SEC 150 Assignment: Cracking Passwords

Titus Barik (tbarik@staff.waynecc.edu)

Version 1.0

1 Assignment Description

In this assignment, you will crack encrypted passwords from a sample Apache `.htpasswd` web server file using the password cracking tool John the Ripper (JTR). JTR is a very general tool; it can be used to crack Solaris DES passwords, FreeBSD MD5 passwords, Windows LM passwords, and more.

Upon completion of this assignment, you will have knowledge of how to crack passwords for a variety of applications and operating systems, using brute-force and more sophisticated techniques such as word lists and rule mangling.

2 Pre-Requisites

Before starting this assignment, watch the lecture video on John the Ripper.

3 Warm-Up

If we know that a password is two lowercase letters, we can say that the first character can have 26 possibilities (a through z). The second character can also have 26 possibilities. So the total possible two lowercase letter passwords is $26 \times 26 = 676$. Quite hard to guess by hand, but trivial for a computer!

Complete the following questions and submit them in a file called `warmup.txt`:

1. Given a PIN number that is 4 digits, how many PIN combinations are possible? (Examples: `0000`, `0101`, `5823`, `9981`).

2. Given a password that has four lowercase letters, how many password combinations are possible? (Examples: `abcd`, `hylx`, `zzyx`, `alcb`).

3. Given a password that contains a total of four lowercase and uppercase letters, how many password combinations are possible? (Examples: `aBcD`, `HYLX`, `zzYx`, `ALcB`).

4. Given a password that has only lowercase and uppercase letters, with a maximum length of 4 and a minimum length of 1, how many password combinations are possible? (Examples: `a`, `aB`, `zzz`, `zjJq`)

You should be able to see that increasing the password requirements only slightly has a dramatic effect on the number of possible combinations; this is why many companies require numbers, capitals, or punctuation in their password requirements.

4 Instructions

1. Run `john-mmx --test`. Make note of the test results for Traditional DES. Note that `c/s` is (roughly) the number of passwords guessed per second. For even moderate desktop computers, this number is easily over 500,000 password attempts per second.
2. Run `john-mmx .htpasswd` for a long period of time. Most passwords will be cracked fairly quickly using the default word list found in the file `passwd.lst`.
3. The password for `harper` is somewhat difficult, but will eventually found by this technique within a few hours.
4. The password for `everett` is quite difficult; it requires brute-force by requires JTR to run continuously for several days.
5. The password for `barik` can easily be obtained, but requires the use of a wordfile. If we know that barik likes mythology, then we should apply the `mythology-legends` file (using `--wordlist=mythology-legends`) with rule mangling `--rules` to obtain his password.

Hint: You can use the `--session` parameter to resume password cracking in case you cannot leave the system running for an extended period of time. For example, you can use `john --session=sec150 .htpasswd` to save the session as `sec150`. Then, you can hit `CTRL + C` to abort JTR. You will find a `sec150.rec` file in your directory. When re-run with the `--session sec150` parameter, JTR will resume from where it left off before by using this file.

5 Milestone

Submit a screen capture showing JTR running on your local system.

6 Submission

Submit the output of `john --show .htpasswd` as `found.txt`. You will receive points based on the number of passwords that you were able to discover. In addition, submit your work and answers to the warm-up exercises in a file called `warmup.txt`.