

## Lab 12

Karsen Diepholz  
CSP544

### Task 1

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ useradd  
bash: useradd: command not found  
kali@kali:~$ su  
Password:  
su: Authentication failure  
kali@kali:~$ su  
Password:  
su: Authentication failure  
kali@kali:~$ su  
Password:  
su: Authentication failure  
kali@kali:~$ sudo su  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
root@kali:/home/kali# useradd foo  
root@kali:/home/kali# passwd foo  
New password:  
Retype new password:  
passwd: password updated successfully  
root@kali:/home/kali# useradd foo  
useradd: user 'foo' already exists  
root@kali:/home/kali# ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
root@kali:/home/kali# grep foo  
^C  
root@kali:/home/kali# grep foo /etc/shadow  
grep: /etc/shadow: No such file or directory  
root@kali:/home/kali# cd ..  
root@kali:/home# ls  
kali  
root@kali:/home# grep foo /etc/shadow  
grep: /etc/shadow: No such file or directory  
root@kali:/home# pwck -r /etc/shadow  
pwck: cannot open /etc/shadow  
root@kali:/home# cat /etc/shadow  
cat: /etc/shadow: No such file or directory  
root@kali:/home# sudo cat /etc/shadow  
cat: /etc/shadow: No such file or directory  
root@kali:/home# sudo cat /etc/passwd  
cat: /etc/passwd: No such file or directory  
root@kali:/home# exit  
exit  
kali@kali:~$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
kali@kali:~$ grep foo /etc/shadow  
grep: /etc/shadow: No such file or directory  
kali@kali:~$ sudo su  
root@kali:/home/kali# grep foo /etc/shadow  
foo:$6$N2PCaFtW/FULTK3g$1dzp8X.HTFhQZY.zoL0QG65tXpB1BHgy/rKMTedp6nfWusW8/ExOmX1B0Z7ToXR8f1aQGpf.UAwJe4Fb70pV0:18345:0:99999:7 :::  
root@kali:/home/kali# python3 -c 'import crypt; print(crypt.crypt("mightyak3", "$6$N2PCaFtW/FULTK3g$"))'  
$6$N2PCaFtW/FULTK3g$1dzp8X.HTFhQZY.zoL0QG65tXpB1BHgy/rKMTedp6nfWusW8/ExOmX1B0Z7ToXR8f1aQGpf.UAwJe4Fb70pV0  
root@kali:/home/kali#
```

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

```
File Actions Edit View Help
kali@kali:~/Desktop/Lab 12
kali@kali:~$ python ./crack.py
python: can't open file './crack.py': [Errno 2] No such file or directory
kali@kali:~$ ls
Desktop Documents Downloads john Music passwd passwords Pictures Public shadow Templates Videos
kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ ls
'Lab 12'
kali@kali:~/Desktop$ cd 'Lab 12'
kali@kali:~/Desktop/Lab 12$ ls
crack.py Task1.png
kali@kali:~/Desktop/Lab 12$ python ./crack.py
File "./crack.py", line 17
    candidate = f"{first}{second}{third}".strip()
                                         ^
SyntaxError: invalid syntax
kali@kali:~/Desktop/Lab 12$ python ./crack.py
File "./crack.py", line 17
    candidate = f"{first}{second}{third}"
                                         ^
SyntaxError: invalid syntax
kali@kali:~/Desktop/Lab 12$ python ./crack.py
Usage: crackhash>
kali@kali:~/Desktop/Lab 12$ python ./crack.py foo
kali@kali:~/Desktop/Lab 12$ time ./crack.py foo
./crack.py: line 1: import: command not found
./crack.py: line 2: import: command not found
./crack.py: line 4: syntax error near unexpected token `('
./crack.py: line 4: `def main():'

real    0m0.004s
user    0m0.004s
sys      0m0.000s
kali@kali:~/Desktop/Lab 12$ time python ./crack.py foo

real    0m0.094s
user    0m0.087s
sys      0m0.006s
kali@kali:~/Desktop/Lab 12$
```

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

