Hash Cracking with Rainbow Tables

Introduction

This document explains the rcrack program. The rcrack program lookup existing rainbow tables for the plaintext of user supplied hash.

Six similar programs are available:

Program	User Interface	GPU Acceleration
rcrack	Command Line	
rcrack_cuda	Command Line	NVIDIA CUDA
rcrack_cl	Command Line	AMD OpenCL
rcrack_gui	GUI	
rcrack_cuda_gui	GUI	NVIDIA CUDA
rcrack_cl_gui	GUI	AMD OpenCL

Command line program is ideal for batch processing, and GUI program is easy to use.

Rainbow tables used by rcrack program must already be sorted with rtsort program, and optionally converted to .rtc file format with rt2rtc program.

Rainbow Table Lookup with rcrack/rcrack_cuda/rcrack_cl Program

General Use

Assume rainbow tables are in directory c:\rt.

To crack single hash:

```
rcrack      c:\rt -h fcea920f7412b5da7be0cf42b8c93759
rcrack_cuda c:\rt -h fcea920f7412b5da7be0cf42b8c93759
rcrack_cl   c:\rt -h fcea920f7412b5da7be0cf42b8c93759
```

To crack multiple hashes:

```
rcrack      c:\rt -l hash_list_file
rcrack_cuda c:\rt -l hash_list_file
rcrack_cl   c:\rt -l hash_list_file
```

In the example above, hash_list_file is a text file with each hash in one line.

To lookup rainbow tables in multiple directories:

```
rcrack      c:\rt1 c:\rt2 -l hash_list_file

rcrack_cuda c:\rt1 c:\rt2 -l hash_list_file

rcrack_cl   c:\rt1 c:\rt2 -l hash_list_file
```

In the example above, the rcrack/rcrack_cuda/rcrack_cl program will lookup rainbow tables in c:\rt1 and c:\rt2 directories sequentially.

Special Consideration for LM/NTLM Hash

LM/NTLM hashes are usually saved in text file of pwdump format.

Content of typical pwdump file:

```
Administrator:500:1c3a2b6d939a1021aad3b435b51404ee:e24106942bf38b
cf57a6a4b29016eff6:::

Guest:501:a296c9e4267e9ba9aad3b435b51404ee:9d978dda95e5185bbeda9b
3ae00f84b4:::
```

To load and crack LM hashes from pwdump file:

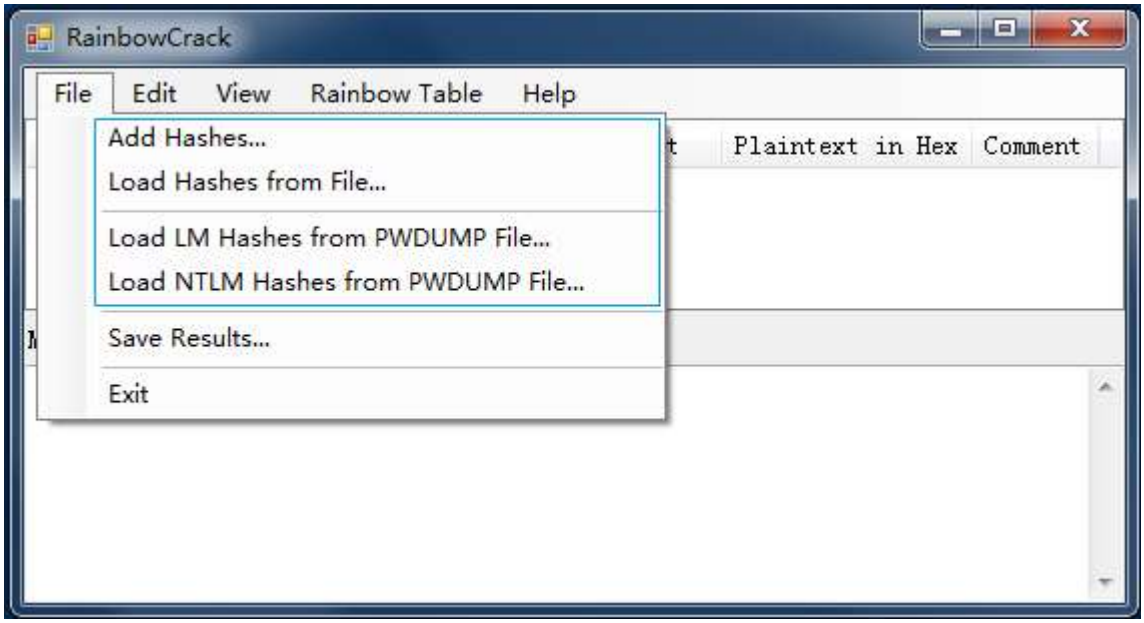
```
rcrack      c:\rt -lm pwdump_file

rcrack_cuda c:\rt -lm pwdump_file

rcrack_cl   c:\rt -lm pwdump_file
```

