

@JOELGMSEC



CLOUDTOPOLIS: ROMPIENDO HASHES
EN LA NUBE [GRATIS!]

Cloudtopolis: Rompiendo hashes en la nube (gratis!)

whoami

Joel Gámez Molina

- Administrador de sistemas durante +10 años
- Ex-Director técnico de Cyberguard
- Actualmente Security Analyst en Deloitte
- Creador y escritor del blog darkbyte.net



twitter.com/JoeIGMsec



github.com/JoeIGMSec



m.publicinbox.com/JoeIGMSec



DISCLAIMER

- No me hago responsable de su mal uso
- No subas hashes privados a la nube
- Esta herramienta ha sido creada para fines educativos y CTF's
- Respeta las normas de uso



Cloudtopolis: Rompiendo hashes en la nube (gratis!)

CONTENIDO

Cloudtopolis es una herramienta que facilita la instalación y el aprovisionamiento de Hashtopolis en la plataforma Google Cloud Shell, de forma rápida y totalmente desatendida (y además, gratis!). Junto con Google Colaboratory, nos permite romper hashes sin necesidad de hardware dedicado desde cualquier navegador.



Password
Cracking



Obtención de
Hashes



Google Cloud
Platform



Cloudtopolis
Free vs Pro

Cloudtopolis: Rompiendo hashes en la nube (gratis!)



Password
Cracking

Password Cracking

En criptoanálisis y seguridad informática, el password cracking es el proceso de recuperación de contraseñas a partir de un hash conocido. Para llevarlo a cabo, se comprueba que el valor de una contraseña coincide con el hash de forma consecutiva.

Un acercamiento común, es el ataque de fuerza bruta, que consiste en adivinar una contraseña a través de prueba y error.



Cloudtopolis: Rompiendo hashes en la nube (gratis!)

Password Cracking

Hash-Mode	Hash-Name	Example
0	MD5	8743b52063cd84097a65d1633f5c74f5
100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130
400	WordPress, Joomla (MD5)	\$P\$984478476lagS59wHZvyQMArzfx58u.
1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b
1400	SHA-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935
2500	WPA/WPA2	https://hashcat.net/misc/example_hashes/hashcat.hccapx
2501	WPA/WPA2 PMK	https://hashcat.net/misc/example_hashes/hashcat-pmk.hccapx
2600	md5(md5(\$pass))	a936af92b0ae20b1ff6c3347a72e5fbe
3000	LM	299bd128c1101fd6
7900	Drupal7	\$S\$C33783772bRXEx1aCsvY.dqgaaSu76XmVIKrW9Qu8IQlvxHlmzLf
8100	Citrix NetScaler	1765058016a22f1b4e076dccd1c3df4e8e5c0839ccded98ea
9900	Radmin2	22527bee5c29ce95373c4e0f359f079b

Password Cracking

Ataque de máscara

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQ..

?d = 0123456789

?s = « »!"#\$%&'()*+,-./,:<=>?@[\]^_`{}~

?a = ?l?u?d?s



Password Cracking

Diccionarios

- rockyou
- kaonashi
- xato–net
- darkcOde

Recursos

- seclists
- weakpass
- crackstation
- skullsecurity



- CAUTION -

HACKING DEMO '1

CRACKING PASSWD

Cloudtopolis: Rompiendo hashes en la nube (gratis!)

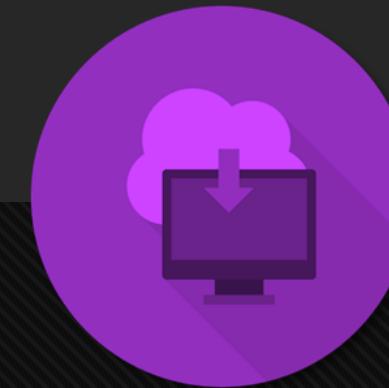
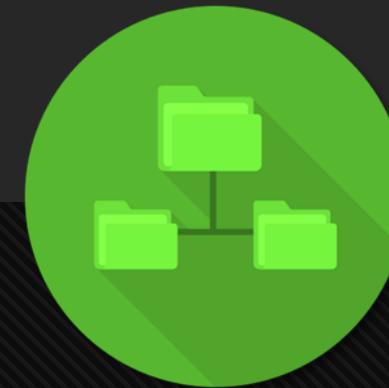


Obtención de
Hashes

Obtención de Hashes

Un hash es el resultado de una operación criptográfica, que tiene como objetivo codificar cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

Independientemente de la longitud de los datos de entrada, el valor del hash de salida siempre tendrá la misma longitud. Estos hashes, nos sirven para asegurar la integridad de los datos, almacenar contraseñas de forma segura y la firma de documentos electrónicos.



