Passwörter cracken in der Cloud

von Sascha Ohms

Über mich

- Sascha Ohms
- 26 Jahre
- IBM Notes / Domino Administrator
- "Hobby-Hacker"

Warum?

- (warum nicht?)
- nur-mal-eben-schnell etwas cracken
- eine Frage des Geldes
 - Rentabilität
 - Profit?

"Cloud"?

- sogenannte "Computing Instances"
- diverse Anbieter
 - o cloud.google.com
 - o aws.amazon.com (inkl. GPU!)
 - o rapidswitch.com

Zutaten

- GPU Instance für maximale Power
- aktuelle 64bit NVIDIA Treiber
 - http://www.nvidia.com/object/unix.html
- Hashcat
 - https://hashcat.net/files/hashcat-3.00.7z
- 'ne Liste mit Wörtern

Liste mit Wörtern?

- Dictionary Attack mit Klartextwörtern
- effizienter als Bruteforce bei großen Mengen
- Archive mit Listen
 - http://weakpass.com/lists
 - https://github.com/danielmiessler/SecLists
 - https://wiki.skullsecurity.org/Passwords
 - https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

Hash-Kätzchen?

- "World's fastest password cracker"
- Free + Open Source
- Multi-Platform
- hunderte unterstützte Algorithmen
- tl;dr einzig wahre Software!

Ablauf

- AWS EC2 Instance erstellen
- via SSH verbinden
- Treiber installieren
- Hashcat herunterladen + entpacken
- Wordlist laden
- go!

Ablauf #2

Bruteforce (alphanumerisch lower/capital) auf MD5 mit 5 zeichen

```
$ hashcat64.bin -m 1500 hash.txt -a 3 -1 ?1?u?d ?1?1?1?1?1
```

Dictionary Attack auf SHA1

```
$ hashcat64.bin -m 1400 hashes200k rockyou.txt -o cracked.txt
```

Vergleich: Preise

Kurzer Einblick in die Preise der Anbieter

Vergleich zu GTX 970: ~300€ einmalig

Google (CPU)

Machine Type	Price Per Hour
Standard Machines 1-32 Virtual CPUs	\$0.050 - \$1.600
Micro w/CPU Bursting 1 Virtual CPU	\$0.008- \$0.027
High Memory Machines 2-32 Virtual CPUs	\$0.126 - \$2.016

Amazon (GPU)

GPU Instances - Current Generation

g2.2xlarge	8	26	15	60 SSD	\$0.702 per Hour
g2.8xlarge	32	104	60	2 x 120 SSD	\$2.808 per Hour

https://cloud.google.com/compute/pricing

https://aws.amazon.com/ec2/pricing/

Ergo:

- auf kurze Sicht: ganz okay
- auf lange Sicht: lieber Hardware kaufen
 - o im Vergleich zu n EC2 Instances auf Dauer definitiv günstiger

Vergleich: Leistung

	GTX 1080	NVIDIA Grid
MD5	24943.1 MH/s	776.9 MH/s
SHA1	8538.1 MH/s	700.1 MH/s
SHA512	1071.1 MH/s	72592.4 kH/s

Quellen

- https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40
- https://hashcat.net/wiki/doku.php?id=hashcat
- https://aws.amazon.com/ec2/pricing/
- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using_cluster_computing.html
- https://hashcat.net/forum/thread-4143.html