

Secure SHell (o de como ahora que padeces de insomnio quisieras morir de siesta)

"Los que sueñan de día vienen a conocer muchas cosas que escapan a los que solo duermen de noche. En sus confusas visiones logran ver algo de eternidad y se sobrecogen, durmiendo, al advertir que se han hallado al borde del gran secreto. A retazos, aprenden algo de la sabiduría del bien, y más todavía de la sabiduría del mal. Penetran, aunque sin timón ni brújula, en el vasto océano de la luz inefable y, asimismo, como los aventureros del geógrafo Nubiense aggressi suni mare tenebrarum, quid in eo esset exploraturi (se han propuesto explorar lo que hay en el mar de las tinieblas)".

Eleonora - Edgar Allan Poe

Secure Shell es un sistema de inicio de sesión seguro y un buen sustituto de telnet, rlogin, rsh, rcp y rdist. El RFC (Request For Comment - Solicitud para Comentario) de Secure Shell explica:

**"SSH (Secure SHell) es un programa para conectarse a otro equipo a**

traves de una red, para ejecutar comandos en una maquina remota y para mover archivos de una maquina a otra. Proporciona una exhaustiva autentificacion y comunicaciones seguras en redes no seguras."

Secure Shell admite varios algoritmos y protocolos, entre los que se incluyen:

BlowFish(Pez Globo): Creado por Bruce Schneier, usa un algoritmo de 64 bits.

Triple DES (Data Encryption Standar - Estandar de Cifrado de Datos): Diseñado originalmente por la National Bureau of Standars (Oficina Nacional de Normas) e IBM en 1974 y publicado en 1977, es usado por el gobierno estadounidense para la protección de los datos no clasificados y para las contraseñas por los sistemas UNIX-Linux. Cifra bloques de 64 bits de largo con una clave de 56 bits (8 caracteres de 7 bits de longitud).

IDEA (International Data Encryption Standart - Norma Internacional de Cifrado de Datos): Algoritmo de cifrado de bloques con una clave de 128 bits, más seguro y rápido que 3DES (Triple DES). Diseñado por James L. Massey y Xuejia Lai y publicado en Zurich en 1990. Es usado por PGP (Pretty Good Privacy - Privacidad Muy Buena de Phil Zimmermann).

RSA (Rivest-Shamir-Adleman): Utiliza un sistema de claves privada/pública. Está implementado en la mayoría de los navegadores de Internet. Puede usarse tanto para cifrar información como para ser la base de un sistema digital de firmas. Usado por PGP.

MD4 (y MD5): Algoritmo de resumen de mensajes que produce una huella digital unívoca de 32 bits de entrada especificada (es, en teoría, matemáticamente imposible crear un duplicado). Se utiliza en la autentificación de integridad de sesiones y archivos. También produce un número de 128 bits desde un bloque de texto de cualquier longitud. Es rápido, compacto y optimizado para ser usado en máquinas con pocos recursos. Fue creado por Ronald Rivest. Ver RFCs 1186 y 1319 al 1321.

Kerberos: Desarrollado en el Instituto de Tecnología de Massachusetts (MIT, Massachusetts Institute of Technology), su principal uso está dado en aplicaciones de red y está basado en servidores de terceras personas para la autentificación. Complejo y complicado de implementar y mantener, utiliza cifrado DES en su funcionamiento. Una versión (modificada y no compatible con el estándar) es usada por el Directorio Activo de Microsoft.

AES: Creado en por , utiliza claves de 128, 192 y 256 bits.

CAST:

SHA (Secure Hash Algorithm - Algoritmo Seguro de Dispersión): Desarrollado por NIST (National Institute of Standards and Technology - Instituto Nacional de Normas y Tecnología) y la NSA (National Security Agency - Agencia Nacional de Seguridad) de Estados Unidos, similar a MD4, excepto porque produce una salida de 160 bits en lugar de 128.

LDAP (Protocolo de Acceso Ligero a Directorios - Light Weight Directory Access Protocol): Es un modelo de autentificación distribuida multiservidor y multiplataforma muy potente y versátil. La versión de Microsoft es llamada Directorio Activo (Active Directory) debido a la modificación del estándar realizada por la gente de Redmond.

