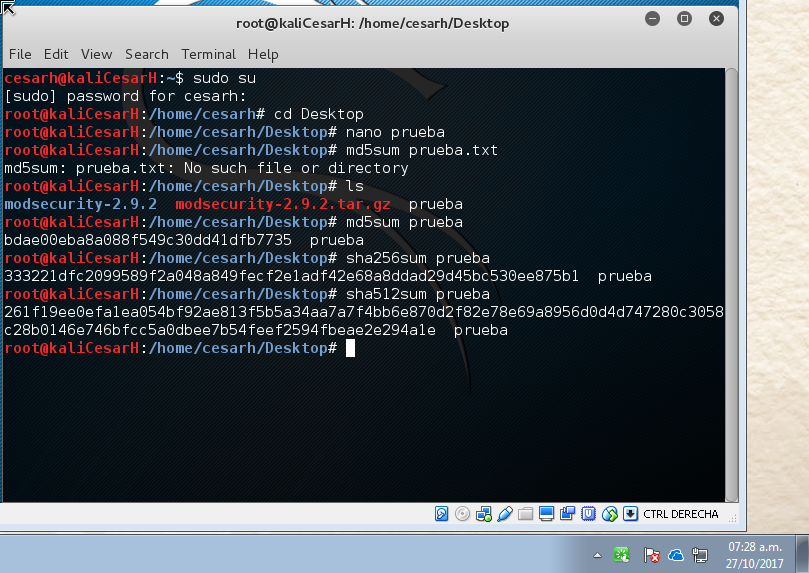
TRABAJO FINAL SEGURIDAD EN REDES.

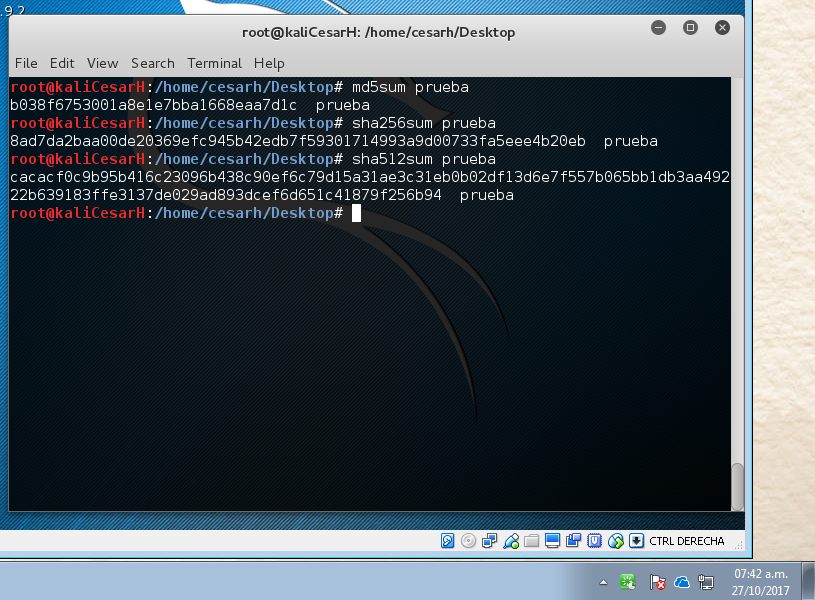
1. INTEGRIDAD

a. Se calcula el hash de un archivo plano



b. modifique el contenido del archivo.

c. Se ejecutan nuevamente los Hash:



Se identifica que el hash tiene el mismo tamaño, pero cambia sus caracteres.

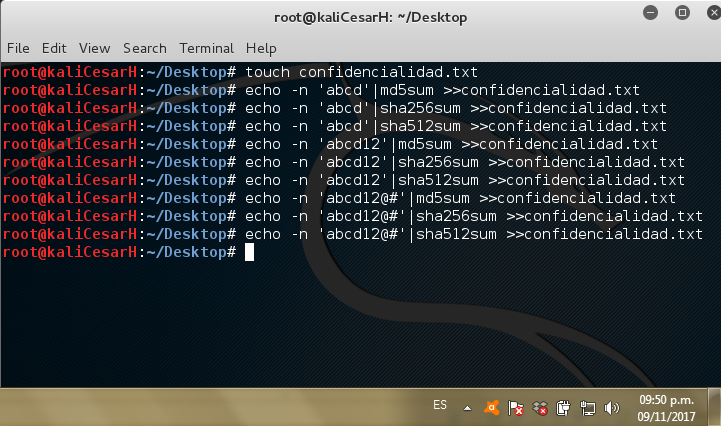
1. CONFIDENCIALIDAD
2. Seleccione 3 palabras que correspondan a contraseñas ficticias con las siguientes características:

i. Baja complejidad = abcd

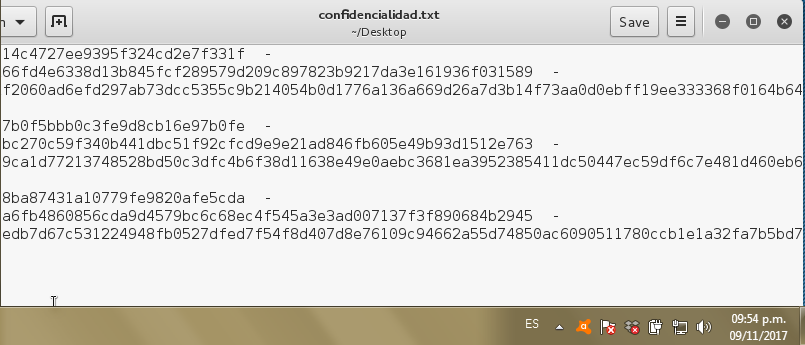
ii. Mediana complejidad = abcd12

iii. Alta complejidad = abcd12@#

1. Calcule los Hashes MD5, SHA256 y SHA 512 de las palabras seleccionadas desde la consola de Linux, En total debe quedar con 9

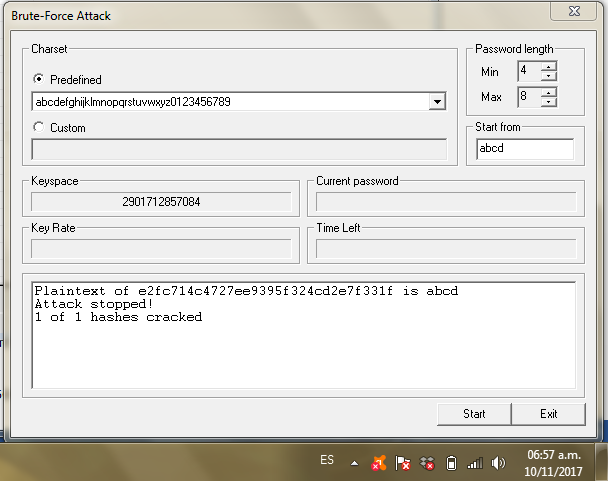


Se guardan las los Hashes en un archivo con el fin de analizarlos por medio de CAIN

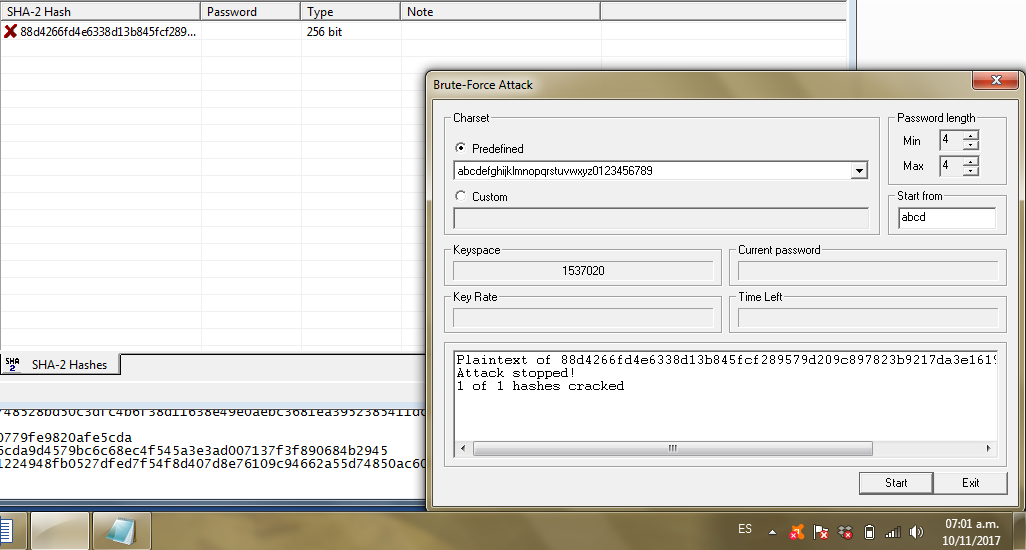


1. Siga las instrucciones sobre el uso del software CAÍN e intente hacer rompimiento por fuerza bruta de los hashes calculados con el fin de probar su fortaleza.

