Passwords Hashes Cracking as Service (PHCaS)

Servicio de rotura de Hashes Online

Tipo de documento: Presentación
Autor del documento: CS³ Group (Pedro C. aka s4ur0n)
Documento: PHCaS.pdf (TLP:GREEN)
Versión: 1.1

Categoría: DOSSIER INFORMATIVO PHCaS
Fecha de elaboración: 31/01/2022
Nº de Páginas: 22

1. General

Password Hashes Cracking as Service (PHCaS)

Password Hashes Cracking as Service

Uno de los principales problemas con los hashes de las contraseñas para intentar su rotura *(ya que no es posible garantizarla actualmente con la capacidad de cálculo disponible debido a la complejidad que se emplee en las mismas)*, es **disponer del hardware adecuado** y **dedicado en exclusividad** para poder intentarlo. Esto es realizado mediante **diccionarios personalizados**, **reglas**, **máscaras** y **combinaciones híbridas** entre todos ellos.

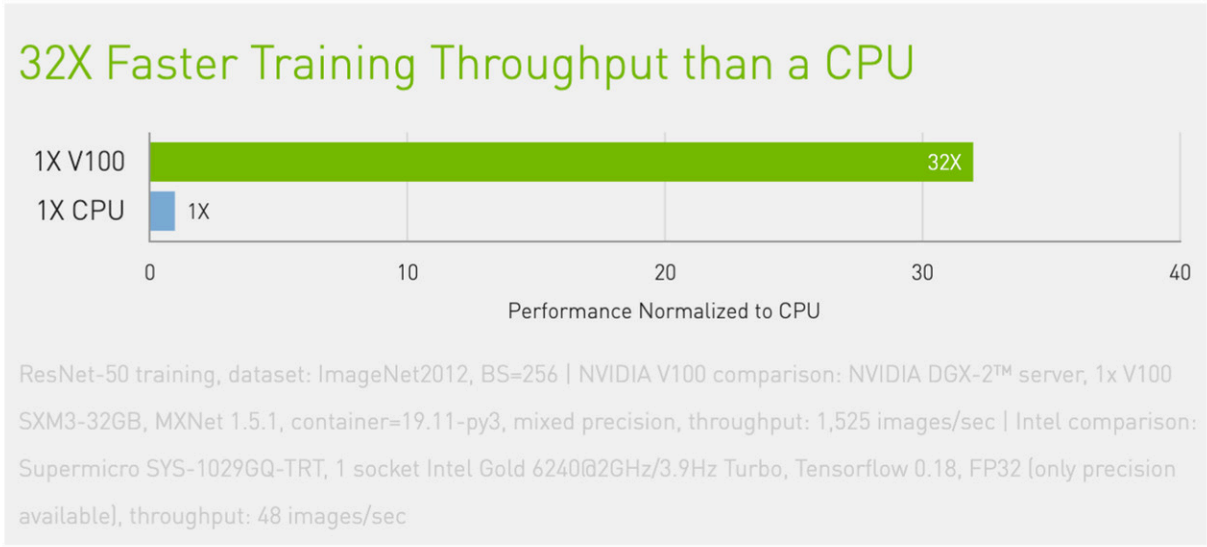
Incluso para realizar un **ataque de fuerza bruta**, es necesario disponer de equipos adecuados y muchas veces imposibles de conseguir, para poder intentarlo.

Nuestro servicio **PHCaS** de **rotura online de hashes** elimina la necesidad de disponer de **hardware dedicado** y **los gastos de energía eléctrica** derivados de su mantenimiento.

Es flexible, económico, disponible 24/7/365 y garantiza los **SLAs** contratados.

