

1. John the Ripper

What is the Tool?

John the Ripper (JtR) is a password cracking tool originally produced for UNIX-based systems. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks.

Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike.

How does John the Ripper work?

Password crackers and cryptanalysis tools typically work in three different ways. The common objective in all these is ultimately to correctly guess ("crack") a password:

1. **Dictionary attack:** In this type of attack the tool tries passwords provided in a pre-fed list of large number of words, phrases and possible passwords derived from previously leaked data dumps or breaches. The tool enters every single password in the application from the list, in an attempt to find the correct one.
2. **Brute-force attack:** In this type of attack, the tool asks the user to configure a few settings, for example, the minimum and maximum lengths the correct password may fall into and what types of characters it could possibly consist of (e.g., letters only, letters and numbers, or special characters) and at what positions (say, for every password it generates, first four would be alphabets followed by two digits and two special characters). It takes a bit of guesswork and expertise to find the ideal brute-forcing configuration. The tool then guesses every combination of password possible within this range and specified by the criteria. On a successful match, user is notified of the correct password.
3. **Rainbow tables:** Because mission-critical and security-oriented applications seldom store passwords in plaintext and instead store their fixed-length hashes, rainbow tables can be efficient especially if a large list of hashed passwords is available (for example, from a leaked data dump). In this case, a pre-computed list of password hashes (derived from commonly set passwords) is compared against an existing data dump to find the correct password in its plaintext form. Using rainbow tables is faster than brute-forcing as the hashed data is precalculated. A rainbow table will be ineffective when password hashes are salted and salt values are too large, all of which increases the overall complexity.

John the Ripper modes

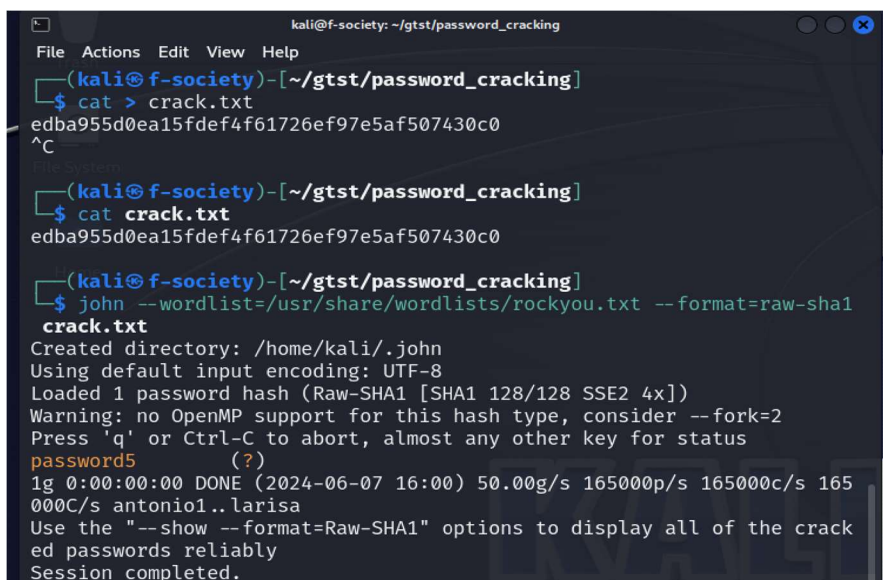
It provides at least three modes along with an “external” mode, which is basically letting a user define a customized mode via a configuration file.

1. **Single crack mode:** the creators recommend running this mode first as it’s considered the quickest. Single crack mode uses information from UNIX passwd files — users’ full names, usernames, etc. — as present in GECOS fields within UNIX passwd/shadow files to “guess” passwords. This can be helpful in cases when a user has set a password for an account based on commonly available information or phrase in the username (e.g. admin: admin, michael: michael123).
2. **Wordlist mode:** Akin to dictionary attack, this mode relies on the user providing a text file with a list of passwords, ideally one per line and no duplicates. JtR does not sort the passwords provided in the wordlist. However, this can be done trivially beforehand by the user, if needed. The command recommended by JtR guide to sort a wordlist is: `tr A-Z a-z TARGET` The application also comes with a set of default wordlist(s), with Pro version offering more.
3. **Incremental mode:** JtR’s equivalent of brute-force is the most powerful cracking mode, but is so time consuming that for a password complex enough, it may never be able to complete in practical course of time and never terminate. The guide reads: “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.”

How to install John the Ripper

John the Ripper is built-in Kali Linux but if it is not installed, we can install it using:

➤ Sudo apt install john



```
kali@f-society: ~/gtst/password_cracking
File Actions Edit View Help
(kali@f-society)-[~/gtst/password_cracking]
$ cat > crack.txt
edba955d0ea15fdef4f61726ef97e5af507430c0
^C

(kali@f-society)-[~/gtst/password_cracking]
$ cat crack.txt
edba955d0ea15fdef4f61726ef97e5af507430c0

(kali@f-society)-[~/gtst/password_cracking]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1
crack.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password5 (?)
1g 0:00:00:00 DONE (2024-06-07 16:00) 50.00g/s 165000p/s 165000c/s 165
000C/s antonio1..larisa
Use the "--show --format=Raw-SHA1" options to display all of the crack
ed passwords reliably
Session completed.
```

2. Hashcat

What is the tool?

