

```
Time.Estimated... : Sat Feb 18 00:24:37 2023 (0 secs)
Guess.Base..... : File (/usr/share/wordlists/rockyou.txt)
Guess.Queue..... : 1/1 (100.00%)
Speed.#1..... : 1437.9 kH/s (0.56ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered..... : 5/7 (71.43%) Digests
Progress..... : 14344385/14344385 (100.00%)
Rejected..... : 0/14344385 (0.00%)
Restore.Point.... : 14344385/14344385 (100.00%)
Restore.Sub.#1... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1.... : $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
```

Remove File Containing Hash Values (hashes.txt) & Edit Script File (generate.sh)

Started: Sat Feb 18 00:23:35 2023

Stopped: Sat Feb 18 00:24:38 2023

sec@kali:~\$ ls -l

```
total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 479 Feb 18 00:02 generate.sh
-rw-r--r-- 1 sec sec 231 Feb 18 00:05 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 207 Feb 18 00:24 passwords.txt
```

Remove file containing hash values

sec@kali:~\$

sec@kali:~\$ sudo nano passwords.txt

sec@kali:~\$ sudo nano passwords.txt

sec@kali:~\$

sec@kali:~\$ sudo rm hashes.txt

[sudo] password for sec:

sec@kali:~\$

sec@kali:~\$ ls -l

```
total 48
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 479 Feb 18 00:02 generate.sh
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 207 Feb 18 00:24 passwords.txt
```

Edit script file with editor (nano)

sec@kali:~\$

sec@kali:~\$

sec@kali:~\$ sudo nano generate.sh

```
GNU nano 4.9.3 generate.sh
echo -n "Password" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "HELLO" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "MYSECRET" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "Test1234" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "P455w0rd" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "GuessMe" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "S3CuReP455Word" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "pass1234" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "1234pass" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "guessme" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "GUESSME" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
echo -n "H4d+" | openssl md5 | cut -c 10-41 | tee -a hashes.txt
```

Generate 5 More Hash Values from Their Respective Passwords

```
sec@kali:~$ sudo rm hashes.txt
```

```
[sudo] password for sec:
```

```
sec@kali:~$
```

```
sec@kali:~$ ls -l
```

```
total 48
```

```
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 479 Feb 18 00:02 generate.sh
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 207 Feb 18 00:24 passwords.txt
```

```
sec@kali:~$
```

```
sec@kali:~$
```

```
sec@kali:~$ sudo nano generate.sh
```

```
sec@kali:~$ sudo nano generate.sh
```

```
sec@kali:~$
```

```
sec@kali:~$ ./generate.sh
```

```
dc647eb65e6711e155375218212b3964
eb61eead90e3b899c6bcbe27ac581660
958152288f2d2303ae045cffc43a02cd
2c9341ca4cf3d87b9e4eb905d6a3ec45
75b71aa6842e450f12aca00fdf54c51d
031cbcccd3ba6bd4d1556330995b8d08
b5af0b804ff7238bce48adef1e0c213f
b4af804009cb036a4ccdc33431ef9ac9
b3d34352fc26117979deabdf1b9b6354
81a58e89df1f34c5487568e17327a219
56b2ab035abb810274ebd8699bd26102
3337abe8677a3115f8a59617821bac8b
```

```
sec@kali:~$
```

```
sec@kali:~$ ls -l
```

```
total 52
```

```
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 207 Feb 18 00:24 passwords.txt
```

```
sec@kali:~$
```

Run Script File (generate.sh) to Generate File of Hashes (hashes.txt)

