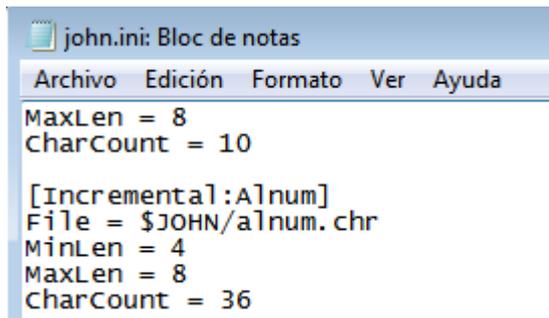


¡Muy buenas a todos!

Soy Rolo y voy a proceder a explicar como completar el concurso 1 de **HDC**.

Como bien imagináis todos lo primero que hay que hacer es descargárselo: <https://mega.co.nz/#!t883SYJS!FFL7jrAIBhHh14pqC-fBAIbYvQC--WKtB-h26mwO6tQ>

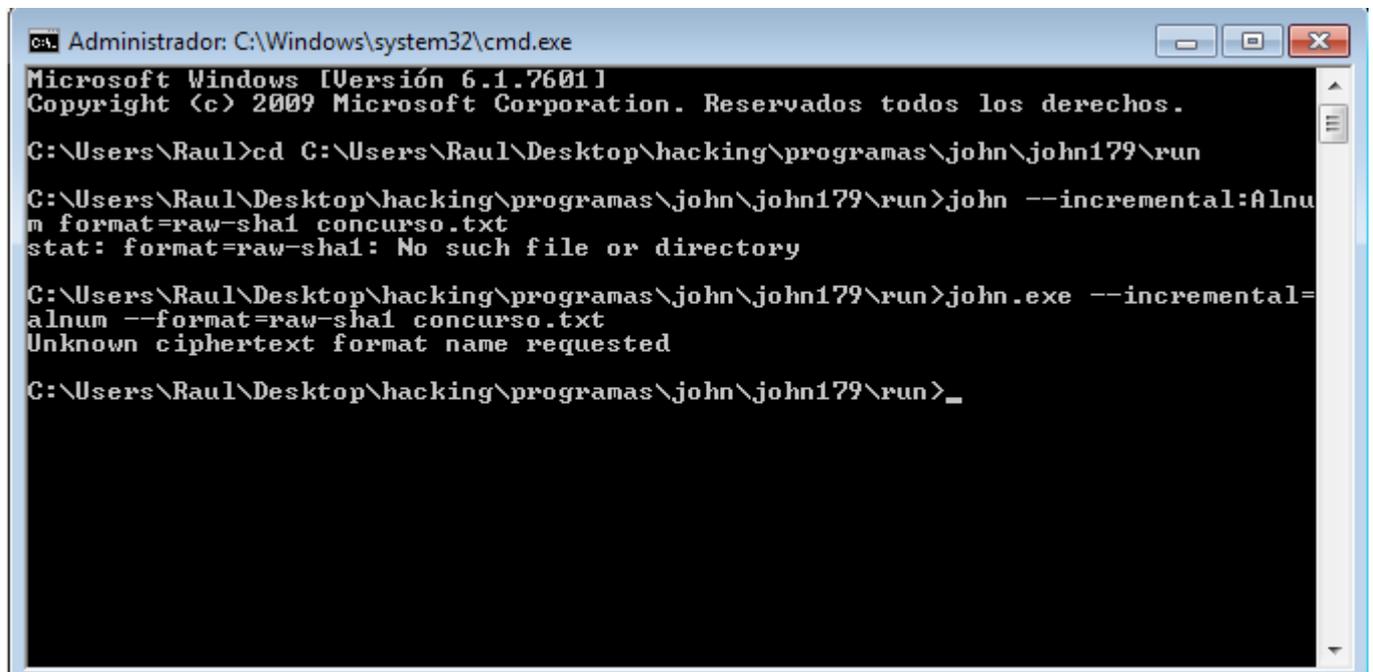
En el zip que te descargas vienen dos archivos, el primero es un archivo con extensión .txt, que dice que la contraseña para abrir el .zip, que viene junto a este archivo, está **cifrada** en **SHA1** y es: **2f6794702b5e8811bce657ec225e95ff6755365a**, también dice que la contraseña tiene entre 4 y 8 caracteres y que solo contiene **números** y letras **minúsculas**.



```
john.ini: Bloc de notas
Archivo Edición Formato Ver Ayuda
MaxLen = 8
CharCount = 10

[Incremental:A]num
File = $JOHN/alnum.chr
MinLen = 4
MaxLen = 8
CharCount = 36
```

Con estos datos ya nos podemos poner manos a la obra, lo primero que se nos pasa por la cabeza es usar a nuestro buen amigo John. **Cambiamos los parámetros de Alnum** y ponemos entre 4 y 8 caracteres, y usamos el comando **“john --incremental:Alnum --format=raw-sha1 concurso.txt”** (previamente tenemos que haber creado un archivo txt llamado concurso.txt donde este escrita la contraseña), cuando estamos dispuestos a descubrir la contraseña nos encontramos esto:



```
ca. Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Raul>cd C:\Users\Raul\Desktop\hacking\programas\john\john179\run

C:\Users\Raul\Desktop\hacking\programas\john\john179\run>john --incremental:Alnum
format=raw-sha1 concurso.txt
stat: format=raw-sha1: No such file or directory

C:\Users\Raul\Desktop\hacking\programas\john\john179\run>john.exe --incremental=
alnum --format=raw-sha1 concurso.txt
Unknown ciphertext format name requested

C:\Users\Raul\Desktop\hacking\programas\john\john179\run>_
```

