

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Son muchos los hilos del foro que buscan ¿Cómo conseguir la contraseña del administrador en W2K/XP?, por ello este documento.

Lo primero que hay que resaltar es que no hay “trucos mágicos” ni utilidades del tipo damela.exe, conseguirlo, en casi todas las ocasiones es una tarea que exige paciencia.

Antes de nada voy a enumerar algunos de los métodos para conseguirlo:

- ?? Ingeniería Social. Ya sabes, “*lo de echarle rostro a la vida y que te la den...*”
- ?? Robando la SAM y crackeandola después
- ?? Asaltando “por la fuerza” a los recursos compartidos
- ?? Utilizando Keyloggers o similares que “registren” las pulsaciones del teclado
- ?? Utilizando Sniffers o similares que “escuchen” lo que pasa por el cable de red
- ?? Utilizando exploits, bug y demás que nos permitan añadirnos al grupo de administradores o la todopoderosa cuenta de System, luego todo lo demás será un juego de niños.

Alguna de estas técnicas necesitan acceso físico al equipo, otras disponer al menos de un usuario y contraseña válidos, también las hay que necesitan acceder al registro o instalar determinados archivos y también las hay de las que no necesitamos nada de esto.

Para todos los ejercicios de esta **FAQ** y siguientes supongo el siguiente escenario:

Estamos en un entorno de Red Interna, aunque muchas de las prácticas pueden hacerse directamente hacia/sobre equipos conectados a Internet.

Tenemos una cuenta de usuario (local o de dominio) sin privilegios administrativos, vamos que sólo podemos hacer lo que nos dejen y no lo que queramos, esto incluye LA IMPOSIBILIDAD DE INSTALAR APLICACIONES que necesiten tocar el registro o tareas que sólo el administrador puede hacer.

Esto es muy importante que lo recuerdes, porque vamos a usar sólo utilidades que “*ya vienen*” con el Sistema Operativo y/o no precisan instalación, basta con llevárnoslas en un disquete y ejecutarlas.

El principal inconveniente de ello, es que la salida de información que nos muestren “*esas herramientas*” puede ser muy cruda, pero **FUNCIONAL**. De otra forma, que no esperes colorines, gráficos vistosos y manejo del ratón. **TODO LO HAREMOS DESDE LA SHELL DEL SISTEMA.**

Averiguar la contraseña de algo o de alguien pasa por conocer primero qué es ese algo y quién ese alguien, así que vamos a estructurar el asunto en las siguientes partes:

- ?? Conocer el entorno que nos rodea
- ?? Identificar los servidores, clientes, servicios y direcciones válidas en la red
- ?? Averiguar los nombres de usuario válidos
- ?? Encontrar los recursos que se comparten en la red (discos, archivos, impresoras..)
- ?? Conocer el estado de Bloqueos de cuentas, auditoría, etc
- ?? Utilizar el mejor método posible para conseguir la contraseña
- ?? Obtener Interactividad con el equipo (si es remoto o no tenemos acceso físico)
- ?? Borrar huellas
- ?? Dejar una puerta trasera para no tener que repetir “todo cada día”

Muchos de vosotros pensareis, pues se coloca un sniffer o un keylog, o se le envía un correo malicioso....y déjate de tantos rollos...

Cierto!! Si lo conseguimos tendremos éxito, pero

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

¿Y si no tenéis acceso físico a la víctima?

¿Y si la víctima no navega por internet o no lee el correo?

¿Y si se tratase del servidor de pruebas HXC sin radmin, sin bugs IIS, etc.?, es broma o ¿no?

Lo que quiero hacer entender es que colocar un keylogger “sin más” puede no ser efectivo por que a lo mejor ni podemos ni encontramos las contraseñas que buscábamos.

Como el tema va para rato, he colgado el documento en Internet, este es el enlace:

Además del PDF, tenéis las utilidades necesarias para seguir los ejemplos, la mayor parte de ellas son gratuitas y de libre distribución, las que no lo son solamente subo las versiones trial o demo, el resto os toca a vosotros.

Esta FAQ cubre sólo el descubrimiento de las contraseña mediante el asalto a los recursos compartidos, el robo de contraseñas con sniffers, keyloggers, etc. dispondrán de una FAQ específica, espero ponerla en los próximos días.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

EXPLORANDO EL ENTORNO

Después de “*pasear*” por el foro, he visto que existen muchos post de gente que no tiene muy claro lo que es iniciar una sesión en una red con dominio o de forma local.

