Part A

Step 1 (sudo useradd <*username*>; sudo passwd <*username*>):

1. user1 password = happy
2. user2 password = 1234
3. user3 password = cracking2
4. user4 password = 3shadow!
5. user5 password = 13darkness20
6. user6 password = Cookie!Run4Fun$

Step 2 (sudo cat /etc/shadow | tail -6 > 01277094.hash; sudo john --format=crypt xxxx.hash --wordlist=/home/tiaw/rockyou.txt):

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ sudo cat /etc/shadow | tail -6
user1:$y$j9T$FrcqQsbGVRxIXN8Hhnrr7.$OnbjH8GOsYrkpti.X5h..kDabCeUPPLSwByY0Rt4ldC:20364:0:99999:7:::
user2:$y$j9T$abcY4Jo7baSTYtc6RFHGx0$waA6JVTqTxrtkSlYnJh67JnUdM0ngtZp9JlsdVb8lRC:20364:0:99999:7:::
user3:$y$j9T$CeWIImRHhu9iLY0J0m2Op1$wGDpzgNHzSxPs4xnH7WyC0inheIskBTC4yqVKjxPoY5:20364:0:99999:7:::
user4:$y$j9T$zJOoyxIy2UUrx2BFQ7u4z0$BTfTTZ2UtchqEdRkwCNIHixyzWf.F4Sehb.o1uSS0r9:20364:0:99999:7:::
user5:$y$j9T$V3m7V.OkM2vMA8DMia8qi/$nqxTWBHgkLXrwny8dNkY8qh7iv1rEfGwkXfHYaJkbpD:20364:0:99999:7:::
user6:$y$j9T$aZGEb8X6aXMVcLs8iVHJm/$scbDGf2pQZGa1lJ4eAfu1BZjXzAwqgm6l9b5eFa2Se4:20364:0:99999:7:::

┌──(tiaw㉿Tia-Kali)-[~]
└─$ sudo cat /etc/shadow | tail -6 > 01277094.hash

┌──(tiaw㉿Tia-Kali)-[~]
└─$ cat 01277094.hash
user1:$y$j9T$FrcqQsbGVRxIXN8Hhnrr7.$OnbjH8GOsYrkpti.X5h..kDabCeUPPLSwByY0Rt4ldC:20364:0:99999:7:::
user2:$y$j9T$abcY4Jo7baSTYtc6RFHGx0$waA6JVTqTxrtkSlYnJh67JnUdM0ngtZp9JlsdVb8lRC:20364:0:99999:7:::
user3:$y$j9T$CeWIImRHhu9iLY0J0m2Op1$wGDpzgNHzSxPs4xnH7WyC0inheIskBTC4yqVKjxPoY5:20364:0:99999:7:::
user4:$y$j9T$zJOoyxIy2UUrx2BFQ7u4z0$BTfTTZ2UtchqEdRkwCNIHixyzWf.F4Sehb.o1uSS0r9:20364:0:99999:7:::
user5:$y$j9T$V3m7V.OkM2vMA8DMia8qi/$nqxTWBHgkLXrwny8dNkY8qh7iv1rEfGwkXfHYaJkbpD:20364:0:99999:7:::
user6:$y$j9T$aZGEb8X6aXMVcLs8iVHJm/$scbDGf2pQZGa1lJ4eAfu1BZjXzAwqgm6l9b5eFa2Se4:20364:0:99999:7:::

┌──(tiaw㉿Tia-Kali)-[~]
└─$
```

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ sudo john --format=crypt 01277094.hash --wordlist=/home/tiaw/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Step 3 - Cracked passwords after waiting 15 mins:

happy (user1)
1234 (user2)

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ sudo john --format=crypt 01277094.hash --wordlist=/home/tiaw/rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
happy            (user1)
1234             (user2)
2g 0:00:10:41 0.20% (ETA: 2025-10-07 12:00) 0.003119g/s 52.86p/s 214.4c/s 214.4C/s loverose..giorgos
2g 0:00:14:37 0.27% (ETA: 2025-10-07 11:20) 0.002280g/s 53.29p/s 215.1c/s 215.1C/s winny..smokers
2g 0:00:15:15 0.28% (ETA: 2025-10-07 11:00) 0.002184g/s 53.48p/s 215.7c/s 215.7C/s 110277..041585
```

Extra Credit (Crack MD5)

I made a file (vi md5_extra-credit.hash) and pasted the two md5 hashes into it:

I then did man john and john --help to read the manual pages and figure out the options for --format:

```
--format=[NAME|CLASS][,..] Force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats.
                           See also doc/OPTIONS for more advanced selection of
                           format(s), including using classes and wildcards.
```

I tried md5crypt & md5crypt-long from the --list=formats, but then didn't work:

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ john --list=formats | grep md5
416 formats (149 dynamic formats shown as just "dynamic_n" here)
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
django-scrypt, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32,
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
```

So then I checked the --list=subformats | grep md5:

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ john --list=subformats | grep md5
Format = dynamic_0   type = dynamic_0: md5($p) (raw-md5)
Format = dynamic_1   type = dynamic_1: md5($p.$s) (joomla)
Format = dynamic_2   type = dynamic_2: md5(md5($p)) (e107)
Format = dynamic_3   type = dynamic_3: md5(md5(md5($p)))
Format = dynamic_4   type = dynamic_4: md5($s.$p) (OSC)
Format = dynamic_5   type = dynamic_5: md5($s.$p.$s)
Format = dynamic_6   type = dynamic_6: md5(md5($p).$s)
Format = dynamic_8   type = dynamic_8: md5(md5($s).$p)
Format = dynamic_9   type = dynamic_9: md5($s.md5($p))
Format = dynamic_10  type = dynamic_10: md5($s.md5($s.$p))
Format = dynamic_11  type = dynamic_11: md5($s.md5($p.$s))
Format = dynamic_12  type = dynamic_12: md5(md5($s).md5($p)) (IPB)
Format = dynamic_13  type = dynamic_13: md5(md5($p).md5($s))
Format = dynamic_14  type = dynamic_14: md5($s.md5($p).$s)
Format = dynamic_15  type = dynamic_15: md5($u.md5($p).$s)
Format = dynamic_16  type = dynamic_16: md5(md5(md5($p).$s).$s2)
Format = dynamic_18  type = dynamic_18: md5($s.Y.$p.0×F7.$s) (Post.Office MD5)
Format = dynamic_19  type = dynamic_19: md5($p) (Cisco PIX)
Format = dynamic_20  type = dynamic_20: md5($p.$s) (Cisco ASA)
Format = dynamic_22  type = dynamic_22: md5(sha1($p))
Format = dynamic_23  type = dynamic_23: sha1(md5($p))
Format = dynamic_29  type = dynamic_29: md5(utf16($p))
Format = dynamic_34  type = dynamic_34: md5(md4($p))
Format = dynamic_39  type = dynamic_39: md5($s.pad16($p)) (net-md5)
```

And then tried --format=raw-md5, which then cracked it when using the rockyou.txt wordlist:

```
┌──(tiaw㉿Tia-Kali)-[~]
└─$ sudo john --format=raw-md5 md5_extra-credit.hash --wordlist=/home/tiaw/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
root             (?)
2g 0:00:00:00 DONE (2025-10-03 18:05) 50.00g/s 20179Kp/s 20179Kc/s 20188KC/s rory17..ronald918
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```