

Password Cracking GUI

IT Security Workshop 2019

Jessica Kranz

Dr. Wolf Müller (HUB), Dominik Oepen (HiSolutions)

Motivation

Wörterbuchangriffe und Hashcat

Installation

Demo

Ausblick

Agenda



Hashcat bietet keine
parallele Ausführung
mehrerer Jobs auf
einer Ressource.



Vergleichen Sie Open
Source Tools, die Job
Scheduling bieten.

Motivation



Menschen merken sich
Wörter leichter als
kryptische Zeichenketten.



Passwörter entstammen
mit hoher
Wahrscheinlichkeit einem
Wörterbuch



Wörterbuchangriffe sind
um ein Vielfaches
schneller als Brute-Force-
Angriffe.



Adaptionen (z.B.
Anhängen von Ziffern am
Ende) können
berücksichtigt werden.

Wissensbasis - Wörterbuchangriffe

Hashcat

nach einem Tutorial von [Infosec](#)

Test-Hash erstellen

```
#echo -n „password“ | md5sum
```

Hashcat

nach einem Tutorial von [Infosec](#)

Test-Hash erstellen

```
#echo -n „password“ | md5sum
```

Hashliste erstellen (oder herunterladen)

```
#echo -n „password“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „1234567“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „geheim9“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „computer“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „iloveyou“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „admin“ | md5sum | tr -d „ -„ >> target_hashes.txt  
#echo -n „toor“ | md5sum | tr -d „ -„ >> target_hashes.txt
```

Hashcat nach einem Tutorial von [Infosec](#)

Pfad zum Wörterbuch ermitteln

```
# locate rockyou  
/usr/share/wordlists/rockyou.txt
```

Hashcat cracken lassen

```
# hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt /usr/share/wordlists/rockyou.txt
```

Hashcat

nach einem Tutorial von [Infosec](#)

Ergebnisse anzeigen

```
# cat cracked.txt
df53ca268240ca76670c8566ee54568a:computer
0b3364569955a095cd07ba6bad26091d:Iloveyou
21232f297a57a5a743894a0e4a801fc3:admin
0d13251926ed92cdb59e189f37665712:geheim9
5f4dcc3b5aa765d61d8327deb882cf99:password
fcea920f7412b5da7be0cf42b8c93759:1234567
```


Exkurs: Hashcat ausführbar machen

Hashcat starten

```
#hashcat -l  
* Device #1: Not a native Intel OpenCL runtime. Expect massive speed loss.  
You can use --force to override, but do not report related errors.  
No devices found/left.
```

Abhängigkeiten nachinstallieren

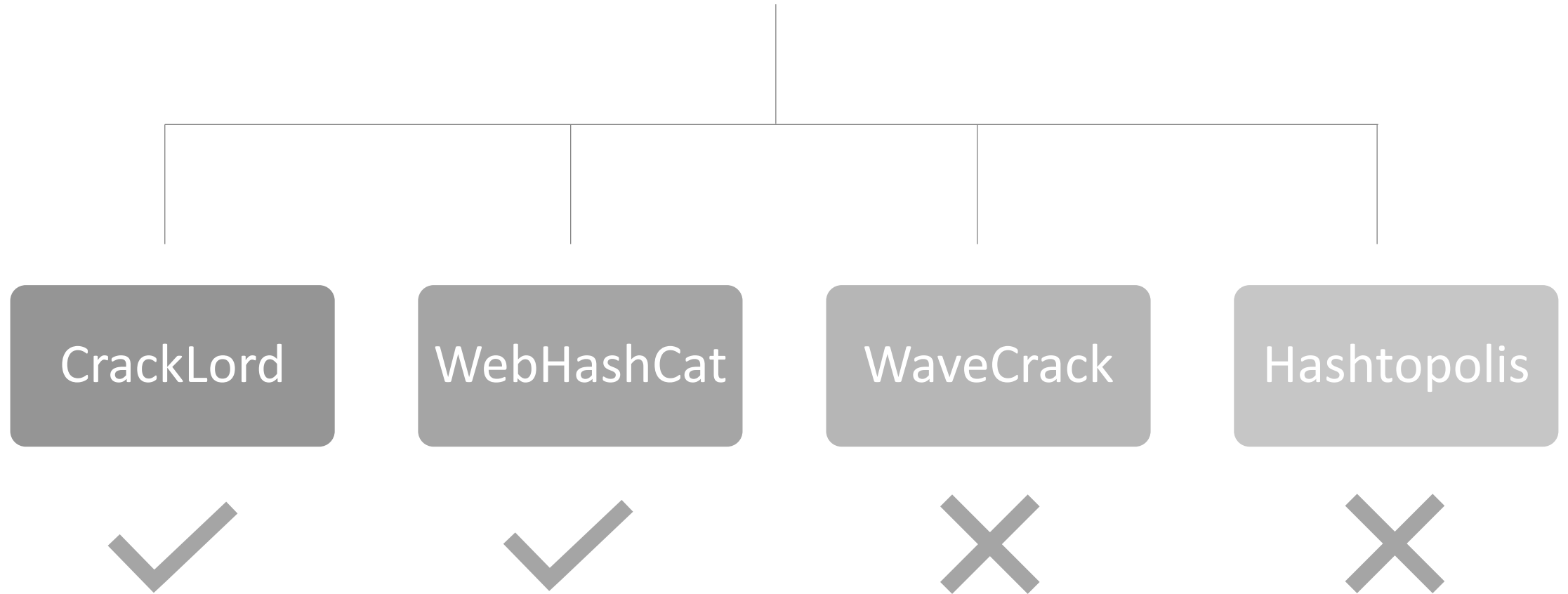
```
#apt install -y ocl-icd-libopencl1 nvidia-driver nvidia-cuda-toolkit  
#  
#apt-get remove libcublas10  
#apt-get install libcublas10=10.1.105-3+b1
```