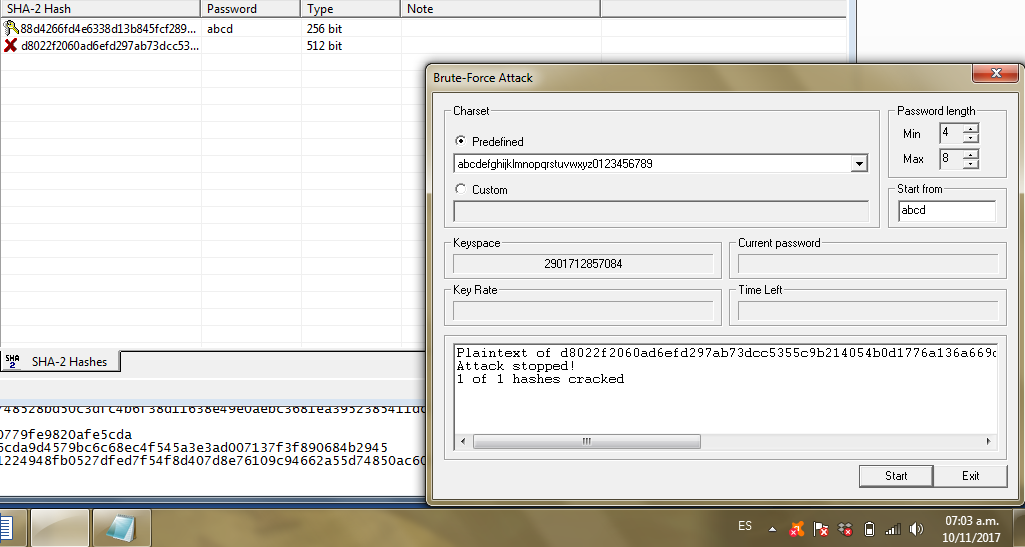
Se calcula md5sum para la contraseña “abcd” y se identifica que el programa CAIN interpreta la contraseña con mucha facilidad.



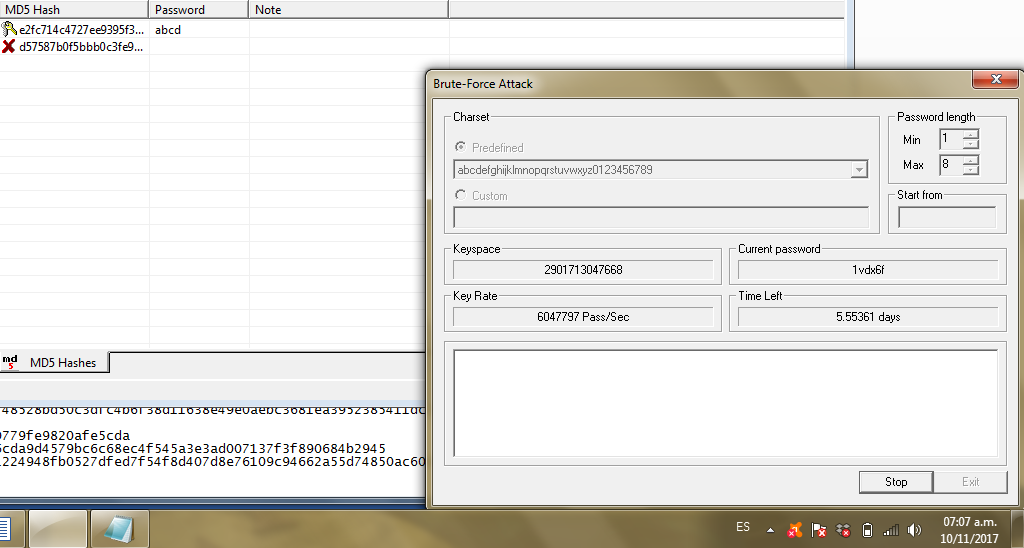
Se calcula sha256sum para la contraseña “abcd”, y se identifica que también interpreta la contraseña rápidamente.



