TALLER DE GANANDO ACCESO

CURSO FASES DE UN ATAQUE.

NIVEL BASICO

Después de la fase de footprinting donde se sacó la información básica e inicial del objetivo nos queda la siguiente información:

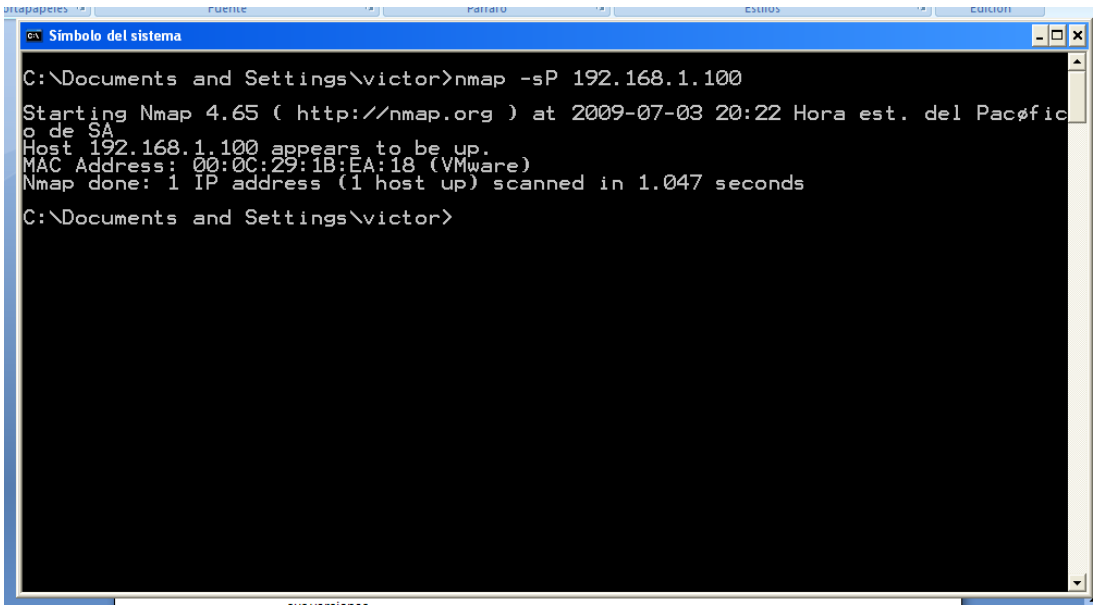
Red intranet, local que alberga una pagina web con servicios a usuarios.

Servidor intranet Dirección IP 192.168.1.100

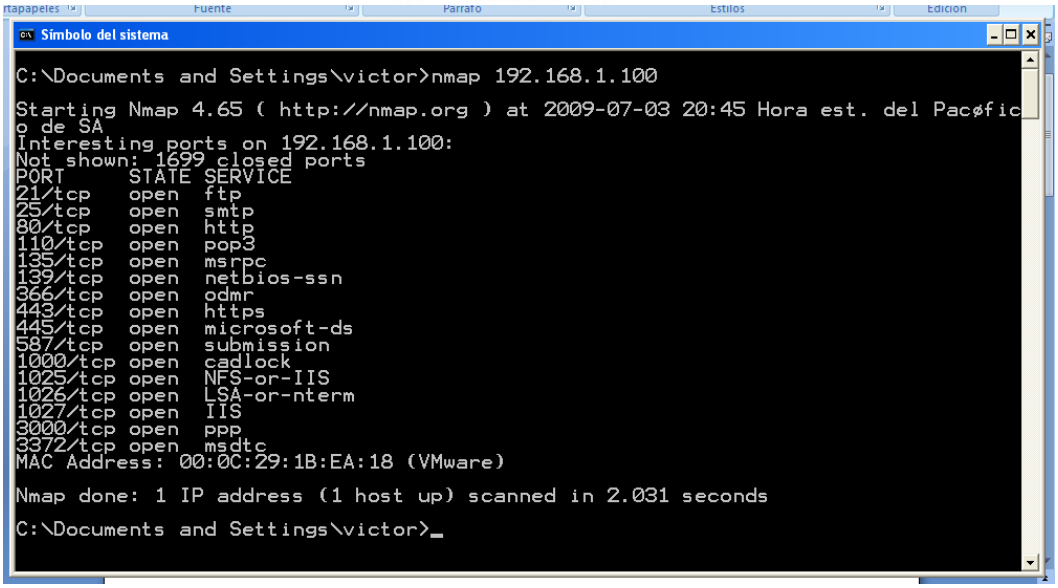
Usuarios posibles para acceso al portal: caludia lucia lopez, carlos alvarez, jose chaguendo. Con sus datos como celulares y cargos lo que nos da info suficiente para luego ver si esta relacionada con claves o perfiles en el servidor y asi poder escalar privilegios.

FASE DE SCANING

1. Nmap de rastreo de MAC y de la Ip para saber que el sistema o host este vivo. Seria el siguiente comando nmap –sP 192.168.1.100

