GovCracker

User Manual
v5.0
Stand: 05.04.2024

GovCracker & GovTools
by Decrypta Technologies

GovCracker

GovCracker is the world's best-known decryption software with "Hashcat" as the "crack engine" for decrypting passwords in criminal IT forensics.

GovCracker was primarily developed for use in international law enforcement agencies, universities and IT forensic companies.

Further information can be found at www.govcracker.com or Github.

Notes:

1. All copyrights of this program belong exclusively to the author, unless waived in writing.

2. You may not misuse this software to decrypt passwords for which you have no authorization.

3. No guarantee or liability of any kind is assumed. You use the software at your own risk. The author is not liable for loss of data, damage, loss of profit or any other type of loss or damage.

Table of contents

1 GovCracker

1.1 Targets

1.1.1 Target hash

Here you can select the hash file that you have extracted from the encrypted target using GovTools.

1.1.2 Hash type

Here you can select the correct hash type from the list. You can call up a detailed list using the "magnifying glass". Manual entry is also possible.

Special features of VeraCrypt / TrueCrypt

If you have selected VeraCrypt or TrueCrypt, you have the option of specifying PIM or a key file. PIM stands for "Personal Iterations Multiplier". It is a parameter that was introduced in VeraCrypt 1.12. Its value controls the number of iterations used by the "Header Key Derivation Function". The minimum PIM value for short passwords is "98" for system encryption. This does not apply to SHA-512 and Whirlpool. The standard PIM "485" is used for all others. For a password with 20 characters or more, the minimum PIM value is 1. In all other cases, the PIM remains empty. Both PIM fields must be filled in. You also have the option of selecting a potential keyfile.

1.1.3 Wordlist encoding

Most wordlists worldwide are created in UTF-8 format. GovCracker can calculate the wordlist entries without any problems if the entries do not contain any special characters (German umlauts, Turkish characters, etc.). If the wordlist contains special characters that could be relevant for the respective case, the encoding must be specified accordingly. For German umlauts, for example, this is ISO-8859-1. There are many encoding options - the most common ones are listed in the drop-down menu.

1.1.4 Session name

The session name is preset with the current date. It is recommended to enter the name of the target person or the file number + the current date. The "Open session" button can be used to restart an aborted session or attack (from the point at which it was aborted).

1.1.5 Crack mail

If crack mail is activated, an e-mail is automatically sent to the e-mail address stored under "Settings" as soon as a password has been decrypted.

1.1.6 Status mail

You will be informed of the status by e-mail at regular intervals (see Settings).

1.1.7 Brain server

If Brain server is activated, all checked passwords are logged on the Brain server for this hash. This ensures that a password is never checked twice, regardless of which attack mode is used.

The entries for the Brain server (server and client side) must be entered under "Settings".

1.1.8 Interfaces

You can choose between two interfaces here:

1) GovInterface: The analysis parameters of the current attack are displayed. The parameters are updated every 5 seconds.

2) Manual: The hashcat outputs are "streamed" into the display window. In addition, the hashcat command parameters can be viewed and changed if necessary.

1.2 Attacks

1.2.1 Wordlist-Attack

You can select any wordlist or a folder with wordlists that are checked one after the other. The "GovCracker_Wordlist.txt" is stored in the "_Wordlists" directory and contains around 32 million entries. These include the world's most popular first names, pet names, pet names, the 1000 most words in around 20 languages, etc. The standard rules and additional special GovCracker rules can be added under Rules. The descriptions of the individual rules are largely derived from the labeling. Any number can be entered under "Generate Rules". The number entered determines the number of randomly generated rules per wordlist entry. If, for example, the number 1000 is entered there, then each wordlist entry is randomly changed 1000 times by the machine. The attack mode is started via "START". The "Batchjob" button can be used to save several different attack modes. These can be started together in the "Batchjob" area.

1.2.2 Mask-Attack

Any masks can be entered under "Mask".

The following mask parameters can be inserted:

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?h = 0123456789abcdef
- ?H = 0123456789ABCDEF
- ?s = "space"!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ?a = ?l?u?d?s

- ?b = 0x00 - 0xff

Standard masks can be called up using the buttons. HCMASK files can also be loaded.

Customized mask parameters can be checked with "Charset1" to "Charset 4". These can be called up with ?1, ?2, ?3 or ?4.

The "Increment mode" can be used to specify password lengths. For example, with the mask ?a?a?a?a?a?a?a, a brute force attack would be carried out on a password with six digits. If the password only has five digits, it could not be decrypted with this mask.

