

Saga de Seguridad

Indice

1.	Prólogo.....	3
2.	Introducción a la Seguridad.....	3
	2.1. ¿Estamos seguros?.....	3
	2.2. ¿por qué hackear?.....	5
3.	Mitos.....	5
4.	Inicios.....	6
	4.1. Breve historia.....	6
	4.2. Teoría de la seguridad cuando estamos conectados.	7
	4.3. ¿Cómo accederá entonces un hacker a nuestro ordenador?.....	8
	4.4. Bueno, y ¿cómo podemos evitarlo?.....	8
5.	Ideas.....	9
	5.1. Normas de seguridad.....	9
6.	Firewalls.....	10
	6.1. Intrusismo:.....	11
	6.2. ¿Qué hace un Firewall?.....	12
	6.3. ¿Qué ventajas nos puede ofrecer?.....	12
7.	Implementar la seguridad.....	13
	7.1. Agujero: Mala configuración de la conexión y/o de la red.....	13
	7.2. Agujero: Vigilar los puertos de comunicaciones, los TCP o UDP.	13
	7.3. Ataque Dos (Denial of Service) Denegación de Servicio.	14
	7.4. Troyanos, control remoto de equipos.....	14
	7.5. Escaneo de puertos.....	14
	7.6. Detección de proxys mal configurados.....	14
	7.7. Firewall.....	15
8.	Al ataque.....	15
	8.1. Vulnerabilidad de Windows 9.x.....	15
	8.2. Conexión directo a recursos compartidos de win9.x.....	17
	8.3. Contraataques.....	17
	8.4. Autenticación hash y los servidores de acceso telefónico en win9.x.	17
	8.5. Atacar al registro remotamente.....	18
9.	Puertas traseras.....	18
10.	Black Ice Defender 2.1.45.....	20
	10.1. Settings/configuraciones.....	21

Saga de Seguridad

1. Prólogo

Bueno, como veo que os vais enfriando y aprovechando que tengo fiebre y no puedo salir de casa, me he preparado unas notas, a ver si sirven para ayudaros en algo, o al menos, a que discutamos de cosas.

A veces he leído cosas en las news que no comparto, y que además creo que andan bastante desencaminadas con la realidad, eso creo, a menos claro que tanto haya cambiado el asunto desde mis inicios en la informática.

Por ejemplo:

Yo sé que si quieren robar en mi casa lo harán, no sabré quienes, pero lo harán. Ello no significa que no tenga puertas y ventanas, que las cierre cuando no estoy (incluso cuando estoy), o que me planteé poner una alarma antirobo. ¿verdad?

Entonces, la frase de ¿para que quieres herramientas en tu ordenador si los que saben entrarán igual, y ¿los que no saben no entran aún sin defensa?

Quiero decir, que no comparto las ideas de hacer innecesaria una buena política de defensa en nuestras conexiones a Internet, y por supuesto muy fervorosamente en aquéllas que lo son continuas y con IP fija.

Una buena defensa evitará cualquier intento de penetración, en busca de lo que sea, en nuestro ordenador, y si efectuamos un seguimiento lógico y "no caducamos", creo que las posibilidades se reducirán exactamente a aquéllos que realmente quieren penetrar en el sistema de "pepito", por las razones que sean, y que en éste caso, aumentaremos las defensas, al fin y al cabo es una guerra total, en la que participan empresas, usuarios, hackers, crackers, lamers, tontos, aprendices, trolls, pornos, no pornos, católicos, protestantes, musulmanes, judíos, etc... etc... etc... No acabaría nunca. Quiero decir, por si no me explico demasiado bien, que aquéllos que sepan desde donde le van a venir los ataques, pues tendrán ventajas e inconvenientes, las ventajas son que saben algo más que los usuarios normales y los inconvenientes son que tienes enemigos. Supongo que un servidor que defiende posiciones Israelíes, será atacado por hackers Palestinos, sería lógico por otra parte.

En resumen, sí a las medidas de seguridad, sí a la defensa de nuestras conexiones a Internet, NO al relajamiento, NO al pánico, NO a la desinformación...

2. Introducción a la Seguridad

2.1. ¿Estamos seguros?

Esta pregunta está de moda últimamente, desde luego existen ciertos tabúes al respecto.

En cierto momento intenté clarificar varios conceptos y ayudar a algunos compañeros ante sus dudas ante tanta información por la RED. La verdad es que algunos salieron un poco ranas, pero como tengo los artículos que publiqué y seguro que os encantan, pues los pongo.

NOTA: Cualquier coincidencia con la realidad es eso, simple coincidencia.

Nada de lo expuesto y en ningún momento se refiere a mi persona, la realidad y la ficción se acercan tanto a veces que puede confundirnos, normalmente el árbol no deja ver el bosque, porque si ves el bosque es que tienes ojo de águila.

No espero que me creáis, sino más bien que os sirva de camino.... Nada de lo que expongo es cierto y verdadero al 100%, las diferencias entre métodos y métodos son simple y llanamente diferencias entre la imaginación de unos u otros. Si de algo estáis seguros y yo digo lo contrario, seguramente lo correcto es lo que tenéis seguro.

Mientras han existido, existen y existirán ordenadores, han existido, existen y existirán hackers.

Para explicarlo a mi manera, tomaré prestado el punto de vista de hacker.

Hubo un tiempo en que a hurtadillas, ciertos grupos de personas (la mayoría de habla inglesa) nos...digo SE dedicaron a la investigación del océano de inet. Hoy el 100% trabaja en el lado contrario, la defensa de los sistemas.

Las primeras normas que se establecieron para el grupo de arcangeles eran claras y concisas, las escisiones del grupo condujeron a la presencia de crackers, pheakers, lamers y otras definiciones.

Los diez mandamientos no sólo existen en la religión cristiana.

- 1) No dañar INTENCIONADAMENTE ningún SISTEMA.(NINGUNO!!!!)
- 2) No alterar los archivos de sistema, a excepción de los imprescindibles para asegurar nuestro anonimato y posibles regresos.
- 3) No dejar ningún rastro hacia nuestros datos personales verdaderos.
- 4) Ojito con quienes compartimos nuestra información. Hay muchos tramposos.
- 5) No dar datos personales verdaderos a nadie.
- 6) No hackear ordenadores del gobierno, tienen tiempo y recursos para encontrarnos.
- 7) No uses códigos delante de gente, de NADIE. Espera a estar sólo y seguro.
- 8) No tengas problemas en ser paranoide, recuerda que estás quebrantando la LEY.

No tengas lástima para almacenar todos los datos en tu disco duro, pero hazlo encriptado.

