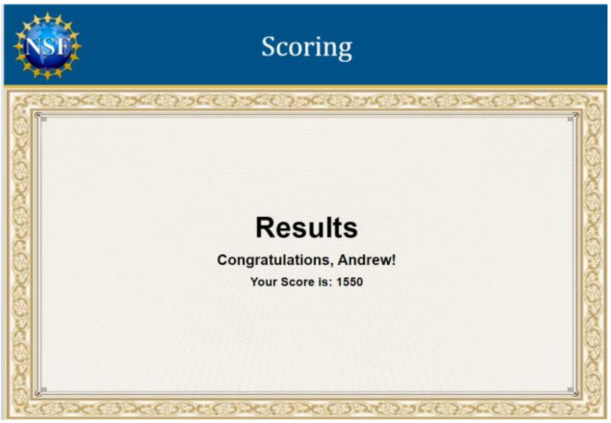
A1-6: Access Control

1. Access the Authentication puzzle-based learning exercise at https://cbt.weltec.ac.nz/cs6501/auth/story_html5.html. Please work your way through the exercise. The deliverable is a screenshot of your final result. It will look like



Scoring

Results

Congratulations, Andrew!

Your Score is: 1550

2. Please complete the following Netlab exercises:

2.1. Lab 12: Password Cracking with Hashcat from the CySA+ series
2.2. Password Cracking from the Labtainer Series
2.3. Linux Access Controls Lists from the Labtainer series
2.4. Deny Hosts from the Labtainer series

The deliverables for items 1 and 2.1-2.3 are a separate document for each lab. The screenshot for completing the authentication puzzle should be pasted in a separate document. The NetLab exercises should be a separate document showing show the occasional screenshot (which includes your student ID and name) and a brief narrative describing what you are observing. This indicates to me that you have attempted the lab and I can confirm this by viewing the reservation logs on the system. The narrative explaining the screenshot indicates to me whether you understand what it is that is captured in the screenshot.

The deliverables for the labtainer exercises are the submission of the .lab file in the *xfer directory on the Desktop of the virtual machine.

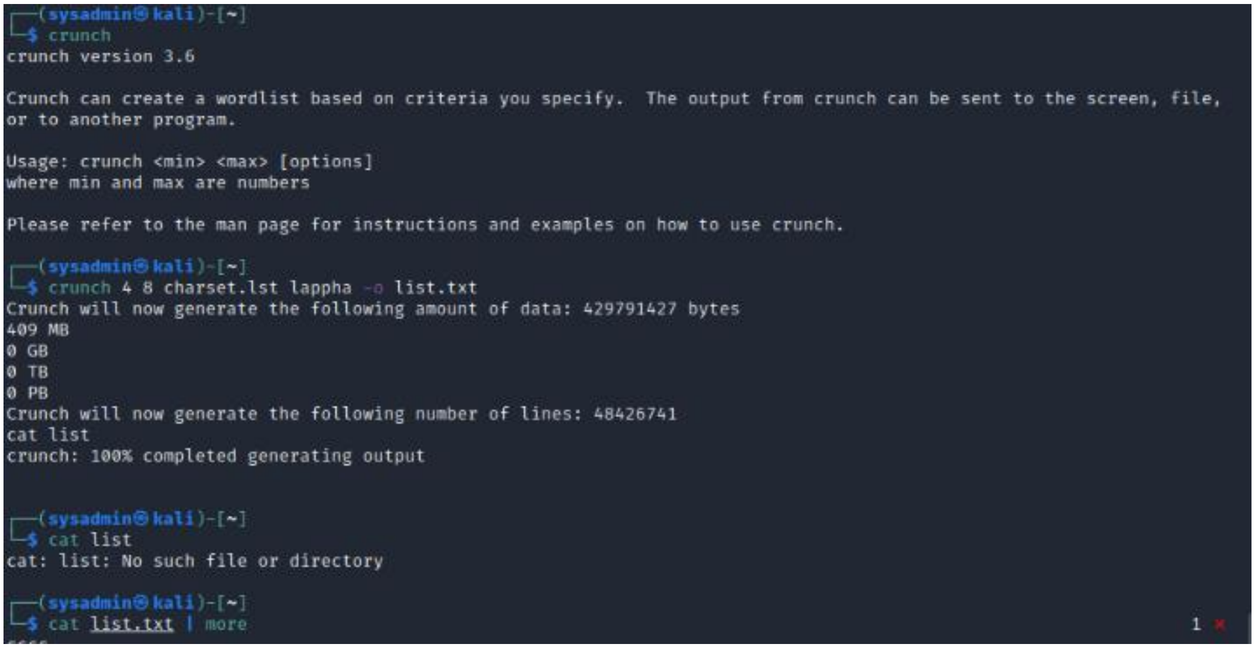
Please submit via Moodle when you have completed the required exercises.