However, if 1 to 6 is entered in "increment mode", a brute force attack would be carried out on all passwords with 1 to 6 digits.

1.2.3 Combinator-Attack

Here, two wordlists are "combinate" together. Each entry in the second wordlist is appended to each entry in the first wordlist. For example, numbers and special characters can be "swapped out" in a second wordlist and "appended" or "prefixed" with this attack.

Rule parameters can also be specified: see Attachement 1.

1.2.4 Hybrid-Attack

Here, <> masks are appended to a wordlist or <> a wordlist is appended to masks.

This attack is a combination of wordlist and mask attack.

1.2.5 Automatic-Attack

The "Automatic-Mode" is a GovCracker invention. The aim was to provide people who do not have in-depth knowledge of password decryption with a good and effective option.

In automatic mode, the hash type is analyzed and divided into slow, medium and fast hashes. This value is automatically taken into account in the "Hash speed" field. The respective attack strategies are thus automatically adapted.

The language of the target person must then be selected. This entry adjusts the mask attacks (special characters and umlauts). Please note that the "Encoding" for the wordlist may need to be adjusted.

If the "Wordlister" is activated, subjective key points for the target person are queried after START. These entries are used to generate a comprehensive subjective wordlist. All special characters, numbers and number combinations and the year of birth 1980 to 2040 are automatically entered in the "Standard wordlist" field. Manual entries in this field are possible without any problems. They are separated by commas. It is also possible to copy in information. Separation by commas is carried out automatically. These entries are combined with all other entries. The result is exported to the "_Wordlists" folder.

You can enter any wordlist under Wordlist. The "GovCracker_Wordlist.txt" is preset.

The number of "Generate Rules" is specified automatically and is automatically preset by the hash analysis. This value can be changed manually if required.

You can export or import the subjective parameters entered for the target person in order to use them multiple times if necessary.

1.2.6 Batchjob

The collected batch jobs are collected in this area and can be started together.

1.2.7 Hash-Identifier

A hash file can be selected in this area. This is then analyzed. All possible hash types are displayed.

2 GovCracker-Tools

2.1 Wordlist-Download

This section displays links to good wordlists. You use the links at your own risk. The best and most comprehensive wordlists can be found at www.weakpass.com.

2.2 WPA/WPA2 (hcxtools)

There you can convert recorded WLAN handshake files (e.g. from airodump-ng) into a usable hash format.

2.3 Wordlister

One of the most effective attacks are subjective wordlists. Subjective wordlists contain key points about the target person, such as surname and first name of the target person, spouse, children, dates of birth, hobbies, names of pets, favorite club, etc.

Wordlist generators can be used to create millions of password candidates from this information by combining numbers and special characters and carrying out permutations.

Subjective key points about the target person are queried. These inputs are used to generate an extensive subjective wordlist. All special characters, numbers and number combinations and the year of birth 1980 to 2040 are automatically entered in the "Standard wordlist" field. Manual entries in this field are possible without any problems. These entries are combined with all other entries. They are separated by commas. It is also possible to copy in information. Separation by commas is carried out automatically.

The result is exported to the "_Worlists" folder.

3 Settings

3.1.1 Language

You can select the language here. English and German are currently available. The languages will be successively expanded.

3.1.2 GovTools path

Here you can enter the path to the GovTools folder. This allows you to start quickly via the "GovTools" button at the top left.

3.1.3 Favorite Wordlist

Your favorite wordlist can be stored here as a default setting.

3.1.4 Use CPU only (-D 1).

Only the CPU is used for the calculations here. GPUs are not used.

3.1.5 Disable pot file (--potfile-disable)

GovCracker collects all cracked passwords in the file "GovCracker.potfile" which is located in the folder "_Crackout". GovCracker exports every cracked password to the "_Crackout" folder.

3.1.6 Log files

This GovCracker option collects all started commands in the GovCracker folder "Logs". The file name is composed as follows: Session name + execution date (YYYY_MM_DD_HH_mm_ss) + hash type. The logs are useful for documenting all attacks against a hash.

3.1.7 Optimized OpenCL kernel (-O)

This configures use the optimized OpenCL kernel, but at the cost of limited password length support.

3.1.8 Status mail

Here you can enter the time interval for the status mails in minutes.

3.1.9 Speed (-w)

The speed can be set here or you can decide how many resources are made available.