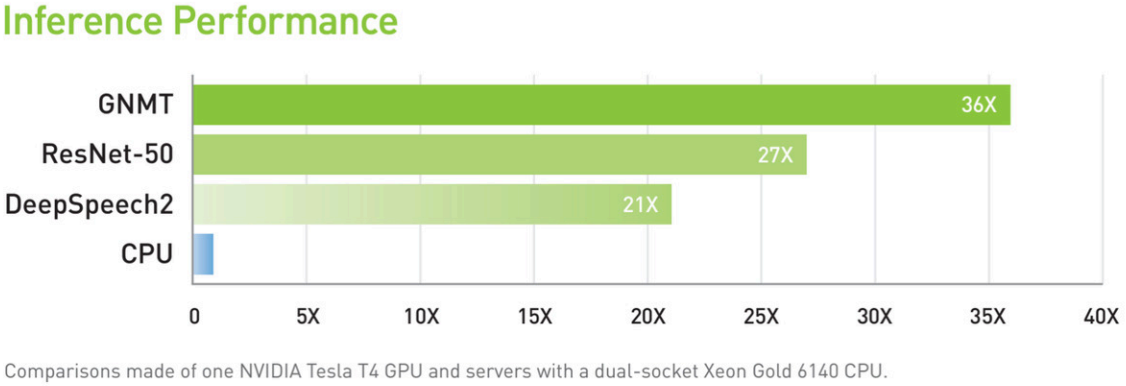
Password Hashes Cracking as Service

Nuestro **hardware dedicado** en el servicio, consiste en **agentes distribuidos** (clúster exclusivo según SLA contratado) basados en varias tarjetas gráficas de las **más potentes que existen en el mercado** empleando sus **GPUs** con alta capacidad de proceso (https://www.nvidia.com/en-us/data-center/v100/) con las **NVIDIA Tesla V100 SXM2 16 GB** (GV100 core, 5120 cores, 320 TMUs, 128 ROPs, 16 GB RAM HBM2, 4 Kb de bus).



Password Hashes Cracking as Service

Además, se dispone de **nuevos agentes bajo demanda según SLA contratado** con las **GPUs NVIDIA Tesla T4** (https://www.nvidia.com/content/dam/en-zz/Solutions/Data-Center/tesla-t4/t4-tensor-core-datasheet-951643.pdf) con un menor consumo (**75 W** vs 250 W, 320 núcleos Turing sensor, 2560 núcleos Nvidia CUDA, GDDR6 de 16 GB y un ancho de banda de más de 320 GB/s).



Password Hashes Cracking as Service

Graphics Processor	
GPU Name:	GV100
Architecture:	Volta
Foundry:	TSMC
Process Size:	12 nm
Transistors:	21,100 million
Die Size:	815 mm²

Memory	
Memory Size:	16 GB
Memory Type:	HBM2
Memory Bus:	4096 bit
Bandwidth:	897.0 GB/s

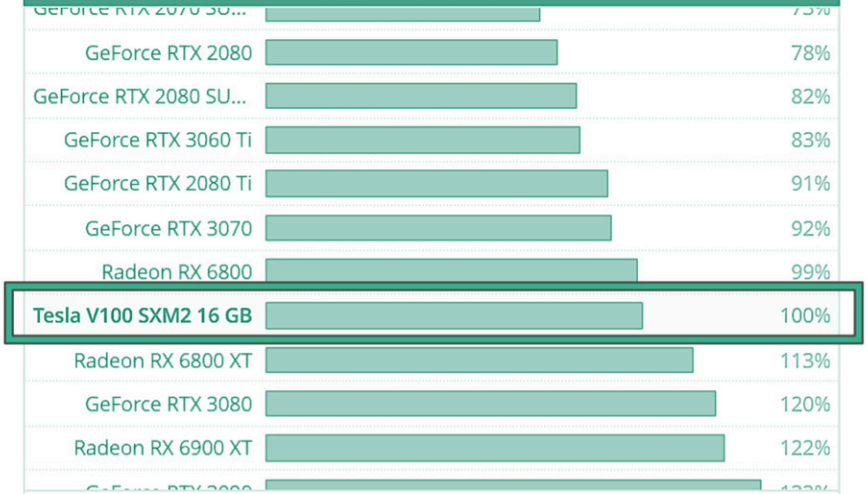
Graphics Features	
DirectX:	12 (12_1)
OpenGL:	4.6
OpenCL:	1.2
Vulkan:	1.2
CUDA:	7.0
Shader Model:	6.4

