GovCracker

User Manual
v5.0
Stand: 05.04.2024

GovCracker & GovTools
by Decrypta Technologies

GovCracker

GovCracker ist weltweit die bekannteste Entschlüsselungssoftware mit „Hashcat“ als „Crack-Engine“, für die Entschlüsselung von Passwörtern in der kriminalistischen IT-Forensik.

GovCracker wurde in erster Linie für den Einsatz in internationalen Strafverfolgungsbehörden, Universitäten und für IT-Forensik-Unternehmen entwickelt.

Weitere Informationen unter www.govcracker.com oder Github.

Hinweise:

1. Alle Urheberrechte dieses Programms liegen ausschließlich beim Autor, außer es wurde schriftlich darauf verzichtet.

2. Diese Software dürfen Sie nicht zum Entschlüsseln von Passwörtern missbrauchen, für die Sie keine Befugnis haben (vgl. § 202 a ff. StGB).

3. Es wird keine Garantie oder Haftung jeglicher Art übernommen. Sie verwenden die Software auf eigene Gefahr. Der Autor haftet nicht für Datenverlust, Schäden, Gewinnverlust oder jeglicher andere Arten von Verlust oder Beschädigung.

Inhaltsverzeichnis

1 GovCracker

1.1 Angriffsauswahl

1.1.1 Ziel-Hash

Hier können Sie die Hash-Datei, die Sie mit GovTools aus dem verschlüsselten Ziel extrahiert haben, auswählen.

1.1.2 Hashtyp

Hier können Sie aus der Liste den richtigen Hashtyp auswählen. Über die „Lupe“ können Sie eine detaillierte Liste aufrufen. Eine manuelle Eingabe ist ebenfalls möglich.

Besonderheiten bei VeraCrypt / TrueCrypt

Wenn Sie VeraCrypt oder TrueCrypt ausgewählt haben, haben Sie die optionale Möglichkeit PIM oder ein Keyfile anzugeben. PIM steht für "Personal Iterations Multiplier". Es ist ein Parameter der in VeraCrypt 1.12 eingeführt wurde. Dessen Wert steuert die Anzahl der Iterationen, die von der „Header Key Derivation Function“ verwendet wird. Der PIM-Mindestwert für kurze Kennwörter beträgt bei System-Verschlüsselungen "98". Dies gilt nicht bei SHA-512 und Whirlpool. Bei allen anderen wird die Standard-PIM "485" genutzt. Bei einem Kennwort mit 20 Zeichen und mehr beträgt der PIM-Mindestwert 1. In allen anderen Fällen bleibt die PIM leer. Beide PIM Felder müssen ausgefüllt werden. Außerdem haben Sie die Möglichkeit ein potentielles Keyfile auszuwählen.

1.1.3 Wordlist-Encoding

Die meisten Wordlists werden weltweit im UTF-8 Format erstellt. GovCracker kann die Wordlisteinträge problemlos berechnen, wenn die Einträge keine besonderen Schriftzeichen (deutsche Umlaute, türkische Schriftzeichen, usw.) enthalten. Sollte

die Wordlist besondere Schriftzeichen enthalten die für den jeweiligen Fall von Bedeutung sein könnten, muss das Encoding entsprechend angegeben werden. Bei deutschen Umlauten ist dies bspw. ISO-8859-1. Es gibt sehr viele Encoding-Möglichkeiten – die bekanntesten wurden im Drop-Down-Menü hinterlegt.

1.1.4 Sitzungsname

Der Sitzungsname ist mit dem aktuellen Datum voreingestellt. Es empfiehlt sich den Namen der Zielperson oder das Aktenzeichen + das aktuelle Datum einzutragen. Über den Button „Session öffnen“ kann eine abgebrochene Sitzung bzw. Angriff erneut (ab der Stelle des Abbruchs) gestartet werden.

1.1.5 Crack-Mail

Wenn Crack-Mail aktiviert ist, wird automatisch eine E-Mail an die hinterlegte E-Mail-Adresse unter „Settings“ gesendet, sobald ein Passwort entschlüsselt wurde.

1.1.6 Status-Mail

In regelmäßigen Abständen (siehe Einstellungen) werden Sie über den Status per E-Mail informiert.