He pensado en aclarar estos términos desde un punto de vista práctico, sin demasiados tecnicismos, con ejemplos y herramientas prácticas, eso sí, para redes Windows y en lo que concierne exclusivamente a los usuarios y contraseñas, repito, podemos llenar páginas y páginas acerca de lo que es un dominio, para lo que sirve, etc. aquí solo trataremos el tema de las contraseñas y nombres de usuario

La teoría:

Aunque se debe diferenciar lo que es una Intranet y una Red Local (LAN), yo voy a utilizar ambos términos como si fuesen la misma cosa, esto va para los puristas ☹

Básicamente podemos encontrarnos en una LAN

Grupo de Trabajo: Las máquinas comparten archivos, impresoras y servicios (como Internet) de igual a igual y cada equipo debe ser administrado de forma individual

Dominio: Como el grupo de trabajo, pero los equipos “necesitan” a otros para determinados servicios (como por ejemplo iniciar una sesión), a estos últimos les llamaremos Controladores de Dominio (PDC)

Los usuarios que utilizan un ordenador que forme parte de un dominio pueden elegir si desean iniciar su sesión de forma local (sin pertenecer al dominio) o como usuarios del dominio, esto normalmente se consigue poniendo el signo @ seguido del nombre del dominio o seleccionado la opción correspondiente en la pantalla de inicio de sesión (inicio de sesión en el equipo local o en el dominio el_que_sea)

El dominio de una red interna no tiene porque existir en Internet, esto es, que si el PDC está configurado de ese modo podemos encontrarnos un dominio como:

micasa.esp
micolegio.kkk, etc.

Los usuarios que pertenezcan a ese tipo de dominios podrían iniciar sus sesiones, con nombres de usuario o login como estos:

[andres@micasa.esp](#)
[alumno111@micolegio.kkk](#)

e incluso pueden tener cuentas de correo, ftp, etc dentro del dominio, obviamente esos usuarios, dominios, etc. no serán accesibles desde Internet,

Aclarando dudas:

Un Windows 2000 Server no tiene por qué ser un PDC

He leído algún post que decía algo así como “....*tengo un dominio porque cuando el ordenador x no está enchufado no tengo acceso a Internet...*”

Bueno, pues eso, no quiere decir que el ordenador x sea un PDC, puede ser un Proxy, un DNS o cualquier otra cosa, es posible que el PDC sea otro, puesto que si no hay PDC ni controladores adicionales de dominio NO SE PUEDE INICAR LA SESION EN EL DOMINIO, imagina que tienes una cuenta de terra para el acceso a internet y el servidor de dominio de terra, ni ningún otro están encendidos, pues no te conectas.

Cuando nos encontramos un W2k Server que no es un PDC se dice que es un Servidor Independiente o Servidor de Miembro.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Los servidores más comunes que nos podemos encontrar en una Red son:

PDC: Controladores principales de dominio, puede haber más de uno, los demás serían secundarios o adicionales

DNS: Resolución de nombres, relaciona nombres con IP's. Es más fácil de recordar Hackxcrack.com que xxx.xxx.xxx.xxx

DHCP: Asigna números IP automáticamente, esto es, que los clientes solicitan al servidor DHCP que les de una dirección IP válida y así evitarnos tener que ir máquina por máquina de la red poniendo una para cada equipo.

PROXY: Para conectar a una red con otra haciendo pasar todas las peticiones y servicios por él.

NAT: Traduce Direcciones IP privadas en direcciones IP públicas, imagina un red con 10 ordenadores (10 ip's) y una única conexión a internet (IP pública), pues NAT lo que hace es traducir las ip privadas junto con los puertos de conexión a la IP pública para salir a Internet, por ejemplo.

RAS: Acceso remoto, Imagina que desde tu casa "te pudieras" conectar a la red interna de tu empresa, colegio, etc. como si estuvieses sentado allí mismo con tu Pc, aunque no es exactamente lo mismo, a ese tipo de redes se les llama VPN (Redes privadas virtuales) y construyen lo que se llama una Extranet.

WINS: Asigna nombres NetBios a direcciones IP, en entornos "puros" de w2k/xp ya no se necesita Wins, vamos que en una red de equipos formados sólo por w2k/xp "esa función" sobra.

