SSN Cracking a standard Unix password

Remco Hobo

November 26, 2004

Preface

For this excercise, we had to crack a Unix password. Normally these passwords, even though they are hashed, are stored in a so called shadow file. This file is normally only readable by the root user, so other users can not read it. In this file, each user‘s password is stored like the following:
root:1VX1lHZHp$vSkuNiiztm584x7nuqgrm0:12730:0::::: For this excercise we will get two of these files, both send by our coordinator, and both signed by him. We have to check which of the two files is more trustworthy and we have to crack both files to get the passwords.

Decrypting and cracking

I received two emails with two files, which I named 4remco1.asc and 4remco2.asc. The first step is to decrypt these files

- gpg -d 4remco1.asc ¿ decrypt1
- gpg -d 4remco2.asc ¿ decrypt2

After this, both keys can be verified with

- gpg -verify decrypt1
- gpg -verify decrypt2

After this, both keys appear to be genuine, names, email addresses etc. are correct. We know that one of the keys is wrong. One of the things a person can do is make a key more trustworthy by letting other people sign it. Afer a little investigation, it turned out one key wasn't signed by anyone else and the other one was signed by a number of people who participate to the course. This way, I knew this was the right key.

After this, the right key had to be decrypted. For this, the program 'john the ripper' can be used to do a brute force attack. The given passwords are 'weak' ones. They occur in the dictionary. After a couple of seconds, the password was hacked.

Checking integrity of own Unix password

To test the strength of my Unix passowrd, I let john run for about two days but no password was recovered. My password is about eight characters long and consists of numbers and figures. This makes a password difficult to crack.

To make sure all users have a 'strong' password, automated passwords might be a good idea. This way, the user will get a password from the authorisation authority. Also, screening of passwords for weak ones may be a solution.

Getting passwords from other machines

There are several ways for a hacker to obtain passwords from other machines.

- Physical access: If a hacker can obtain physical access to the machine, it is very easy to obtain password information. This can be done by cracking the password lists, but installing a sniffer can be even more rewarding for the hacker.

- Security exploits: Many programs, open source or commercial, have security flaws. Especially programs that run under root preferences can be very internesting for hackers. Haacking one of these programs can yield root shell access.
- Social engineering: Normal users are very careless with their passwords. In a dutch test, users gave their passwords for a pen. They where offered a pen if they gave their password. A lot of people gave their passwords without hasitation.

References

[1] John the Ripper website, brute force cracker, `http://openwall.com/john`

[2] Openwall website, great site and resources for hacking, `http://openwall.com/john`