```
kali@kali: ~/Desktop/Lab 12
File Actions Edit View Help
kali@kali:~/Desktop/Lab 12$ time python ./crack.py foo
real    0m0.094s
user    0m0.087s
sys     0m0.006s
kali@kali:~/Desktop/Lab 12$ john
bash: john: command not found
kali@kali:~/Desktop/Lab 12$ sudo su
[sudo] password for kali:
root@kali:/home/kali/Desktop/Lab 12# john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,...]]  "single crack" mode, using default or named rules
--single=:rule[,...]      same, using "immediate" rule(s)
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                        --pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but extract words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]          PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODINGS and --list-hidden-options.
--rules[=SECTION[,...]]  enable word mangling rules (for wordlist or PRINCE
                        modes), using default or named rules
--rules=:rule[,...]      same, using "immediate" rule(s)
--rules-stack=SECTION[,...] stacked rules, applied after regular rules or to
                        modes that otherwise don't support rules
--rules-stack=:rule[,...] same, using "immediate" rule(s)
--incremental[=MODE]     "incremental" mode [using section MODE]
--mask[=MASK]            mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]       "Markov" mode (see doc/MARKOV)
--external=MODE          external mode or word filter
--subsets[=CHARSET]      "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]       just output candidate passwords [cut at LENGTH]
--restore[=NAME]         restore an interrupted session [called NAME]
--session=NAME           give a new session the NAME
--status[=NAME]          print status of a session [called NAME]
--make-charset=FILE      make a charset file. It will be overwritten
--show[=left]           show cracked passwords [if =left, then uncracked]
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN[UID[,...]] [do not] load this (these) user(s) only
--groups=[-]GID[,...]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][, ...] load salts with[out] cost value Cn [to Mn]. For
                        tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL  this node's number range out of TOTAL count
--fork=N               fork N processes
--pot=NAME             pot file to use
--list=WHAT            list capabilities, see --list-help or doc/OPTIONS
--format=NAME          force hash of type NAME. The supported formats can
                        be seen with --list-formats and --list-subformats

root@kali:/home/kali/Desktop/Lab 12# time john -users:foo /etc/shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
foo (foo)
1g 0:00:00.00 DONE 1/3 (2020-03-24 19:50) 100.0g/s 800.0p/s 800.0c/s 800.0C/s foo..foo999
Use the "--show" option to display all of the cracked passwords reliably
Session completed

real    0m0.461s
user    0m0.470s
sys     0m0.191s
root@kali:/home/kali/Desktop/Lab 12#
```

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

### Task 4

```
kali@kali: ~/Desktop/Lab12
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 /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#
```



```
kali@kali: ~/Desktop/Lab12
File Actions Edit View Help

Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:05:32 3/3 0g/s 3430p/s 3430c/s 3430C/s jrm199..jrmryn
Session aborted
root@kali:/home/kali# ls
Desktop Documents Downloads john Music passwd passwords Pictures Public shadow Templates Videos
root@kali:/home/kali# cd Desktop
root@kali:/home/kali/Desktop# ls
'Lab 12'
root@kali:/home/kali/Desktop# cd ..
root@kali:/home/kali# ls
Desktop Documents Downloads john Music passwd passwords Pictures Public shadow Templates Videos
root@kali:/home/kali# john -users:bar /etc/shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:10:47 3/3 0g/s 3440p/s 3440c/s 3440C/s 106/7..154cb
0g 0:00:10:53 3/3 0g/s 3440p/s 3440c/s 3440C/s dandii..dancuk
0g 0:00:10:54 3/3 0g/s 3440p/s 3440c/s 3440C/s davvva..dadino
0g 0:00:10:55 3/3 0g/s 3440p/s 3440c/s damuti..dampop
0g 0:00:10:57 3/3 0g/s 3440p/s 3440c/s denint..dendle
0g 0:00:10:58 3/3 0g/s 3440p/s 3440c/s dearki..deaudu
0g 0:00:10:59 3/3 0g/s 3440p/s 3440c/s desoto..derete
0g 0:00:11:08 3/3 0g/s 3440p/s 3440c/s dobsam..dragla
Session aborted
root@kali:/home/kali# for i in bears cubs whitesocks fire blackhawks abcd qwert password; do echo $i >> wordlist; done
root@kali:/home/kali# grep bar /etc/shadow > crackme
root@kali:/home/kali# hashcat --force -m 1800 crackme wordlist
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Core(TM) i5-8259U CPU @ 2.30GHz, 512/1493 MB allocatable, 2MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* 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 /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'
* Device #1: Kernel m01800-pure.c39fb3dc.kernel not found in cache! Building may take a while...
```

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/Lab12
File Actions Edit View Help
Status.....: Running
Hash.Type.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: $6$HbAAJeQS7aZrse7$1lXefW/GC436GXvfHG/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.....: $6$HbAAJeQS7aZrse7$1lXefW/GC436GXvfHG/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.....: $6$HbAAJeQS7aZrse7$1lXefW/GC436GXvfHG/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.....: $6$HbAAJeQS7aZrse7$1lXefW/GC436GXvfHG/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/Lab12#
```