IIS: Pues ya sabes, Servicios de Internet, WEB, FTP, etc.

Bueno hay muchos más (correo, noticias, etc) , pero con estos nos sirven de momento, seguro que tienes muchas dudas, ¿Se necesitan todos? ¿Se necesita una ordenador para cada cosa?

Que exista uno o más servidores depende claro está de los servicios que quiera ofrecer nuestra red, si no queremos ofrecer páginas web, pues IIS nos sobra, o si no queremos que la red "salga" a ningún otro sitio, pues pueden sobrar NAT, Proxy, DNS, etc.

¿Cuántos servidores hacen falta?

Pues también depende de muchos factores, dinero, medios, carga de la red, ancho de banda, etc.

Podemos tener tantos servidores como servicios o solamente unos pocos, e incluso podemos tener sólo 1, pero figúrate como iría la cosa si ponemos un único servidor en una red con 1000 usuarios y además tiene que ofrecer "servicios externos" de páginas web, ftp, correo, etc.

Además hay un servicio muy especial que suelen dar los servidores de una red interna a sus usuarios: **DATOS**

Podemos encontrarnos servidores independientes que guardan la información que crean o utilizan sus usuarios en lo que se llama unidades de red, así nos encontraremos, Servidores de Aplicaciones y Bases de Datos (Oracle, SQL....) o simplemente servidores que comparten carpetas o unidades de disco enteras para que los usuarios guarden allí sus documentos de word, excel, imágenes, los exámenes, las notas, las nóminas....

Cuando todos estos servidores y servicios "se integran" y funcionan ofreciendo a sus usuarios todos los recursos disponibles estamos ante una Intranet.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

¿Y todo esto para qué?

Pues porque es fundamental “encontrar” qué es cada cosa para poder atacar sus puntos débiles, ¿de qué serviría el bug del code-unicode aplicado a un servidor que no está corriendo IIS.?

Como averiguar quién es quién

Pues una forma básica es mediante un escaneo de puertos, dime qué puertos usas y te diré quién eres, 80 Servidores WEB, 110 Correo entrante, 25 correo saliente, 53 DNS, etc.

Con los proxys lo tenemos algo más duro, normalmente son el 8080, 1080, pero pueden ser otros.

Aun así nos falta conocer lo fundamental en una red con dominio

¿Quién es o son los PDC?

Lo primero que tenemos que hacer es conocer “nuestro entorno”, así que necesitaremos:

- ?? Averiguar nuestra IP y todo lo que sea posible de nuestra conexión de Red
- ?? Realizar un Barrido ping del entorno próximo
- ?? Escanear puertos de todas o de una determinada máquina
- ?? Detectar los servidores PDC y lo que sea.


Herramientas:

No pienses que son como las Iptools, Languard y demás que has visto en la revista, recuerda que de momento no tenemos privilegios de administrador y no podemos instalar “ese tipo de software”

- ?? Ipscan
- ?? Ipconfig (Sistema Operativo)
- ?? Nbtstat (Sistema Operativo)
- ?? Nltest (Kit de Recursos)
- ?? Networkscanner
- ?? Nbtscan

Lo primero conocer nuestra IP, abrimos una shell y:

Ipconfig /all



```
Símbolo del sistema
Nombre del host . . . . . : laptop-vic
Sufijo DNS principal . . . . . : 
Tipo de nodo . . . . . : Difusión
Enrutamiento de IP habilitado . . . . . : No
Proxy de WINS habilitado . . . . . : No

Ethernet adaptador Conexión de área local 2:

Sufijo DNS específico de la conexión. : 
Descripción . . . . . : Fast Ethernet CardBus PC Card
Dirección física. . . . . : 00-10-60-5C-6B-13
DHCP habilitado . . . . . : No
Dirección IP. . . . . : 172.28.0.9
Máscara de subred . . . . . : 255.255.0.0
Puerta de enlace predeterminada . . . . . : 172.28.0.2
Servidores DNS . . . . . : 172.28.0.98

D:\np>
```

Encontramos el nombre netbios, si usamos o no DHCP, Wins, DNS, etc.

Una primera aproximación: Muchos servidores PDC de redes internas (pequeñas) suelen ser además los servidores DNS, por tanto la dirección 172.28.0.98 podría ser el PDC y DNS.