Run script file

12 hash values (previously 7) generated and output to screen

New file of hash values generated

Remove File Containing Recovered Passwords (passwords.txt)

```
sec@kali:~$  
sec@kali:~$  
sec@kali:~$ sudo nano generate.sh  
sec@kali:~$ sudo nano generate.sh  
sec@kali:~$  
sec@kali:~$ ./generate.sh  
dc647eb65e6711e155375218212b3964  
eb61eead90e3b899c6bcbe27ac581660  
958152288f2d2303ae045cffc43a02cd  
2c9341ca4cf3d87b9e4eb905d6a3ec45  
75b71aa6842e450f12aca00fdf54c51d  
031cbcccd3ba6bd4d1556330995b8d08  
b5af0b804ff7238bce48adef1e0c213f  
b4af804009cb036a4ccdc33431ef9ac9  
b3d34352fc26117979deabdf1b9b6354  
81a58e89df1f34c5487568e17327a219  
56b2ab035abb810274ebd8699bd26102  
3337abe8677a3115f8a59617821bac8b  
sec@kali:~$  
sec@kali:~$ ls -l  
total 52  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
-rw-r--r-- 1 root root 207 Feb 18 00:24 passwords.txt  
sec@kali:~$  
sec@kali:~$ sudo rm passwords.txt  
sec@kali:~$  
sec@kali:~$ ls -l  
total 48  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
sec@kali:~$
```

```
total 48
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
```

```
sec@kali:~$
```

```
sec@kali:~$
```

```
sec@kali:~$
```

```
sec@kali:~$
```

```
sec@kali:~$ sudo hashcat -m 0 -a 1 hashes.txt -o passwords.txt /usr/share/wordlists/rockyou.txt ./lab4/dicts/small.txt
```

```
[sudo] password for sec:
```

```
hashcat (v6.0.0) starting ...
```

```
OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1429/1493 MB (512 MB allocatable), 2MCU
```

```
Minimum password length supported by kernel: 0
```

```
Maximum password length supported by kernel: 256
```

```
Dictionary cache hit:
```

```
* Filename..: /usr/share/wordlists/rockyou.txt
```

```
* Passwords.: 14344385
```

```
* Bytes.....: 139921507
```

```
* Keyspace..: 14344385
```

```
Dictionary cache built:
```

```
* Filename..: ./lab4/dicts/small.txt
```

```
* Passwords.: 129799
```

```
* Bytes.....: 1208404
```

```
* Keyspace..: 129799
```

```
* Runtime...: 0 secs
```

```
Hashes: 12 digests; 12 unique digests, 1 unique salts
```

```
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
```

```
Applicable optimizers:
```

```
* Zero-Byte
```

```
* Early-Skip
```

```
* Not-Salted
```

```
* Not-Iterated
```

```
* Single-Salt
```

```
* Raw-Hash
```

Recover Passwords from Hashes Using Hashcat Under Attack Mode 1 Combinator Attack

Dictionary 1

Dictionary 2

Can Dictionary 1 = Dictionary 2 ?

The number of passwords contained in the dictionary (rockyou.txt)

The number of passwords contained in the dictionary (small.txt)


```

Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started.....: Sat Feb 18 04:54:45 2023 (27 mins, 45 secs)
Time.Estimated...: Mon Feb 20 01:26:31 2023 (1 day, 20 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 11614.3 kH/s (10.95ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered.....: 8/12 (66.67%) Digests
Progress.....: 19372634368/1861886828615 (1.04%)
Rejected.....: 0/19372634368 (0.00%)
Restore.Point....: 149248/14344385 (1.04%)
Restore.Sub.#1...: Salt:0 Amplifier:3072-4096 Iteration:0-1024
Candidates.#1....: hartini091185 → gramma11071ultrix

```

Estimated time to complete the process

Combine two dictionaries into all the combinations of appended passwords

Recovered 8 out of 12 passwords

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit ⇒ q

It took too long to complete the process. Hence, we quit the running process before completion

Note:

If you quit the running process too early, you may not get the "password.txt" file. Hence, you may prefer to wait until the running process is completed, and the "password.txt" is generated. This may take about 15 to 30 minutes. Please refer to the next slide for the details.

```

Session.....: hashcat
Status.....: Quit
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started.....: Sat Feb 18 04:54:45 2023 (33 mins, 19 secs)
Time.Estimated...: Mon Feb 20 01:03:25 2023 (1 day, 19 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 11717.3 kH/s (10.70ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered.....: 8/12 (66.67%) Digests
Progress.....: 23193523712/1861886828615 (1.25%)
Rejected.....: 0/23193523712 (0.00%)
Restore.Point....: 178688/14344385 (1.25%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidates.#1....: upyours20 → trillville021476590