Exkurs: Hashcat ausführbar machen

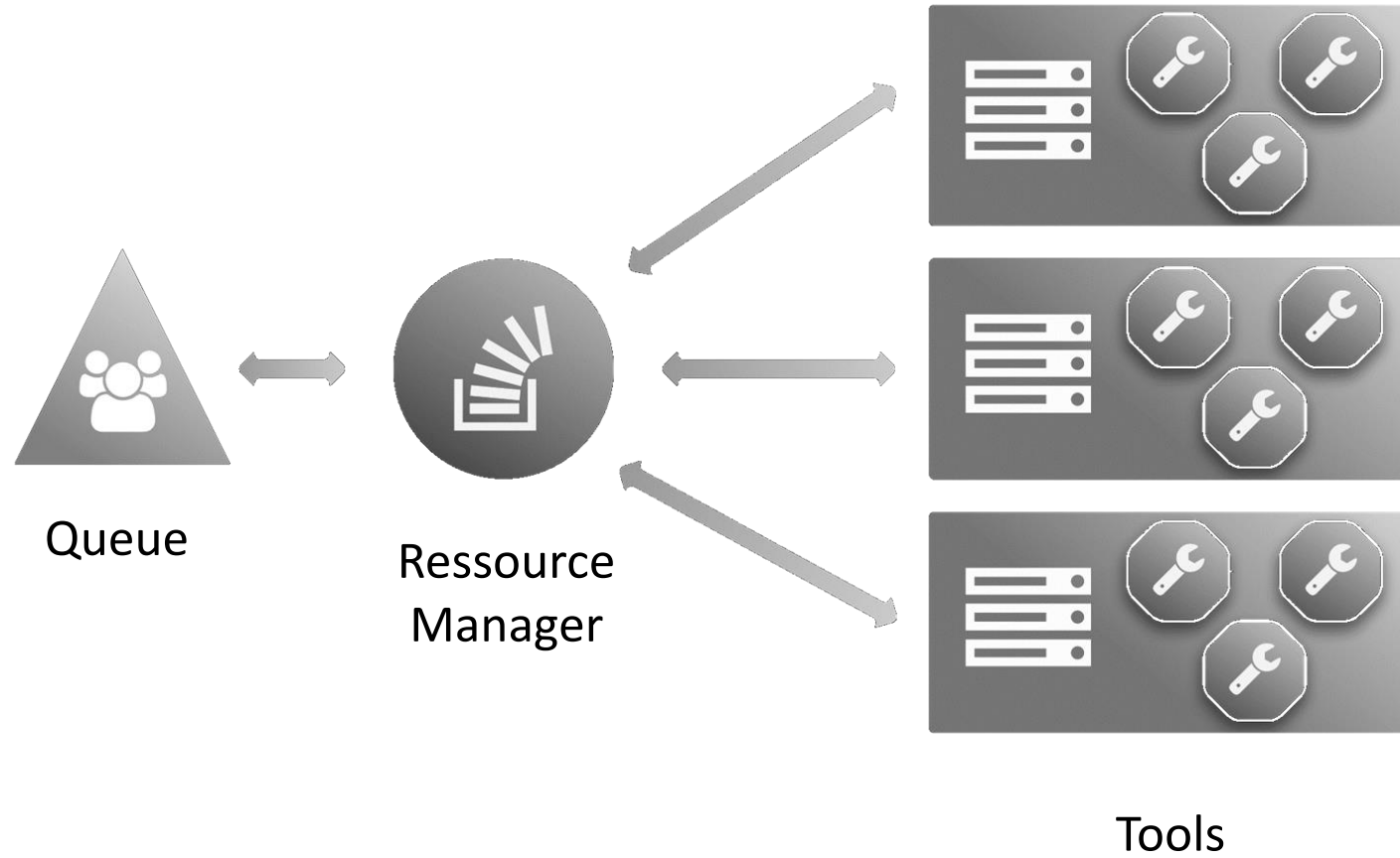
Hashcat starten

```
# hashcat -l  
hashcat (v5.1.0) starting...  
  
OpenCL Info:  
  
Platform ID #1  
Vendor   : NVIDIA Corporation  
Name     : NVIDIA CUDA  
Version  : OpenCL 1.2 CUDA 10.1.120  
  
Device ID #1  
Type     : GPU  
...
```