Graphics Card	
Release Date:	Jun 21st, 2017
Generation:	Tesla (Vxx)
Production:	Active
Bus Interface:	PCIe 3.0 x16

Clock Speeds	
Base Clock:	1312 MHz
Boost Clock:	1530 MHz
Memory Clock:	876 MHz 1752 Mbps effective

Board Design	
Slot Width:	Dual-slot
TDP:	250 W
Suggested PSU:	600 W
Outputs:	No outputs
Power Connectors:	None

Relative Performance



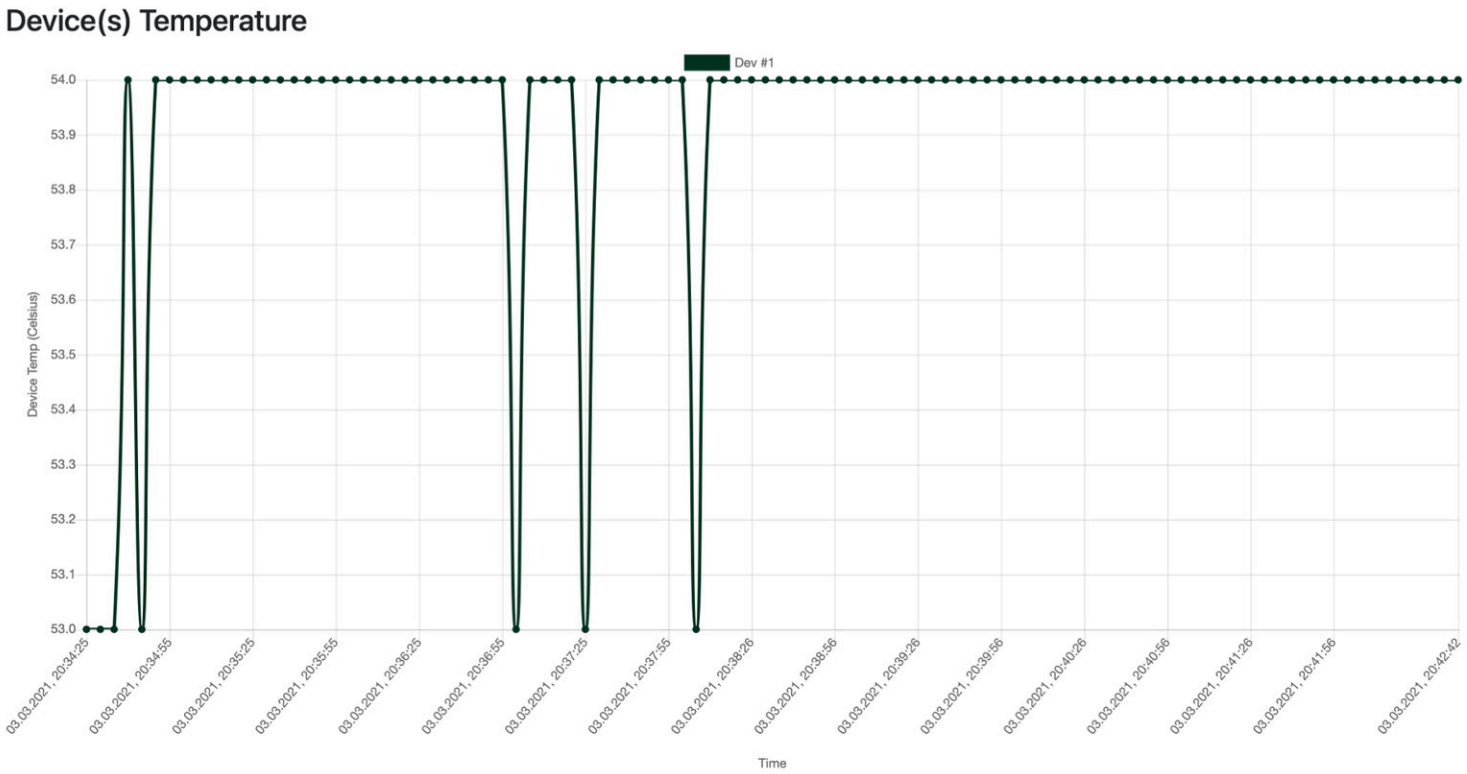
Based on TPU review data: "Performance Summary" at 1920x1080, 4K for 2080 Ti and faster.
Performance estimated based on architecture, shader count and clocks.

