R V COLLEGE OF ENGINEERING

Name: Dhanush M **USN:** 1RV18IS011 **Dept/Lab:** ISE/CSDF **Expt No.:** 03 a
Date: 03/12/2021 **Title:** PASSWORD ATTACK TOOLS

---

a. PASSWORD CRACKING USING **JOHN THE RIPPER**

INTRODUCTION

Hacking is an attempt to explore methods of breaching a defense mechanism and exploiting a weakness of a system to prevent unauthorized parties into the system by sealing the loopholes found in the system. This form of hacking is commonly known as penetration testing, also known as pen test. This is an attempt to identify the level of a security system by trying to gain access into the system through identified vulnerabilities with permission from authorized personnel.

Types of Penetration testing - External Pen Test, Internal Pen Test, and Social Engineering.

John the Ripper is a free, open-source password cracking and recovery security auditing tool available for most operating systems. It has a bunch of passwords in both raw and hashed format. This bunch of passwords stored together is known as a password dictionary.
John the Ripper will identify all potential passwords in a hashed format. It will then match the hashed passwords with the initial hashed password and try to find a match. If a match is found in the password hash, John the Ripper then displays the password in raw form as the cracked password. The process of matching the password hashes to locate a match is known as a dictionary attack.

Objectives - To spot the weak passwords in a system and use John the Ripper in the password cracking process.

EXECUTION STEPS

1. **Installing John the ripper from a package**
   Command - *sudo apt install john*
   Command to run John the ripper - *john*

2. **Cracking passwords using John the ripper**
   During the cracking process, John the Ripper uses a rainbow table approach where it takes words from an in-built dictionary that comes with it. It then compiles the variations of that dictionary and compares the hashed password to what is in the password file trying to find a match. This is repeated until a match is found.
   John the ripper works in 3 different modes to crack the passwords -
   a. Single Crack Mode
   b. Wordlist Crack Mode
   c. Incremental Mode

Examples cases of cracking passwords

1. **John the ripper Single crack mode**

   In this mode John the ripper makes use of the information available to it in the form of a username and other information. This can be used to crack the password files with the format of Username:Password.

   Syntax: john [mode/option] [password file]

   john --single --format=raw-sha1 file.txt

```
┌──(root💀kali)-[/home/kali]
└─# john --single --format=raw-sha1 file.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Hello            (Hello)
1g 0:00:00:00 DONE (2021-12-01 02:18) 100.0g/s 200.0p/s 200.0c/s 200.0C/s Hello..hello
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

2. **John the ripper Wordlist crack mode**

   In this mode John the ripper uses a wordlist that can also be called a Dictionary and it compares the hashes of the words present in the Dictionary with the password hash. John also comes in-built with a password.lst which contains most of the common passwords.

   Syntax: john [wordlist] [options] [password file]

   john --wordlist=/usr/share/john/password.lst --format=raw-sha1 file.txt

```
┌──(root💀kali)-[/home/kali]
└─# john --wordlist=/usr/share/john/password.lst --form=raw-sha1 file.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (hello)
1g 0:00:00:00 DONE (2021-12-01 02:16) 100.0g/s 2400p/s 2400c/s 2400C/s service..hello
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

3. **Incremental mode**

   This is the most powerful cracking mode, it can try all possible character combinations as passwords. However, it is assumed that cracking with this mode will never terminate because of the number of combinations being too large (actually, it will terminate if you set a low password length limit or make it use a small charset), and you'll have to interrupt it earlier.

   That's one reason why this mode deals with trigraph frequencies, separately for each character position and for each password length, to crack as many passwords as possible within a limited time.

   Syntax: *john --incremental [password file]*

   john --incremental crack.txt

```
┌──(kali㉿kali)-[~]
└─$ john --incremental file.txt
Created directory: /home/kali/.john
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
hey              (hello)
1g 0:00:00:05 DONE (2021-12-01 12:00) 0.1751g/s 287277p/s 287277c/s 287277C/s n3..hey
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

Cracking the user credentials

In the Linux operating system, a shadow password file is a system file in which encrypted user passwords are stored so that they are not available to the people who try to break into the system. It is located at /etc/shadow.

1. Open Shadow file -
   cat /etc/shadow
   Find credentials of the user and copy it into a text file. Use john the ripper to crack it -
   john file.txt

```
┌──(root💀kali)-[/home/kali]
└─# john file.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Hello            (Hello)
1g 0:00:00:00 DONE 1/3 (2021-12-01 11:22) 12.50g/s 25.00p/s 25.00c/s 25.00C/s Hello..hello
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

2. To collectively crack credentials of all the users, using John the ripper's utility 'unshadow'
   unshadow /etc/passwd /etc/shadow > file.txt
   This combines both the files so John can use it for effective cracking.
   Using john to crack credentials of all users collectively,
   john --wordlist=/usr/share/john/password.lst file.txt (or) *john /etc/shadow*

```
┌──(root💀kali)-[/home/kali]
└─# john --wordlist=/usr/share/john/password.lst file.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (Hello)
1g 0:00:00:00 DONE (2021-12-01 11:30) 3.571g/s 914.2p/s 914.2c/s 914.2C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

View all formats
To view all encryption formats that John the ripper uses -
john --list=formats
Example: raw-sha1, raw-md5, raw-md4, raw-sha256, ripemd-128, whirlpool

Cracking multiple files
Syntax: john [file1] [file2]
john -form=raw-md5 file1.txt file2.txt

Creating a new user
sudo useradd -r <name>
sudo passwrd <name>

CONCLUSION

1. John the Ripper is a basic, free password cracking software tool.
2. It is a password testing and breaking program as it combines a number of password crackers into one package, auto-detects password hash types, and includes a customizable cracker.
3. It runs against various encrypted password formats including several crypt password hash types.

REFERENCES

1. Password cracking with John the Ripper - https://www.section.io/engineering-education/password-cracking-with-john-the-ripper/#how-to-install-john-the-ripper
2. Beginner's guide for John the Ripper (Part 1) - https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1
3. Password cracking with John the Ripper on Linux - https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux
4. John the Ripper's command line syntax - https://www.openwall.com/john/doc/OPTIONS.shtml
5. John the Ripper usage examples - https://www.openwall.com/john/doc/EXAMPLES.shtml