COMP 8506 Assignment 4

Password Cracking - Ophcrack

Xinghua Wei

A00978597

Ophcrack

Introduction

Ophcrack is a free, open-source program that cracks Windows log-in password by using LM hashes, NTLM hashes through the Rainbow tables.

Analyze

LM hash and NT hash

LM hash is the oldest password storage used by Windows. Due to the limited charset allowed, it could be easily cracked. Users or attackers could obtain a password from the SAM database on a Windows system. Some older systems may still use LM hashes. So, in my demo, I will also provide LM hashes to crack.

NT hash is the way that modern Windows systems store the passwords. It uses NTF-16 and MD4 encryption.

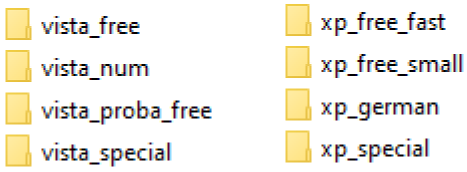
Rainbow table

A Rainbow table is a huge pre-computed list of hash values for every possible combination of characters. A password hash is a password that has been processed by a mathematical algorithm, such as MD4 or DES, and transforms the password into a meaningless string. A hash is usually one-way encryption, so there is no way to get the original string from the hashed string once the string is hashed. A Rainbow table uses a pre-computed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash. Because one string can produce the same hash, so as long as it produces the same hash as the original password, it then cracks the password.

Rainbow table password chain

There are many chains in the Rainbow table. For example, I want to create a password chain of “12345678” using MD5. First, I pass the string to the MD5 hash function and generate a hash. Then I reduce the hash by taking only the first eight characters and re-hash these eight characters. Then I repeat this step with different characters until I have enough hashes for a chain. Finally, I store the chain into a table, and this will be a password cracking chain in a Rainbow table.

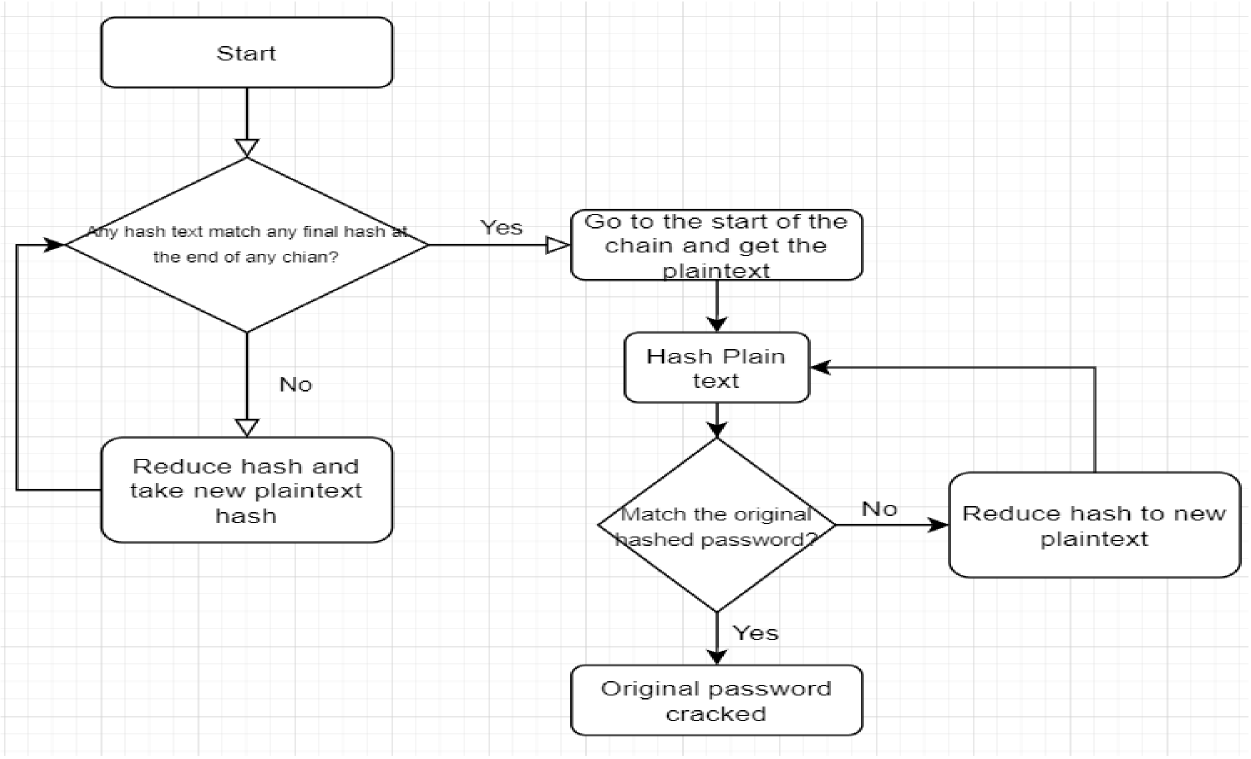
Ideally, the more comprehensive the Rainbow tables are, the higher the chance users could crack the password. For this exercise, I download 8 Rainbow tables. Although those tables are not comprehensive enough, it could crack easy passwords like “password,” “123456,” instantly.



