Authentication Lab – Cracking Passwords

1 Overview

The objective of this lab is to understand how UNIX handles passwords and the techniques that an attackers can use to crack them. In this lab students will use a tool called "John the Ripper" to crack the passwords stored in a file. Unix stores hashes of all its accounts' passwords in a single file i.e. `/etc/passwd` on old systems and `/etc/shadow` on new ones. Students will recover passwords using different techniques.

2 Lab Environment

Virtual Machine. Ubuntu can be downloaded from
https://drive.google.com/open?id=0BxtCKJljOE-NUnY0VGMwaDdyRTA

User Accounts Information. `crack-these.txt` can be downloaded from
https://drive.google.com/open?id=0B9Zd9LxSunxjMkEwd1EyQTZtZnc

Installing John the Ripper: Please download file `john-1.8.0.tar` from Moodle or run `sudo wget http://www.openwall.com/john/g/john-1.8.0.tar.xz` at terminal. Your downloaded file should be in `~/Downloads`; now run the following commands to install `john`.

```
% cd ~/Downloads
% sudo mv john-1.8.0.tar /opt/
% cd /opt
% sudo tar xvf john-1.8.0.tar (use -xvzf if file is tar.gz)
% cd john-1.8.0
% cd src
% sudo make
% sudo make clean generic
% cd ../run
```

If everything goes well, this will create the executables for John and its related utilities, and you're ready to crack passwords.

3 Lab Tasks

3.1 Task 1: Understanding UNIX password handling

Files `shadow` and `passwd` contain user's accounts information, `shadow` has more restrictive permissions than the `passwd` file. Run following commands and examine both files, note the permission restrictions and compare the contents of the files. Why do you think `shadow` file is more restricted than `passwd`?

```
% ls -l /etc/passwd
% ls -l /etc/shadow
% cat /etc/passwd
% cat /etc/shadow
```

In `shadow` file, find your user name and hashed password, an example is shown below

```
ahsan:$6$ViV1fAdR$7J7WsQhS7DpqPqGQQtYqnoLsOm4J0Ixd0WLnU0EN5
jywHCsdhk2qAEgfWdUOso4Hy0VElMsZklDeZlGN3ZG.Q1:16579:0:99999:7:::
```

We are looking for hash of the password, which is second field.

```
$6$ViV1fAdR$7J7WsQhS7DpqPqGQQtYqnoLsOm4J0Ixd0WLnU0EN5jywHCsdhk2qAEg
fWdUOso4Hy0VElMsZklDeZlGN3ZG
```

1. The first field (numerical number) indicates the type of hashing algorithm used

   $1 = MD5
   $2 = Blowfish
   $2a = eksblowfish
   $5 = SHA-256
   $6 = SHA-512

2. The second field is the salt value

   The salt is used to ensure that users with the same password will most likely not have the same encrypted password, and it also strengthen the password.

3. The last field is the hash value of salt + user password

To complete this task: identify number of users in your system (you can add more users with `adduser` command), what hashing algorithms they are using and what are encrypted salt and password values.

3.2 Task 2: Cracking Passwords

We will be using the password cracking program John the Ripper for this task. The basic functionality of John the Ripper is to repeatedly try different passwords and hash them until it finds one which matches the hash of the password we are trying to crack. We will use three techniques to crack passwords in this lab, dictionary attack, hybrid attack and combination attack.

1. **Dictionary Attack:** Since the number of passwords could be infinite, brute force attack (testing all possible passwords) will not be a feasible solution unless the password was very short. Instead, we will be more clever by trying a list of more likely passwords first. This is called a dictionary attack. John the Ripper comes with a small dictionary of some typical passwords located in `/opt/john-1.8.0/run/password.lst`. Take a look at it!. Please download `crack-these.txt` (in `Downloads` folder) file from the provided link which contains account information for 50 users. Now run the following commands to perform the dictionary attack

```
You must be in /opt/john-1.8.0/run/ to run this command
  % sudo ./john -w:password.lst  ~/Downloads/crack-these.txt
```

John has created a list of solved passwords in a file `john.pot`, run `cat /opt/john-1.8.0/run/john.pot` to see it. How many of the 50 passwords it was able to crack, what are they, and the time it took?

2. **Hybrid Attack:** A hybrid attack checks for variations of a word or a combination of dictionary words. For example, we could make it append numbers to the end of all the words in the dictionary, such that if the word cat was in the original dictionary, then it would also try the words cat0, cat1, . . . , cat9, cat00, cat01, etc. The transformations is determined by a set of rules found in the configuration file `/opt/john/john.conf`. Open the file (e.g. by running `cat /opt/john/john.conf` from the terminal) and scroll down to the line containing [List.Rules:Wordlist]. Every line underneath contains a transformation rule which will be applied to every word of the dictionary. The syntax of each rule line is as follows. First comes zero or more rejection rules, all starting with a hyphen, e.g. -c, -8, -s, etc. These are used to decide whether the rest of the transformation rules on the line should be applied to a word or not. You can just ignore these. Next comes the actual transformation rules themselves. For example the rule:

   <5 c r Q

   will only apply to words of length less than 5 (<5); and if so, then it will capitalize (c) and reverse (r) it. The Q command ensures that words that are not changed by the rule are not unnecessarily added to the dictionary. E.g., if cat was in the dictionary, then the above rule would make John the Ripper also try the word taC. To run this attack execute following commands

   ```
   You must be in /opt/john-1.8.0/run/ to run this command
     % sudo ./john -w:password.lst -rules ~/Downloads/crack-these.txt
   ```

   How many more passwords did the hybrid attack crack? Is there any relationship between what it cracked this time, and those from last time? open `/opt/john/john.conf` file and have a look at rules.

3. **Combination Attack:** John the Ripper executes dictionary, hybrid, and bruteforce attacks in combination. Launch a combination attack by executing:

   ```
   You must be in /opt/john-1.8.0/run/ to run this command
     % sudo ./john ~/Downloads/crack-these.txt
   ```

   How many more passwords did the combination attack crack? how long did it take?
   You can add more passwords in `password.lst` file or download a larger file from internet, and try again above attacks.

4 Of optional interest

`hashcat` is another password cracker. Have a look at it!