Obtención de Hashes

Ataques Wireless

- Airgeddon, Fluxion, Wifite..
- Aircrack Suite (Kali Linux)
- Pwnagotchi / Hash Monster
- Acrylic Wifi + Wireshark
- Evil Twin WPA2–PEAP



Obtención de Hashes

Bases de datos

- SQL Injection (sqlmap)
- Acceso web (PHPMyAdmin)
- Acceso con cliente (HeidiSQL)
- Explotación manual (BurpSuite)
- MSSQL (xp_dirtree / xp_cmdshell)



Obtención de Hashes

Sistemas Windows

- Procdump (lsass.exe)
- Secretsdump (Shadow Copy)
- Responder (Rogue Auth)
- CrackMapExec (NTDS.dit)
- Mimikatz, Metasploit, Powershell..



Obtención de Hashes

Copias de seguridad

- Bases de datos (.sql, .bak, .old)
- Imágenes del sistema (.vhdx)
- Máquinas virtuales (.vmdk)
- Capturas de red (.pcap)
- Backup online: Azure, AWS, etc..

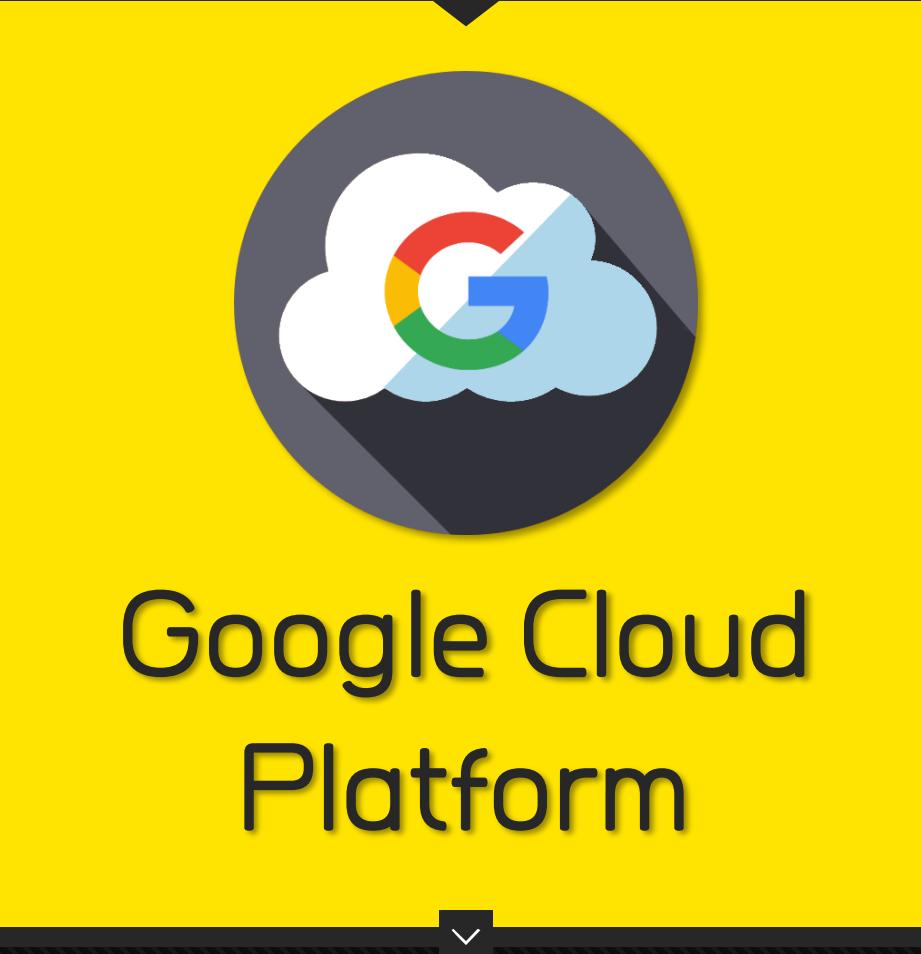


- CAUTION -

HACKING DEMO 2

HASHES & WIFI

Cloudtopolis: Rompiendo hashes en la nube (gratis!)



