Introduction to Password Cracking – part 1

I've seen many administrators concerned with the quality of passwords on theirs systems. There are simple ways to test these passwords and to prove if they are easy to crack or not, being necessary and appropriate to explain and clarify that these same techniques are used by hackers to elevate the privilege on a host after an invasion.

So, password auditing is difficult ? No, I don't believe, but I guess you need to pay attention on small details. Let's make some examples. I've setup a virtual machine environment with Windows 2008 R2 and, afterwards, I've downloaded tools like pwdump 7 (http://passwords.openwall.net/a/pwdump/pwdump7.zip), John the Ripper for Windows – jumbo version (http://www.openwall.com/john/g/john179j5w.zip) , L0phtCrack (trial version on http://www.l0phtcrack.com/lc6setup_v6.0.17.exe) and fgdump (http://fgdump.com/fgdump/fgdump-3.0.0-exeonly.zip).

Honestly, it's essencial to emphasize the need for the correct download version of John the Ripper because the "normal" version doesn't support cracking NTLM v2 password and this jumbo version does. When talking about L0phtCrack trial version, we need to remember that this one doesn't offer brute forcing attack technique.

Not always the only option is to try a sophisticated password attack using specialized tools since there're others very straight ways to get a privileged connection to general devices like switches and router. You can verify that the website http://www.default-password.info/ keeps a huge list of default passwords that can be used to access these kind of network devices which the default password is kept since the installation (the guilty is from Administrator). There can be many unprotected devices in your network and maybe you should check them. ☺

As the reader already know, there are some good password cracking techniques for discovering passwords and perhaps the most famous ones are:

a) **Dictionary Attack**

   A big word dictionary can be loaded into the cracking tool to test these words against the user account passwords.

b) **Brute Forcing Attack**

   Every possible key combinations is tried against the password database until the correct key is discovered. It takes a long time (or not ☺)

c) **Hybrid Attack**

   It's a variation from Dictionary attack, but for each dictionary word is attempted a small change like "linux", "linux1", "linux123", etc….

d) **Syllable Attack**

This attack is a combination of Dictionary attack with Brute Forcing Attack.

e) Rainbow Table Attack

A very large list of precomputed hashes are compared with the password file to discovery all passwords.

This post will just deal with a very basic approach and configuration: dictionary and hybrid attack (L0pht 6 trial version) and brute forcing (John the Ripper).

To initiate our exercise, we should extract the **pwdump7.zip** package and run the following command:

```
C:\Users\Administrator\Desktop\pwdump7\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD**********************:95947E88DC144165EEC12CC2039E56B6:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
user1:1007:NO PASSWORD**********************:D25ECD13FDDBB542D2E16DA4F9E0333D:::
user2:1008:NO PASSWORD**********************:6ABB6E6B1DF505EA88088004DF810DE2:::
alexandre:1009:NO PASSWORD**********************:119798F7924D9041D4CFB46A2A04A18D:::

C:\Users\Administrator\Desktop\pwdump7\pwdump7>
```

Nice !!! We've gotten the password hash of every user from our Windows 2008 R2. As you already know, users passwords are stored in SAM database (**C:\Windows\system32\config\SAM**) which is implemented as a registry file and Windows keeps an exclusive lock on it.

The SAM structure is ***user name:user ID:Lan Manager hash: NTLM hash***. Unfortunately, LM (Lan Manager) hash is horrible because Windows takes your password (until 14 characters), convert it to uppercase, pad it to complete 14 characters, split it in two parts, and encrypt each one them using DES (56 bits) and, finally, Windows joins two parts to make a one hash piece. Urgh !!! You already know that DES algorithm is piece of cake to crack(no more than 5 minutes).

Thanks God, if you realized the output command above, there's a significant fact: there isn't Lan Manager hash (NO PASSWORD). Why ? Because since Windows Vista the LM hash schema was banned (both Windows version use NTLMv2 which is case sensitive and use MD5 128 bits) , then there aren't LM hashes on Windows Vista and Windows 7 anymore. Even when you use Windows XP, for example, it's perfectly possible to avoid using LM forcing passwords with lenghts bigger than 14 characters or making a new registry entry: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash** with value = 1.