Completion of this activity is worth 2 marks, representing 2 out of the maximum of 5 marks if you were to include this lab in your final report. Below is the rubric as a reference:

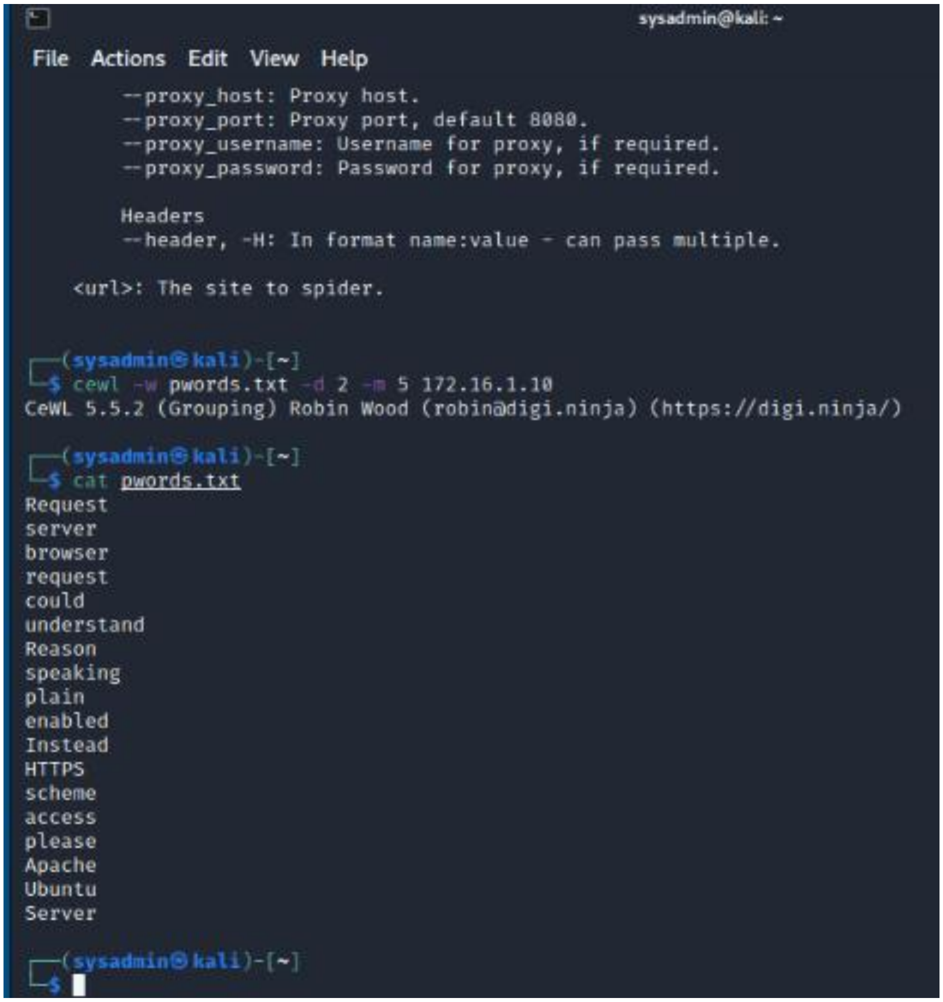
Requirement	Description	Mark
Findings	An account of the activities undertaken in the lab, including interesting or unexpected findings.	**2**
Key Concepts	The central concept behind the lab activity, and its alignment with understanding Information Security Principles.	**2**
Review	An overall review of the lab, with suggestions for changes or improvement.	**1**
		5