```

Started: Sat Feb 18 04:54:44 2023

Stopped: Sat Feb 18 05:28:06 2023

sec@kali:~\$

sec@kali:~\$ ls -l

```

total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 83 Feb 18 04:55 passwords.txt

```

File containing recovered passwords was generated

sec@kali:~\$

Wait for Running Because It May
Take A Very Long Time
Quit the Process Before Completion

File Actions Edit View Help

Hashes: 12 digests; 12 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:

- * Zero-Byte
- * Early-Skip
- * Not-Salted
- * Not-Iterated
- * Single-Salt
- * Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 7 hashes found in potfile.

Host memory required for this attack: 64 MB

Dictionary cache hit:

- * Filename..: /usr/share/wordlists/rockyou.txt
- * Passwords.: 14344385
- * Bytes.....: 139921507
- * Keyspace...: 1861886828615

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session.....: hashcat
Status.....: Running
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started....: Wed Feb 28 03:08:41 2024 (9 secs)
Time.Estimated...: Thu Feb 29 07:15:36 2024 (1 day, 4 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 18395.3 kH/s (7.04ms) @ Accel:128 Loops:512 Thr:1 Vec:8
Recovered.....: 7/12 (58.33%) Digests
Progress.....: 167322368/1861886828615 (0.01%)
Rejected.....: 0/167322368 (0.00%)
Restore.Point....: 1280/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:4608-5120 Iteration:0-512
Candidates.#1....: cuties113661 -> mexico1120730

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session.....: hashcat
Status.....: Running
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started....: Wed Feb 28 03:08:41 2024 (1 min, 3 secs)
Time.Estimated...: Thu Feb 29 09:58:58 2024 (1 day, 6 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 16771.0 kH/s (6.93ms) @ Accel:128 Loops:512 Thr:1 Vec:8
Recovered.....: 8/12 (66.67%) Digests
Progress.....: 1071177728/1861886828615 (0.06%)
Rejected.....: 0/1071177728 (0.00%)
Restore.Point....: 8192/14344385 (0.06%)
Restore.Sub.#1...: Salt:0 Amplifier:30720-31232 Iteration:0-512
Candidates.#1....: total90A1308951 -> annalynAvenger

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Use "s" to check the status

Check the time

Open a new Terminal Emulator and type "**ls -l**" to check if the "passwords.txt" is generated

File Actions Edit View Help

```
sec@kali:~$ ls -l
total 48
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 28 03:06 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 28 03:07 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Feb 26 22:06 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
sec@kali:~$ ls -l
total 48
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 28 03:06 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 28 03:07 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Feb 26 22:06 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
sec@kali:~$
```

```
Time.Started.....: Sat Feb 18 04:54:45 2023 (27 mins, 45 secs)
Time.Estimated...: Mon Feb 20 01:26:31 2023 (1 day, 20 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 11614.3 kH/s (10.95ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered.....: 8/12 (66.67%) Digests
Progress.....: 19372634368/1861886828615 (1.04%)
Rejected.....: 0/19372634368 (0.00%)
Restore.Point....: 149248/14344385 (1.04%)
Restore.Sub.#1...: Salt:0 Amplifier:3072-4096 Iteration:0-1024
Candidates.#1....: hartini091185 → grammal1071ultrix
```

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit ⇒ q

```
Session.....: hashcat
Status.....: Quit
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started.....: Sat Feb 18 04:54:45 2023 (33 mins, 19 secs)
Time.Estimated...: Mon Feb 20 01:03:25 2023 (1 day, 19 hours)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt), Left Side
Guess.Mod.....: File (./lab4/dicts/small.txt), Right Side
Speed.#1.....: 11717.3 kH/s (10.70ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered.....: 8/12 (66.67%) Digests
Progress.....: 23193523712/1861886828615 (1.25%)
Rejected.....: 0/23193523712 (0.00%)
Restore.Point....: 178688/14344385 (1.25%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidates.#1....: upyours20 → trillville021476590
```