Guarda tus notas en sitios extraños y lejos de tu ordenata. Y no te rías que es peor.

- 9) Mejor no dejar notas, ni nada por el estilo. Eso de "ESTO HA SIDO HACKEADO POR..." se lo dejamos a otros...(¿Lamers?)
- 10) No tengas miedo en preguntar, con suerte los más experimentados te digan algo, no será verdad pero algo te dirán seguro. Nadie explica sus formas, cuidado con esto. Uno se enseña estudiando y trabajando.

Finalmente, ten el hack actualizado. Puedes navegar en ordenadores todo lo que quieras, leerás todos los textos que quieras, pero nunca lo sabrás todo. No tendrás nunca una emoción igual como la del primer sistema que hackees con éxito. (Pienso que hay algunas emociones mayores, pero hay que conseguirlo)

2.2. ¿por qué hackear?

El objetivo siempre ha sido el conocimiento, si ya sé que mucha gente normal cree que eso no justifica los medios utilizados.

Un hacker que se precie nunca atentará contra usuarios domésticos, se enfrentará a GOLIAT, y éste siempre viene representado por el enemigo grande, el poderoso, el que representa los males del mundo.

Los otros, los que buscan sólo hacer daño por el placer de hacerlo no son hackers.

3. Mitos

- 1) **Mito:** Este antivirus puede detectar los virus, gusanos y caballos troyanos del hoy y del mañana.
Cierto: No existe tal tecnología, es pedirle a un programa que entienda que hace otro programa (¿un cerebro de programador?), en tiempos de DOS ese era el "slogan" de publicidad, pero esos antivirus simplemente no servirían con virus que infecten documentos en Word o Excel.
- 2) **Mito:** En Linux(Unix) no hay virus
Cierto: ¿Y los virus de Script? ¿y los infectores de ejecutables ELF?
- 3) **Mito:** En Linux(Unix) el sistema quedará en pie por mas ataques víricos que hayan, eso es lo importante.
Cierto: Es cierto que los escritores de virus para Windows y DOS, les gusta borrar secciones críticas para que el sistema no pueda arrancar otra vez. Esto se debe a que en Windows 95/98 los usuarios siempre tienen privilegios de súper usuarios, pero si usasen Windows NT o 2000 con NTFS activado en todas las particiones y corriésemos un virus con usuario restringido, el daño no sería mucho (salvo los documentos del usuario restringido que pueden comprometerse). Así Windows 2000 y Linux ofrecen la misma seguridad. Otro punto es que reinstalar Win 95/98 no es cosa del otro mundo. Linux puede quedar en pie, pero será un triste consuelo si mis documentos y archivos de datos importantes quedan destruidos.
- 4) **Mito:** Los ataques de virus son muy frecuentes.
Cierto: Los periodistas son muy escandalosos, mas pérdidas de datos se han dado por culpa de la mala operación de usuarios finales que por culpa de virus, caballos troyanos, etc.
- 5) **Mito:** Microsoft tuvo una pésima idea en implementar un lenguaje de scripts para Windows ("ILOVEYOU" fue escrito con estos lenguajes)
Cierto: Ni instale Linux o alguna versión de Unix, estos desde que fueron concebidos tienen lenguajes de sripts (Born-Shell, Korn-Shell, C-Shell) y prácticamente no pueden vivir sin tener alguno habilitado. Antes Microsoft se había demorado demasiado en implementar algún lenguaje de scripts para Windows.

- 6) **Mito:** Tengo lo último en Antivirus, Firewalls, detección de intrusos, etc.. Ya no tengo de que preocuparme.
Cierto: Aunque tenga seguro de vida, cinturón negro de karate y una Bazooka, fíjese a ambos lados antes de cruzar la calle. Realmente el conocimiento es la mejor medicina, la ignorancia será su perdición.
- 7) **Mito:** Cierro mi red contra cualquier contacto externo. Seguridad total.
Cierto: En un amplio porcentaje los ataques a sistemas son desde el interior de la organización (séquese la lágrima por haber adquirido ese costoso firewall).
- 8) **Mito:** Debo proteger mi información contra intrusos sin importar el costo
Cierto: ¿Trabaja para una agencia secreta gubernamental? ¿Tiene información "Top Secret" del gobierno sobre civilizaciones extraterrestres? ¿Es perseguido por Papparazi todo el tiempo? ¿Tiene para patentar la cura contra el SIDA?...Vamos! con software gratis, un poco de cuidado y buenos conocimientos es mas que suficiente. La seguridad es importante pero también lo son otros factores como la facilidad de uso y la funcionalidad.
- 9) **Mito:** El virus 'ILOVEYOU' causo pérdidas por 7.000 millones de dolares.
Cierto: Esta cifra fue calculada por una entidad llamada Computer Economics (www.computereconomics.com), los periodistas alrededor del mundo repitieron esta cifra como loros. Yo dudé y envié un correo electrónico (23 de Mayo de 2000) a esta entidad para que me mostrase como hizo para calcular dicha cifra, aún sigo esperando la respuesta.

4. Inicios

Tabú: ¿Qué pasa con la seguridad de Windows 98 en Internet?

4.1. Breve historia

En 1981 cayó en sus manos un ZX81 y se enamoró, y lo hizo como lo haría de una mujer, compartió tiempo y dedicación, se instruyó, estudió, leyó, ... Llegó a conocer a su nuevo amigo más que a sus propios amigos humanos. Pero como casi todo, su amor se extinguió, y lo hizo en cuanto empezó a conocer al Spectrum, y luego al Vic, y al Commodore, y al.... Al final comprendió que no estaba enamorado del aparatito, sino de lo que llamaban &INFORMÁTICA&.

Fueron tiempos de enseñanza, de horas perdidas, buscando los motivos, la razón del todo... ¿por qué? era una continua pregunta a cada paso que daba.

Se unió a otros en su misma situación y juntos comenzaron andaduras.

Pasaban los años, y, llegó Internet, los servidores, evitar el pago a telefónica, la intrusión... El fin justificaba los medios, saber, conocimiento, hurgar...

AVENTURA!!!

Pero todo llega, y un buen día recibió una pequeña advertencia, de como era y de donde procedía era toda una señal. Paso unos días difíciles, pensó y repensó, y lo volvió a pensar... ¿había llegado el momento? Sí. Al final tomó la decisión, sus conocimientos debían de dejar de utilizarse en beneficio del ¿mal?, aunque divertido

no parecía muy correcto, sí mal. ¿Cómo? Pues lo dejó, todo, lo dejó todo. Arrinconó los ordenadores, metió en cajas apiladas en la buhardilla todo su material, direcciones, proxys, routers, blue-box, documentación, exploits, agujeros, listados, ... El tiempo pasó, ese lo cura todo. Incidente incluido.

