CÓMO HACERLO: *http://openvpn.net/howto.html*

Tor y Anonimizadores

Básicamente, Internet es una red abierta basada en la confianza. Cuando usted se conecta a un servidor web en Internet, su tráfico pasa a través de muchos enrutadores diferentes, pertenecientes a una gran variedad de instituciones, corporaciones y personas. En principio, cualquiera de esos enrutadores tiene la posibilidad de observar de cerca sus datos, mirando como mínimo las direcciones de origen y destino, y muy a menudo el contenido de los datos. Aún si sus datos están encriptados por medio de un protocolo seguro, su proveedor de Internet puede monitorear la cantidad de datos y el origen y destino de los mismos. A menudo esto es suficiente para tener una idea clara de sus actividades en línea.

La privacidad y el anonimato son importantes y están unidas estrechamente. Hay muchas razones válidas para considerar proteger su privacidad ***haciendo anónimo*** su tráfico en la red. Supongamos que usted quiere ofrecer conectividad a Internet a su comunidad, instalando varios puntos de acceso para que la gente se conecte. Tanto si usted les cobra por el acceso como si no, existe siempre el riesgo de que la gente utilice la red para alguna actividad ilegal en su país o región. Usted podría argumentar luego, en caso de verse envuelto en problemas legales, que esa acción ilegal no fue realizada por usted sino por cualquiera conectado a su red. Sin embargo, el problema legal puede evadirse elegantemente si no es técnicamente factible determinar adónde fue realmente dirigido su tráfico. ¿Y qué pasa con la censura en Internet? Publicar páginas web anónimamente puede ser necesario para evitar la censura del gobierno.

Existen herramientas que le permiten hacer anónimo su tráfico de formas relativamente sencillas. La combinación de ***Tor*** (*http://tor.eff.org/*) y ***Privoxy*** (*http://www.privoxy.org/*) es una forma poderosa de correr un servidor *proxy* local que pasa su tráfico de Internet a través de varios servidores dispersos por la red, dificultando seguir el rastro de la información. Tor puede activarse en un PC local bajo Microsoft Windows, Mac OSX, Linux y una variedad de BSDs, donde el tráfico se hace anónimo desde el navegador a esa máquina en particular. Tor y Privoxy también pueden instalarse en una pasarela (*gateway*), o también en un pequeño punto de acceso embebido (como el Linksys WRT54G) donde se provee anonimato automáticamente para todos los usuarios de la red.

Tor funciona haciendo rebotar repetidamente sus conexiones TCP a través de varios servidores esparcidos en Internet, y envuelve la información de enrutamiento en varias capas encriptadas (de ahí el término enrutamiento ***cebolla***), que se van quitando cuando el paquete se mueve por la red. Esto

significa que, en cualquier punto en la red, la dirección de la fuente y la del destino no pueden relacionarse una con la otra. Esto hace que el análisis del tráfico sea extremadamente difícil.

La necesidad del proxy de privacidad Privoxy en combinación con Tor se debe al hecho de que las solicitudes de nombre del servidor (solicitudes DNS) en la mayoría de los casos no pasan a través del servidor proxy, y alguien que esté analizando su tráfico puede ser capaz de ver que usted está intentando acceder a un sitio específico (por ejemplo google.com) por el hecho de que envía una solicitud DNS para traducir google.com a la dirección IP apropiada. Privoxy se conecta a Tor como un proxy SOCKS4a, el cual usa nombres de servidores (no direcciones IP) para entregar sus paquetes en el destino deseado.

En otras palabras, utilizar Privoxy con Tor es una forma simple y efectiva de prevenir el análisis del tráfico que relaciona su dirección IP con los servicios que utiliza en línea. Combinado con protocolos de encriptación seguros (como los que hemos visto en este capítulo), Tor y Privoxy proveen un alto nivel de anonimato en Internet.

Monitoreo

Las redes de computadoras (y las inalámbricas en particular) son invenciones increíblemente entretenidas y útiles. Excepto, por supuesto, cuando no funcionan. Sus usuarios se pueden quejar de que la red es “lenta” o “no funciona” ¿pero qué significa esto realmente? Sin comprender qué es lo que realmente está pasando, administrar una red puede ser muy frustrante.