La compatibilidad con diversos algoritmos y protocolos fue buscada para que el producto fuera mas flexible y ampliable, de manera que se puede cambiar en cualquier desarrollo las rutinas de encriptacion sin modificar el comportamiento del sistema en general.

Tanto la autentificacion como el posterior cifrado de la sesion se realiza de manera totalmente transparente de cara al usuario, lo cual conlleva una curva de aprendizaje minima y/o inexistente.

Basicamente, la principal utilidad de SSH reside en el hecho de poder reforzar la resistencia de la red a "escuchas electronicas" (sniffers), ya bien brindando un shell seguro, como asi tambien pudiendo realizar todas las comunicaciones dentro de canales seguros, lo que evita en gran parte la captura de contraseñas y/o datos, al forzar a que todo el trafico viaje encriptado, pero con la ventaja de no tener que configurar un servidor para VPNs (Virtual Private Networks o Redes Privadas Virtuales) y el consiguiente mantenimiento del mismo.

Tambien se pueden cifrar sesiones PPP estandar sobre sesiones SSH estandar, lo que permite establecer eficazmente un tunel entre dos redes, como si de una VPN se tratara, aunque su uso mas difundido es para comunicarse con entidades externas desde detras de un cortafuegos (firewall o fw), como por ejemplo, una sesion de X-Window desde un cliente MS-Windows, haciendo uso de un tunel cifrado a traves de Internet o incluso enviar y/o recuperar correos de una manera relativamente mas segura.

Existen clientes ssh en casi cualquier Sistema Operativo (SO), lo que extiende su universalidad de uso en redes heterogeneas.

Es altamente recomendado usar el propio cliente scp durante la copia de archivos de/hacia un sistema SSH, debido a la muy buena implementacion del protocolo sftp y el consiguiente ahorro en el ancho de banda y capacidad de procesador(es) del sistema remoto, amen del tiempo empleado.

No tengo noticias de la implementacion de un servidor SSH bajo entornos operativos MS-Windows, pero es factible (personalmente testado en entornos de produccion) instalar el entorno CygWin y la version de libre distribucion de SSH (OpenSSH), permitiendo la funcionalidad de un servidor SSH bajo el SO de Microsoft y sin la necesidad de tener que disponer de un servidor SSH bajo otros sistemas operativos (como GNU-Linux u otros).

Este conjunto nos ofrece toda la versatilidad de la consola de los sistemas Linux, pero tambien soporta la implementacion de utilidades graficas, por ejemplo, redirecciones hacia el programa de administracion remota como WinVNC o incluso el mismisimo Windows Terminal Services, lo cual nos permite cruzar cualquier cortafuegos y realizar todo tipo de tareas remotamente y de una manera segura y comoda. Podemos, asimismo, restringir el uso de cualquier tipo de programas que consideremos, lo que dota de una extrema facilidad en cuanto a administracion de usuarios remotos se refiere, y sin tener que recurrir a programas de terceros. Una solucion muy simple para brindar cuentas restringidas.

Si bien parece una tarea, en principio, muy dificil de realizar, si antes nos tomamos una pequena molestia y leemos los manuales detalladamente (RTFM - Read The F... "ine" Manual), podemos implementar esta solucion medianamente rapido y sin mayores inconvenientes en nuestra red, lo cual mejorara sensiblemente la seguridad de la misma, sin tener que hacer concesiones que puedan debilitar la integridad de nuestro cortafuegos y el riesgo inherente que eso conlleva.

Y gracias a la existencia de las licencias GPL no tenemos como una unica alternativa, prohibitivamente caras soluciones comerciales, que no permitian muchas veces la integracion de otros tipos de sistemas, o el ambito de prueba, altamente necesarias para comprobar la eficiencia de la futura (o no) implementacion, al margen de evitar las discutidas practicas monopolisticas de algunas empresas de software.