¿1995? o ¿1996?

A alguien en la empresa se le ocurrió que debido al auge de la informática se debería informatizar todas las dependencias. ¿Pero y técnico, tenemos técnico? ¿Dónde? ¿Quién?

Oye y que tal fulanito, ese tenía algunos trastos de esos.

¿Te gustaría echarnos una mano? Uy! y ¿porqué no?

Cualquier coincidencia con la realidad es eso, pura coincidencia.

4.2. Teoría de la seguridad cuando estamos conectados.

Hay CABALLEROS hackers (Como debe haber los JEDI en el pensamiento de George Lucas -Star Wars-) y los hay que abusando de ese concepto hacen maldades (Crackers, pheakers, lamers... lo que se os ocurra).

Como toda buena RELIGIÓN, tiene sus mandamientos, los he puesto en algún otro artículo.

¿Estamos seguros?

Bueno, dependerá de algunos factores y de nosotros mismos.

¿Queremos estarlo?

La verdad es que los hackers no van por ahí irrumpiendo en ordenadores personales de usuarios domésticos y que además tienen el añadido de conectarse aleatoriamente con un módem (aunque ya tenemos a gran cantidad que se va poniendo la adsl, y así empezamos a entrar dentro de las posibilidades), y además utilizan windows98 en su mayoría (descartaremos los otros s.o. de momento).

Windows 98, por definición es parco en dar posibilidades de intrusión, y lo es por que carece de herramientas de acceso remoto (a menos que nosotros las instalemos) en su propia instalación.

Hay dos formas de penetrar en un sistema, o estás delante de él o lo tienes que hacer remotamente. No hay más.

Descartaremos el estar delante, así que debemos centrarnos en hacerlo remotamente.

Como digo, Windows 98 no tiene herramientas de acceso remoto por defecto, aunque podemos instalar algunas que sí vienen en el CD original y/o incluso de terceros. Pero tampoco es que digamos que no es posible entrar, hay muchos "exploits"-errores, puertas, etc...- En los protocolos (especialmente TCP/IP, o en el redirector NETBIOS) que pueden hacer que se obtenga información, que no un control total de la máquina.

Somos nosotros mismos, los que incoscientemente dejamos ciertas puertas abiertas y que además no controlamos las posibilidades, es decir, leer disquetes de terceras personas, ejecutar archivos desconocidos, instalar programas bajados de cualquier parte de internet, despreocuparse del correo.

4.3. *¿Cómo accederá entonces un hacker a nuestro ordenador?*

Pues seguramente ni siquiera será él mismo el que nos deje una herramienta de acceso remoto, puede haber sido cualquier otro, pero lo que sí hará es escanear nuestros puertos en busca del servidor de esa herramienta y que en caso de existir le dará el control de nuestra máquina.

La otra forma será más simple, buscará los puertos 137/138 y 139, en busca del redirector NETBIOS y la posibilidad de entrar a nuestros recursos compartidos.

En el primer caso hablo de los "Troyanos", en un principio surgieron para darnos ese control remoto que no poseían los sistemas windows, y que luego fueron derivando en ser utilizados para acceder de forma no autorizada.

En el segundo hablo de los recursos compartidos de nuestro ordenador y que por dejadez nuestra están activados, llámese "Compartir archivos y impresoras", o tener protocolos innecesarios configurados, IPX, NWlink, ...

Los conocidos Firewalls sólo servirán de advertencia para ver la cantidad de personas que se dedican a escanear rangos de IPs en busca de los troyanos, en realidad si no tenemos ninguno en nuestro sistema, pues no pasa de eso, de un escaneo. Ello me recuerda que no hay que contestar a ninguno de ellos, ni con ping, ni con nada. Ni saben que existimos.

(Y lo afirmo, los firewalls no son perfectos, también tienen exploits, os asombraríais con que facilidad se puede saltar estos programas)

Por tanto, deberemos preocuparnos de tener controlado nuestro ordenador para no tener ningún troiano y por otra parte cerrar los puertos en la conexión a internet, que no en la de intranet o LAN (bueno, dependerá de la LAN y de lo que nos fiemos).

4.4. *Bueno, y ¿cómo podemos evitarlo?*

En el caso de los troyanos (mal llamados virus) debemos seguir unas pautas rigurosas, tales como no fiarse de información almacenada en disquetes de desconocidos, de las instalaciones de programas de Internet de páginas dudosas, de no ejecutar archivos que desconozcamos que son, de desconfiar de los adjuntos en los correos de desconocidos, de desactivar los modos de html y ejecución de controles ActiveX en los mensajes de correo (sólo texto, plano), y porque no, tener un antivirus siempre a la última.

En el segundo caso sólo hemos de hacer unas pequeñas configuraciones en nuestro sistema:

- **Quitar protocolos que no usemos**

Clic derecho en entorno de red Ventana Red, pestaña Configuración

Elegir el adaptador de salida a Internet, normalmente Acceso telefónico a Redes, pero si tenemos conexión por otro medio será otro el adaptador.

Eliminar las asociaciones de protocolos distintos a TCP/IP a nuestro adaptador.

Sólo al de salida a Internet, si tenemos uno de LAN los dejaremos por si son utilizados.

- **Desvincular servicios de TCP/IP innecesarios**

Elegimos el adaptador de salida a Internet propiedades pestaña enlaces

Sólo puede quedar activo, en todo caso, el cliente de redes Microsoft.

Nada de otros protocolos, ni compartir archivos y impresoras...

Ante el posible mensaje de No ha seleccionado una unidad con la que crear vínculos. ¿Desea seleccionar una ahora?, la respuesta es NO.

5. Ideas

Los hackers atacan ip's fijas de servidores en la red, nunca amenazan la seguridad de usuarios particulares con ip's cambiantes.

Los escaneos que se sufran son efectuados por aprendices, en busca de información, en principio no para atacar.

Sin puertos abiertos y con servidores (troyanos) no activos en nuestro ordenador, les será difícil introducirse en nuestro sistema, aunque no imposible.(por supuesto no voy a explicar cómo)

Cualquier "Lamer" especie de autosuficiente hacker sin pudor ni moralidad, puede efectuar un ataque DoS contra cualquier ip activa, y dependiendo de las conexiones, ancho de banda, tanto del atacante como la posible víctima, en pocos minutos saturar nuestra conexión y tirarnos de la Red. Ello no significa que hayan entrado en nuestro sistema ni que nos hayan fastidiado nada. En realidad esto está muy mal visto en la comunidad Hacker.

