Práctica desencriptación contraseñas Windows/Linux

06/12/2017

Athos Orío Choperena

Contenido

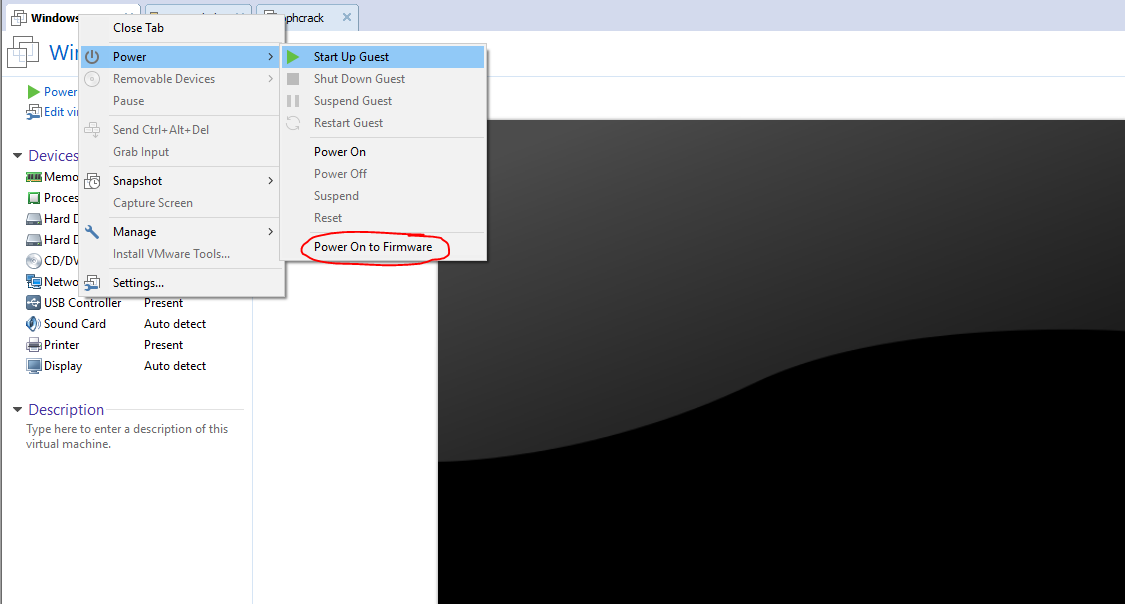
[Desencriptación contraseñas de windows 2](#_Toc500325761)

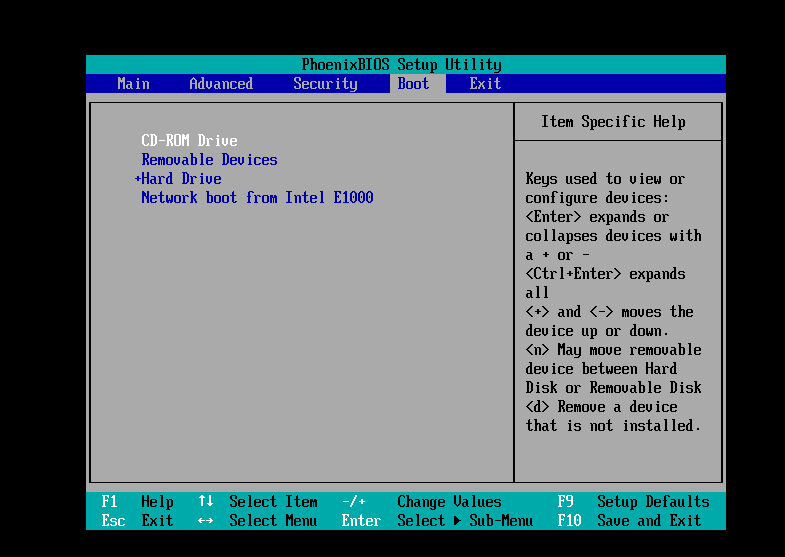
[Des encriptación contraseñas shadow de Linux 5](#_Toc500325762)

