



**Tema destacado:** Guía rápida para descarga de **herramientas gratuitas de seguridad y desinfección**.

- Foro de elhacker.net
- Seguridad Informática
- Hacking Avanzado
- Hacking Básico (Moderadores: zhyzura, toxeeek)
- Como entrar a un PC por NETBIOS

**G+1** 302 0 Usuarios y 1 Visitante están viendo este tema.

Páginas: [1] 2 [ir abajo](#)

[responder](#) [imprimir](#)

**Autor** Tema: **Como entrar a un PC por NETBIOS (Leído 31,115 veces)**

**\_DarkZeus\_** **Como entrar a un PC por NETBIOS**  
« en: 25 Mayo 2007, 13:26 »

Desconectado

Mensajes: 11



Buenas!

Tengo esta guía de hace mucho tiempo y el otro día quise probarla, pero no sé si en el Windows XP no rula o algo porque puse /run nstat y me ponía que no existía esta aplicación, y así con la mayoría de cosas...

Alguien sabe o tiene una guía para poder entrar a un pc con archivos compartidos a través de NETBIOS que funcione actualmente en windows XP?

Saludos y gracias de antemano ^^ Ahora posteo la guía aquí abajo por si es de interés.

**G+1** 0 En línea

**\_DarkZeus\_** **Re: Como entrar a un PC por NETBIOS**  
« **Respuesta #1** en: 25 Mayo 2007, 13:27 »

Desconectado

Mensajes: 11



## CÓMO ENTRAR EN UNA MÁQUINA WINDOWS CON RECURSOS COMPARTIDOS

Este hack no se basa en un fallo del windows ni nada parecido. Algunos usuarios tienen redes de trabajo, se reúnen para jugar a quake, cambiar fotos porno... ese tipo de cosas, y comparten recursos y no ponen passwords. Si encontramos a uno de estos individuos... le podemos joder lo que queramos o la mayoría de las veces, sacar passwords y archivos importantes (o juegos o fotos porno o...). En esta mini-guía se explican los pasos a seguir para hackear una máquina con recursos compartidos en windows.

### 1. Fijar blanco

Necesitamos una IP, si no tenemos un objetivo pensado (como podría ser: el hijoputa de la clase, el profe de mates, el ordenata del director...) puedes entrar en el irc y buscar gente por ahí. Una buena sugerencia es la de elegir a alguien de un canal en el que te gustaría tener op, alguien que te ha jodido y le quieres quitar el nick si lo ha registrado, o simplemente necesitas a alguien para probar y... lo siento chico, te ha tocado a ti xDDD (y eliges uno cualquiera en el canal o si usas mIRC puedes poner:

Para saber la gente que hay en un canal sin entrar en el:  
/names #canal

Para pillar una IP aleatoria del canal en el que estamos:  
//dns \$nick(,\$rand(1,\$nick(,0)))

Si quieres pillar la IP de un nick que ya sabes pones:  
/dns nick (nick es el nick del que quieres averiguar la IP)  
Entonces ocurrirá algo como esto en el status:

```
*** Looking up ctv21225141110.ctv.es
```

```
*** Resolved ctv21225141110.ctv.es to 212.25.141.110
```

Tenemos la IP, que en este caso es 212.25.141.110, podemos pasar al siguiente paso.

## 2. Averiguar el nombre de la máquina objetivo

Para poder entrar primero necesitamos saber cuál es el nombre de la máquina, para ello usaremos el programa nbtstat con el parámetro -A, que sirve para pillar la tabla de nombres de la máquina objetivo a partir de la IP. Este comando se usa así: 'nbtstat -A 123.123.123.123'. Podemos ejecutarlo desde un prompt del DOS, desde Inicio-Ejecutar o desde mIRC con el comando: /run nbtstat -A DirecciónIP

Una sugerencia para mIRC es escribir éstas líneas en los remotes:

```
On 1:Dns: {  
echo $iaddress  
clipboard $iaddress  
run nbtstat -A $iaddress  
}
```

Y cuando hagas un dns te hará el nbtstat automaticamente.