Existen herramientas para revisar nuestros puertos, pero que a su vez sirven para comprobar los de los demás, son los escáneres, hay multitud de este tipo de herramienta, en principio dirigidas a los Administradores de sistema y que finalmente se utilizan por los hackers para sacar información del objetivo.

Sabed, que un objetivo vulnerable o no, ha de sufrir un seguimiento, el cual podría convertirse en exhaustivo si el interés del intruso es proporcional a la dificultad de acceder al mismo.

Una conexión corriente de usuario, que cambia de ip cada vez que se conecta es difícil de atacar, siempre OJO!! que no tengamos troyanos activos, y que seamos ajenos a los escaneos (no tener un firewall, no activar el estado de los puertos (netstat) y observar el tráfico en nuestro ordenador).

Si tenemos un troyano activo, BO, Netbus, SubSeven, Control total, etc... (cualquier antivirus detecta su presencia), y además no se vigilan los puertos, se prestaría a un dominio total de nuestra máquina por parte del intruso. Y en realidad esto último es lo que se busca con los escaneos que sufrimos, ver si hay activos troyanos.

Muchos logs de los firewalls, buenos o corrientes, marcan los pings del Netbus, BO y Subseven, si no tenemos esos troyanos, mejor pasar de los pings, y con la información de IP atacante, mandar un e-mail a nuestro ISP, informándoles de los escaneos de que somos objeto. Cosa que podemos hacer también con el ISP del atacante si sabemos descifrar los datos que nos aporta el firewall.

5.1. *Normas de seguridad*

- 1) Instalar un firewall

- 2) Ante un aviso de escaneo, ver los datos del log.
- 3) No intentar averiguar si el atacante está activo, no efectuar pings a su IP, delataríamos nuestra existencia, con ello si provocamos su chulería nos podemos ganar un DoS inmediato y la caída de nuestro sistema.
- 4) Abrir Netstat en ms-dos o símbolo del sistema(w2k) y observar el tráfico y puertos abiertos, si hay alguno que desconocemos o nos haga sospechar que ha logrado superar el firewall, cortar la conexión a internet enseguida.
- 5) Con los datos del log, advertir de los escaneos a los ISP, suelen tener una dirección e-mail para tal efecto.
- 6) Acostumbrarse a ver los escaneos, pero no pasar de enviar los e-mails a los ISP. Si al final nos hacen caso, no encontrarán ISP que les faciliten conexión, y conseguiremos que sólo los Hackers de verdad queden en la Red.

NOTA: Los buenos no necesitan casi nada para centrarse en un objetivo y conseguirlo.

En cuanto a los que tengáis IP's fijas (o semi-fijas), hay algunos ISP en España por ejemplo, que protegen los puertos del 1 al 1024 (aprox) ellos mismos, y cuentan normalmente con un departamento de seguridad que monitoriza la red, ONO, Infoville, etc...

Ello obliga a la utilización de puertos por encima del 1024, con lo que nuestras aplicaciones activas (ftp, http, telnet, u otras) deberán configurarse para los puertos que deseemos (recordemos que podemos tener hasta el 65535), ello hace que la IP que tenga que acceder a nuestros servicios conozca el puerto para establecer la comunicación. OJO!! va para todos, los escaneos no se hacen al total de puertos posibles sino a los que presumiblemente deben estar activos, el telnet por el pto23, o el ftp por el 21, si ignoran que tenemos activo el 26000 o el 25000, no encontrarán actividad de este tipo en nuestros sistemas, y no podrán utilizar los conocidos bugs de las aplicaciones ftp, http, etc... Os aseguro que existen BBS con la suficiente información sobre los errores(bugs) y comandos necesarios paso por paso (step to step) para introducirse al sistema gracias a estos agujeros.

Pero, si no encuentran actividad, pasan a otro.

No voy a poner herramientas de monitorización o testeo de puertos, podéis comprobar vuestro ordenata en www.grc.com, no es la panacea, pero una idea os dará.

No tener recursos compartidos (archivos e impresoras) cuando conectéis a Internet, con SMBS aparecerían inmediatamente y aunque los tengáis con clave, una simple brute force haría saltar el recurso y dejaros algún regalito.

6. Firewalls

Sea por software o por hardware, estos dispositivos son exclusivamente para intercalar entre nuestra red y Internet, con el fin de vigilar las entradas/salidas de paquetes por los puertos de los ordenadores.

Adicionalmente sus configuraciones nos permitirán la posibilidad de restringir las entradas/salidas de los puertos seleccionados.

Mientras que win2000 tiene la posibilidad de hacerlo sin necesidad de ningún software de terceros, el XP incluye una de estas herramientas bastante correcta.

Para el que no lo sepa:

En NT/2000:

Propiedades de conexión a Internet

marcar el protocolo TCP/IP

propiedades

Avanzada

Opciones

Filtrado TCP/IP

propiedades

podemos habilitar el filtrado a todos los adaptadores

Tenemos tres listas

PUERTOS TCP, PUERTOS UDP Y PROTOCOLOS IP.

Y dos opciones,

permitir todos, permitir sólo (los que indiquemos en cada lista).

En principio yo aconsejaría los firewalls para personas con conexión permanente a Internet, por hardware para LAN que sale a INET, y por software a los usuarios domésticos.

6.1. ***Intrusismo:***

- **Ataques DoS (Denial (Deny) of Service)**

Aunque realmente es un ataque para desbordar la pila y dejar momentáneamente inutilizado el ordenador, para tener que reiniciarlo. El propósito en todo caso sería hacerle perder el trabajo que no se haya guardado en disco.

- **Caballos de Troya (troyanos)**

Son programas, la mayoría parecen inocentes juegos o bromas, son específicamente para dar el control del ordenador a un atacante. El mayor problema es que son muchos los que escanean buscando los troyanos activos y que su único fin es destruir.

- **Barridos**

Simplemente están buscando puertos TCP/IP o UDP abiertos e intentar aprovecharse de los servicios que dependen de ellos. Normalmente es el primer paso antes de un ataque.

Recordemos que un puerto está abierto cuando al recibir una petición de establecimiento de conexión el sistema responde en caso contrario se considerará cerrado.

- **Detectar proxies**

Aquí quizás el movimiento es de alguien con más imaginación, pretenden recopilar información de los proxies que normalmente están entre nuestro ordenador y el router/firewall/conexión y que utilizamos para compartir una

conexión para una red. El objetivo no es entrar en esa propia red, es algo más ingenioso, se busca las posibles malas configuraciones y/o exploits, con el fin de poderlos utilizar en contra de otros objetivos y así hacerlo enmascarados (anonimamente).