[Compilación John: 7](#_Toc500325763)

# Desencriptación contraseñas de windows

Lo primero que vamos a hacer es arrancar cargar la iso de ophcrack en el lector de cd (virtual) de vmware (en la máquina que tiene el windows del cual queremos sacar las contraseñas), tras esto, arrancaremos y nos meteremos en la BIOS para modificar el orden de arranque de los dispositivos disponibles, poniendo como primera opción el lector de cdrom



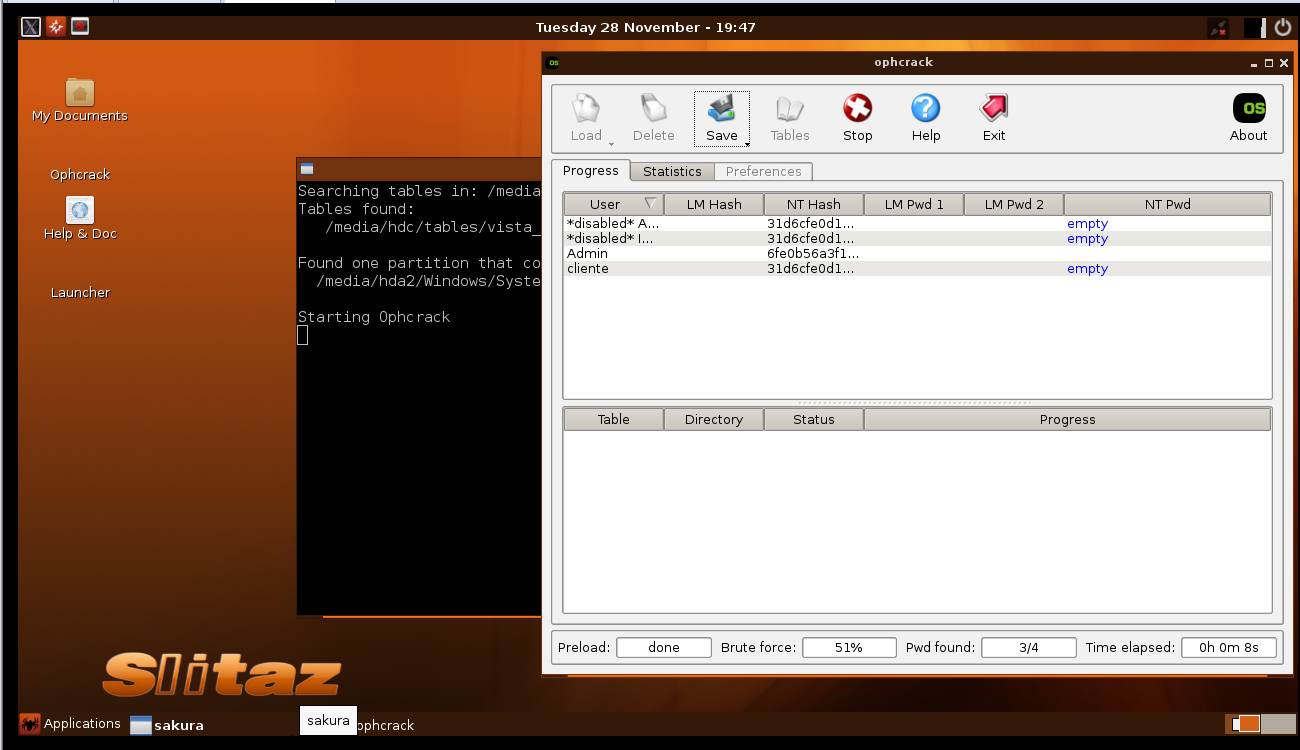


Luego salvaremos y al reiniciar veremos el menú de arranque de ophcrack

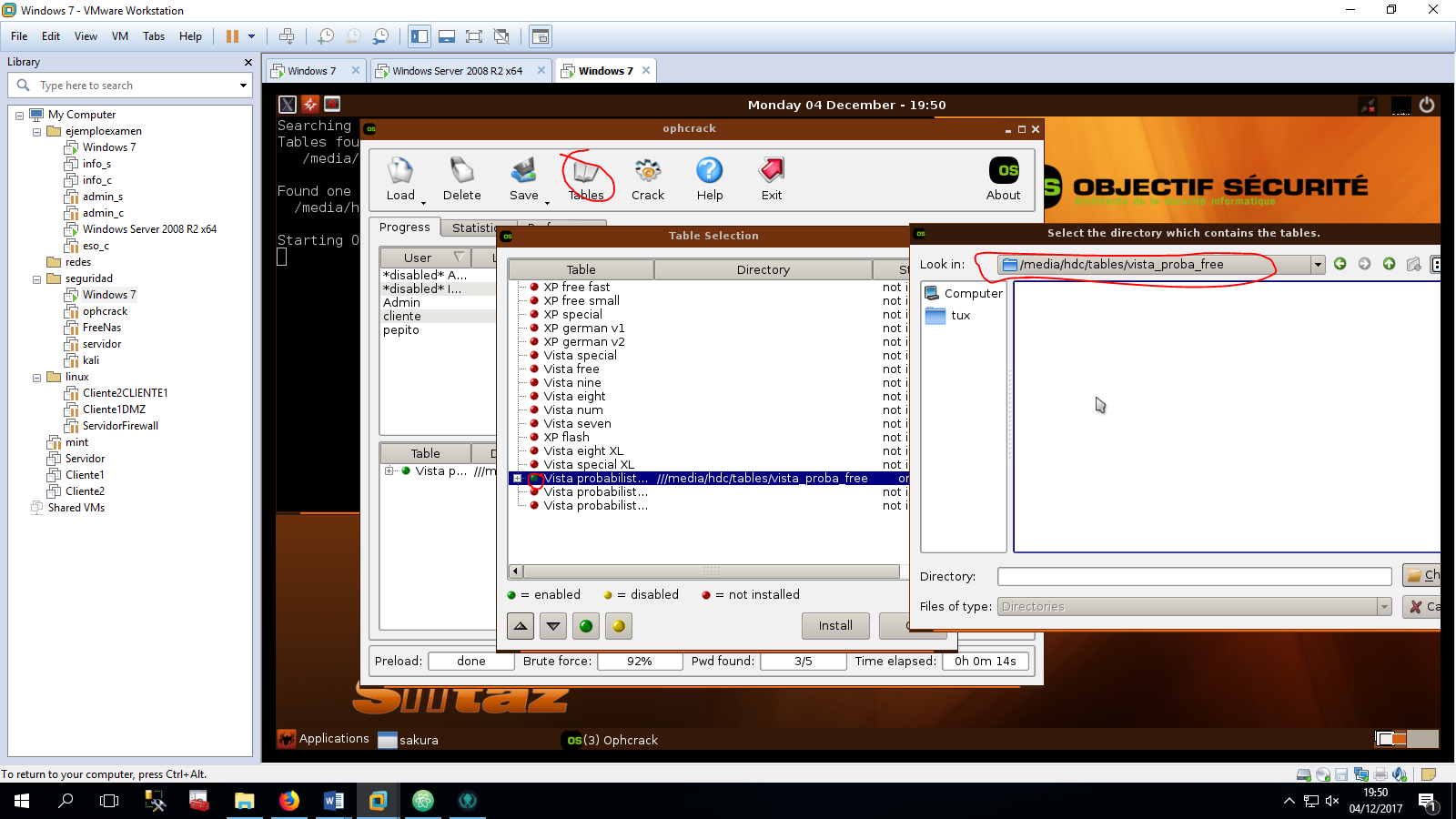


Seleccionaremos la opción por defecto y dejaremos que el sistema arranque.

