

INFORMATION NETWORK & SECURITY

IA-2

Topic: John The Ripper password cracker

Team Members:

Zenith Mehta.....	16010120028
Yash Salunkhe.....	16010120043
Parth Sangoi.....	16010120044
Krish Bhat.....	16010120060

Content:

- Problem statement
- Introduction
- Requirements
- Kali linux installation
 - Steps to use use john the ripper
- Possible flag options in john
- Hash options to crack
- Manual for john
- Md5 and sh1 hash generator
- Advantages and disadvantages
- Applications
- Future scope
- Conclusion
- Reference

Problem statement-

John the Ripper is a popular password cracking tool used to find weak passwords in computer systems. It uses various methods such as brute force and dictionary attacks to guess passwords based on information such as username, email, or other personal information.

Introduction to John The Ripper

John the Ripper uses a variety of techniques to crack passwords, including dictionary attacks, brute force attacks, and rainbow table attacks. It is able to crack passwords for a wide range of systems, including Unix, Windows, and other operating systems, as well as various encryption algorithms such as MD5, SHA-1, and SHA-256.

One of the key features of John the Ripper is its ability to use multiple processors or cores to accelerate the password cracking process, making it a very efficient tool for cracking large numbers of passwords. It also supports a wide range of plugins and custom rules, allowing users to tailor the tool to their specific needs.

Overall, John the Ripper is a powerful and versatile password cracking tool that can be used for a variety of security testing purposes. However, it should only be used with proper authorization and in accordance with ethical guidelines.

One of the modes John can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

John also offers a brute force mode. In this type of attack, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash. John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords that do not appear in dictionary wordlists, but it takes a long time to run.

JtR has four modes of operation; incremental, single, wordlist, and external. The incremental mode simply applies the brute-force method while the wordlist and single modes use the dictionary method. The wordlist mode uses a user-definable text file as the dictionary while single mode generates its own dictionary using data found in the password file, such as the user name and account information. The external mode allows user defined modes of operation to be run using program code created with a subset of the C language.

A wide variety of options can be specified to customize JtR's operation. By default, if JtR is run without additional command line parameters, the single mode will be used first followed by the wordlist mode and finally the incremental mode.

JtR has been extended over the years to work with a wide variety of password file formats. The basic setup, without extensions, supports the following formats:

- Unix crypt(3) hashes:
 - o traditional and double-length DES
 - o BSDI extended DES
 - o FreeBSD MD5
 - o OpenBSD Blowfish
- Kerberos AFS
- Windows LM hash

Requirements

The requirements for using John the Ripper depend on the operating system and the version of the tool being used.

Here are the general requirements for using John the Ripper:

1. Operating System: John the Ripper is supported on various operating systems including Windows, Linux, Unix, and macOS.
2. CPU: John the Ripper is a CPU-intensive tool, so the faster your processor, the faster the password cracking process will be. However, it can run on most modern CPUs.
3. RAM: The amount of RAM you need will depend on the size of the password file you are trying to crack. A large password file will require more RAM.
4. Disk Space: You will need enough disk space to store the password file, John the Ripper executable, and any other files required by the tool.
5. GPU: If you have a supported graphics card, you can use John the Ripper with GPU acceleration for faster password cracking.

6. Access: Depending on the operating system and the password file you are trying to crack, you may need administrative or root access to run John the Ripper.
7. Wordlists: John the Ripper relies on wordlists to crack passwords. You will need to have one or more wordlists available to use with the tool. It is also important to note that John the Ripper is a command-line tool, so you will need some familiarity with the command line to use it effectively.

