Willis Allstead
September 16, 2018
CS 450

Homework 1

1.

Basically, a password salt is used to enhance the security of a password database. If a program has cracked a popular hashing algorithm, and the same two passwords exist in two databases, as long as the salt is different for each one it will make it harder to use precomputed hash tables to find both of the passwords.

Salts should be treated as if they are public knowledge, and if they are truly public it will still do its job of making the cracking itself take longer. If an attacker cracks one user's password the crack won't be usable for another user.

2.

95 printable ASCII characters = A
Passwords are 10 characters in length = B
Encryption rate of 6.4 million / second = C

Time to test all possible passwords = X

X = (A ^ B) / C = (95 ^ 10) / 6,400,000 = 9,355,264,675,599 seconds
X = ~ 296,450 years

As you can see, the total time that it would take to exhaustively test all possible passwords on a UNIX machine would be the amount of characters to the power of how many characters in a password divided by the rate at which the password cracker encrypts.

3. all generated with `openssl rand -base64 32`

Fb945aKikwe5YpMvgLWl4CpsM/WThQvc0gv2Ls1lb/I
➔ 10,000+ centuries
EGte4albCiYXBI9M3qmXl4H7fqUHCGmKirDjEQG03dI
➔ 10,000+ centuries
QfMMDKRVgOPpW2Q88hs+kkv65j01jUxcMS5tLeb6n74
➔ 10,000+ centuries
CnTJFpvvauWmfAHO9Y/eg7frBBBNSiF1jzKdvnhMr2s
➔ 10,000+ centuries
XPyVjmRKapI8DuRQrh2eHRpK5ryDPxC6pMKVKZLfHUc
➔ 10,000+ centuries