1 - Low

2 - Standard

3 - Speed

4 - Race

3.1.10 Temperature monitoring (--hwmon-temp-abort=90)

Hardware errors can be avoided by monitoring the temperature. Settings between 70 - 100°C are possible. A temperature of 90°C should not be exceeded.

3.1.11 Devices (-d)

GovCracker basically tries to use all devices (CPUs and GPUs) for the calculations. This function can be used to select specific devices.

3.1.12 Further parameters

You can enter further parameters for Hashcat here.

3.1.13 Brain (client-side)

The Brain function enables all password candidates that have been checked for a hash to be written to the "Brain". This means that the same password candidates for a hash are never checked twice, e.g. by a wordlist attack and later by a mask attack. This also makes it possible to work with several computers or GPU servers on a hash at the same time without password candidates being checked multiple times.

The brain (client side) is the brain side that executes the attacks, i.e. the cracker. In contrast, the brain (server side) is the side on which the checked password candidates are recorded.

3.1.14 Brain (server-side)

The brain server side collects all the hashes checked on the various computers. The IP address in the network is entered under Server.

The port can be set under Port, basically port: 80.

The Brain password is freely selectable.

3.1.15 E-mail (SMTP)

Here you can enter SMTP parameters to which a notification is sent.

Attachment 1

(Source: www.hashcat.net)

Name	Function	Description	Example Rule	Input Word	Output Word
Nothing	:	Do nothing (passthrough)	:	p@ssW0rd	p@ssW0rd
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd
Invert Capitalize	C	Lowercase first found character, uppercase the rest	C	p@ssW0rd	p@SSW0RD
Toggle Case	t	Toggle the case of all characters in word.	t	p@ssW0rd	P@SSw0RD
Toggle @	TN	Toggle the case of characters at position N	T3	p@ssW0rd	p@sSW0rd
Reverse	r	Reverse the entire word	r	p@ssW0rd	dr0Wss@p
Duplicate	d	Duplicate entire word	d	p@ssW0rd	p@ssW0rdp@ssW0rd
Duplicate N	pN	Append duplicated word N times	p2	p@ssW0rd	p@ssW0rdp@ssW0rdp@ssW0rd
Reflect	f	Duplicate word reversed	f	p@ssW0rd	p@ssW0rddr0Wss@p
Rotate Left	{	Rotate the word left.	{	p@ssW0rd	@ssW0rdp
Rotate Right	}	Rotate the word right	}	p@ssW0rd	dp@ssW0r
Append Character	$X	Append character X to end	$1	p@ssW0rd	p@ssW0rd1
Prepend Character	^X	Prepend character X to front	^1	p@ssW0rd	1p@ssW0rd
Truncate left	[	Delete first character	[	p@ssW0rd	@ssW0rd
Trucate right	]	Delete last character	]	p@ssW0rd	p@assW0r
Delete @ N	DN	Delete character at position N	D3	p@ssW0rd	p@sW0rd
Extract range	xNM	Extract M characters, starting at position N	x04	p@ssW0rd	p@ss

Omit range	ONM	Delete M characters, starting at position N	O12	p@ssW0rd	psW0rd
Insert @ N	iNX	Insert character X at position N	i4!	p@ssW0rd	p@ss!W0rd
Overwrite @ N	oNX	Overwrite character at position N with X	o3$	p@ssW0rd	p@s$W0rd
Truncate @ N	'N	Truncate word at position N	'6	p@ssW0rd	p@ssW0
Replace	sXY	Replace all instances of X with Y	ss$	p@ssW0rd	p@$$W0rd
Purge	@X	Purge all instances of X	@s	p@ssW0rd	p@W0rd
Duplicate first N	zN	Duplicate first character N times	z2	p@ssW0rd	ppp@ssW0rd
Duplicate last N	ZN	Duplicate last character N times	Z2	p@ssW0rd	p@ssW0rddd
Duplicate all	q	Duplicate every character	q	p@ssW0rd	pp@@ssssWW00rrdd
Extract memory	XNMI	Insert substring of length M starting from position N of word saved to memory at position I	lMX428	p@ssW0rd	p@ssw0rdw0
Append memory	4	Append the word saved to memory to current word	uMl4	p@ssW0rd	p@ssw0rdP@SSW0RD
Prepend memory	6	Prepend the word saved to memory to current word	rMr6	p@ssW0rd	dr0Wss@pp@ssW0rd
Memorize	M	Memorize current word	lMuX084	p@ssW0rd	P@SSp@ssw0rdW0RD