

Práctica 44. Control Remoto (Por HxC Mods-Adm)

Realmente con éste título ya sería suficiente para expresar todo lo que voy a contar, pero merece algo de explicación.

En la sección de prácticas se muestra el uso de psexec.exe, pues en esta ocasión vamos a conseguir lo mismo y más pero con CONTROL GRAFICO

Ya conocemos la filosofía de cliente-servidor en las comunicaciones, pero....

¿Qué os parecería algo como el Radmin, pero sin necesidad de subir el programa servidor al objetivo?

Pues de eso se trata, sólo necesitaremos esto:

- La herramienta: ATELIER WEB REMOTE COMMANDER
- Un nombre usuario válido
- La contraseña de dicho usuario

Como en el psexec, pero mejor; porque tendremos control de lo siguiente:

- Escritorio (Desktop)
- Información del sistema (Sysinfo)
- Información de la topología de la red (NetworkInfo)
- Transferencia de ficheros (FileSystem)
- Información de usuarios y grupos (Users and Group) Además esta función permitirá averiguar los hashes de los users remotos y pasarlos al LC3 o LC4 para crackearlos
- Chat, podremos hablar con el objetivo (mensajitos, etc) y él con nosotros si lo deseamos.

Vamos, si lo del psexec lo calificasteis de bomba, peligro, etc. ESTO LE DA 1000 VUELTAS.

Para los que penséis que esto es una lamerada, ya sabéis mi opinión, para mi esto es una herramienta de administración, que puede y es muy útil, dependerá del uso que se le dé, para que pase a estar en un bando o en otro.

Funciona correctamente en entornos windows 2000, 2003 y XP, la filosofía, limitaciones, etc. se irán exponiendo a medida que lo vayáis usando y probando, el que no lo haga se va a perder algo bueno.

Lo único que hay que hacer es instalar el programita en nuestro equipo, para ello lo podéis bajar de éstos sitios:

<http://www.atelierweb.com/rcomm/awrc31.zip>

<ftp://atelierweb.com/rcomm/awrc31.zip>

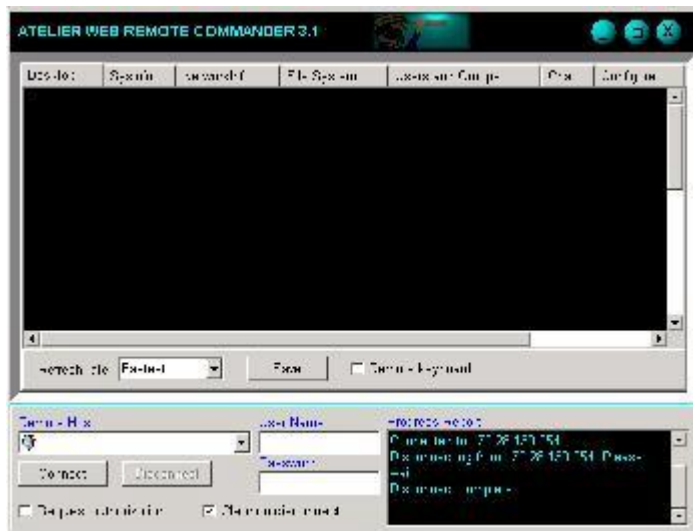
Es una licencia de 15 días, ni os cuento dónde y cómo se puede ampliar esta versión.

La versión de evaluación tiene "algunas" limitaciones, tiempo de conexión, tiempo de uso, opciones, etc.. los que "compréis" la versión completa: Bienvenidos al mundo Remoto de AWRC

Funcionamiento:

Una vez descargado e instalado el AWRC en nuestro equipo, ejecutad el Atelier Web Remote Commander desde el menú de inicio o desde el icono de acceso directo que os creará.

Veréis algo así:



ES MUY IMPORTANTE NO VERIFICAR LA CASILLA Request Authorization, si lo hacéis cuando os conectéis al equipo remoto, le saldrá una ventanita diciendo que la ip tal.y.tal usuario fulano desea establecer la conexión... y eso no es bueno si queremos pasar desapercibidos

Una vez comprobado que esa casilla no está verificada, escribimos la ip remota, el usuario y la contraseña, luego Connect

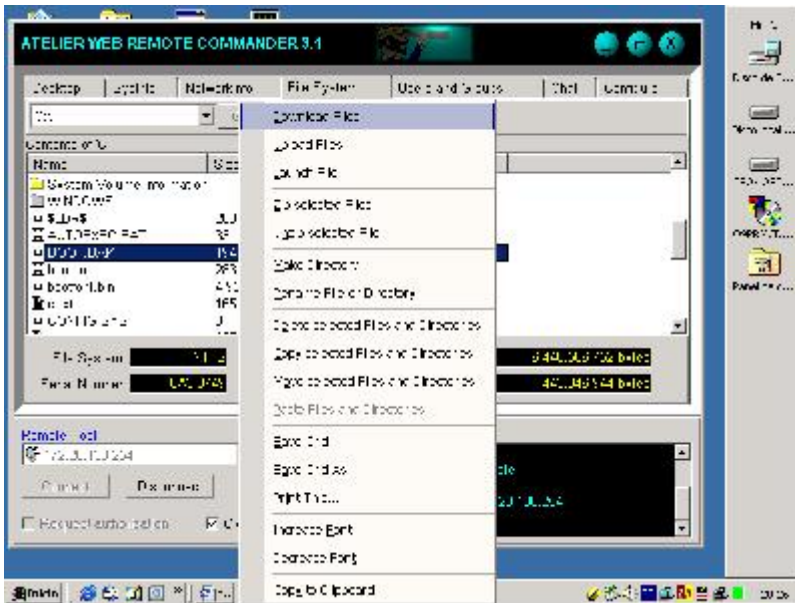
y....



Joder, acabamos de obtener el escritorio remoto del equipo!!!!

Vaaale, el resto os lo dejo a vosotros, podéis cambiar las opciones en Options y también en FileSystem podéis bajar-subir-borrar-crear etc, bastará con que seleccionéis la unidad de disco pulsad en GET y luego sobre el contenido del directorio el botón derecho del ratón...

más o menos algo así:



Por supuesto, se pueden ejecutar programas, servicios, detenerlos, buff. miedo me está dando.

Otras herramientas del mismo tipo son:

Remote Task Manager <http://www.amtsoft.com/remotetask/download.htm>

Omniquad <http://www.voodoofiles.com/getit.asp?id=10325&g=1&d=21&s=694068259>

Control IT <http://www.dbl.co.uk/remoteForm.htm>

Active Network Monitor

http://www.peachseed.com/download.html?dl_title=Active%20Network%20Monitor&dl_url=http://www.protect-me.com/anm.zip

Active Task Manager http://www.orionsoftlab.com/orion_tm.zip