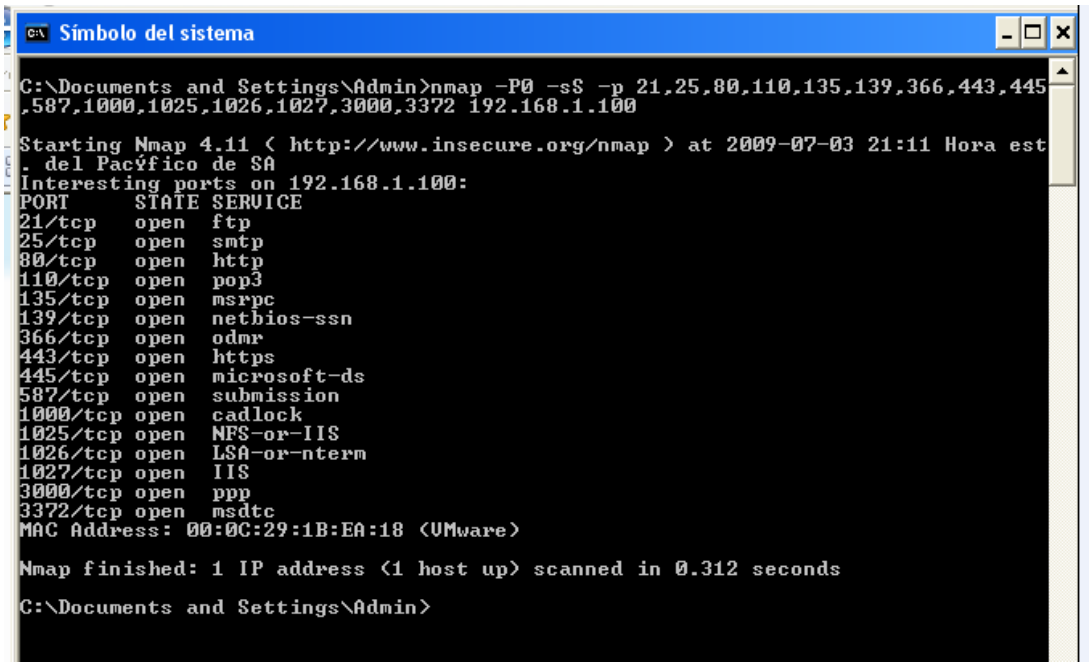


2. Hacer un mapeo de los puertos del host objetivo. Nmap 192.168.1.100

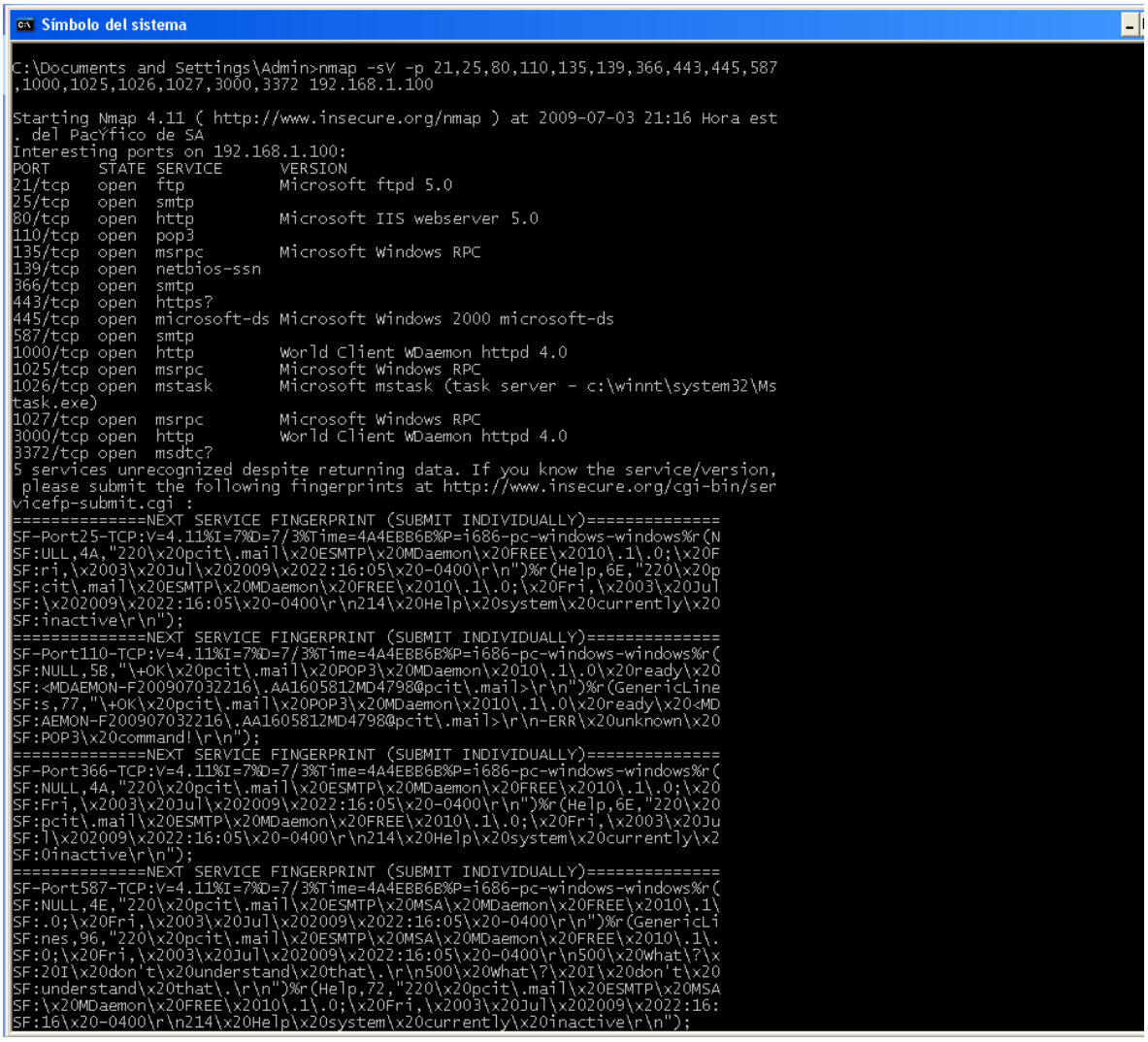


3. Hacer ya un mapeo silencioso, con la herramienta nmap también, esto me daría los servicios que se están ejecutando en los puertos que están en escucha, es con el comando:

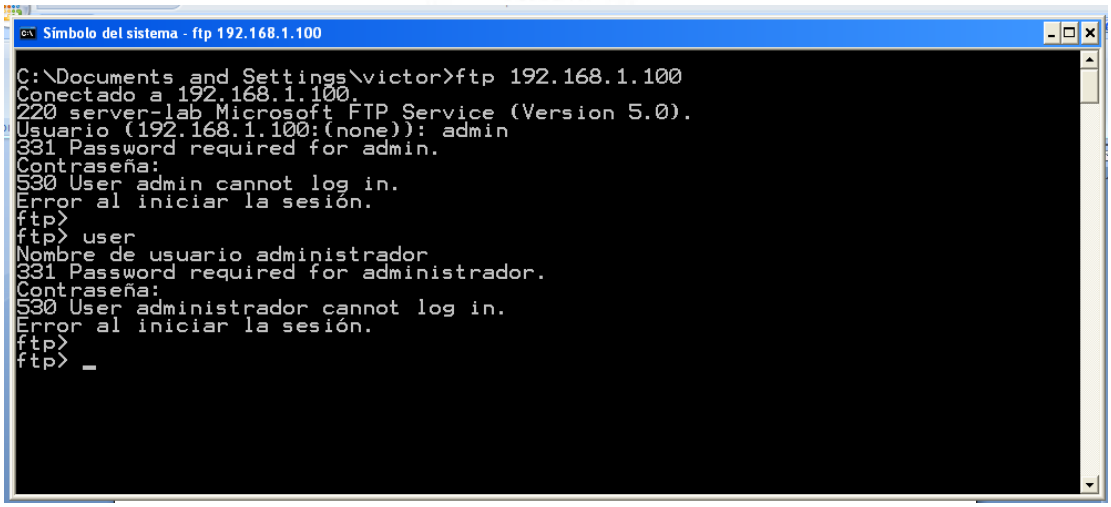
   nmap –P0 -sS –p 21,25,80,135,139,443,445,1000,1025,1026,3372 192.168.1.100



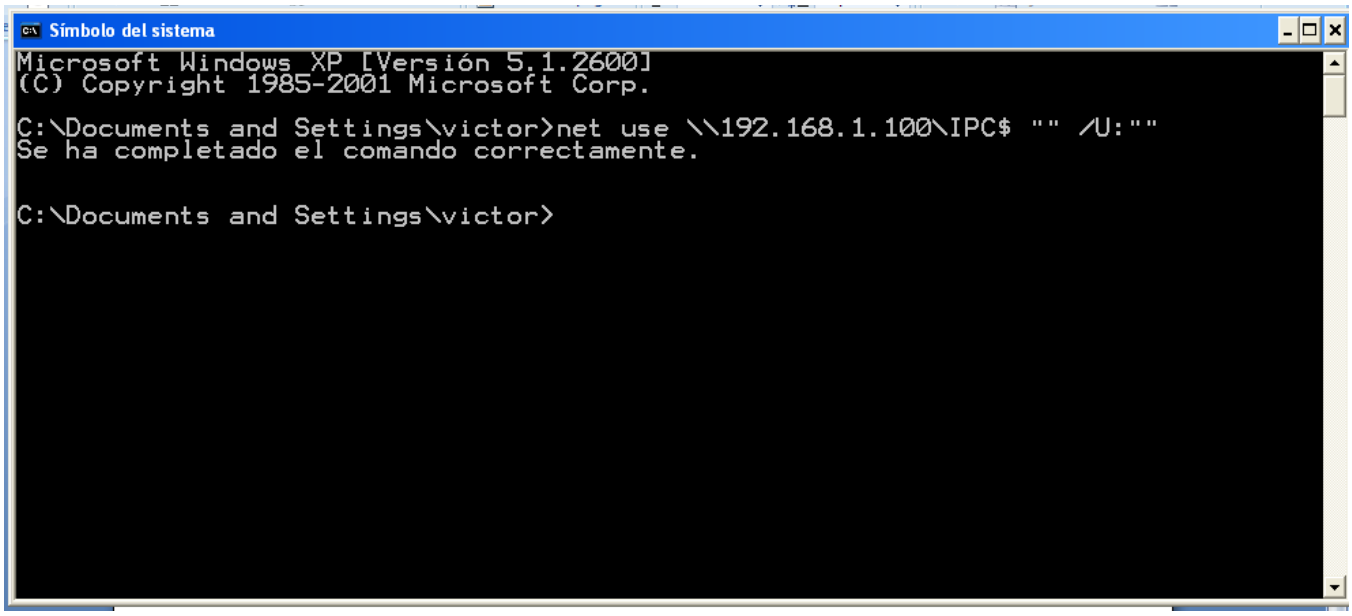
4. El paso siguiente seria buscar las versiones de los servicios, o sea hacer un fingerptint del objetivo. Seria con : nmap –sV –p ,25,80,135,139,443,445,1000,1025,1026,3372 192.168.1.100



4. Después es comenzar a hacer intentos de conexión con los puertos del objetivo, para ver de que manera nos responde y el comportamiento de los mismos ya que podríamos estar ante un HONEY POT. Los procesos de acceso los hacemos con comandos de consola sencillos como: telnet, ftp, ssh y demás comandos dependiendo como digo de los servicios que estén arriba y sus versiones.