vista_free
vista_num
vista_proba_free
vista_special
xp_free_fast
xp_free_small
xp_german
xp_special

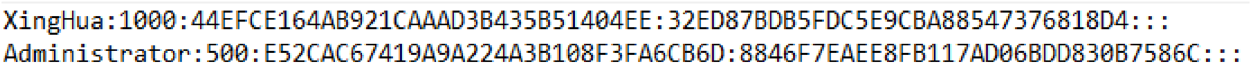
Cracking a password

To crack a password, a Rainbow table checks if the hashed password exits directly in the table. If nothing matched, it goes to the start of the chain and starts hashing until a match. When the match is found, the password is cracked. Otherwise, the password is not cracked.


Start
Any hash text match any final hash at the end of any chian?
Yes
Go to the start of the chain and get the plaintext
No
Reduce hash and take new plaintext hash
Hash Plain text
Match the original hashed password?
No
Reduce hash to new plaintext
Yes
Original password cracked

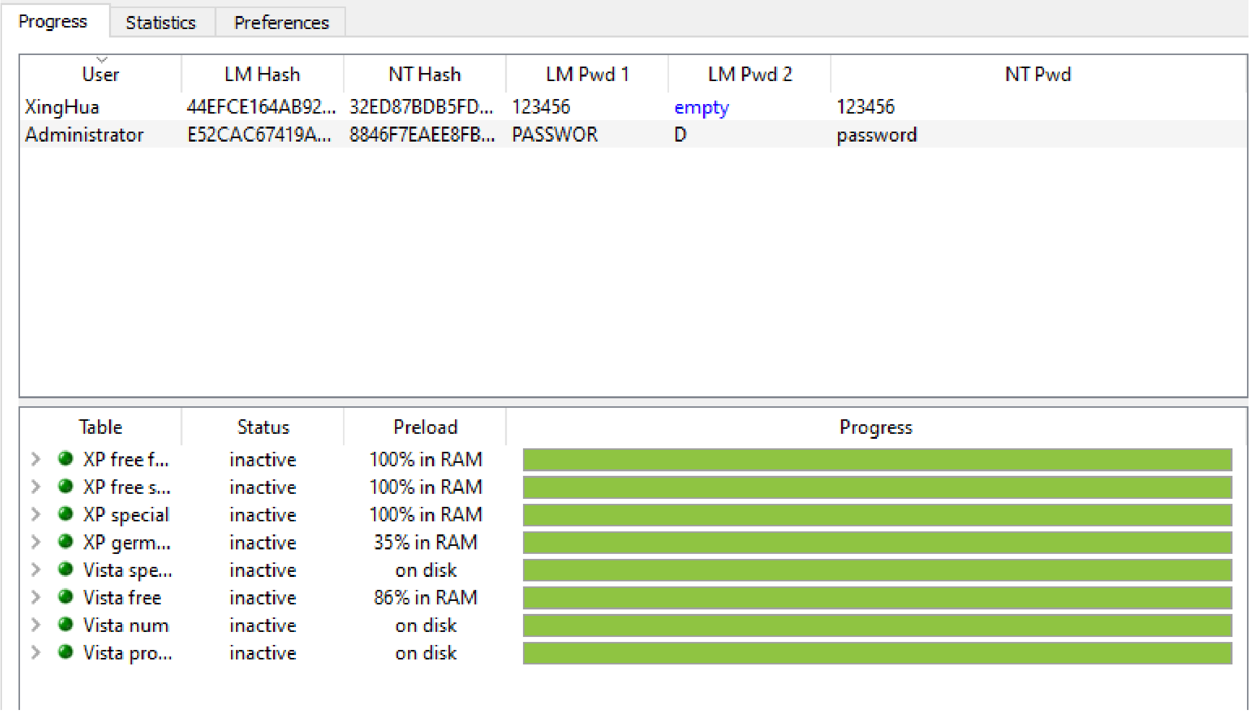
Ophcrack

Demo



```
XingHua:1000:44EFCE164AB921CAAAD3B435B51404EE:32ED87BDB5FDC5E9CBA88547376818D4:::
Administrator:500:E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:::
```

I have a pwdump file obtained from my system, and I modified the hash for this exercise. The English characters on the left are the user names. The following numeric values indicate what authentication level of those users. For example, 1000 is a guest and 500 is the administrator. Then it follows by an LM hash and an NT hash by order. Sometimes there is no LM hash because some systems nowadays do not use LM hash anymore.



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
XingHua	44EFCE164AB92...	32ED87BDB5FD...	123456	empty	123456
Administrator	E52CAC67419A...	8846F7EAEE8FB...	PASSWOR	D	password

Table	Status	Preload	Progress
● XP free f...	inactive	100% in RAM	🟩
● XP free s...	inactive	100% in RAM	🟩
● XP special	inactive	100% in RAM	🟩
● XP germ...	inactive	35% in RAM	🟩
● Vista spe...	inactive	on disk	🟩
● Vista free	inactive	86% in RAM	🟩