Password Cracking Labtainers

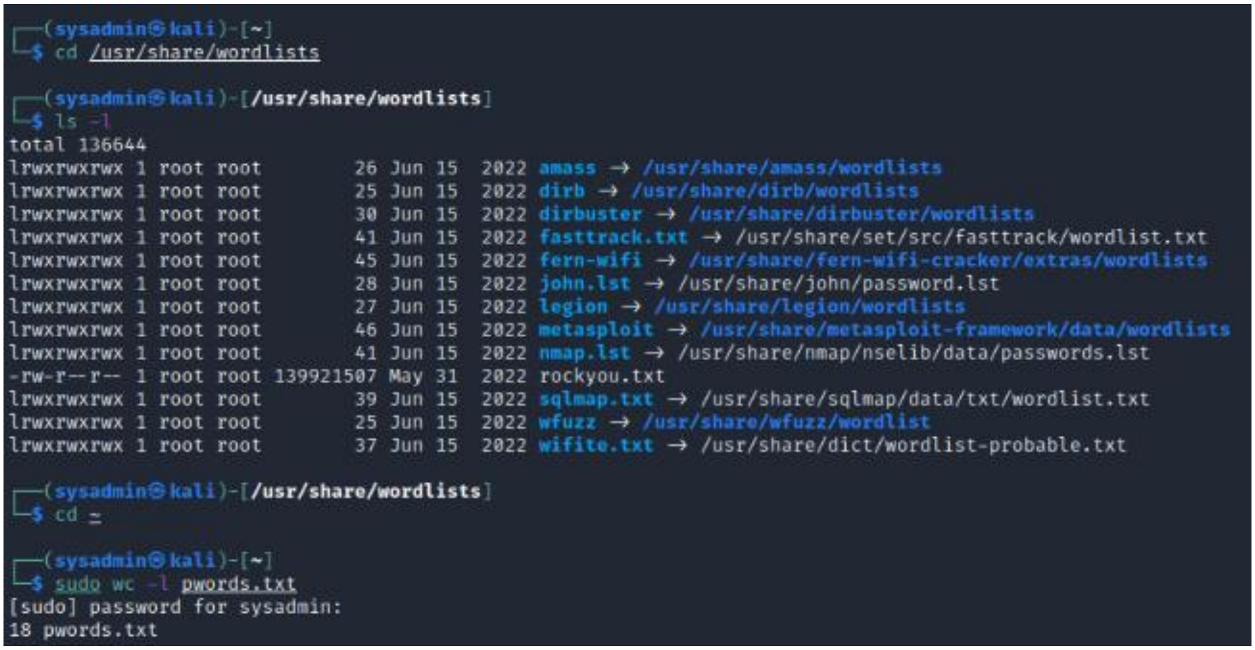
\Lab 13:



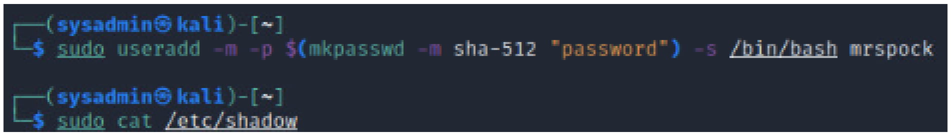
```
┌──(sysadmin㉿kali)-[~]
└─$ crunch
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.  The output from crunch can be sent to the screen, file,
or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.

┌──(sysadmin㉿kali)-[~]
└─$ crunch 4 8 charset.lst lappha -o list.txt
Crunch will now generate the following amount of data: 429791427 bytes
409 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 48426741
cat list
crunch: 100% completed generating output


┌──(sysadmin㉿kali)-[~]
└─$ cat list
cat: list: No such file or directory

┌──(sysadmin㉿kali)-[~]
└─$ cat list.txt | more                                                                                          1 ✗
```