Open Source Password Cracking Tools with GUI



Cracklord - Aufbau



Cracklord - Installation

Herunterladen <https://packagecloud.io/emperorcow/cracklord>

Installieren

```
dpkg -i Downloads/cracklord-queued_1.0-beta-98-ge2bd792_amd64.deb  
dpkg -i Downloads/cracklord-resourced_1.0-beta-98-ge2bd792_amd64.deb
```

Anpassen

```
apt-get install mc
```

Home anlegen

```
mkdir /home/cracklord  
chown -r cracklord:cracklord
```



Korrekte Angabe des
Hashcat-Binary-Files



Schreibrechte in der
Working Directory



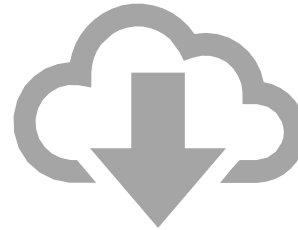
Funktionierendes
Wörterbuch (Pot-Files)



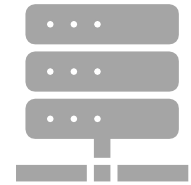
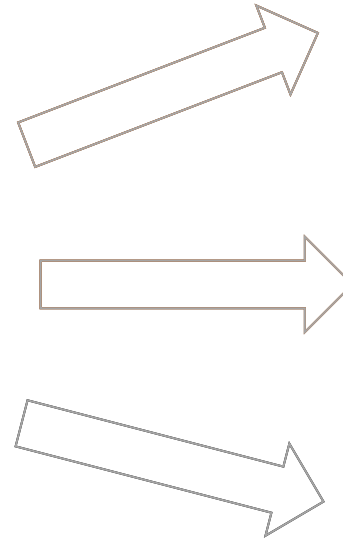
Definieren einer leeren
Rule

Cracklord – Installationstücken

WebHashcat - Aufbau



WebHashcat-Server



Services

- MySQL-Server
- Redis-Server
- HashcatNode-Server

WebHashcat - Installation

Installationsanleitung befolgen <https://github.com/hegusung/WebHashcat>



Zertifikate (Alias)



Fehlende Funktionalität (CRUD)

WebHashcat - Installationstücken



Demo

Cracklord benutzen

Cracklord-queued starten

```
/usr/bin/cracklord-queued --conf=/etc/cracklord/queued.conf
```

Cracklord-resourced starten

```
./start_cracklord-resourced.sh
```

WebHashcat benutzen

Services starten

```
systemctl restart mysql  
systemctl restart hashcatnode  
systemctl restart redis-server
```

WebHashcat-Server starten

```
/root/WebHashcat-master/WebHashcat/manage.py runserver
```

Ausblick

Der Vergleich der verfügbaren
Tools auf dem kostenfreien
Markt längst nicht
abgeschlossen.

Weitere Tests sind notwendig.