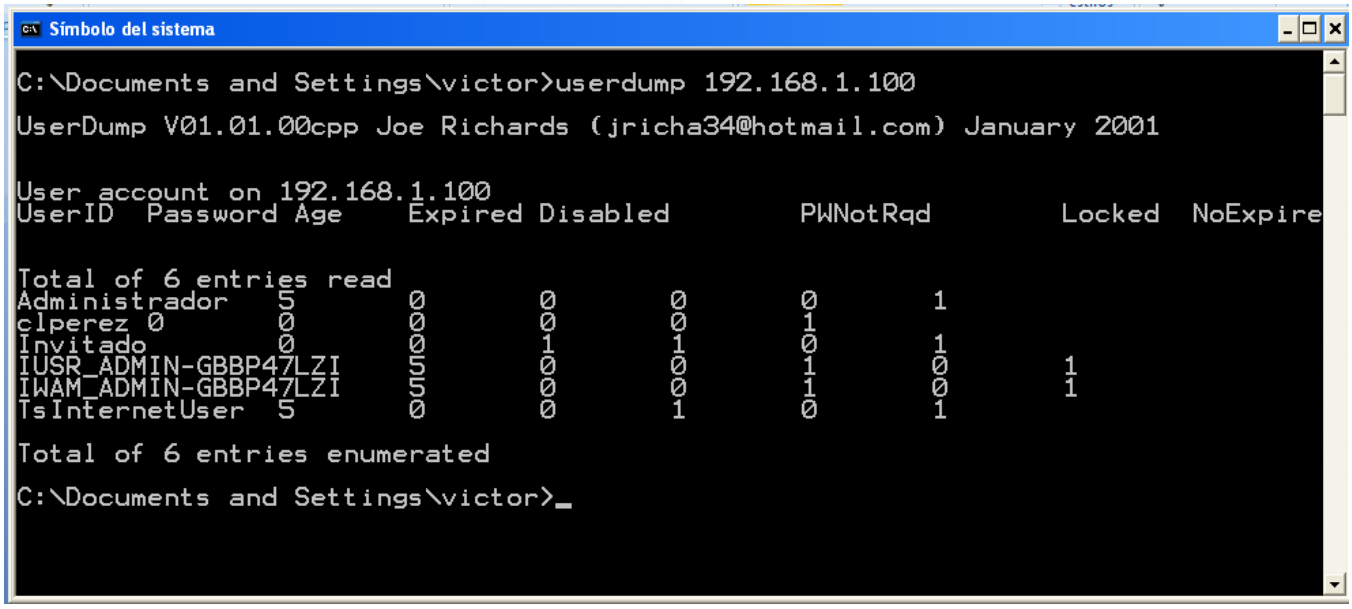


O tratar de entrar con sesión nula al Win2K



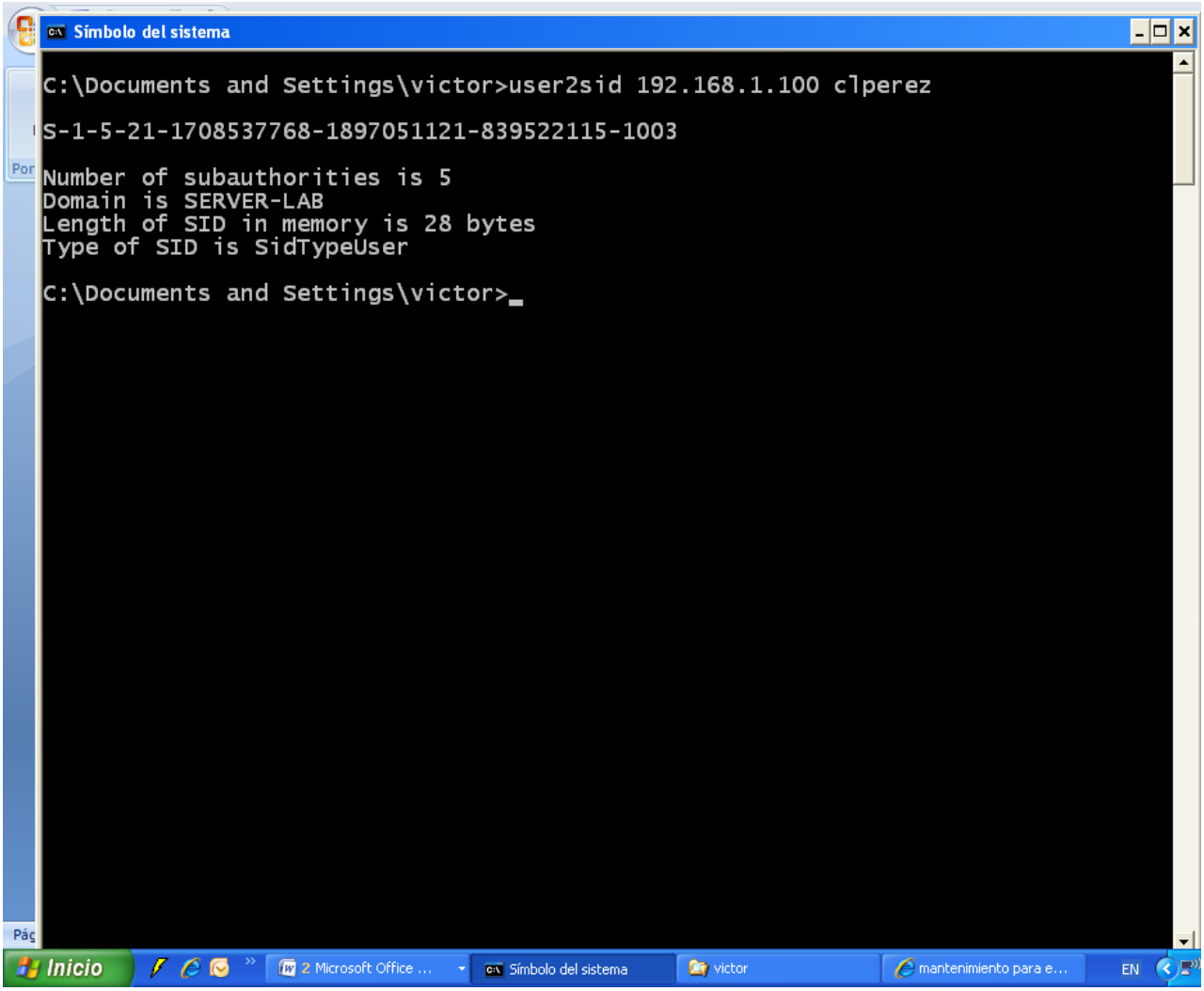
Luego se puede enumerar posibles usuarios que tenga el sistema según la lista de usuarios que tenemos recolectados de la página web.