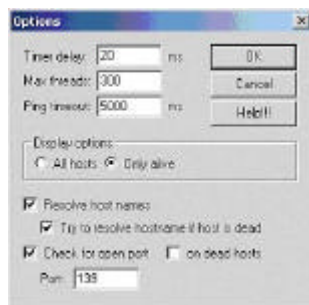
Lo realmente importante de esta pantalla es la ip, en el ejemplo 172.28.0.9, luego el siguiente paso será efectuar un barrido ping de las direcciones próximas para “ver” que equipos responden

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Podemos usar la orden ping del sistema operativo, pero eso vale para una sólo máquina o podemos repetirla para unas cuantas, pero para 1000 Ufff!!!

Bueno en una red local, será más fácil desde el entorno de Red, lo que ocurre es que sólo nos mostrará sus nombres NetBios o la descripción del equipo (que no tiene por qué coincidir con el nombre NetBios), así que vamos a usar IPScan, es malo, muy malo, pero será suficiente

Lo ejecutamos y en el menú de options, seleccionamos options y ponemos los valores como éstos:



Pulsamos OK y ahora seleccionamos el rango de IP's a escanear, ya voy a escanear todo el rango 172.28.x.x, así que tardará un poquito, por eso la casilla max threads la he subido de valor, es el número de “procesos” simultáneos que usará ipscan para el escaneo

En el puerto he puesto el 139, es NetBios, podríamos usar cualquier otro, IPScan sólo escanea un puerto por cada vez, no es un escaneador de puertos, pero es muy rápido para identificar Hosts “vivos”

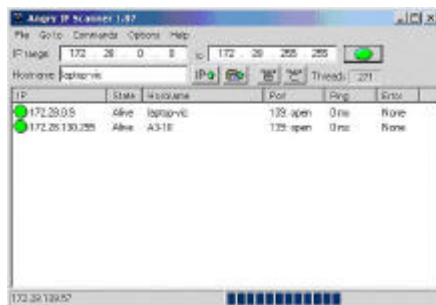
Mientras termina el barrido, os diré algo acerca de ping, en internet es posible que un host “este vivo” y no responda a peticiones ping.

Ping se basa en un protocolo llamado ICMP y muchos Firewalls y Routers filtran y/o rechazan las peticiones echo del protocolo ICMP que usa ping, en una LAN será menos frecuente que esto ocurra.

Si quieres prueba a mandar un ping a www.arsys.es y verás que no responde, sin embargo puedes acceder a la web desde el Explorador web, esto se debe a lo que he dicho antes, realmente podemos usar otras técnicas que lo engañen, pero esa es otra guerra....

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Bueno ya habrá terminado, he puesto una dirección muy alejada para que veas lo importante que son los barridos IP.



Una vez que tenemos las direcciones IP de nuestro entorno, podemos averiguar más información de esas máquinas,

Nbtstat -A 172.28.130.255

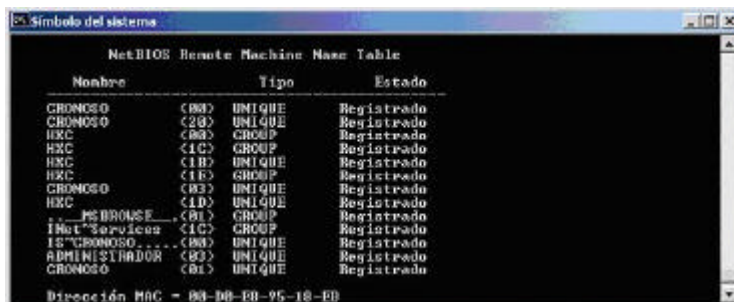


La columna izquierda pertenece al nombre Netbios y lo que me interesa que conozcas de aquí son los dígitos <XX> que aparecen a su derecha, simplificando:

<00> Estación de trabajo
<20> Servidor
<1C> PDC

Hay más, muchas más, pero estas son las que necesitamos para identificar algunas máquinas.