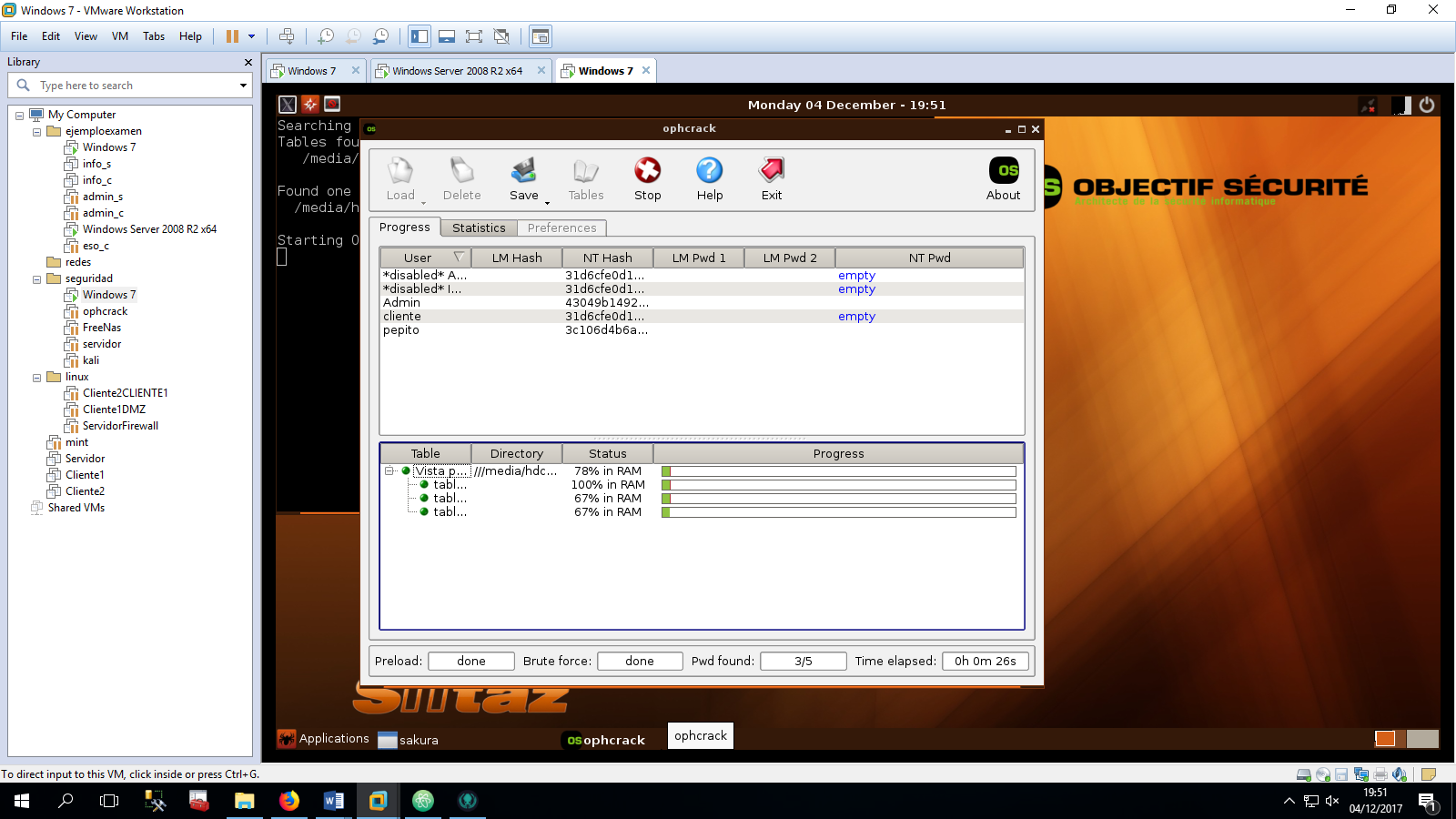
Al arrancar, vemos que automáticamente ophcrack detecta los usuarios del sistema



