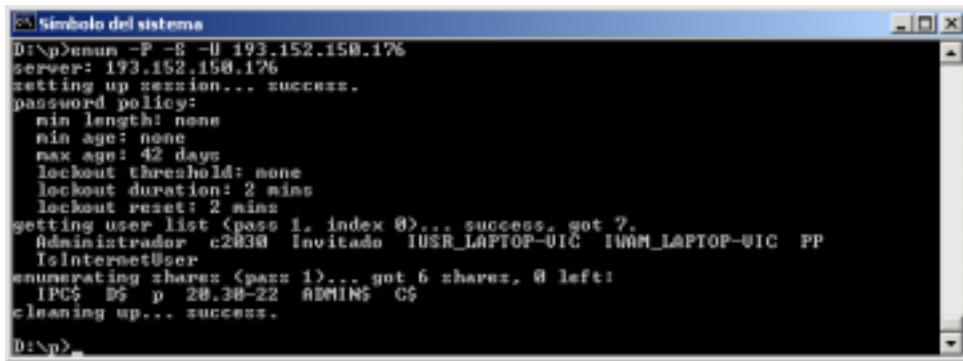


## Práctica: 33. Enumeración de Usuarios (Por HxC Mods-Adm)

*Enum*, es una buena herramienta para la enumeración de usuarios, recursos y más

Prueba las opciones -U, -S y -P

Enum por sí mismo ya establece la sesión nula, por lo que no es preciso que la hagas,



```
D:\p>enum -F -S -U 193.152.150.176
server: 193.152.150.176
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 2 mins
  lockout reset: 2 mins
getting user list (pass 1, index 0)... success, got 7:
Administrator c2030 Invitado IUSR_LAPTOP-UIC IUSR_LAPTOP-UIC PP
IInternetUser
enumerating shares (pass 1)... got 6 shares, 0 left:
IPC$ D$ p 20.30-22 ADMIN$ C$
cleaning up... success.
D:\p>
```

Como verás -P nos muestra la política de contraseñas, -S los recursos compartidos y -U los usuarios.

Otras dos herramientas interesantes son *UserInfo* y *UserDump*

Las dos muestran la misma información lo que difiere es como la consiguen:

*Userinfo* necesita una dirección objetivo y un nombre de usuario válido.

*UserDump* necesita una dirección objetivo el nombre de la cuenta de invitado y un valor.

*UserDump* muestra el mismo contenido, pero puede enumerar varias cuentas, esto es:

Si le indicamos un nombre de usuario y un valor mostrará la pantalla anterior por cada usuario que encuentre, tantos como el valor numérico que se le dé.

*UserDump* obtendrá siempre como primer valor el del administrador (id 500) y luego las de los usuarios (1000, 1001, 1002,...), por ejemplo:

*UserDump* **\\193.152.150.176 Invitado 5,**

mostrará la información anterior (como la de *userinfo*) para el administrador y los primeros 5 usuarios creados.

Fíjate bien que en la sintaxis se ha incluido *Invitado*, así es como trabaja *UserDump*, primero localiza la cuenta del invitado y luego “encuentra” la del administrador y después las de los usuarios

Si el idioma o lenguaje de la máquina objetivo fuese inglés, debes poner *guest* en lugar de *invitado*, si fuese alemán *gast*???

Vamos aprobar UserInfo

```
Símbolo del sistema
D:\p>userinfo \\193.152.150.176 administrador

UserInfo v1.5 - thor@hammerofgod.com
Querying Controller \\193.152.150.176

USER INFO
Username:      Administrador
Full Name:    Cuentas para la administraci3n del equipo o dominio
Comment:
User Comment:
User ID:      500
Primary Grp:  513
Prius:        Admin Prius
OperatorPrius: No explicit OP Prius

SYSTEM FLAGS (Flag dword is 66049)
User's pwd never expires.

MISC INFO
Password age:  Mod Feb 19 12:34:03 2003
LastLogon:     Fri Feb 21 00:17:52 2003
LastLogoff:    Thu Jan 01 00:00:00 1970
Acct Expires:  Never
Max Storage:   Unlimited
Workstations:
UnitsperWeek:  168
Bad pw Count:  0
Num logons:    218
Country code:  0
Code page:     0
Profile:
ScriptPath:
Homedir drive:
Home Dir:
PasswordExp:   0

Logon hours at controller, GMT:
Hours-        12345678901M12345678901M
Sunday        11111111111111111111111111111111
Monday        11111111111111111111111111111111
Tuesday       11111111111111111111111111111111
Wednesday    11111111111111111111111111111111
Thursday      11111111111111111111111111111111
Friday        11111111111111111111111111111111
Saturday      11111111111111111111111111111111
```