Hashcat is a fast password recovery tool that helps break complex password hashes. It is a flexible and feature-rich tool that offers many ways of finding passwords from hashes.

Hashcat is also one of the few tools that can work with the GPU. While CPUs are great for sequential tasks, GPUs have powerful parallel processing capabilities. GPUs are used in Gaming, Artificial intelligence, and can also be used to speed up password cracking.

How to install Hashcat?

Hashcat comes pre-installed in Kali and Parrot OS. To install it if not installed:

➤ **Sudo apt install hashcat**

Core attack modes

- ❖ **Dictionary attack** - trying all words in a list; also called “straight” mode (attack mode 0, -a 0)
- ❖ **Combinator attack** - concatenating words from multiple wordlists (-a 1)
- ❖ **Brute-force attack** and **Mask attack** - trying all characters from given charsets, per position (-a 3)
- ❖ **Hybrid attack** - combining wordlists+masks (-a 6) and masks+wordlists (-a 7); can also be done with rules
- ❖ **Association attack** - use a username, a filename, a hint, or any other pieces of information which could have had an influence in the password generation to attack one specific hash (-a 9)

```
kali@f-society: ~/gtst/password_cracking
File Actions Edit View Help
dc647eb65e6711e155375218212b3964

(kali@f-society)-[~/gtst/password_cracking]
$ hashcat -O -m 0 -a 0 -o Done.txt hashes.txt /usr/share/wordlists/r
ockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SP
IR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl pr
object]

=====
=====
=====
* Device #1: cpu-penryn-13th Gen Intel(R) Core(TM) i7-1360P, 704/1473
MB (256 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 r
otates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c
```

3. Hydra

What is the tool?

Hydra is a popular open-source password cracking tool that is used for performing brute force and dictionary attacks on various login systems and protocols. It is highly flexible and supports multiple attack modes, making it a valuable tool for security professionals.

How Hydra works?

1. **Target Specification:** The user specifies the target system and the protocol or service they want to attack. This includes providing the target's IP address or hostname, port number, and the login protocol.
2. **Credential Lists:** Hydra requires a list of potential usernames and passwords. Users can provide these as input in various formats, such as plaintext files, and specify the format using command-line options.
3. **Attack Configuration:** Users configure the attack by specifying the protocol, attack mode (brute force, dictionary, hybrid), and any other relevant options, such as rate limiting, session resumption, and logging settings.
4. **Initiating the Attack:** Once configured, Hydra initiates the attack by systematically trying each username/password combination against the target system. It performs login attempts based on the chosen attack mode and input lists.
5. **Result Analysis:** Hydra monitors login attempts and checks for successful logins. If successful, it records the valid credentials and reports the results to the user.

How to install Hydra

1. Update your system.
2. Install the required dependencies.
3. Download Hydra.
 - `git clone https://github.com/vanhauser-thc/thc-hydra.git`
 - `cd thc-hydra/`
 - `./configure`
 - `make`
 - `sudo make install`

```
kali@f-society: ~/gtst/password_cracking
File Actions Edit View Help
(kali@f-society)-[~/gtst/password_cracking]
$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.100.151 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purposes
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-07 16:41:12
[WARNING] Many SSH configurations limit the number of parallel tasks,
it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100410793 login tries (l:7/p:14344399), ~6275675 tries per task
[DATA] attacking ssh://192.168.100.151:22/
```

4. FFUF

What is the Tool?

FFUF stands for “Fuzz Faster U Fool,” which is a web fuzzer or a web application security testing tool. It’s used for discovering hidden files and directories on web servers by employing brute-force techniques. FFUF helps in identifying paths, filenames, or other potential entry points that might not be directly linked from a website’s main pages. This tool is often utilized by security professionals and ethical hackers to find vulnerabilities and strengthen web application security.

How to install

1. First you need to install go
2. Then you can install it from kali repository
 - Sudo apt install ffuf

* You can download from GitHub repository if you want to.

How we can do VHOST, subdomain and Directory enumeration using FUFF

Subdomain Enumeration is a technique that consists of finding out the subdomains related to a domain name.

1. **Virtual host** is a method of hosting multiple websites or domains on a single web server by using a single IP address.

Virtual host enumeration involves finding all virtual hosts associated with an IP address or domain. It helps penetration testers to find hidden assets that may be vulnerable to attacks so they can secure them.

FFUF can be used to discover subdomains by the use of virtual hosts and changing the Host header:

- `ffuf -w ~/wordlists/subdomains.txt -H "Host: FUZZ.ffuf.me" -u http://ffuf.me`

NOTE

In summary, John the Ripper and Hashcat are primarily used for cracking passwords stored in hashes, with Hashcat being particularly optimized for GPU acceleration. Hydra, on the other hand, focuses on network authentication and supports a wide range of protocols for brute force attacks.