Para ser un administrador de red efectivo, necesita tener acceso a herramientas que le muestren exactamente qué es lo que está sucediendo en su red. Existen varias clases diferentes de herramientas de monitoreo. Cada una le muestra un aspecto diferente de lo que “está pasando”, desde la interacción física del radio a las formas en que las aplicaciones de los usuarios interactúan entre ellas. Al observar el desempeño de la red a través del tiempo se puede tener una idea de lo que es “normal” para ella, y ser notificado automáticamente cuando las cosas están fuera de orden. Las herramientas que presentamos en esta sección son bastante poderosas, y se pueden descargar gratuitamente de las fuentes listadas.

Detección de redes

Las herramientas de monitoreo comunes, simplemente proveen una lista de redes disponibles con información básica (tales como intensidad de la señal y canal). Le permiten detectar rápidamente redes cercanas y determinar si están dentro de su alcance o si están causando interferencia.

- **Las incorporadas en el cliente.** Todos los sistemas operativos modernos proveen soporte incorporado para redes inalámbricas. En general este incluye la habilidad de explorar en búsqueda de redes disponibles, permitiéndole al usuario elegir una red de la lista. Si bien prácticamente todos los dispositivos inalámbricos incluyen una utilidad simple de exploración, las funcionalidades puede variar ampliamente entre implementaciones. En general, son útiles solamente para configurar una computadora en su hogar o en la oficina. Tienden a proveer poca información además de los nombres de las redes y la señal disponible para el punto de acceso en uso actualmente.
- **Netstumbler** (*http://www.netstumbler.com/*). Es la herramienta más popular para detectar redes inalámbricas utilizando Microsoft Windows. Soporta una variedad de tarjetas inalámbricas, y es muy sencilla de utilizar. Detecta redes abiertas y encriptadas, pero no puede detectar redes inalámbricas "cerradas". También ofrece un medidor de señal/ruido que grafica la señal recibida a lo largo del tiempo. También se puede integrar con una variedad de dispositivos GPS, para registrar ubicaciones precisas e información sobre la potencia de la señal. Todo esto hace que Netstumbler sea una herramienta accesible para realizar una prospección informal de la zona.
- **Ministumbler** (*http://www.netstumbler.com/*). De los realizadores de Netstumbler, Ministumbler provee muchas de las mismas funcionalidades que la versión de Windows, pero funciona en las plataformas Pocket PC. Ministumbler se puede correr en PDAs portátiles con una tarjeta inalámbrica para detectar puntos de acceso en la zona.
- **Macstumbler** (*http://www.macstumbler.com/*). Si bien no está relacionado directamente con Netstumbler, Macstumbler brinda muchas de sus funcionalidades pero para la plataforma Mac OS X. Funciona con todas las tarjetas Apple Airport.
- **Wellenreiter** (*http://www.wellenreiter.net/*). Wellenreiter es un buen detector gráfico de redes inalámbricas para Linux. Requiere Perl y GTK, y soporta tarjetas inalámbricas Prism2, Lucent, y Cisco.

Analizadores de protocolos

Los analizadores de protocolos de redes una gran cantidad de detalles de la información que fluye por una red, permitiendo inspeccionar paquetes individualmente. Para las redes cableadas, pueden inspeccionar paquetes en la capa de enlace de datos o en una superior. Para el caso de las redes inalámbricas, se puede inspeccionar información hasta las tramas 802.11. Aquí hay varios analizadores de protocolos de redes populares (y gratuitas):

- **Ethereal** (*http://www.ethereal.com/*). Ethereal probablemente sea el analizador de protocolos más popular de los que tenemos a disposición. Funciona con Linux, Windows, Mac OS X, y con varios sistemas BSD. Ethereal capturara los paquetes directamente "del cable" y los despliega en una interfaz gráfica intuitiva. Puede decodificar más de 750 protocolos, desde las tramas 802.11 a los paquetes HTTP. Fácilmente reensambla los paquetes fragmentados y sigue las sesiones TCP por completo, aún si otros datos se han intercalado en la muestra. Ethereal es muy importante para resolver problemas difíciles de la red, y averiguar que es exactamente lo que está sucediendo cuando dos computadoras conversan "en el cable".

