-1John The Ripper:
An Illustrated Guide

By Ethernet

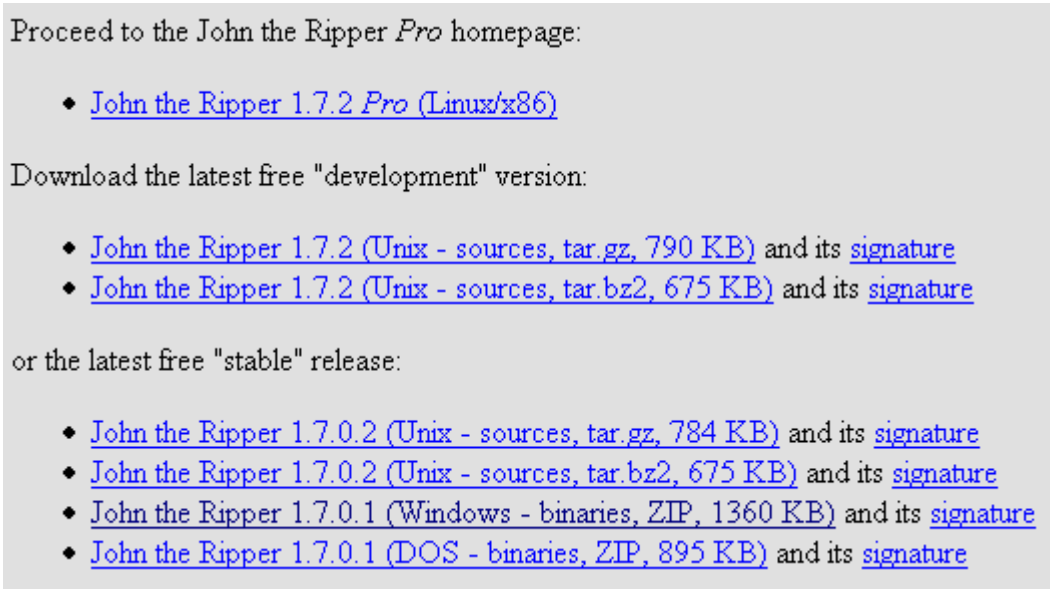
www.Securitydb.org

Contents:

Whenever we attack a website, run an exploit or otherwise, we can encounter something called a 'hash'. Hashing is a technique which uses highly complex algorithms to change a plaintext password into an unreadable string on numbers and letters. 574AB36AA9A7AA4025D6B40EEBB1AA69 Is what the text "Ethernet" looks like in, the commonly used, MD5 hashing algorithm. The most important thing to remember about hashes is that they are, what's called, 'one way'. Meaning you cant just reverse them to view the plaintext. So, how are we going to crack this hash? Simple - a hash breaking program called John The Ripper (JTR)[Download].

The program can crack several algorithms,
DES/BSDI/MD5/BF/AFS/LM
Using two methods, Brute Force and a Dictionary Attack.

Please note, when I use the term 'crack' we aren't technically 'cracking' anything. How these attacks are carried out will be reviewed later in the appropriate section.



Proceed to the John the Ripper *Pro* homepage:

- John the Ripper 1.7.2 *Pro* (Linux/x86)

Download the latest free "development" version:

- John the Ripper 1.7.2 (Unix - sources, tar.gz, 790 KB) and its signature
- John the Ripper 1.7.2 (Unix - sources, tar.bz2, 675 KB) and its signature

or the latest free "stable" release:

- John the Ripper 1.7.0.2 (Unix - sources, tar.gz, 784 KB) and its signature
- John the Ripper 1.7.0.2 (Unix - sources, tar.bz2, 675 KB) and its signature
- John the Ripper 1.7.0.1 (Windows - binaries, ZIP, 1360 KB) and its signature
- John the Ripper 1.7.0.1 (DOS - binaries, ZIP, 895 KB) and its signature

---

d[ownload] http://www.openwall.com/john/John The Ripper is supported on several different platforms, including windows and *nix systems.

When Will I Use John The Ripper?
[1a]

"When will I actually have to use this (amazing) software?" you ask? There are three (main) times that you will use this program.