No te confundas <20> son servicios de servidor, no que sea un PDC, fíjate en la siguiente pantalla, se ha hecho contra el servidor de pruebas de HXC, luego comentamos



Aparece dos veces <1C> con nombres netbios HXC y InetServices, esto indicará que HXC probablemente sea el PDC del Dominio y el otro corresponde al Servidor IIS, es decir, que “nuestros amigos” tienen un PDC que además es Servidor Web.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Otras entradas que pueden ser interesantes son:

<01> y <03> Mensajería (máquina CRONOSO)
<1B> Explorador principal de Dominio
<06> Servidor RAS (en este caso no lo es)

Hay más, seguro que en google encuentras más información.

Como ves una forma de identificar si un equipo es un PDC es comprobar si en la salida de nbtstat -A aparece la “etiqueta” <1C>

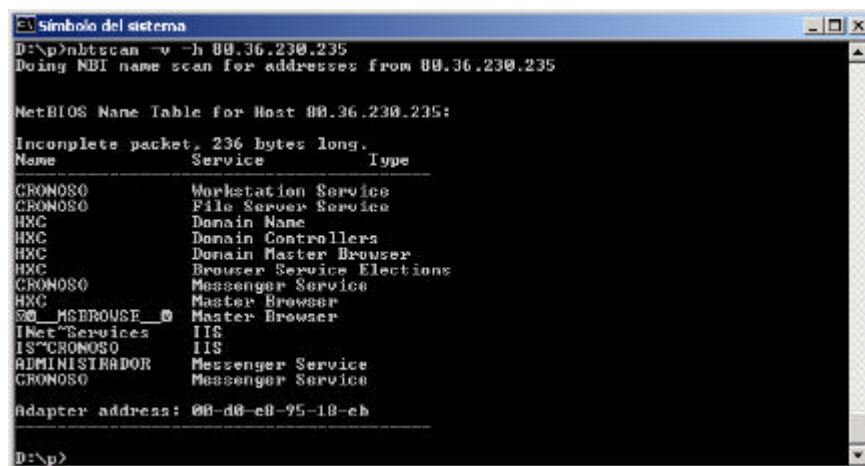
Pero para eso hay una herramienta mejor, del Kit de Recursos y se llama nltest,

Simplemente escribes **nltest /dclist:dominio** y se mostrarán los Controladores principales y adicionales si existen, claro que para que funcione debemos pertenecer al Dominio, por ejemplo si formásemos parte del dominio academia, la sintaxis sería:

Nltest /dclist:academia

Una herramienta alternativa a nbtstat, es nbtscan, la salida es más simple:

Nbtscan -v -h 80.36.230.235



```
Símbolo del sistema
D:\np>nbtscan -v -h 80.36.230.235
Doing NBT name scan for addresses from 80.36.230.235

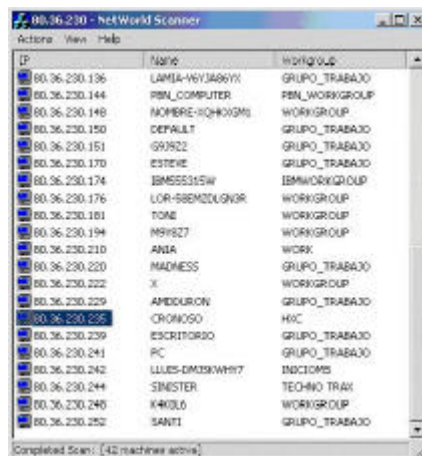
NetBIOS Name Table for Host 80.36.230.235:
Incomplete packet, 236 bytes long.
Name          Service      Type
-----
CROMOSO       Workstation Service
CROMOSO       File Server Service
HXC           Domain Name
HXC           Domain Controllers
HXC           Domain Master Browser
HXC           Browser Service Elections
CROMOSO       Messenger Service
HXC           Master Browser
00_MSEBROUSE_0 Master Browser
INet Services IIS
IS~CROMOSO    IIS
ADMINISTRADOR Messenger Service
CROMOSO       Messenger Service

Adapter address: 08-d0-e0-95-10-e0

D:\np>
```


FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Otra herramienta muy rápida que nos muestra los nombres netbios y grupos o dominios, ips, etc es network scanner



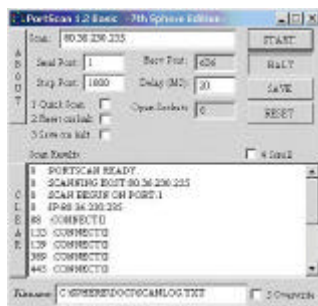
Observa “*nuestro server de prácticas*” como se muestra resaltado.

