

NETWORK SECURITY SPRING 2015

Renuka Kumar
amritanetsec@gmail.com



LAB-1

Programming Assignment-1

- 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.

Programming Assignment-1 Contd.

Write a `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`

Programming Assignment-1 Contd.

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

- Different txt files for each run
- E.g.
 - ‘allcrackedpasswords.txt’ will contains a list of all cracked passwords in the format
username:password

Programming Assignment-1 Contd.

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. ^
- Not invoke external programs
- Not use external libraries other than GNU libc and –
lccrypt
- Compile and run on a standard installation of
Ubuntu

Programming Assignment-1 Contd.

- Submit your code with a **short write** up in PDF format. The write up should include
 - Instructions on how to run your program.
 - Screenshot(s) of program output running on your terminal window in the writeup
 - If you have not finished your assignment, write what you have completed
 - **Zip the program and the pdf into a file of the form NetSec_<Assignment#>_<Name>.zip**
e.g. NetSec_1_Renuka.zip