**Pass The Hash attack**

**Description 1.**

In cryptanalysis and computer security, pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

After an attacker obtains valid user name and user password hash values (somehow, using different methods and tools), they are then able to use that information to authenticate to a remote server or service using LM or NTLM authentication without the need to brute-force the hashes to obtain the cleartext password (as it was required before this technique was published). The attack exploits an implementation weakness in the authentication protocol, where password hash remain static from session to session until the password is next changed. [1]

**Description 2.**

Password hashes are equivalent to clear-text passwords. If the attacker manages to obtain the hash, it is possible to use it to gain access to a system without the need to know the password used to create it. This type of attack is known as "pass-the-hash" attack. Password hashes are loaded into the Local Security Authority Subsystem (Lsass). Lsass runs as the executable %SystemRoot%\System32\Lsass.exe, which is responsible for user authentication, among other things (Russinovich, Solomon, & Ionescu, 2009). Using hash dumping tools, an attacker can dump the passwords' hashes for this attack. [2]

**Description 3.**

A pass the hash attack is an exploit in which an attacker steals a hashed user credential and, without cracking it, reuses it to trick an authentication system into creating a new authenticated session on the same network. [3]

References

[1] https://en.wikipedia.org/wiki/Pass\_the\_hash

[2] Ewaida, Bashar. "Pass-the-hash attacks: Tools and Mitigation." *Last accessed September* 11 (2013).

[3] http://searchsecurity.techtarget.com/definition/pass-the-hash-attack