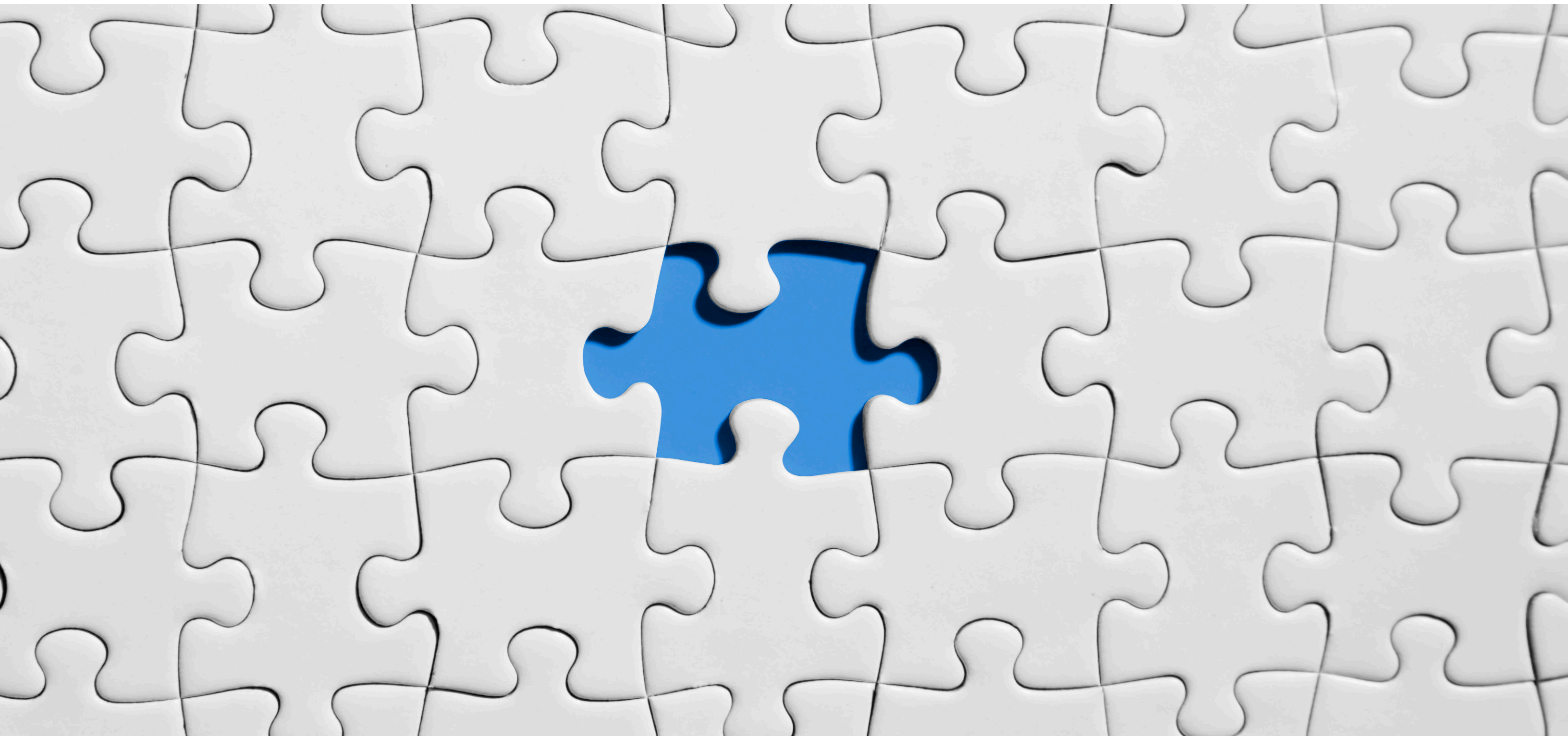
PASS THE HASH



Nikhil Gowda

Dell Technologies

Nikhil.gowdag@Dell.com

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world’s most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Hash....................4

Pass the Hash....................4

Mitigations....................7

References....................7

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Hash

Before understanding Pass the Hash we'd like to understand about the Hash. once we logon to any kind of operating system and enters the username and password, The password isn't actually sent over the network instead the Hash of the password is generated. Hash could be a fixed length mathematical code which springs from the password and which may uniquely represent the password but can't be mathematically reversed or revealed what the password is.