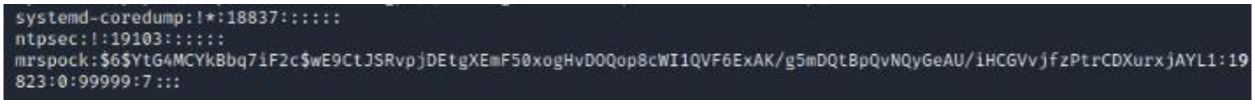
```
        --proxy_host: Proxy host.
        --proxy_port: Proxy port, default 8080.
        --proxy_username: Username for proxy, if required.
        --proxy_password: Password for proxy, if required.

        Headers
        --header, -H: In format name:value - can pass multiple.

    <url>: The site to spider.


┌──(sysadmin㉿kali)-[~]
└─$ cewl -w pwords.txt -d 2 -m 5 172.16.1.10
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(sysadmin㉿kali)-[~]
└─$ cat pwords.txt
Request
server
browser
request
could
understand
Reason
speaking
plain
enabled
Instead
HTTPS
scheme
access
please
Apache
Ubuntu
Server

┌──(sysadmin㉿kali)-[~]
└─$ 
```



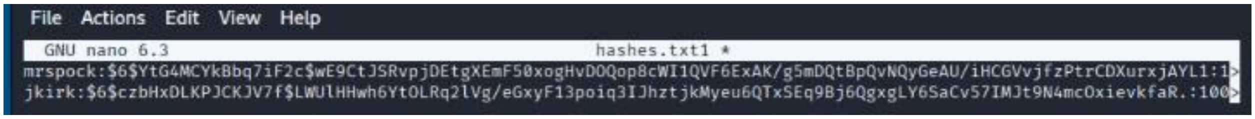
```
┌──(sysadmin㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(sysadmin㉿kali)-[/usr/share/wordlists]
└─$ ls -l
total 136644
lrwxrwxrwx 1 root root        26 Jun 15  2022 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root        25 Jun 15  2022 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root        30 Jun 15  2022 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root        41 Jun 15  2022 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root        45 Jun 15  2022 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root        28 Jun 15  2022 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root        27 Jun 15  2022 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root        46 Jun 15  2022 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root        41 Jun 15  2022 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 May 31  2022 rockyou.txt
lrwxrwxrwx 1 root root        39 Jun 15  2022 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root        25 Jun 15  2022 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root        37 Jun 15  2022 wifite.txt → /usr/share/dict/wordlist-probable.txt

┌──(sysadmin㉿kali)-[/usr/share/wordlists]
└─$ cd ~

┌──(sysadmin㉿kali)-[~]
└─$ sudo wc -l pwords.txt
[sudo] password for sysadmin:
18 pwords.txt
```



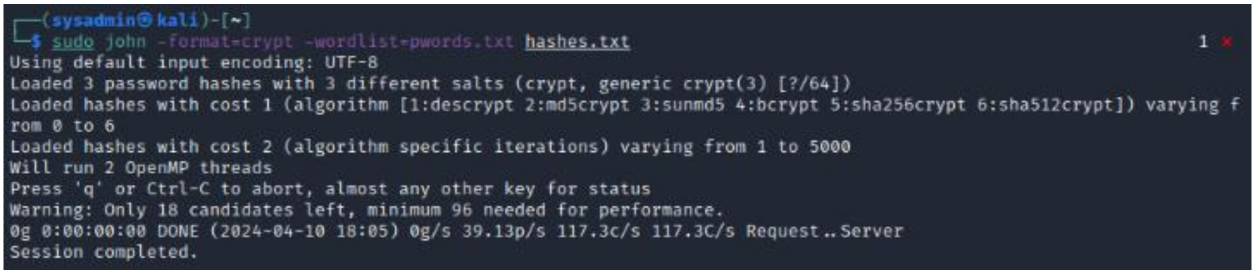
```
┌──(sysadmin㉿kali)-[~]
└─$ sudo useradd -m -p $(mkpasswd -m sha-512 "password") -s /bin/bash mrspock

┌──(sysadmin㉿kali)-[~]
└─$ sudo cat /etc/shadow
```