Render Config	
Shading Units:	5120
TMUs:	320
ROPs:	128
SM Count:	80
Tensor Cores:	640
L1 Cache:	128 KB (per SM)
L2 Cache:	6 MB

Theoretical Performance	
Pixel Rate:	195.8 GPixel/s
Texture Rate:	489.6 GTexel/s
FP16 (half) performance:	31.33 TFLOPS (2:1)
FP32 (float) performance:	15.67 TFLOPS
FP64 (double) performance:	7.834 TFLOPS (1:2)

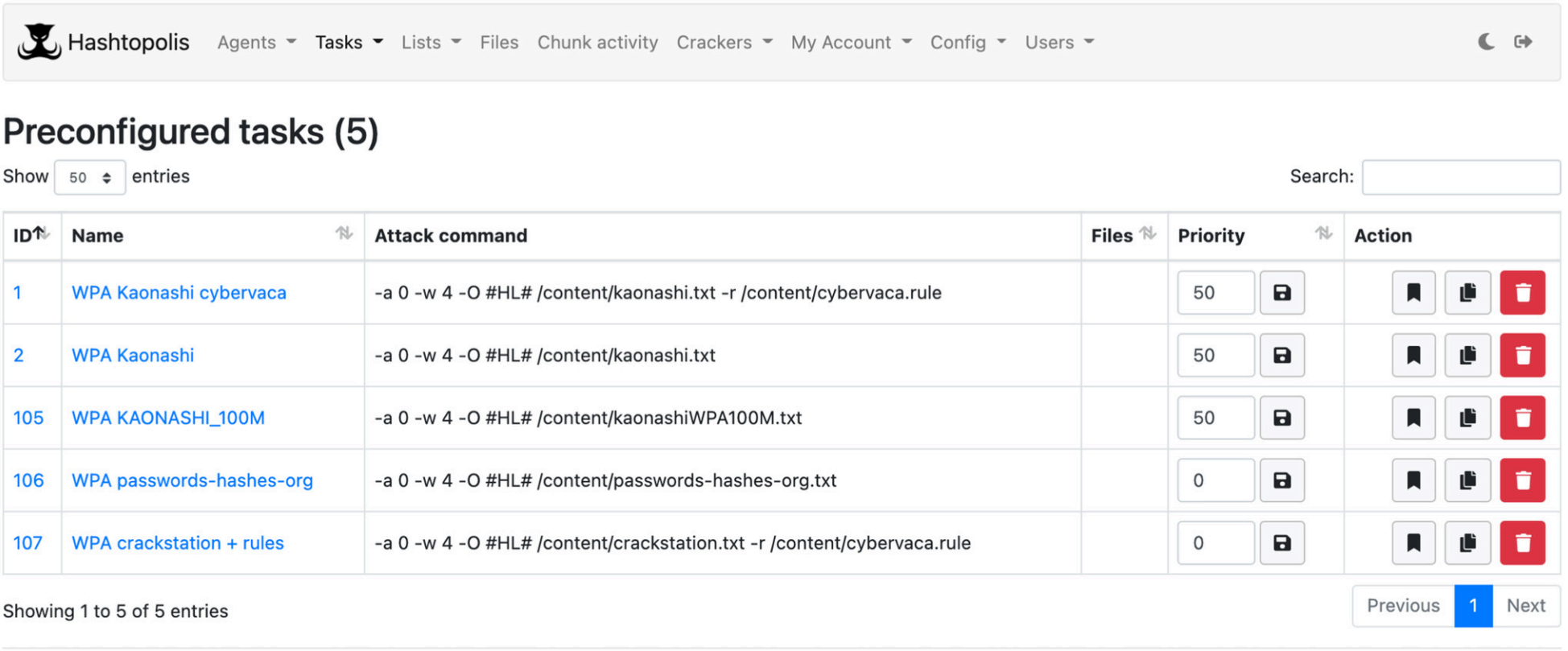
Password Hashes Cracking as Service

El alojamiento en **Cloud** en uno de los principales **CPDs** mundiales con redundancia en varios continentes, garantiza en todo momento las **condiciones ideales de trabajo** con la **alimentación eléctrica adecuada**, excelente refrigeración y control de **temperatura** (nunca superior a 90º C) y **disponibilidad 24/7/365** sin que tenga que preocuparse de su funcionamiento o averías de hardware (cambio inmediato de tarjeta en caso de error).



Password Hashes Cracking as Service

Panel de control **exclusivo** y **no compartido** con sus usuarios, contraseñas, listas de hashes, reglas, máscaras, API propia, etc. basado en **hashtopolis** con monitorización continua de las tareas y **disponibilidad para cambios 24/7/365**



Password Hashes Cracking as Service

Diccionarios incluidos **descomprimidos** sin importar el espacio ocupado en las unidades de almacenamiento (**discos SSD** de alto rendimiento):

- Crackstation (16 GB descomprimido)
- Kaonashi (2.35 GB comprimido)
- Passwords-hashes-org.txt (5 GB comprimido)
- KaonashiWPA100M (323.9 MB comprimido –especial castellano-)
- Etc.

Ofrecemos la posibilidad de **personalización de diccionarios** basados en idiomas, comportamientos, patrones observados, aficiones, crawling de contenidos ofrecidos en web, etc. (**consultar precios**).