Is there another way to get the same hashes ?! Sure, there's a good one.The fgdump tool does the same job like pwdump7.exe, but it can connect to remote hosts and get the user passwords easily. Let's see a simple local example:

C:\Users\Administrator\Desktop\fgdump\fgdump\Release**> fgdump.exe -h 127.0.0.1 -u Administrator -p ceh123!**

fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

--- Session ID: 2013-08-01-21-56-49 ---
Starting dump on 127.0.0.1

** Beginning dump on server 127.0.0.1 **
OS (127.0.0.1): Microsoft Windows Unknown Server (Build 7600) (64-bit)
Passwords dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1

As you can see, we've gotten the hashes successfully. Now, you can verify them reading the output file:

C:\Users\Administrator\Desktop\fgdump\fgdump\Release> **more 127.0.0.1.pwdump**

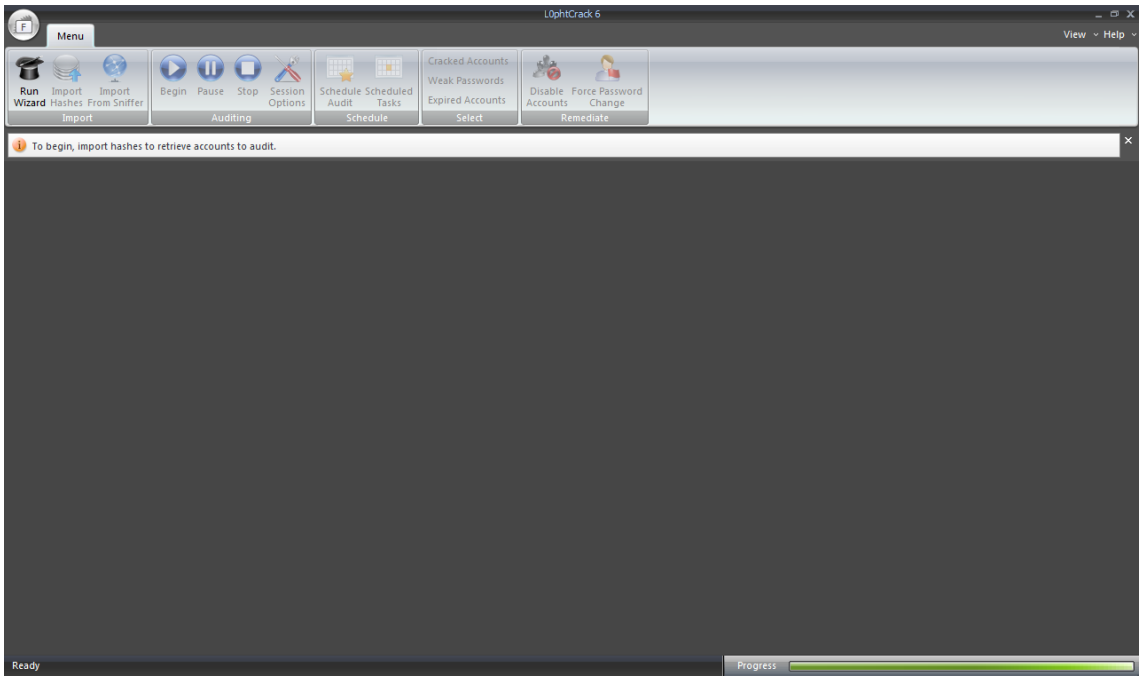
Administrator:500:NO PASSWORD**********:95947E88DC144165EEC12CC2039E56B6:::
alexandre:1009:NO PASSWORD**********:119798F7924D9041D4CFB46A2A04A18D:::
Guest:501:NO PASSWORD**********:NO PASSWORD**********:::
user1:1007:NO PASSWORD**********:D25ECD13FDDBB542D2E16DA4F9E0333D:::
user2:1008:NO PASSWORD**********:6ABB6E6B1DF505EA88088004DF810DE2:::

C:\Users\Administrator\Desktop\fgdump\fgdump\Release> **copy 127.0.0.1.pwdump C:\passwords.txt**