Herramienta USERDUMP: USERDUMP 192.168.1.100 usuario

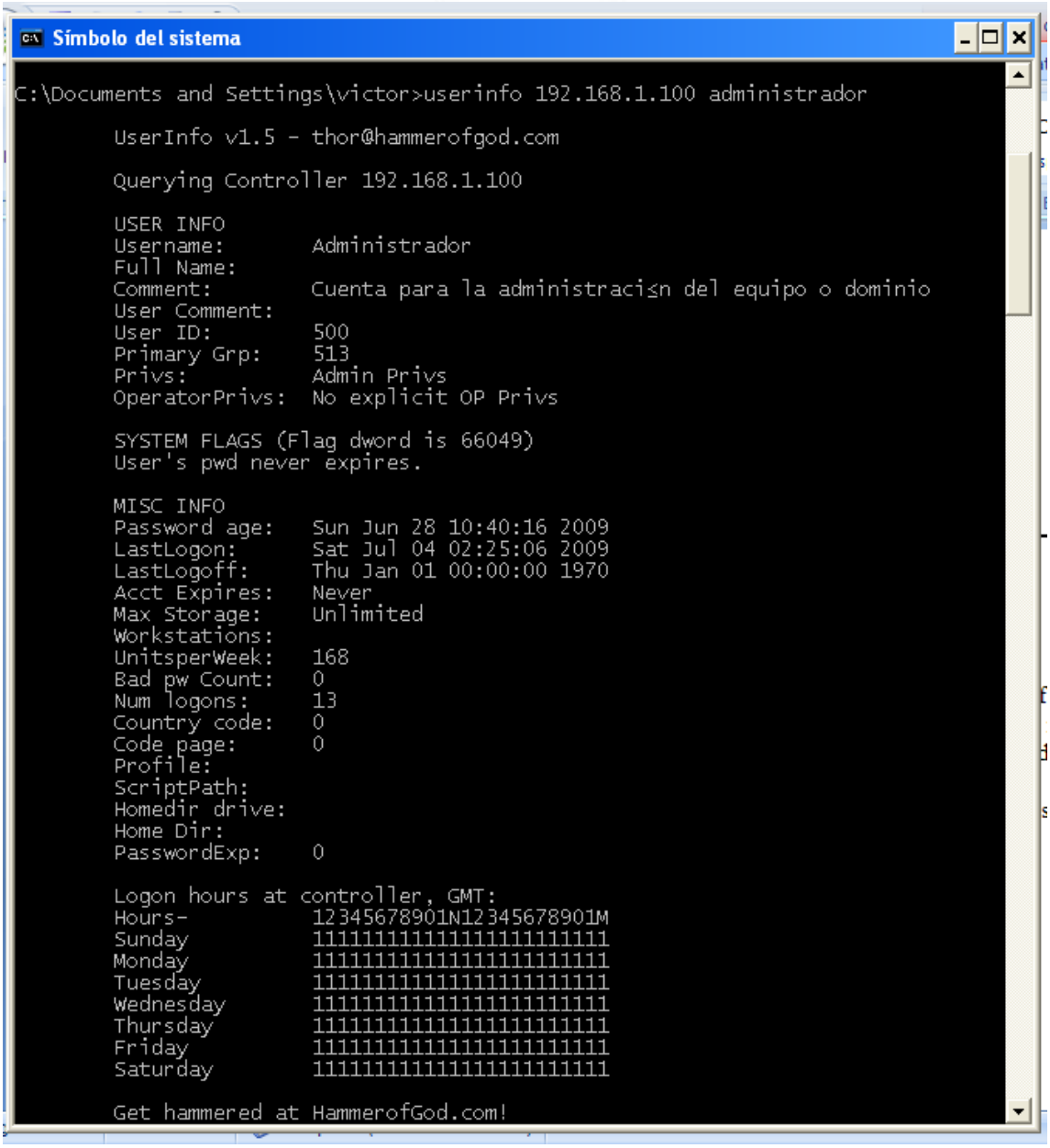


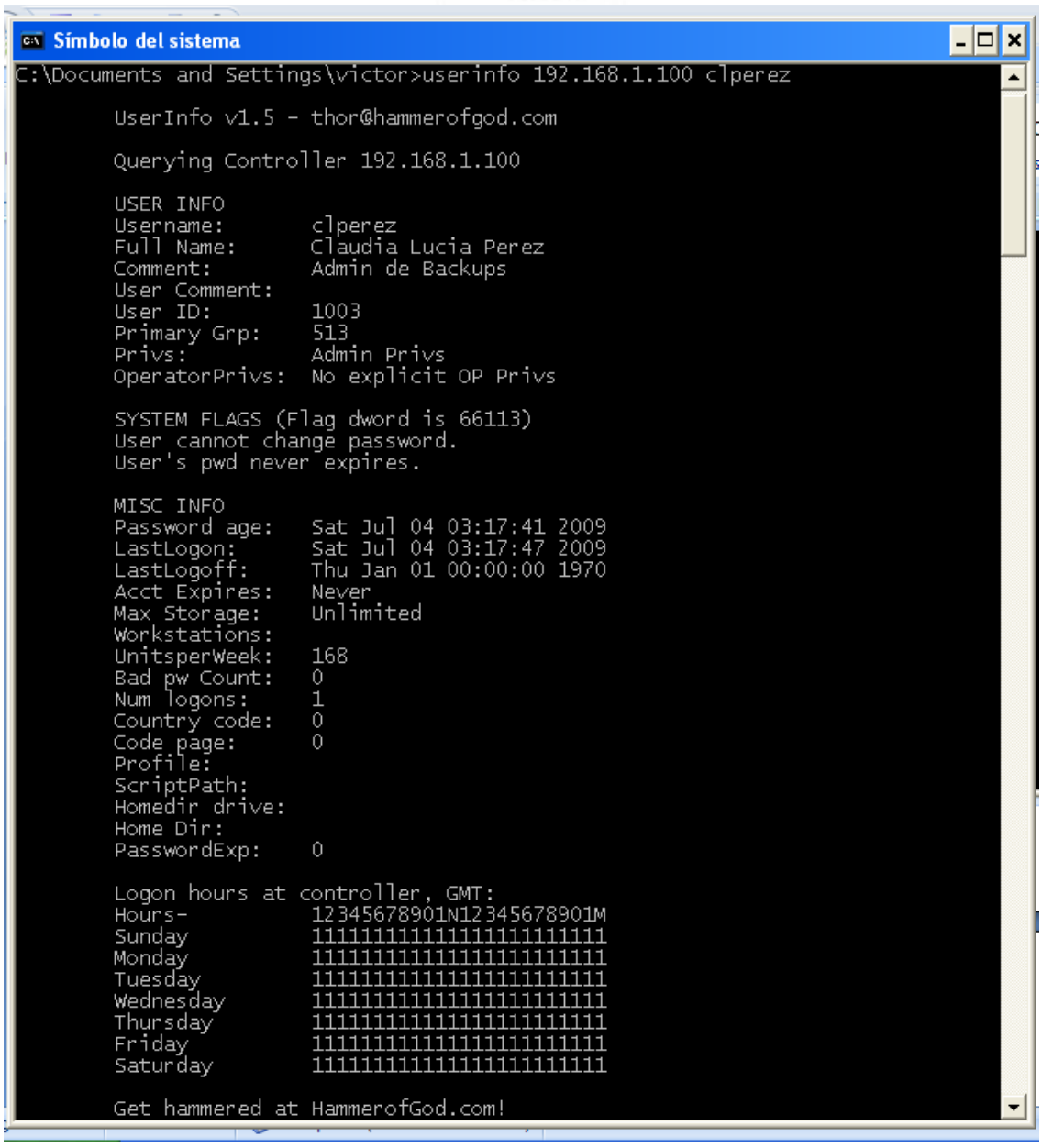
Userdump y la dirección ip sencilla me daría la lista sin mucho problema.

Luego puedo reconocer o enumerar la SID del usuario que deseo ver en este caso lo haremos con clperez para saber si es un usuario administrador también.



después debo sacar la info de cada usuario con la herramienta userinfo la dir ip y el nombre del usuario.