1.1.7 Brain-Server

Wenn Brain-Server aktiviert ist, werden zu diesem Hash alle abgeprüften Passwörter auf dem Brain-Server geloggt. Dadurch ist sichergestellt, dass niemals ein Passwort zweimal abgeprüft wird, egal welcher Angriffsmodus durchgeführt wird.

Unter „Settings“ sind die Eingaben zum Brain-Server (Server- und Client-Seite) einzutragen.

1.1.8 Interfaces

Sie haben hier die Möglichkeit zwischen zwei Interfaces zu wählen:

1) **GovInterface**: Die Analyse-Parameter der laufenden Attacke werden angezeigt. Alle 5 Sekunden werden die Parameter aktualisiert.

2) **Manuell**: Die Hashcat Ausgaben werden in das Anzeigefenster „gestreamt". Zusätzlich können die Befehlsparameter eingesehen und ggfs. geändert werden.

1.2 Attacken

1.2.1 Wordlist-Attacke

Sie können eine beliebige Wordlist auswählen oder ein Ordner mit Wordlists, die nacheinander abgeprüft werden.

Die „GovCracker_Wordlist.txt" ist im Verzeichnis „_Wordlists" hinterlegt und beinhaltet ca. 32 Millionen Einträge. Dazu zählen die weltweit beliebtesten Vornamen, Haustiernamen, Kosenamen, die 1000 meisten Wörter in ca. 20 Sprachen, usw.

Unter Rules können die Standard-Rules und zusätzlich spezielle GovCracker-Rules hinzugefügt werden. Die Beschreibungen der einzelnen Rules ergeben sich größtenteils aus der Beschriftung.

Unter „Generate Rules" kann eine beliebige Zahl eingetragen werden. Die eingegebene Anzahl bestimmt die Höhe der maschinell zufällig generierten Rules je Wordlist-Eintrag.

Sollte bspw. die Zahl 1000 dort eingetragen werden, dann wird jeder Wordlisteintrag 1000x zufällig maschinell verändert.

Über „START" wird der Angriffsmodus gestartet.

Über den Button „Batchjob“ können mehrere verschiedenen Angriffsmodis zwischen gespeichert werden. Im Bereich „Batchjob“ können diese zusammen gestartet werden.

1.2.2 Mask-Attacke

Unter „Mask“ können beliebige Masken eingetragen werden.

Folgende Masken-Parameter können eingefügt werden:

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?h = 0123456789abcdef
- ?H = 0123456789ABCDEF
- ?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ?a = ?l?u?d?s
- ?b = 0x00 - 0xff

Über die Buttons können Standard-Masken abgerufen werden. Außerdem können HCMASK-Dateien geladen werden. Die hinterlegten GovCracker-HCMASK-Dateien „German“ prüfen bspw. deutsche Umlaute (ä, ö, ü, ß) mit ab.

Mit „Charset1“ bis „Charset 4“ können selbsterstellte Masken-Parameter abgeprüft werden. Diese können mit ?1, ?2, ?3 oder ?4 aufgerufen werden.

Mit dem „Increment-Mode“ können Passwortlängen vorgegeben werden. Bspw. würde bei der Maske ?a?a?a?a?a?a eine Brute-Force-Attacke auf ein Passwort mit sechs Stellen durchgeführt. Sollte das Passwort nur fünf Stellen besitzen, könnte es mit dieser Maske nicht entschlüsselt werden.

Wird aber im „Increment-Mode“ 1 bis 6 eingebeben, dann würde eine Brute-Force Attacke bei sämtlichen Passwortstellen von 1 bis 6 Stellen durchgeführt.

1.2.3 Combinator-Attacke

Hier werden zwei Wordlist miteinander „verbunden“. Jeder Eintrag der zweiten Wordlist, wird an jeden Eintrag der ersten Wordlist angehangen. Es können bspw. Zahlen und Sonderzeichen in einer zweiten Wordlist „ausgelagert“ werden und mit diesem Angriff „angehangen“ oder „vorangestellt“ werden.

Zusätzlich können noch Rule-Parameter angegeben werden:

s. Anlage 1

1.2.4 Hybrid-Attacke

Hier wird an eine Wordlist <> Masken angehangen oder es werden an Masken <> eine Wordlist angehangen.