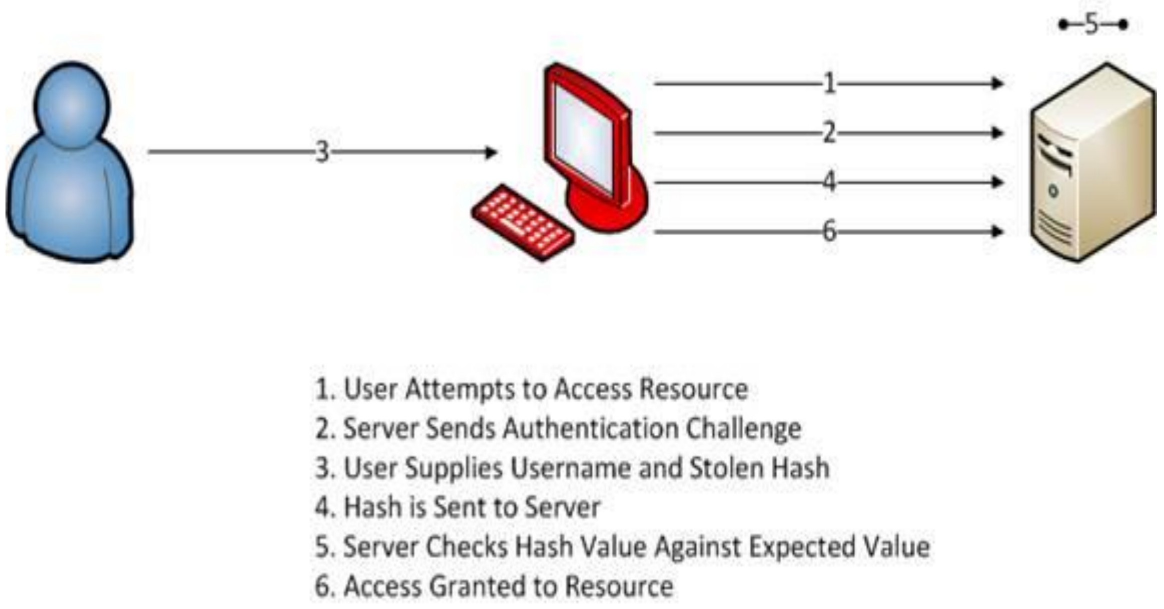
Pass the Hash

Pass the Hash is a Credential theft technique attackers use to impersonate users. Once credentials are obtained, attackers use them to infiltrate and take over the entire network. Passwords are the most commonly used security today. Strong passwords are perhaps the most significant aspect of data security; conversely, weak passwords lead to security failures.

Attackers authenticate to the remote server and repair using the underlying NTLM and LAN and hash of the user's passwords, rather than requiring the user's password as is normally the case.

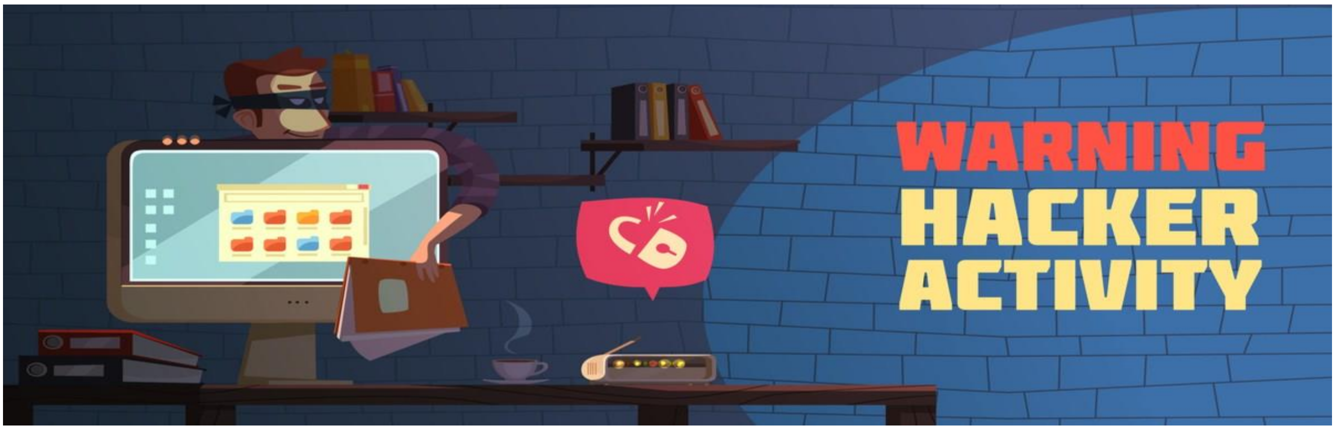
After the attacker obtains the valid user name and password hash values – somehow using different methods and tools – they're able to apply the user's information to authenticate to the remote server or service without brute force to the hash to get the code or password (since it was required before this system was published.)

