CAPEC-644: Use of Captured Hashes (Pass The Hash) (Version 3.9)

Archived: 2026-04-05 17:37:39 UTC

Description

An adversary obtains (i.e. steals or purchases) legitimate Windows domain credential hash values to access systems within the domain that leverage the Lan Man (LM) and/or NT Lan Man (NTLM) authentication protocols.

Extended Description

When authenticating via LM or NTLM, an authenticating account's plaintext credentials are not required by the protocols for successful authentication. Instead, the hashed credentials are used to determine if an authentication attempt is valid. If an adversary can obtain an account's hashed credentials, the hash values can then be passed to a system or service to authenticate, without needing to brute-force the hashes to obtain their cleartext values. Successful Pass The Hash attacks result in the adversary fully authenticating as the targeted account, which can further allow the adversary to laterally move within the network, impersonate a legitimate user, and/or download/install malware to systems within the domain. This technique can be performed against any operating system that leverages the LM or NTLM protocols even if the operating system is not Windows-based, since these systems/accounts may still authenticate to a Windows domain.

Likelihood Of Attack

Typical Severity

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

This table shows the views that this attack pattern belongs to and top level categories within that view.

Execution Flow

Explore

1. **Acquire known Windows credential hash value pairs:** The adversary must obtain known Windows credential hash value pairs of accounts that exist on the domain.

Techniques

An adversary purchases breached Windows credential hash value pairs from the dark web.
An adversary conducts a sniffing attack to steal Windows credential hash value pairs as they are transmitted.
An adversary gains access to a Windows domain system/files and exfiltrates Windows credential hash value pairs.
An adversary examines outward-facing configuration and properties files to discover hardcoded Windows credential hash value pairs.

Experiment

1. **Attempt domain authentication:** Try each Windows credential hash value pair until the target grants access.

Techniques
Manually or automatically enter each Windows credential hash value pair through the target's interface.

Exploit

1. **Impersonate:** An adversary can use successful experiments or authentications to impersonate an authorized user or system, or to laterally move within the domain
2. **Spoofing:** Malicious data can be injected into the target system or into other systems on the domain. The adversary can also pose as a legitimate domain user to perform social engineering attacks.
3. **Data Exfiltration:** The adversary can obtain sensitive data contained within domain systems or applications.

Prerequisites

The system/application is connected to the Windows domain.
The system/application leverages the Lan Man (LM) and/or NT Lan Man (NTLM) authentication protocols.
The adversary possesses known Windows credential hash value pairs that exist on the target domain.

Skills Required

[Level: Low]

Once an adversary obtains a known Windows credential hash value pair, leveraging it is trivial.

Resources Required

A list of known Window credential hash value pairs for the targeted domain.

Indicators

Authentication attempts use credentials that have been used previously by the account in question.
Authentication attempts are originating from IP addresses or locations that are inconsistent with the user's normal IP addresses or locations.
Data is being transferred and/or removed from systems/applications within the network.
Suspicious or Malicious software is downloaded/installed on systems within the domain.
Messages from a legitimate user appear to contain suspicious links or communications not consistent with the user's normal behavior.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	**Impact**	**Likelihood**
Confidentiality Access Control Authentication	Gain Privileges	
Confidentiality Authorization	Read Data	
Integrity	Modify Data	

Mitigations

Prevent the use of Lan Man and NT Lan Man authentication on severs and apply patch KB2871997 to Windows 7 and higher systems.

Leverage multi-factor authentication for all authentication services and prior to granting an entity access to the domain network.
Monitor system and domain logs for abnormal credential access.
Create a strong password policy and ensure that your system enforces this policy.
Leverage system penetration testing and other defense in depth methods to determine vulnerable systems within a domain.

Example Instances

Adversaries exploited the Zoom video conferencing application during the 2020 COVID-19 pandemic to exfiltrate Windows domain credential hash value pairs from a target system. The attack entailed sending Universal Naming Convention (UNC) paths within the Zoom chat window of an unprotected Zoom call. If the victim clicked on the link, their Windows usernames and the corresponding Net-NTLM-v2 hashes were sent to the address contained in the link. The adversary was then able to infiltrate and laterally move within the Windows domain by passing the acquired credentials to shared network resources. This further provided adversaries with access to Outlook servers and network storage devices. [REF-575]
Operation Soft Cell, which has been underway since at least 2012, leveraged a modified Mimikatz that dumped NTLM hashes. The acquired hashes were then used to authenticate to other systems within the network via Pass The Hash attacks. [REF-580]

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping

Entry ID	Entry Name
1550.002	Use Alternate Authentication Material:Pass The Hash

References

Content History

Submissions		
Submission Date	**Submitter**	**Organization**

2018-07-31 (Version 2.12)	CAPEC Content Team	
Modifications		
Modification Date	**Modifier**	**Organization**
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Consequences, Description, Example_Instances, Execution_Flow, Indicators, Likelihood_Of_Attack, Mitigations, Prerequisites, References, Related_Attack_Patterns, Related_Weaknesses, Resources_Required, Skills_Required, Taxonomy_Mappings	
2022-02-22 (Version 3.7)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Extended_Description	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Description	

More information is available — Please select a different filter.