- **Smurf/Fraggle**

Estos ataques o "pitufos" siempre amparan ataques masivos a servidores. La técnica no es fácil, se mandan paquetes a una subred con una IP falseada y que pertenece al servidor que se quiere atacar, todos los que reciben los paquetes emiten una respuesta a esa IP, y con ello sobrecargan inmediatamente al servidor, haciéndolo caer o en todo caso que deniege servicios a clientes debidamente autorizados.

La diferencia entre Pitufos y Fraggle son el tipo de paquete enviado, UDP o ping.

Recordemos, cuando en una red configurada con hubs, un equipo lanza una petición ésta irá dirigida a todos los ordenadores de la misma, hasta que el destinatario responda (broadcasting); esto se puede evitar con la utilización de swichs, que por una parte no nos divide el ancho de banda en cada puerto (los hubs si lo hacen) y además cualquier petición emitida sólo llegará al destinatario por medio de la MAC de su tarjeta de red (es única para cada adaptador fabricado en el mundo).

6.2. *¿Qué hace un Firewall?*

Éste término anglo-sajón designa una utilidad informática cuya función es el aislamiento de redes de otras redes. Se supone que es una barrera lógica de protección delante de nuestro propio sistema, y que debería examinar todos los paquetes entrantes y salientes. El filtrado de tales paquetes se efectúa siguiendo las configuraciones que consideremos. Es muy importante que el firewall que tengamos vigile los salientes, ya que con ello mantenemos a los troyanos controlados aún si los tenemos dentro del sistema.

La verdadera potencia del Firewall reside en su capacidad de decisión de dejar pasar un paquete en uno u otro sentido. Gracias al bit ACK, también puede saber si el paquete proviene de una conexión establecida o un intento de penetración externa. Y además, el llevar un registro (logs) de todo el tráfico e intentos de conexión.

6.3. *¿Qué ventajas nos puede ofrecer?*

En principio y como norma general (ya que también existe la posibilidad de rodear al firewall y penetrar en un sistema), nos protegerá de tráfico indeseado desde el exterior.

Impedirá que utilicen nuestro ordenador para atacar otros.

Limitar la acción de los troyanos al impedir paquetes salientes que no autoricemos.

Investigando los logs, encontrar referencias a ataques predeterminados y su origen.

Conocer los puertos utilizados por las aplicaciones.

7. Implementar la seguridad

Vamos a ver los sistemas Windows, al fin y al cabo las encuestas dicen que son los que más usamos.

Cuando nos conectamos a Internet se nos asigna una IP pública, es una dirección que nos identificará durante el tiempo que mantengamos dicha conexión, por supuesto si es conexión permanente la IP será fija(casi con seguridad). La IP facilitará la entrada a los pertinaces busca recursos en cuanto nos descuidemos. Si la duración de la conexión no es grande, pues el peligro (aunque está presente, y de muchas formas) es menor. Estoy seguro que la mayoría de los que se conectan no disponen de unas mínimas normas de seguridad, ni siquiera empresas con pequeñas redes y salida a Internet.

Aunque no los vamos a ver en este artículo, recomiendo con todas mis fuerzas la instalación de un Firewall en conexiones permanentes, y si os lo podéis permitir, mejor hardware que por software, pero bueno ya veremos algo.

7.1. *Agujero: Mala configuración de la conexión y/o de la red.*

Un usuario doméstico fallará en la configuración de la conexión, sea por módem u otra, pues ésta se realiza normalmente de forma automática en WindowsX, añadiendo protocolos y servicios de red, tanto a los adaptadores de redes domésticas(si las hay) como a los de acceso telefónico y/o otro adaptador para la conexión a Internet.

Solución: Revisar la configuración y eliminar protocolos innecesarios en la conexión a Internet. Deberíamos dejar sólo TCP/IP.

En cuanto a los servicios del protocolo, deben desactivarse los que no necesitemos, que serán todos (seguro) pero especialmente "Compartir impresoras y archivos".

Netbios, si nos es posible y sabemos cómo, podríamos probar a desactivarlo.

7.2. *Agujero: Vigilar los puertos de comunicaciones, los TCP o UDP.*

La vigilancia la debería realizar un firewall (se rumorea que Whistler lleva uno incorporado, será verdad¿?). De todas formas siguiendo reglas de filtrado TCP/IP podemos bloquear/permitir los puertos que utilicemos/no utilicemos. (mejor permitir a los que utilicemos, que son menos)

El filtrado es una característica en Windows 2000.

De recordatorio, los más utilizados (si nadie me contradice) son:

21 FTP

25 SMTP

80 WWW

110 POP

119 NNTP (ojo, algunos grupos en cotopaxi están en el 1190, por ejemplo)

137 al 139 son utilizados por NETBIOS, si lo tenemos desactivado, jem jem, y sinó ¿???

143 IMAP

443 HTTPS

531 IRC = troyanos y más troyanos, abomino del IRC I'm sorry.

7070 RealAudio, por si lo tenemos instalado.

555 phAse zero

1243 SubSeven

31337 Backorifice

... ehhhhhh, que estos hemos de bloquearlos, joder ya se me escapaban....

La verdad es que algo que nos servirá también para proteger nuestra conexión a Internet es un buen Anti-virus, que sí hombre que sí, que seguro que es bueno, ahora, eso sí, la pregunta del millón ¿Cuál? Pues escoge tu mismo, o que alguien nos ayude a elegir...

7.3. *Ataque Dos (Denial of Service) Denegación de Servicio.*

Este ataque sólo nos inutiliza el equipo hasta que lo reiniciemos, reconocerlo no es fácil, la mayoría de las veces va y lo casca antes de poder hacer algo, que digo la mayoría... siempre.

Verdaderamente, no sé si lo comenté hace algún tiempo, esto no significa ninguna entrada a nuestro equipo, puede hacernos perder algunos datos que no se hayan guardado y poco más, creo. Reiniciamos y listo, quien no lo hace (con windows :-)))))). Por supuesto, el que utilice IP fija tiene un pequeño problema, deberá ir pensando en quién le quiere tanto. (La comunidad no ve con buenos ojos utilizar armas para ataques DoS, puede que el demonio (un ex-ángel) si que le guste).

Por supuesto deberán darse unas pequeñas condiciones para el éxito del DoS.

7.4. *Troyanos, control remoto de equipos*

Permiten el control del sistema al atacante, un buen Antivirus y listo, en cuanto intenten colarnos uno empezará la sesión musical...