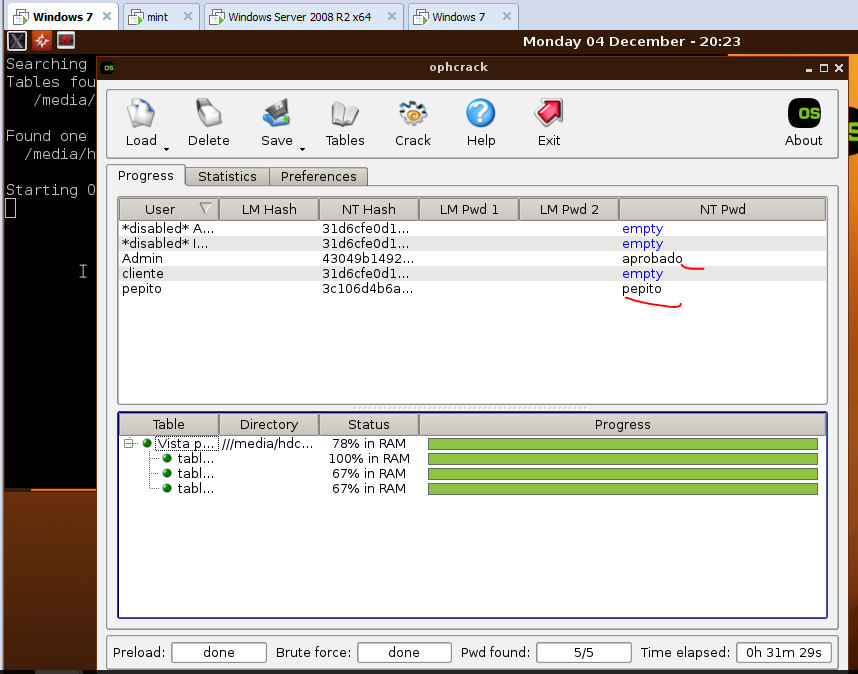
Ahora, tendremos que ir instalando las tablas necesarias para qué ophcrack, para esto, pincharemos en tablas, luego en install y buscaremos las tablas (previamente descargadas)



Ahora picharemos en crack y esperaremos



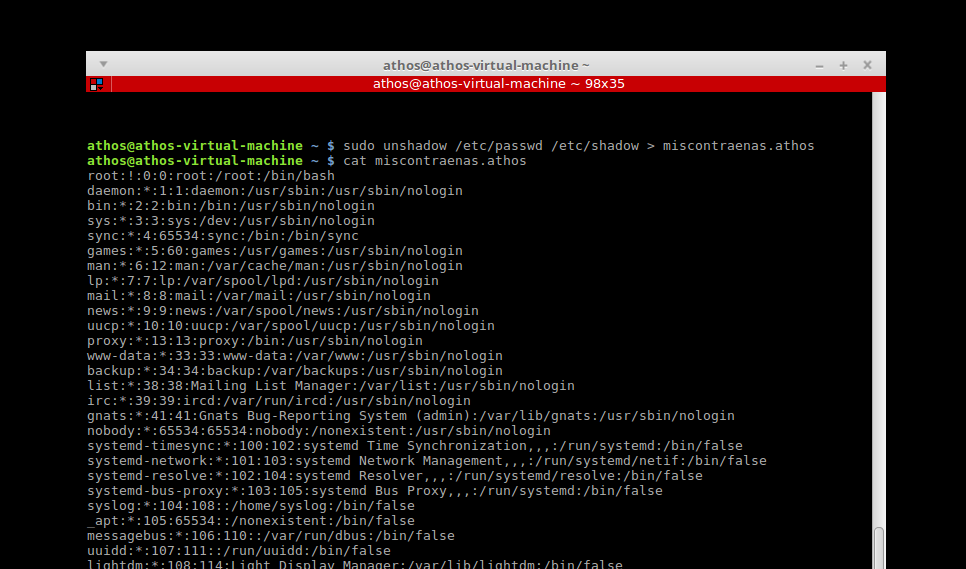
Si todo va bien nos sacara la contraseña.