Bueno, ya sabes las hay mucho mejores, pero para lo que se trataba nos vale, ahora ya sabemos identificar un PDC de otro que no lo es.

La último que nos falta para terminar esta sección es escanear puertos para determinar los servicios que corren, volvemos a lo de siempre, necesitamos utilidades que no precisen instalación nada de SSS, ni de Languard ni nada de eso.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Una muy simple es PortScan, será suficiente, vamos a escanear los puertos de nuestro server,



En stop port he puesto 1000 porque nuestro server tiene más puertos abiertos que cuartos de baño Isabel Presley ¿por qué será? Y para variar observa que el 80 no está abierto, vamos que no funciona lo del bug de IIS porque no está corriendo el servidor web.

Hasta aquí con el conocimiento del entrono, ahora te toca a ti, practica explora “otras redes” “otras ips” y vete recogiendo dudas para que entre todos podamos resolverlas.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

IDENTIFICAR USUARIOS Y RECURSOS

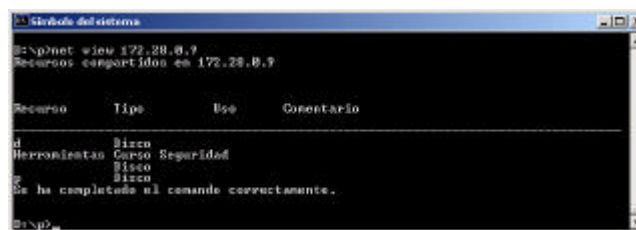
Aunque parezca una perogrullada es igual de importante conocer el nombre de los usuarios como sus contraseñas, de nada sirve lo uno sin lo otro, si además queremos acceder a un recurso (archivo, carpeta, impresora) pues también será importante saber Qué comparte nuestro “amigo”

Empecemos con los recursos compartidos.

Herramienta Net view del Sistema Operativo

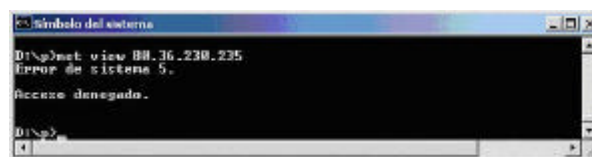
Probamos con nuestra propia ip:

Net view 172.28.0.9



La tentación nos hace probarlo con el server de prácticas:

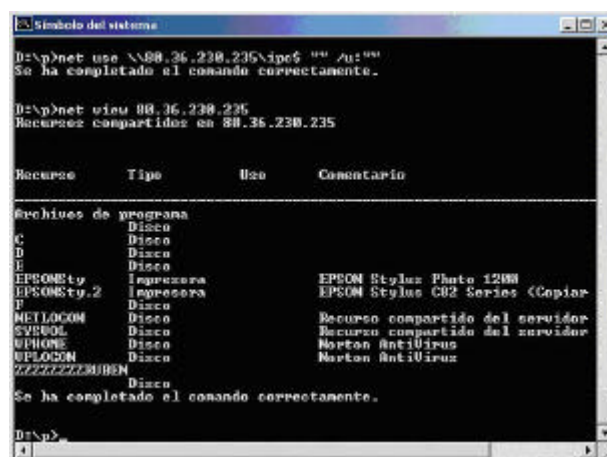
Net view 80.36.230.235



¿Te lo esperabas? No podemos, todavía....

Establecemos una sesión nula, esto es conectarse de forma anónima a un recurso especial que se llama IPC\$ que usan los windows para la comunicación interna entre procesos y después volvemos a ejecutar net view

Sesión nula: **net use \\80.36.230.235\ipc\$ "" /u:""**



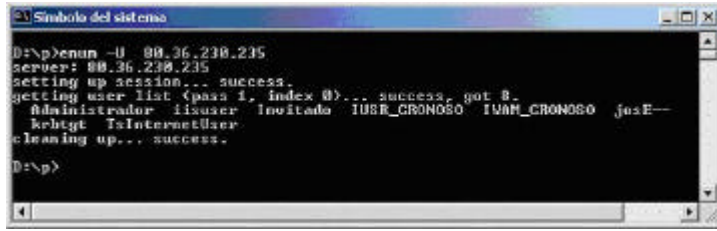
Ahora ya conocemos los recursos disponibles, vamos a por los usuarios

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Para los usuarios vamos a utilizar `enum`, `userdump`, `userinfo`, `user2sid` y `getacct`

Cualquiera de éstas nos serán suficientes, cada una nos lo muestra “a su manera”,

Enum –U 80.36.230.235, nos mostrará los usuarios de 80.36.230.235



Enum, por sí solo, ya establece la sesión nula y después la cierra, gran cosa por que si se nos olvida cerrarla, si el equipo remoto apaga, le saldrá ese cartelito de que Hay 1 usuario conectado y bla, bla, bla, por lo que se nos pueden mosquear.

