Credential Based Attacks

Credential based attacks occur when attackers steal credentials to gain access, bypass an organizations security measures, and steal critical data.

There are different types of Credential Based Attacks:

1. Brute Force Attacks
2. Dictionary Attack
3. Birthday Attack
4. Rainbow table Attack
5. Pass the hash attack
6. Broken Authentication

Brute Force Attack

A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing

Correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

“A successful brute-force attack gives cybercriminals remote access to the target computer in the network”

Mitigations:

1. Encourage users to use complex passwords

2. Lockout accounts after few attempts

3. Use Multi-factor authentication.

4. Use Captcha to slow down brute-force

Dictionary Attack

A dictionary attack tries combinations of common words and phrases. Originally, dictionary attacks used words from a dictionary as well as numbers, but today dictionary attacks also use passwords that have been leaked by earlier data breaches. These leaked passwords are available for sale on the dark web and can even be found for free on the regular web.

For example, the software will replace a lowercase “l” with a capital “I” or a lowercase “a” with an “@” sign.

The software only tries the combinations its logic says are most likely to succeed.

Mitigations:

1. Advise users not to keep a simple word or easily identifiable information as password.
2. Encourage users to use complex passwords
3. Lockout accounts after few attempts
4. Use Captcha to slow down brute-force
5. Use multifactor authentication

Birthday attack

Birthday attack is a type of cryptographic attack that belongs to a class of brute force attacks. It exploits the mathematics behind the birthday problem in probability theory. The success of this attack largely depends upon the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations, as described in the birthday paradox problem

Mitigations:

1. Not to Use Personal details as Passwords
2. Encourage users to use complex passwords
3. Lockout accounts after few attempts
4. Use Captcha to slow down brute-force
5. Use multifactor authentication

Rainbow table attack

A rainbow table attack is a type of hacking wherein the perpetrator tries to use a rainbow hash table to crack the passwords stored in a database system. A rainbow table is a hash function used in cryptography for storing important data such as passwords in a database. Sensitive data are hashed twice (or more times) with the same or with different keys in order to avoid rainbow table attacks.

Mitigations:

1. Rainbow table attacks can easily be prevented by using salt techniques,

   -**Salt** is a random data that is passed into the hash function along with the plain text.

2. Lockout accounts after few attempts
3. Use Captcha to slow down brute-force
4. Use multifactor authentication

Pass the hash Attack

Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying hash of a user's password, instead of requiring the associated plaintext password as is normally the case .

This will reduce the effort of the attacker as he does not have to crack the plaintext password from the stolen hash.

Mitigations:

1. Restrict and protect high privileged domain accounts:

   -This mitigation reduces the risk of administrators from inadvertently exposing privileged credentials to higher risk computers.

2. Restrict and protect local accounts with administrative privileges

   -This mitigation restricts the ability of attackers to use administrative local accounts for lateral movement attacks.

3. Restrict inbound traffic using the Windows Firewall

   -This mitigation restricts attackers initiating lateral movement from a compromised workstation by blocking in bound connections on all other workstations with the local Windows Firewall.

Broken Authentication

Broken Authentication weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

1.Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.

2.Permits brute force or other automated attacks.

3.Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".

4.Uses weak or ineffective credential recovery and forgot-password processes.

5.Uses plain text or weakly hashed passwords

Mitigations:

1. Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force attacks.
2. Do not ship or deploy with any default credentials, particularly for admin users.
3. Implement weak-password checks, such as testing new or changed passwords \ against a list of the top 10000 worst passwords.
4. Lock user accounts after certain failed attempts