August 4-5, 2021

ARSENAL

#BHUSA @BLACKHATEVENTS

Cloudtopolis:

Zero Infrastructure Password Cracking

whoami

Joel Gámez Molina

(aka @JoelGMSec)

- System Administrator for +10 years
- Former Cyberguard Technical Director
- Currently Security Analyst at Deloitte
- Creator and writer of the blog darkbyte.net

twitter.com/JoelGMsec

github.com/JoelGMSec

mypublicinbox.com/JoelGMSec

Disclaimer

- I'm not a programmer
- Be carefully with terms and conditions
- Sensitive information could be exposed
- Free accounts have usage limits
- I have to take a lot of things for granted
- Don't do bad things 😇 😈

About the tool

Cloudtopolis is a tool that facilitates the installation and provisioning of Hashtopolis on Google Cloud Shell Platform, quickly and completely unattended (and for free!).

Together with Google Colaboratory, it allows us to break hashes without the need for dedicated hardware from any browser.

A little basic theory

In cryptanalysis and computer security, password cracking is the process of recovering passwords from a known hash. To do this, the value of a password is checked to ensure that it matches the hash consecutively.

A common approach is the brute force attack, which consists of guessing a password through trial and error.

Password Cracking

Hash-Mode	Hash-Name	Example
0	MD5	8743b52063cd84097a65d1633f5c74f5
100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130
400	WordPress, Joomla (MD5)	P984478476IagS59wHZvyQMArzfx58u.
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
3000	LM	299bd128c1101fd6

Password Cracking

Mask attack

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQ..

?d = 0123456789

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

?a = ?l?u?d?s

Password Cracking

Dictionaries

- rockyou
- kaonashi
- xato-net
- darkc0de

Resources

- seclists
- weakpass
- crackstation
- skullsecurity

Google Cloud Shell (Server)

Google Cloud Platform is a set of cloud computing services, running on the same infrastructure that Google uses for its end-user products, such as Gmail, Google Drive or YouTube.

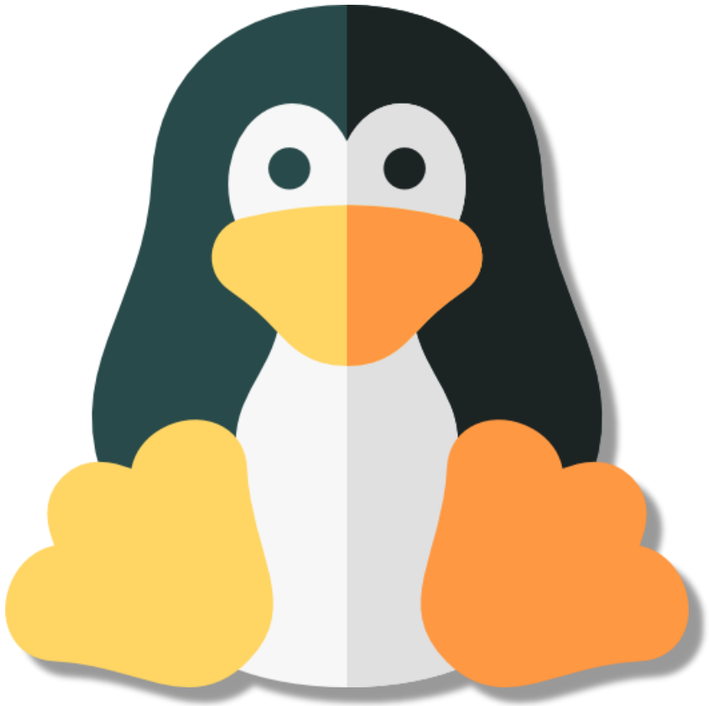
Along with a set of management tools, it provides a suite of cloud services including computing, storage, data analytics and machine learning.

Windows App (Client & Server)

- The installation of both parts is automatic
- Client allows us to use our own hardware
- Server raises an instance in Google Cloud Shell
- It is possible to connect to your own VPS
- There are no usage limits on client side
- Different accounts can be used collaboratively

Linux App (Client & Server)

- The installation of both parts is automatic
- Client allows us to use our own hardware
- Server raises instances on local or remote
- Deployment on server is done via docker
- There are no usage limits on client side
- Different accounts can be used collaboratively



Google Colaboratory (Client)

- Process of connecting to the server is automatic
- GPU is randomly depending on availability
- Can be accessed from your phone or any device
- Can be used for free or with a paid account
- There are usage limits on client side
- Different accounts can be used collaboratively


CLOUDTOPOLIS
DEMO!

Things to do

- Build my own all-in-one docker
- Automate Colab client with selenium
- Add more cloud providers (Azure, AWS..)
- Improve the collaborative network
- One-line clients using parameters
- Automate data migration between servers

Thank you!

Questions?