This particular demonstration is done on kali linux operating system

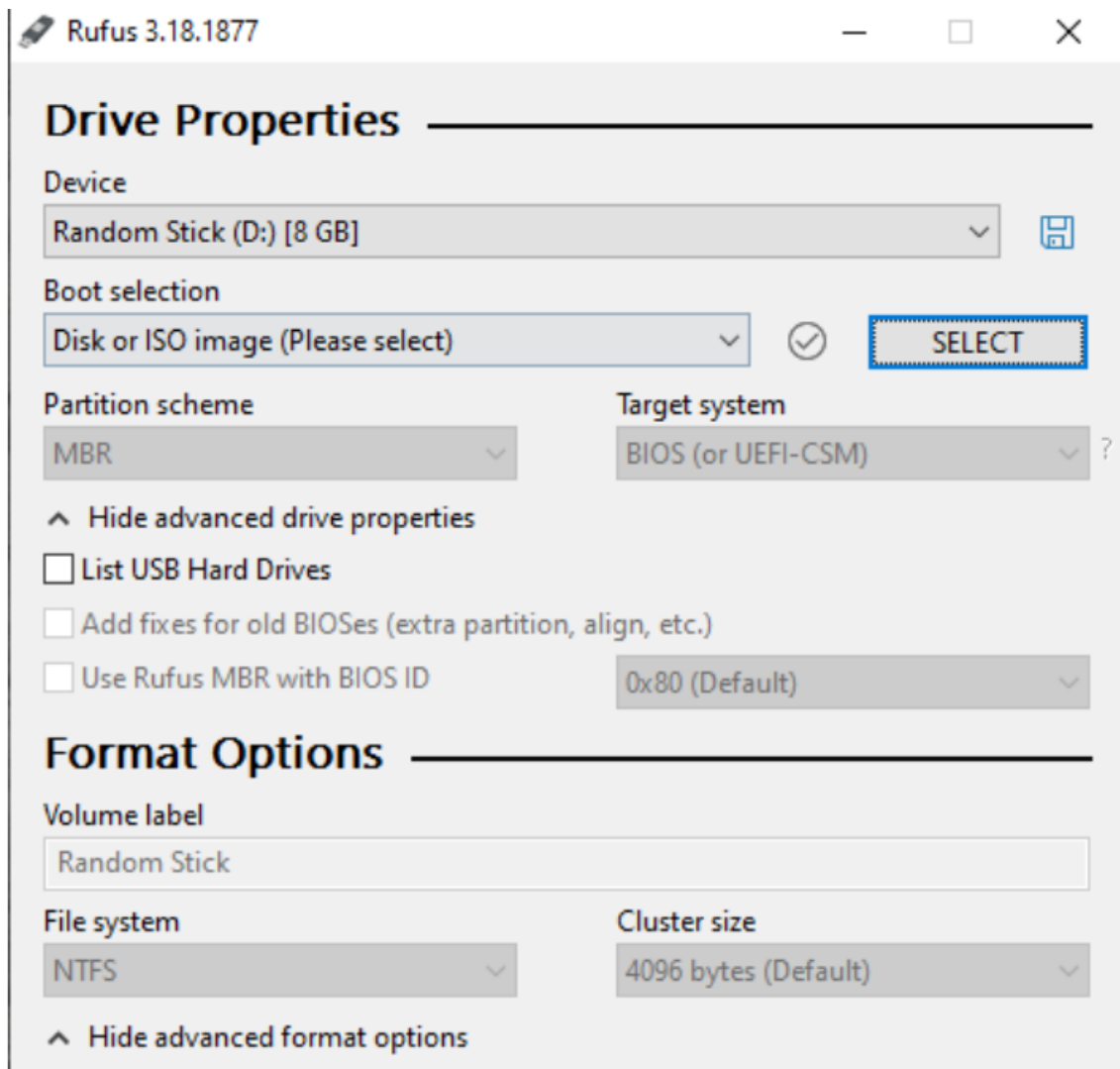
Kali linux installation:

Kali Linux is a popular operating system for security professionals and hackers. Here are the steps to install Kali Linux:

1. Download Kali Linux ISO: Visit the official Kali Linux download page and download the appropriate ISO file for your computer.