Password Hashes Cracking as Service

Otras características del servicio:

- Reglas **avanzadas** para hashcat.
- **Máscaras** ordenadas para hashcat y para el **tipo** de hash en función de su longitud y características previas.
- Máscaras para **fuerza bruta** con varios juegos de caracteres (incluye francés, inglés, árabe, ruso, chino, etc.) con sus juegos específicos.
- **Tareas predefinidas configuradas** para el tipo de hash (subir hash y asignar tarea).
- Selección de **prioridad** para las tareas.
- **Importación/Exportación** de hashes pre-computados
- **Avisos a Telegram/Discord/Otros** con la rotura de hashes, tareas, etc.

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

MD4	GOST R 34.11-94	md5($salt.sha1($salt.$pass))
MD5	Half MD5	md5($salt.utf16le($pass))
SHA1	Java Object hashCode()	md5(md5($pass))
SHA2-224	Keccak-224	md5(md5($pass).md5($salt))
SHA2-256	Keccak-256	md5(sha1($pass))
SHA2-384	Keccak-384	md5(sha1($pass).md5($pass
SHA2-512	Keccak-512	a1($pass))
SHA3-224	Whirlpool	md5(sha1($salt).md5($pass)
SHA3-256	SipHash	md5(strtoupper(md5($pass))
SHA3-384	BitShares v0.x -	md5(utf16le($pass).$salt)
SHA3-512	sha512(sha512_bin(pass))	sha1($pass.$salt)
RIPEMD-160	md5($pass.$salt)	sha1($salt.$pass)
BLAKE2b-512	md5($salt.$pass)	sha1($salt.$pass.$salt)
GOST R 34.11-2012 (Streebog)	md5($salt.$pass.$salt)	sha1($salt.sha1($pass))
256-bit, big-endian	md5($salt.md5($pass))	sha1($salt.utf16le($pass))
GOST R 34.11-2012 (Streebog)	md5($salt.md5($pass.$salt))	sha1($salt1.$pass.$salt2)
512-bit, big-endian	md5($salt.md5($salt.$pass))	sha1(CX)