(se nota que soy scripter)

He ejecutado el nbtstat con fliper (víctima):

```
nbtstat -A 212.25.141.110
```

y me ha respondido algo así:

Host not found.

Lo que quiere decir que o no tiene el netbios activo, o no usa windows o no se encuentra nada en esa IP (puede que se haya desconectado, que la hayas escrito mal...), o sea, Paso1 y a buscarse otra víctima.

Repetimos, ya tengo otra víctima y ejecuto el comando 'nbtstat -A IPdelavíctima'

Esta vez ha contestado algo como:

```
NetBIOS Remote Machine Name Table  
Name Type Status
```

```
-----  
SUSO <00> UNIQUE Registered  
SUSOHACKER <00> GROUP Registered  
SUSO <03> UNIQUE Registered  
MAC Address = 44-45-53-54-00-00
```

Ahora sabemos que el nombre de la máquina es SUSO (primera entrada <00>), que el nombre del grupo es SUSOHACKER.

El nombre de la máquina es el primer UNIQUE de la tabla, y los grupos que hay son reconocidos fácilmente por GROUP.

Pero antes de qué empieces a dar saltos de alegría por haber encontrado un objetivo válido, he de decirte que este no nos vale (que malo soy... xDDDDDD). Para que el objetivo valga (o sea que haya posibilidades de entrar en él) tiene que haber por al menos una entrada <20>, y en este caso no la hay.

Repetimos Paso1, hacemos el 'nbtstat -A Ipvíctima' y encontramos un individuo con una entrada <20>:

```
NetBIOS Remote Machine Name Table  
Name Type Status
```

```
-----  
SANTI <00> UNIQUE Registered  
CORBA <00> GROUP Registered  
SANTI <03> UNIQUE Registered  
SANTI <20> UNIQUE Registered  
CORBA <1E> GROUP Registered  
MAC Address = 44-45-53-54-00-00
```

Este individuo tiene una entrada <20> y es la que nos vale, tenemos el nombre de su máquina qué es SANTI, recuerda que es el primer UNIQUE. Podemos pasar al Paso3.

El que os haya puesto víctimas que no valían era para que vierais los resultados más comunes antes de pasar a la acción, y si no te sale a la primera, saldrá a la segunda. También decirte que tienes que tener en la conexión que estés usando en propiedades la casilla de NetBEUI y Conectarse a la red activadas, luego ve al Panel de Control y en Red, comprueba que tienes Compartir impresoras y archivos activados.

## 3. Añadiéndole a nuestra lista de hosts

Abrimos el archivo C:\WINDOWS\lmhosts (no confundir con lmhosts.sam, que es un ejemplo (sam de sample)) y escribimos (con el bloc de notas, no me seas burro) en la ultima línea (qué puede ser la primera si acabamos de crear el archivo xD, quiero decir que podemos tener varios ordenatas metidos en la lista):

```
'123.123.123.123 NOMBRE'
```

Ésta es una parte de mi lmhosts para que os hagais una idea:

```
212.25.137.75 LINUX  
152.71.32.128 BLEIS239  
147.156.122.7 BLANC  
194.224.88.221 JOSU  
147.83.4.168 ANT
```

Y lo guardais. Ahora lo más importante, que en todos los textos que había leído sobre esto antes de conseguir hacerlo no lo nombraban (lo que me hace suponer que se habrían limitado a copiárselo de otro y no lo habían hecho nunca)

Decirle al NetBIOS que actualice la lista, que añada el nuevo host. Esto es así:

'nbtstat -R'

y responderá:

Successful purge and preload of the NBT Remote Cache Name Table.

Lo ejecutais donde querais. En Inicio, mIRC, DOS...

Añadido a la lista y pasamos al Paso4.

4. Qué comparte y como entrar

Usamos el comando net view para ver lo que comparte:

'net view \\ANT'

Saldrá algo así:

Recursos compartidos \\ZEUS

Compartido Tipo Comentario

-----

CDROM Disco

C Disco

PRINTER1 Impresora

El comando ha sido ejecutado con éxito.