Started: Sat Feb 18 04:54:44 2023

Stopped: Sat Feb 18 05:28:06 2023

sec@kali:~\$

sec@kali:~\$ ls -l

```
total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 83 Feb 18 04:55 passwords.txt
```

sec@kali:~\$

sec@kali:~\$ sudo nano passwords.txt

[sudo] password for sec:

Open File Containing Recovered Passwords (passwords.txt)


```
GNU nano 4.9.3 passwords.txt
b4af804009cb036a4ccdc33431ef9ac9:pass1234
81a58e89df1f34c5487568e17327a219:guessme
```

"pass" + "1234"

"guess" + "me"

Password Recovered Using Combinator Attack

```
sec@kali:~$  
sec@kali:~$  
sec@kali:~$ ls -l  
total 52  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
-rw-r--r-- 1 root root 83 Feb 18 04:55 passwords.txt  
sec@kali:~$  
sec@kali:~$ sudo rm passwords.txt  
[sudo] password for sec:  
sec@kali:~$  
sec@kali:~$ ls -l  
total 48  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
sec@kali:~$  
sec@kali:~$
```

Remove file containing recovered passwords (passwords.txt)

Remove File Containing Recovered Passwords (passwords.txt)

```
sec@kali:~$  
sec@kali:~$ ls -l  
total 48  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
sec@kali:~$  
sec@kali:~$ sudo hashcat -m 0 -a 3 hashes.txt -o passwords.txt ?u?u?u?u?u?u  
[sudo] password for sec:  
hashcat (v6.0.0) starting...
```

Recover Passwords from Hashes Using Hashcat Under Attack Mode 3 - Mask Attack

Attack Mode 3 - Mask Attack - Successor of brute-force attack. Trying every combination of passwords using character mask.

Character Mask - 7 uppercase characters

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1429/1493 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 12 digests; 12 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:

- * Zero-Byte
- * Early-Skip
- * Not-Salted
- * Not-Iterated
- * Single-Salt
- * Brute-Force
- * Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 8 hashes found in potfile.

Host memory required for this attack: 64 MB

Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 8 hashes found in potfile.

Host memory required for this attack: 64 MB

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started.....: Sun Feb 19 03:33:00 2023 (1 min, 23 secs)
Time.Estimated...: Sun Feb 19 03:34:23 2023 (0 secs)
Guess.Mask.....: ?u?u?u?u?u?u [7]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 97178.5 kH/s (9.14ms) @ Accel:512 Loops:1024 Thr:1 Vec:8
Recovered.....: 9/12 (75.00%) Digests
Progress.....: 8031810176/8031810176 (100.00%)
Rejected.....: 0/8031810176 (0.00%)
Restore.Point....: 456976/456976 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:17408-17576 Iteration:0-1024
Candidates.#1....: NFQHCQJ → XWXQFZV

Started: Sun Feb 19 03:32:50 2023

Stopped: Sun Feb 19 03:34:24 2023

sec@kali:~\$

sec@kali:~\$ ls -l

```
total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 41 Feb 19 03:33 passwords.txt
sec@kali:~$
```

Observe Password Recovery Results


```
Time.Started.....: Sun Feb 19 03:33:00 2023 (1 min, 23 secs)
Time.Estimated... : Sun Feb 19 03:34:23 2023 (0 secs)
Guess.Mask.....: ?u?u?u?u?u?u [7]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 97178.5 kH/s (9.14ms) @ Accel:512 Loops:1024 Thr:1 Vec:8
Recovered.....: 9/12 (75.00%) Digests
Progress.....: 8031810176/8031810176 (100.00%)
Rejected.....: 0/8031810176 (0.00%)
Restore.Point....: 456976/456976 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:17408-17576 Iteration:0-1024
Candidates.#1....: NFQHCQJ → XWXQFZV
```

```
Started: Sun Feb 19 03:32:50 2023
```

```
Stopped: Sun Feb 19 03:34:24 2023
```

```
sec@kali:~$
```

```
sec@kali:~$ ls -l
```

```
total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 41 Feb 19 03:33 passwords.txt
sec@kali:~$
sec@kali:~$ sudo nano passwords.txt
```

