Adopted & modified from Herbert Bos's course on Network Security

Given:

• /etc/passwd file

• /etc/shadow file

• A dictionary file

Goal:

To recover as many user passwords as possible using a dictionary of words commonly used in passwords.

Use unshadow command (just like in John the ripper), that combines the contents of the /etc/passwd and /etc/shadow files to create a combined file called 'passwordfile.txt'. Your command to run will look like this.

Use Makefile to generate the executable

unshadow /tmp/password /tmp/shadow

Inputs to the C program is passwordfile.txt and the dictionary file

• To compile – use make

• To run - 'make runall'

The make runall command must automatically run

guessword –i hash.txt –d dictionary.txt –o all

guessword –i hash.txt –d dictionary.txt –o current

guessword –i hash.txt –d dictionary.txt –o root

HINT: Use getopt

Program Output

A text file called ‘allcrackpasswd.txt’ which contains a list of cracked passwords in the format

username:password

• How many passwords you cracked

• Time you took to crack those many passwords

• Can you improve on your time?

Program must :

• Be indented & documented properly.

• Be written entirely by yourself

• Use proper coding standards – if you don’t know what it is – google it. J

• Not invoke external programs

• Not use external libraries other than GNU libc and –lcrypt

• Compile and run on a standard installation of Ubuntu