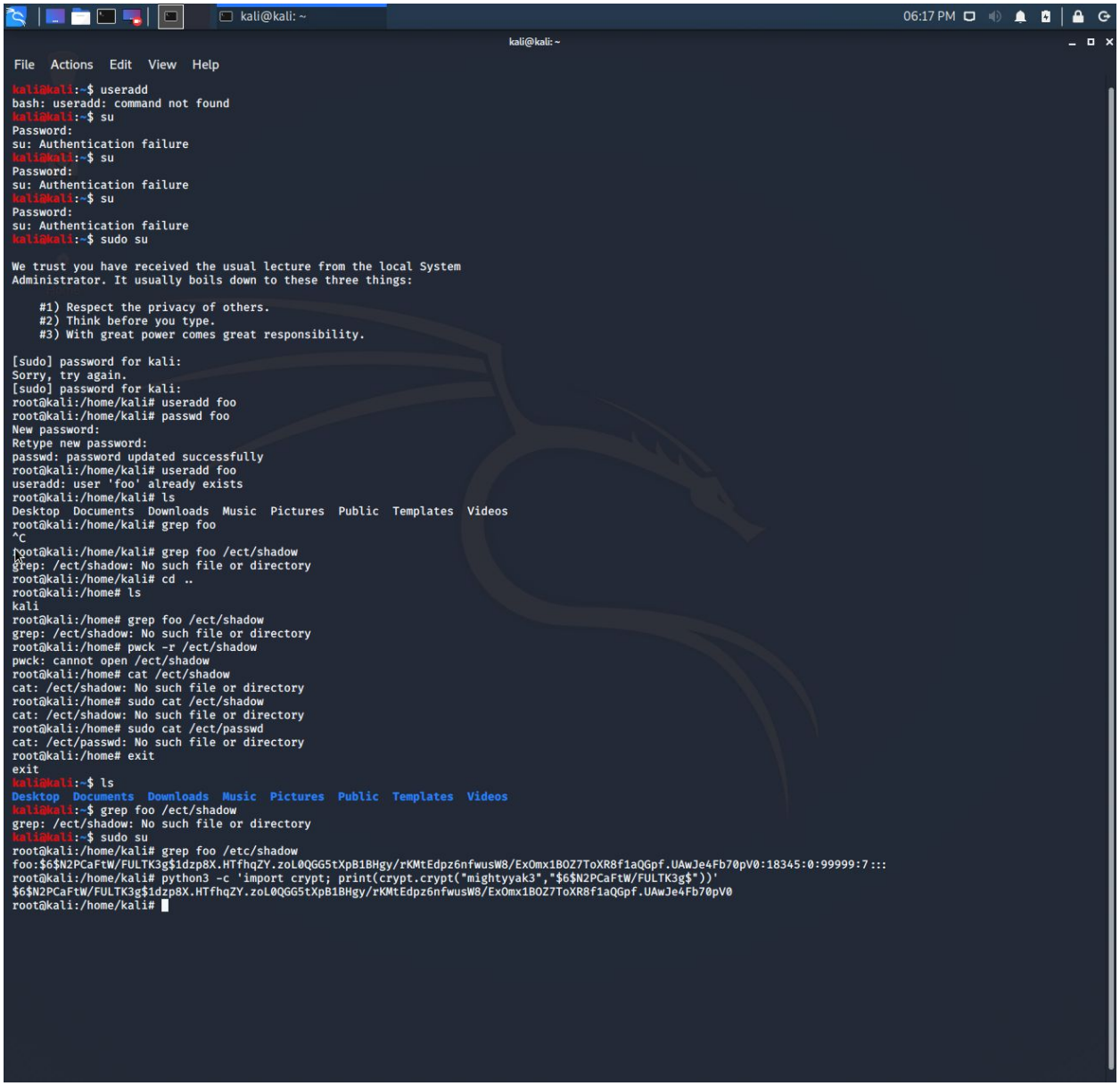
Lab 12

Karsen Diepholz

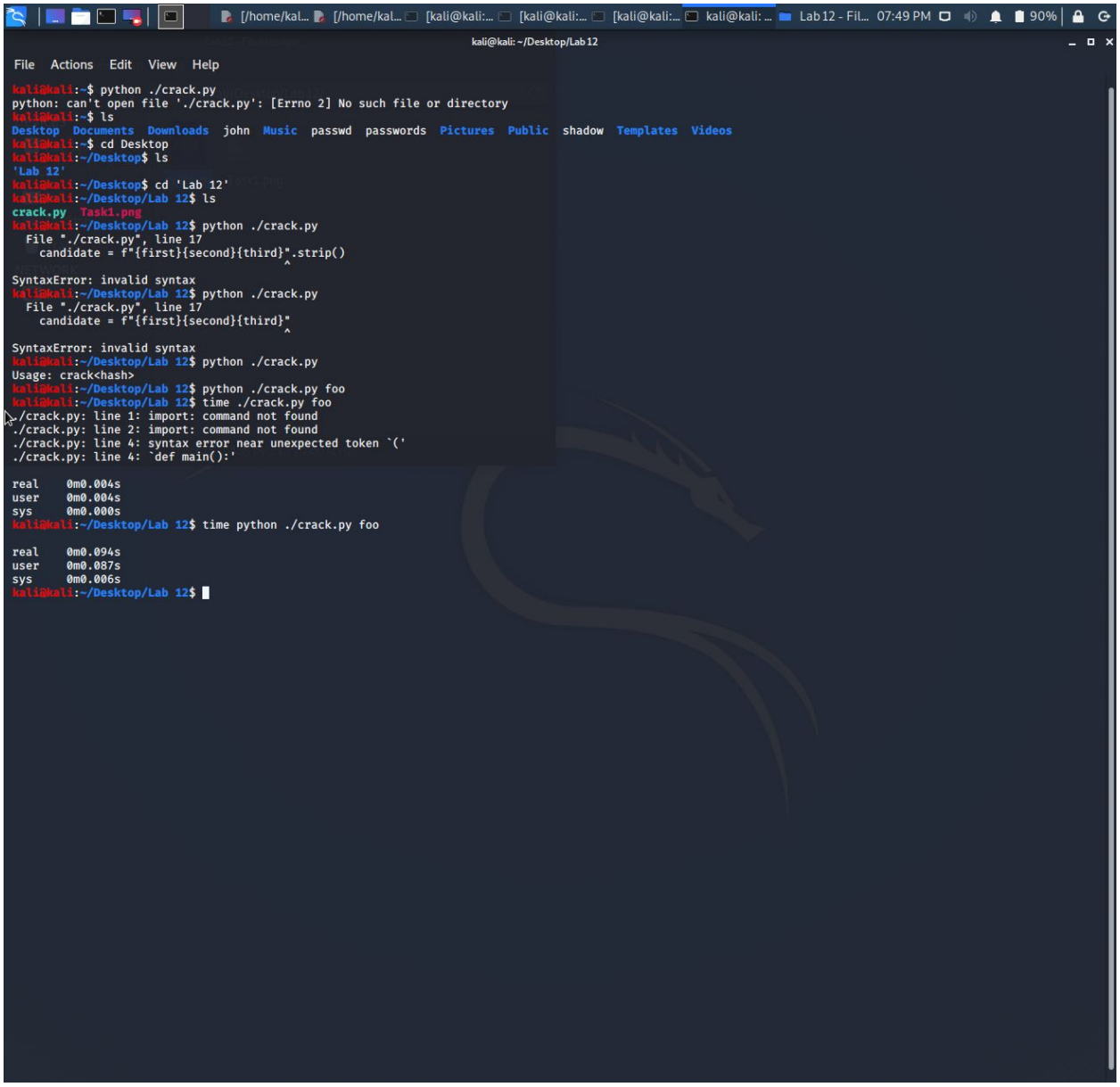
