

# Capítulo 4 - Enumeración

La enumeración es una subfase del escaneo y consiste en recabar mayor información acerca de la víctima u objetivo, esto usualmente se hace aprovechando una debilidad en uno o más de los protocolos o servicios activos detectados previamente.

Por citar un ejemplo, una enumeración de un sistema *Windows* podría recuperar datos como nombres de cuentas de usuarios, grupos, recursos compartidos, hashes de claves, etc.

Hay muchos protocolos susceptibles de enumeración, esto debido a fallas de programación del fabricante del software o bien, debido a configuraciones por defecto o débiles de parte de los administradores de sistemas.

He aquí algunos de los protocolos más populares para enumerar:

- NetBIOS
- DNS
- LDAP
- SNMP

## Protocolos NetBIOS y CIFS/SMB

### NetBIOS

NetBIOS es un protocolo que data de los años 80's, desarrollado por la empresa *Sytek Inc.* y que fue inicialmente utilizado para proveer servicios a la capa de sesión del *modelo OSI*, con el objetivo de permitir que aplicaciones residentes en diferentes computadores se puedan comunicar a través de la red<sup>30</sup>.

*Microsoft* implementó su versión de NetBIOS por primera vez en 1985 para incluirlo con su sistema operativo *Windows 1.0*, e inicialmente la comunicación en red se realizaba a través del protocolo NBF (NetBIOS Frames Protocol). Posteriormente surgió un método para transportar NetBIOS *sobre* TCP/IP, lo cual perdura hasta nuestros días.

Cuando una computadora usa este protocolo se le asigna un nombre NetBIOS en la red, que no necesariamente es igual al nombre DNS del host. Los servicios como el entorno de red y la compartición de archivos e impresoras en una red *Windows* usan normalmente NetBIOS sobre TCP/IP (ver Tabla2).

### ¿Pero cuál es el tema con *NetBIOS*?

Bueno, en el pasado este ha sido un protocolo susceptible de enumeración o explotación, principalmente por debilidades en la programación del código de diferentes versiones implementadas del mismo y también debido a configuraciones por defecto inseguras que son a menudo descuidadas por los administradores (ver Figura 64).

Lo anterior hace que valga la pena probar la enumeración NetBIOS para tratar de obtener mayor información a través de sus servicios activos.

### Servicios y puertos NetBIOS

Tabla 2 - Servicios y puertos NetBIOS

Nombre del servicio	Puerto
Servicio de nombres	137 TCP/UDP
Distribución de datagramas (detección de errores y recuperación)	138 UDP
Servicio de sesión	139 TCP
Compartición de archivos e impresoras del protocolo SMB (*)	445 TCP

**Nota (\*):** En versiones previas de *Windows* el protocolo SMB (Service Message Block) requería transportarse sobre NetBT (NetBIOS sobre TCP/IP), pero en la actualidad puede hacerlo directamente sobre TCP/IP.

**NetBIOS Information Discovery**  
Discover host information through NetBIOS  
[MODULE DETAILS](#)

**NetBIOS Information Discovery Prober**  
Discover host information using sequential NetBIOS Probes  
[MODULE DETAILS](#)

**WPAD.dat File Server**  
This module generates a valid wpad.dat file for WPAD mitm attacks. Usually this module is used in combination with DNS attacks or the 'NetBIOS Name Service Spoofer' module. Please remember as the server will be running by default on TCP port 80 you will need the required privileges to open that port.  
[MODULE DETAILS](#)

**LLMNR Spoofer**  
LLMNR (Link-local Multicast Name Resolution) is the successor of NetBIOS (Windows Vista and up) and is used to resolve the names of neighboring computers. This module forges LLMNR responses by listening for LLMNR requests sent to the LLMNR multicast address (224.0.0.252) and responding with a user-defined spoofed IP address.  
[MODULE DETAILS](#) | <http://www.ietf.org/rfc/rfc47...> [Exploit](#)

**NetBIOS Name Service Spoofer**  
This module forges NetBIOS Name Service (NBNS) responses. It will listen for NBNS requests sent to the local subnet's broadcast address and spoof a response, redirecting the querying machine to an IP of the attacker's choosing. Combined with `auxiliary/capture/server/smb` or `capture/server/http_ntlm` it is a highly effective means of collecting crackable hashes on common networks. This module must be run as root and will bind to tcp/137 on all interfaces.  
[MODULE DETAILS](#) | <http://www.packetstan.com/201...> [Exploit](#)

Figura 64 - Vulnerabilidades recientes de NetBIOS. Fuente: Exploit Database - Metasploit

## ¿Qué son las sesiones nulas?

Una sesión se establece usualmente con el fin de hacer uso de recursos compartidos tales como archivos e impresoras. Al establecer una sesión hacia un **host B** lo usual es que se soliciten credenciales para autenticarse y verificar la identidad de quien desea establecer la conexión.

El mecanismo de autenticación más común consiste en suministrar un nombre de usuario y la clave respectiva, aunque por supuesto podrían agregarse segundos factores de autenticación como smartcards, tokens usb, reconocimiento biométrico entre otros.

El protocolo SMB/CIFS (de sus siglas en inglés Server Message Block / Common Internet Filesystem) es usado en los sistemas *Windows* y en algunos *Unix/Linux* que implementan el aplicativo *SAMBA*, primordialmente para compartir archivos e impresoras y autenticación entre procesos.

Lo que hace “interesante” al protocolo SMB es su capacidad para establecer sesiones entre hosts sin tener que suministrar credenciales, es decir a través de sesiones nulas (sin usuario ni clave).

La razón inicial por la que se permitió el establecimiento de sesiones nulas fue la necesidad de establecer relaciones de confianza entre dominios en las primeras versiones de *Windows*. La idea detrás de esto consistía en permitir:

- Que la cuenta SYSTEM se autentique y enumere recursos del sistema.
- Que los dominios de confianza enumeren recursos.
- Que equipos no pertenecientes al dominio puedan autenticarse y enumerar usuarios.

Tomemos en cuenta que este protocolo data de inicios de los años 80's, época en la cual la

seguridad informática no se trataba con la severidad del caso como ocurre en la actualidad. Sin embargo, es lamentable que a pesar de que los riesgos presentados por la enumeración SMB a través del uso de sesiones nulas fuera un hecho bien conocido por los fabricantes de software, no se corrigiera el problema de inmediato.

Tomemos por ejemplo a *Windows*, las sesiones nulas estaban habilitadas por defecto en *NT* y en *2000*, permitiendo a una persona cualquiera con acceso a la red el listar usuarios, grupos, recursos compartidos, etc.; y todo esto sin suministrar credenciales.

Posteriormente en *XP* y *2003* se continuó permitiendo por defecto el establecimiento de sesiones nulas, pero se limitó la enumeración a las carpetas compartidas, salvaguardando información de usuarios y grupos.

Es recién a partir de *Windows Vista* y *2008* que se “endurecen” las configuraciones por defecto y es poco lo que se puede recuperar en estas versiones y sus superiores con una sesión nula.

Para mitigar la vulnerabilidad de las sesiones nulas, *Microsoft* provee una característica que se puede manejar a través de una clave de registro llamada *RestrictAnonymous*. Dicha clave se puede configurar a través del editor del registro en la ruta *HKLM\SYSTEM\CurrentControlSet\Control\Lsa*. La Tabla 3 presenta los valores posibles para esta clave.

Tabla 3 - Valores posibles para la clave *RestrictAnonymous*<sup>31</sup>

Valor	Nivel de seguridad
0	Ninguno (se basa en los permisos predeterminados)
1	Restricción de usuarios anónimos (no permite enumeración de cuentas o nombres SAM <sup>xxxi</sup> , políticas de cuentas e información del sistema )
2	No permite acceso sin permisos anónimos explícitos

Adicionalmente la clave *RestrictAnonymousSAM* permite mitigar las enumeraciones de la SAM solamente. Por ejemplo en *Windows 7*, *RestrictAnonymous* viene por defecto con el valor “0” y *RestrictAnonymousSAM* en “1”; esto quiere decir que se pueden enumerar recursos compartidos, pero no cuentas de usuarios o grupos a través de la red (ver Figura 65).

