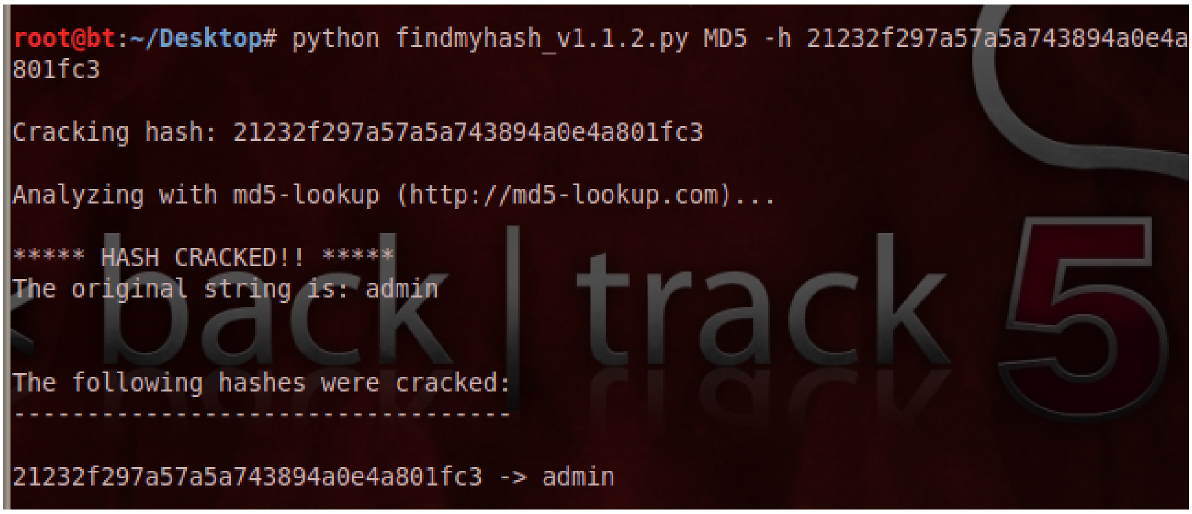
FindMyHash

pentestlab.blog/category/tools/page/3

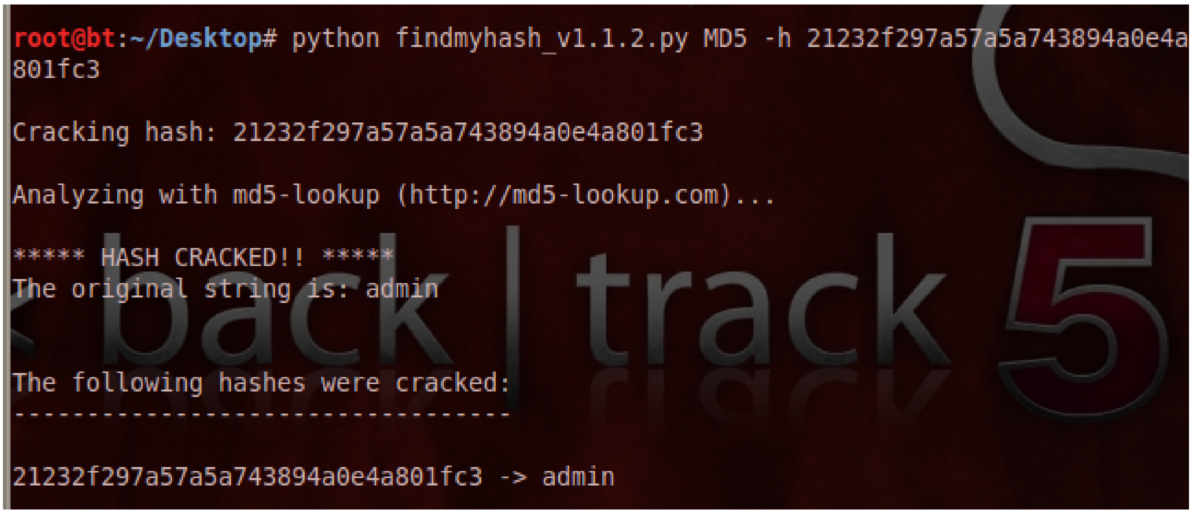
May 6, 2013



```
root@bt:~/Desktop# python findmyhash_v1.1.2.py MD5 -h 21232f297a57a5a743894a0e4a
801fc3

Cracking hash: 21232f297a57a5a743894a0e4a801fc3

Analyzing with md5-lookup (http://md5-lookup.com)...

***** HASH CRACKED!! *****
The original string is: admin


The following hashes were cracked:
----------------------------------

21232f297a57a5a743894a0e4a801fc3 -> admin
```

Often in penetration tests we discover password hashes. In this situation every penetration tester use the password cracking tool of his convenience (like john the ripper) in order to crack the hashes offline and to escalate privileges. The sooner that the hash cracks the better for the results of the engagement as the penetration tester will have more time to search on the system for other important things while he has a valid password.

For that reason a script created that allows the penetration tester to crack hashes using free online services or even Google if the hash is common. The usage of the script is very simple and it can be seen below:



```
root@bt:~/Desktop# python findmyhash_v1.1.2.py MD5 -h 21232f297a57a5a743894a0e4a
801fc3

Cracking hash: 21232f297a57a5a743894a0e4a801fc3

Analyzing with md5-lookup (http://md5-lookup.com)...

***** HASH CRACKED!! *****
The original string is: admin


The following hashes were cracked:
----------------------------------

21232f297a57a5a743894a0e4a801fc3 -> admin
```

FindMyHash Script in action

This is definitely something that every penetration tester should check before he starts the process of cracking a hash.

Author: https://twitter.com/laXmarcaellugar

Email: bloglaxmarcaellugar@gmail.com

Script: http://code.google.com/p/findmyhash/