CSP544

Task 1



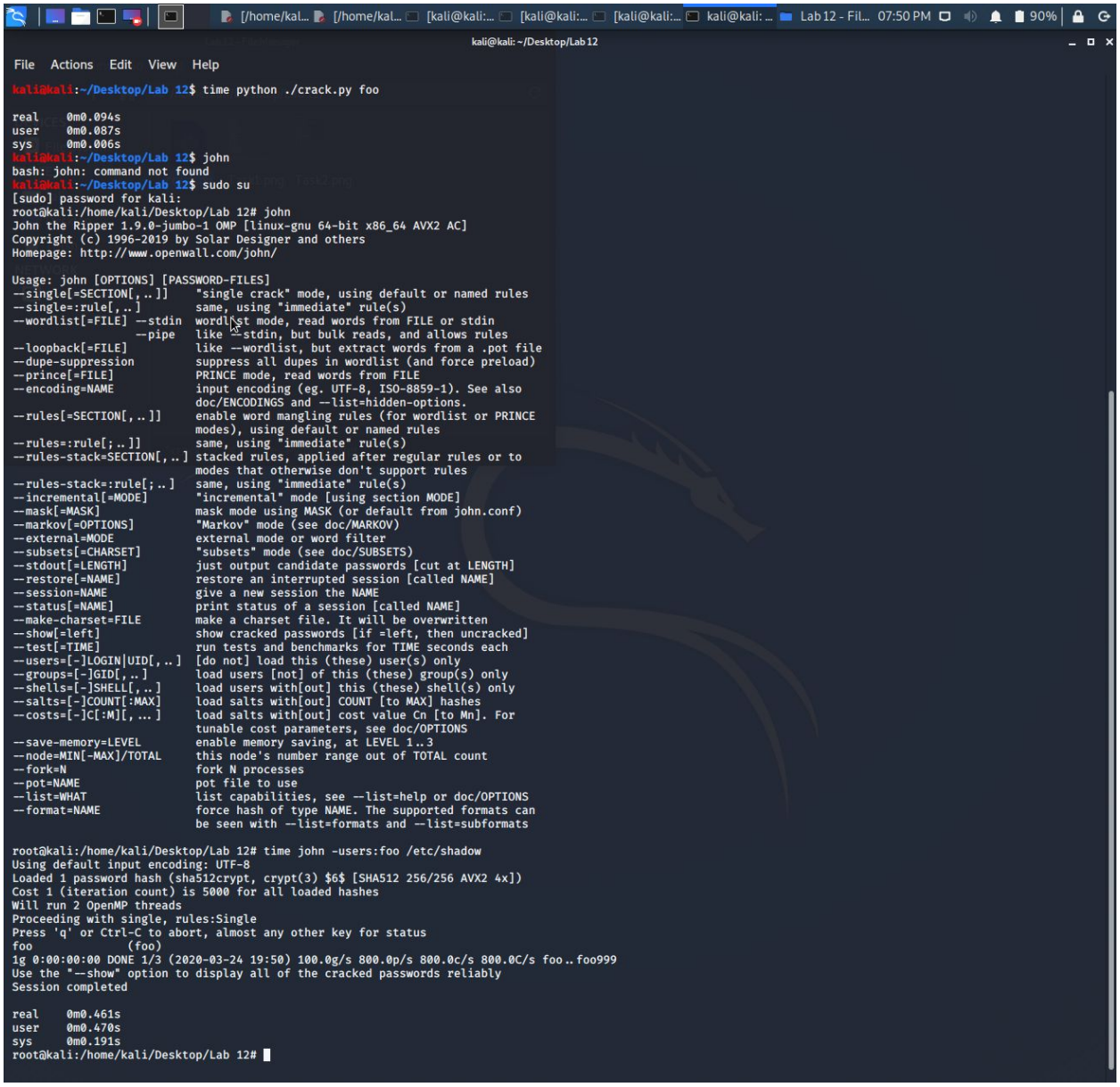
Here we can see the hash that my Password “Foo” puts out, it is also the same if we use the python script (no surprise).