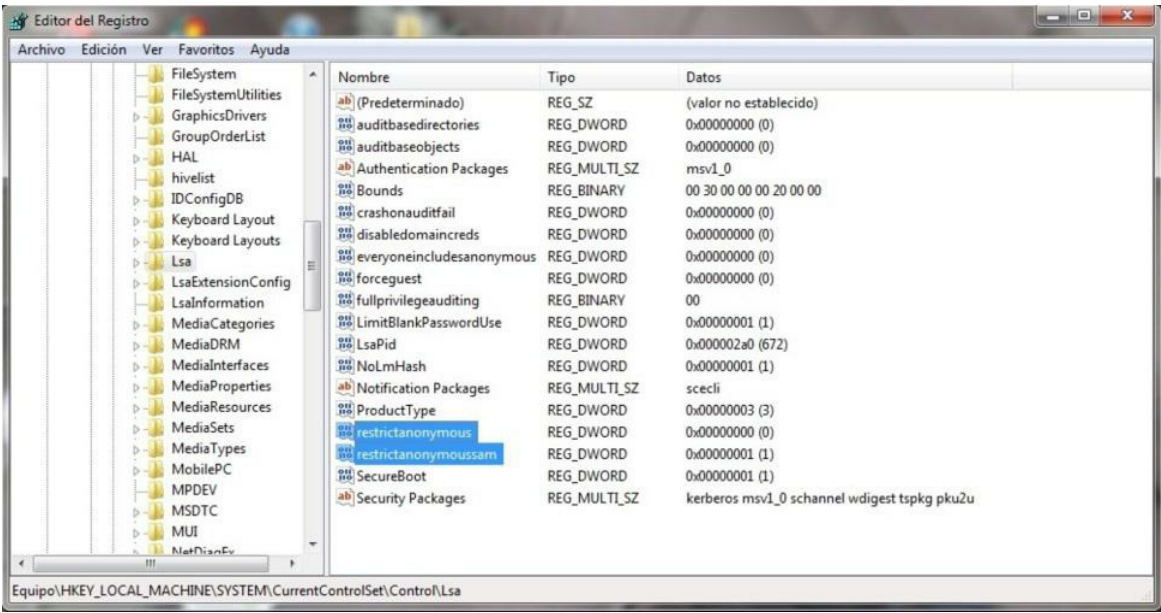


Figura 65 - *RestrictAnonymous* y *RestrictAnonymousSAM* en *Windows 7*

El establecimiento de la sesión nula es sumamente sencillo y sólo requiere que conozcamos la IP o el nombre del host al que nos queremos conectar. Para ello abrimos una línea de comandos (cmd) y escribimos:

```
net use \nombrehost_o_IP\IPC$ "" /u:""
```

Nótese que para establecer la sesión nula hacemos uso del recurso compartido IPC\$ (Inter-process Communications), el cual siempre está activo por defecto en un sistema *Windows* para facilitar la comunicación y compartición de datos entre aplicaciones.

A partir del establecimiento de la sesión nula podremos usar diferentes comandos y herramientas que nos facilitarán la enumeración del sistema víctima.

## Enumeración de Windows con comandos y herramientas de software

*Windows* incluye algunos comandos que permiten realizar enumeración, por ejemplo el comando `net` permite ver, actualizar o realizar cambios de configuración de red. La sintaxis del mismo es similar en las distintas versiones de *Windows*.

Revisemos brevemente la sintaxis de este comando para un sistema *XP*:

```
net [ accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view ]32
```

En este laboratorio nos interesa la opción `view`:

```
net view [\\NombreDeEquipo] [/domain[:NombreDeDominio]]
```

Esto nos permitirá listar dominios, grupos de trabajo, computadoras o recursos compartidos en un equipo dado. Si no se indica ningún parámetro veremos un listado de los equipos de nuestro dominio o grupo de trabajo.

Para efectos de demostración en esta sección usaremos dos máquinas virtuales, una con *Windows XP* (el hacker) y otra con *Windows 2003 Server SP1* (la víctima).

**Nota:** En este ejemplo usaremos *Windows 2003* y no una versión superior, precisamente porque queremos demostrar lo que una configuración por defecto en una versión vieja sin parches actualizados puede acarrear. Más adelante - en el capítulo de Hacking - usaremos otros sistemas operativos víctimas como *Windows 2008 Server*, *Windows 7* y *Linux*.

La Figura 66 nos muestra el resultado de ejecutar el comando `net view /domain` desde *XP*:



```

C:\Documents and Settings\Karina>net view /domain
Dominio
-----
DEMO
INTRO-HACKING
Se ha completado el comando correctamente.

C:\Documents and Settings\Karina>net view /domain:DEMO
Servidor          Descripción
-----
\\SUR1
Se ha completado el comando correctamente.

C:\Documents and Settings\Karina>

```

Figura 66 - Enumerando con net view

Dado que INTRO-HACKING es el grupo de trabajo de la estación *XP*, nuestro interés se centrará en DEMO. En base a esto, procedemos a enumerar con mayor detalle tal y como se muestra en la Figura previa, logrando identificar un equipo llamado SVR1.

Nuestro siguiente paso será establecer una sesión nula hacia dicho equipo y determinar la dirección IP del mismo. La Figura 67 muestra el establecimiento exitoso de la sesión nula con el comando net use.

```

C:\Documents and Settings\Karina>net use \\SUR1 "" /u:""
Se ha completado el comando correctamente.

C:\Documents and Settings\Karina>net use
Se registrarán las nuevas conexiones.

Estado      Local      Remoto      Red
-----
Conectado    \\SUR1\IPC$  Red de Microsoft Windows
Se ha completado el comando correctamente.

C:\Documents and Settings\Karina>ping SUR1
Haciendo ping a SUR1 [192.168.91.133] con 32 bytes de datos:
Respuesta desde 192.168.91.133: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.91.133: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.91.133: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.91.133: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.91.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Karina>_

```

Figura 67 - Estableciendo una sesión nula

Ahora obtendremos información adicional del protocolo NetBIOS haciendo uso del comando nbtstat incluido con *Windows*, como se demuestra en la Figura 68.

La ejecución de este comando nos muestra los nombres de los servicios NetBIOS registrados en el equipo indicado, pero en un formato hexadecimal (ver Tabla 4). De acuerdo a *Microsoft* se usan códigos hexadecimales debido a que dichos nombres pueden ser muy largos y

no entrar en la pantalla. Esto último nos obliga a recurrir a una tabla provista por *Microsoft* para interpretar los códigos de los servicios<sup>33</sup>.

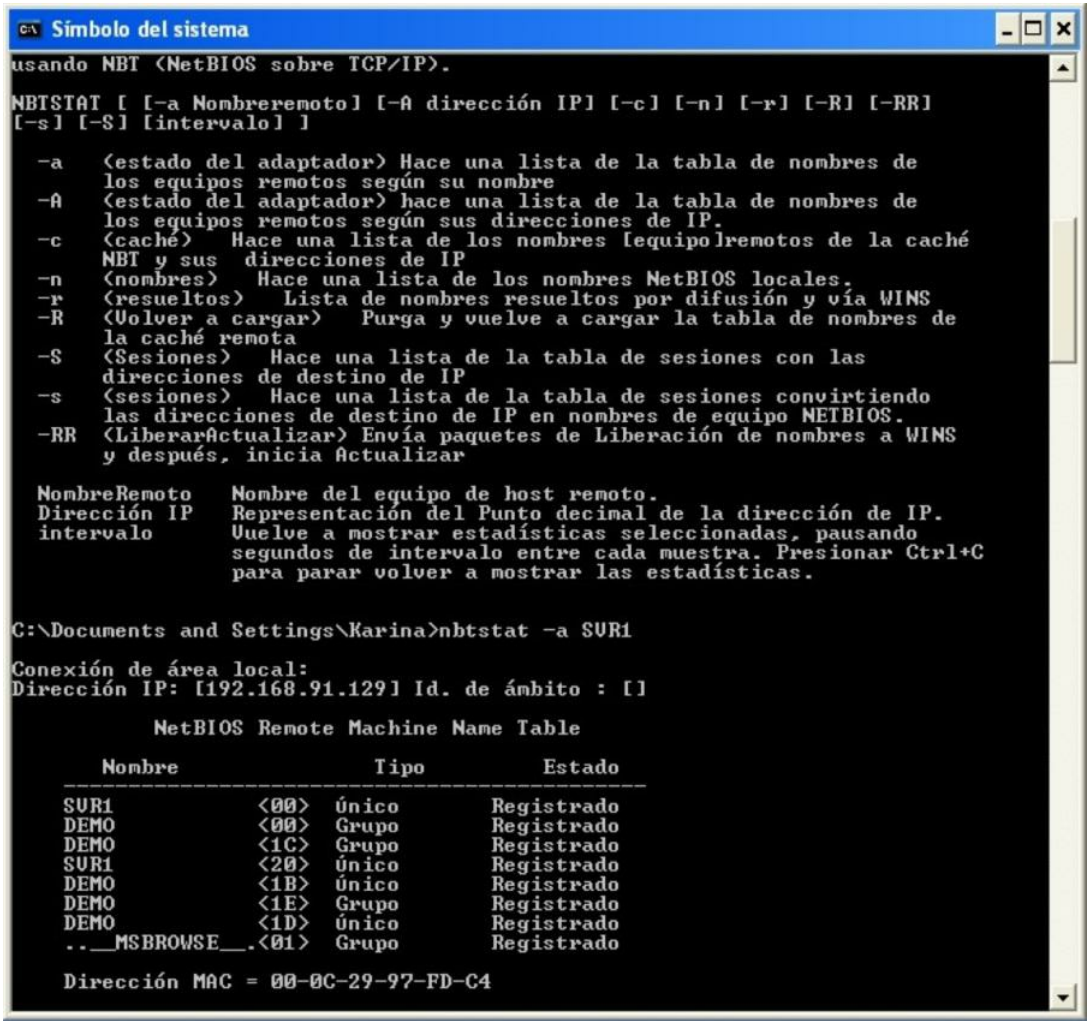


Figura 68 - Sufijos de NetBIOS obtenidos con nbtstat

Tabla 4 - Extracto tabla sufijos NetBIOS

Nombre	Valor	Tipo	Descripción
<computername>	00	U	Servicio de estación de trabajo
<computername>	01	U	Servicio Messenger
<\\--_MSBROWSE_>	01	G	Examinador principal
<computername>	03	U	Servicio Messenger
<computername>	06	U	Servicio Servidor RAS
<computername>	1F	U	Servicio NetDDE
<computername>	20	U	Servicio Servidor de archivos
<computername>	21	U	Servicio Cliente RAS
<domain>	00	G	Nombre de dominio
<domain>	1B	U	Examinador principal de dominio
<domain>	1C	G	Controladores de dominio

Comparando con los valores obtenidos por nbtstat encontramos información útil, como por

ejemplo que **DEMO** es un nombre de dominio (sufijo 00/G) y no un grupo de trabajo, y que **SVR1** es un controlador de dominio (sufijo 1C/G).