De todas formas, conociendo los puertos que utilizan, o bloquearlos y/o observar el tráfico que generen, para esto se necesita un firewall. (Si ya se que hay otras herramientas, y del sistema....)

7.5. *Escaneo de puertos*

Nos escarban todos los puertos, en busca de identificar que puertos TCP y/o UDP están activos y a ser posible abiertos, es un proceso de recopilación de información para su posterior uso.

Últimamente es el pasatiempo favorito de los aprendices cuakers, la mayoría terminan siendo lamers, trolls y revienta grupos de noticias, con sus aseverancias de la libertad total y el ataque indiscriminado a todo lo que se mueva, lo malo está en los medios que utilizan para alcanzar su fin, los trolls son para mí los que no superan la barrera de la inteligencia y se vuelven retrogradados, están deprimidos...

7.6. *Detección de proxys mal configurados*

La pantalla que efectúan los proxys entre internet y nuestro/s equipo/s puede ser utilizada, esto es materia de buenos hackers, digo que puede ser utilizados para

realizar incursiones a otros sitios, sin desvelar su identidad (IP) pues utilizan a éstos, que al fin y al cabo comparten la conexión con varios equipos de una Red.

7.7. Firewall

Firewall = fuegomuro, muro al fuego, muro ante el fuego, barrera al fuego, ...

Aquí diremos Cortafuegos y chin-pun.

Pos vale, y pa que sirve este cortafuegos, nos vamos a dedicar ahora a echar agua como los bomberos? Pues no, esto es un término utilizado para definir (o al menos así lo intentan) esa barrera lógica que establecemos entre Internet y nuestra RED, aislándola (bueno aísla redes de redes, sería más correcto), y su función sería, y además sería, examinar todos los paquetes que intenten atravesarla (la barrera lógica) o atravesarlo (firewall). Por supuesto, con nuestra inconmensurable configuración, realizaremos una especie de Mandamientos, para que el firewall, deje o no deje, pasar al amigo o amiga de fuera a dentro de la discoteque, y de dentro a la calle, vamos eso es lo que yo le pediría a un buen firewall, los que entran y los que salen...

Como digo, un firewall deberá interceptar todos y cada uno de los paquetes destinados a, o procedentes de nuestro equipo, y lo deberá hacer antes que cualquier otro servicio los pueda recibir.

Un puerto estará abierto sí:, cuando llega un paquete de petición de establecimiento de conexión, el sistema responde. En caso contrario el puerto está cerrado y no puede conectarse con él.

Un buen firewall después de analizar el paquete, decidirá si lo deja pasar o no, si se debe responder o no. Y además diferenciará si el paquete pertenece a una comunicación establecida o si es un intento de penetración externo.(no confundir el término penetración, gracias.)

Un buen firewall llevará un registro detallado del tráfico (log) y los intentos de conexión.

Los hay en hardware y en software, mejor hardware pero son algo carillos para un usuario doméstico.

En software, los hay de pago y freeware para uso personal.

ZoneAlarm (regularcillo)

BlackIce Defender (Supera el notable)

AttGuard (que bueno, que bueno...)

Norton (No lo he probado)

La verdad es que fui probando, en mi red(trabajo) uso AttGuard (para protegerme de mis usuarios, jeje) pero la Red tiene un cortafuegos por hardware y muy bien configurado, con que sepáis que no lo he configurado yo, pues ya sabéis que está bien...;-)

8. Al ataque

8.1. Vulnerabilidad de Windows 9.x

Seamos realistas, Windows 9.x no fue diseñado para ser un sistema seguro, sino más bien fácil de usar, se sacrificó la seguridad, al menos yo lo creo así.

En principio NT sí que buscaba esa seguridad, aunque ya sabemos que parece que no se libra nadie de agujeros, vulnerabilidades y otras hierbas.

También sabemos que w2000 mejoró ese aspecto en referencia a NT, y suponemos que Whistler hará lo mismo.

En cuanto a Windows 9.x, esto constituye un riesgo elevado, los administradores que a fecha de hoy, sigan utilizando como clientes éste S.O. son muy atrevidos y en cuanto a los usuarios finales, que voy a decir de ellos, con lo fácil que es poner una simple contraseña para entrar en Windows y hasta eso lo saltan, pensando "pero si no hace falta para entrar" con pulsar ESCape también entramos, uy, que equivocados estamos y cuantas veces repetimos que hay que entrar con contraseña para activar ciertas medidas de seguridad que no se instalan por defecto.

En cuanto a estos usuarios dentro de las empresas con redes y con este S.O. suelen ser una puerta de entrada a la LAN sin dificultades. Por supuesto, con las ventajas actuales, tarifas, cables, adsl... esto empeora, chicos y a que velocidad.

Por otra parte, es tan simple en ciertos aspectos, con su diseño -no es un S.O. multiusuario- posee herramientas de administración remota muy limitadas.

Las formas en que un intruso puede adueñarse de un win9.x pueden definirse fácilmente, engañar tal usuario ejecutando un código de su elección (troyano) o accediendo físicamente al ordenata.

Las estrategias de ataque son básicamente dos, remotas o locales, ¿hay más?

En principio un w9.x remotamente no es controlable totalmente, a menos claro, que lo deseemos y facilitemos esos accesos. En cuanto a un acceso local (rabillo en usuarios caseros !!!) si es en una empresa, facilitaría la primera estrategia, ya que si consigue acceder físicamente puede ampliar las posibilidades a su alcance.

Una explotación remota pasa por:

- Recursos compartidos
- Troyanos
- Vulnerabilidades conocidas de aplicaciones y/o negación de servicios(DoS)

De hecho, el usuario ha de querer, sí... ha de querer que entren en su equipo para que lo hagan.

Una mínima preocupación y creencia en la seguridad le bastará para evitarse disgustos.

Relajemos un poco, contemos alguna historia... pero no digáis que he sido yo ;-)

Un artista necesita sentir como fluye por su cuerpo la sangre, como le embarga la emoción del viaje que se ha preparado tan minuciosamente. Cualquiera desea ser ese artista, pero no es así ;-)

Los sistemas no son fáciles de penetrar y menos si están bien configurados, los hackers viajan por la oscuridad, seleccionan el objetivo, lo siguen, vigilan, sondean, recopilan información... estudian vulnerabilidades del sistema y poco a poco van preparando la conquista. Traspasan ese muro inicial, aún cuando no tienen vía libre total, no han llegado a su interior.