Como nota añadiré, que para tener más oportunidades de que ophcrack descifre las contraseña conviene que instalemos el mayor número de tablas que podamos.

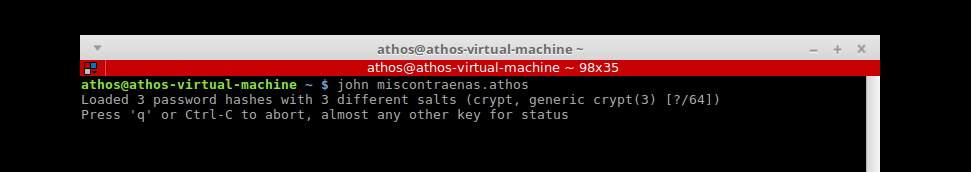
# Des encriptación contraseñas shadow de Linux

Lo primero vamos a unir los archivos /etc/password y /etc/shadow para que cuando nos saque las contraseñas saber de qué usuario es cada una.

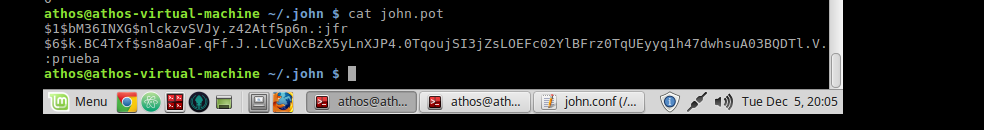


Ahora vamos a probar a ejecutar John pasando como parámetro únicamente el archivo de hashes (miscontrasenas.athos)

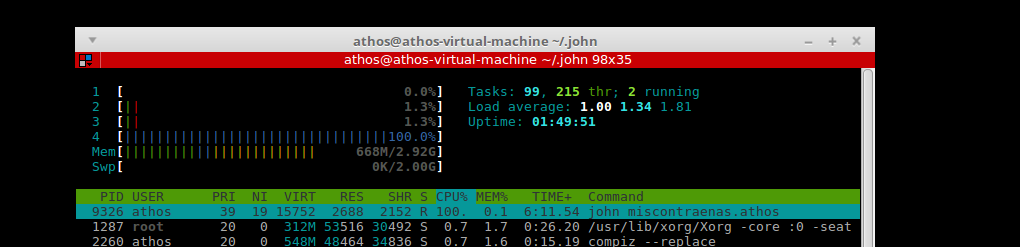
Vemos que ha encontrado tres usuarios de los cuales podemos sacar las contraseñas



Si vamos al archivo John.pot dentro de la carpeta oculta John veremos que tenemos las contraseñas que nos vaya sacando



Mientras esperamos a que saque las contraseñas, he mirado el uso de procesadores del equipo y me encuentro lo siguiente.



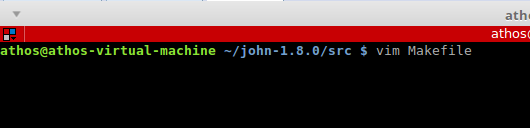
De los cuatro, solo está usando uno. Esto es porque por defecto John viene compilado para usar solo uno de los procesadores. Podríamos compilarlo nosotros para que usase los cuatro.