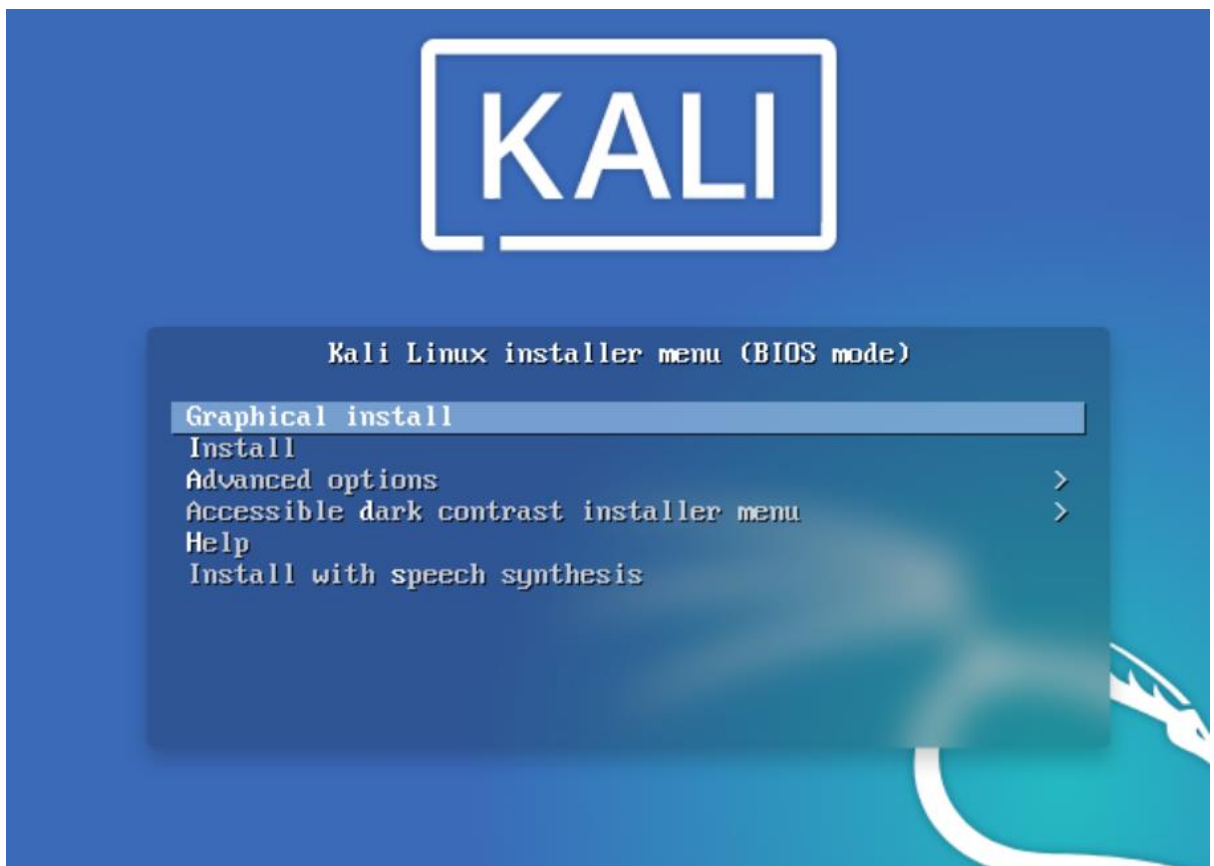
2. Create a bootable USB drive: Use a tool like Rufus to create a bootable USB drive with the Kali Linux ISO.



3. Boot from the USB drive: Insert the USB drive into your computer and restart it. Press the key to enter the BIOS or boot menu (usually F2 or F12) and select the USB drive as the boot device.



4. Install Kali Linux: Once Kali Linux has booted from the USB drive, select "Graphical Install" to begin the installation process. Follow the prompts to select your language, time zone, keyboard layout, and disk partitioning options.



K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

5. Set up users and passwords: During the installation process, you will be prompted to create a root user and set a password. You should also create a regular user account for day-to-day use.



BY OFFENSIVE SECURITY

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot Go Back Continue

6. Complete the installation: After the installation is complete, remove the USB drive and restart your computer. You can now log in to Kali Linux using the root or regular user account you created.



STEPS to initiate john

Where to find john in the machine?

> kali machine → password attacks → john



Certain flag options in John

flags are command-line options that are used to modify the behavior of the tool or specify additional parameters. It could be simply accessed by typing 'john' in terminal


```
--rules[=SECTION[, ..]] doc/ENCODINGS and --list=hidden-options.  
enable word mangling rules (for wordlist or PRINCE  
modes), using default or named rules  
--rules=:rule[; ..]] same, using "immediate" rule(s)  
--rules-stack=SECTION[, ..] stacked rules, applied after regular rules or to  
modes that otherwise don't support rules  
--rules-stack=:rule[; ..] same, using "immediate" rule(s)  
--incremental[=MODE] "incremental" mode [using section MODE]  
--mask[=MASK] mask mode using MASK (or default from john.conf)  
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)  
--external=MODE external mode or word filter  
--subsets[=CHARSET] "subsets" mode (see doc/SUBSETS)  
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]  
--restore[=NAME] restore an interrupted session [called NAME]  
--session=NAME give a new session the NAME  
--status[=NAME] print status of a session [called NAME]  
--make-charset=FILE make a charset file. It will be overwritten  
--show[=left] show cracked passwords [if =left, then uncracked]  
--test[=TIME] run tests and benchmarks for TIME seconds each  
--users=[-]LOGIN|UID[, ..] [do not] load this (these) user(s) only  
--groups=[-]GID[, ..] load users [not] of this (these) group(s) only  
--shells=[-]SHELL[, ..] load users with[out] this (these) shell(s) only  
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes  
--costs=[-]C[:M][, ...] load salts with[out] cost value Cn [to Mn]. For  
tunable cost parameters, see doc/OPTIONS  
--save-memory=LEVEL enable memory saving, at LEVEL 1..3  
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count  
--fork=N fork N processes  
--pot=NAME pot file to use  
--list=WHAT list capabilities, see --list=help or doc/OPTIONS  
--format=NAME force hash of type NAME. The supported formats can  
be seen with --list=formats and --list=subformats
```

