Brute Force: Password Cracking, Sub-technique T1110.002 - Enterprise

Archived: 2026-04-05 18:12:18 UTC

Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. OS Credential Dumping can be used to obtain password hashes, this may only get an adversary so far when Pass the Hash is not an option. Further, adversaries may leverage Data from Configuration Repository in order to obtain hashed credentials for network devices.[1]

Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network.[2] The resulting plaintext password resulting from a successfully cracked hash may be used to log into systems, resources, and services in which the account has access.

Source: https://attack.mitre.org/techniques/T1110/002