Pero tener que revisar valores hexadecimales en una tabla no es mi idea de diversión por eso prefiero usar la herramienta `nbtscan` en lugar de la nativa `nbtstat`. `Nbtscan` fue desarrollado y es mantenido por *Steve Friedl* en su sitio web personal *Unixwiz*, aquí se pueden descargar esta y otras aplicaciones muy útiles de forma libre<sup>34</sup>.

Realicemos la misma operación, esta vez usando `nbtscan`. Vemos claramente en la Figura 69 que el resultado es el mismo, pero esta vez obtenemos un nombre descriptivo del sufijo NetBIOS, lo que nos ahorra tiempo.

Ya que hemos determinado que nuestra víctima es un servidor de dominio *Windows* durante nuestra enumeración, podríamos ayudarnos de un escáner como *NMAP* para tratar de determinar la versión exacta del sistema operativo.

Como se puede ver en la figura Figura 70, *NMAP* reporta que el sistema escaneado puede ser *Windows XP SP2* o *Windows 2003 Server SP1 o SP2*. Dado que sabemos que el equipo es un controlador de dominio, descartamos *Windows XP* y ahora estamos bastante seguros que se trata de *Windows 2003 Server*.

Ahora gracias a nuestro conocimiento sobre las configuraciones por defecto de las variables `RestrictAnonymous` y `RestrictAnonymousSAM` en *2003*, probaremos si podemos enumerar los usuarios de la base SAM.

```
Símbolo del sistema
C:\Documents and Settings\Karina\Escritorio\Enumeration>nbtscan
nbtscan 1.0.35 - 2008-04-08 - http://www.unixwiz.net/tools/

usage: nbtscan [options] target [targets...]

Targets are lists of IP addresses, DNS names, or address
ranges. Ranges can be in /nbits notation ("192.168.12.0/24")
or with a range in the last octet ("192.168.12.64-97")

-U      show Version information
-f      show Full NBT resource record responses (recommended)
-H      generate HTTP headers
-v      turn on more Verbose debugging
-n      No looking up inverse names of IP addresses responding
-p <n>  bind to UDP Port <n> (default=0)
-m      include MAC address in response (implied by '-f')
-T <n>  Timeout the no-responses in <n> seconds (default=2 secs)
-w <n>  Wait <n> msec after each write (default=10 ms)
-t <n>  Try each address <n> tries (default=1)
-l      Use Winsock 1 only
-P      generate results in perl hashref format

C:\Documents and Settings\Karina\Escritorio\Enumeration>nbtscan -f SUR1
192.168.91.133 DEMO\SUR1 SHARING DC
SUR1 <00> UNIQUE Workstation Service
DEMO <00> GROUP Domain Name
DEMO <1c> GROUP Domain Controller
SUR1 <20> UNIQUE File Server Service
DEMO <1b> UNIQUE Domain Master Browser
DEMO <1e> GROUP Browser Service Elections
DEMO <1d> UNIQUE Master Browser
.._MSBROWSE_ <01> GROUP Master Browser
00:0c:29:97:fd:c4 ETHER SUR1

C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

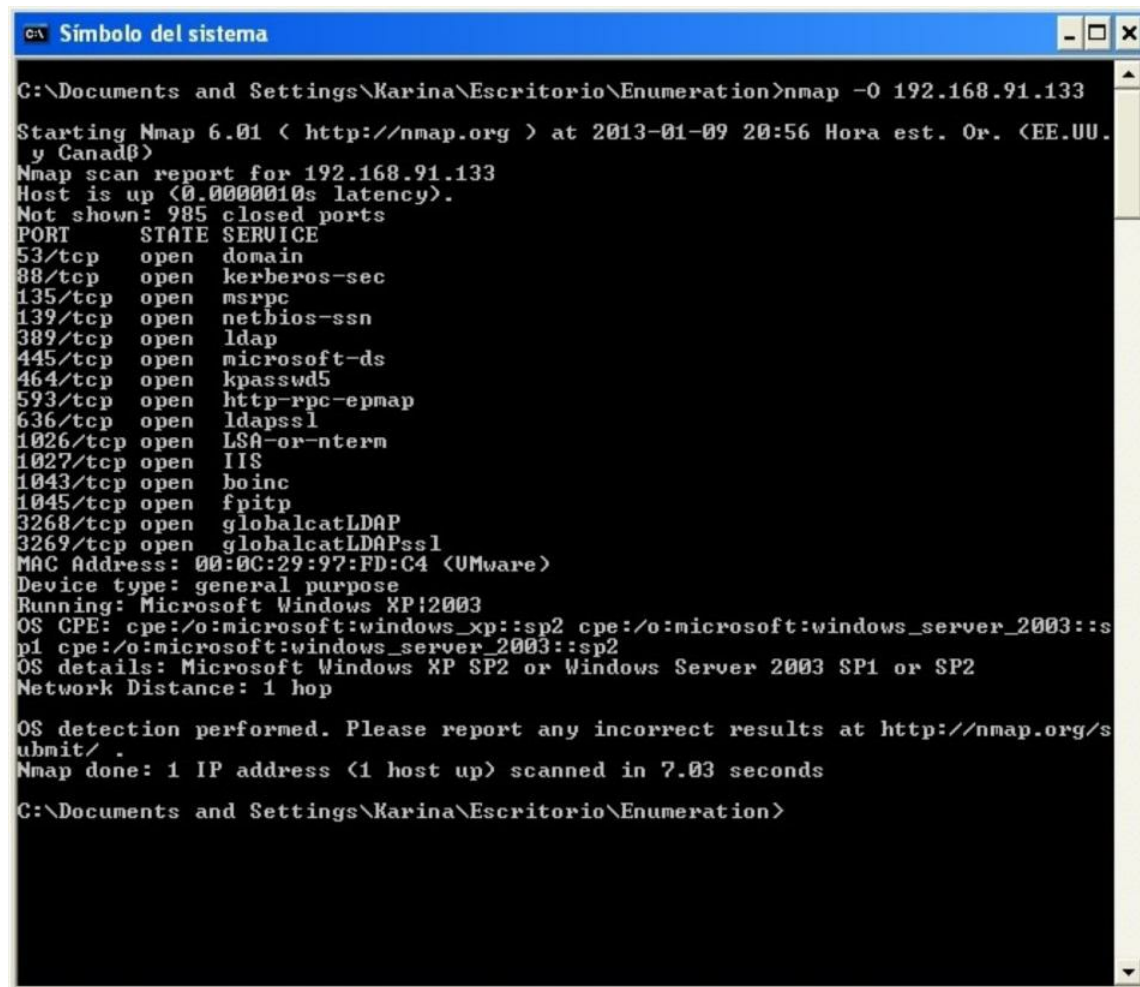
Figura 69 - Enumeración con nbtscan

Para obtener información de usuarios y grupos existen diversas herramientas disponibles, pero antes de revisarlas es necesario explicar algo acerca de cómo *Windows* identifica internamente a las entidades conocidas como “*Security Principals*”, en español: *Sujetos*.

Los *Sujetos* son elementos a los que el sistema operativo *Windows* les puede asignar un identificador llamado *SID* (*Security Identifier*). Las cuentas de usuarios, grupos, computadoras y los servicios (en las últimas versiones) son ejemplos de *Sujetos*.

La idea detrás de esto es poder controlar quién (*Sujeto*) puede acceder a un recurso (*Objeto*) y qué puede hacer con él (*Permisos*).





```
C:\Documents and Settings\Karina\Escritorio\Enumeration>nmap -O 192.168.91.133
Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-09 20:56 Hora est. Or. <EE.UU. y Canadá>
Nmap scan report for 192.168.91.133
Host is up (0.0000010s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1043/tcp  open  boinc
1045/tcp  open  fptp
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 00:0C:29:97:FD:C4 (VMware)
Device type: general purpose
Running: Microsoft Windows XP!2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

Figura 70 - Detección de sistema operativo con Nmap

El *SID* como su nombre sugiere es un identificador único dentro del sistema, el cual tiene una estructura como la expresada en la Figura 71.