Task 2



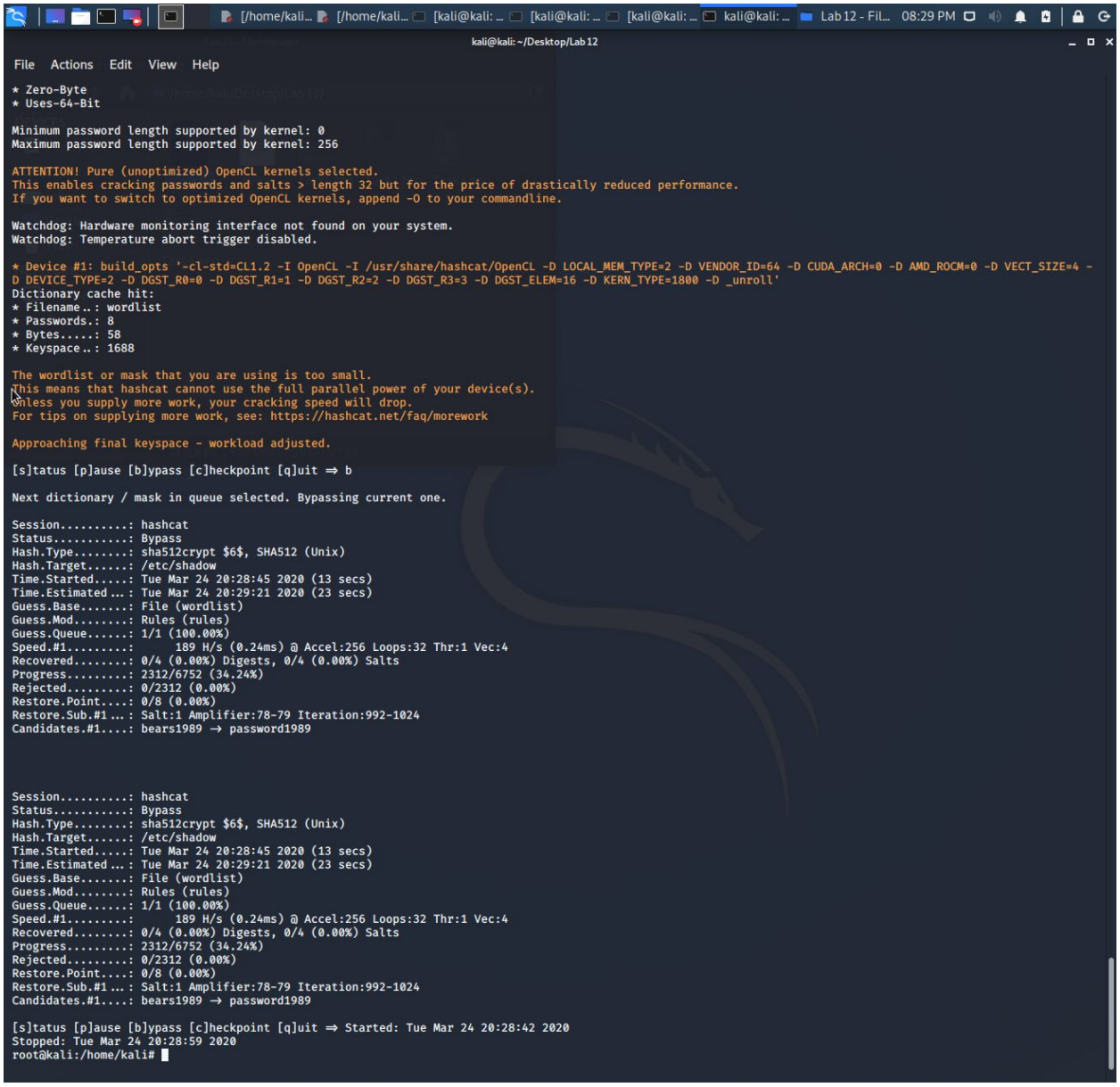
Here we measured how long crack.py (my own code) took to crack the password, we can also see how long it took john to crack the password in the next Task.