Cloudtopolis: Rompiendo hashes en la nube (gratis!)

Google Cloud Platform

Google Cloud Platform es un conjunto de servicios de computación en la nube, que se ejecuta en la misma infraestructura que Google utiliza para sus productos de usuario final, como Gmail , Google Drive o YouTube. Junto con un conjunto de herramientas de gestión, proporciona una serie de servicios en la nube que incluyen informática, almacenamiento, análisis de datos y aprendizaje automático.



Google Cloud

Google Cloud Platform

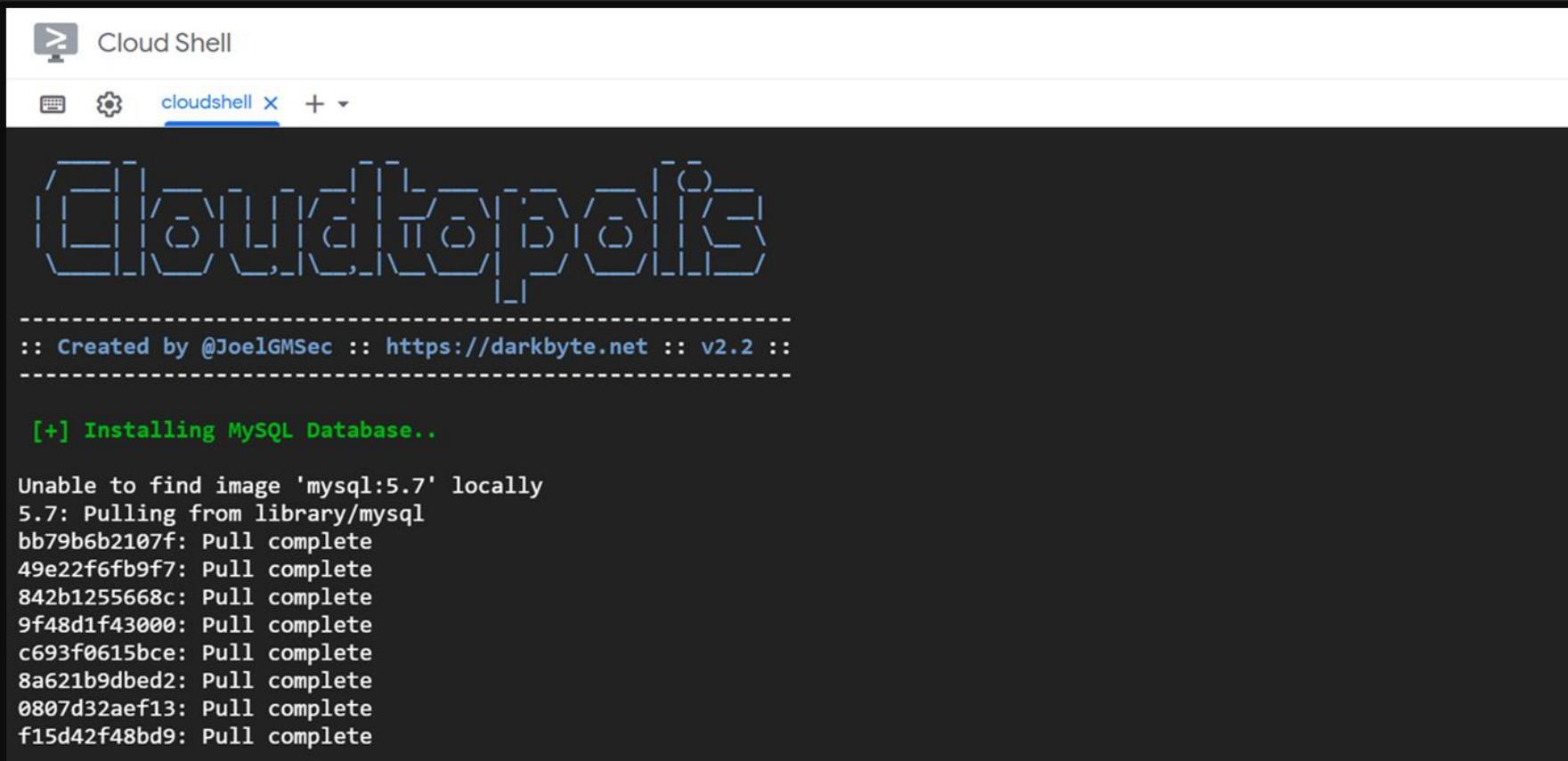
Google Cloud Shell

- Maquina virtual basada en Debian
- Almacenamiento persistente de 5 GB
- Su propósito es la gestión de GCloud
- Acceso desde cualquier navegador
- No tiene coste pero sí límites de uso



Cloudtopolis: Rompiendo hashes en la nube (gratis!)

Google Cloud Platform



The screenshot shows a Google Cloud Shell interface with a terminal window. The terminal title is "Cloud Shell" and the tab is "cloudshell". The terminal content includes a logo consisting of a grid of squares, followed by the text ":: Created by @JoelGMSec :: https://darkbyte.net :: v2.2 ::", and then a command for installing a MySQL database.

```
[+] Installing MySQL Database..  
Unable to find image 'mysql:5.7' locally  
5.7: Pulling from library/mysql  
bb79b6b2107f: Pull complete  
49e22f6fb9f7: Pull complete  
842b1255668c: Pull complete  
9f48d1f43000: Pull complete  
c693f0615bce: Pull complete  
8a621b9dbed2: Pull complete  
0807d32aef13: Pull complete  
f15d42f48bd9: Pull complete
```