También podemos hacer Inicio-Buscar-PC... \\ZEUS

Luego desde DOS podemos hacer DIR \\ZEUS para ver los archivos, o en ejecutar \\ZEUS y se abrirá una ventana con lo que tiene compartido. Ahora le podemos copiar archivos, leer archivos y tal como si estuvieran en nuestro ordenata (irá muuuy lento, no os desespereis).

5. Estamos dentro, qué hacer?

Archivos para pillar:

- System.ini: no es otra cosa sino que el archivo de configuración de Windows. No ocupa demasiado así que es de lo primero que debemos coger. Si lo abrimos con el bloc de notas y vamos a la sección [Password Lists] nos dirá los logins y las listas de passwords para los usuarios del ordenata. Nos aportará mucha información importante.

- \*.PWL: son los archivos de PassWord List, arriba se indica como cogerlos nos darán algunos password de los usuarios.

- Otros ficheros de passwd: Si vemos algún programa como el cuteFTP podemos cogerle los archivos de passwords que se guardan en el disco duro. Ej: users.dat

- Logs: si algún usuario conecta al irc, que si hemos pillado su IP en el IRC será porque conecta, puede que esté guardando logs. Busca logs con el nombre de bots como: NiCK.log, CHaN.log, etc. Si es admin de un canal o está registrado, o queremos pillarle el nick estos son los archivos que nos ayudarán.

- Malos usos: También podemos robar fotos porno, leer ficheros confidenciales, pringar mp3... Pero seguro que todo lo anterior tampoco era bueno XDD

Si por suerte tenemos acceso total:

Si por alguna casualidad de la vida tenemos acceso total:

- Troyanos: le podemos meter troyanos, simplemente lo subimos y se lo añadimos al autoexec.bat por ejemplo, la próxima vez que reinicié se le instalará. Tiene el inconveniente de que si le queremos meter el NetBUS o el BO o lo que sea no se le instalará en el momento. AH!!!! Ni se os ocurra intentar instalarselo desde vuestro ordenador, a lo mejor os pensais que haciendo 2click en el icono se le instalará, y lo que estarás haciendo es traerlo a vuestro ordenador y ejecutandolos en el vuestro.

- Viruses: como antes los troyanos le puedes meter cualquier virus que se te ocurra, también puedes reemplazarle algún fichero que vaya a usar por el virus para joder más, como renombrarlo a command.com. Si entiendes un poquito más le puedes coger algún programa y en ensamblador meterle algunas instrucciones más. O con el resource workshop cambiarle el icono, las propiedades del fichero... y hacerle creer que se trata de otro programa! XD


- Todos contra la pornografía infantil: si te encuentras con un directorio lleno de fotos chungas desas, puedes bajartelas (si eres un pederasta, pedófilo, infanticida...) o puedes borrarlas todas...

- Ser cabrón: borra todo lo que se te ocurra o te de tiempo, modifica los programas con un HexEditor y con cortar un cachito ya quedará inservible el fichero. Este uso es un pelín... cracker-lamer y siempre que hagas cosas de estas procura no dejarte nada dentro.

- Firmar: si no has hecho nada malo puedes dejarle un txt en el escritorio con tu nick, fecha, hora y si eres bueno y honrado "hasta" puedes decirle que ponga passwords o no comparta nada.

- Deja volar la imaginación: todo tipo de programas y acciones dependiendo de cuál sea tu objetivo.

Esto se ha acabado y creo que con eso estarás entretenido unas horitas... A ver si os animais y escribís sobre cosas que sepais que siempre le será útil a alguien por muy malo que seas. Podeis encontrarme por el irc-hispano con el nick de DarkAngel en los canales #100scripts y #hack, pero mejor me pones en la notify porque es muy probable que esté por ahí trapichando.


 En línea

NewLog



**Re: Como entrar a un PC por NETBIOS**

« Respuesta #2 en: 25 Mayo 2007, 15:48 »

 Desconectado

Con XP ya no se puede usar esta técnica.