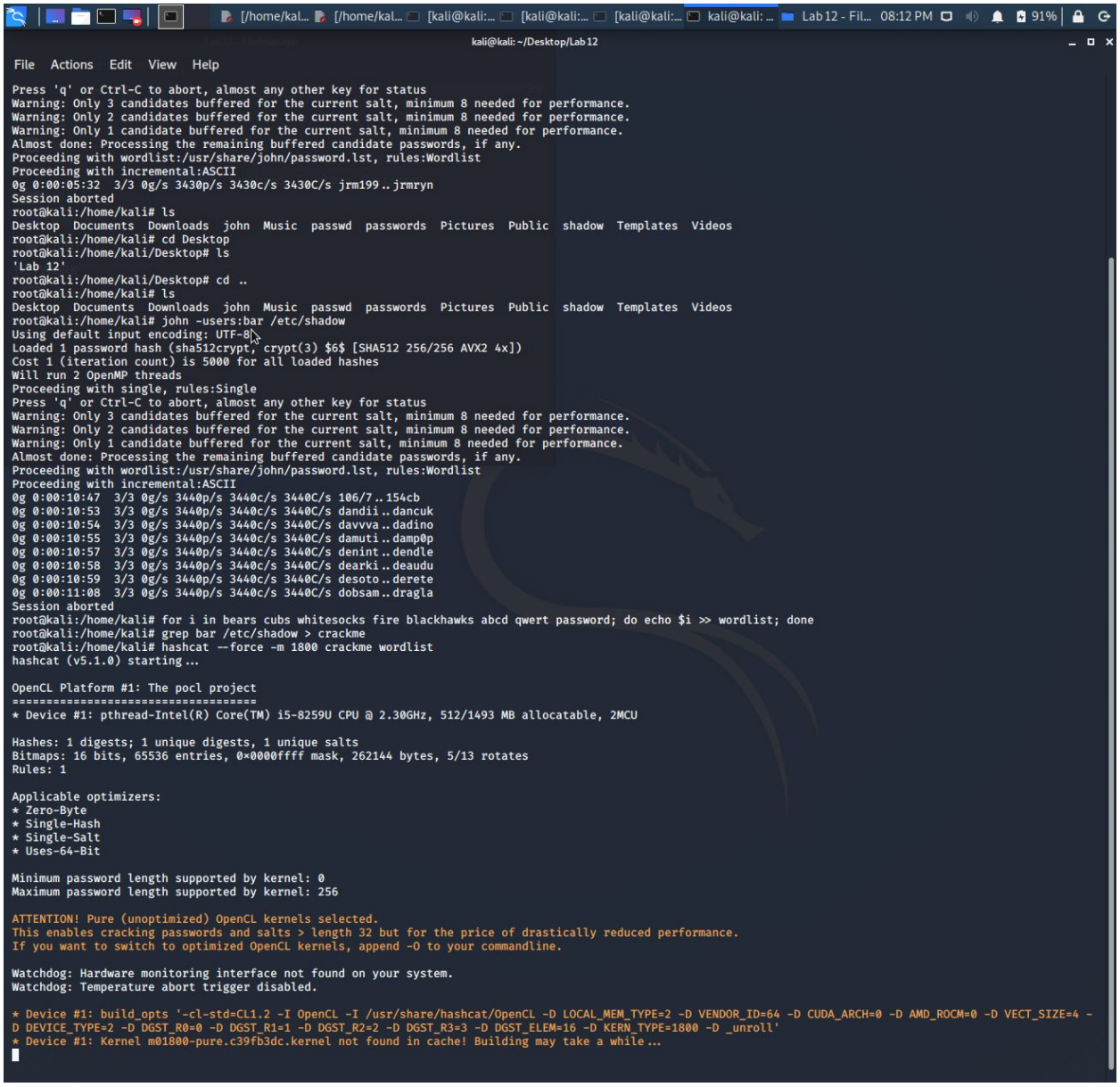
Task 3



Here we can see John runs much faster than my own script.