Hashes John can crack

Password hashes are one-way transformations of passwords that are used to store passwords securely without revealing the original password. John the Ripper can crack many types of password hashes. It could be simply accessed by typing 'john—list=formats' in terminal

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

```
(root@kali)-[~]  
# john --list=formats  
descript, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,  
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssh1, aix-ssh256,  
aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5,  
AxCrypt, AzureAD, BestCrypt, bfegg, Bitcoin, BitLocker, bitshares, Bitwarden,  
BKS, Blackberry-ES10, WoWSRP, Blockchain, chap, Clipperz, cloudkeychain,  
dynamic_n, cq, CRC32, sha1crypt, sha256crypt, sha512crypt, Citrix_NS10,  
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,  
dominosec8, DPAPImk, dragonfly3-32, dragonfly3-64, dragonfly4-32,  
dragonfly4-64, Drupal7, eCryptfs, eigrp, electrum, EncFS, enpass, EPI,  
EPiServer, ethereum, fde, Fortigate256, Fortigate, FormSpring, FVDE, geli,  
gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa, hMailServer, hsrp, IKE, ipb2,  
itunes-backup, iwork, KeePass, keychain, keyring, keystore, known_hosts,  
krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs, krb5-17, krb5-18, krb5-3,  
kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS, MD2, mdc2, MediaWiki,  
monero, money, MongoDB, scram, Mozilla, mscash, mscash2, MSCHAPv2,  
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,  
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,  
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,  
o3logon, o5logon, ODF, Office, oldoffice, OpenBSD-SoftRAID, openssl-enc,  
oracle, oracle11, Oracle12C, osc, ospf, Padlock, Palshop, Panama,  
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,  
PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda, pgpwde, phpasp, PHPS,  
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,  
RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512, Raw-Blake2,  
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,  
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,  
Raw-SHA384, ripemd-128, ripemd-160, rsvp, Siemens-S7, Salted-SHA1, SSHA512,
```

Manual for john

In this manual, the basic usage of John the Ripper is covered.

1. Installation

- Download the latest version of John the Ripper from the official website.
- Extract the downloaded file to a directory of your choice.
- Open a terminal or command prompt and navigate to the directory where John the Ripper is installed.

2. Usage

- To crack a password, you need to have a password file. This file contains a list of hashed passwords that you want to crack. John the Ripper supports various password file formats such as /etc/passwd, shadow files, and Windows SAM databases.
- Once you have the password file, run John the Ripper with the following command:

```
john [options] password_file
```

The options allow you to specify the type of attack you want to perform. For example, the **-wordlist** option specifies a dictionary attack using a wordlist file, while the **-incremental** option performs a brute-force attack.

It could be simply accessed by typing 'man john' in terminal

K. J. Somaiya College of Engineering, Mumbai-77

(A Constituent College of Somaiya Vidyavihar University)

```
NAME
 john - a tool to find weak passwords of your users

SYNOPSIS
 john [options] password-files

DESCRIPTION
 This manual page documents briefly the john command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known as John the Ripper, is a tool to find weak passwords of users in a server. John can use a dictionary or some search pattern as well as a password file to check for passwords. John supports different cracking modes and understands many ciphertext formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.

USAGE
 To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental".

 Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot. John will read this file when it restarts so it doesn't try to crack already done passwords.

 To see the cracked passwords, use

 john -show passwd

 Important: do this under the same directory where the password was cracked (when using the cronjob, /var/lib/john), otherwise it won't work.
```