Dieser Angriff stellt eine Kombination zwischen Wordlist und Masken-Attacke dar.

1.2.5 Automatic-Attacke

Der „Automatic-Mode“ ist eine GovCracker Erfindung. Ziel war es, auch Personen die keine tiefgreifenden Kenntnisse in der Passwort Entschlüsselung besitzen, eine gute und effektive Möglichkeit an die Hand zu geben.

Im Automatic-Mode wird der Hashtyp analysiert und in langsame, mittlere und schnelle Hashes eingeteilt. Dieser Wert wird automatisch im Feld „Hash-Geschwindigkeit“ berücksichtigt. Die jeweiligen Attacken-Strategien werden dadurch automatisch angepasst.

Danach ist die Sprache der Zielperson auszuwählen. Durch diesen Eintrag werden die Maskenangriffe angepasst (spezielle Schriftzeichen und Umlaute). Bitte beachten Sie, dass das „Encoding“ für die Wordlist ggfs. anzupassen ist.

Wenn der „Wordlister“ aktiviert ist, wird nach dem START subjektive Eckpunkte zur Zielperson abgefragt. Durch diese Eingaben wird eine umfangreiche subjektive Wordlist erzeugt. Im Feld „Standard-Wordlist“ werden sämtliche Sonderzeichen, Zahlen und Zahlenkombinationen und die Geburtsjahr 1980 bis 2040 automatisch

vorgegeben. Händische Einträge in diesem Feld sind problemlos möglich. Sie werden durch Komma getrennt. Auch das reinkopieren von Informationen ist möglich. Eine Trennung durch Kommas wird automatisch vorgenommen. Diese Einträge werden mit sämtlichen anderen Einträgen kombiniert. Das Ergebnis wird in den Ordner „_Wordlists“ exportiert.

Unter Wordlist können Sie eine beliebige Wordlist eintragen. Die „GovCracker_Wordlist.txt“ ist voreingestellt.

Die Anzahl der „Generate Rules“ wird automatisch vorgegeben und wird durch die Hash-Analyse automatisch voreingestellt. Dieser Wert kann bei Bedarf händisch geändert werden.

Die eingegebenen subjektiven Parameter zur Zielperson können Sie ex- oder importieren, um diese ggfs. mehrfach zu benutzen.

1.2.6 Batchjob

In diesem Bereich werden die gesammelten Batchjobs gesammelt und können gemeinsam gestartet werden.

1.2.7 Hash-Identifier

In diesem Bereich kann eine Hash-Datei ausgewählt werden. Diese wird anschließend analysiert. Alle in Betracht kommenden Hashtypen werden angezeigt.

2 GovCracker-Tools

2.1 Wordlist-Download

In diesem Bereich werden Fundstellen zu guten Wordlists angezeigt. Die Verlinkungen benutzen Sie auf eigene Gefahr.

Die besten und umfangreichsten Wordlists sind unter www.weakpass.com eingestellt.

2.2 WPA/WPA2 (hcxtools)

Hier können Sie mitgeschnittene WLAN-Handshake-Dateien (bspw. von airodump-ng) in ein nutzbares Hash-Format konvertieren.

2.3 Wordlister

Einer der effektivsten Angriffe sind subjektive Wordlists. Subjektive Wordlists enthalten Eckpunkte zur Zielperson, wie bspw. Name und Vorname der Zielperson, des Ehepartners, der Kinder, Geburtsdaten, Hobbies, Name der Haustiere, Lieblingsverein, usw.

Aus diesen Informationen können mit Wordlist-Generatoren Millionen von Passwort-Kandidaten erstellt werden, in dem Zahlen und Sonderzeichen kombiniert und Permutationen durchgeführt werden.

Es werden subjektive Eckpunkte zur Zielperson abgefragt. Durch diese Eingaben wird eine umfangreiche subjektive Wordlist erzeugt. Im Feld „Standard-Wordlist“ werden sämtliche Sonderzeichen, Zahlen und Zahlenkombinationen und die Geburtsjahr 1980 bis 2040 automatisch vorgegeben. Händische Einträge in diesem Feld sind problemlos möglich. Diese Einträge werden mit sämtlichen anderen Einträgen kombiniert. Sie werden durch Komma getrennt. Auch das reinkopieren von Informationen ist möglich. Eine Trennung durch Kommas wird automatisch vorgenommen.