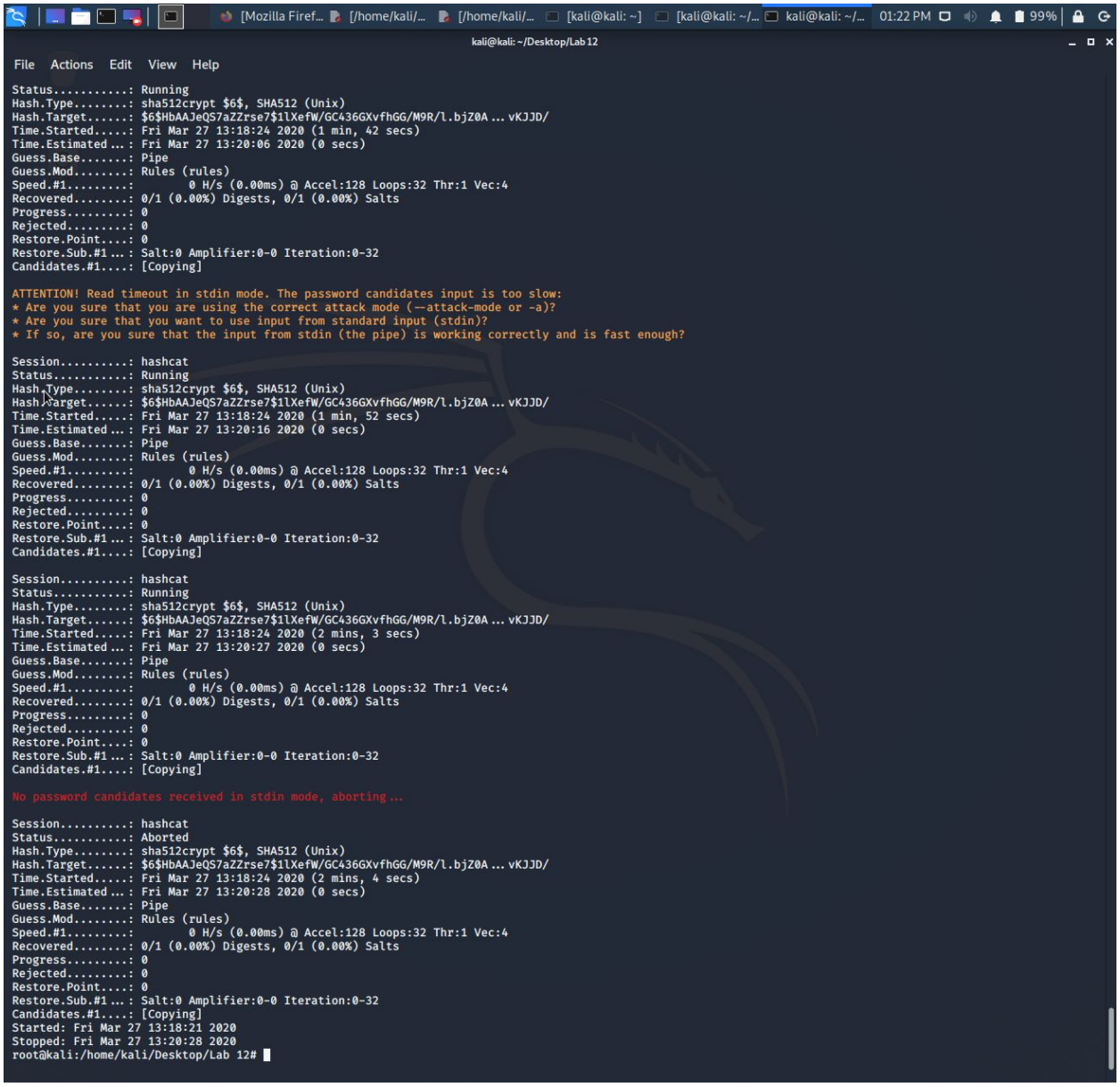
Task 4


[/home/kali... [/home/kali... [kali@kali: ... [kali@kali: ... [kali@kali: ... kali@kali: ... Lab 12 - Fil... 08:29 PM
kali@kali: ~/Desktop/Lab 12
File Actions Edit View Help
* Zero-Byte
* Uses-64-Bit
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=4 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST_ELEM=16 -D KERN_TYPE=1800 -D _unroll'
Dictionary cache hit:
* Filename..: wordlist
* Passwords.: 8
* Bytes.....: 58
* Keyspace..: 1688
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework
Approaching final keyspace - workload adjusted.
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => b
Next dictionary / mask in queue selected. Bypassing current one.
Session..........: hashcat
Status...........: Bypass
Hash.Type........: sha512crypt 6, SHA512 (Unix)
Hash.Target......: /etc/shadow
Time.Started.....: Tue Mar 24 20:28:45 2020 (13 secs)
Time.Estimated...: Tue Mar 24 20:29:21 2020 (23 secs)
Guess.Base.......: File (wordlist)
Guess.Mod........: Rules (rules)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 189 H/s (0.24ms) @ Accel:256 Loops:32 Thr:1 Vec:4
Recovered........: 0/4 (0.00%) Digests, 0/4 (0.00%) Salts
Progress.........: 2312/6752 (34.24%)
Rejected.........: 0/2312 (0.00%)
Restore.Point....: 0/8 (0.00%)
Restore.Sub.#1...: Salt:1 Amplifier:78-79 Iteration:992-1024
Candidates.#1....: bears1989 -> password1989
Session..........: hashcat
Status...........: Bypass
Hash.Type........: sha512crypt 6, SHA512 (Unix)
Hash.Target......: /etc/shadow
Time.Started.....: Tue Mar 24 20:28:45 2020 (13 secs)
Time.Estimated...: Tue Mar 24 20:29:21 2020 (23 secs)
Guess.Base.......: File (wordlist)
Guess.Mod........: Rules (rules)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 189 H/s (0.24ms) @ Accel:256 Loops:32 Thr:1 Vec:4
Recovered........: 0/4 (0.00%) Digests, 0/4 (0.00%) Salts
Progress.........: 2312/6752 (34.24%)
Rejected.........: 0/2312 (0.00%)
Restore.Point....: 0/8 (0.00%)
Restore.Sub.#1...: Salt:1 Amplifier:78-79 Iteration:992-1024
Candidates.#1....: bears1989 -> password1989
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => Started: Tue Mar 24 20:28:42 2020
Stopped: Tue Mar 24 20:28:59 2020
root@kali:/home/kali#