Veamos un ejemplo de *SID*:

**S-1-5-21-1856294723-2589421158-136412327-500**

Los valores S-1-5 indican que se trata de un *SID* con nivel de revisión 1 y el valor 5 nos dice que fue generado por la autoridad *Windows NT*, es decir por el sistema operativo per se.

El valor 21 implica que este es un *SID* que no es universalmente único, es decir que solo es único para el dominio en donde se generó.

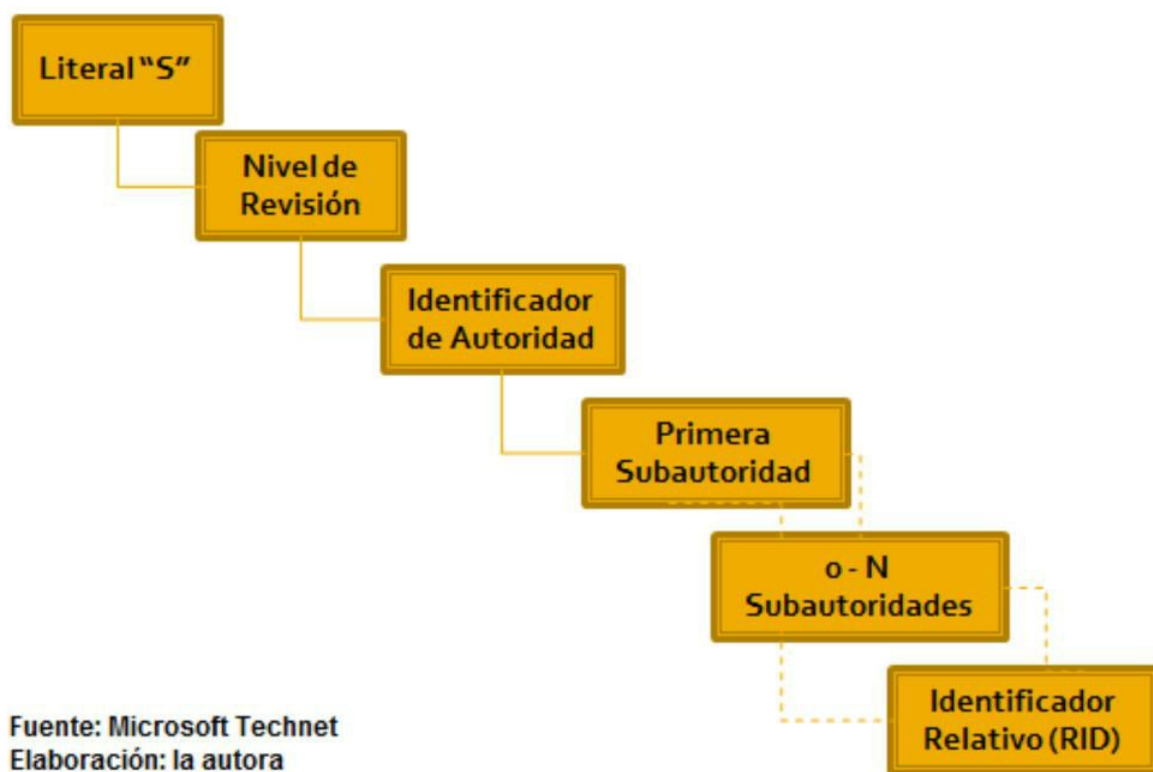


Figura 71 - Estructura del SID

Los siguientes valores 1856294723-2589421158-136412327, tres sub-autoridades juntas, identifican al dominio que generó el *SID*.

Y por último el valor 500 representa de manera única dentro del dominio dado a la cuenta que denota, para este ejemplo: la cuenta del usuario Administrador built-in (creada por defecto durante la instalación del sistema operativo).

Las tablas que indican el significado de estos valores se encuentran detalladas en el sitio web de soporte de *Microsoft*. Veamos un extracto de algunas de ellas (Tablas 5 a 7).

Tabla 5 - Autoridades

ID de Autoridad	Significado
0	SECURITY_NULL_SID_AUTHORITY. Se usa para realizar comparaciones cuando se desconoce el identificador de autoridad.
1	SECURITY_WORLD_SID_AUTHORITY Usada para construir SIDs que representan a todos los usuarios.
2	SECURITY_LOCAL_SID_AUTHORITY Se usa para crear SIDs que representan usuarios que ingresan a una consola local.
3	SECURITY_CREATOR_SID_AUTHORITY Utilizado para crear SIDs que indican al creador o dueño de un objeto.
5	SECURITY_NT_AUTHORITY Representa al sistema operativo.

Fuente: Microsoft Technet  
Elaboración: La autora

Tabla 6 - Sub-autoridades

ID de Subautoridad	Significado
5	Usado para otorgar permisos a las aplicaciones que se ejecutan en una sesión específica.
6	Usado cuando un proceso se autentica como servicio.
21	Especifica SIDs de computadoras y usuarios que no son únicos universalmente, es decir tienen significado local.
32	Identifica SIDs de tipo predefinidas (built-in).
80	Sirve para identificar SIDs de servicios.

Fuente: Microsoft Technet  
Elaboración: La autora

*Tabla 7 - RIDs bien conocidos*

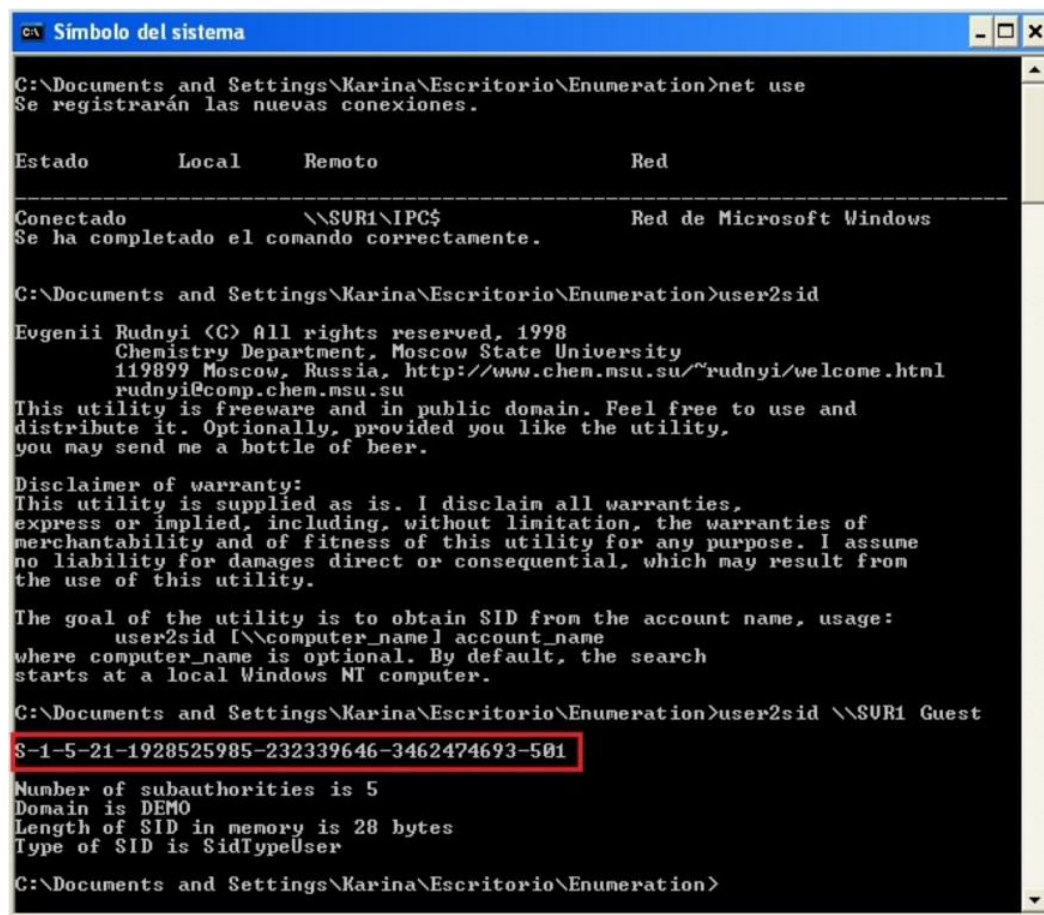
RID	Significado
500	Administrador
501	Invitado
502	Kerberos
512	Administradores de Dominio

Fuente: Microsoft Technet  
Elaboración: La autora

Sé que toda esta teoría puede resultar aburrida y que la estructura del *SID* pareciera ser compleja, pero por favor acepten mi palabra de que me he tomado la molestia de explicar todo esto porque tener claro este concepto será útil para nuestro propósito de enumerar las cuentas de usuarios y grupos y nos dará una ventaja sobre otros pseudo-consultores que desconocen cómo *Windows* maneja internamente la seguridad de sus elementos.

Dicho esto pongámonos a la obra, empezaremos usando el comando `user2sid`<sup>35</sup>.