- **Kismet** (*http://www.kismetwireless.net/*). Kismet es un poderoso analizador de protocolos inalámbrico para Linux, Mac OS X, y la distribución Linux embebida OpenWRT. Funciona con cualquier tarjeta inalámbrica que soporte el modo monitor pasivo. Además de la detección básica de redes, Kismet registra pasivamente todas las tramas 802.11 al disco o la red en el formato estándar PCAP, para su futuro análisis con herramientas como Ethereal. Kismet también ofrece información asociada del cliente, impresión digital del modelo del AP, detección con Netstumbler, e integración GPS.

  Como es un monitor pasivo de la red también puede detectar redes inalámbricas "cerradas", analizando el tráfico enviado por los clientes. Se puede instalar Kismet en varias computadoras al mismo tiempo, y hacer que todas reporten a través de la red a una misma interfaz de usuario. Esto permite realizar un monitoreo inalámbrico sobre grandes áreas, tales como un campus universitario o corporativo. Como utiliza el modo de monitoreo pasivo, hace todo esto sin transmitir ningún dato.

- **KisMAC** (*http://kismac.binaervarianz.de/*). Desarrollado exclusivamente para la plataforma Mac OS X, KisMAC puede hacer mucho de lo que Kismet hace, pero con una interfaz gráfica Mac OS X muy elaborada. Es un rastreador pasivo que registra datos al disco en un formato PCAP compatible con Ethereal. No soporta un rastreo pasivo con tarjetas AirportExtreme (debido a las limitaciones en el manejador inalámbrico), pero soporta el modo pasivo con una variedad de tarjetas inalámbricas USB.

- **Driftnet y Etherpeg**. Estas herramientas decodifican datos gráficos (como los archivos GIF y JPEG) y los despliegan como un collage. Como mencionamos anteriormente, herramientas como ésta tienen un uso limitado en la resolución de problemas, pero tienen mucho valor para demostrar la inseguridad de los protocolos sin encriptación. Etherpeg está disponible en http://www.etherpeg.org/, y Driftnet puede descargarse en *http://www.ex-parrot.com/~chris/driftnet/*.

Monitoreo del ancho de banda

La red está lenta. ¿Quién está acaparando todo el ancho de banda? Utilizando una buena herramienta de monitoreo, puede determinar fácilmente la fuente que inunda su red de correo no deseado y de virus. Dichas herramientas también lo pueden ayudar a planificar los incrementos de capacidad requeridos para mantener los usuarios satisfechos. Al mismo tiempo le dan una representación visual de cómo fluye el tráfico en la red, incluyendo el que proviene de una computadora o servicio en particular.

- **MRTG** (*http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*). La mayoría de los administradores de red se han encontrado con MRTG en algún punto de su carrera. Escrito originalmente en 1995, MRTG posiblemente sea la aplicación de monitoreo de ancho de banda más usada. Utilizando Perl y C, construye una página web llena de gráficos detallando el tráfico saliente y entrante en un dispositivo de red en particular. Con MRTG es muy sencillo consultar conmutadores de red, puntos de acceso, servidores, así como otros dispositivos, y desplegar los resultados como gráficos en función del tiempo.
- **RRDtool** (*http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*). Desarrollado por la misma gente que escribió mrtg, rrdtool es una aplicación de monitoreo genérica más poderosa. RRD es una abreviatura de base de datos de recorrido circular (*Round-Robin Database por su nombre en inglés*). Este es un formato de datos genérico que le permite seguir cualquier punto de datos como un conjunto promediado en el tiempo. Si bien rrdtool no monitorea directamente interfaces o dispositivos, muchos paquetes de monitoreo confían en él para almacenar y desplegar los datos que colectan. Con unos pocos programas de consola, puede monitorear fácilmente los conmutadores y puntos de acceso de su red, y trazar de forma gráfica en una página web el ancho de banda utilizado.
- **ntop** (*http://www.ntop.org/*). Para realizar un análisis histórico del tráfico y del uso de la red, seguramente usted va a querer investigar ntop. Este programa construye un reporte detallado en tiempo real de lo que observa en el tráfico de la red, y lo despliega en su navegador web. Se integra con rrdtool, y realiza gráficos y cuadros visuales que representan cómo está siendo usada la red. En redes muy pesadas ntop puede consumir mucha capacidad de la CPU y espacio del disco, pero le brinda un extensivo análisis de cómo está siendo utilizada su red. Funciona en Linux, BSD, Mac OS X, y Windows.
- **iptraf** (*http://iptraf.seul.org/*). Si necesita tomar una instantánea de la actividad de la red en un sistema Linux, inténtelo con iptraf. Ésta es una utilidad de línea de comando que le brinda en segundos una mirada sobre las conexiones y el flujo de su red, incluyendo puertos y protocolos. Puede ser muy buena para determinar quién está usando un enlace inalámbrico

