Willis Allstead
September 26, 2018
CS 450

Lab 1

1. When applied to the file crack-these-please, how many of its 50 passwords were cracked at each phase:

a. dictionary attack solved 11 of the passwords

b. hybrid attack solved 12 of the passwords

c. combination attack solved 39 of the passwords

d. 11 of the passwords were never solved within the time spent

On the following page I have included the screenshot of my terminal for the output of these three commands. The important parts are boxed by the blue lines. As you can see, it took <1 second for the first attack, 1 second for the hybrid, and 1 hour, 22 minutes, and 17 seconds for the combination attack. I had to stop the combination myself because it was taking too long.

```
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
money            (crack21)
cowboy           (crack07)
hello            (crack14)
test             (crack29)
blue             (crack03)
japan            (crack16)
bonjour          (crack04)
dog              (crack10)
pass             (crack24)
www              (crack43)
www              (crack44)
11g 0:00:00:00 100% 275.0g/s 88550p/s 3876Kc/s 3876KC/s temp..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
Williss-MacBook-Pro:run willisallstead$ cat john.pot
M.h.0vk3BhbbE:money
hSWM/OxbN7mLg:cowboy
VtsKjVbDshURM:hello
HNTH57eGshHyQ:test
qOehxlruvN3F6:blue
TviJwR4elCrEk:japan
oPWWjG8dOl7Jk:bonjour
bVbJ8EjFft7Ig:dog
J1KYaW5A7YmTw:pass
NbXi5ONo1R11g:www
krwhufvZUsT/Q:www
Williss-MacBook-Pro:run willisallstead$ ./john crack-these-please -w=password.lst -rules
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Remaining 39 password hashes with 39 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
wwwwww           (crack47)
1g 0:00:00:01 100% 0.9174g/s 127766p/s 4870Kc/s 4870KC/s Sssing
Use the "--show" option to display all of the cracked passwords reliably
Session completed
Williss-MacBook-Pro:run willisallstead$ ./john crack-these-please -w=password.lst -rules --show
Invalid options combination or duplicate option: "--show"
Williss-MacBook-Pro:run willisallstead$ ./john crack-these-please -w=password.lst -rules -show
Invalid options combination or duplicate option: "-show"
Williss-MacBook-Pro:run willisallstead$ ./john crack-these-please -w=password.lst -rules
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Remaining 38 password hashes with 38 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 100% 0g/s 130154p/s 4945Kc/s 4945KC/s Sssing
Session completed
Williss-MacBook-Pro:run willisallstead$ ./john crack-these-please
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Remaining 38 password hashes with 38 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
1337             (crack18)
bloody           (crack02)
bread            (crack05)
perro            (crack11)
more             (crack22)
bike             (crack01)
bueno            (crack06)
mind             (crack20)
kaput            (crack17)
ddd              (crack08)
tall             (crack28)
smc              (crack26)
linux            (crack19)
dejavu           (crack09)
w                (crack41)
stir             (crack27)
really           (crack25)
nauj             (crack39)
fido             (crack12)
hackme           (crack36)
abcdefgh         (crack23)
ww               (crack42)
wwww             (crack45)
wwwww            (crack46)
usa              (crack30)
into             (crack15)
sayonara         (crack31)
27g 0:01:22:17 3/3 0.005468g/s 225668p/s 2747Kc/s 2747KC/s lhygricu..lhygosid
```

2. Windows stores passwords in the registry file located at:

C:\windows\system32\config\SAM

Source (As I do not own a windows machine):
https://security.stackexchange.com/questions/63890/does-windows-have-a-built-in-password-store

3.

a. If the length of a numbers-only password is 17, it would take 332.01 years to crack.
b. Given today's computing power, it would take a password of length 18 to make a computer take over 50 years to crack my password. If I put in 18 as the count of digits in the number password, it gives an estimate of 207.51 years.
c. If Moore's law never stops being true, with a special factor of 40,000,000 , a password length of 24 would be required to make the cracking take above 50 years, 83 years in this case.
d. Using the same special factor as in part [c.] but instead using the "PURELY Random Combo of Alpha/Numeric/Special", I find that a password of length 13 would be required to surpass 50 years in cracking time, in this case taking 3,713.22 years.