Open File Containing Recovered Passwords (passwords.txt)

Open File Containing Recovered Passwords

56b2ab035abb810274ebd8699bd26102:GUESSME

The newly recovered password using a mask of 7 uppercase characters

Observe Recovered Passwords

```
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 41 Feb 19 03:33 passwords.txt
```

```
sec@kali:~$
sec@kali:~$ sudo nano passwords.txt
```

```
sec@kali:~$
sec@kali:~$ ls -l
```

```
total 52
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
-rw-r--r-- 1 root root 41 Feb 19 03:33 passwords.txt
```

```
sec@kali:~$
sec@kali:~$ sudo hashcat -m 0 -a 3 hashes.txt -o passwords.txt ?a?a?a?a
hashcat (v6.0.0) starting...
```

```
OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1429/1493 MB (512 MB allocatable), 2MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
Hashes: 12 digests; 12 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
```

```
Applicable optimizers:
```

- * Zero-Byte
- * Early-Skip
- * Not-Salted
- * Not-Iterated
- * Single-Salt
- * Brute-Force
- * Raw-Hash

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

Recover Passwords from Hashes Using Hashcat Under Attack Mode 3 Using A Mask of All Character Types

Brute-force attack with character mask.

Character mask - 4 characters of any type

The file (passwords.txt) not deleted.
The newly recovered password(s) will be added to the previously recovered password(s).

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 9 hashes found in potfile.

Host memory required for this attack: 64 MB

Approaching final keypace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Name.....: MD5
Hash.Target.....: hashes.txt
Time.Started.....: Sun Feb 19 03:47:37 2023 (1 sec)
Time.Estimated...: Sun Feb 19 03:47:38 2023 (0 secs)
Guess.Mask.....: ?a?a?a?a [4]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 79136.1 kH/s (2.07ms) @ Accel:1024 Loops:95 Thr:1 Vec:8
Recovered.....: 10/12 (83.33%) Digests
Progress.....: 81450625/81450625 (100.00%)
Rejected.....: 0/81450625 (0.00%)
Restore.Point....: 857375/857375 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-95 Iteration:0-95
Candidates.#1....: ss%-> ~}

Started: Sun Feb 19 03:47:34 2023
Stopped: Sun Feb 19 03:47:39 2023

```
sec@kali:~$  
sec@kali:~$ ls -l  
total 52  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Desktop  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 Documents  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 Downloads  
-rwxr-xr-x 1 root root 812 Feb 18 00:54 generate.sh  
-rw-r--r-- 1 sec sec 396 Feb 18 00:57 hashes.txt  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab1  
drwxr-xr-x 4 sec sec 4096 Nov 18 2020 lab2  
drwxr-xr-x 2 sec sec 4096 Nov 18 2020 lab3  
drwxr-xr-x 6 sec sec 4096 Nov 17 2020 lab4  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab5  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6  
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7  
-rw----- 1 root root 79 Feb 19 03:47 passwords.txt  
sec@kali:~$  
sec@kali:~$ sudo nano password.txt
```

Open File Containing Recovered Passwords (passwords.txt)

Open file containing recovered passwords

GNU nano 4.9.3 passwords.txt
56b2ab035abb810274ebd8699bd26102:GUESSME
3337abe8677a3115f8a59617821bac8b:H4d+

Previously recovered passwords using a mask of 7 uppercase characters.

Newly recovered passwords using a mask of 4 characters of any type (uppercase, lowercase, digit, symbol, etc..)

Observe Recovered Passwords

Exercise

Read the document COMP3052.SEC LAB: PASSWORDS prepared by Mike Pound.

Work on the exercises described under the following sections:

Page 6 – HASHCAT

Page 6 – LAB 4 FILES

Page 7 – ALL THE PASSWORDS

Page 9 – GOING IT ALONE