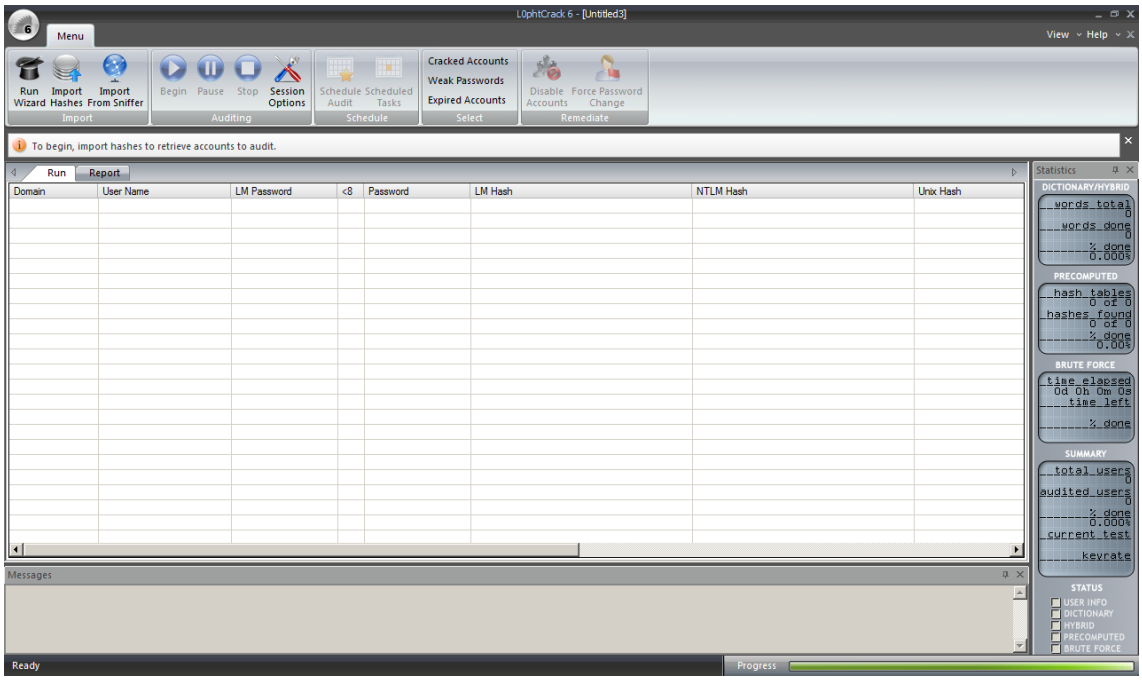
We've achieved our goal, so we can take a step forward. Now, we should concentrate our efforts to crack these NTLM v2 hashes (MD5). The first attempt will be use the L0pht Crack version 6 (LC6). As I'm using LC6 on trial mode, there're some limitations and one of them is that this version doesn't offer brute force password cracking. That's ok because my purpose is

show you a very initial cracking procedure and, if some of our passwords are weak enough, we will find it. ☺