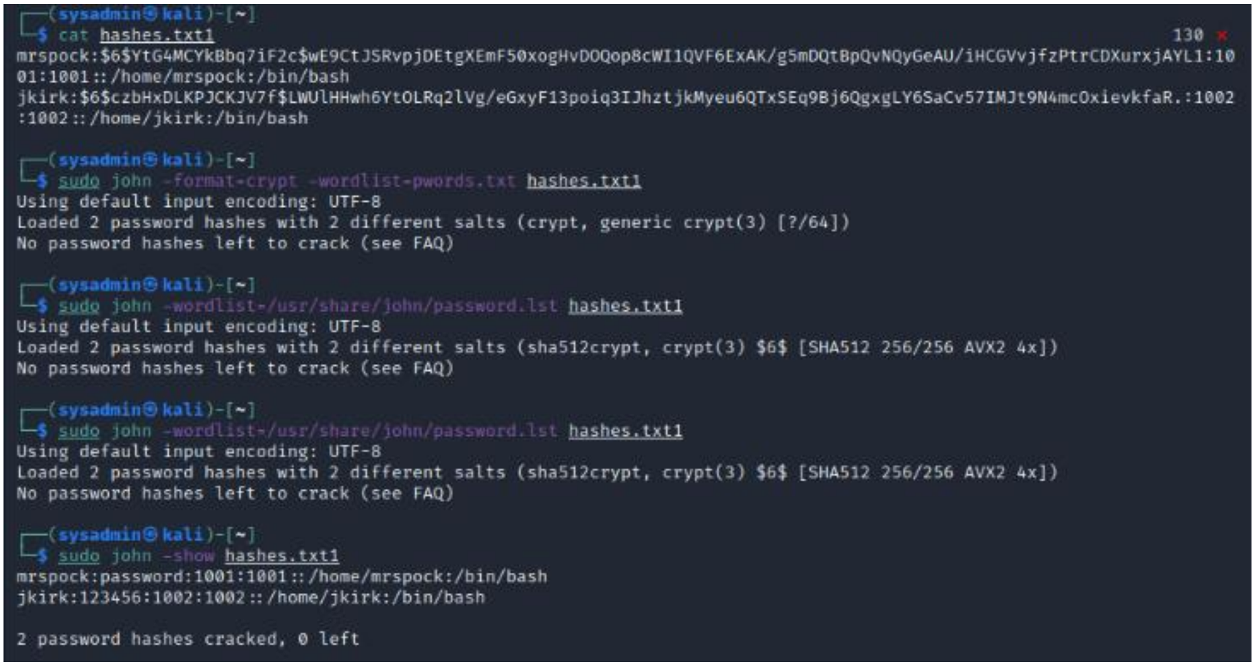
```
systemd-coredump:!*:18837::::::
ntpsec:!:19103::::::
mrspock:$6$YtG4MCYkBbq7iF2c$wE9CtJSRvpjDEtgXEmF50xogHvDOQop8cWI1QVF6ExAK/g5mDQtBpQvNQyGeAU/iHCGVvjfzPtrCDXurxjAYL1:19
823:0:99999:7:::
```