**WHK**

吴阿卡

Moderador Global

**Re: Como entrar a un PC por NETBIOS**

« Respuesta #3 en: 25 Mayo 2007, 18:32 »

Desconectado

Mensajes: 5.650

The Hacktivism  
is not a crime

Ese manual es del año en que se creó la calculadora

Me recuerda cuando recién entré al foro posteando manuales antiquísimos hasta el ejemplo es el mismo que aparecen en todas las páginas webs sobre "como entrar en una pc con recursos compartidos" Aunque no está de más saber algo de comandos :p

De todas maneras si quieres entrar con recursos compartidos a una pc en Windows XP o Vista puedes hacer lo siguiente:

Si la otra pc comparte una carpeta pero tu no puedes ver la red, entonces haz ping escaneando rangos como por ejemplo:

```
ping -n 1 192.168.1.1
ping -n 1 192.168.1.2
ping -n 1 192.168.1.3
```

etc tc etc o hacerlo automáticamente con netscan:

Haz click para ver la imagen

Luego solo le haces doble click a la carpeta donde quieres entrar y ya estás dentro   
<http://www.softperfect.com/download/netscan.exe>

Puedes guardar este programa en un pendrive, en tu correo, en un ftp, etc etc...

Si no puedes, entonces cuando encuentres la ip de la pc que tiene las carpetas compartidas ejecuta:

```
net computer \\ip /add
```

Y de esta forma te aparecerán las carpetas compartidas... otra forma es escribiendo en tu explorador:

```
\\ip
```

Y te aparecerán las carpetas de igual forma.

Si por algún motivo no sabes en que rango comienza la ip de tu red entonces ejecuta **ipconfig** y si tu ip es por ejemplo: **155.25.3.1** entonces los demás son **155.25.3.x** fácil no? (por lo general los servidores terminan en 1 o 2).

Otro tip:

```
FOR /L %i IN (1,1,254) DO ping 80.36.230.%i >>escaner.txt
```

Con este comando realizas un escaner de ip sobre un rango.

Si necesitas saber más puedes leer la revista de hackxcrack donde hay muchos ejemplos para escanear una ip a través del DOS (COMO\_Escaneando\_desde\_MS DOS.pdf).

<http://foro.elhacker.net/index.php/topic,150448.0.html>

[Mi Empresa de seguridad informática oznet.cl](http://miempresa.com) - <http://whk.elhacker.net> - [WHK Conversor](http://whk.com) -

**nica**

Desconectado

Mensajes: 46

**Re: Como entrar a un PC por NETBIOS**

« Respuesta #4 en: 26 Mayo 2007, 00:05 »


tampoco es tan así, por lo general si la cuenta del admin tiene pwd no podrás entrar a las carpetas que tienen el símbolo "\$" (excepto utilizar el IPC\$), o al menos que tengas una cuenta de usuario y pwd válido para la pc. lo que puedes hacer en otro caso sería subirle algún programa que deje un puerto a la escucha y troyanizado con un nombre e ícono interesante para que se autoinstale cuando el usr lo ejecute y después ya verás que más puedes hacer.....


por cierto se me olvidó esta mejor el "essentials net tools" ta más completo

« Última modificación: 26 Mayo 2007, 00:12

**\_DarkZeus\_** Desconectado

Mensajes: 11

**Re: Como entrar a un PC por NETBIOS**« **Respuesta #5** en: 26 Mayo 2007, 01:32 »[Cita de: WHK en 25 Mayo 2007, 18:32](#)Ese manual es del año en que se creó la calculadora 

Me recuerda cuando recién entré al foro posteando manuales antiquísimos  hasta el ejemplo es el mismo que aparecen en todas las paginas webs sobre "como entrar en una pc con recursos compartidos" Aunque no está de mas saber algo de comandos :p


De todas maneras si quieres entrar con recursos compartidos a una pc en Windows XP o Vista puedes hacer lo siguiente:

Si la otra pc comparte una carpeta pero tu no puedes ver la red, entonces haz ping escaneando rangos como por ejemplo:

**ping -n 1 192.168.1.1****ping -n 1 192.168.1.2****ping -n 1 192.168.1.3**

etc tc etc o hacerlo automaticamente con netscan:

Haz click para ver la imagen

Luego solo le haces doble click a la carpeta donde quieres entrar y ya estas dentro 

<http://www.softperfect.com/download/netscan.exe>


Puedes guardar este programa en un pendrive, en tu correo, en un ftp, etc etc...


