

Lab Assignment 6

Cracking Passwords

1. Objective

In this lab, you will experiment with cracking some passwords with a popular password hacking tool, “John The Ripper”. You will learn how to crack weak passwords with “john” and how to create stronger passwords, and increase the complexity of the password cracking process time/space.

2. Lab Environment

We will use our VMs as our test environment for “John The Ripper”. This tool can be configured to crack passwords efficiently. One objective of this lab is for you to determine the parameter values that will make the tool crack passwords within a short period of time (e.g. within one minute or less than 10 minutes.) As you are trying to discover which parameters lead to efficient cracking, you may want to use the tool on your own personal machine, or on our lab machines. This will prevent us from consuming too many Jetstream resources.

Please go to the link <http://www.openwall.com/john/doc/EXAMPLES.shtml> and read about john-the-ripper’s features and usage.

Please go to the link <http://www.openwall.com/john/doc/RULES.shtml> to learn about word mangling rules.

2.1 Install John the Ripper

These instructions is designed to guide students who want to setup John on the Jetstream infrastructure. If you want to install it on a different machine, you may need to tweak some instructions but mostly the installation steps should be the same in any Linux machines.

John the Ripper (<http://www.openwall.com/john/>) is a useful tool for cracking password hashes. You will need to download and install John the Ripper in your home directory on your client VM.

- On the Jetstream VM
 1. Use apt-get

```
apt-get install john john-data
```
- On another linux machine
 1. Download the tarball

```
wget https://www.openwall.com/john/j/john-1.8.0-jumbo-1.tar.gz
tar xzf john-1.8.0-jumbo-1.tar.gz
```
 2. Compile and install

```
cd john-1.8.0-jumbo-1/src
./configure && make
```

2.2 Download Hashes

Get your assigned password hash file from the following link:

http://homes.sice.indiana.edu/dingchan/B544/<your_IU_username>_1

There are 4 password hash files that you need to download and they have the following formats:

<your_IU_username>_1

<your_IU_username>_2

<your_IU_username>_3

<your_IU_username>_4

You should use command *wget* to download all these four files.

3. Basic Usage

3.1 Hash data and its format

The password hash data that you will deal with is created by “htpasswd” which is the password utility in the apache package. It uses the md5 hash by default. We used the same hash function. It is possible to switch the hash function with an option on htpasswd. (e.g., htpasswd -d -c <password_file> <username>. This option uses DES and if you want to know more details, as usual please refer to its manpage).

The output of htpasswd is composed of the username and hash:

dingchan:\$apr1\$WW.gIL4e\$YvnOtheCWyrkRQ99RgRJ9

3.2 Basic John command

john <password file>

4. Password Cracking

4.1 Hash data and its format

You need to crack all four hashes you have downloaded using john-the-ripper.

4.1. [1 point] The first hash (<your_IU_username>_1) is very easy to crack because the password used to generate this hash is a word taken from the john-the-ripper dictionary. You should be able to crack the password using the command in Section3.

4.2. [4 points] The second hash (<your_IU_username>_2) is a bit more complicated than the first. The password used to generate this hash is made up of a word from the john -the-ripper dictionary plus a two-digit number. For example, if apple is a word from the john-the-ripper dictionary, a possible password that fits the above description is apple45. Please read all instructions below to determine how to configure John the Ripper to crack this new password file.

4.2.1. You will not be able to crack this password by using the default configuration of john-the-ripper. You can verify this by running the command in section 3 for the second hash file (<your_IU_username>_2). However, this will run a long time before giving up, so please kill the process by pressing “q” or Ctrl-c after a minute or so to avoid over-consumption of VM’s CPU.

4.2.2. In order to crack this password we have to create a rule, which mangles the words in the dictionary to meet the above description, and add it to the /etc/john/john.conf file.

4.2.3. The rule `[$[0-9]$[0-9]` basically asks john-the-ripper to append each word in the dictionary with two numbers (each between 0 and 9) before checking to see if it was used to generate the hash.

4.2.4. Please make a backup copy of the `/etc/john/john.conf` file before making changes to it. You can create a backup copy of `john.conf` by using the following command: `cp john.conf john_backup.conf` (your current working directory should be `/etc/john/`).

4.2.5. At any point in the assignment, if you want to revert back to the original version of `john.conf` file, you can implement the following command:

```
cp john_backup.conf john.conf
```

4.2.6. We can now add the rule under `[List.Rules:Wordlist]` (line 217) in the `/etc/john/john.conf` file. We suggest you to add the rule right below `[List.Rules:Wordlist]` so that john-the-ripper runs this rule first (before checking for other rules).

Now you should be able to crack the password using the command in section 3.

4.3. [5 points] The password used to generate the third hash (`<your_IU_username>_3`) is very similar to second one except for a minor difference. This password has two numbers (between 1 and 2) after the first two characters and two numbers (between 1 and 2) at the end. Again, if apple is the word in the john-the-ripper dictionary the password would be something like `ap11ple12`. Generate a rule and add it to the `.conf` file. Now, try cracking the password using the command in Section 3. *Note: this may take more than 20 mins.*

4.4. [5 points] The fourth hash (`<your_IU_username>_4`) has been generated using a word from the Dutch dictionary. You will have to download the Dutch dictionary from

<ftp://ftp.openwall.com/pub/wordlists/languages/Dutch/1-clean/lower.gz> to crack this password. Please read the following commands.

4.4.1. Download the file using the command `wget`.

4.4.2. Gunzip the file using the command `gzip -d lower.gz`

4.4.3. Rename the file from `lower` to `dutch` by using the command `mv lower dutch` and copy the file in directory `/etc/john/`.

4.4.4. Now crack the password by giving the Dutch word list as input to john-the-ripper.

Dictionaries for other languages can be downloaded from:

<ftp://ftp.openwall.com/pub/wordlists/languages> .

5. Questions: [15 points]

5.1. [3 points] Explain how a “white hat” security professional might use john-the-ripper to make her institution more secure.

5.2. [3 points] Why can john-the-ripper crack the passwords even though they are not in a form that is directly readable?

5.3. [3 points] Explain how John the Ripper limits/reduces password cracking time?

5.4. [3 points] What system policies for passwords would make user passwords considerably harder to crack by a password cracker such as john-the-ripper? What are the downsides of enforcing such policies?

5.5. [3 points] How much does a salt of size N increase the processing required by precomputed dictionary offline attacks?

6. Submission:

You must submit to canvas your write-up which includes: a) the passwords cracked in the Section 4 along with the rules you used and b) your answers to the questions in the Section 5.