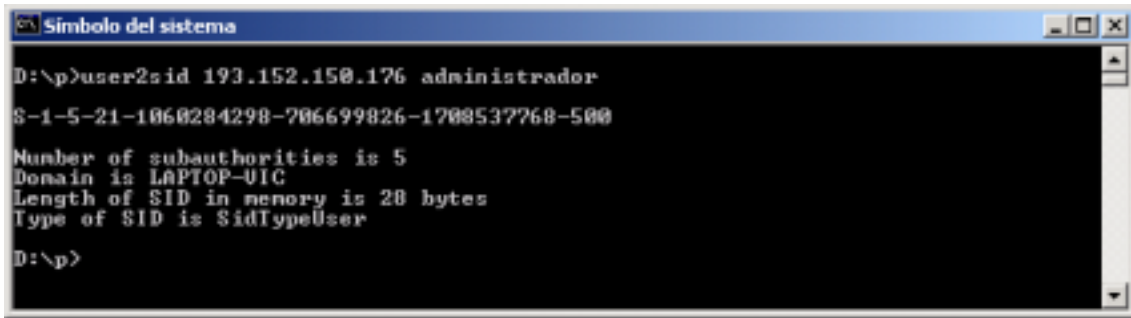
La informaci3n es jugosa, desde el n3mero de logins de la cuenta, hasta las horas de inicio permitido de sesiones, algo as3 como las propiedades de la cuenta en cuesti3n.

Presta especial atenci3n al dato User-Id:500, 3ste valor indica la cuenta del administrador.

Las herramientas por excelencia para la enumeraci3n de usuarios son *user2sid* y *sid2user*

Para utilizar estas herramientas se debe establecer primero una sesi3n nula y funcionar3n incluso si se estableci3 *RestrictAnonymous* a 1.

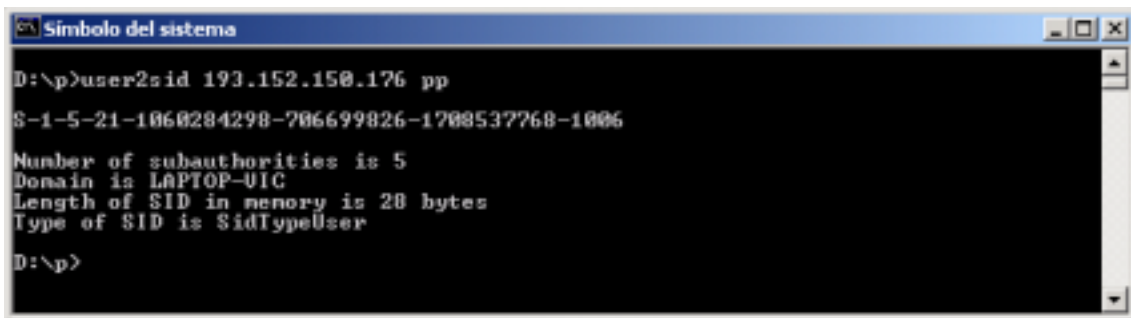
Probando:



```
D:\p>user2sid 193.152.150.176 administrador
S-1-5-21-1060284298-706699826-1708537768-500

Number of subauthorities is 5
Domain is LAPTOP-UIC
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

D:\p>
```



```
D:\p>user2sid 193.152.150.176 pp
S-1-5-21-1060284298-706699826-1708537768-1006

Number of subauthorities is 5
Domain is LAPTOP-UIC
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

D:\p>
```

Explicando todos esos números...