[1] Cracking an .htpasswd file.
These files carry within them the administrative password for a given file.
They are encrypted in the DES algorithm, for the most part.
Once cracked you have full reign over the files/folders it was protecting.

[2] Cracking an MD5 Hash For a Database
When viewing a hacked database backup you will be viewing the passwords encrypted in the MD5 algorithm.
When using exploits that retrieve administrative hashes via SQL Injection etc.

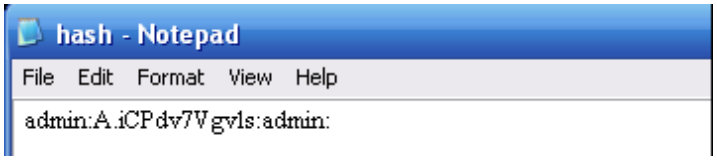
[3] To send/receive secret messages
You can easily encrypt important text with MD5, provided you have the answer in a wordlist.
Looks like gibberish to the casual viewer.

In all three of the above examples you will require John The Ripper at one point or another. Each method will be outlined for us in the following sections.

Getting Ready To Crack
[2a]

Before actually carrying out the password attack we must first follow a couple simple steps to 'prep' our hash for John The Ripper.

First off we must put our hash into a text file for John to read off of. For this demo I will be using a DES hash, but the same method is applied to all others. My text documents includes the following DES hash:
admin:A.iCPdv7Vgvls:admin:
I now name this 'hash.txt', as shown below.



Save it and we can move on to the next section.

Brute Force Attack
[2b]

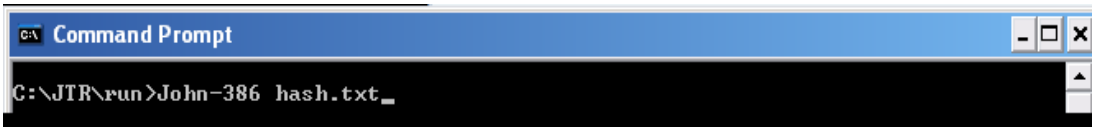
The first method of attack we will be looking at is, what's known as, a Brute Force attack. This attack works by our program producing a hash and seeing if it equals the hash we are trying to crack. So…

900150983CD24FB0D6963F7D28E17F72 (abc) !=
574AB36AA9A7AA4025D6B40EEBB1AA69 (unknown)

574AB36AA9A7AA4025D6B40EEBB1AA69 (ethernet) ==
574AB36AA9A7AA4025D6B40EEBB1AA69 (unknown)

Since the program 'knows' what it generated we can see, if the hashes are equal, what the unknown hash is.

In John The Ripper we execute a brute force attack like so:



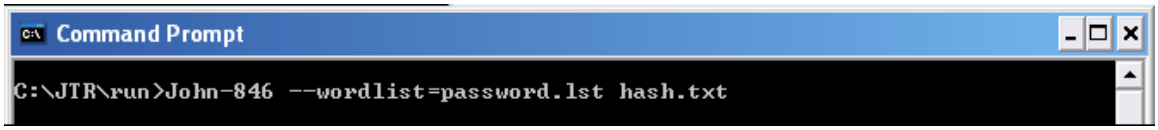
This command string 'John-386 hash.txt', where hash.txt is where the hash is stored, will run a basic Brute Force attack on the hash. Luckily for us we can make this command much more specific with some of the following commands:

--format=Hash Type - If you know the hash type you can add the string --format=DES.
--single - This command is used when you are only cracking one hash at a time.

Of course you aren't limited to these commands, they are just basics that are most often used.

Dictionary Attack
[2c]

This second attack we will look at is the Dictionary Attack, which takes words out of a dictionary file, hash them, and compare them to the unknown hash. John The Ripper comes with quite a nice password list (password.lst). A basic dictionary attack against a hash located in hash.txt might look something like this:



We use the --wordlist tag to specify a Dictionary Attack and we follow that with the word list we wish to use. If the password is contained in the word list it will be cracked in seconds, depending on the size of the word list.

Keep in mind that all the other flags I showed you in the Brute Force section still apply (like --format etc).

Conclusion
[0b]

This concludes the quick illustrated tutorial brought to you by Ethernet. I hope you are now able to harness the power of this great tool to accomplish many hash cracking ventures.

~Ethernet