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

sha1(md5($pass))
sha1(md5($pass).$salt)
sha1(md5($pass.$salt))
sha1(md5(md5($pass)))
sha1(sha1($pass))
sha1(utf16le($pass).$salt)
sha256($pass.$salt)
sha256($salt.$pass)
sha256($salt.$pass.$salt)
sha256($salt.utf16le($pass))
sha256(md5($pass))
sha256(sha256($pass).$salt)
sha256(sha256_bin($pass))
sha256(utf16le($pass).$salt)
sha512($pass.$salt)
sha512($salt.$pass)
sha512($salt.utf16le($pass))
sha512(utf16le($pass).$salt)
Ruby on Rails Restful-Authentication
HMAC-MD5 (key = $pass)
HMAC-MD5 (key = $salt)
HMAC-SHA1 (key = $pass)
HMAC-SHA1 (key = $salt)
HMAC-SHA256 (key = $pass)
HMAC-SHA256 (key = $salt)
HMAC-SHA512 (key = $pass)
HMAC-SHA512 (key = $salt)
HMAC-Streebog-256 (key = $pass), big-endian
HMAC-Streebog-256 (key = $salt), big-endian
HMAC-Streebog-512 (key = $pass), big-endian
HMAC-Streebog-512 (key = $salt), big-endian
CRC32
3DES (PT = $salt, key = $pass)
DES (PT = $salt, key = $pass)
ChaCha20
Skip32 (PT = $salt, key = $pass
PBKDF2-HMAC-MD5
PBKDF2-HMAC-SHA1
PBKDF2-HMAC-SHA256
PBKDF2-HMAC-SHA512
scrypt
phpass
Ansible Vault
Atlassian (PBKDF2-HMAC-SHA1)
Python passlib pbkdf2-sha512

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

Python passlib pbkdf2-sha256	Kerberos 5, etype 17, TGS-REP	AIX {ssha1}
Python passlib pbkdf2-sha1	Kerberos 5, etype 18, TGS-REP	AIX {ssha256}
TACACS+	Kerberos 5, etype 17, Pre-Auth	AIX {ssha512}
SIP digest authentication (MD5)	Kerberos 5, etype 18, Pre-Auth	LM
IKE-PSK MD5	NetNTLMv1 / NetNTLMv1+ESS	QNX /etc/shadow (MD5)
IKE-PSK SHA1	NetNTLMv2	QNX /etc/shadow (SHA256
WPA-PBKDF2-PMKID+EAPOL	Skype	QNX /etc/shadow (SHA512
WPA-PMK-PMKID+EAPOL	Telegram Desktop App	DPAPI masterkey file v1
IPMI2 RAKP HMAC-SHA1	Passcode (PBKDF2-HMAC-SHA1)	DPAPI masterkey file v2
CRAM-MD5		GRUB 2
iSCSI CHAP authentication, MD5(CHAP)	Telegram Mobile App Passcode (SHA256)	MS-AzureSync PBKDF2-H SHA256
JWT (JSON Web Token)	PostgreSQL CRAM (MD5)	BSDi Crypt, Extended DES
Kerberos 5, etype 23, AS-REQ Pre-Auth	MySQL CRAM (SHA1)	NTLM
	XMPP SCRAM	macOS v10.4, macOS v10
Kerberos 5, etype 23, TGS-REP	RACF	MacOS v10.6
Kerberos 5, etype 23, AS-REP	AIX {smd5}	macOS v10.7