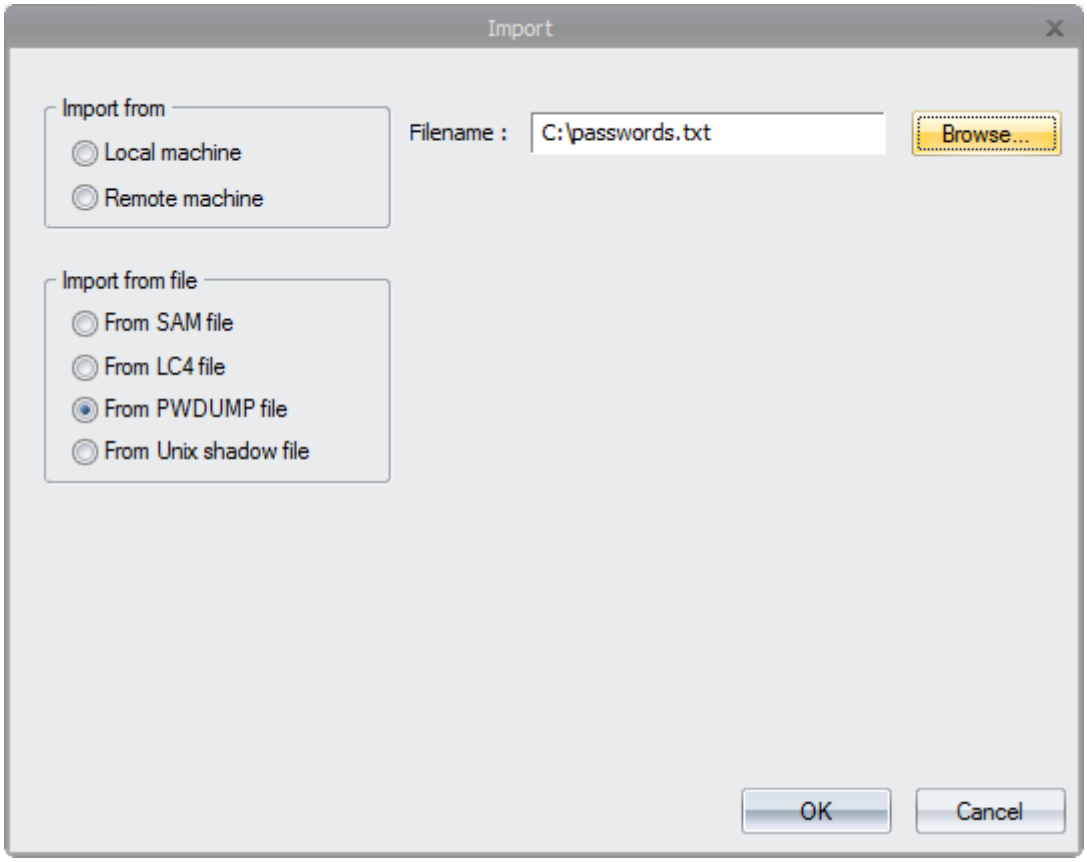
First, we must execute LC6:

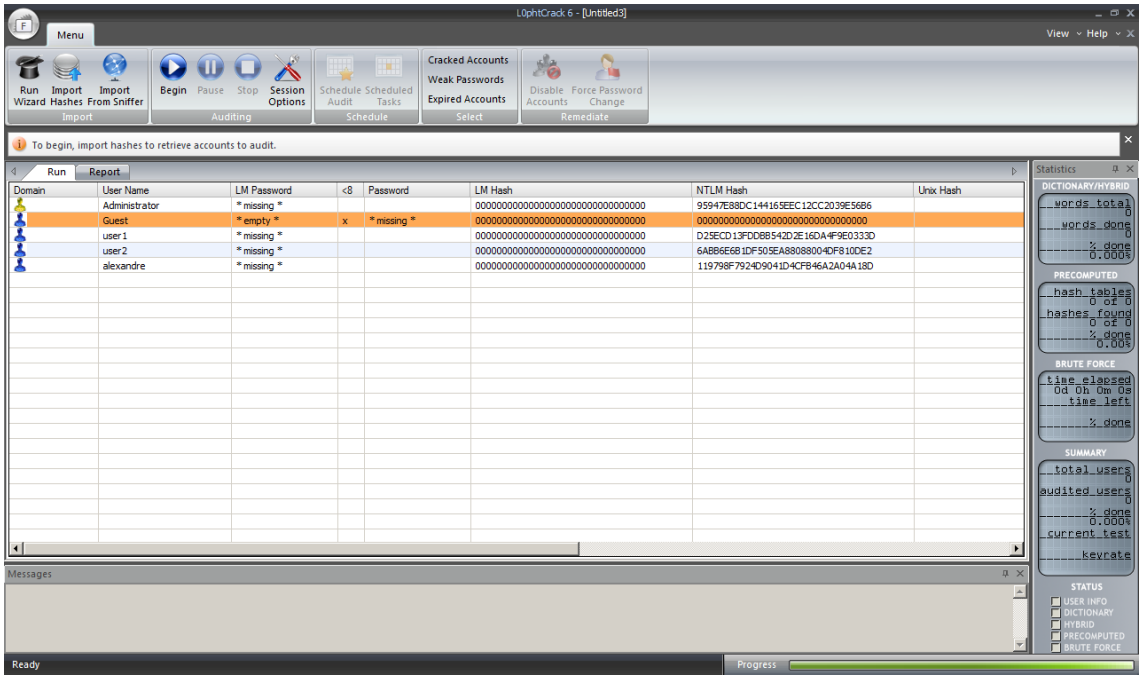


Second, we should go to LC menu (upper left) and choose **“New Session”:**



Third, we need to take the pwdump7/fgdump output and save it in a file named **“C:\passwords.txt”.** Afterwards, we click on **“Import Hashes”** , choose **“Import from PWDUMP file”** and browse the password file **(C:\passwords.txt”):**



