

## PASSWORD CRACKING

Password cracking is the process of attempting to recover a password from its encrypted form. In this report, I used John the ripper and crack-station as our cryptographic attack tools. Crack-station is an online password cracking service that allows users to submit password hashes for cracking. It provides information about the password's strength and potential matches from its extensive database. Crack-station allow hashes in SHA variants such as sha1, sha224, sha256, sha384, sha512. It also allows MD5 variants that include MD5LM, NTLM, md2, md4, md5, md5(md5\_hex) and md5-half. Additionally, it gives room for other algorithms like ripeMD160, whirlpool and MySQL 4.1+ LM. I started with a weak password which was hashed in MD5 format and it only took crack-station microseconds to crack the password.

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with the site name and links to Defuse.ca and Twitter. Below this is a section titled "Free Password Hash Cracker". A text input field contains the hash "384701c26cd11aea3cb6e9d31c3a2ccb". To the right of the input field is a reCAPTCHA "I'm not a robot" checkbox, which is checked. Below the input field, a list of supported hash types is shown: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults. Below this, a table displays the results of the crack:

Hash	Type	Result
384701c26cd11aea3cb6e9d31c3a2ccb	md5	betito

Below the table, a color code legend indicates: Green for Exact match, Yellow for Partial match, and Red for Not found. At the bottom of the section, there is a link to "Download CrackStation's Wordlist".

I tried cracking a complex password using special characters, numbers, capital letters and small letters. Crack-station could crack the password. Crack-station could not crack password hashes which were in yescrypt format since yescrypt format is more complex to crack or brute-force. The shorter the password the shorter the time used to crack.

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with the site name and links to Defuse.ca and Twitter. Below this is a section titled "Free Password Hash Cracker". A text input field contains the hash "d87740368e28001784a0". To the right of the input field is a reCAPTCHA "I'm not a robot" checkbox, which is unchecked. Below the input field, a list of supported hash types is shown: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults. Below this, a table displays the results of the crack:

Hash	Type	Result
d87740368e28001784a0	Unknown	Not found.

Below the table, a color code legend indicates: Green for Exact match, Yellow for Partial match, and Red for Not found. At the bottom of the section, there is a link to "Download CrackStation's Wordlist".

I stored two hashed passwords on a hash.txt file and used john the ripper to crack the password. John cracked on a simple password which was in sha1 format.

```
Parrot Terminal
File Edit View Search Terminal Help
googleCalendar.png test.zip
hashes.txt updates.png
hash.txt
[beryl@parrot]~/Pictures
$ nano hash.txt
[beryl@parrot]~/Pictures
$ john hash.txt
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
Warning: only loading hashes of type "Raw-SHA1", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of 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=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
12345678 (?)
lg 0:00:00:00 DONE 2/3 (2024-10-13 17:07) 50.00g/s 400.0p/s 400.0c/s 400.0C/s 123456..abc123
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
[beryl@parrot]~/Pictures
$
```

While trying a more complex password, john the ripper took long to output the results.