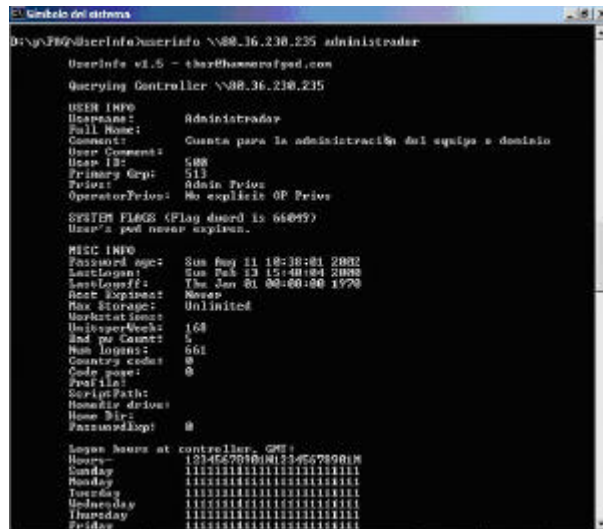
Si a enum le damos los prámetros $-S -P$, nos mostrará los recursos compartidos y políticas de seguridad de contraseñas, ¿A qué esperas?

Enum –P –S –U 80.36.230.235

Para conocer más acerca de algún usuario podemos usar Userinfo, pero primero asegúrate de haber establecido una sesión nula con el objetivo , sino no funcionará.

```
net use \\80.36.230.235\ipc$ "" /u:""
```

Userinfo \\80.36.230.235 Administrador



No está mal, ahora conocemos hasta el número de veces que se han logeado, si la password expira o no, las horas de inicio de sesión permitidas, etc, etc.

Userdump funciona de forma muy similar, se le da el nombre de la cuenta de invitado y un valor numérico y volcará la misma información que antes pero para cada usuario, por ejemplo:

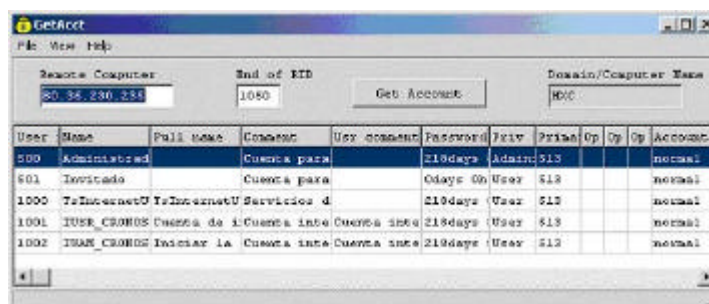
Userdump [\80.36.230.235](#) **Invitado** Esto mostrará la información de la cuenta del administrador y de los primeros 5 usuarios que encuentre, userdump funciona así, recuerda que si el idioma del server es inglés debes poner guest en lugar de invitado, si es ruso (ni idea)

La salida de userdump no la pongo por lo extensa que es, PRUEBALA TU

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

En XP tenemos un problema, los inicios de red con conexiones anónimas no están disponibles por defecto, aun así pruébalo, de todos modos lo que nos interesa son las cuentas de un Server, cuando las consigamos ya nos ocuparemos de XP, aunque bueno hay otras maneras, pero va a ser algo extenso explicar los SID-RID, etc. de momento sigamos con esto

Para los que queráis una salida “con ventanitas” usad **getacct** como se muestra a continuación:



FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

BUSCANDO EL MEJOR METODO PARA AVERERIGUAR LA CONTRASEÑA

Esto es realmente difícil de elegir, dependiendo de las situaciones podemos usar unos u otros, así que voy a exponerlos con sus ejemplos y prácticas y luego tu eliges

Desde el punto de vista de los usuarios y contraseñas, que es lo que nos ocupa aquí, vamos a ver que ventajas tiene usar un dominio o no,

Supongamos un colegio con 200 alumnos (100 por la mañana y 100 por la tarde), 5 clases de informática y 20 ordenadores por clase.

