# TTP Detail – T1110.002

## TTP Information

Name: Password Cracking

Description: 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](https://attack.mitre.org/techniques/T1003) can be used to obtain password hashes, this may only get an adversary so far when [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) is not an option. Further, adversaries may leverage [Data from Configuration Repository](https://attack.mitre.org/techniques/T1602) in order to obtain hashed credentials for network devices.(Citation: US-CERT-TA18-106A)

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.(Citation: Wikipedia Password cracking) 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.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Net Crawler

## APTs (Intrusion Sets)

* APT3
* Dragonfly
* FIN6
* Salt Typhoon