A Password Cracking Tutorial Using John the Ripper

UNO CTF

Contents

1 John Installation

If you haven't installed John before, you (on a Debian style distro such as Ubuntu) can run the command "`sudo apt-get install john`" to install the tool. You will probably need to provide your password in order to do so.

2 Unshadowing the Password File

1. On modern Linux systems, password hashes are no longer stored in the `/etc/passwd` file. Instead, these are stored in the `/etc/shadow` file, which is only readable by root, and the two files must first be combined in order to crack password hashes. John is provided with a tool used to do this, called "`unshadow`". To use `unshadow`, you simply provide the password and shadow files to it: `unshadow [password-file] [shadow-file]`. You'll probably need to run this command with sudo (`sudo unshadow [password-file] [shadow-file]`) for it to succeed due to the permissions of the `shadow` file.

2. The first step prints out the combined unshadowed file to the terminal, so you'll want to run the unshadow command again, this time running "`sudo unshadow [password-file] [shadow-file] > unshadowed`". This redirects the output of the `unshadow` command

to a file titled "`unshadowed`" in your current working directory, saving it that way.

3 Cracking Passwords

1. Finally, you can run "`john unshadowed`". This may take a minute, but when it finishes, if it succeeded, it will have printed the decrypted password of each user alongside the relevant username.