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

macOS v10.8+ (PBKDF2-SHA512)
Radmin2
Samsung Android Password/PIN
bcrypt $2*$, Blowfish (Unix)
md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)
descrypt, DES (Unix), Traditional DES
sha256crypt 5, SHA256 (Unix)
sha512crypt 6, SHA512 (Unix)
Windows Phone 8+ PIN/password
Cisco-ASA MD5
Cisco-IOS 8 (PBKDF2-SHA256)
Cisco-IOS 9 (scrypt)
Cisco-IOS type 4 (SHA256)
Cisco-PIX MD5
Citrix NetScaler (SHA1)
Citrix NetScaler (SHA512)
Domain Cached Credentials (DCC), MS Cache
Domain Cached Credentials 2 (DCC2), MS Cache 2
FortiGate (FortiOS)
ArubaOS
Juniper IVE
Juniper NetScreen/SSG (ScreenOS)
Juniper/NetBSD sha1crypt
MSSQL (2000)
MSSQL (2005)
MSSQL (2012, 2014)
PostgreSQL
Oracle H: Type (Oracle 7+)
Oracle S: Type (Oracle 11+)
Oracle T: Type (Oracle 12+)
MySQL323
MySQL4.1/MySQL5
MySQL A (sha256crypt)
Sybase ASE
hMailServer
DNSSEC (NSEC3)
CRAM-MD5 Dovecot
SSHA-256(Base64), LDAP {SSHA256}
SSHA-512(Base64), LDAP {SSHA512}
RedHat 389-DS LDAP (PBKDF2-HMAC-SHA256)

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

FileZilla Server >= 0.9.55
ColdFusion 10+
Apache $apr1$ MD5, md5apr1, MD5 (APR)
Episerver 6.x < .NET 4
Episerver 6.x >= .NET 4
nsldap, SHA-1(Base64), Netscape LDAP SHA
nsldaps, SSHA-1(Base64), Netscape LDAP SSHA
SAP CODVN B (BCODE)
SAP CODVN B (BCODE) from RFC_READ_TABLE
SAP CODVN F/G (PASSCODE)
SAP CODVN F/G (PASSCODE) from RFC_READ_TABLE
SAP CODVN H (PWDSALTEDHASH) iSSHA-1
PeopleSoft
PeopleSoft PS_TOKEN
SolarWinds Orion
Lotus Notes/Domino 5
Lotus Notes/Domino 6
Lotus Notes/Domino 8
Oracle Transportation Management (SHA256)
Huawei sha1(md5($pass).$salt)
AuthMe sha256
AES Crypt (SHA256)
BitLocker
eCryptfs
LUKS
VeraCrypt
FileVault 2
DiskCryptor
Android FDE (Samsung D
Android FDE <= 4.3
Apple File System (APFS
TrueCrypt
PDF 1.1 - 1.3 (Acrobat 2
PDF 1.1 - 1.3 (Acrobat 2 collider #1
PDF 1.1 - 1.3 (Acrobat 2 collider #2
PDF 1.4 - 1.6 (Acrobat 5
PDF 1.7 Level 3 (Acrobat
PDF 1.7 Level 8 (Acrobat 11)
MS Office 2007
MS Office 2010

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

MS Office 2013
MS Office <= 2003 $0/$1, MD5 + RC4
MS Office <= 2003 $0/$1, MD5 + RC4, collider #1
MS Office <= 2003 $0/$1, MD5 + RC4, collider #2
MS Office <= 2003 $3/$4, SHA1 + RC4
MS Office <= 2003 $3, SHA1 + RC4, collider #1
MS Office <= 2003 $3, SHA1 + RC4, collider #2
Open Document Format (ODF) 1.2 (SHA-256, AES)
Open Document Format (ODF) 1.1 (SHA-1, Blowfish)
Apple Keychain
Apple Secure Notes
JKS Java Key Store Private Keys (SHA1)
1Password, agilekeychain
1Password, cloudkeychain
Password Safe v2
Password Safe v3
LastPass + LastPass sniffed
KeePass 1 (AES/Twofish) and KeePass 2 (AES)
Bitcoin/Litecoin wallet.dat
Electrum Wallet (Salt-Type 1-5)
Blockchain, My Wallet
Blockchain, My Wallet, V2
Blockchain, My Wallet, Second Password (SHA256)
Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256
Ethereum Wallet, PBKDF
HMAC-SHA256
Ethereum Wallet, SCRYP
MultiBit Classic .key (MD5
MultiBit HD (scrypt)
7-Zip
RAR3-hp
RAR5
PKZIP (Compressed)
PKZIP (Compressed Mult
PKZIP (Mixed Multi-File)
PKZIP (Mixed Multi-File Checksum-Only)
PKZIP (Uncompressed)
PKZIP Master Key
PKZIP Master Key (6 byte optimization)
SecureZIP AES-128