Uno de los más conocidos, Kevin Mitnick, comprendió perfectamente el paradigma. El defecto de seguridad más frecuente es una mala gestión de los nombres de usuarios/contraseñas. Y son las llaves más usadas en este reino de la información, la mayoría de intrusiones pasan por la obtención de estos datos, de la forma que sea necesaria. De hecho éste genio de la técnica, Mitnick fue, probablemente, muy hábil en los medios no técnicos que utilizaba para obtener información de los usuarios de los sistemas que violó. No sé por que pienso enseguida que se echaría novia en más de una empresa ;-)

Seguimos: Y cuando un objetivo ha sido tocado... si cuando más grande, peor será..

No sé como tendrá MS, últimamente sus DNS etc... pero si logran entrar en tu sistema, algo dejan siempre para vacaciones extras, o una cosa así...

8.2. *Conexión directo a recursos compartidos de win9.x.*

Existen unas variantes de acceso al sistema en forma remota, compartir archivos e impresoras, un servidor de acceso telefónico a redes y la posible manipulación remota del registro.

Manipular el registro es en principio la menos factible, fuera de un entorno LAN es raro ver personalizaciones avanzadas y seguridad a nivel de usuario. Lo que comenté en el artículo anterior y es que el diseño de w9x le limita bastante.

Por lo que apetece más es atacar los recursos compartidos, dejaremos las impresoras, al fin y al cabo para que van a querer imprimir :-))))

El hacker obtendrá una lista de recursos compartidos (seleccionará los objetivos), explorando la red, sabéis que existen herramientas para ello, la mejor ya la mencionamos alguna vez "SMBS", hay otras, pero...

Bueno, explorará la red y definirá si los hay sin contraseña (aún quedará alguno así? pues SÍ!), y atacará mediante fuerza bruta los que tengan contraseña (no es difícil, y si ya tenemos un buen listado de palabrejas y contraseñas, etc... combinaciones en definitiva, pues mejor).

Una vez consiga penetrar, conseguirá datos, éstos pueden ser variados e incluso facilitarles la entrada a otras partes del sistema.

Imaginaos tener compartido todo el C:\, pues al ataquerrrrrrr.

8.3. *Contraataques*

Deberíais saber la respuesta, algo puse en los artículoillos de la fiebre.

Desactivar la compartición de archivos.

Si se han de utilizar, poner contraseñas complejas (alfanuméricos incluyendo metacaracteres, o ASCII no imprimibles) y añadir el signo \$ al final del nombre.

Si hay varios equipos y se hace tedioso, utilizar Poledit.

8.4. *Autenticación hash y los servidores de acceso telefónico en win9.x.*

Win9.x, no es un S.O seguro, eso no hará falta repetirlo más, pero ello no significa que su acceso sea fácil, pues al no estar pensado como un s.o. propiamente de uso profesional y con grandes defectos o necesitado de accesorios se limita el sólo, tampoco hará falta repetirlo.

Como dije, el acceso a un w9.x no es fácil y es fácil a la vez, técnicamente se necesita la ayuda del propio usuario o en su caso tener un acceso físico al puesto de operador.

El usuario puede ayudarnos a facilitar las cosas, ¿cómo? ya dijimos que compartiendo los archivos en w9.x sería la forma en que tendríamos un acceso que a su vez podría facilitarnos una entrada más completa al equipo y ¿por qué no? al resto de la RED si existe.

En sus limitaciones, w9.x, utiliza un desafío para comprobar la unión usuario/contraseña, (hash = mezclar criptográficamente), mientras el usuario circula por la red en un simple modo texto.

Pues una vulnerabilidad es la de emitir en la red durante aproximadamente 15 minutos el mismo desafío, por lo que un escucha en la red podría volver a enviar una petición idéntica a la correcta y activar la compartición de archivos.(el valor de la contraseña hash es idéntico durante los quince minutos). Claro, para escuchar debes estar en la RED, así que a ver como lo aprovechan.

No digo que no, pero creo que el trabajo necesario para ello sería excesivo, si se piensa en aquello que se podría conseguir.(mejor atacar a NT o Unix y datos interesantes, para hacernos con a saber qué...)

La utilidad de Servidor de acceso telefónico a redes, se añadió a microsoft 95 plus y luego ya viene en los win9.x siguientes en el paquete original. Es otra de las posibilidades de entrada a nuestros equipos, aunque como repito, siempre a medias - esas limitaciones- (y eso que pensamos que win9.x es malo ¿qué?).

Un buen Administrador(no será muy bueno si no convence a su empresa de cambiar w9.x por otros clientes) deberá pensar un poco, y con alguna utilidad procurar que los usuarios no puedan instalar estos servidores de acceso telefónico a redes o estará facilitando puertas innecesarias a toda la red.

Al fin y al cabo, el servidor necesita compartir para ser efectivo.... y a compartir = entrada a la disco:-)))

No haremos defensa de esto, mejor evitar su instalación.

8.5. Atacar al registro remotamente

Siendo como es, win9.x no brilla por su capacidad de acceder remotamente al registro, a diferencia de sus hermanos de núcleo NT. Aún así, nos añadieron una maravillosa utilidad en el CD original para tener un servicio de acceso remoto (remotreg).

Si en algún momento pensamos en instalar este servicio, hay que ir pensando una contraseña compleja e ir cambiando, el acceso a un equipo con el servicio remoto activo significa ceder el control al intruso. Pero no preocuparse, no se instala y chin-pun, a dormir medio tranquilo, al menos el registro no lo tocarán.

Y finalmente si instalamos el SNMP (simple network management protocol) en el cd de w9.x, también existe la posibilidad de que un atacante saque información, pero repito es muy limitado.

9. Puertas traseras

Bueno tenemos el win9.x a salvo, no compartimos recursos, ni instalado el servidor de acceso telefónico, ni el servicio remotreg.

Eso de bueno no queda tan claro.

Al principio comenté que la forma de controlar totalmente un w9.x tenía unas variantes, una la más peligrosa y llamativa es la de las puertas traseras, por cierto, les bautizan con el nombre de troyanos, Backdoor, BackOffice, NetBus, etc...

Estas herramientas fueron diseñadas para un control remoto de win9.x.

Sus capacidades han variado asombrosamente, añadir y borrar claves del registro, reiniciar el sistema, copiar/borrar/enviar/recibir archivos, ver contraseñas, crea.....

Se han añadido funcionalidades para trabajar por los canales IRC(algunos muy específicos), pueden informar de las IP a cualquiera mal llamado hacker que frecuente dichos canales.