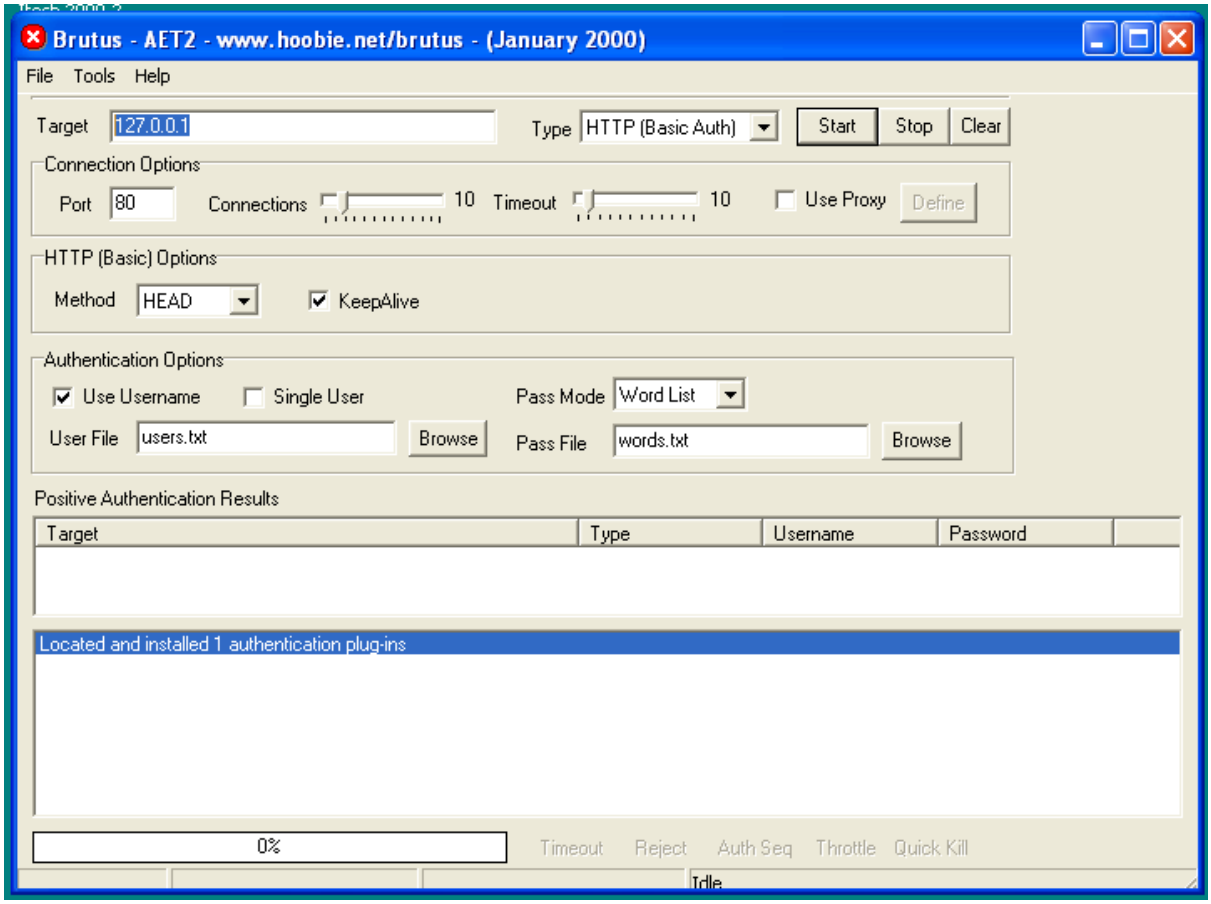

Símbolo del sistema
C:\Documents and Settings\victor>userinfo 192.168.1.100 administrador
UserInfo v1.5 - thor@hammerofgod.com
Querying Controller 192.168.1.100
USER INFO
Username: Administrador
Full Name:
Comment: Cuenta para la administraci≤n del equipo o dominio
User Comment:
User ID: 500
Primary Grp: 513
Privs: Admin Privs
OperatorPrivs: No explicit OP Privs
SYSTEM FLAGS (Flag dword is 66049)
User's pwd never expires.
MISC INFO
Password age: Sun Jun 28 10:40:16 2009
LastLogon: Sat Jul 04 02:25:06 2009
LastLogoff: Thu Jan 01 00:00:00 1970
Acct Expires: Never
Max Storage: Unlimited
Workstations:
UnitsperWeek: 168
Bad pw Count: 0
Num logons: 13
Country code: 0
Code page: 0
Profile:
ScriptPath:
Homedir drive:
Home Dir:
PasswordExp: 0
Logon hours at controller, GMT:
Hours- 12345678901N12345678901M
Sunday 111111111111111111111111
Monday 111111111111111111111111
Tuesday 111111111111111111111111
Wednesday 111111111111111111111111
Thursday 111111111111111111111111
Friday 111111111111111111111111
Saturday 111111111111111111111111
Get hammered at HammerofGod.com!



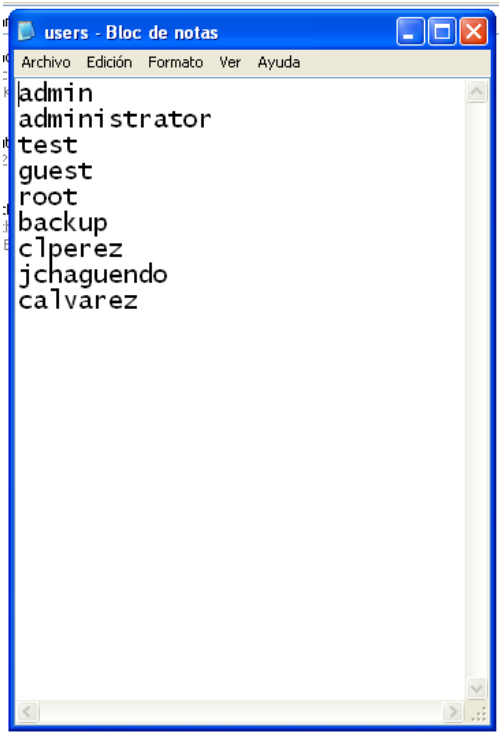
Después de tener los usuarios del sistema con la info básica de ellos tendríamos que pasar a enumerar o realizar rompimiento de claves con herramientas de fuerza bruta. Dichas herramientas pueden ser John de ripper o con brutus, y de una vez usar los directorios de palabras que creamos cuando se hizo el footprinting o los que uno pueda conseguir en internet.

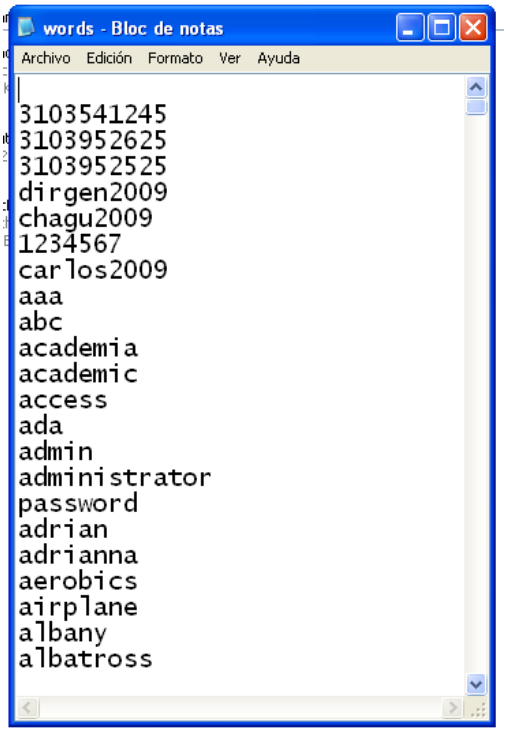
Usaremos BRUTUS para este caso.

