

Intro to Cybersecurity

1.1.4 - Password Hashing



GALANTECH —with—
GARDEN STATE CYBER


CYBER.ORG

Identity Proofing ≠ Authentication

- A person claims to be a user but cannot authenticate
 - Example: When someone loses their password.
- They are then asked to provide a different value like the answer to a security question
 - Example: What is your mother's maiden name?
- Note that does not get them into the account
 - It merely sends a reset of the password to a previously set communication like email.

Account help for
John Smith@gmail.com

Answer the following to verify this account is yours.



Answer the security question you
added to your account

Brother's middle name



PASSWORDS – What you know

Single Sign-On (SSO): one authentication gives access to many servers or resources

Passphrases: a string of words provides more protection than a strong password BUT users are resistant to typing and it is not mobile device friendly.

Ex: *The 3 little pigs say do not forget the bacon!*



Where are Passwords stored?

Windows machine: *SAM registry hive* holds all account details like usernames and passwords

Linux: store usernames, passwords, some settings

- **/etc/passwd** = default file, not used for passwords
 - Not secure, can be hacked because more than **root** can access this file.
- **/etc/shadow** = hidden file used to store usernames, passwords, some settings.
 - **ONLY root** user has access



Password Storage & Hashing

- Passwords should never be stored in plain text
- Most common method of safely storing passwords is to HASH the password

Hashing – what is it??

Definition: *a special mathematical function that performs one-way conversion.*



GALANTECH —with—
GARDEN STATE CYBER

Hashing

- Hashing is intended as one-way conversion. Once the algorithm is processed, the hashed password is stored by the system.
- Authentication happens when a hashed password is compared against the original hash stored by the system – this will confirm that you have the correct original plaintext.
- **MD5, SHA256, and SHA512** are commonly used hashing algorithms



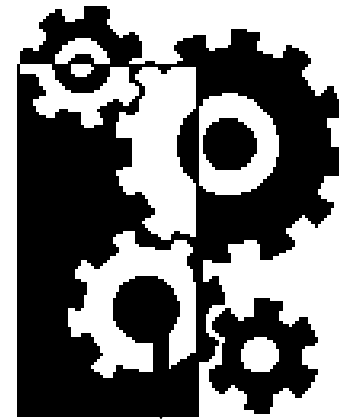
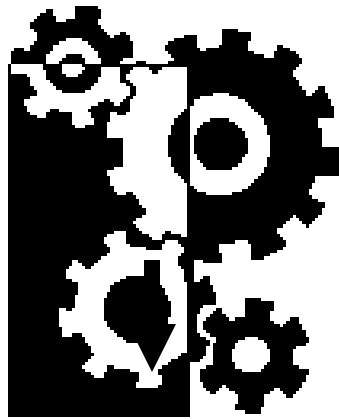
A simplified version of Hashing

- Password: *this*
- ASCII Values $t = 116$, $h = 104$, $i = 105$, $s = 115$
- These values are multiplied by 2 to get the calculated numbers, which would be 232, 208, 210, 230.
- These numbers are added together then divided by 10 →
 $(232+208+210+230)/10 = 88$
- This gives you a hash of 88,
 - But there are other number/letter combinations that would produce this hash.
- The actual hashing algorithms are much more complex and do much more than just performing arithmetic operations on relatively small numbers. It is extremely difficult to determine the data that was hashed, even if you know the algorithm used to generate the hash.



HASHING

User1, Pa\$\$word MATCH – ACCESS APPROVED
User1, Pa\$\$word NO MATCH – ACCESS DENIED !!!



e52cac67419a9

UGFzc3dvcmQ1

Store this as: User1, password = e52cac67419a9



Attacking Hashed Passwords with Rainbow Tables

- Rainbow Tables - Definition: *a file of pre-computed hash values for every possible combination of characters. VERY BIG FILE!!*
- SALT = method of protecting against Rainbow Table hacks.
- Normal password storage:
 $\text{md5} \times (\text{password}) = \text{hash of } 5f4dcc3b5aa765d61d8327d$
- Salted password storage:
 $\text{md5} \times (\text{'randomstring'+password}) = \text{fb985bc394cf7ec1f46feac5ff}$



STOP video at 9:24 min



Attacking Hashed Passwords

- **Define term: Hash collision** - when two or more source data convert to the same hash value.
- **Birthday Attack** – in a group of >22 people, the chance that two people share a birthday is greater than 50%.
- This attack takes advantage of the fact that when collecting a large number of hashes, it is likely that there will be multiple data items (like passwords) that have the same hash value.
- With a “hash collision” collection of data, you could reverse engineer the key used for hashing.



GALANTECH —with—
GARDEN STATE CYBER

Attacking Hashed Passwords

- **Pass the Hash attack** – this attack doesn't try to crack the password. Instead, the attacker gets to the SAM hive or etc/shadow file to dump the hashes from system storage.
- Using special software, the attacker logs in with the username and password hash instead of the text password.



GALANTECH —with—
GARDEN STATE CYBER



Intro to Cybersecurity



Activity – Hashing and Salts with CyberChef