La herramienta `user2sid` nos trae como resultado el *SID* a partir de indicar un *Sujeto* conocido (ver Ilustración 72). En el ejemplo hemos probado suerte con la cuenta `Guest` la cual es bien conocida y está presente en todos los sistemas *Windows*. Si no hubiésemos obtenido respuesta nuestro siguiente intento sería con la cuenta `Invitado`, por si se tratara de una versión del sistema en español.



```
C:\Documents and Settings\Karina\Escritorio\Enumeration>net use
Se registrarán las nuevas conexiones.

Estado          Local          Remoto          Red
-----
Conectado          \\SUR1\IPC$          Red de Microsoft Windows
Se ha completado el comando correctamente.

C:\Documents and Settings\Karina\Escritorio\Enumeration>user2sid

Eugenii Rudnyi <C> All rights reserved, 1998
Chemistry Department, Moscow State University
119899 Moscow, Russia, http://www.chem.msu.su/~rudnyi/welcome.html
rudnyi@comp.chem.msu.su
This utility is freeware and in public domain. Feel free to use and
distribute it. Optionally, provided you like the utility,
you may send me a bottle of beer.

Disclaimer of warranty:
This utility is supplied as is. I disclaim all warranties,
express or implied, including, without limitation, the warranties of
merchantability and of fitness of this utility for any purpose. I assume
no liability for damages direct or consequential, which may result from
the use of this utility.

The goal of the utility is to obtain SID from the account name, usage:
  user2sid [\\computer_name] account_name
where computer_name is optional. By default, the search
starts at a local Windows NT computer.

C:\Documents and Settings\Karina\Escritorio\Enumeration>user2sid \\SUR1 Guest
S-1-5-21-1928525985-232339646-3462474693-501
Number of subauthorities is 5
Domain is DEMO
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

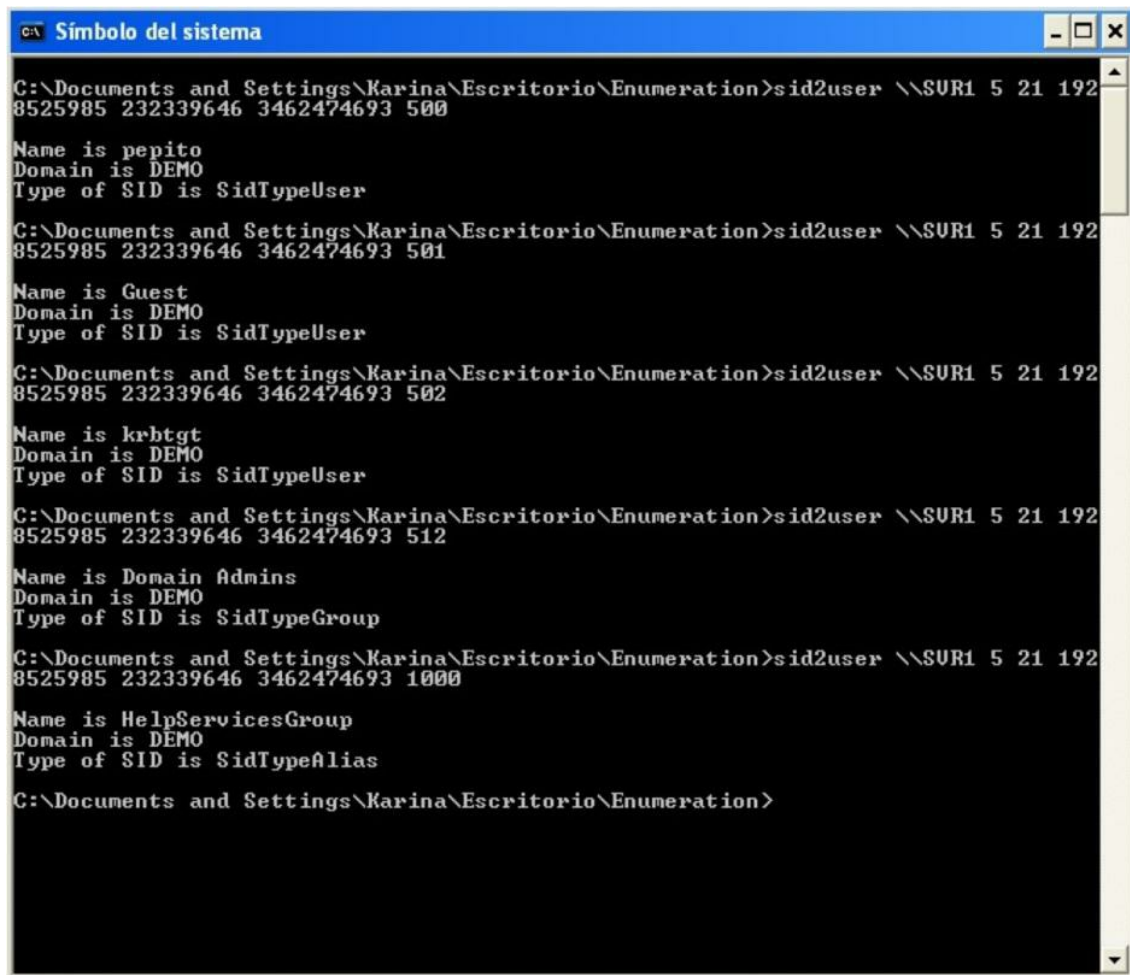
C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

Figura 72- Resultado de ejecutar user2sid con la cuenta Guest

¿Pero para qué queremos el *SID*? Muy simple, al obtener el *SID* del dominio, podemos usarlo luego para enumerar las cuentas de usuarios y grupos cambiando cada vez el valor del *RID* solamente. Recordemos que el *RID* es el identificador relativo, es decir que es único solo dentro del dominio, por ello aunque el resto del *SID* varía para cada dominio (valores diferentes de subautoridades generados al momento de la instalación) los *RIDs* bien conocidos se mantienen y podemos aprovechar esto para identificar cuentas importantes como la del Administrador built-in.

Observemos en la Figura 73 el resultado de ejecutar sid2user repetidas veces variando cada vez el valor del *RID*.





```
C:\Documents and Settings\Karina\Escritorio\Enumeration>sid2user \\SUR1 5 21 192
8525985 232339646 3462474693 500

Name is pepito
Domain is DEMO
Type of SID is SidTypeUser

C:\Documents and Settings\Karina\Escritorio\Enumeration>sid2user \\SUR1 5 21 192
8525985 232339646 3462474693 501

Name is Guest
Domain is DEMO
Type of SID is SidTypeUser

C:\Documents and Settings\Karina\Escritorio\Enumeration>sid2user \\SUR1 5 21 192
8525985 232339646 3462474693 502

Name is krbtgt
Domain is DEMO
Type of SID is SidTypeUser

C:\Documents and Settings\Karina\Escritorio\Enumeration>sid2user \\SUR1 5 21 192
8525985 232339646 3462474693 512

Name is Domain Admins
Domain is DEMO
Type of SID is SidTypeGroup

C:\Documents and Settings\Karina\Escritorio\Enumeration>sid2user \\SUR1 5 21 192
8525985 232339646 3462474693 1000

Name is HelpServicesGroup
Domain is DEMO
Type of SID is SidTypeAlias

C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

Figura 73 – Enumeración de cuentas con Sid2user

El comando *sid2user* tiene la siguiente sintaxis:

```
sid2user [\computer_name] authority subauthority_1 ...
```

De esa manera, copiamos el valor del *SID* obtenido por *user2sid* y lo pegamos como parámetro de *sid2user*, pero omitiendo S-1, es decir desde el valor de autoridad (5) y colocando espacios en lugar de guiones, como se observa en la Figura previa.

Al ir variando los *RIDs* el resultado es que enumeraremos los usuarios y grupos del sistema, ¡y todo esto con tan solo una sesión nula!

Analizando el resultado obtenido con este comando nos percatamos que en un intento de confundir a los intrusos, el administrador del servidor le ha cambiado el nombre a la cuenta Administrator por Pepito. Pero dado que el *RID* es 500 sabemos con certeza que se trata de la cuenta del Administrador built-in. ¿Y qué tiene de especial esta cuenta? Bueno, aparte de que tiene todos los privilegios para administrar el sistema, una característica particular de esta cuenta es que está configurada por defecto para no bloquearse, precisamente como una *protección* puesta por *Microsoft* para evitar que un administrador se auto-bloquee por error. ¿Les he dicho que amo a *Microsoft*?