Google Cloud Platform

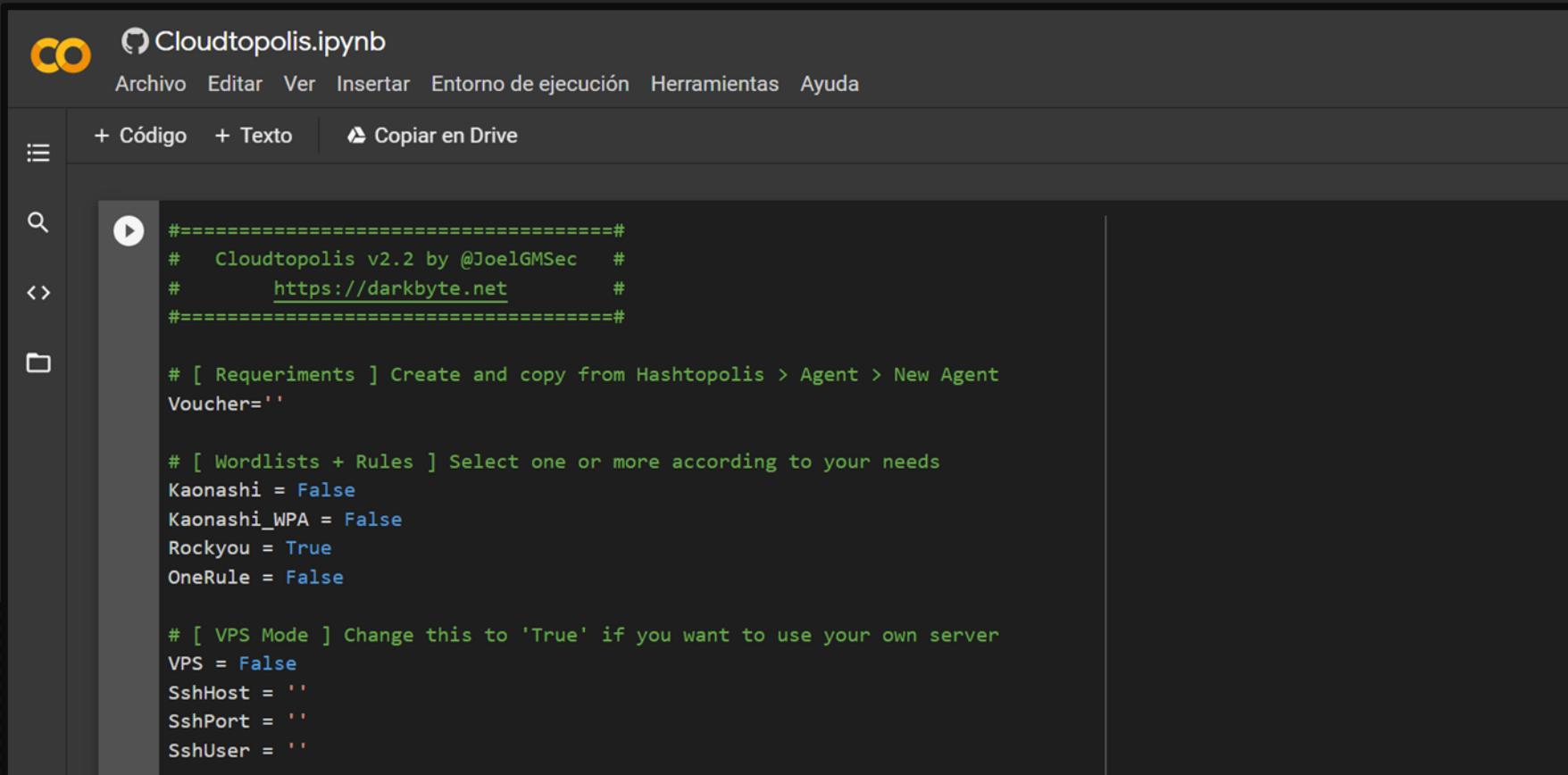
Google Colaboratory

- Maquina virtual basada en Ubuntu
- Aceleración gráfica muy potente
- Altas prestaciones sin persistencia
- Acceso desde cualquier navegador
- No tiene coste pero sí límites de uso



Cloudtopolis: Rompiendo hashes en la nube (gratis!)

Google Cloud Platform



The screenshot shows a Google Colab notebook titled "Cloudtopolis.ipynb". The interface includes a toolbar with file operations like "Archivo", "Editar", "Ver", "Insertar", "Entorno de ejecución", "Herramientas", and "Ayuda". Below the toolbar are buttons for "Código" and "Texto", and a "Copiar en Drive" button. On the left, there's a sidebar with icons for search, copy/paste, and folder navigation. The main code cell contains Python code for the Cloudtopolis tool:

```
#=====#
#  Cloudtopolis v2.2 by @JoelGMSec  #
#      https://darkbyte.net          #
#=====#

# [ Requirements ] Create and copy from Hashtopolis > Agent > New Agent
Voucher=''

# [ Wordlists + Rules ] Select one or more according to your needs
Kaonashi = False
Kaonashi_WPA = False
Rockyou = True
OneRule = False

# [ VPS Mode ] Change this to 'True' if you want to use your own server
VPS = False
SshHost = ''
SshPort = ''