## Compilación John:

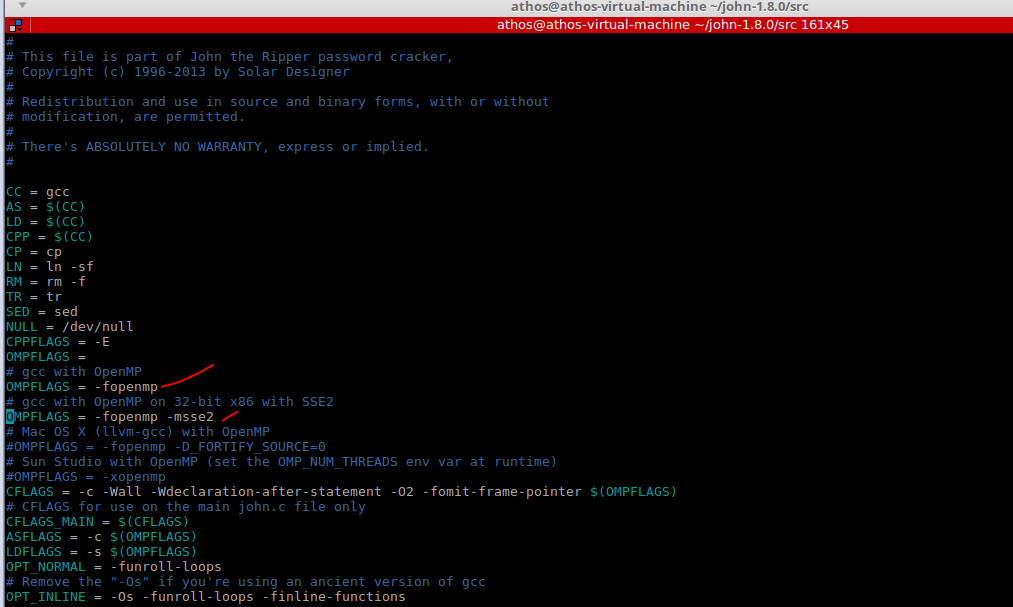
Lo primero es ir a la página oficial de John y descargarnos la última versión (gratuita ya que también hay versión de pago)



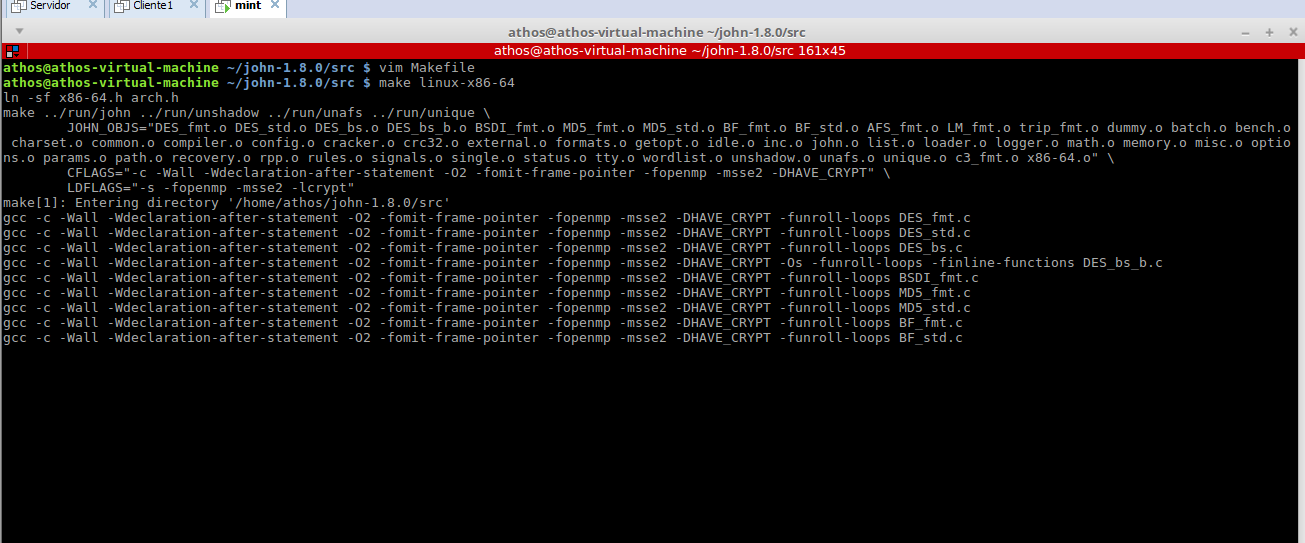
Nos metemos en la carpeta src y editamos el archivo Makefile