Si quisiéramos tener una cuenta para cada alumno, como es lógico debemos crearnos 200 puesto que es el número de alumnos totales, pero...

Si quisiéramos que cualquier alumno pudiese iniciar su sesión en cualquier ordenador de cualquier clase

En una red sin dominio, se deben crear:

200 cuentas x 5 clases x 20 Pc's = 20.000 cuentas de usuarios locales

En una red con un dominio, se deben crear:

200 cuentas de usuarios del dominio en el PDC

Por tanto ya tenemos la primera diferencia:

Las cuentas y contraseñas locales se almacenan en cada ordenador

Las cuentas y contraseñas de usuarios de un dominio se almacenan en el PDC

Si averiguamos una contraseña de un usuario local, ésta no tiene por qué ser la misma que en el dominio y viceversa

Las contraseñas locales se guardan en la SAM, que suponiendo que el directorio de instalación de Windows fuese Winnt, el archivo SAM estaría en:

Winnt\system32\config\SAM

Los Controladores de dominio guardan los datos de la cuenta del usuario en:

\\winnt\ntds\ntds.dit

Ambos archivos son “intocables” mientras windows se esté ejecutando así que lo más probable es que no nos podamos llevar la SAM a casa, por otra parte W2K/XP utilizan un método de seguridad llamado SYSKEY que fortalece la SAM y no permite descifrar las contraseñas con facilidad.

Vamos a establecer tres métodos:

- 1º) Ataque por diccionario a los recursos compartidos
- 2º) Instalación de un keylogger
- 3º) Instalación de un snifer que escuche el protocolo SMB

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Ataques por Dicionario

Aunque pueden darse en Internet, la lentitud del proceso puede desesperar a más de uno, aproximadamente 4 a 10 palabras por segundo, pongamos 5 como ejemplo,

Al minuto.... 300, A la hora....18.000

Además si la contraseña no figura en nuestro diccionario pues no lo conseguiremos, claro. Aun así en una Red local merece la pena intentarlo, allí la velocidad puede ser de 1000 palabras por segundo más o menos, con lo que con un buen diccionario en la mano si le dedicamos un par de horas podríamos chequear unos TRES MILLONES de posibilidades, no está mal.

Si lo probamos en el equipo local la velocidad se multiplica considerablemente, por lo que aunque existe la posibilidad cierta que la contraseña que buscamos no esté en el diccionario, intentarlo no está de más, las contraseñas simples, como perro, salchichón, manolo, etc. son fáciles de descubrir.

Además en Siempre tenemos la posibilidad de la fuerza bruta, esto es, probar y probar combinaciones de letras, números y signos, la tarea es larga pero se conseguirá, al menos en el equipo local para descubrir la contraseña del administrador local, una vez conseguido ésta, instalar keyloggers, sniffers y otras herramientas más potentes será sencillo.

Los ejemplos que siguen a continuación utilizan un diccionario de nombres comunes (unos 5000) entre los que se supone está la contraseña del equipo, vamos a usar: **Enum y SmbCrack**

Sintaxis de Enum

Enum -D -u administrador -f d.txt 172.28.0.9

172.28.0.9 es el equipo a craquear y d.txt debe ser el diccionario de palabras

Después de muuuuuchas salidas erróneas la ejecución de enum se detendrá cuando encuentre el pass

```
> Inicializo el sistema
(660) administrador | hracs
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(667) administrador | hredy
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(668) administrador | hrucs
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(669) administrador | cade
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(670) administrador | cadcs
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(671) administrador | cain
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(672) administrador | carp
password 132$, Error de inicio de sesión: nombre de usuario desconocido o contraseña incorrecta.
(673) administrador | ceclisa
password found: ceclisa
```

SMBcrack funciona de forma muy similar, pero más rápido

SMBCrack 172.28.0.9 administrador d.txt



```
Símbolo del sistema
SMB Cracker -Prototype for Fluxay 5, by netKeyes 2002

Processing Words: 574/5627
Found! administrator's password is cecilia

D:\>
```

Tanto enum como smbcrack realizan previamente una sesión nula con el objetivo