BootCon Presentation: Rainbowcrack

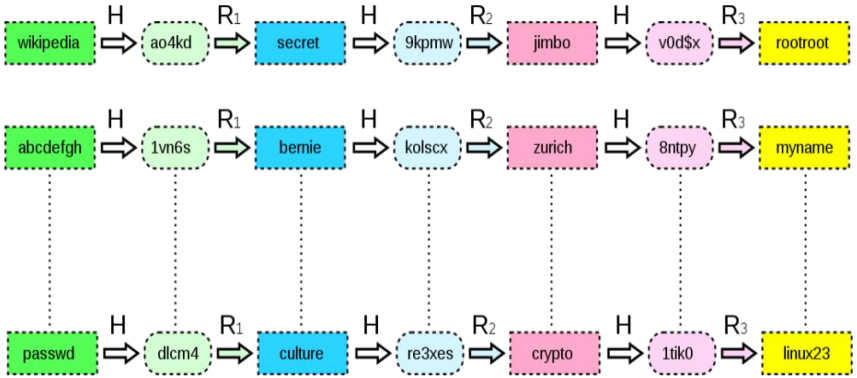
By Wallace Martin

Rainbowcrack Summary, Features, & the Goal

- Rainbowcrack is a cybersecurity tool that is designed to crack password hashes with rainbow tables.
- Windows and Linux compatible.
- Can be performed on the command line or with the GUI.
- The goal of this project is to simulate a rainbow table attack, attempting to successfully crack a list of MD5 password hashes stolen from a vulnerable application.

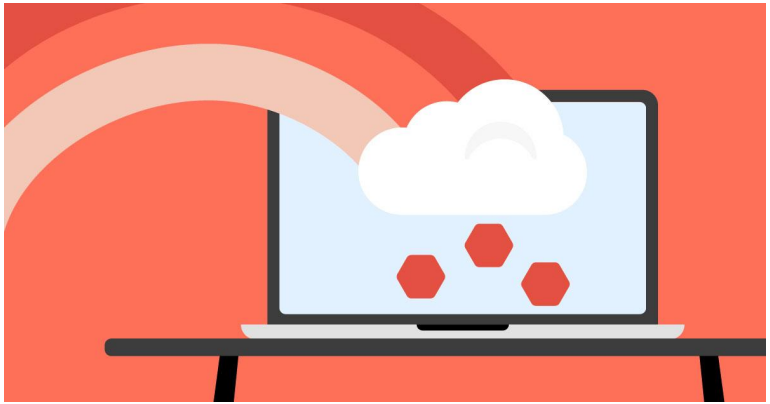
Rainbow Tables & Rainbow Table Attacks

- A rainbow table attack is a password cracking method that uses a rainbow table to crack the password hashes in a database.
- As we know, secure applications don’t store passwords in plaintext, but instead encrypt passwords using hashes.
- A rainbow table is a precomputed table that holds the password hash value for each plaintext character used during authentication.



Example Scenarios of Rainbow Table Attacks

- Active directory vulnerability such as too many users with high privileges, and one of those user's account gets hacked. That can lead to the hacker gaining access to a list of password hashes belonging to a company.
- A web application that has obsolete hashing techniques. A rainbow table can decrypt the passwords of the users of that application.



Demonstration Preview & Setup Process

- Version Specifications
- Generating a Rainbow Table
- Sorting the Rainbow Table
- Load Hashes (Video Demo)
- Load Rainbow Table (Video Demo)
- Analyze Results

Rainbowcrack Specifications

- rtgen command displays usage of rainbowcrack and the syntax used.
- Some hash algorithms are already configured and included, but you can add more in the charset.txt file provided.

```
C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64>rtgen
RainbowCrack 1.8
Copyright 2020 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index
       rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index -bench

hash algorithms implemented:
    lm HashLen=8 PlaintextLen=0-7
    ntlm HashLen=16 PlaintextLen=0-15
    md5 HashLen=16 PlaintextLen=0-15
    sha1 HashLen=20 PlaintextLen=0-20
    sha256 HashLen=32 PlaintextLen=0-20

examples:
    rtgen md5 loweralpha 1 7 0 1000 1000 0
    rtgen md5 loweralpha 1 7 0 -bench
```