en particular, y cuanta carga se le está imponiendo. Por ejemplo, al mostrar una estadística detallada acerca de una interfaz, usted puede encontrar instantáneamente los usuarios de programas de intercambio entre pares (*P2P o peer-to-peer como se les conoce en inglés*) y determinar exactamente cuánto ancho de banda están utilizando en cierto momento.

Resolución de problemas

¿Qué hace cuando la red se daña? Si no puede acceder a una página web o a un servidor de correo electrónico, y el problema no se soluciona presionando el botón de "actualizar", ustedes hace necesario aislar la ubicación exacta del problema. Estas herramientas lo van a ayudar a determinar dónde se encuentra exactamente un problema de la conexión.

- **ping**. Casi todos los sistemas operativos (incluyendo Windows, Mac OS X, y por supuesto Linux y BSD) incluyen una versión de la utilidad *ping*. Utiliza paquetes ICMP para intentar contactar un servidor específico y le informa a usted cuánto tiempo lleva obtener una respuesta.

  Saber qué contactar es tan importante como saber cómo hacerlo. Si usted no puede conectarse a un servicio en su navegador web (por ejemplo, *http://yahoo.com/*), puede intentar contactarlo:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Presione control-C cuando haya terminado de colectar datos. Si los paquetes se toman mucho tiempo en regresar, puede haber una congestión en la red. Si el retorno de los paquetes de contacto tiene un ttl inusualmente bajo, puede que haya problemas de enrutamiento entre su computadora y el extremo remoto. ¿Pero qué sucede si el contacto no regresa ningún dato? Si está contactando un nombre en lugar de una dirección IP, puede que tenga problemas de DNS.

Intente contactar una dirección IP en Internet. Si no puede acceder a ella, es una buena idea observar si puede contactar su enrutador por omisión:

```
$ ping 216.231.38.1
PING 216.231.38.1 (216.231.38.1): 56 data bytes
64 bytes from 216.231.38.1: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 216.231.38.1: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 216.231.38.1: icmp_seq=2 ttl=126 time=13.897 ms
^C
--- 216.231.38.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms
```

Si no puede contactar a su enrutador por omisión, entonces lo más probable es que tampoco pueda acceder a Internet. Si tampoco puede contactar otras direcciones IP en su LAN local, es tiempo de verificar su conexión. Si está utilizando cable Ethernet, ¿está enchufado? Si está utilizando una conexión inalámbrica, ¿esta usted conectado a la red correcta, y está la red dentro de su alcance?

El diagnóstico de problemas de la red con *ping* es casi un arte, pero es muy útil. Ya que probablemente usted va a encontrar *ping* en casi cualquier computadora con la que trabaje, es una buena idea aprender cómo usarlo apropiadamente.

- **traceroute** y **mtr** (*http://www.bitwizard.nl/mtr/*). Como sucede con *ping*, *traceroute* está en la mayoría de los sistemas operativos (en algunas versiones de Microsoft Windows se le denomina **tracert**). Si corre *traceroute*, puede rastrear la ubicación de los problemas entre su computadora y cualquier punto en Internet:

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
 1  10.15.6.1  4.322 ms  1.763 ms  1.731 ms
 2  216.231.38.1  36.187 ms  14.648 ms  13.561 ms
 3  69.17.83.233  14.197 ms  13.256 ms  13.267 ms
 4  69.17.83.150  32.478 ms  29.545 ms  27.494 ms
 5  198.32.176.31  40.788 ms  28.160 ms  28.115 ms
 6  66.249.94.14  28.601 ms  29.913 ms  28.811 ms
 7  172.16.236.8  2328.809 ms  2528.944 ms  2428.719 ms
 8  * * *
```

La opción **-n** le dice a *traceroute* que no se preocupe por resolver los nombres en el DNS, y hace que el programa corra más rápido. Usted puede ver que en el salto siete, el tiempo de recorrido de ida y vuelta se dispara a más de dos segundos, mientras que los paquetes parece que se desechan en el salto ocho. Esto puede indicar un problema en ese punto

de la red. Si esta parte de la red está bajo su control, vale la pena comenzar sus esfuerzos para resolver el problema por allí.

My TraceRoute (mtr) es un programa que combina *ping* y *traceroute* en una sola herramienta. Corriendo mtr, puede obtener un promedio de la latencia y la pérdida de paquetes hacia un servidor en cierto lapso, en lugar de la visión instantánea que ofrecen *ping* y *traceroute*.