To load and crack NTLM hashes from pwdump file:

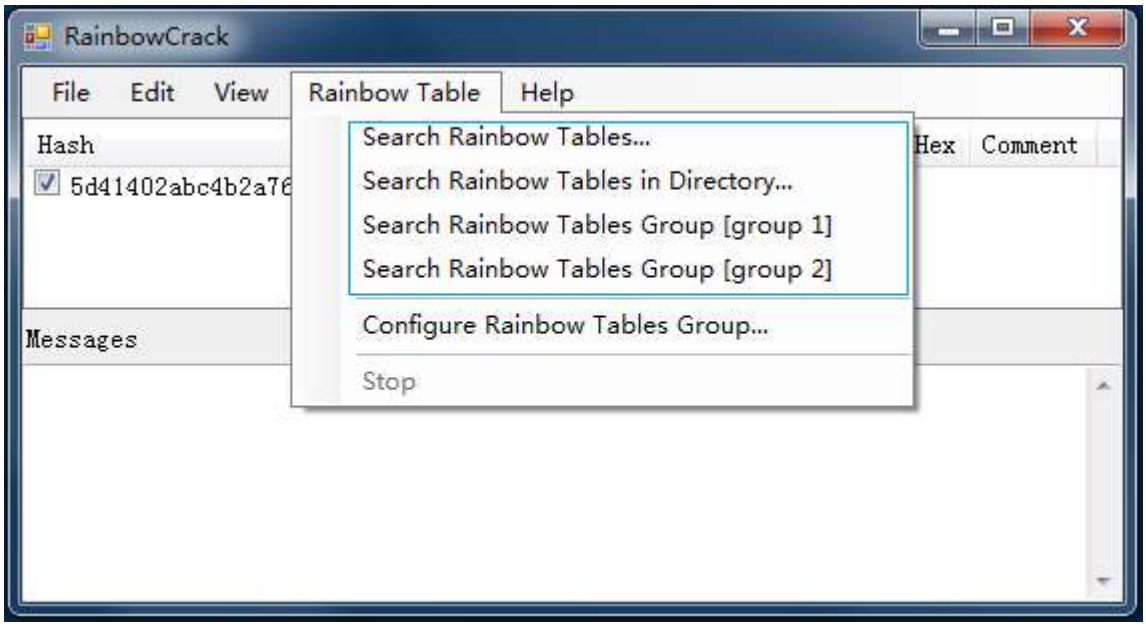
```
rcrack      c:\rt -ntlm pwdump_file

rcrack_cuda c:\rt -ntlm pwdump_file

rcrack_cl   c:\rt -ntlm pwdump_file
```

Rainbow Table Lookup with rcrack_gui/rcrack_cuda_gui/rcrack_cl_gui Program

Step 1: Load the Hashes



Step 2: Specify the Rainbow Tables to be Searched



Select "Search Rainbow Tables..." to search individual rainbow tables.

Select "Search Rainbow Tables in Directory..." to search all rainbow tables in a directory.

Select "Search Rainbow Tables Group [group name]" to search rainbow tables in multiple directories sequentially. All rainbow table groups are defined in configuration file group.txt.

When rainbow tables are specified, hash cracking will start.

Performance Tips

Memory Requirement

4 GB memory is minimal and 8 GB or more memory is recommended. Larger memory always help to improve performance when searching large rainbow tables.

Hard Disk

Because rainbow table must be loaded from hard disk to memory to look up and some rainbow table set can be as large as hundreds of GB, hard disk performance becomes a very important factor to achieve overall good hash cracking performance.

We suggest put rainbow tables in RAID 0 volume with multiple hard disks. Windows operating system natively support software RAID 0 called "striped volume".

The rcrack program always read data from hard disk sequentially. There is no random access.

Multiple GPUs

RainbowCrack software supports GPU acceleration with CUDA enabled GPUs from NVIDIA and OpenCL enabled GPUs from AMD.

GPU acceleration with multiple GPUs is supported. To get optimal performance, all GPUs need be of same model.