Abrimos la herramienta BRUTUS

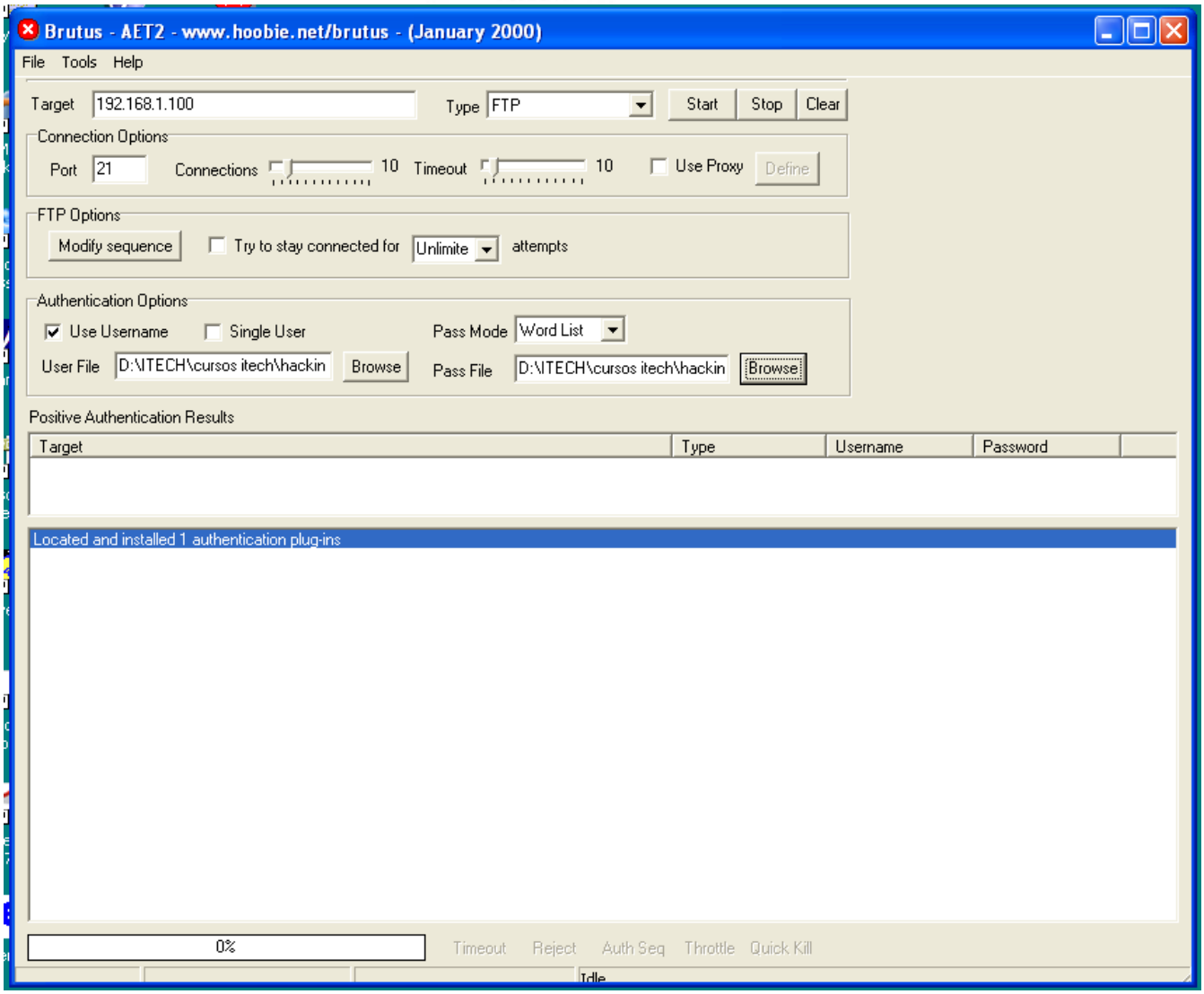


Se debe colocar los usuarios que descubrimos según userdump en el archivo de users.txt y las posibles palabras que creemos que sea las claves, como números de tel. cargos, fechas, combinaciones del c=nombre etc.

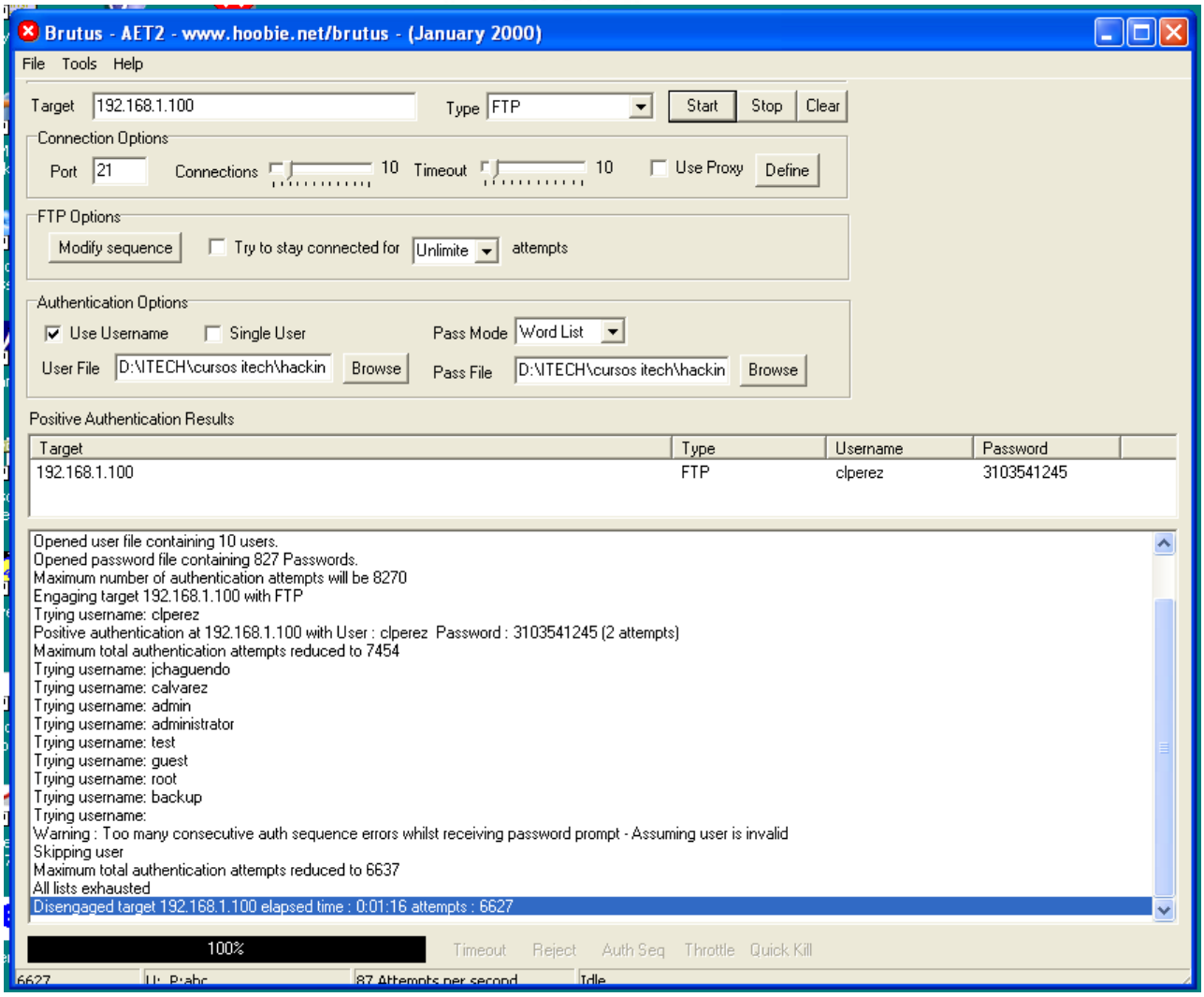




Luego se digitan los datos necesarios para que brutus haga el brute forcé crack password.

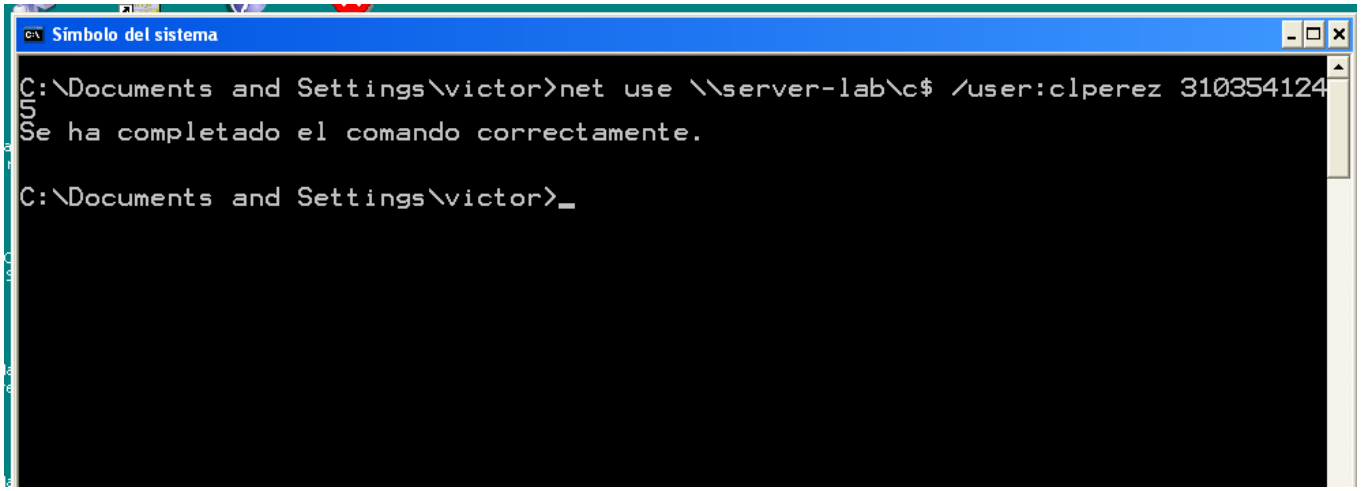


después le damos start y el sistema debe romper contraseñas según los datos de los archivos de directorios.