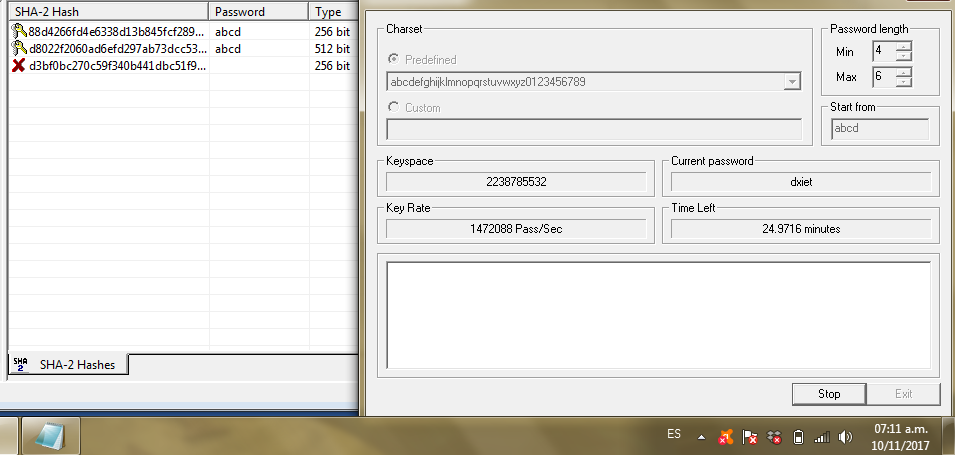
Se calcula sha516sum para la contraseña “abcd”, y se identifica que también interpreta la contraseña rápidamente.



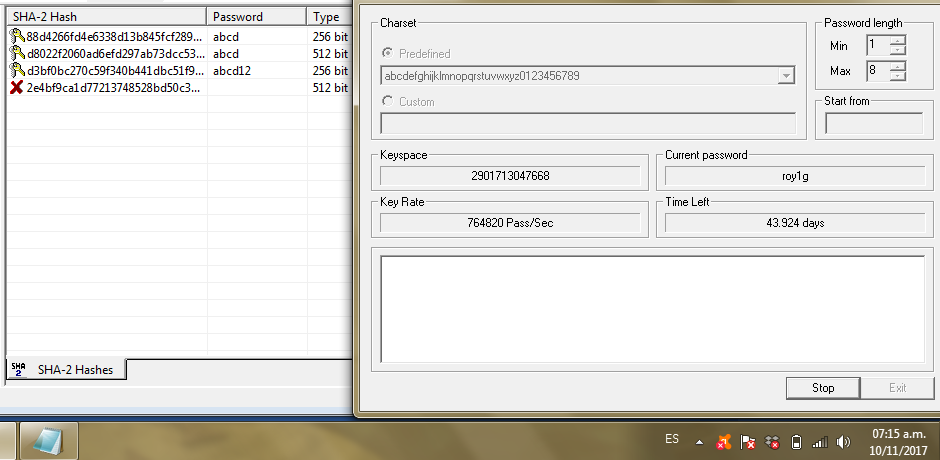
Se calcula md5sum para la contraseña “abcd12”, y se identifica que se demora mas en interpretar la contraseña y en “timeleft” vemos cuanto se podría demorar.



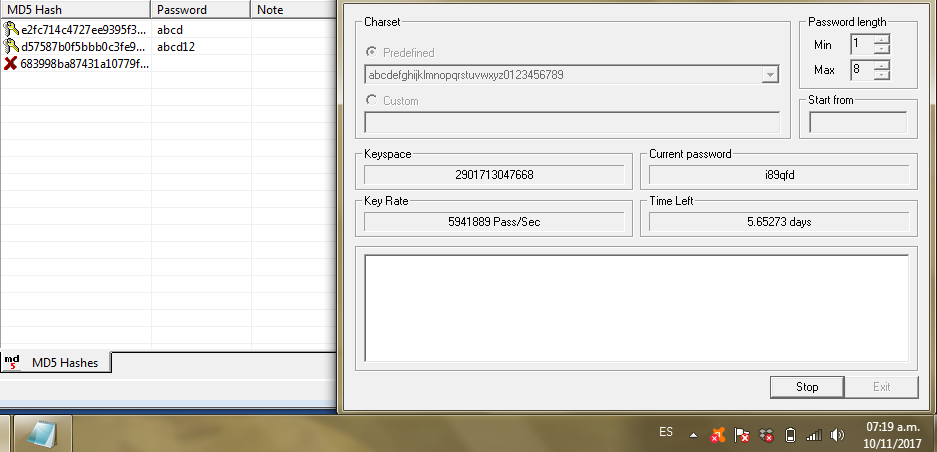
Se calcula sha256sum para la contraseña “abcd12”, y se identifica que también se demora en interpretar la contraseña, y dando algunos indicios como máximo tamaño de clave y como puede empezar a buscar, disminuye el tiempo de búsqueda.



