U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE®
PROGRAM

CyberForce® 101

John the Ripper

October 2023

cyberforcecompetition@anl.gov

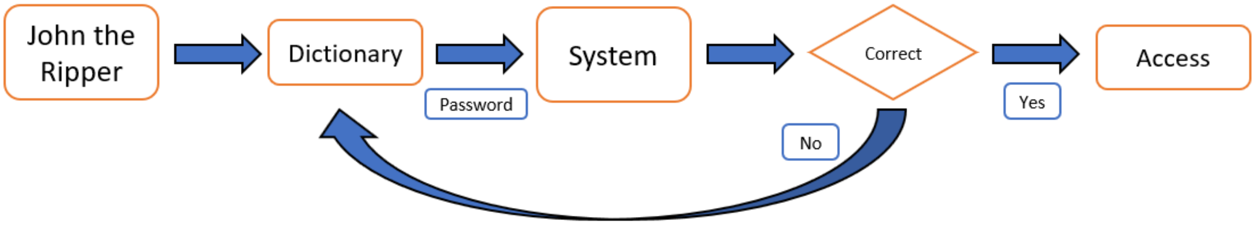
John the Ripper 101

John the Ripper

John the Ripper is a free password cracking software that uses a combination of attacks. It has gained popularity because it has multiple modes to launch more specialized attacks. It also has options for many different skill levels. The most common attacks launched by JTR are dictionary and brute force attacks.

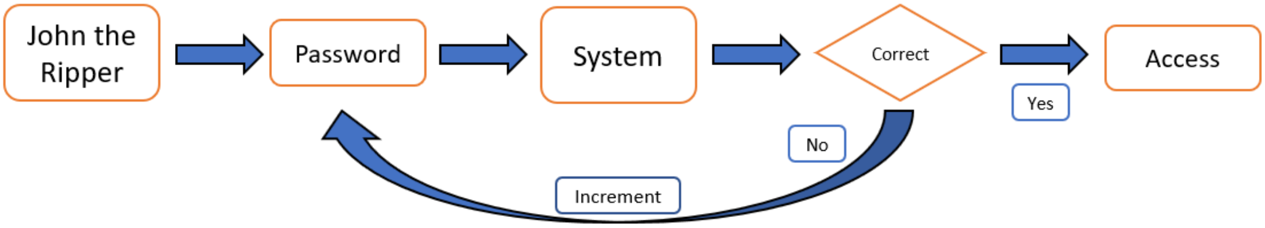
Types of Attacks

A dictionary attack is when the software uses a pre-determined dictionary (list of words/phrases) as possible passwords. It enters each item on list and compares its hash to the hash of the correct password stored on the system (This is not a rainbow table!). The dictionary may be a list of the most popular passwords or have something more specific to the person/people who created the password. When JTR does this it is in Wordlist Mode.



John the Ripper can also use rainbow tables to crack passwords. A rainbow table is a collection of plaintext passwords and their hash. They are more efficient than a dictionary attack because it eliminates the need to actually hash the passwords. All JTR needs to do is compare the hashes and return the plaintext version of the correct hash (the password is stored in the rainbow table).

A brute force attack is when software systematically tries every possible combination of characters until it finds the password. When JTR does this it in Incremental Mode.



John the Ripper also has Single Crack Mode. This is when it uses the names of files, dictionaries and other information in the system to base its potential passwords on. This is the most common starting spot if the user is attempting to crack a single password at once.

Installation and Wordlist Tutorial

To install John the Ripper download it and enter the command:

```
sudo apt-get install john
```

To start john on Wordlist Mode, enter the command:

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.txt
```

/usr/share/wordlists/ is the location of the file rockyou.txt which holds the list of potential passwords. The name and location of files with the potential passwords will vary from system to system.

--format=raw-sha1 crack.txt is used to format the results and put them in a text file for documentation and future access. This is important if a report needs to be filed or the results need to be used later. Otherwise, the results will be deleted when the terminal is closed.

Sources

- John The Ripper | Bugcrowd
- John the Ripper - cracking modes (openwall.com)
- John the Ripper - command line options (openwall.com)
- How to Crack Passwords using John The Ripper – Pentesting Tutorial (freecodecamp.org)

Additional Resources

- https://www.golinuxcloud.com/john-the-ripper-password-cracker/#Wordlist_Cracking_Mode
- https://www.youtube.com/watch?v=XjVYI1Ts6XI