All the options recognized by john start with a single dash ('-'). A summary of options is included below.

```
-external:MODE
 Enables an external mode, using external functions defined in ~/.john.ini's [List.External:MODE] section.

-format:NAME
 Allows you to override the ciphertext format detection. Currently, valid format names are DES, BSDI, MD5, BF, AFS, LM. You can use this option when cracking or with '-test'. Note that John can't crack password files with different ciphertext formats at the same time.

-groups:[-]GID[, .. ]
 Tells John to load users of the specified group(s) only.

-incremental[:MODE]
 Enables the incremental mode, using the specified ~/.john.ini definition (section [Incremental:MODE], or [Incremental:All] by default).

-makechars:FILE
 Generates a charset file, based on character frequencies from ~/.john/john.pot, for use with the incremental mode. The entire ~/.john/john.pot will be used for the charset file unless you specify some password files. You can also use an external filter() routine with this option.

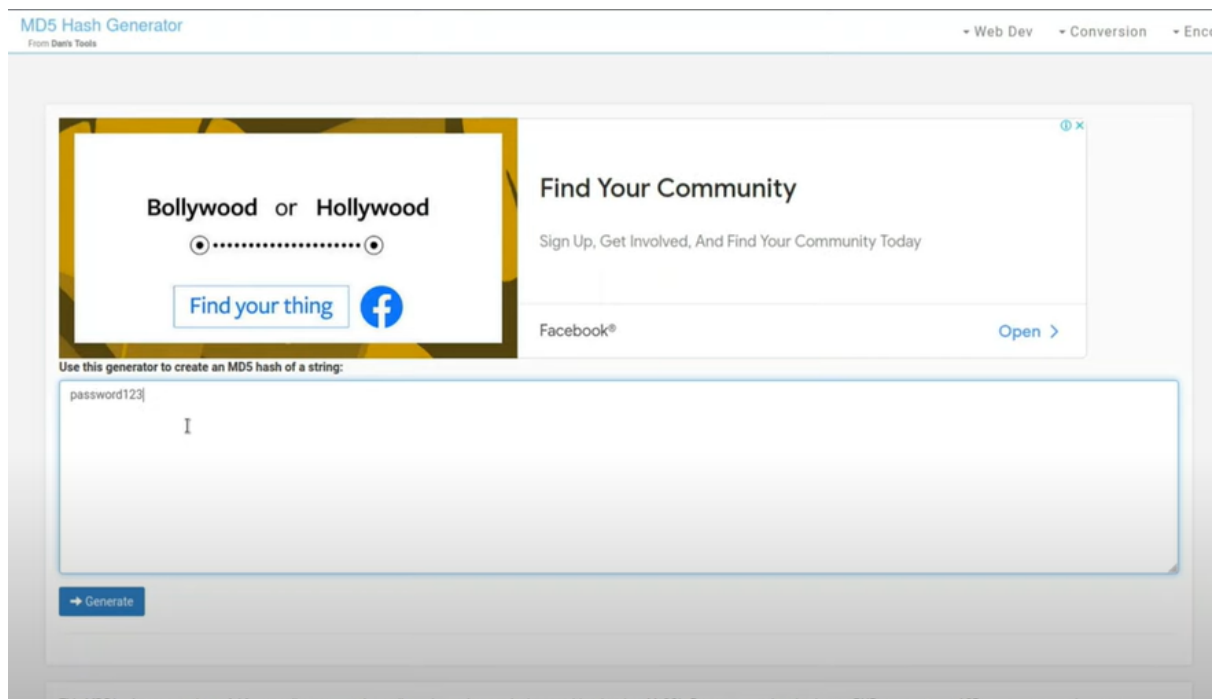
-restore[:FILE]
 Continues an interrupted cracking session, reading point information from the specified file (~/.john/john.rec by default).

-rules
 Enables wordlist rules, that are read from [List.Rules:Wordlist] in /etc/john/john.conf (or the alternative configuration file you might specify on the command line).
 This option requires the -wordlist option to be passed as well.
```

Practical implementation of some hashes

1. md5

- Open md5 hash generator in browser
- Try a password (password123)
- Its md5 hash value is created
- Hash value can be saved in text file (nano testmd5.txt)
- To crack the file certain syntax is used (john -w==/ PATH OF TEXT FILE)
- Important point is syntax must contain 'raw-md5' format because its md5 hash value
- Password will be shown within a second