Esto pasa porque el John que tenemos descargado **no acepta el formato SHA1**, y por eso lo único que tenemos que hacer es descargar el John the Ripper **Jumbo** de esta página web:

<http://www.openwall.com/john/>. Repetimos los mismos pasos y se pondrá manos a la obra para decirnos la contraseña en, aproximadamente, **15 minutos**.

Nos dará la contraseña “**roadd128**”, lo único que tenemos que hacer es extraer el .zip y descargar la siguiente parte que está en el link del archivo de texto.

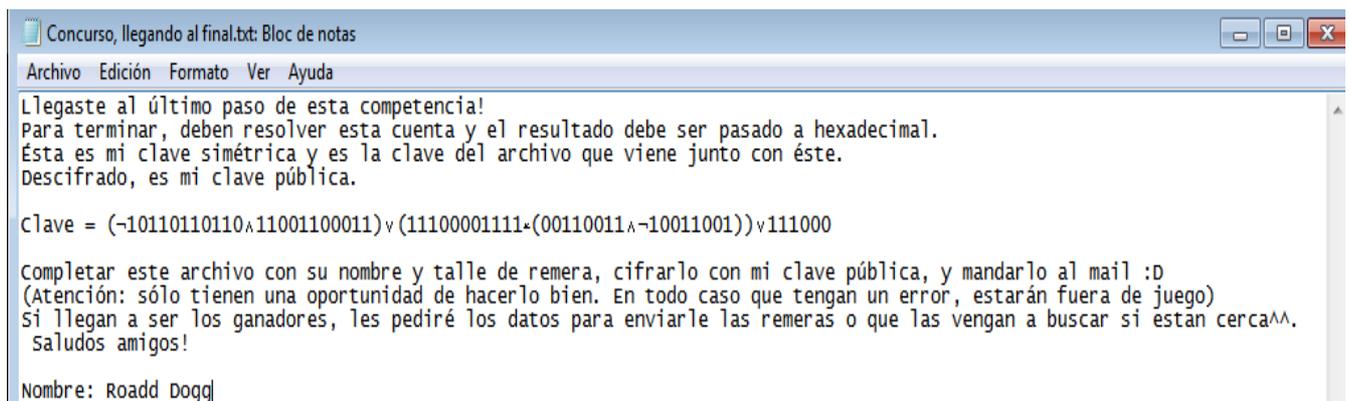
La siguiente parte nos dara nuevamente dos archivos, en el archivo de texto nos dara una contraseña “**mvkgfml**” encriptada bajo **atbash**, lo que hay que hacer es informarse y a lo primero que acude uno en estos casos es a **wikipedia** (no digan que no →). <http://es.wikipedia.org/wiki/Atbash>. En wikipedia hay una tabla comparativa y solo tenemos que darle la vuelta, en wikipedia también nos da este enlace que lo descripta solo

<http://pedrocarrasco.org/projects/criptografia/atbash.php?text=mvkgfml>, como vereis la contraseña descifrada es **Neptuno**.

(edit by Roadd: o pueden hacerlo a mano, vagos xD)

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Ya sólo nos queda abrir el archivo, es una archivo con terminacion .gpg y si no recordáis mal esa es la extensión que dejan los archivos cifrados con **GPA**, solo tenemos que señalar la cuenta que creamos, pulsamos abrir. Le damos al archivo .gpg, pulsamos **Decrypt** y la contraseña **Neptuno**. Ya lo único que nos queda es abrir el archivo de texto y ver el link hacia la última fase.



En la parte final nos dan un archivo sin ninguna terminación y otro .zip. Después de un rato de curiosidad, intenté abrirlo con **Notepad** y ¡voilà!, ahí estaba el procedimiento de la última fase totalmente escrito. Nos dice que la contraseña de la última parte es el resultado **hexadecimal** de unas cuentas de operaciones lógicas. Vosotros podéis hacerlo con algún programa o como queráis, pero yo lo hice a mano.

**01001001001 and 11001100011 = 1001000001**

**00110011 and 01100110 = 100010**

**100010 xor 11100001111 = 11100101101**

**1001000001 or 11100101101 = 11101101101**

**11100101101 or 111000 = 11101111101**

**11101111101 a hexadecimal es 77D**

Ponemos **77D** en el .zip, y ya tenemos la public key. Ya sólo nos queda poner nuestro nombre, cifrar

el archivo y mandarselo a **Roadd**. Yo lo cifré con **AxCript**. Le damos **click derecho en el archivo-> Axcrypt-> Encrypt-> key file y elegimos la public key**.

**Muchas gracias a todos por parar a leerlo y un saludo.**

**Este es un post hecho por Rolo Mijan Titos y retocado por Roadd Dogg.**

**Espero haya gustado:). Comento que los links van a seguir subidos para que los usen siempre que quieran.**