Password Cracking

Adrianna Holden-Gouveia
Website: https://aholdengouveia.name
: aholdengouveia
: aholdengouveia
: aholdengouveia

Objectives:

1. Learn how password cracking works
2. Make better choices with your passwords and hopefully share this knowledge with others

Complete the following problems

This lab is about password cracking. You are going to use John the Ripper. This lab needs to be done through your Kali virtual machine

First we're going to practice using Kali on a list of passwords I'm giving you, it's called "passwords.zip" and contains a file called "crack-these-please"

1. Download the "Passwords.zip unzip. You need to make sure this file is unzipped and in your Kali virtual machine. This should have 50 users with various passwords not in plain text. Look at your unzipped crack-these-please file using cat, what's it look like?
2. John the Ripper is a command line tool. Check under "usage example" to see what this looks like when it's run `http://tools.kali.org/password-attacks/john` If you run into any problems or need to troubleshoot go to John's homepage at `http://www.openwall.com/john/`

3. A dictionary attack uses a word database, and tries it repeatedly. John the Ripper has this capability. Find one of the dictionaries included in Kali, either password.lst or RockYou, Where did you find them? Dump the file's contents to the screen and then take a screenshot, use the command more. Press the spacebar, or hold it down, to make the display advance to the end of the file. You see that it is a list of potential passwords.

4. Enter the following command to launch a dictionary attack: john –wordlist="dictionary" crack-these-please Where "dictionary" is the dictionary you've chosen, no quotes. Take a screenshot showing how many of the 50 passwords it was able to crack, what they are, and the time it took.

5. John has created a list of solved passwords called john.pot. Find that file and take a screenshot of that filed open. You see the same passwords you did before. But previously they were displayed along with the users who own them, now with their hashed versions. The hashed versions were the input to John's process; that's what got cracked.

6. In default usage John the Ripper executes dictionary, hybrid, and bruteforce attacks in combination. Launch a combination attack by executing: john crack-these-please

7. While john is working, examine the CPU utilization of your computer. Take a screenshot of it.

8. Let John run long enough to do some more cracking. Note the time it took and how many additional passwords it was able to crack. Also note what the passwords are. The simpler ones should have been cracked in the earlier attempts, the ones that are being cracked now should be less simple passwords Getting all the passwords can take awhile, so if it is taking too long, you can hit CTRL-C to stop the run.

Making your own file of passwords to share with others

1. Making your own password files Kali includes a utility called htpasswd to make your own password files.

2. htpasswd takes several commands, including:

- -c Create a new file.
- -m Use MD5 hash.
- -s Use SHA hash.

3. So the command "htpasswd -cm [passwordfile] [username]" without quotes or [], would create a new file called passwordfile, and adds a user named username to it.

4. If you wanted to add another user, you would enter "htpasswd -m [passwordfile] [username]"

5. Make sure you are adding users to the file not recreating the file every time. You only need the -c option the first time you are making the file.

Deliverables

1. Write how many passwords you cracked, what they were and how long it took you from step 2. To show the passwords you have cracked in your files use the -show option with john. Make sure you remember to pass john your password file.

2. Take a screen shot of your CPU utilization. With the hybrid attack, how many more passwords were you able to crack? What were they? How many of the cracked passwords contain varied combinations of letters, symbols, numerals, and case? Do the cracked passwords tend to be long or short?

3. Try running john -test What happened? What do you think this could be useful for? What does your research say? Don't just guess what -test does

4. Using htpasswd try making a password file with only a single user, and use a dictionary word as the password. Then make another file with the same user and password, but use MD5 hash. Then run a dictionary attack on both of them. Which one takes longer? Why do you think that is?

5. Using htpasswd and a SHA and md5 option make a file of at least 10 usernames with passwords that are easy (12345) to difficult (fjkwrhrT!@!) and switch with another student on the discussion board. Make sure to include at least 2 of each type.

    - Don't tell them your passwords.
    - Use John the Ripper to crack the password file they gave you
    - Pass in the name of the student you switched with along with the file they gave you, how many passwords you were able to crack, which ones, and how long it took you.
    - Include what you had to do differently to get more passwords (hint: did you have to change the –format to something else?)

6. Your report must include your passwords, the passwords you cracked and answers to all the questions asked in the lab and all screenshots requested.