K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Your Hash: 482c811da5d5b4bc6d497ffa98491e38
Your String: password123
Use this generator to create an MD5 hash of a string:

```
File Actions Edit View Help
GNU nano 5.3 testmd5.txt *
482c811da5d5b4bc6d497ffa98491e38

File Actions Edit View Help
(root@kali)~# john -w=/usr/share/wordlists/rockyou.txt --format=raw-md5 testmd5.txt

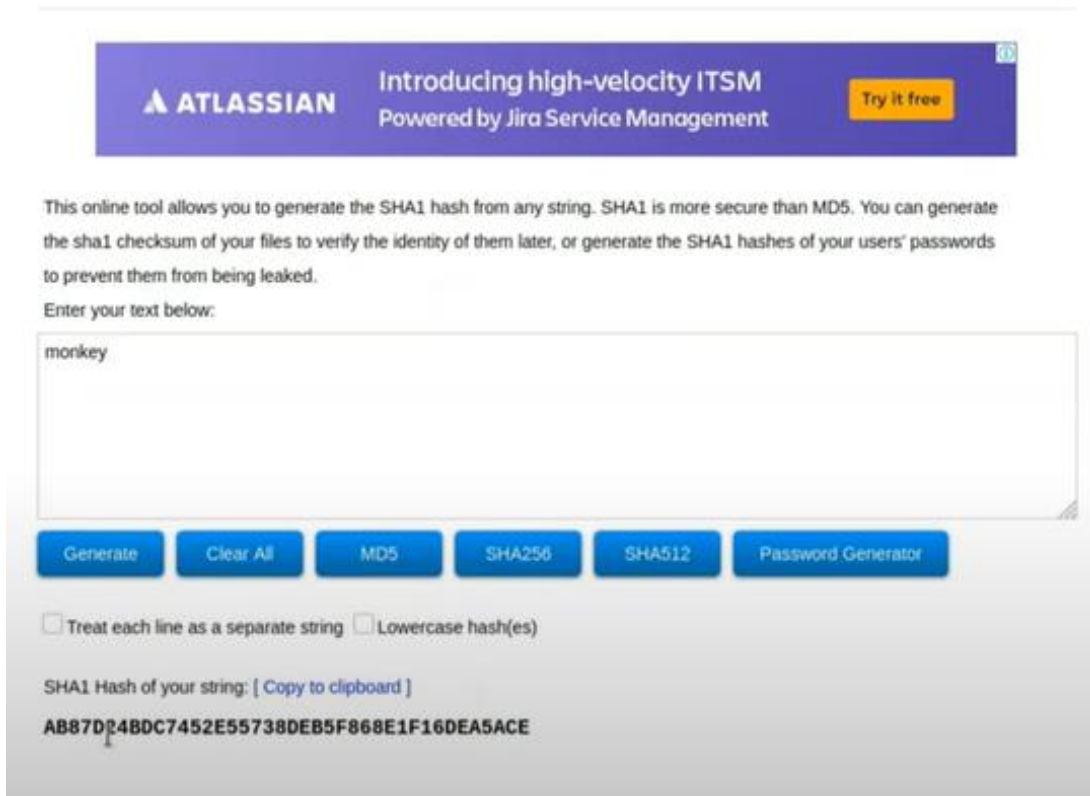
(root@kali)~# john -w=/usr/share/wordlists/rockyou.txt --format=raw-md5 testmd5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:00 DONE (2021-04-30 19:40) 100.0g/s 153600p/s 153600c/s 153600C/s 753951..mexico1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

2. sha1

- Open sha1 hash generator in browser
- Try a password (monkey)
- Its sha1 hash value is created
- Hash value can be saved in text file (nano testsha1.txt)
- To crack the file certain syntax is used(john -w==/ PATH OF TEXT FILE)
- Important point is syntax must contain 'raw-sha1' format because its md5 hash value
- Password will be shown within a second

SHA1 Hash Generator



The screenshot shows the 'SHA1 Hash Generator' web application. At the top, there is a purple banner for 'ATLASSIAN' with the text 'Introducing high-velocity ITSM Powered by Jira Service Management' and a 'Try it free' button. Below the banner, a paragraph explains the tool's purpose: 'This online tool allows you to generate the SHA1 hash from any string. SHA1 is more secure than MD5. You can generate the sha1 checksum of your files to verify the identity of them later, or generate the SHA1 hashes of your users' passwords to prevent them from being leaked.' Below this text, it says 'Enter your text below:' followed by a text input field containing the word 'monkey'. Under the input field are six buttons: 'Generate', 'Clear All', 'MD5', 'SHA256', 'SHA512', and 'Password Generator'. Below the buttons are two checkboxes: 'Treat each line as a separate string' and 'Lowercase hash(es)'. At the bottom, it displays the 'SHA1 Hash of your string: [Copy to clipboard]' followed by the hash value 'AB87D34BDC7452E55738DEB5F868E1F16DEA5ACE'.

ATLASSIAN Introducing high-velocity ITSM
Powered by Jira Service Management Try it free

This online tool allows you to generate the SHA1 hash from any string. SHA1 is more secure than MD5. You can generate the sha1 checksum of your files to verify the identity of them later, or generate the SHA1 hashes of your users' passwords to prevent them from being leaked.

Enter your text below:

monkey

Generate Clear All MD5 SHA256 SHA512 Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

SHA1 Hash of your string: [Copy to clipboard]

AB87D34BDC7452E55738DEB5F868E1F16DEA5ACE

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