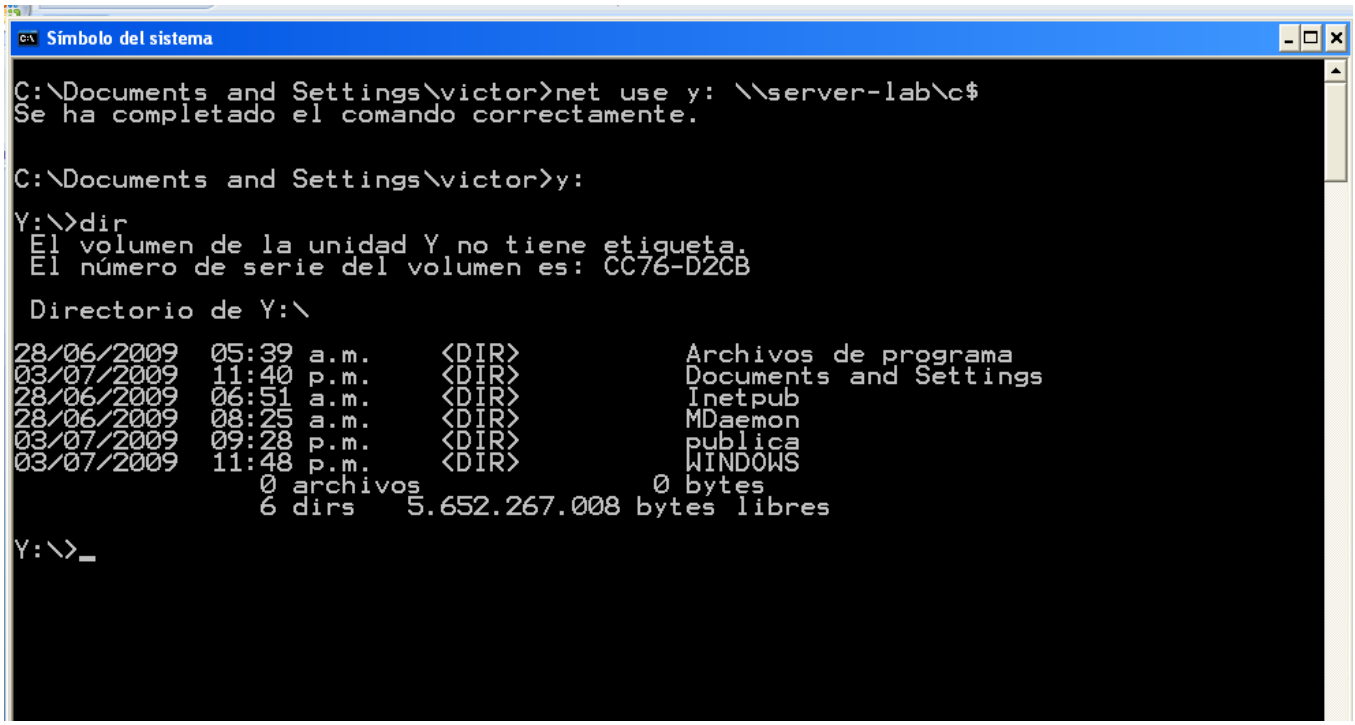


Aquí vemos que ha detectado el password del user clperez, con ese usuario podemos ingresar al sistema y tratar de escalar privilegios en el sistema.

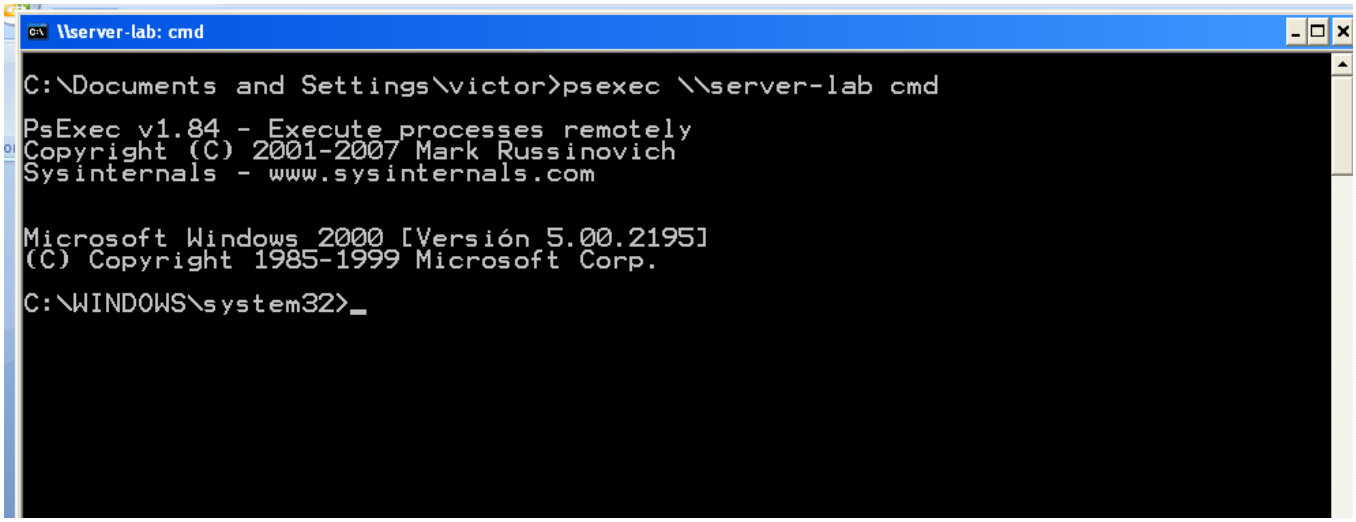
Lo haremos con el comando net use.



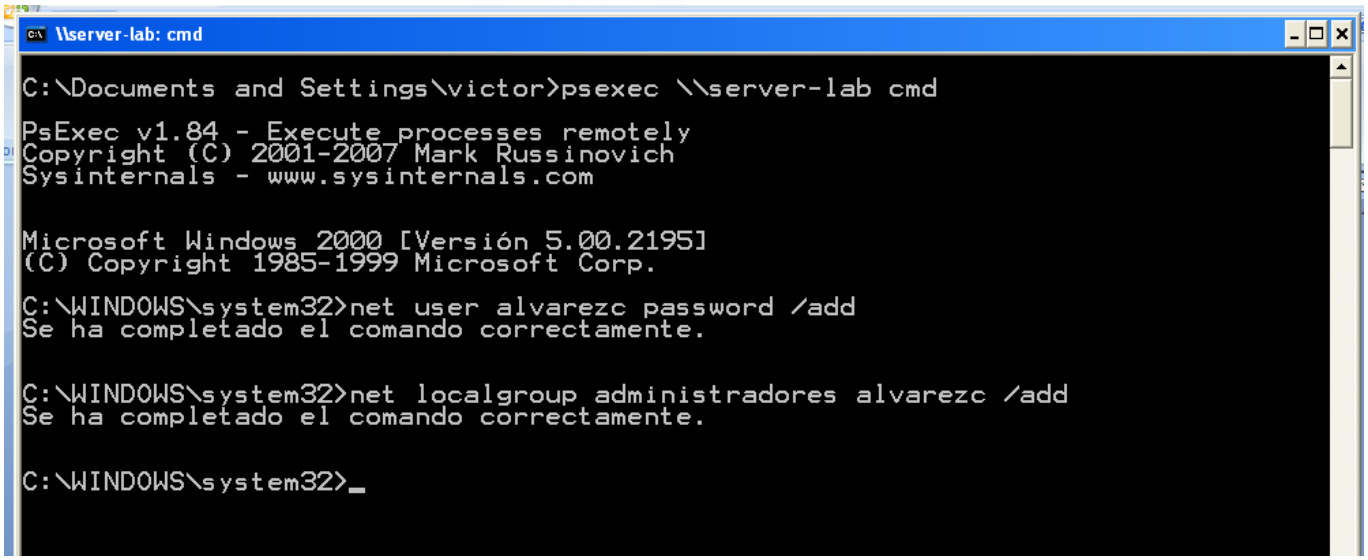
Luego debo asegurar la conexión creando una unidad mapeada para no crear sospechas.



