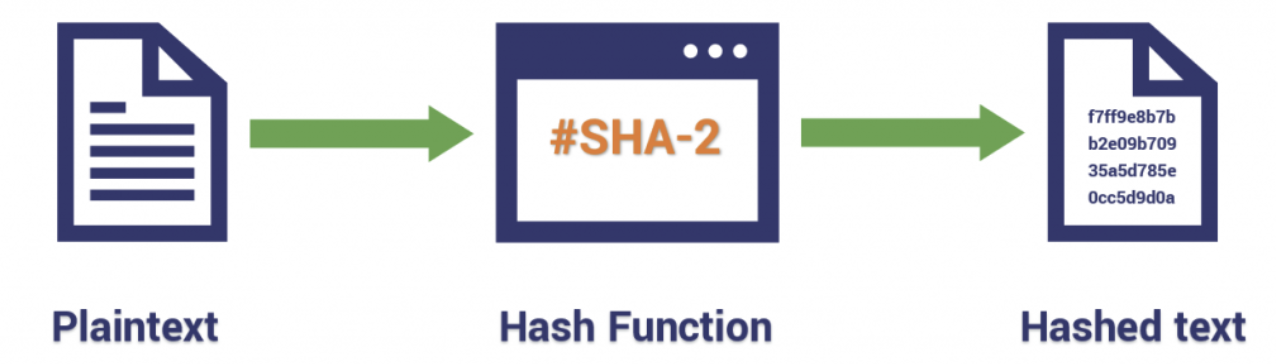
**Password Cracking Lab - 2024**

**Think Like an Adversary & Confidentiality**

**Intro:** Passwords are used in nearly every aspect of computers to help protect accounts and data. These passwords are almost always stored as a hash on the computer instead of the plaintext version of the password. A hash is just the output of a of a one way mathematical equation. When a user tries to log in with their password, the computer takes the entered password, hashes it, and then compares the hash to the stored hash. If the hashes match, the user is allowed in, if they don’t match then the user is prompted to retry their password.



**LAB:**

**1)** Determine what type of hash algorithm is being used for the below samples. Here’s a website with sample hash types: <https://hashcat.net/wiki/doku.php?id=example_hashes>

|  |  |
| --- | --- |
| 8743b52063cd84097a65d1633f5c74f5 |  |
| c73d08de890479518ed60cf670d17faa26a4a71f995c1dcc978165399401a6c4:53743528 |  |
| b89eaac7e61417341b710b727768294d0e6a277b |  |
| $ASN$\*1\*20000\*80771171105233481004850004085037\*d04b17af7f6b184346aad3efefe8bec0987ee73418291a42 |  |

**2)** There are many online resources to hash plaintext. One such website is <https://www.md5hashgenerator.com/> Use this website to create hashes for the following plaintext passwords using the specificied hash algorithm:

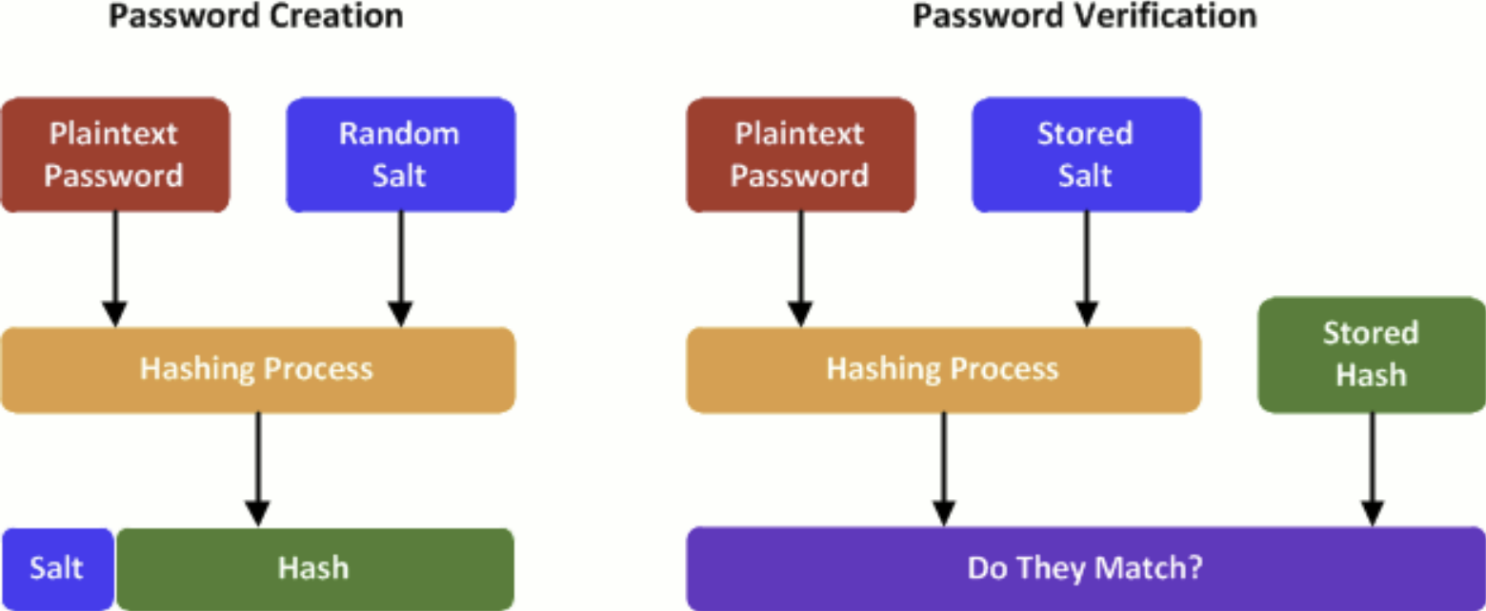
|  |  |  |
| --- | --- | --- |
| ReturnOfTheKing! | MD5 |  |
| ProtectTheRingFrodo!!12345 | MD5 |  |
| ThoseWhoWanderAreLost! | SHA256 |  |
| One\_Ring\_To\_Rule\_Them\_All | SHA512 |  |

**3)** Now let’s try the opposite and see if you can figure out what the plaintext passwords are for the following hashes. A site like <https://www.crackstation.net> might be helpful. Find the password and the hash algorithm used:

|  |  |  |
| --- | --- | --- |
| **HASH** | **ALGORITHM** | **PLAINTEXT PASSWORD** |
| aa293598348f661c2e4524692bc6ab15 |  |  |
| fe42829a38a4134aa1c2fb67addf509676c89795 |  |  |
| 3A04243F881FC67D4FE2EDEF9DB85441 |  |  |
| 9349B0AE0698668013638C9DADE4B6A5CCC220FB83013EE165E4EA6872F1E89414FAF50968F77C109D21CA758971D016E25BDC3A0853F55A42BF7DDE00BAA100 |  |  |

**BONUS:** You’re getting stronger with the password cracking force...but can you figure out what the plaintext version of the following two hashes are? Hint: The message may be “encoded.” <https://cryptii.com/> might be a helpful website.

|  |  |
| --- | --- |
| wosdi pgmcy zlltk nsfhr bpnkw oy |  |
| -.... -.... ...-- -.-. ---.. -... -... -.-. .---- ----- -... -.... -.... .---- ....- ---.. . -.. ....- ....- --... -.... ...-- -.. ..... ----. .- ..--- . . ....- . |  |



Once you have finished, there is a fun password cracking activity on TryHackMe that you can do! Get into the pairs you created yesterday, and work through it. You can access the Password Cracking assignment called “John the Ripper”.

1. Go to tryhackme.com
2. Sign into your account.
3. Go to Learn > Assignments.
4. Click the “Password Cracking – JohnTheRipper” lab and have fun!