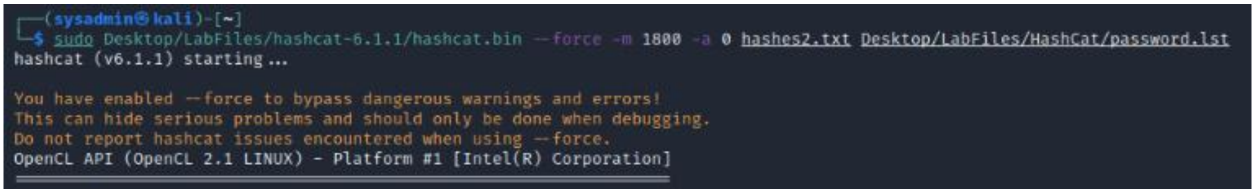
```
  GNU nano 6.3                                        hashes.txt1 *
mrspock:$6$YtG4MCYkBbq7iF2c$wE9CtJSRvpjDEtgXEmF50xogHvDOQop8cWI1QVF6ExAK/g5mDQtBpQvNQyGeAU/iHCGVvjfzPtrCDXurxjAYL1:1>
jkirk:$6$czbHxDLKPJCKJV7f$LWUlHHwh6YtOLRq2lVg/eGxyF13poiq3IJhztjkMyeu6QTxSEq9Bj6QgxgLY6SaCv57IMJt9N4mcOxievkfaR.:100>
```



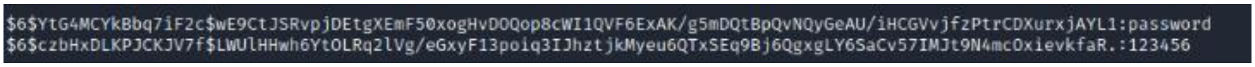
```
┌──(sysadmin㉿kali)-[~]
└─$ sudo john -format=crypt -wordlist=pwords.txt hashes.txt                                                    1 ✖
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Loaded hashes with cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) varying f
rom 0 to 6
Loaded hashes with cost 2 (algorithm specific iterations) varying from 1 to 5000
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 18 candidates left, minimum 96 needed for performance.
0g 0:00:00:00 DONE (2024-04-10 18:05) 0g/s 39.13p/s 117.3c/s 117.3C/s Request..Server
Session completed.
```



```
┌──(sysadmin㉿kali)-[~]
└─$ cat hashes.txt1                                                                                          130 ✖
mrspock:$6$YtG4MCYkBbq7iF2c$wE9CtJSRvpjDEtgXEmF50xogHvDOQop8cWI1QVF6ExAK/g5mDQtBpQvNQyGeAU/iHCGVvjfzPtrCDXurxjAYL1:10
01:1001::/home/mrspock:/bin/bash
jkirk:$6$czbHxDLKPJCKJV7f$LWUlHHwh6YtOLRq2lVg/eGxyF13poiq3IJhztjkMyeu6QTxSEq9Bj6QgxgLY6SaCv57IMJt9N4mcOxievkfaR.:1002
:1002::/home/jkirk:/bin/bash

┌──(sysadmin㉿kali)-[~]
└─$ sudo john -format=crypt -wordlist=pwords.txt hashes.txt1
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)

┌──(sysadmin㉿kali)-[~]
└─$ sudo john -wordlist=/usr/share/john/password.lst hashes.txt1
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

┌──(sysadmin㉿kali)-[~]
└─$ sudo john -wordlist=/usr/share/john/password.lst hashes.txt1
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

┌──(sysadmin㉿kali)-[~]
└─$ sudo john -show hashes.txt1
mrspock:password:1001:1001::/home/mrspock:/bin/bash
jkirk:123456:1002:1002::/home/jkirk:/bin/bash

2 password hashes cracked, 0 left
```



```
┌──(sysadmin㉿kali)-[~]
└─$ sudo Desktop/LabFiles/hashcat-6.1.1/hashcat.bin --force -m 1800 -a 0 hashes2.txt Desktop/LabFiles/HashCat/password.lst
hashcat (v6.1.1) starting...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 2.1 LINUX) - Platform #1 [Intel(R) Corporation]
==================================================================
```



```
$6$YtG4MCYkBbq7iF2c$wE9CtJSRvpjDEtgXEmF50xogHvDOQop8cWI1QVF6ExAK/g5mDQtBpQvNQyGeAU/iHCGVvjfzPtrCDXurxjAYL1:password
$6$czbHxDLKPJCKJV7f$LWUlHHwh6YtOLRq2lVg/eGxyF13poiq3IJhztjkMyeu6QTxSEq9Bj6QgxgLY6SaCv57IMJt9N4mcOxievkfaR.:123456
```