ACROPOLIS
Enlightening wisdom

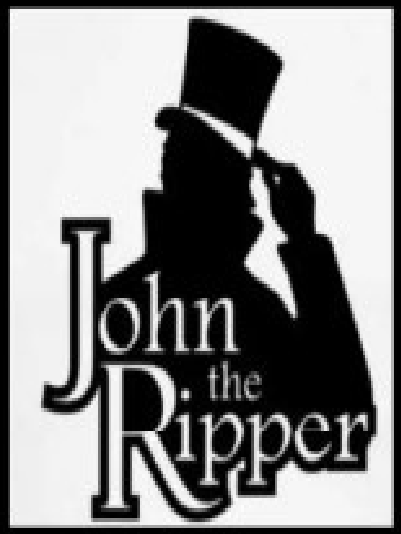
EVALUATION OF INTERNSHIP

CSIT
COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

SESSION : 2022-23

SUBMITTED TO:
Prof. Nidhi Nigam
Assistant Professor
CSIT Department

SUBMITTED BY :
Kratik Pandey
0827CI*201095*



JHON THE RIPPER

Definition

- **Password cracking** is one of the oldest hacking arts. Every system must store passwords somewhere in order to authenticate users. However, in order to protect these passwords from being stolen, they are encrypted. Password cracking is the art of decrypting the passwords in order to recover them.

What a program can do

- A password cracking program if used ethically can be used by the system administrator to detect weak passwords amongst the system so they can be changed. A password Cracking program is most likely used to check the security of you're your own system

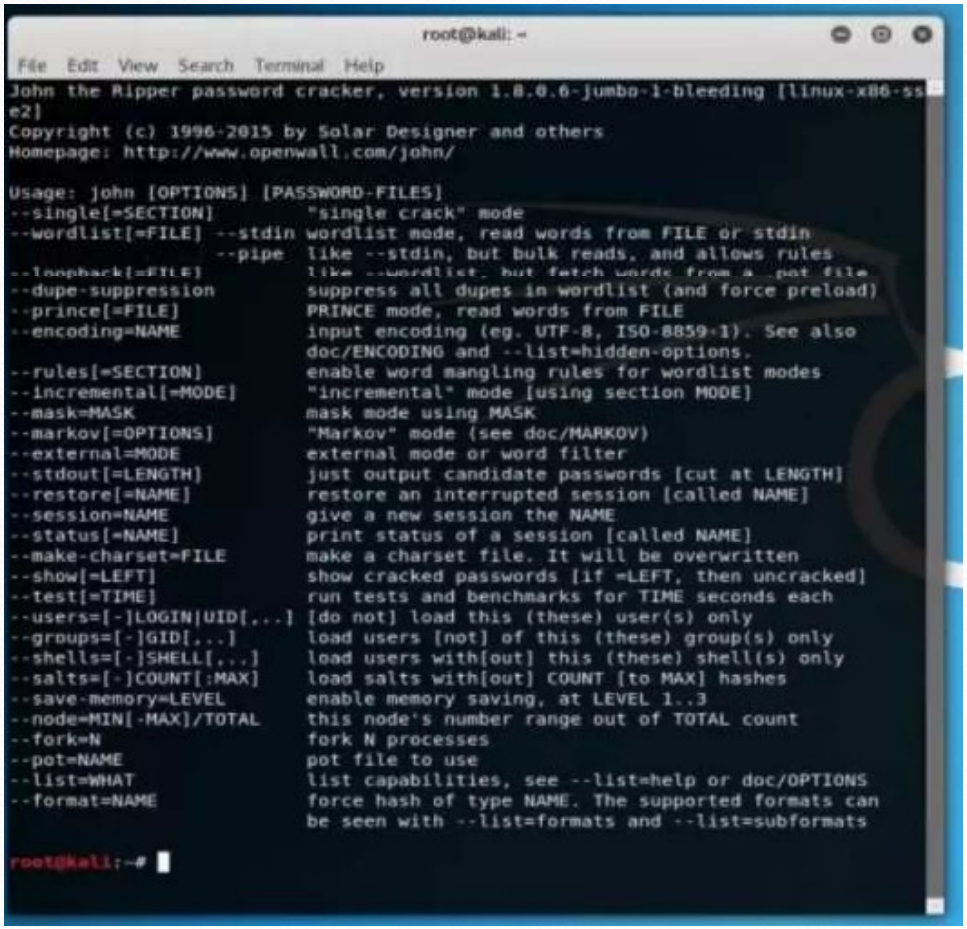
Crack

- Crack is a type of password cracking utility that runs through combinations of passwords until it finds one that it matches. It also scans the content of a password file looking for weak login passwords.

John the Ripper

- John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. (openfirewall.com)

Here are the commands for what john the ripper can do



John the Ripper

- In order to run John the Ripper, we went to a site and downloaded the documents for windows that gave instructions on how to run it. (this included the password file, and other documents about john)
- To run John, we did the following:

Start >Accessories>Windows Explorer>My computer>John>

- In the command prompt, we typed:

– cd c:\John\john171w\john1701\run

-dir

-john386pass

- This invoked John

Stages

- Though there are different types of password cracking utilities, most of these go through the same types of stages when trying to crack passwords:
- -tries common passwords, such as "password" or the name of the account in question
- -runs through all the words in the dictionary and lists of common passwords.
- -runs through all the words in foreign dictionaries and special "crack" dictionaries.
- -tries all combinations of letters out to a certain size, such as 5 letters.
- -tries all combinations of letters, upper/lower case, numbers, and punctuation out to a certain size, such as 3 characters

Our Results

- We used the program John the Ripper on a windows machine, using the command prompt
- We ran it 3 times, the first time 3 passwords were cracked, the second time none, and the third time two were cracked
- The simplest passwords were cracked instantly (i.e.: same password as username, the person's initials which John extracted from their full name in their user information, a word found in the dictionary)
- On the first try it took four days to crack the last of the three passwords

Websites used

- http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/crack/default.htm
- http://www.openwall.com/john/