# TTP Detail – T1550.002

## TTP Information

Name: Pass the Hash

Description: Adversaries may “pass the hash” using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash.

When performing PtH, valid password hashes for the account being used are captured using a [Credential Access](https://attack.mitre.org/tactics/TA0006) technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Adversaries may also use stolen password hashes to "overpass the hash." Similar to PtH, this involves using a password hash to authenticate as a user but also uses the password hash to create a valid Kerberos ticket. This ticket can then be used to perform [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003) attacks.(Citation: Stealthbits Overpass-the-Hash)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: lateral-movement

## Malware

* BADHATCH
* Cobalt Strike
* HOPLIGHT

## Tools

* CrackMapExec
* Empire
* Mimikatz
* Pass-The-Hash Toolkit
* PoshC2

## APTs (Intrusion Sets)

* APT1
* APT28
* APT32
* APT41
* Aquatic Panda
* Chimera
* Ember Bear
* FIN13
* GALLIUM
* Kimsuky
* Wizard Spider