Here we edited rules in order to crack user “Bar”s password faster. In order to do this, we added birthdays and substitutions to our rules, and ultimately got to crack the password..

Task 5


[Mozilla Firef... [/home/kali/... [/home/kali/... [kali@kali: ~] [kali@kali: ~/... kali@kali: ~/... 01:22 PM 99%
kali@kali: ~/Desktop/Lab 12
File Actions Edit View Help
Status.....: Running
Hash.Type.....: sha512crypt 6, SHA512 (Unix)
Hash.Target.....: 6HbAAJeQS7aZZrse7$1lXefW/GC436GXvfhGG/M9R/l.bjZ0A ... vKJJD/
Time.Started.....: Fri Mar 27 13:18:24 2020 (1 min, 42 secs)
Time.Estimated...: Fri Mar 27 13:20:06 2020 (0 secs)
Guess.Base.....: Pipe
Guess.Mod.....: Rules (rules)
Speed.#1.....: 0 H/s (0.00ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0
Rejected.....: 0
Restore.Point....: 0
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-32
Candidates.#1....: [Copying]
ATTENTION! Read timeout in stdin mode. The password candidates input is too slow:
* Are you sure that you are using the correct attack mode (--attack-mode or -a)?
* Are you sure that you want to use input from standard input (stdin)?
* If so, are you sure that the input from stdin (the pipe) is working correctly and is fast enough?
Session.....: hashcat
Status.....: Running
Hash.Type.....: sha512crypt 6, SHA512 (Unix)
Hash.Target.....: 6HbAAJeQS7aZZrse7$1lXefW/GC436GXvfhGG/M9R/l.bjZ0A ... vKJJD/
Time.Started.....: Fri Mar 27 13:18:24 2020 (1 min, 52 secs)
Time.Estimated...: Fri Mar 27 13:20:16 2020 (0 secs)
Guess.Base.....: Pipe
Guess.Mod.....: Rules (rules)
Speed.#1.....: 0 H/s (0.00ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0
Rejected.....: 0
Restore.Point....: 0
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-32
Candidates.#1....: [Copying]
Session.....: hashcat
Status.....: Running
Hash.Type.....: sha512crypt 6, SHA512 (Unix)
Hash.Target.....: 6HbAAJeQS7aZZrse7$1lXefW/GC436GXvfhGG/M9R/l.bjZ0A ... vKJJD/
Time.Started.....: Fri Mar 27 13:18:24 2020 (2 mins, 3 secs)
Time.Estimated...: Fri Mar 27 13:20:27 2020 (0 secs)
Guess.Base.....: Pipe
Guess.Mod.....: Rules (rules)
Speed.#1.....: 0 H/s (0.00ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0
Rejected.....: 0
Restore.Point....: 0
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-32
Candidates.#1....: [Copying]
No password candidates received in stdin mode, aborting...
Session.....: hashcat
Status.....: Aborted
Hash.Type.....: sha512crypt 6, SHA512 (Unix)
Hash.Target.....: 6HbAAJeQS7aZZrse7$1lXefW/GC436GXvfhGG/M9R/l.bjZ0A ... vKJJD/
Time.Started.....: Fri Mar 27 13:18:24 2020 (2 mins, 4 secs)
Time.Estimated...: Fri Mar 27 13:20:28 2020 (0 secs)
Guess.Base.....: Pipe
Guess.Mod.....: Rules (rules)
Speed.#1.....: 0 H/s (0.00ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 0
Rejected.....: 0
Restore.Point....: 0
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-32
Candidates.#1....: [Copying]
Started: Fri Mar 27 13:18:21 2020
Stopped: Fri Mar 27 13:20:28 2020
root@kali:/home/kali/Desktop/Lab 12#