

Práctica 39. Exploits para obtener shell de system

Aunque este exploit es algo viejo todavía puede seguir funcionando en muchos sistemas windows, ya comenté en la parte teórica que es prácticamente imposible mantener un equipo totalmente parcheado, igual de difícil es que un exploit sea operativo de por vida... como muestra de este tipo de ataques, basta un botón:

Bueno, se trata de ganar el acceso como administrador en una máquina W2k a la cual tenemos acceso físico y podemos iniciar sesión LOCAL como usuarios autenticados e interactivos, pongo lo de local en mayúsculas porque si se trata de usuarios del dominio no funcionará.

- 1º) Nos buscamos una herramienta llamada netddemsg.exe
- 2º) Iniciamos la sesión con nuestro usuario y contraseña válidos
- 3º) copiamos el archivo al pc y abrimos una shell
- 4º) Iniciamos el servicio netdde,

net start netdde

- 4º) desde el directorio donde copiamos el archivo netddemsg.exe lo ejecutamos de la siguiente forma:

netddemsg -s chat\$ cmd.exe

Esto abrirá una nueva ventana de comandos con privilegios de SYSTEM

- 5º) desde la nueva ventana de comandos que se abrió, escribimos:

net localgroup administradores usuario /add

Siendo usuario el nombre del usuario con que iniciaste la sesión en w2k o el nombre de usuario que quieras añadir al grupo de administradores.

- 6º) Cerrar todas las ventanas y reiniciar la sesión, no hace falta reiniciar el equipo solo cerrar la sesión y volver a entrar, a partir de ese momento FORMARAS PARTE DEL GRUPO DE ADMINISTRADORES.

Precauciones:

Si el administrador (el verdadero) "es un ser" preocupado por la seguridad se dará cuenta, por ejemplo si tiene habilitada la auditoría de cuentas, etc. así que borra o modifica las huellas que dejes.

Si la cuenta de acceso es como usuario del dominio NO VA

No lo probeis en remoto, SE NECESITA formar parte de INTERACTIVOS