Si no puedes, entonces cuando encuentres la ip de la pc que tiene las carpetas compartidas ejecuta:

**net computer \\ip /add**

Y de esta forma te aparecerán las carpetas compartidas... otra forma es escribiendo en tu explorador:

**\\ip**

Y te aparecerán las carpetas de igual forma. 

Si por algún motivo no sabes en que rango comienza la ip de tu red entonces ejecuta **ipconfig** y si tu ip es por ejemplo: **155.25.3.1** entonces los demas son **155.25.3.x** facil no?  (por lo general los servidores terminan en 1 o 2).

Otro tip:

**FOR /L %i IN (1,1,254) DO ping 80.36.230.%i >>escaner.txt**

Con este comando realizas un escaner de ip sobre un rango.

Si necesitas saber mas puedes leer la revista de hackxcrack donde hay muchos ejemplos para escanear una ip atraves del DOS (COMO\_Escaneando\_desde\_MS DOS.pdf).

<http://foro.elhacker.net/index.php/topic,150448.0.html>

Merci ^^

He probado con el netscan y me sale todo lo que a ti menos el simbolo "+" al lado del ordenador y no puedo entrar entonces... :S

Y he probado con el essential net tools pero nose como seguir apartir de aquí xD

Haz click para ver la imagen

A ver si alguien que entienda me podría explicar detallado que se hace apartir de aquí o decirme donde bajar el programa que sirva para ver las guias esas que han puesto arriba si esk allí lo explican xD Salu2

**WHK**

吴阿卡

Moderador Global

**Re: Como entrar a un PC por NETBIOS**« **Respuesta #6** en: 26 Mayo 2007, 06:02 » Desconectado

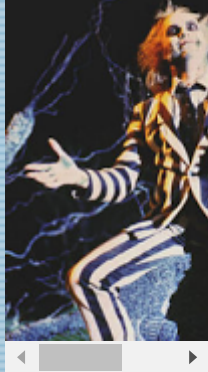
Mensajes: 5.650

Aver.... recursos compartidos atraves de netbios es solamente valido para redes LAN dentro de un mismo rango de IPs.

85.58.28.x no es una ip interna.

Si quieres ingresar a esa pc con netbios entonces necesitarás otras tecnicas como ARP Spoofing y esas cosas para poder registrar tu pc como parte de un dominio interno.





The Hacktivism  
is not a crime



Si quieres entrar entonces te recomiendo hacerlo de la manera mas clasica:


- **Tomar una shell.**
- **Tomar Control atraves de otro sistema como ftp o http shell.**


Hay mucho sobre eso en el foro desde exploits remotos hasta backdoors, etc etc etc...

Es como si quisieras entrar en las carpetas compartidas de un servidor web desde internet :p

En ese manual que expusiste primero se ve como obtener una ip, despues como ver si tiene alguna carpeta compartida con **nbtstat -A** y luego entrar con el tipico "\\\" o ingresandolo a la lista de PCs compartidos. pero de toodas formas puedes entrar sin hacer toda esa rola.

Resumen: "**Como entrar a un PC por NETBIOS**" funciona solamente dentro de una misma red.

 En línea


[Mi Empresa de seguridad informática oznet.cl](http://whk.elhacker.net) - <http://whk.elhacker.net> - [WHK Conversor](#) - 

**\_DarkZeus\_**

 Desconectado

Mensajes: 11



 **Re: Como entrar a un PC por NETBIOS**

« **Respuesta #7** en: 26 Mayo 2007, 10:03 »

[Cita de: WHK en 26 Mayo 2007, 06:02](#)

Aver... recursos compartidos atraves de netbios es solamente valido para redes LAN dentro de un mismo rango de IPs.

85.58.28.x no es una ip interna.