Rainbow Table Generation

- Generating a Rainbow Table that will attempt to crack MD5 hashes.
- Command: rtgen md5 mixalpha-numeric 1 9 0 2400 24652134 0
- The cracked hashes will only be plaintext passwords that are 1-9 characters long, along with containing only letters (both lowercase and/or capital) and/or numbers.

```
C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64>rtgen md5 mixalpha-numeric 1 9 0 2400 24652134 0
rainbow table md5_mixalpha-numeric#1-9_0_2400x24652134_0.rt parameters
hash algorithm:         md5
hash length:            16
charset name:           mixalpha-numeric
charset data:           abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
charset data in hex:    61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 30 31 32 33 34 35 36 37 38 39
 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 30 31 32 33 34 35 36 37 38 39
charset length:         124
plaintext length range: 1 - 9
reduce offset:          0x00000000
plaintext total:        6987337810155938124

sequential starting point begin from 0 (0x0000000000000000)
generating...
524288 of 24652134 rainbow chains generated (0 m 16.5 s)
1048576 of 24652134 rainbow chains generated (0 m 15.7 s)
1572864 of 24652134 rainbow chains generated (0 m 17.7 s)
2097152 of 24652134 rainbow chains generated (0 m 17.2 s)
```

Sorting the Table

- rtsort . command converts generated tables into .rt files, which is the file type that will be loaded on rainbowcrack to start cracking passwords.
- Can sort multiple tables into a folder for easy access.

```
C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64>rtsort .
.\md5_mixalpha-numeric#1-9_0_2400x24652134_0.rt:
9874690048 bytes memory available
loading data...
sorting data...
writing sorted data...
```

- We can now start cracking these hashes!

Rainbowcrack GUI Demonstration, Results at 18:15

https://app.screencastify.com/v3/watch/fevyCO9Kc2mhUt5am1vU

A Successful Test

- 6 plaintext passwords found out of 2351 hashes in 762 seconds

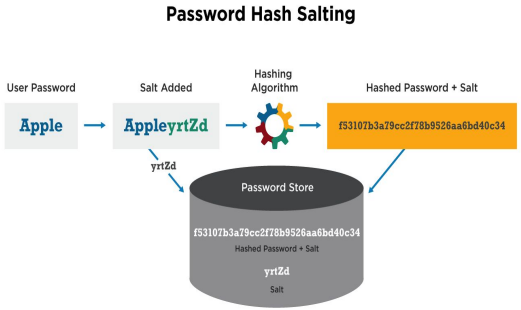
```
Messages
6 rainbow tables found
memory available: 7869995417 bytes
memory for rainbow chain traverse: 38400 bytes per hash, 90278400 bytes for 2351 hashes
memory for rainbow table buffer: 6 x 394434160 bytes
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_0_2400x24652134_0.rt: 394434144 bytes read
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_1_2400x24652134_0.rt: 394434144 bytes read
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_2_2400x24652134_0.rt: 394434144 bytes read
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_3_2400x24652134_0.rt: 394434144 bytes read
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_4_2400x24652134_0.rt: 394434144 bytes read
disk: C:\Users\mwall\Downloads\rainbowcrack-1.8-win64\rainbowcrack-1.8-win64\md5_mixalpha-numeric#1-9_5_2400x24652134_0.rt: 394434144 bytes read
disk: finished reading all files
plaintext of 009f25a425c179da52a4f69b60bf81fc is dawn
plaintext of 0cc175b9c0f1b6a831c399e269772661 is a
plaintext of ele1d3d40573127e9ee0480caf1283d6 is R
plaintext of 9cdfb439c7876e703e307864c9167a15 is lol
plaintext of d37f3f4c67d915e7e8f62264be4d68c8 is ldtp
plaintext of ce1b09ae5ec7956ffa96bda839fe50c7 is hak5

statistics
--------------------------------------------------------------------
plaintext found:                            6 of 2351
total time:                                 762.00 s
time of chain traverse:                     722.91 s
time of alarm check:                        0.02 s
time of disk read:                          1.11 s
hash & reduce calculation of chain traverse: 40505097600
hash & reduce calculation of alarm check:   57076
number of alarm:                            100
performance of chain traverse:              56.03 million/s
performance of alarm check:                 3.36 million/s
```

Demonstration Summary

- Generated Rainbow Tables that searched for hashes with plaintext passwords of 1-9 characters, lowercase/capital letters, no special characters.
- Loaded Hashes and Rainbow Tables into Rainbowcrack for password cracking.
- First Test: No plaintext found. Stronger minimum password requirements.
- Successful Test: Plaintext found. Weaker minimum password requirements.

Mitigation Strategies

- A very prevalent mitigation strategy known as salting has reduced the amount of Rainbow Table Attacks that take place. Salting is when an extra random value is added to every hashed password, creating different hash values.
- Enact passwordless authentication methods.
- Rid your application or server of outdated hashing algorithms such as MD5 and SHA1.
- Actively monitor your servers.
- Strong password requirements for all user accounts



Conclusion & Closing Thoughts

- While Rainbow Table Attacks have become less common, it's still an effective method for mass cracking weak and simple passwords.
- Cracking complex passwords is definitely possible but would take extra steps.
- Simple setup once you learn how each step connects, which required more outside research.
- Time consuming to generate tables and wait for the cracking to finish.
- Unsure of future use cases as of now, but I'm glad I learned this tool!