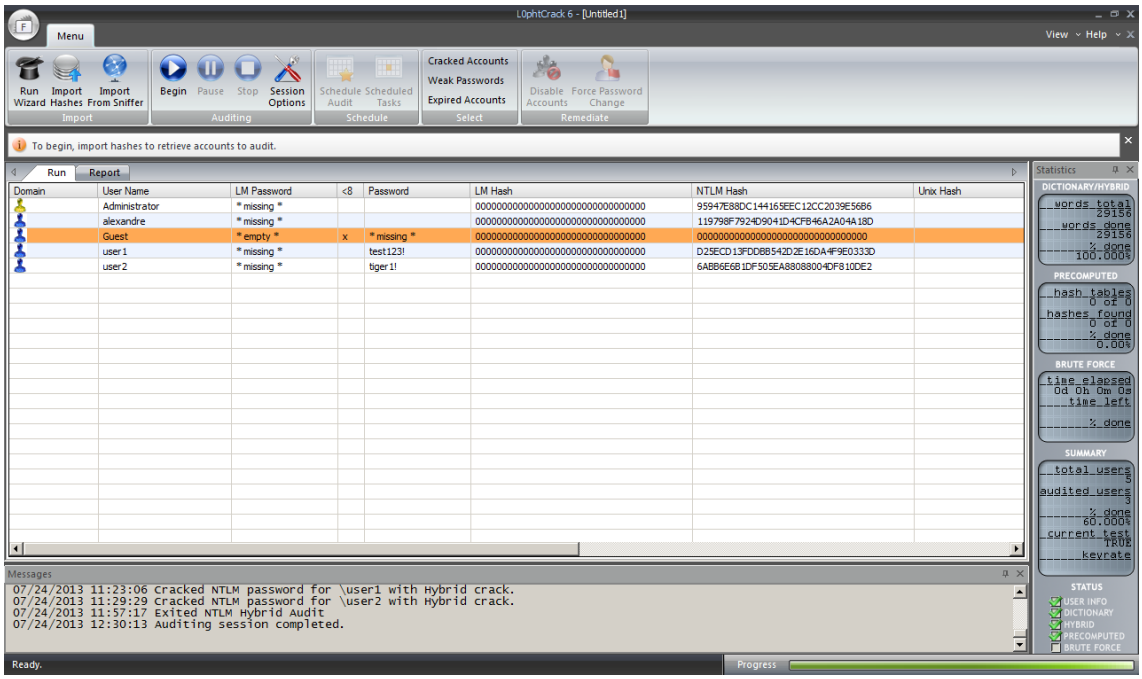


As you should see, Windows 2008 R2 doesn't use LM hashes, so there are only NTLM v2 hashes.

Now, it's easy: we can click on **"Begin"** and LC6 will begin to crack the passwords using dictionary attack, hybrid attack, precomputed attack (like rainbow tables) and brute force

respectively (unfortunately, the last mode is only available on a paid LC version). You can see this exact sequence at right lower corner.

After some time, we will get a output showing the cracked password from user1 and user2. Nice. We couldn't get all users passwords, but even so it's already a good news. ☺



In the last section we are going to another approach and use John the Ripper for Windows (version 1.7.9 – jumbo – 5) which is an extended edition from normal John the Ripper and it's made to crack password hashes like NTLM v2.

