Cloudtopolis: Zero Infrastructure Password Cracking

@JoelGMSec

Whoami

Joel Gámez Molina

- Security Consultant en Deloitte (Red Team)
- Administrador de sistemas durante más de 10 años
- Ex-Director técnico de Cyberguard (2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell
- Ponente en congresos de ciberseguridad a nivel nacional e internacional (Black Hat USA 20/21)
- Creador del blog darkbyte.net y herramientas como AutoRDPwn: The Shadow Attack Framework

mypublicinbox.com/JoelGMSec

@JoelGMSec

Prólogo

Cloudtopolis es una herramienta multi-plataforma que facilita la instalación y el aprovisionamiento de Hashtopolis en Google Cloud Shell Platform, de forma rápida y completamente desatendida (¡y gratuita!).

Junto con Google Colaboratory, nos permite romper hashes sin necesidad de hardware dedicado desde cualquier navegador, o incluso, utilizando nuestros propios recursos de forma simultánea.

En términos técnicos, 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 en cuestión, de forma consecutiva.

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

Ataque de máscara

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

Password Cracking

Diccionarios

- ❑ rockyou
- ❑ kaonashi
- ❑ xato-net
- ❑ darkc0de

Recursos

- ❑ seclists
- ❑ weakpass
- ❑ crackstation
- ❑ skullsecurity

Google Cloud Shell (Servidor)

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.

Además de una gran cantidad de herramientas de gestión, esta plataforma, ofrece un conjunto de servicios en la nube que incluyen computación, almacenamiento, análisis de datos y aprendizaje automático.

Dentro de este entorno, existe una máquina virtual llamada Google Cloud Shell. Esta máquina basada en Debian, dispone de 5GB de espacio persistente y su finalidad es hacer de puente para administrar el resto de servicios contratados.

Windows App (Cliente & Servidor)

- El proceso de instalación y configuración es automático
- El cliente nos permite utilizar nuestro propio hardware
- El servidor crea una instancia en Google Cloud Shell
- El cliente permite conectarse a un servidor VPS
- No existen límites de uso en la parte cliente
- Pueden usarse diferentes cuentas de forma simultánea

Linux App (Cliente & Servidor)

- El proceso de instalación y configuración es automático
- El cliente nos permite utilizar nuestro propio hardware
- El servidor crea instancias en local o en remoto
- El despliegue en el servidor se hace vía Docker
- No existen límites de uso en la parte cliente
- Pueden usarse diferentes cuentas de forma simultánea

Google Colaboratory (Cliente)

- El proceso de conexión al servidor es automático
- La GPU es aleatoria en función de la disponibilidad
- Se puede acceder desde cualquier dispositivo
- Se puede utilizar de forma gratuita o profesional
- Hay límites de uso en el lado del cliente
- Pueden usarse diferentes cuentas de forma simultánea


CLOUDTOPOLIS
DEMO!

Cosas por hacer

- Construir mi propio Docker “todo en uno”
- Automatizar el cliente de Colab con Selenium
- Añadir más proveedores Cloud (Azure, AWS..)
- Mejorar la red de colaboración (P2P)
- Aplicaciones *one-line* usando parámetros
- Automatizar la migración de datos entre servidores

Muchas Gracias!

Preguntas?