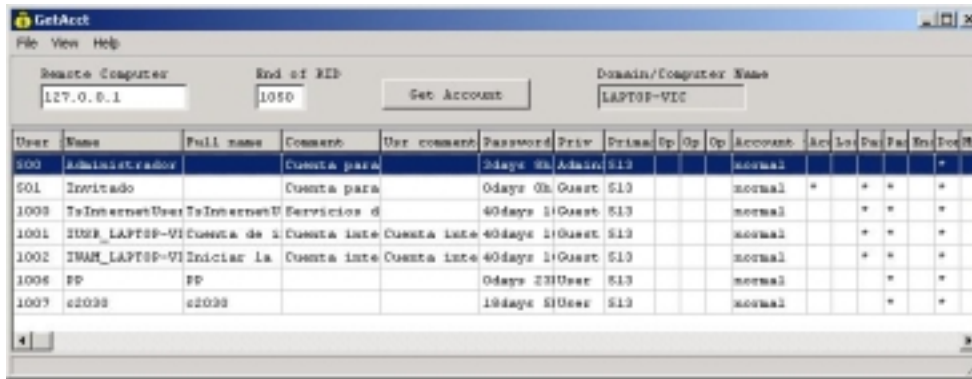
**S-1-5-21** será un valor constante que identifica a una **máquina Windows 2000**

Los tres grupos numéricos de **0000000000-11111111111-22222222222** son el **SID** de usuario, número único de identificación para todo el dominio o grupo de trabajo.

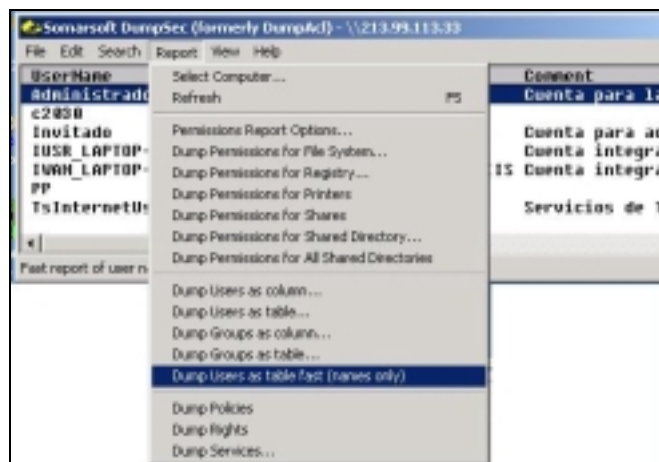
El último grupo de dígitos **500** para el *administrador* ó **1006** para el usuario *pp* es el **RID**, que sigue las siguientes normas:

- RID 500 para el Administrador
- RID 501 para el Invitado
- RID 1000 para la primera cuenta creada
- RID 1001 para la segunda, ....
- .....
- .....

Una herramienta parecida a éstas es GetAcct,



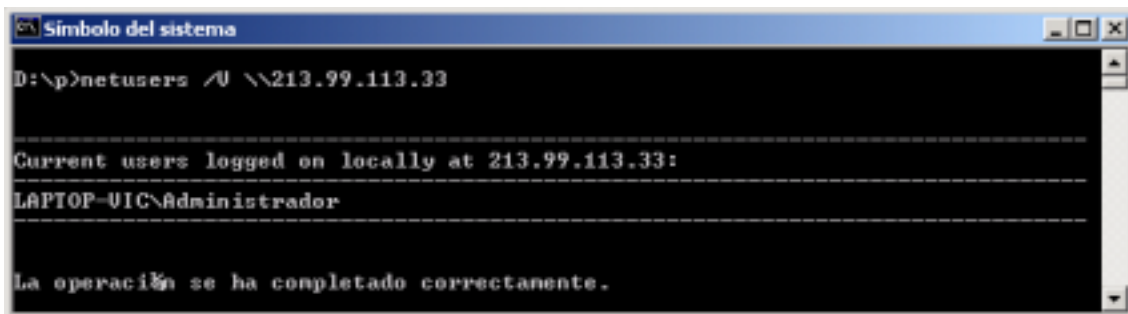
*DumpSec* es otra herramienta que hace más que auditar usuarios, *DumpSec* puede mostrar Grupos, Recursos Compartidos, Políticas de contraseñas, registro, etc. Bastará que en el menú *Reports-Select Computer* se le indique el equipo destino para luego “sacar” la información deseada.



Otra herramienta, cuanto menos curiosa, es netusers.

Mediante netusers podrás comprobar los usuarios que están conectados actualmente a una máquina remota o local.

Puede que necesites efectuar una sesión nula con el objetivo para que funcione.



Para finalizar con la enumeración de usuarios voy a presentarte un programa especial, se trata de Hyena, casi podría dedicar un capítulo íntegro para ésta aplicación, puede descubrir usuarios, recursos compartidos, dominios, etc. en realidad puede sustituir a la consola de usuarios de active directory, es una GRAN HERRAMIENTA.