To initiate the exercise, let's prepare and format the password file to crack it. Taking the pwdump7 or fgdump output, we need to format it like this (the given name is C:\Users\Administrator\Desktop\john179j5w\john179j5\run **password2.txt**):

Administrator:95947E88DC144165EEC12CC2039E56B6
alexandre:119798F7924D9041D4CFB46A2A04A18D
user1:D25ECD13FDDBB542D2E16DA4F9E0333D
user2:6ABB6E6B1DF505EA88088004DF810DE2

What did we do ? We removed the UID field, LM hash field (NO PASSWORD) and trailling colons.

Before executing the password cracking procedure, it's suggested to list all options that John the Ripper offers to us:

C:\Users\Administrator\Desktop\john179j5w\john179j5\run> **john.exe**

John the Ripper password cracker, ver: 1.7.9-jumbo-5 [win32-cygwin-x86-sse2i]
Copyright (c) 1996-2011 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

```
--config=FILE           use FILE instead of john.conf or john.ini
--single[=SECTION]      "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
            --pipe    like --stdin, but bulk reads, and allows rules
--encoding=NAME         the input data is in a 'non-standard' character.
                    encoding. NAME = utf-8, koi8-r, and others. For a
                    full list, use --encoding=LIST
--rules[=SECTION]       enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--markov[=LEVEL[:opts]]  "Markov" mode (see documentation)
--external=MODE         external mode or word filter
--stdout[=LENGTH]       just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
--make-charset=FILE     make a charset file. It will be overwritten
--show[=LEFT]           show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]  load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]  load salts with[out] COUNT [to MAX] hashes
--pot=NAME              pot file to use
--format=NAME           force hash type NAME: des/bsdi/md5/bf/afs/lm/
                    dynamic_n/bfegg/dmd5/dominosec/epi/hdaa/ipb2/krb4/
                    krb5/mschapv2/mysql-fast/mysql/netlm/netlmv2/netntlm/
                    netntlmv2/nethalflm/md5ns/nt/phps/po/xsha/crc32/
                    hmac-md5/lotus5/md4-gen/mediawiki/mscash/mscash2/
                    mskrb5/mssql/mssql05/mysql-sha1/nsldap/nt2/oracle11/
                    oracle/phpass-md5/pix-md5/pkzip/raw-md4/raw-md5thick/
                    raw-md5/raw-sha1/raw-sha/raw-md5u/salted-sha1/sapb/
                    sapg/sha1-gen/raw-sha224/raw-sha256/raw-sha384/
                    raw-sha512/xsha512/hmailserver/sybasease/trip/ssh/pdf/
                    rar/zip/dummy
--subformat=LIST        get a listing of all 'dynamic_n' formats
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
--mem-file-size=SIZE    size threshold for wordlist preload (default 5 MB)
--field-separator-char=C  use 'C' instead of the ':' in input and pot files
--fix-state-delay=N     performance tweak, see documentation
--nolog                 disables creation and writing to john.log file
--crack-status          emit a status line whenever a password is cracked
```

Finally, we can crack all users passwords taking the same sequence of LC6, but this time including the brute force method:

C:\Users\Administrator\Desktop\john179j5w\john179j5\run> **john --format=nt2 password2.txt**

Loaded 4 password hashes with no different salts (NT v2 [SSE2i 12x])

tiger1! (user2)

test123! (user1)
ceh123! (Administrator)
debian2! (alexandre)

guesses: 4 time: 0:00:27:12 DONE (Mon Jul 29 18:38:42 2013) c/s: 29598K trying: debian26 - debian2s
Use the "--show" option to display all of the cracked passwords reliably

C:\Users\Administrator\Desktop\john179j5w\john179j5\run>

Congratulations !!! You've found every passwords from the system !!! As it has taken us a very short time to accomplish, it would be advisable to change them and to pick a more complex passwords.

Please, you should pay attention to the "format" parameter: we've chosen its value equal to "nt2" because we've wanted to crack NTLM v2 passwords. There are other interesting formats and I recommend you doing some research on it. ☺

If we wished to suspend the cracking session to resume it later, we should press any key and, after that, to press **"Ctrl + C".** To resume the job, we could run:

C:\Users\Administrator\Desktop\john179j5w\john179j5\run> **john --restore**

A file named **"john.pot**" controls our progress and it's used to resume the job.

We've finished it. I hope you 've enjoyed.

Have a nice day. ☺

Alexandre Borges