```
(root@kali)~# nano testsha1.txt

(root@kali)~# john -w=/usr/share/wordlists/rockyou.txt --format=raw-sha1 testsha1.txt
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
monkey (?)
1g 0:00:00:00 DONE (2021-04-30 19:43) 100.0g/s 1600p/s 1600c/s 1600C/s 12345678..jessica
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

3. Already cracked password cannot be cracked again

It will show that no hash left to crack(no password)

```
(root@kali)~# john -w=/usr/share/wordlists/rockyou.txt --format=raw-md5 testmd5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
```

Advantages of john the ripper

1. **Multiple Platforms:** John the Ripper is a cross-platform tool, meaning it can run on a variety of operating systems including Windows, Linux, and macOS.
2. **High Performance:** John the Ripper is designed to be highly efficient and can process large amounts of data quickly, making it a great choice for cracking passwords in bulk.
3. **Customizable:** John the Ripper is highly customizable and can be configured to use different cracking modes, such as dictionary-based attacks, brute force attacks, and hybrid attacks.
4. **Free and Open-Source:** John the Ripper is free to download and use, and it is also open-source, which means that anyone can inspect the code and make modifications to it.
5. **Supports Many Encryption Formats:** John the Ripper supports a wide range of encryption formats, including many popular ones such as MD5, SHA-1, and bcrypt.
6. **Plugins and Scripts:** John the Ripper can be extended with various plugins and scripts, which can enhance its functionality and make it more effective in cracking passwords.
7. **Active Development:** John the Ripper is actively developed and maintained by a dedicated team of developers, which means that it is constantly improving and evolving to keep up with new security threats and challenges.

Overall, John the Ripper is a powerful tool that can help security professionals test the strength of their passwords and identify weaknesses in their security infrastructure. However, it should only be used for ethical purposes and with the appropriate legal permissions.

Disadvantages of john the ripper

1. **Requires Technical Knowledge:** John the Ripper is a complex tool that requires a good understanding of computer systems and cryptography to use effectively. Users who are not familiar with these concepts may find it difficult to use.
2. **Time-Consuming:** Cracking passwords with John the Ripper can be a time-consuming process, especially if the passwords are complex or use strong encryption methods.
3. **Limited Success Rate:** While John the Ripper is a powerful tool, it is not always successful in cracking passwords. Some passwords are simply too complex or well-protected to be cracked using John the Ripper's methods.
4. **Legal Issues:** Using John the Ripper to crack passwords without the owner's permission is illegal and can lead to serious consequences.
5. **May Be Detected by Antivirus:** Some antivirus programs may detect John the Ripper as a hacking tool and flag it as malware, leading to problems for users.
6. **Limited User Interface:** John the Ripper has a command-line interface, which may be challenging for users who prefer a graphical user interface (GUI).
7. **May Cause System Instability:** Running John the Ripper for extended periods of time may cause system instability or crashes, especially on older or less powerful systems.

Overall, while John the Ripper is a useful tool, it requires careful consideration and a clear understanding of its limitations and potential risks. Users should only use it for legal and ethical purposes and take appropriate precautions to ensure the security of their systems.

Applications

1. Password Auditing: John the Ripper is commonly used by security professionals to audit the strength of passwords used in their organization's systems. This can help identify weak passwords that are vulnerable to attacks and improve the overall security of the organization's systems.

```
(parrot@parrot)~[~/Desktop]
$ john --single shadow.hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 X 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
john doe      (john doe)
karen         (karen)
2g 0:00:00:00 DONE (2021-08-01 15:23) 66.66g/s 500.0p/s 533.3c/s 533.3C/s karen..john doe
Use 'john --show' option to display all of the cracked passwords reliably
Session completed
```

2. Penetration Testing: John the Ripper can be used as part of a penetration testing process to test the security of a system by attempting to crack passwords and gain access to sensitive data or resources.

```
kali@kali:~/src/john/src$ ./configure
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking whether to compile using MPI... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking additional paths... -L/usr/local/lib -I/usr/local/include
checking arg check macro for -m with gcc... yes
```

3. Forensic Investigations: John the Ripper can be used as a forensic tool to recover passwords from encrypted data, such as password-protected files or archives.