Si quieres ingresar a esa pc con netbios entonces necesitarás otras tecnicas como ARP Spoofing y esas cosas para poder registrar tu pc como parte de un dominio interno.

Si quieres entrar entonces te recomiendo hacerlo de la manera mas clasica:

- **Tomar una shell.**
- **Tomar Control atraves de otro sistema como ftp o http shell.**

Hay mucho sobre eso en el foro desde exploits remotos hasta backdoors, etc etc etc...

Es como si quisieras entrar en las carpetas compartidas de un servidor web desde internet :p


En ese manual que expusiste primero se ve como obtener una ip, despues como ver si tiene alguna carpeta compartida con **nbtstat -A** y luego entrar con el tipico "\\\" o ingresandolo a la lista de PCs compartidos. pero de toodas formas puedes entrar sin hacer toda esa rola.

Resumen: "**Como entrar a un PC por NETBIOS**" funciona solamente dentro de una misma red.


Merci xD Y entonces como se cuala es una ip interna?

Y las 2 últimas dudas, se puede ocultar ip de alguna manera mientras scaneas? y otra cosa, estuve haciendo **netstat -n** para comprobar la IP mientras recibes algo por msn pero veo que en XP no funciona, no te sale la ip del otro xD Hay alguna otra manera de ver la ip k no sea la de hotmail k ya la se?

Salu2

 En línea

**zhynar\_X**

 Desconectado

Mensajes: 514



Use linux my  
friend...

 **Re: Como entrar a un PC por NETBIOS**

« **Respuesta #8** en: 26 Mayo 2007, 11:19 »

Hola


[Cita de: \\_DarkZeus\\_ en 26 Mayo 2007, 10:03](#)

Y las 2 últimas dudas, se puede ocultar ip de alguna manera mientras scaneas? y otra cosa, estuve haciendo **netstat -n** para comprobar la IP mientras recibes algo por msn pero veo que en XP no funciona, no te sale la ip del otro xD Hay alguna otra manera de ver la ip k no sea la de hotmail k ya la se?

Salu2

Ami con **netstat -a** me sigue funcionando y tengo windows XP



 En línea

Me he creado un blog:


<http://zhynar.blogspot.com> Aver si os gusta! 

**\_DarkZeus\_**



**Re: Como entrar a un PC por NETBIOS**

« **Respuesta #9** en: 26 Mayo 2007, 20:17 »

 Desconectado

Mensajes: 11



[Cita de: zhynar X en 26 Mayo 2007, 11:19](#)

Hola


[Cita de: DarkZeus en 26 Mayo 2007, 10:03](#)

Y las 2 últimas dudas, se puede ocultar ip de alguna manera mientras scaneas? y otra cosa, estuve haciendo **netstat -n** para comprobar la IP mientras recibes algo por msn pero veo que en XP no funciona, no te sale la ip del otro xD Hay alguna otra manera de ver la ip k no sea la de hotmail k ya la se?

Salu2

Ami con **netstat -a** me sigue funcionando y tengo windows XP

pues a mi no me sale ni en cmd ni en command, ni netstat -a, ni netstat -n... :S

 En línea

**Páginas:** [1] 2 [ir arriba](#)

 **responder**

 **imprimir**

Ir a:

<a href="#">DriverLandia</a>	<a href="#">MundoDivx</a>	<a href="#">Hisbyte</a>	<a href="#">Truzone</a>
<a href="#">Yashira.org</a>	<a href="#">indetectables.net</a>	<a href="#">Seguridad Colombia</a>	<a href="#">Seguridad Informática</a>
<a href="#">Internet móvil</a>	<a href="#">ADSL</a>	<a href="#">eNYe Sec</a>	<a href="#">Seguridad Wireless</a>
<a href="#">Underground México</a>	<a href="#">El Lado del Mal</a>	<a href="#">Blog Uxio</a>	<a href="#">thehackerway</a>
<a href="#">Tienda Wifi</a>	<a href="#">underc0de</a>		

Todas las webs afiliadas están libres de publicidad engañosa.

Aviso Legal - Powered by SMF 1.1.21 | SMF © 2006-2008, Simple Machines