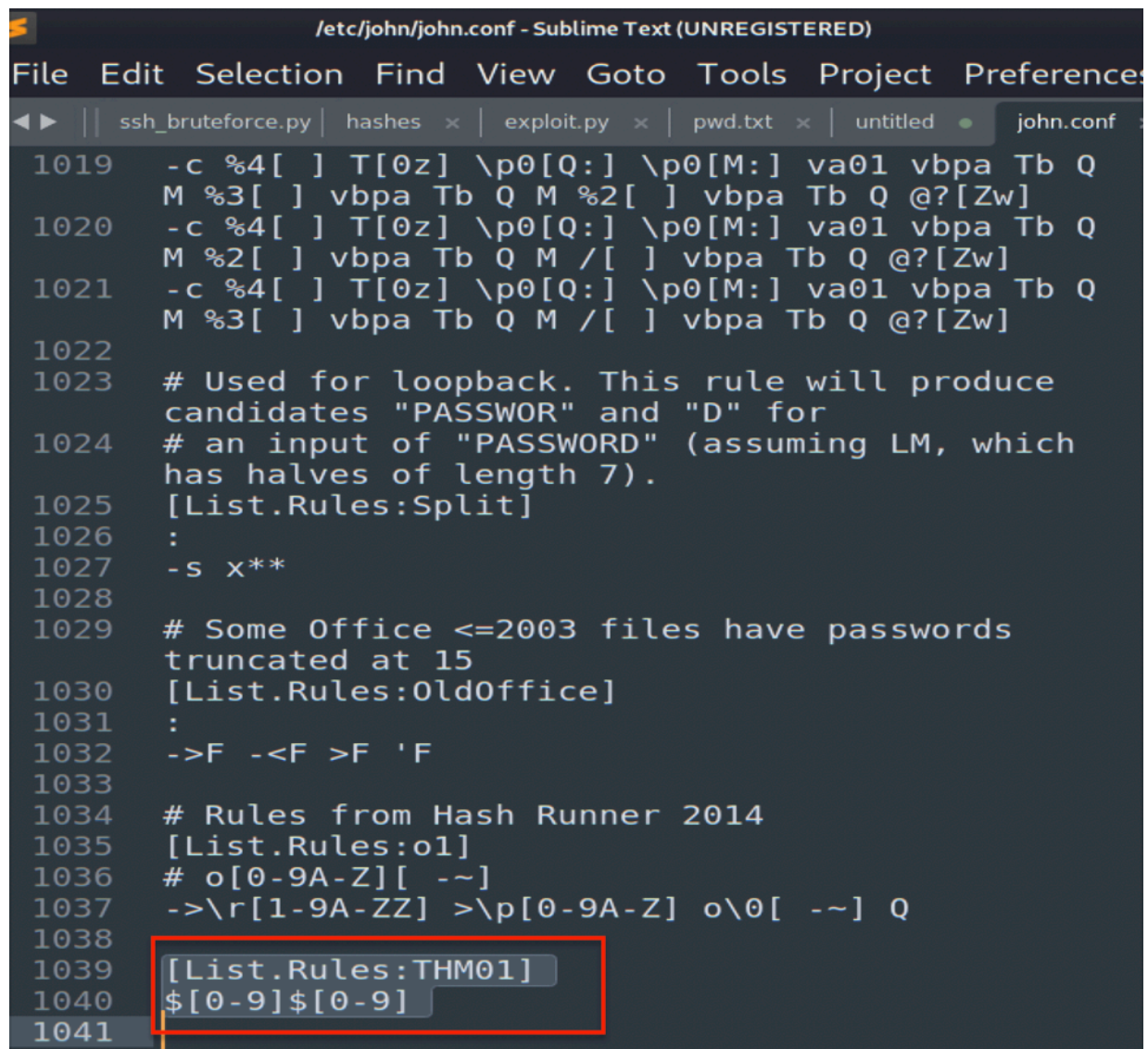


JOHN THE RIPPER

making rules (mangling):

you can add rules to the /etc/john/john.conf file, using Sublime. Here we added a new rule called THM01:



```
/etc/john/john.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences
ssh_bruteforce.py | hashes x | exploit.py x | pwd.txt x | untitled | john.conf
1019 -c %4[ ] T[0z] \p0[Q:] \p0[M:] va01 vbpa Tb Q
      M %3[ ] vbpa Tb Q M %2[ ] vbpa Tb Q @?[Zw]
1020 -c %4[ ] T[0z] \p0[Q:] \p0[M:] va01 vbpa Tb Q
      M %2[ ] vbpa Tb Q M /[ ] vbpa Tb Q @?[Zw]
1021 -c %4[ ] T[0z] \p0[Q:] \p0[M:] va01 vbpa Tb Q
      M %3[ ] vbpa Tb Q M /[ ] vbpa Tb Q @?[Zw]
1022
1023 # Used for loopback. This rule will produce
1024 # candidates "PASSWORD" and "D" for
1025 # an input of "PASSWORD" (assuming LM, which
1026 # has halves of length 7).
1027 [List.Rules:Split]
1028 :
1029 -s x**
1030
1031 # Some Office <=2003 files have passwords
1032 # truncated at 15
1033 [List.Rules:OldOffice]
1034 :
1035 ->F -<F >F 'F
1036
1037 # Rules from Hash Runner 2014
1038 [List.Rules:ol]
1039 # o[0-9A-Z][ -~]
1040 ->\r[1-9A-ZZ] >\p[0-9A-Z] o\0[ -~] Q
1041
1042 [List.Rules:THM01]
1043 $[0-9]$[0-9]
```

run john with the newly created rule:THM01 against the file (hash.txt) that contains the hash, with your chosen wordlist(ex. 10K-most-common.txt)

```
(max@kali)-[~/Downloads/wordlistctl]
$ john hash.txt --format=raw-sha1 --wordlist=/usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt --rules=THM01
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 ASIMD 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
moonligh56 (?)
1g 0:00:00:00 DONE (2021-07-21 15:41) 25.00g/s 14133Kp/s 14133Kc/s 14133KC/s hot
rats56..modena56
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

—show cmd using the file containing the hash you just cracked will display the cracked passwd:

```
(max@kali)-[~/Downloads/wordlistctl]
$ john hash.txt --show
?:moonligh56

1 password hash cracked, 0 left
```

googled top malenames english list on Github:

```
https://github.com/x-o-r-r-o/Cracking/blob/master/top_1000_usa_malenames_english.txt
```

created new rule in /etc/john/john.conf

```
/etc/john/john.conf - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences
sha256cr | ssh_bruteforce.py x | hashes x | exploit.py x | pwd.txt x | john.conf x
1038
1039 [List.Rules:THM_Advise1]
1040 c$1$2$3$4$[$%&*-_+=#@~!]
1041
1042 [List.Rules:o2]
1043 # o[0-9A-E][ -~] Q M o[0-9A-E][ -~] Q
1044 ->[1-9A-F] ->[1-9A-F] >\p1[0-9A-E] >\p2[
0-9A-E] o\3[ -~] Q M o\4[ -~] Q
```

John cmd to run our hash.txt file against our wordlist and mangle with our new rule

```
(max@kali)-[~/Downloads/wordlistctl]
$ john hash.txt --format=raw-md5 --wordlist=/usr/share/seclists/Usernames/Names/male-names-usa-top1000.txt --rules=THM_Advise1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Zachariah1234* (?)
1g 0:00:00:00 DONE (2021-07-23 12:00) 100.0g/s 409600p/s 409600c/s 409600C/s Valentin1234*..Chris1234+
Use the "--show --format=Raw-MD5" options to display all of the cracked password
```