Universidad de La Laguna

Práctica de Laboratorio 10. Gestión de contraseñas

En esta práctica vamos a utilizar las herramientas comentadas en clase para la generación de contraseñas y para comprobar su fortaleza. Empezaremos por instalar las herramientas en una de las máquinas virtuales (el cliente por ejemplo). Allí haremos las pruebas.

Ejercicios

1. Instalar `pwgen`, `makepasswd`, `apg` y `john` (John the Ripper) que están en el gestor de paquetes de Debian: apt-get install ...
2. Generar un fichero de contraseñas con hashes MD5. Podemos utilizar la herramienta `makepasswd` para esto:

   ```
   echo "mypassword" | makepasswd --clearfrom=- --crypt-md5 |awk '{ print $2 }'
   ```

   Si tienen problemas con la generación de las claves, es debido a la baja entropía que tiene el generador de números aleatorios en las máquinas virtuales del IaaS-ULL (son servidores headless). Para resolverlo, instalen haveged (aquí tienen unas instrucciones para debian)

3. Para empezar copiamos `/etc/passwd` a un directorio de trabajo. Podemos utilizar los usuario ya existentes y asignarles claves de menor a mayor fortaleza (utilizar alguna secuencia de números, palabras del diccionario, combinaciones de palabras del diccionario con dos dígitos, etc). Añadir alguna clave generada con `pwgen` o `apg`.
4. Utilizar el archivo creado anteriormente como entrada para la herramienta John the Ripper, ver la Descripción de John the Ripper. El objetivo es analizar cuantas claves se rompen con los distintos niveles de pruebas de los que dispone. Probar los modos single, wordlist e incremental. Utilizar como configuración de entrada `/etc/john/john.conf`. Las listas de palabras que pueden utilizar estan en `/usr/share/john/passwd.lst` o en `/usr/dict`. También pueden crear una *adhoc* para comprobar el funcionamiento de JTR.
5. Visitar el enlace Passwd Cracking e intentar romper alguna de las claves que allí se comentan (ejercicio al principio de la página)

Escribir un breve informe comentando las pruebas realizadas.