COMP 8506 Assignment 4

Password Cracking - John

Xinghua Wei

A00978597

John

Introduction

John the Ripper is a great tool for cracking passwords using some brute force attacks like dictionary attack or custom wordlist attack. It is even used to crack the hashes. In this exercise, I will be crack a password from a Windows 10 pwdump file.

Analyze

Pwdump file

```
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 usernames. 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.

Cracking

Because the pwdump file already contains hashes, and I do not need to unshadow it. If the user need unshadow a file, use

Unshadow /etc/passwd /etc/passwd > <file directory>

```
john --format=NT --rules -w=/usr/share/wordlists/rockyou.txt ~/t
```

The format of pwdump hash is NT hash, and LM hash, which john can detect which hash it is, and I have specified the hash format to NT. Then I use pre-installed password lists call rockyou.txt that contains a list of commonly used passwords.

```
PASSWOR          (Administrator:1)
123456           (XingHua)
D                (Administrator:2)
```

It cracks the correct password and shows it on the command line.

Defence

Like Ophcrack, John is an off-line cracking tool, which makes it hard to detect. But user can still defence their password from being cracked.

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.

Users could also modify the authentication level of their files. For example, /etc/passwd in Linux is a file that every user can access. Users should prevent that file from being accessed by others other than the admin itself.

Users could also use PowerShell or other tools to pull all active accounts. Then users would know what computers are logged in and how many are on the same network to detect unknown connections.

Conclusion

John the Ripper is a great tool for cracking passwords using some brute force attacks like dictionary attack or custom wordlist attack. It is fast and efficient if attackers have useful lists of passwords or password dictionaries. Since it is an off-line cracking tool, it is also sneaky and hard to detect for regular users. However, users can still prevent such action by using uncommon, long and strong passwords. Or modify their password hashes for better security.