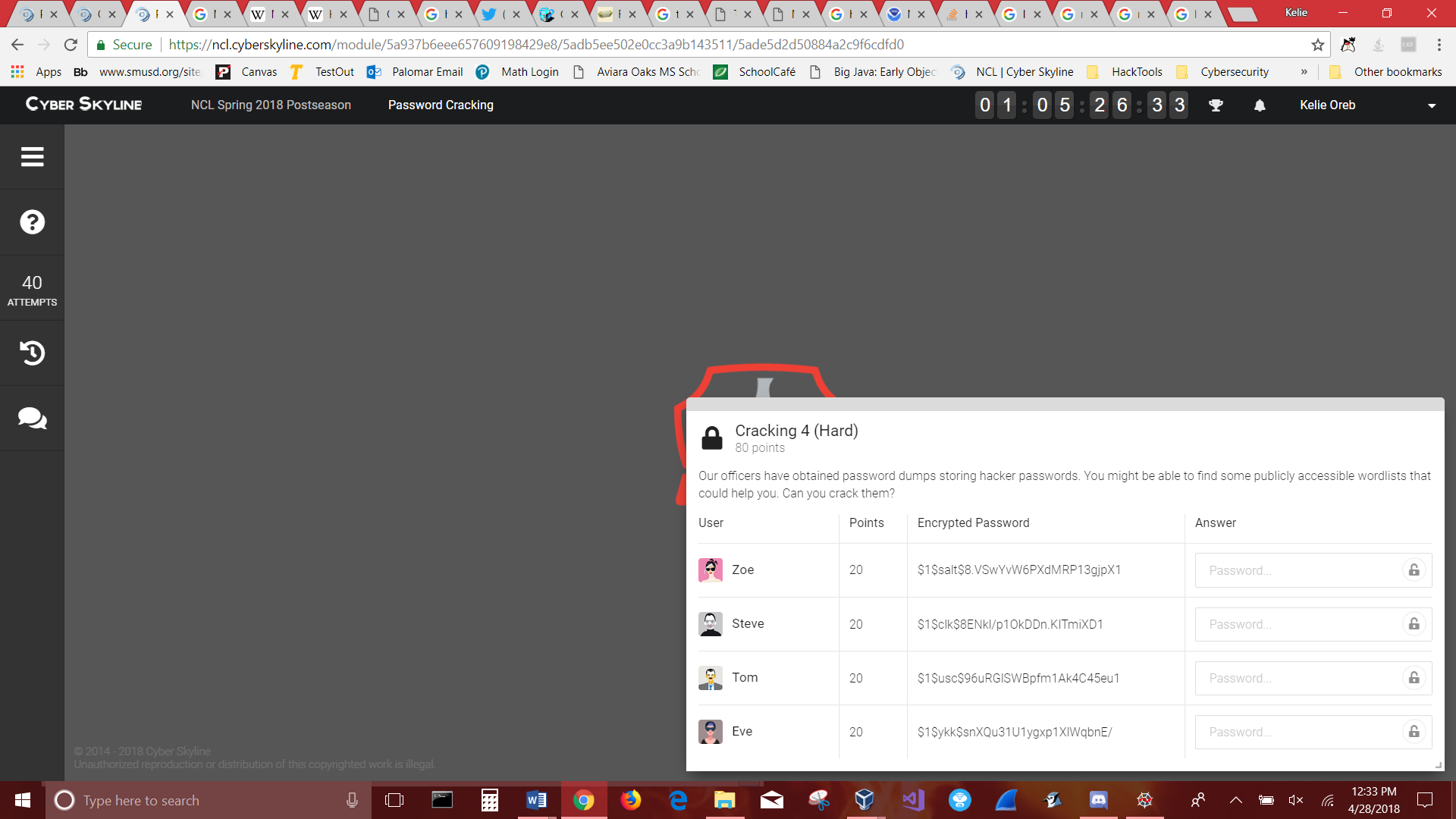
Password Cracking 4 Hard

$1$salt$8.VSwYvW6PXdMRP13gjpX1   
$1$clk$8ENkl/p1OkDDn.KITmiXD1  
$1$usc$96uRGlSWBpfm1Ak4C45eu1  
$1$ykk$snXQu31U1ygxp1XlWqbnE/



$1$ md5

$2a$ Blowfish

$2y$ Blowfish, with correct handling of 8 bit characters

$5$ sha256

$6$ sha512

The output is the concatenation of the version identifier ``$1$'', the salt, a ``$'' separator, and the 128-bit hash output.

**-m 10** specifies the hash-type. Running –help will print you a full list of supported types

20 = md5($salt.$pass)

**-a 0** defines the attack mode. There are six modes which you can choose one from:

0 = Straight (just the word found in $wordlist: foobar)

1 = Combination (words combinated: foobar)

2 = Toggle-Case (toggled case: Foobar, FOobar, FOObar, ...)

3 = Brute-force (tries all combinations from a given keyspace)

4 = Permutation (permutations like abc, acb, bac, ...)

5 = Table-Lookup (read [here](<http://hashcat.net/wiki/doku.php?id=table_lookup_attack)>)

https://hashcat.net/wiki/doku.php?id=example\_hashes

|  |  |  |
| --- | --- | --- |
| 500 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5) 2 | $1$28772684$iEwNOgGugqO9.bIz5sk8k/ |

**Algorithm Name:**MD5 / crypt(3) / $1$

**Description:**A very common crypt(3) implementation of MD5. Hashes starting with "$1$" are generated using crypt(3)-MD5 algorithm method.