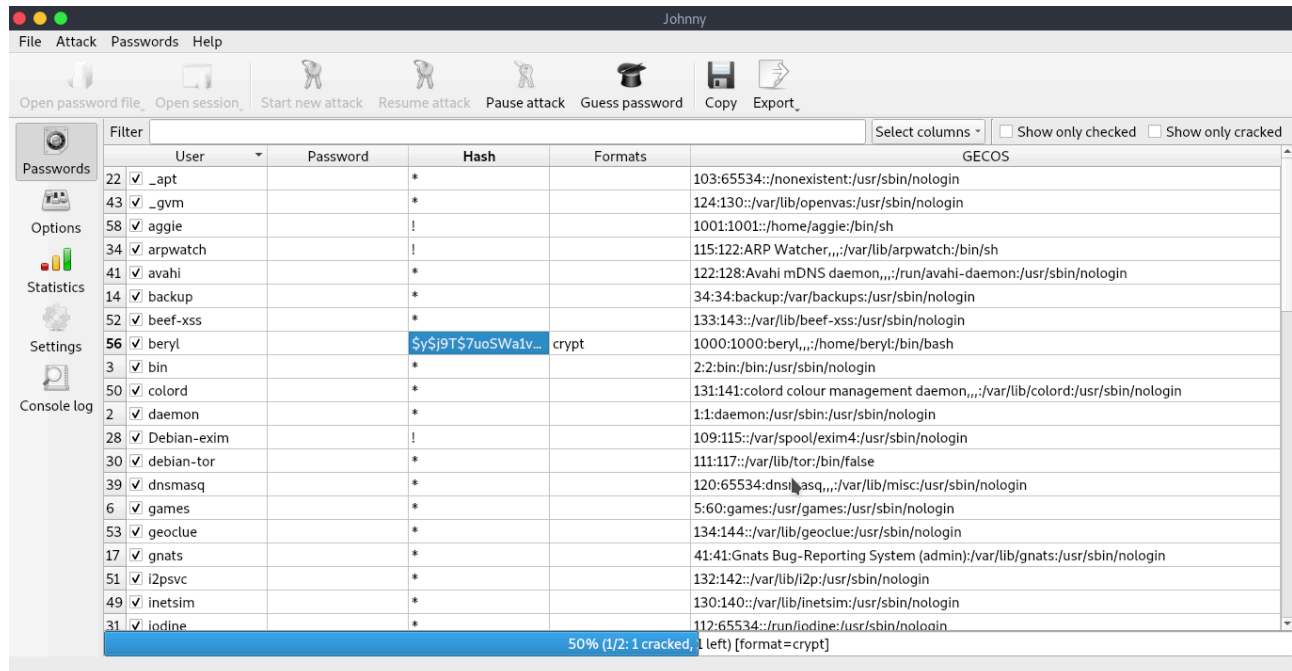
```
Parrot Terminal
File Edit View Search Terminal Help
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates left, minimum 8 needed for performance.
0g 0:00:00:01 DONE (2024-10-13 17:22) 0g/s 11952Kp/s 11952Kc/s 11952KC/s 0xCvBnM,...*7iVamos!
Session completed
[beryl@parrot]~/Pictures
$ john hash.txt
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=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Warning: Only 6 candidates left, minimum 8 needed for performance.
Proceeding with incremental:ASCII
beryl92 (?)
lg 0:00:01:26 DONE 3/3 (2024-10-13 17:26) 0.01162g/s 18104Kp/s 18104Kc/s 18104KC/s berylvm..beryl95
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
[beryl@parrot]~/Pictures
$
```

The systems password stored in my etc/shadow were in a yescrypt hash format which is hard to crack using john the ripper unless I use john-jumbo.

Parrot os had a GUI interface for john the ripper called johnny which is easier to use than the terminal. It automatically identifies the has format for a particular password. In this case I uploaded a file containing all my hashed passwords that are in my etc/shadow file.

Johnny						
File Attack Passwords Help						
Open password file, Open session, Start new attack, Resume attack, Pause attack, Guess password, Copy, Export						
Passwords	Filter	User	Password	Hash	Formats	GECOS
		46 nm-openconnect		*		127:134:NetworkManager OpenConnect plugin,,,/var/lib/networkmanager:/usr/sbin/nologin
Options		45 nm-openvpn		*		126:133:NetworkManager OpenVPN,,,/var/lib/openvpn/chroot:/usr/sbin/nologin
		18 nobody		*		65534:65534:nobody:nonexistent:/usr/sbin/nologin
Statistics		26 ntp		*		107:113:nonexistent:/usr/sbin/nologin
		40 postgres		*		121:127:PostgreSQL administrator,,,/var/lib/postgresql/bin/bash
		12 proxv		*		13:13:proxv/bin:/usr/sbin/nologin

Jonny used wordlists and cracked the weakest password for my root user in seconds. The tool was designed to be intuitive and accessible, even for users who are not experienced with password cracking. The interface is straightforward, and the tool provides clear instructions and error messages. Additionally, John the Ripper offers a wide range of options and configurations, allowing users to customize the tool to their specific needs.



Since user beryl has a complex password I had to cancel the process because it took forever to crack the password.

To prevent brute-force attacks, one needs to use complex passwords which are a combination of uppercase, lowercase letters, numeric numbers and special characters. This makes it difficult for an attacker to brute-force the correct password. Longer passwords are encouraged because longer passwords are more difficult to crack. Furthermore one is encouraged to avoid common words and that can be quickly discovered in a dictionary attack. Ideally, using password managers can help create and store passwords.

In summary, strong passwords and encryption are essential tools to protect against brute force attacks and other security threats. By using complex, unique passwords and implementing encryption, you can significantly reduce the risk of unauthorized access to your systems and data.