```
                                My traceroute  [v0.69]
tesla.rob.swn (0.0.0.0)         (tos=0x0 psize=64 bitpatSun Jan  8 20:01:26 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                          Packets               Pings
 Host                                    Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. gremlin.rob.swn                       0.0%     4    1.9   2.0   1.7   2.6   0.4
 2. er1.sea1.speakeasy.net                0.0%     4   15.5  14.0  12.7  15.5   1.3
 3. 220.ge-0-1-0.cr2.sea1.speakeasy.      0.0%     4   11.0  11.7  10.7  14.0   1.6
 4. fe-0-3-0.cr2.sfo1.speakeasy.net       0.0%     4   36.0  34.7  28.7  38.1   4.1
 5. bas1-m.pao.yahoo.com                  0.0%     4   27.9  29.6  27.9  33.0   2.4
 6. so-1-1-0.pat1.dce.yahoo.com           0.0%     4   89.7  91.0  89.7  93.0   1.4
 7. ae1.p400.msr1.dcn.yahoo.com           0.0%     4   91.2  93.1  90.8  99.2   4.1
 8. ge5-2.bas1-m.dcn.yahoo.com            0.0%     4   89.3  91.0  89.3  93.4   1.9
```

Los datos van a ser actualizados y promediados continuamente. Al igual que con *ping*, cuando haya terminado de observar los datos debe presionar control-C. Tenga en cuenta que para usar mtr debe tener privilegios de administrador (root).

Si bien estas herramientas no van a revelar exactamente qué es lo que está funcionando mal en una red, pueden darle información suficiente para saber por dónde continuar en la resolución de problemas.

Prueba de rendimiento

¿Cuán rápido puede funcionar la red? ¿Cuál es la capacidad real utilizable en un enlace específico de la red? Puede obtener una muy buena estimación de su capacidad de rendimiento inundando el enlace con tráfico y midiendo cuánto demora en transferir los datos. Aunque existen páginas web que pueden hacer una "prueba de velocidad" en su navegador (como *http://www.dslreports.com/stest*), esas pruebas son altamente inexactas si usted está lejos de la fuente de prueba. Aún peor, no le permiten medir la velocidad de un enlace en particular, sino solamente la velocidad de su enlace a Internet. Le presentamos dos herramientas que le van a permitir realizar una prueba de rendimiento en su propia red.

- **ttcp** (*http://ftp.arl.mil/ftp/pub/ttcp/*). Actualmente es una parte estándar de la mayoría de los sistemas tipo Unix. ttcp es una simple herramienta de prueba de red. Se corre en cualquier lado del enlace que usted quiera probar. El primer nodo actúa en modo receptor, y el otro transmite:

```
node_a$ ttcp -r -s

node_b$ ttcp -t -s node_a
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp -> node_a
ttcp-t: socket
ttcp-t: connect
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw
```

Después de recolectar los datos en una dirección, debe invertir el par de transmisión y recepción para probar el enlace en la otra dirección. Puede probar flujos UDP así como TCP, alterar varios parámetros TCP y el largo de la memoria intermedia (*buffer*) para probar la red bajo fuertes exigencias. Además, el usuario puede especificar los datos a enviar en la prueba, en lugar de enviar datos generados aleatoriamente. Recuerde que la velocidad de lectura está en kilobytes, no en kilobits. Multiplique el resultado por 8 para encontrar la velocidad en kilobits por segundo.

La única desventaja real de ttcp, es que hace años que no ha sido actualizado. Afortunadamente, el código es de dominio público y está disponible gratuitamente. Al igual que *ping* y *traceroute*, ttcp es una herramienta estándar en muchos sistemas.

- **iperf** (*http://dast.nlanr.net/Projects/Iperf/*). Al igual que ttcp, iperf es una herramienta de línea de comandos para estimar el rendimiento de una conexión de red. Soporta muchas de las mismas características que ttcp, pero utiliza un modelo "cliente" y uno "servidor" en lugar del par "receptor" y "transmisor". Para correr iperf, inicie un servidor en un lado y un cliente en el otro:

```
node_a$ iperf -s

node_b$ iperf -c node_a
------------------------------------------------------------
Client connecting to node_a, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-11.3 sec   768 KBytes   558 Kbits/sec
```

El lado del servidor continuará escuchando y aceptando conexiones del cliente en el puerto 5001 hasta que usted presione control-C para detenerlo. Esto puede ser útil si corremos varias tandas de pruebas desde diferentes lugares.

La mayor diferencia entre ttcp e iperf es que iperf está siendo desarrollado activamente, y tiene muchas características nuevas (incluyendo soporte

IPv6). Esto lo hace una buena elección cuando construimos redes nuevas.

Salud de la red

Siguiendo la información a través del tiempo, usted puede tener una idea general de la salud de la red y sus servicios. Estas herramientas muestran las tendencias de su red y pueden incluso notificar a las personas cuando se presenten problemas. Muy a menudo, los sistemas van a notar el problema aún antes de que una persona llame solicitando soporte técnico.

- **cacti** (*http://www.cacti.net/*). Como mencionamos anteriormente, muchas herramientas utilizan RRDtool como programa de soporte (*back-end*) para armar gráficos con los datos que ellas recolectan. Cacti es una herramienta de ese tipo. Es una herramienta de gestión de redes basada en PHP que simplifica la recolección de datos y la generación de gráficos. Almacena su configuración en una base de datos MySQL, y está integrada con SNMP. Cacti hace muy sencillo el mapeo de todos los dispositivos en su red y monitorea todo, desde el flujo de la red hasta la carga del CPU. Tiene un esquema extensible de recolección de datos que le permite captar casi cualquier tipo de datos que se le ocurra (tales como señales de radio, ruido, o usuarios asociados) y desplegarlos en un gráfico en función del tiempo. Representaciones pequeñas (*thumbnails*) de sus gráficos pueden combinarse en una única página. Esto le permite observar el estado global de su red de una sola ojeada.
- **SmokePing** (*http://people.ee.ethz.ch/~oetiker/webtools/smokeping/*). Otra de las herramientas desarrollada por Tobias Oetiker es SmokePing. Está escrita en Perl y muestra la pérdida de paquetes y la latencia en un único gráfico. Es muy útil correr SmokePing en un servidor con buena conectividad a toda su red. Con el tiempo, revela tendencias que pueden apuntar a todo tipo de problemas de red. Combinado con MRTG o Cacti, puede observar el efecto que tiene la congestión de la red en la pérdida de paquetes y en la latencia. SmokePing puede enviar alertas cuando se encuentran ciertas condiciones, como cuando se observa una pérdida excesiva de paquetes en un enlace por un período de tiempo largo.
- **Nagios** (*http://www.nagios.org/*). Nagios es una herramienta de monitoreo de servicio. Además de seguir el desempeño de simples contactos (como con SmokePing), Nagios puede observar el desempeño de los servicios reales en varias máquinas. Por ejemplo, puede consultar periódicamente su servidor web, y estar seguro de que devuelve una página web válida. Si una verificación falla, Nagios puede notificar a una o varias personas vía correo electrónico, mensaje de texto al celular (SMS) o mensajería instantánea (IM).

  Aunque Nagios ciertamente ayuda a un único administrador a monitorear una red grande, sus funciones se destacan cuando usted tiene personal

de soporte, con responsabilidades divididas entre varios de sus miembros. La detección de problemas puede ser configurada para ignorar problemas pasajeros, y sólo cuando se amerite enviar las notificaciones únicamente a las personas responsables de solucionarlos. Si el problema sigue por un período de tiempo predeterminado sin ser atendido, se puede notificar adicionalmente a otras personas. Esto permite que los problemas temporales sean simplemente registrados sin molestar al personal, y que sólo los problemas reales tengan que ser atendidos por el equipo.