Password Hashes Cracking as Service

Hashes admitidos en el servicio:

SecureZIP AES-192
SecureZIP AES-256
iTunes backup < 10.0
iTunes backup >= 10.0
WinZip
Android Backup
AxCrypt
AxCrypt in-memory SHA1
WBB3 (Woltlab Burning Board)
vBulletin < v3.8.5
vBulletin >= v3.8.5
PHPS
SMF (Simple Machines Forum) > v1.1
MediaWiki B type
Redmine
Joomla < 2.5.18
OpenCart
PrestaShop
Tripcode
Drupal7
osCommerce, xt:Commerce
PunBB
MyBB 1.2+, IPB2+ (Invision Power Board)
Django (PBKDF2-SHA256)
Django (SHA-1)
Web2py pbkdf2-sha512
TOTP (HMAC-SHA1)

2. Condiciones económicas

Password Hashes Cracking as Service (PHCaS)

Password Hashes Cracking as Service

Condiciones económicas generales 2022:

- **Agentes(*):** 5 (cinco) GPUs **NVIDIA Tesla (modelo V100 o T4)** con dedicación exclusiva al servicio **24/7/365**.
- **Panel de control**: Dedicado sin compartir con otros usuarios (Servidor independiente).
- **Alta del servicio**: Sin coste.
- **Precio mensual**:
  - **5 tarjetas gráficas** a 30 euros/mes/unidad = 150 euros/mes (alquiler de hardware e infraestructura del clúster incluyendo energía eléctrica).
  - **1 servidor dedicado** a 30 euros/mes (alquiler infraestructura hashtopolis)
- **Ampliación de GPUs (tarjetas gráficas):** Consultar disponibilidad.

(*) Contratación mínima: **1 mes**. Impuestos vigentes no incluidos.

*Contratación sujeta al pago **por adelantado mensual** de las cantidades acordadas bajo SLA. Prohibido terminantemente la minería de criptodivisas o similares. Sujeto a cualquier tipo de cláusula de cancelación del proveedor de servicio en Cloud en caso de abuso y/o cambios en los términos y condiciones de su servicio, que deberán ser aceptadas por el cliente final en la firma del contrato. En caso de cancelación anticipada del servicio prestado por cualquier parte, el Cliente declina emprender cualquier tipo de acción judicial, penal, reclamación económica o de cualquier otro tipo, quedando limitada la responsabilidad de CS³ Group, a responder como máximo, con la cantidad máxima de 30 días menos los días prestados como empleo del servicio contratado y que serán abonados al cliente final en caso de no poder prestar el servicio debido a causas propias o ajenas en el mismo (ver clausulas específicas de contratación).*

Password Hashes Cracking as Service

¿Qué opinan nuestros clientes?

- “Mínima inversión, bajo coste y alto rendimiento”.
- “Creíamos que las contraseñas de nuestros usuarios *‘eran seguras’* hasta comprobarlo ya que cumplían con las políticas del directorio activo".
- “Muy lento en WPA2 aunque sería eterno empleado nuestra infraestructura”.
- “Uso muy intuitivo y solventó la pérdida de una contraseña muy importante para recuperar información muy importante”.
- “Queríamos probarlo, contratamos sólo un mes y ahora no podemos prescindir de su servicio”.
- “Estamos salvados porque el hardware es muy caro y nadie tiene *‘esas cosas’* para poder romper algunas de nuestras contraseñas”.

Password Hashes Cracking as Service

“Habíamos probado otros pero es increíble para el Active Directory con sólo un cluster de 5 tarjetas. Hemos quedado asombrados de su capacidad de cálculo… ¡Ciento cinco mil millones de hashes por segundo!”

Keyspace searched:	68171179516 (39.61%)
Time spent:	10:16:16
Estimated time:	15:39:33
Speed:	105.45 GH/s
Hashlist	[redacted] (NTLM)
Cracker binary	Version: 6.1.1 — Binary Name: hashcat

Visual representation

Task Speed