En este punto ya, demas esta decir que Secure SHell es toda una necesidad, especialmente desde que las herramientas de escucha electronica (sniffers) son muy conocidas, y mientras sigan proliferando, como asi tambien las herramientas de busqueda y explotacion de vulnerabilidades, disponibles via Internet mediante una busqueda casi trivial.

Ademas cabe destacar que tenemos miles de sitios en Internet que publican toda suerte de formas de "saltar" las protecciones de seguridad y conseguir acceso a otros sistemas, computadoras y redes, ya bien como "prueba de concepto" o bien como exploit o fallo (bug). Tampoco debemos olvidarnos de las

puertas traseras, los troyanos (o caballos de Troya), los virus y demas fauna indeseable.

Los cortafuegos son herramientas poderosas, pero no deberian utilizarse en lugar de otras medidas de seguridad. Deberian ser usados adicionalmente a dichas medidas, como proxys y NAT e incluso, cortafuegos internos.

Igualmente no somos completamente inmunes a la escucha de todas nuestras transmisiones, ya que, si bien todo nuestro trafico esta siendo encriptado, via SSH, existen otras formas de capturar informacion de nuestra red/computadora, de manera totalmente pasiva y anonima, aunque mas avanzada en cuanto a su implementacion tecnologica, y la relativa dificultad en el ataque.

Seguiremos siendo vulnerables a la tecnologia TEMPEST (Tecnologia de Vigilancia de Pulsos ElectroMagneticos Transitorios - Transient ElectroMagnetic Pulse Surveillance Technology), que es la practica y estudio de captura y/o estudio de senales electromagneticas que emanan de una unidad (en este caso una computadora, router, switch, hub, etc.), pero eso es otra cuestion, ya que la proteccion frente a este tipo de amenazas es sensiblemente mas onerosa y mas compleja de implementar.

De todas formas, no importa que tan seguro sea el sistema, las claves DEBEN protegerse, ya que no tiene sentido invertir tanto tiempo y dinero en cifrar todos los datos, si se dejan las claves de cifrado en un archivo, escritas bajo el teclado o en un papel pegado al costado del monitor.

Mi frase favorita: "Que seas paranoico no significa que NO te esten vigilando".

Referencias: Ninguna =^)

Web: <http://www.ssh.com> <http://www.openssh.com> <http://www.kriptopolis.com> <http://www.cygnus.com>  
<http://ibt.uk.research.att.com/vnc> <http://www.securityfocus.com> <http://www.rfc-es.org>  
<http://www.openldap.org> <http://www.microsoft.com> <http://www.hackemate.com.ar>  
<http://www.enterthematrixgame.com> <http://www.nsa.gov:8080> <http://www.nis.gov> <http://www.first.org/first>

IRC: Canal #Hackemate en irc.elsitio.com

Bibliografia: Eleonora, de Edgar Alan Poe El escarabajo de oro, de Edgar Alan Poe Construya Firewalls para Internet, 2da ed., de D. Brent Chapman y Elizabeth Zwicky (McGraw-Hill). Departament of Defense Trusted Computer System Evaluation Criteria, National Computer Security Center (El Libro Naranja). The Matrix: Computer Networks and Conferencing Systems Worldwide, de John Quarterman (Digital Press).

Agradecimientos A Gloria... que paso mas horas jugando al solitario que yo redactando esto =)

Comentarios y Sugerencias Esta es una experiencia de aprendizaje para mi, he trabajado bastante configurando, instalando y administrando redes, pero redactando siempre tengo problemas, por lo que agradeceria cualquier comentario sobre ello, sientase libre de mandarme un mensaje a [webmaster@deabajo.com.ar](mailto:webmaster@deabajo.com.ar) con sus sugerencias. Tambien acepto donaciones ;-)

Copyright y otras yerbas Este documento es copyright (c) 2003 de Jorge Franco (a.k.a. Vampii). Se anima su distribucion, aunque no deberia modificarse este documento (Vease Comentarios y Sugerencias). Pongase en contacto conmigo si esta interesado en realizar una traduccion, esa es una de las modificaciones con las que puedo vivir. Acentos y enies omitidos deliberadamente Faltas ortograficas puestas aleatoriamente