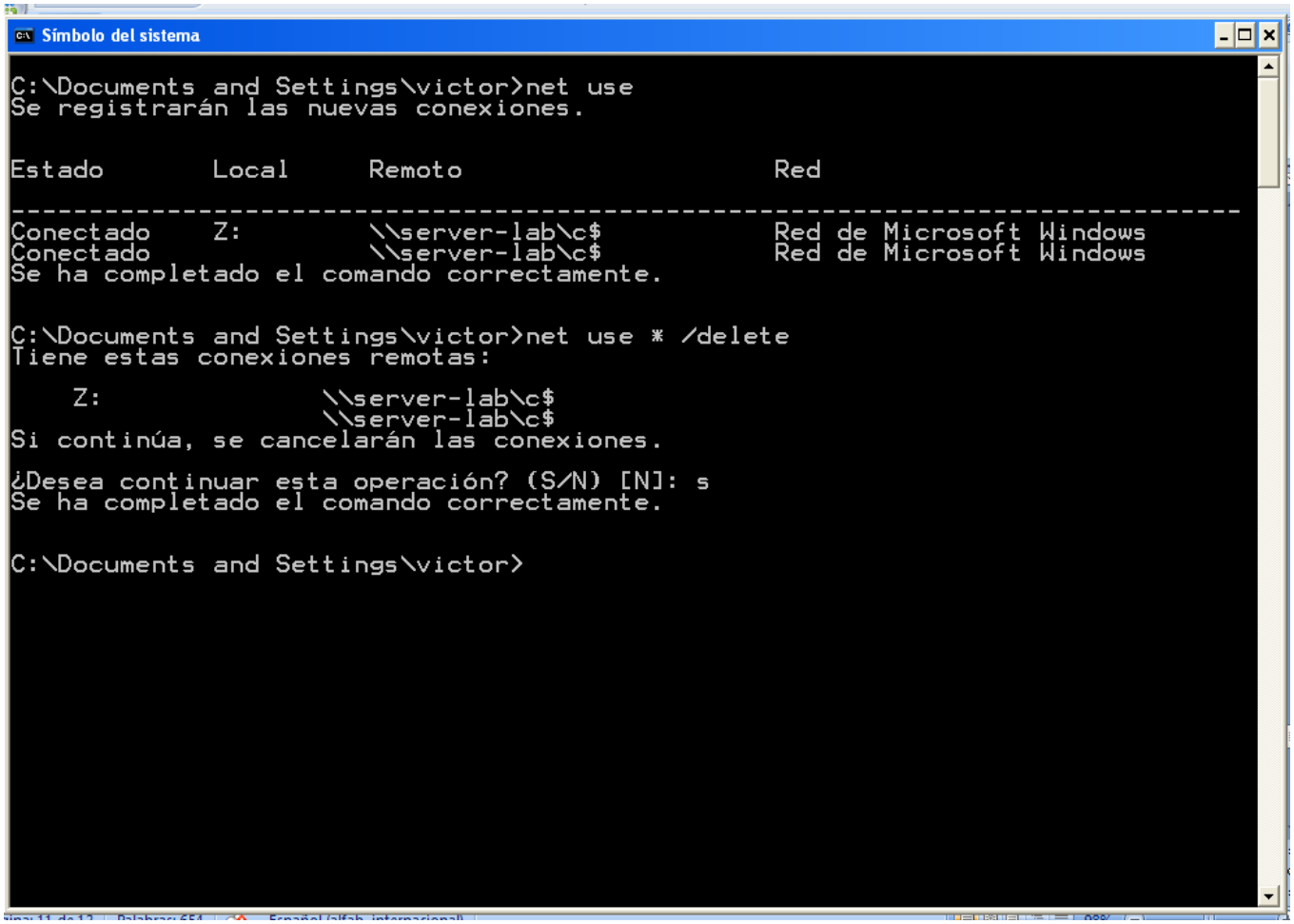
El paso siguiente es remotamente crear un ambiente de trabajo sostenido lo haremos con el comando psexec que nos permite ejecutar comandos remotos.



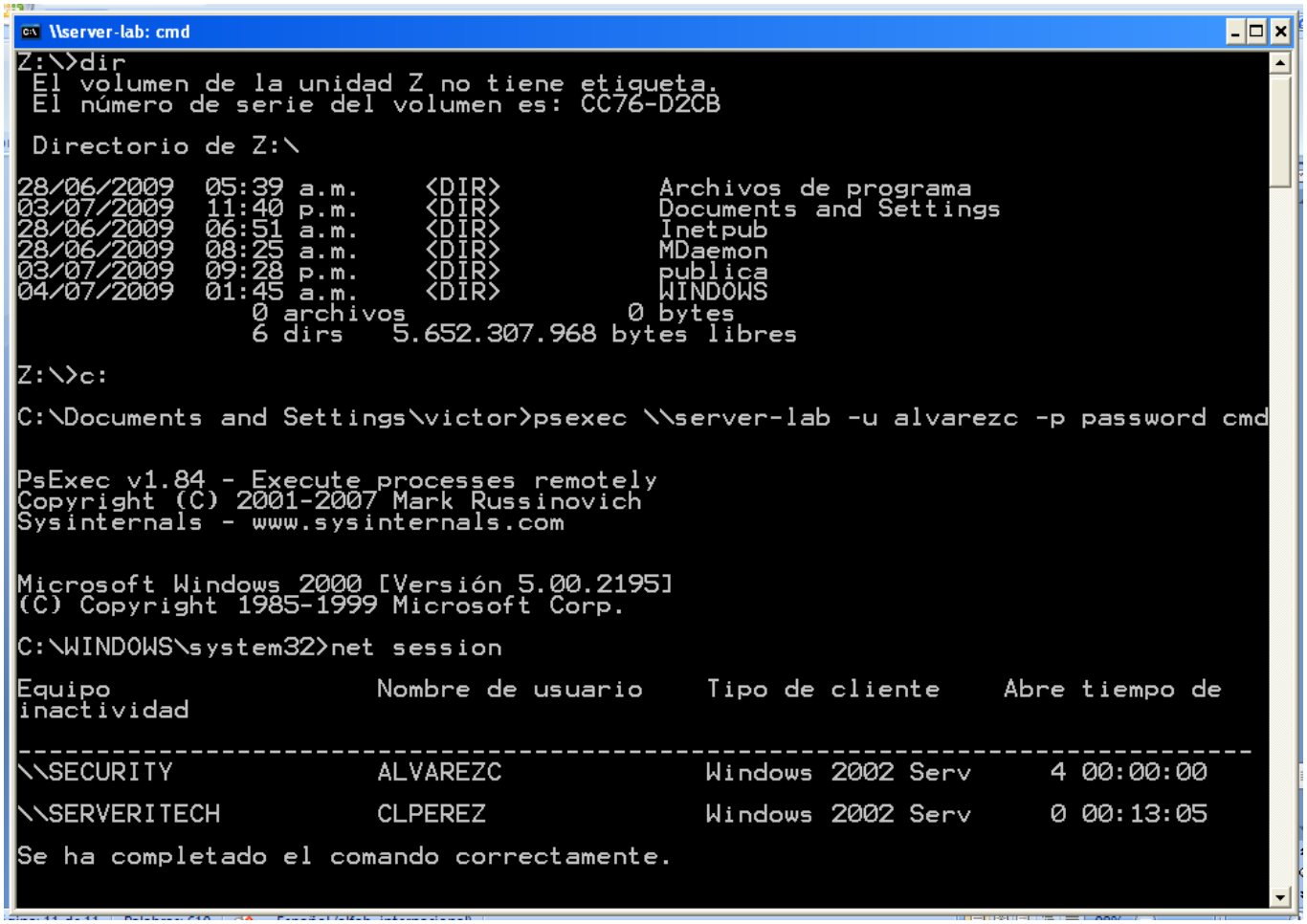
Después debemos escalar privilegios creando un usuario nuevo con privilegios altos o de administrador, lo haremos con el comando net user y net localgroup.



Debo para ir terminando cerrar todas las conexiones



Finalmente para realizar el acceso nos logueamos con este nuevo usuario para pasar desapercibidos. Nos logueamos en el acceso que determinamos para penetrar. O sea penetrar con privilegios.



después de este paso donde ya me loguee con el usuario creado con privilegios de administración y mapear nuevamente una unidad para poder accesar el sistema con este usuario, de ahí para adelante el equipo es nuestro.