SshUser = ''
```

Cloudtopolis: Rompiendo hashes en la nube (gratis!)



Cloudtopolis Free vs Pro

Qué es Cloudtopolis?

- Deploy de Hashtopolis desatendido
- Compatibilidad con VPS / GCloud
- Ejecución de hashcat desde Colab
- Uso colaborativo y compartido
- No necesita ninguna infraestructura



Cloudtopolis Free vs Pro

Cloudtopolis Free

- Límite de uso de Google Cloud Shell (50 h / semana)
- Accesible únicamente desde una sola cuenta de Gmail
- Límite de uso de Google Colaboratory (12 h / día)
- Tarjetas gráficas aleatorias (K80, T4, P4, P100..)
- Muchos agentes para obtener buenos resultados

Cloudtopolis Free vs Pro

Cloudtopolis Pro

- Sin límite de uso y accesible desde cualquier cuenta
- Continuidad indefinida sin exposición pública
- Acceso prioritario a unidades de GPU más potentes
- Más tiempo de ejecución en Google Colaboratory (24 h)
- Menos agentes para obtener los mismos resultados

- WARNING -

TRUE-LIVE DEMO
CLOUDTOPOLIS

Cloudtopolis: Rompiendo hashes en la nube (gratis!)

Cosas por hacer

- Notificaciones Push (Telegram)
- Compatibilidad con nubes gratuitas
- Contenedores propios (Docker)
- Automatización para crear cuentas
- Uso a través de la terminal
- Guía de uso paso a paso



Muchas gracias!

Preguntas?