DIGO mal llamado hacker, por una simple razón, el espíritu hacker nació hace bastante tiempo, su intrusismo ataca grandes compañías (a los Goliats) no daña por dañar (no se me comerá el coco con lo contrario), son artistas y NO SE METEN CON SIMPLES USUARIOS, así que habrá que ir pensando en sacar algún nombre más idóneo para la "MORRALLA" que existe en Internet y que dicen llamarse "Hackers". Todos los troyanos son el sueño de un hacker, pero al nivel que se ha llegado son utilizados abusivamente y con una simple definición "PURA MALDAD".

BO = maldad pura, UDP por el 31337.

Netbus = para hackers con más espíritu. (TCP 12345 o 20034) Los firewall pueden cortar más fácilmente TCP.

Vale, el troyano, y que más....

El objetivo ha de estar en una red (Internet vale) si no... no sirve.

Se ha de forzar la ejecución de código en un sistema y remotamente.

Aprovechar las vulnerabilidades de los clientes de red, hacer uso de engaños, ¿e-mail?.

Código móvil hostil.

Java, ActiveX, Scripts incrustados en HTML, etc... Es el riesgo, pueden ejecutar acciones no deseadas y muy perjudiciales para los usuarios, tienen capacidad para lanzar de forma remota cualquier troyano.

Y podemos contrarrestar esto?

Demos un paso atrás,

Los mecanismos de entrega se basan en el engaño, en las malas configuraciones, en las vulnerabilidades de los clientes (Internet Explorer, Netscape, Outlook Express, Outlook, etc...)

La primera medida pasa por tener actualizado el software y la segunda en vigilar correctamente su configuración.

Aún así, siempre hemos de ser escépticos cuando descargamos cosas de Internet y más cuando hemos de ejecutarlas.

No instalar aplicaciones de servidor en w9.x, por ejemplo PWS Personal Web Server.

Y para acabar, más o menos, NO a herramientas de control remoto, ello significa perder las medidas que adoptemos de seguridad en w9.x y darle la posibilidad a

"otros" de aprovecharse como si estuviesen sentados delante de nuestro ordenador.

10. Black Ice Defender 2.1.45

Categoría: Estrictamente... un firewall por software.

Vigila todos los paquetes del tráfico de la red.(Internet y/o local si la hay)

Una ventana con una barra de menú y un control de páginas (Tab Control TabCTI), con lo que necesita el COMCTL32.DLL versión 4.72 o mayor. Esta versión funciona con w9x, ME y w2k perfectamente. Este control tiene 4 pestañas, que dan acceso a cada página del control, en cada una hay:

Attacks

Intruders

History

Information

En la primera es un log en marcha, es decir, van apareciendo, en el caso de existir, los intentos de penetración en el sistema, la descripción que se nos da es bastante completa.

Un icono, característico de uno de los niveles que el firewall cataloga el intento de penetración, la fecha y la hora, la definición del ataque, el intruso y un contador de veces.

Ejemplo:

Un círculo amarillo con interrogación

(si está cruzado por una línea significa que el firewall ha bloqueado el puerto)

2001-02-03 19:02:45

TCP port probe

162-SEVI-X13.libre.retevision.es

2

Además tiene un botón con AdvICE serigrafiado que nos trasladará a una web con la información existente del intento de penetración o ataque (debe haber uno seleccionado).

En la segunda (se puede llegar a ella con doble click en un ataque determinado), se nos da toda la información (details) posible sobre el intruso, dependerá de su habilidad (del intruso) el que aparezca más o menos información.

Para el ejemplo anterior:

IP: 62.83.64.162

DNS: 162-SEVI-X13.libre.retevision.es

(Ya digo que puede dar mucha más información.)

En la tercera tenemos un historial del tráfico de la red y de los ataques, de forma gráfica y unos pequeños valores que podemos configurar.

En la última tenemos el número de licencia, la finalización del soporte técnico y una ventana que muestra información sobre el producto. (en versiones crakeadas ésta ventana está vacía)

Después tenemos una barra de menús:

File, Tools, Help. (Archivo, Herramientas y Ayuda.)

Una sólo opción en File, "Exit".

En Tools (Herramientas):

- Editar las configuraciones del Blacklce (Edit Blacklce settings)

- Motor de Blacklce (Blacklce Engine)

- Borrar la lista de ataques (primera pestaña) - Clear Attack List -

- Descarga de actualización (Download Update)

- Preferencias (Preferences)

En Help (Ayuda):

- Blacklce topics (archivo de ayuda, estilo windows help compiler)

- Support online (link para soporte en línea)

- www.network.com (link a su web)

- About Blacklce (Acerca de... unos datos de las versiones de los archivos y la licencia)

- Support knowledge base (soporte de una Base de conocimientos, un link.)

10.1. *Settings/configuraciones*

Siete pestañas nos dan acceso a todas las configuraciones de Blacklce.

Proteccion: Seleccionar el nivel de protección que deseemos

Paranoid = Bloquear todo el tráfico no solicitado

Nervous = Bloquear la mayoría del tráfico no solicitado.

Cautious = Bloquear parte del tráfico no solicitado.

Trusting = Permitir todo el tráfico.

Opciones: Permitir compartir archivos en internet

- Permitir NETBIOS en el entorno de red.

Packet Log:

- Activar la grabación del tráfico del sistema en archivos log.

- Configuración de los logs...

Evidence Log:

- Activar la grabación del tráfico sospechoso de ser desde intrusos/atacantes.

- Configuración de los Logs...

Back Trace:

- Configurar las trazas, indirectas e indirectas, lookup de DNS y NetBIOS.

Trusted Addresses:

Aquí pondremos las IP en que confiamos, incluídas las de la RED local, así nos evitamos bloqueos, en equipos de la red, innecesarios. (Sobre todo si utilizamos compartir conexión de internet)

Blocked Addresses:

Aparecen las IP que hemos bloqueado en las opciones ante un ataque.

Aprovechando, cuando recibimos un ataque, tenemos la oportunidad de activar un menú contextual (clic derecho), para confiar, ignorar o bloquear la IP.

ICEcap:

Yo tengo licencia y esto no se activa, así que...

Blackice engine:

Si está detenido podemos activar el firewall y si está activo lo contrario.

Clear attack list:

Borrar los datos que nos aparecen en la pestaña Attacks, dependiendo del tamaño asignado a los logs y cantidad de files, deberíamos regularizar la limpieza de estos datos. (Yo los copio y mando a los ISP, luego los guardo y los borro.)

Download update:

No comment

Preferences:

Configuración de algunas preferencias, si aparecerán las confirmaciones en cuadros de diálogo, activar los chequeos para updates, configurar los iconos y el sonido de los avisos de intrusiones.