● Vista num	inactive	on disk	🟩
● Vista pro...	inactive	on disk	🟩

Then I use Ophcrack and install all the Rainbow tables I have downloaded, and load the pwdump file for cracking. After processing through the Rainbow tables, “123456” and “password” are pre-computed hashes in the table. So, the original plaintext password is cracked.

Conclusion

Pros and Cons

Because Ophcrack uses the Rainbow tables where pre-computed hashes, so it is faster since it only needs to search and compare hashes. Ophcrack also automatically distribute the usage of computer RAM, which boosts the cracking performance a level up. However, because Rainbow tables need to store pre-computed texts and find the matches, they always require huge storage for storing Rainbow tables.

Prevent

Ophcrack can be installed on a portable drive, and your system data files could be hacked through backdoor Trojans. Users should avoid using any unreliable portable drive and avoid downloading any source-unknown application online.

Because passwords are hashed in the same way, so the same password used by different users will be easily cracked. Users should try to use long, complex passwords. Also, users can prevent this by using password salting. A salt randomizes each hash by adding random data that is unique to every user to their password hash. Therefore, the same password will have a different hash. This will lead to no match in the Rainbow table even the password is the same.

In addition, users could avoid using outdated hashing algorithms like MD5 because many rainbow tables contain hashes transformed by those algorithms.

Reference

ParthDutt. (2018, June 10). Understanding Rainbow Table Attack. Retrieved October 21, 2020, from https://www.geeksforgeeks.org/understanding-rainbow-table-attack/