4. Recovery of Lost Passwords: John the Ripper can be used to recover lost or forgotten passwords, such as those used to encrypt personal files or archives.

```
C:\Demo>John-the-Ripper-v1.8.0-jumbo-1-Win-32\run\john.exe --pot=test.pot --wordlist=John-the-Ripper-v1.8.0-jumbo-1-Win-32\password.lst test.hash
Loaded 1 password hash (PKZIP [32/32])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein (test.zip)
lg 0:00:00:00 DONE (2017-05-11 23:00) 250.0g/s 886500p/s 886500c/s 886500C/s 123456...ss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

5. Educational Purposes: John the Ripper can be used in educational settings to teach students about computer security, password cracking techniques, and encryption methods.

```
~ >>> sudo john --wordlist=/tmp/password-list.txt /etc/shadow
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:58 100% 0g/s 559.4p/s 559.4c/s 559.4C/s 0747..070162
Session completed
~ >>>
```

6. Legal and Law Enforcement: John the Ripper can be used in legal and law enforcement investigations to recover passwords and gain access to evidence stored in encrypted files or systems.

John the Ripper is a versatile tool with many different applications, but it should only be used for legal and ethical purposes with appropriate permissions and safeguards in place.

Future scope

Future research may focus on combining the two approaches of workload distribution. One possible approach is to use both methods and implement an additional evaluation logic which will determine which method to apply given a specific scenario.

Beyond JtR's wordlist mode, future work will include creating an MPI implementation of JtR's incremental mode with a focus on exploring the limitations of current MPI implementations and addressing them. There are no current plans to attempt to parallelize JtR's single crack mode, due to its very short run-time even when run serially. While the single mode can conceivably be parallelized, the benefits of such an endeavour are in doubt.

For incremental mode parallelization, a method of consistent load balancing and processor failure management has yet to be attempted and should be explored. When a processor completes its allocated task, it should be allocated more work taken from the remaining workloads of the other processors. The possible scenario of a processor going offline during execution should also be addressed since execution of incremental mode attacks are very time consuming and graceful processor failure resolution should be explored. This might be implemented by dividing the workload of the failed processor among the remaining processors.

Conclusion

John the Ripper is a powerful password cracking tool that is widely used by security professionals and enthusiasts. It has been around for several decades and has evolved into a robust and versatile tool that can handle various password cracking techniques, such as dictionary attacks, brute-force attacks, and hybrid attacks.

The tool is open-source and free to use, making it accessible to anyone who wants to improve their password security or test the security of their own systems. However, it's essential to use it ethically and with the proper permissions and authorizations.

Overall, John the Ripper is a valuable tool for password auditing and testing, but it's crucial to use it responsibly and within legal and ethical boundaries.

References

1. The official website for John the Ripper: <https://www.openwall.com/john/>
2. The John the Ripper documentation: <https://www.openwall.com/john/doc/>
3. John the Ripper on GitHub: <https://github.com/magnumripper/JohnTheRipper>
4. John the Ripper Wikipedia page: https://en.wikipedia.org/wiki/John_the_Ripper
5. A tutorial on how to use John the Ripper: <https://resources.infosecinstitute.com/topic/john-the-ripper-tutorial/>
6. A blog post on using John the Ripper for password cracking: <https://www.hackingarticles.in/breaking-passwords-with-john-the-ripper/>
7. A video tutorial on using John the Ripper: <https://www.youtube.com/watch?v=Q2cEh0Yl>
8. Lim, R., Parallelization of John the Ripper (JtR) using MPI. 2004, Computer Science and Engineering University of Nebraska–Lincoln.
9. Pippin, A., B. Hall, and W. Chen, Parallelization of John the Ripper Using MPI. 2006, University of California, Santa Barbara.
10. OpenWall (2010) John the Ripper's cracking modes.
11. Anderson, J. (2010) John the Ripper
12. OpenWall (2010) MPI with John the Ripper. 2010.