Das Ergebnis wird in den Ordner „_Worlists“ exportiert.

3 Einstellungen

3.1.1 Sprache

Hier können Sie die Sprache auswählen. Z.Zt. stehen „Englisch“ und „Deutsch“ zur Verfügung. Die Sprachen werden sukzessiv erweitert.

3.1.2 GovTools Pfad

Hier können Sie den Pfad zum GovTools Ordner hinterlegen. Dadurch können Sie oben links über den Button „GovTools“ schnell starten.

3.1.3 Favorisierte Wordlist

Hier kann Ihre favorisierte Wordlist als Grundeinstellung hinterlegt werden.

3.1.4 Nur CPU benutzen (-D 1).

Hier wird nur die CPU für die Berechnungen genutzt. GPUs bleiben außen vor.

3.1.5 Pot-File deaktivieren (--potfile-disable)

GovCracker sammelt alle geknackten Passwörter in der Datei „GovCracker.potfile“ die sich im Ordner „_Crackout“ befindet. GovCracker exportiert jedes geknackte Passwort in den Ordner „_Crackout“.

3.1.6 Log-Files

Diese GovCracker-Option sammelt alle gestarteten GovCracker-Kommandos in dem GovCracker-Ordner „Logs“. Die Dateibezeichnung setzt sich wie folgt zusammen: Sessionname + Ausführungsdatum (JJJJ_MM_TT_HH_mm_ss) + Hashtyp. Die Logs sind hilfreich, um alle Angriffe gegen einen Hash zu dokumentieren.

3.1.7 Optimierte OpenCL-Kernel (-O)

Dadurch wird der Angriff so konfiguriert, dass die optimierten OpenCL-Kernels verwendet werden, jedoch auf Kosten einer begrenzten Unterstützung hins. der Passwortlänge.

3.1.8 Status-Mail

Hier können Sie den Zeitabstand für die Status-Mails in Minuten eintragen.

3.1.9 Geschwindigkeit (-w)

Die Geschwindigkeit kann hier eingestellt werden bzw. es kann entschieden werden, wieviel Ressourcen für zur Verfügung gestellt werden.

1 – Low
2 – Standard
3 – Speed
4 – Race

3.1.10 Temperaturüberwachung (--hwmon-temp-abort=90)

Durch die Temperaturüberwachung können Hardwarefehler vermieden werden. Es sind Einstellungen zwischen 70 – 100°C möglich. Eine Temperatur von 90°C sollte grds. nicht überschritten werden.

3.1.11 Devices (-d)

GovCracker versucht grds. alle Devices/Geräte (CPUs und GPUs) für die Berechnungen zu nutzen. Über diese Funktion können bestimmte Devices/Geräte ausgewählt werden.

3.1.12 Weitere Parameter

Hier können Sie weitere Parameter für Hashcat eingeben.

3.1.13 Brain (Client-Side)

Die Brain Funktion ermöglicht es, dass alle Passwortkandidaten die zu einem Hash abgeprüft, wurden in das „Brain“ geschrieben werden. Dadurch werden nie gleiche Passwortkandidaten zu einem Hash zweimal abgeprüft, bspw. durch eine Wordlist-Attacke und später einer Masken-Attacke. Dadurch ist es auch möglich, mit mehreren Computern oder GPU-Server einen einem Hash gleichzeitig zu arbeiten, ohne dass Passwortkandidaten mehrfach abgeprüft werden.

Die Brain (Client-Side) ist die Brain-Seite, die die Attacken ausführt, also der Cracker. Dagegen ist die Brain (Server-Side) die Seite, auf der die abgeprüften Passwort-Kandidaten aufgezeichnet werden.

3.1.14 Brain (Server-Side)

Die Brain-Server-Side sammelt alle abgeprüften Hashes der unterschiedlichen Rechner. Bei Server wird die IP-Adresse im Netzwerk eingetragen.

Unter Port kann der Port eingestellt werden, grds. Port: 80.

Das Brain-Passwort ist frei wählbar.

3.1.15 E-Mail (SMTP)

Hier können Sie SMTP-Parameter erfassen, an die eine Benachrichtigung gesendet wird.

Anlage 1

(Quelle: 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