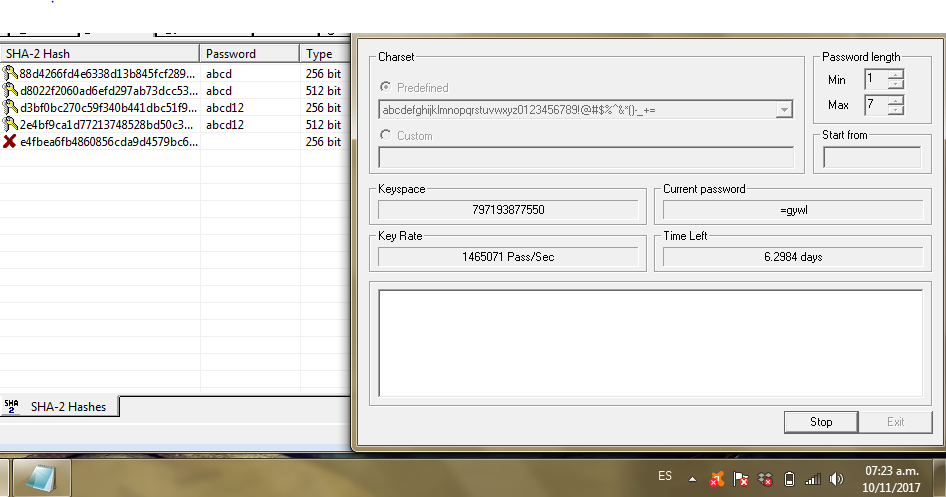
Se calcula sha516sum para la contraseña “abcd12”, y se identifica que también se demora muchísimos más al no darle un indicio de contraseña.



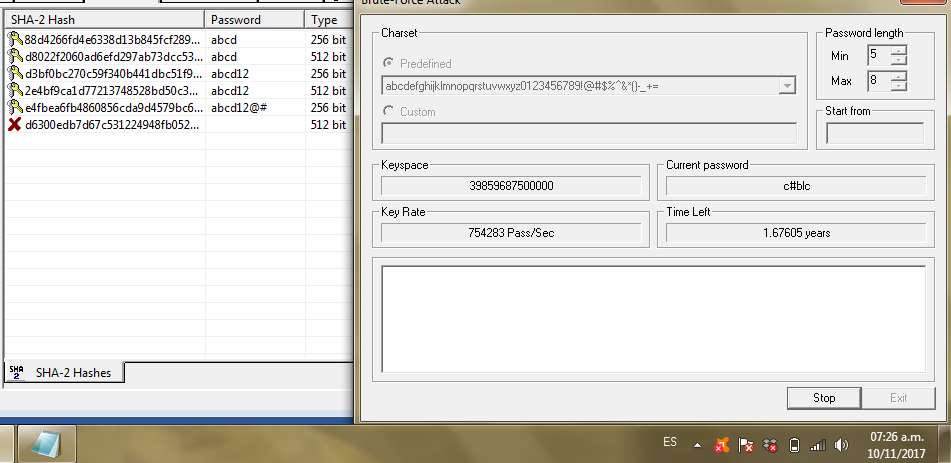
Se calcula md5sum para la contraseña “abcd12@#” y se identifica que con mas complejidad aumenta tiempo y posibilidades de contraseñas, por lo que se va a demorar más.



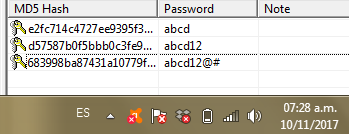
Se calcula sha256sum para la contraseña “abcd12@#”, y se identifica que también se demora en interpretar la contraseña más de 6 días.

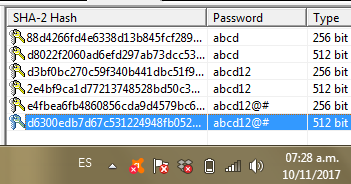


Se calcula sha516sum para la contraseña “abcd12@#”, y se identifica que también se demora muchísimos más al no darle un indicio de contraseña más de un año.



Por último podemos observar los hashes con sus respectivas claves encontradas:





1. Podemos concluir para el ejercicio realizado que entre mas caracteres tenga la contraseña y de diferente tipo, mas difícil es encontrar y cifrar dicha contraseña, mientras que si es más sencilla y de menos caracteres, se puede descifrar fácilmente. Adicional entre mayor sea el Hash utilizado, mayor caracteres tendrá la encriptación y mucho mayor será el tiempo de respuesta para cifrar una contraseña.