Cracking passwords with John the Ripper

Òscar Pérez Castillo

March 19, 2023

Contents

Cracking passwords with John the Ripper **1**

Challenge I 1

Challenge II 2

Cracking passwords with John the Ripper

Challenge I

In order to generate the corresponding list of possible passwords, the following rule was created:

```
[List.Rules:C1]
: [cu] Az"[\-_]" Az"[0-9][0-9][0-9][0-9][0-9][0-9]"
```

Then, with:

- Wordlist

```
$ cat wordlist.txt
admin
user
ronald
```

- Password file with `${user}:${password}`

Command to recover the passwords, specifying the hashes as raw md5:

```
$ john --wordlist=wordlist.txt --rules=C1 --format=Raw-MD5 passwdFile
Created directory: /home/vagrant/.john
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3]
Press 'q' or Ctrl-C to abort, almost any other key for status
Ronald_666669    (ronald)
ADMIN-746981     (admin)
USER_123456      (user)
3g 0:00:00:05 DONE (2023-03-11 06:44) 0.5328g/s 1664Kp/s 1664Kc/s 4016KC/s ADMIN
Use the "--show --format=Raw-MD5" options to display all of the cracked password
Session completed.
```

Challenge II

Wordlist:

```
puton
Vladomor
Vladomorputon
```

And the following rules set:

```
[List.Rules:C2]
: [lcCu] so0 sO0 A0"[a-z][a-z][a-z][a-z]" Az"[!?.]"
```

Command to recover the passwords:

```
$ john --wordlist=wordlist_2.txt --rules=C2 --format=Raw-MD5 passwdFile

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
qlutPut0n!       (puton)
1g 0:00:00:05 DONE (2023-03-19 07:27) 0.1785g/s 1199Kp/s 1199Kc/s 1199KC/s qlugP
Use the "--show --format=Raw-MD5" options to display all of the cracked password
Session completed.
```