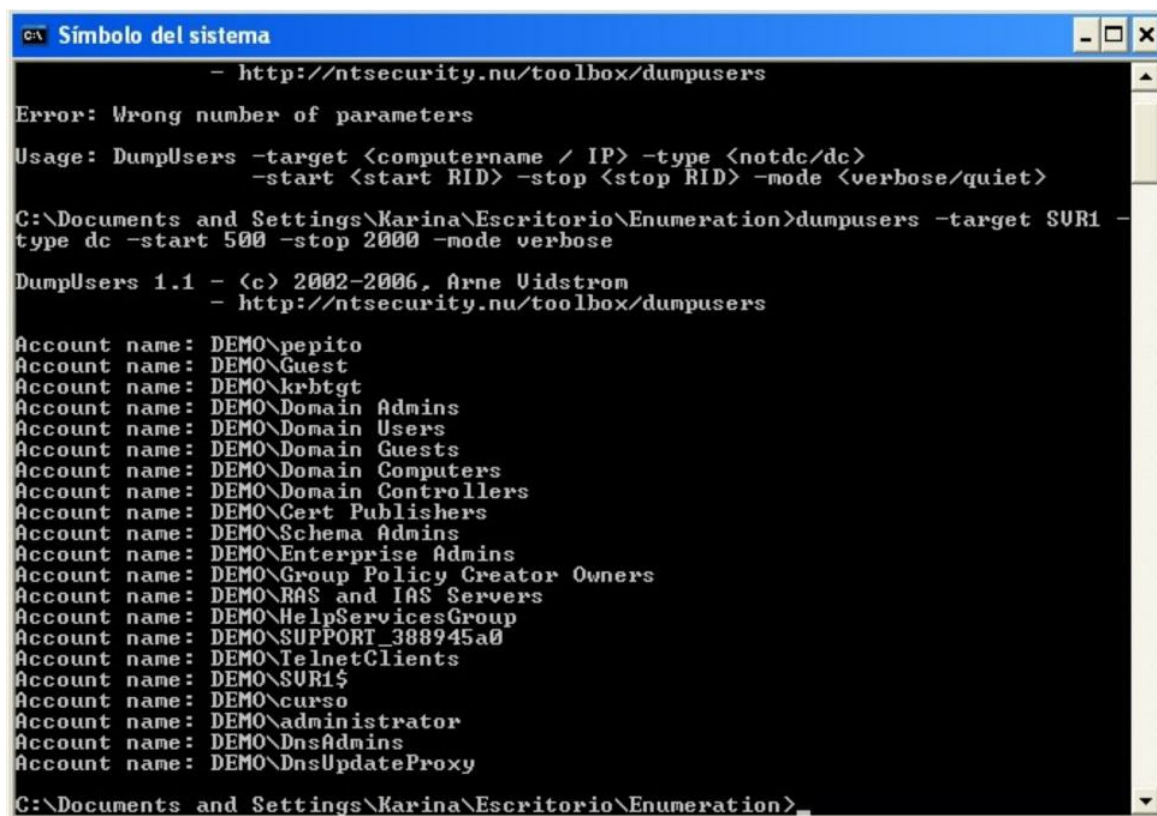
**Nota:** Esto implica que en una fase posterior podríamos ejecutar un ataque de claves contra la cuenta del Administrador built-in, probando distintas combinaciones de caracteres - infinidad de veces - sin el riesgo de bloquearla y sin importar si el administrador ha configurado el bloqueo de cuentas usual en el servidor. Por supuesto, esto asumiendo que no se han restringido los derechos a este usuario para poder autenticarse a través de la red, lo cual es la configuración por defecto.

## Herramientas de enumeración todo-en-uno

Ahora que entendemos cómo funciona internamente la seguridad de cuentas de *Windows* estamos listos para usar herramientas todo-en-uno que abstraigan estos conceptos y nos faciliten la labor de enumerar. Veamos algunos ejemplos.