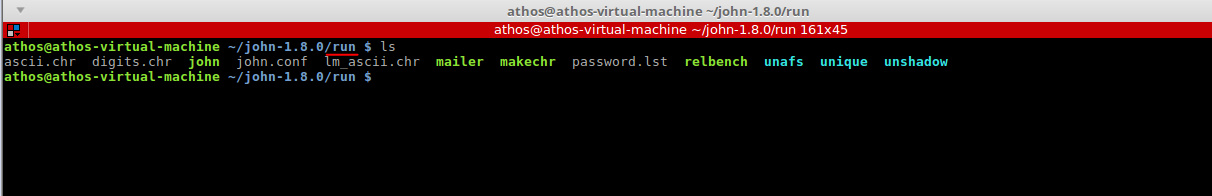
Tendremos que buscar las líneas OMPFLAGS y descomentarlas



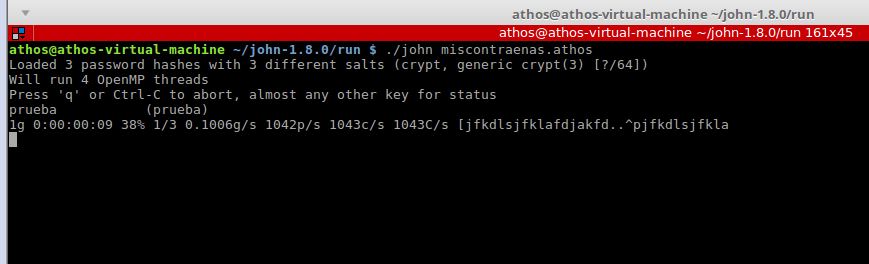
Ahora toca compilar con el comando make linux-x86-64



En la carpeta run nos habrá creado los nuevos ejecutables

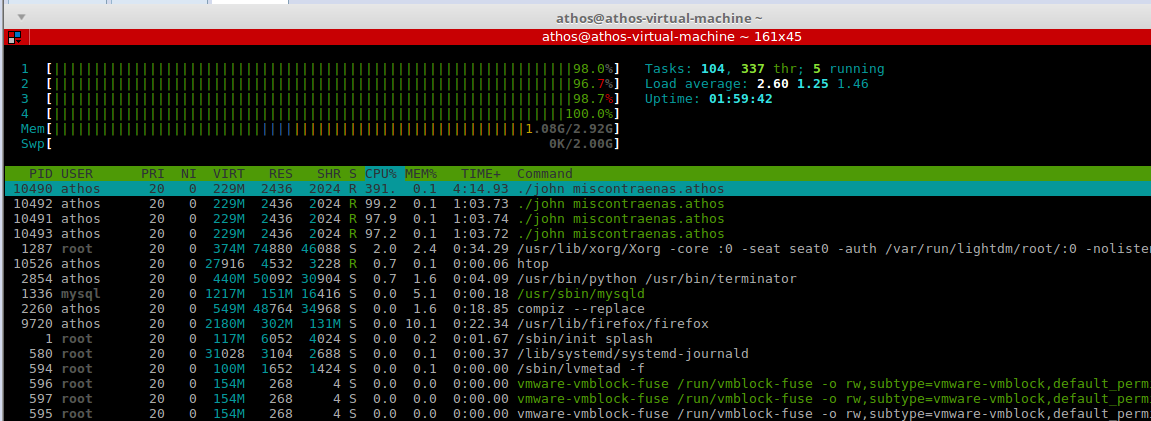


Ahora ejecutamos John como lo hicimos anteriormente y comprobamos los cpus



Como vemos, nos marca que está funcionando con cuatro hilos, y podemos ver que el número de contraseñas por segundo C/s ha aumentado X4

Ahora comprobamos los núcleos con htop



De esta manera, hemos aumentado el rendimiento cuatro veces más.