## Dumpusers

La herramienta *dumpusers* funciona en línea de comandos y su uso es muy sencillo, tal y como podemos observar en la siguiente captura de pantalla (Figura 74).



```

C:\> http://ntsecurity.nu/toolbox/dumpusers

Error: Wrong number of parameters
Usage: DumpUsers -target <computername / IP> -type <notdc/dc>
        -start <start RID> -stop <stop RID> -mode <verbose/quiet>

C:\Documents and Settings\Karina\Escritorio\Enumeration>dumpusers -target SUR1 -
type dc -start 500 -stop 2000 -mode verbose

DumpUsers 1.1 - (c) 2002-2006, Arne Vidstrom
               - http://ntsecurity.nu/toolbox/dumpusers

Account name: DEMO\pepito
Account name: DEMO\Guest
Account name: DEMO\krbtgt
Account name: DEMO\Domain Admins
Account name: DEMO\Domain Users
Account name: DEMO\Domain Guests
Account name: DEMO\Domain Computers
Account name: DEMO\Domain Controllers
Account name: DEMO\Cert Publishers
Account name: DEMO\Schema Admins
Account name: DEMO\Enterprise Admins
Account name: DEMO\Group Policy Creator Owners
Account name: DEMO\RAS and IAS Servers
Account name: DEMO\HelpServicesGroup
Account name: DEMO\SUPPORT_388945a0
Account name: DEMO\TelnetClients
Account name: DEMO\SUR1$
Account name: DEMO\curso
Account name: DEMO\administrator
Account name: DEMO\DnsAdmins
Account name: DEMO\DnsUpdateProxy

C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

Figura 74 - Enumerando con dumpusers

Este programa fue desarrollado y es actualmente mantenido por *Arne Vidstrom*, junto con otras herramientas muy útiles, en su sitio web *NTSecurity*<sup>36</sup>.

Si observamos el reporte obtenido veremos que *dumpusers* ha obtenido fácilmente la lista de cuentas de usuario del servidor víctima, lamentablemente no muestra junto con el nombre el *RID* correspondiente; pero, dado que iniciamos la enumeración desde 500 podemos deducir que la cuenta Pepito es en efecto el Administrador built-in.

Los parámetros requeridos son:

-target        nombre de host o dirección IP de la víctima

-type        opciones posibles son: dc si se trata de un controlador de dominio o notdc si se trata de una estación de trabajo o un servidor miembro.

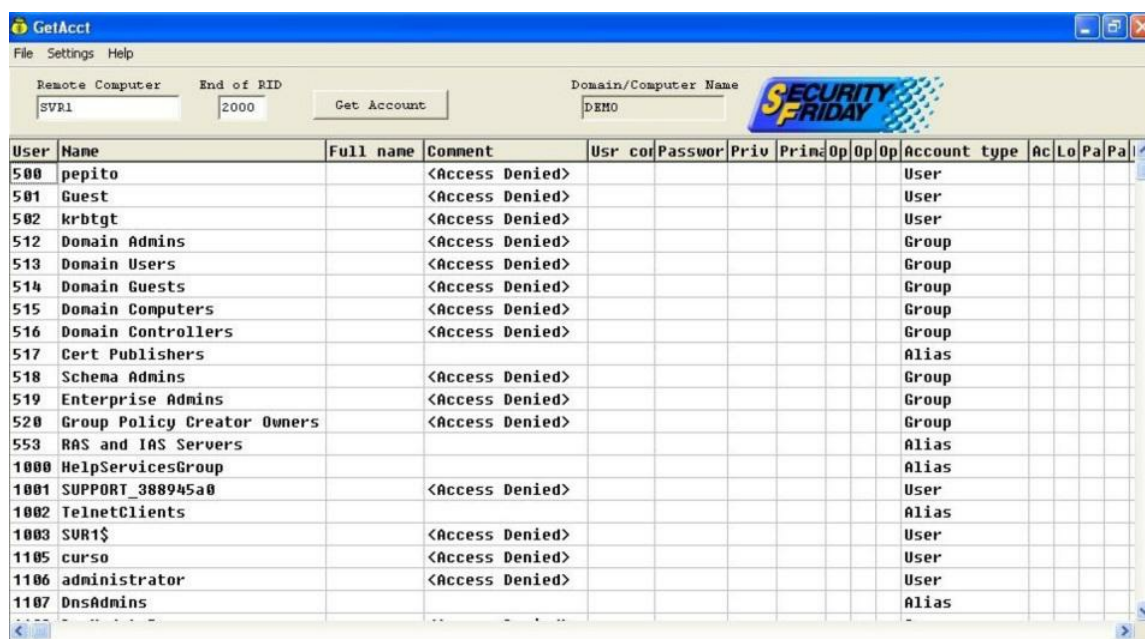
-start        identificador relativo (*RID*) inicial. Ej: 500

-stop        identificador relativo (*RID*) final hasta donde queremos enumerar. Ej: 2000

-mode        opciones posibles: verbose si deseamos que muestre resultados en pantalla tan pronto como los encuentre, o quiet si preferimos que muestre toda la información encontrada al final.

## GetAcct

Este software desarrollado por la empresa *Security Friday*, posee una interfaz gráfica muy amigable y tiene como ventaja que el reporte que presenta en pantalla sí lista el *RID*, además de que enumera no sólo usuarios sino también grupos y el informe puede ser exportado en formato delimitado por comas (.csv).



The screenshot shows the GetAcct application window. At the top, there's a menu bar with 'File', 'Settings', and 'Help'. Below it, there are input fields for 'Remote Computer' (SVR1), 'End of RID' (2000), and 'Domain/Computer Name' (DEMO). A 'Get Account' button is also present. The main area displays a table of results. The table has columns: User, Name, Full name, Comment, Usr cor, Passwor, Priv, Prin, Op, Op, Op, Account type, Ac, Lo, Pa, Pa. The data rows show various users and groups, all with 'Access Denied' in the Comment column. The account types are listed as User, Group, or Alias.

User	Name	Full name	Comment	Usr cor	Passwor	Priv	Prin	Op	Op	Op	Account type	Ac	Lo	Pa	Pa
500	pepito		<Access Denied>								User				
501	Guest		<Access Denied>								User				
502	krbtgt		<Access Denied>								User				
512	Domain Admins		<Access Denied>								Group				
513	Domain Users		<Access Denied>								Group				
514	Domain Guests		<Access Denied>								Group				
515	Domain Computers		<Access Denied>								Group				
516	Domain Controllers		<Access Denied>								Group				
517	Cert Publishers										Alias				
518	Schema Admins		<Access Denied>								Group				
519	Enterprise Admins		<Access Denied>								Group				
520	Group Policy Creator Owners		<Access Denied>								Group				
553	RAS and IAS Servers										Alias				
1000	HelpServicesGroup										Alias				
1001	SUPPORT_388945a0		<Access Denied>								User				
1002	TelnetClients										Alias				
1003	SVR1\$		<Access Denied>								User				
1105	curso		<Access Denied>								User				
1106	administrator		<Access Denied>								User				
1107	DnsAdmins										Alias				

Figura 75 - Reporte generado por GetAcct<sup>37</sup>

La Figura 75 expone un reporte ejemplo generado a partir del aplicativo GetAcct.

## DumpSec y Hyena

Estas dos aplicaciones provistas por la empresa *Somarsoft*<sup>38</sup>, ofrecen opciones interesantes como: listar usuarios, grupos, servicios, sesiones, etc. (ver Ilustraciones 76 a 79). Pese a ello, no todos los reportes son posibles de obtener con una sesión nula, por lo que pueden resultar más útiles durante la fase de hacking, cuando se hubieren obtenido credenciales de un usuario válido.

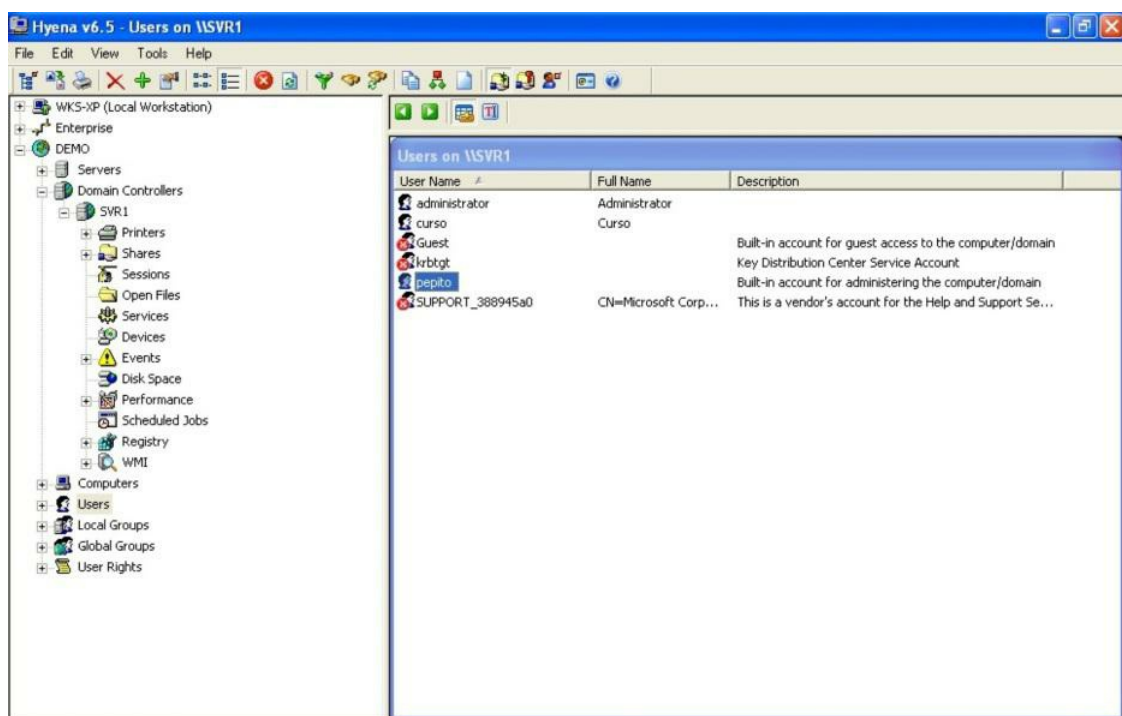


Figura 76 - Listado de usuarios con Hyena

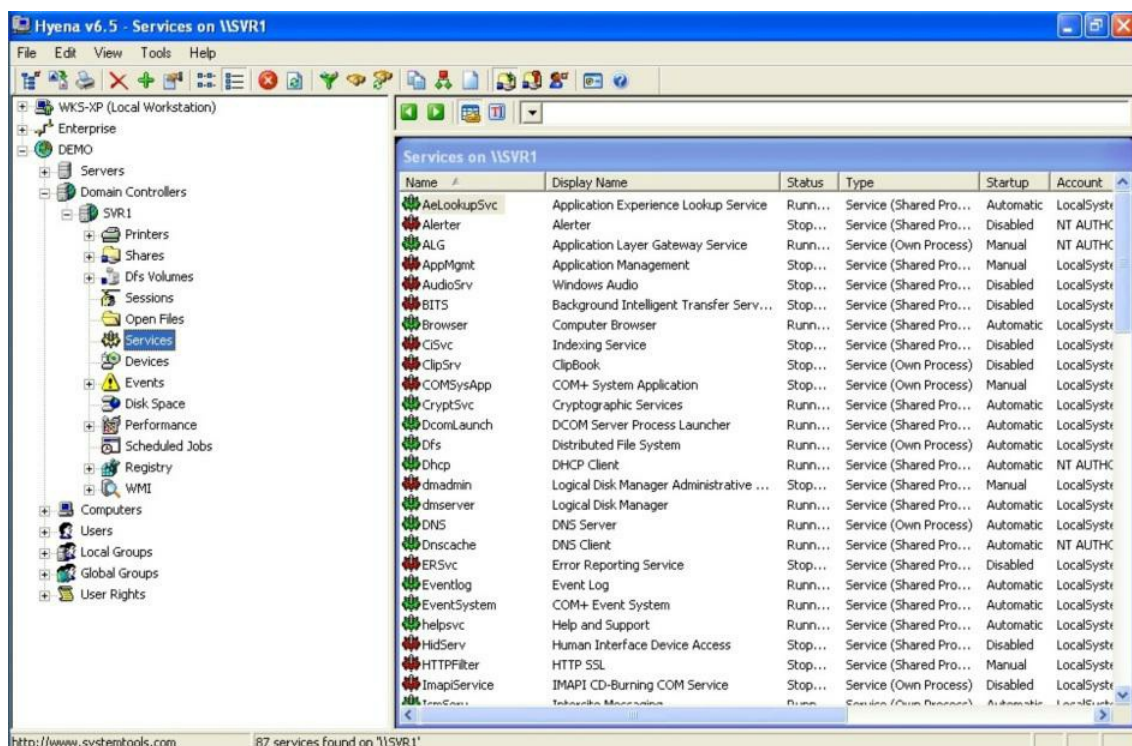


Figura 77 - Listado de servicios con Hyena



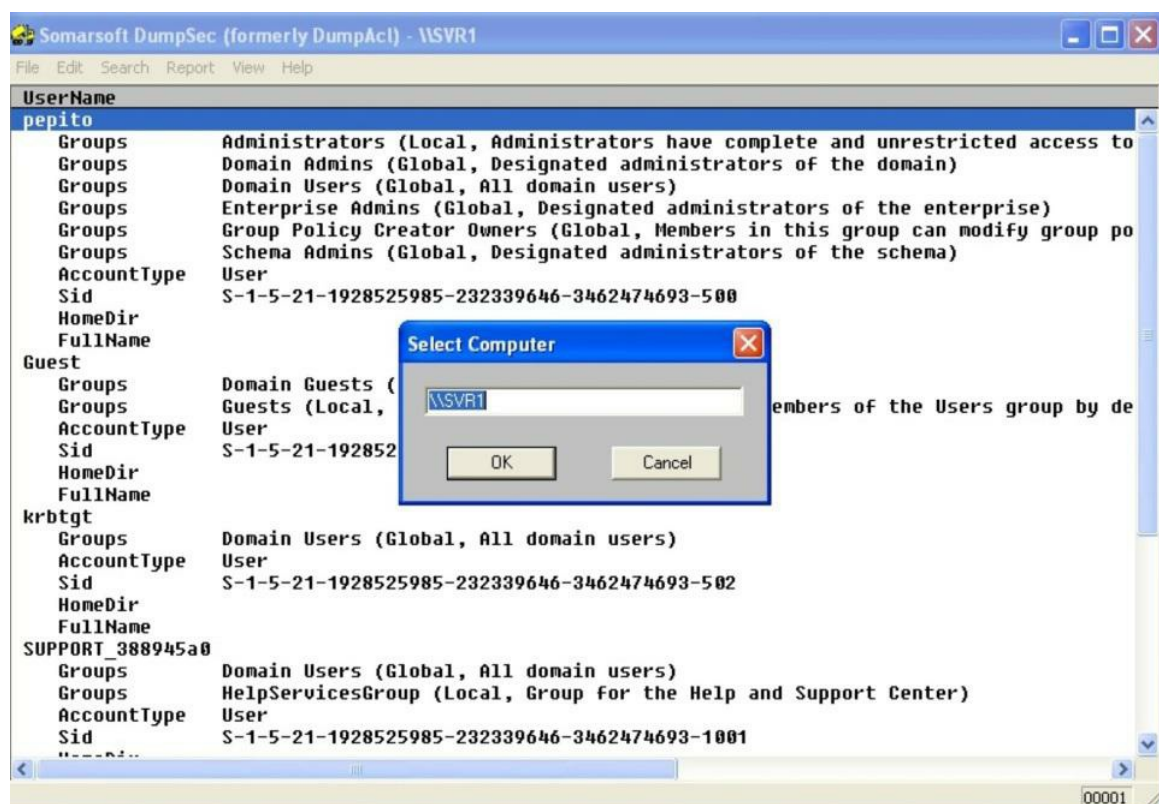


Figura 78 - Reporte de usuarios con DumpSec

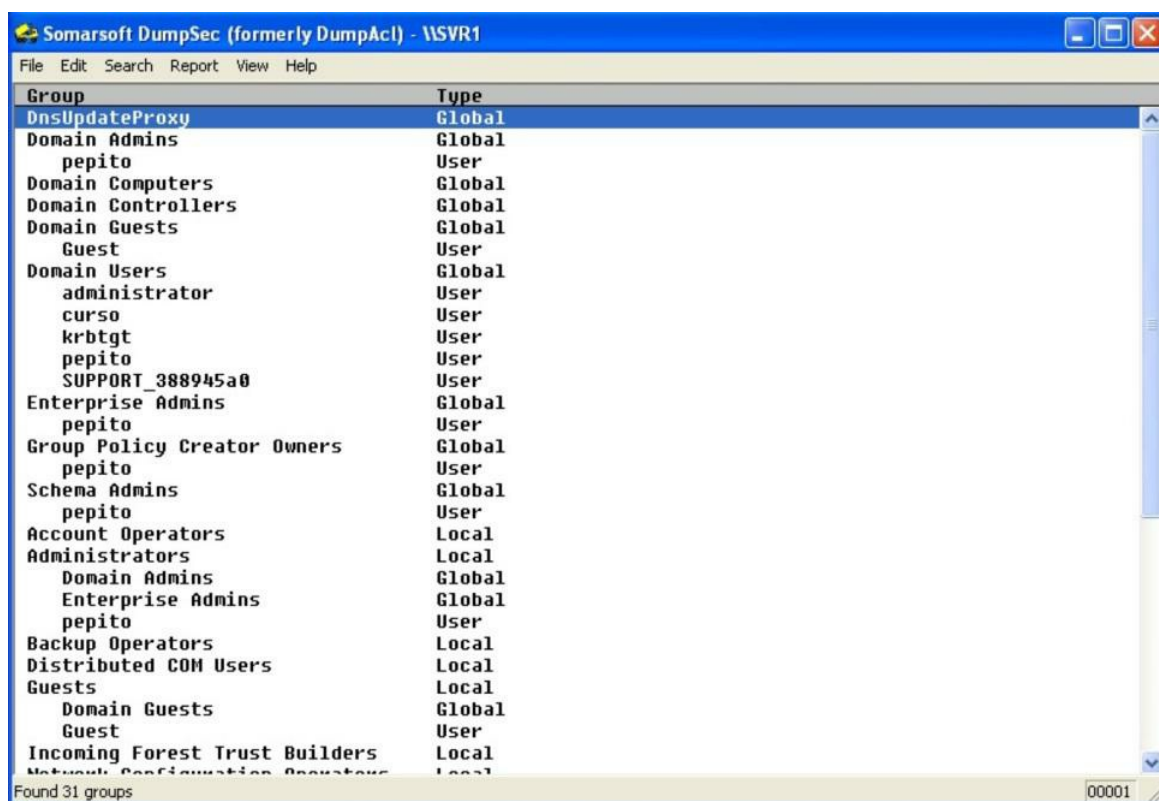


Figura 79 - Enumeración de grupos con DumpSec

Por supuesto existen muchos otros comandos y herramientas de enumeración *todo-en-uno* disponibles, pero hemos cubierto las esenciales.

## Laboratorios de enumeración

### Enumeración de Windows desde el CLI

En el laboratorio actual usted aplicará los conocimientos adquiridos en el capítulo de Enumeración para adquirir información detallada sobre equipos *Windows*, haciendo uso de

## herramientas de enumeración Netbios.

***Nota:** Para la ejecución del laboratorio usaremos Windows XP como estación hacker. Es necesario que existan estaciones Windows adicionales en la red y de forma preferente un equipo Windows Server para que el laboratorio sea productivo. Refiérase al Apéndice A acerca de los consejos para realizar con éxito los laboratorios.*

1. Abra una ventana de comandos en su estación de trabajo Windows y ejecute el comando:

```
net view /DOMAIN
```

1. ¿Qué dominios y grupo de trabajo encontró? ¿Cuáles son las IPs asociadas? Anote sus hallazgos en su bitácora.
2. Abra una sesión nula hacia los servidores objetivos. ¿Qué comando debe ejecutar?
3. Escanee en detalle los servidores con ayuda del comando nbtstat:

```
nbtstat -A IP_ServerX
```

1. Posteriormente efectúe un escaneo del protocolo Netbios sobre los servidores objetivo con ayuda del comando nbtscan:

```
nbtscan -f IP_ServerX
```

1. Ejecute adicionalmente algunos comandos de enumeración de usuarios. ¿Fue factible obtener información de los usuarios del sistema?

```
dumpusers -target IP_ServerX -type dc -start 500 -stop 1100 -mode verbose
```

1. Compruebe la utilidad del comando user2sid para obtener el SID del sistema operativo. Utilice como “carnada” el nombre de un usuario conocido como Administrador, Administrator, Invitado, Guest, etc.

```
user2sid \\ IP_ServerX Administrator
```

1. Una vez obtenido el SID del sistema, use el comando sid2user para enumerar los usuarios y grupos del sistema. ¿Cuál es la sintaxis del comando? Desafío: haga un script en DOS que ejecute el comando sid2user dentro de un lazo (loop).

## Enumeración de Windows con DumpSec

En esta ocasión usaremos una herramienta gráfica de enumeración un tanto añeja, pero no por eso menos útil, *DumpSec*, bajo *Windows XP* para enumerar otros sistemas *Windows* de nuestra red.

***Nota:** Para la ejecución del laboratorio usaremos Windows XP como estación hacker y Windows 2003 y 2008 Server como objetivos. Refiérase al Apéndice A acerca de los consejos para realizar con éxito los laboratorios.*

1. Verifique que el aplicativo *DumpSec* se encuentre instalado y ejecútelo.
2. Seleccione el servidor objetivo: menú **Report** -> **Select Computer** (\\IP\_ServerX) tal y como se expone en la Figura 80.
3. Luego pruebe con los diferentes reportes disponibles bajo la opción **Report**.
4. ¿Hay diferencias en los reportes cuando el objetivo es *Windows 2003* Vs *Windows 2008 Server*?

# Medidas preventivas

Dado que son múltiples los protocolos susceptibles de enumeración cabría preguntarnos ¿cuáles de ellos son realmente necesarios en nuestra red? La medida de prevención obvia es deshabilitar aquellos protocolos inseguros que no son requeridos en nuestra red.

Con todo, esto no siempre es factible, sobre todo si existen aplicaciones heredadas (legacy) en la organización que dependen de protocolos inseguros para operar y para las que no hay una migración programada en el corto plazo.

Algunas medidas paliativas:

- Configurar reglas de filtrado en los firewalls de borde para impedir la publicación en Internet de protocolos susceptibles de enumeración que no cumplan una función pública (por ejemplo Netbios).
- Implementar un plan para subir de versión los sistemas operativos y aplicaciones de forma periódica en función del costo/beneficio. En empresas en donde el número de estaciones es extenso, se podría considerar un proyecto para reemplazar los desktops por clientes livianos haciendo uso de virtualización, usualmente los costos de licenciamiento son menores en ambientes virtuales.
- De forma similar, en ambientes con numerosos servidores, un proceso de consolidación podría no sólo brindar ahorros en consumo de energía eléctrica, sino además en costos de mantenimiento de hardware/software y facilitar la administración de la seguridad informática.
- Si se tiene una red predominantemente *Windows*, se pueden implementar políticas de Directorio Activo para impedir el establecimiento de sesiones nulas y deshabilitar el logon vía red del usuario Administrador built-in. Con todo, se debe tener cuidado con los programas heredados (legacy) que podrían hacer uso de null sessions.

# Recursos útiles

- Libro: [Network Defense: Security Policy and Threats](#)<sup>39</sup>.
- Libro: [Network Defense: Securing and Troubleshooting Network Operating Systems](#)<sup>40</sup>.
- Libro: [Linux Security Cookbook](#)<sup>41</sup>.
- Libro: [Microsoft Windows Security Essentials](#)<sup>42</sup>.
- Url: [TN Microsoft Security Bulletins](#)<sup>43</sup>.