Pass the Hash attack exploits an implementation weakness within the authentication protocol where password Hash remain static from session to session until the password modification is completed. this system is often performed on any server, system and repair except in LM and NT authentication. Whether it runs on the machine with windows, IOS, Linus or the other OS. On systems or services using NTLM authentication, users' passwords are never over the network instead they're provided to the requesting system sort of a domain controller as a Hash as a response to challenge response authentication scheme.



1. User Attempts to Access Resource
2. Server Sends Authentication Challenge
3. User Supplies Username and Stolen Hash
4. Hash is Sent to Server
5. Server Checks Hash Value Against Expected Value
6. Access Granted to Resource

The attack exploits the



implementation weakness within the authentication technique or protocol where the password hash remain codex from session to session until the password is next changed.

This system is often performed with any servers or service accepting LM or NTLM authentication whether it runs on the machine with Windows, Unix, or another OS. On system or the service using NTLM, authentication users' passwords are never sent as a code over the wire. Instead they're provided to the requesting system like domain controller.

Native windows application asks users for the password then that is converted to at least one or two hash values (NT or LM) during NTLM authentication. The analysis of this mechanism show that the password isn't required to finish network authentication successfully, only the hashes are needed. But the knowledge of this attack and its severity remains poor.

Password attacks like password guessing, or password cracking are time-consuming attacks. Tools that create use of precomputed hashes greatly reduce the time needed to get a password. In Pass the Hash technique, the goal is to use the hash directly without cracking it. Analysis of this mechanism have shown that this whole code or password isn't required for the system or server authentication successfully; only the hashes are needed. If an attacker has the hashes of the user's password, They will simply use the arbitrary user account that they harvest and execute channel attack to authenticate against the remote system. In other words, from an attacker perspective, hash is functionally like the code to the password that the users have generated.

Pass the Hash technique was originally published by Paul Ashton in 1997 and consisted of modified TLM and SMB client protocols which uses Hash rather than the code or password. Later versions of SAMBA and other third-party implementations of SMB and NTLM protocol also included the functionality. Implementation of the technique was supported in the SMB stack created by the third party, i.e. SAMBA et al.

SMB protocols have evolved over the years. This suggests that the third party is creating their own implementation of the SMB protocol where they get to implement changes and additions to the protocols after they are introduced by newer versions of Windows and SMB by reverse engineering.

This is extremely complex and time consuming, even after performing NTLM authentication successfully using Pass the Hash technique, Tools like SAMBA and SMB client not like implemented the functionality which the attacker might want to use.

This meant that it's difficult to connect the Windows programs to use Comm or RPC. Also, since the attackers are restricted to use third party clients when carrying the attacks, it was out of the question to use built-in Windows applications because they ask the attackers to enter the codex and password to authenticate and not the Hash value.

In 2008 Harnin published the tool called the Pass the Hash carpenter's kit which enabled Pass the Hash to be preferred natively on Windows. It asks for the username and password for the user to access the system and therefore the hash memory can be taken care of by the local authority.

The tools also introduced the new technique for jumping password hashes cache within the memory of the system not on the disk storage. This became widely utilized by the penetration testers and attackers. The Hash Harvesting technique is more advanced than previously used techniques. i.e. dumping the local security managers database, SAM using dumping similar tools mainly because hash values storage and memory which incorporates credentials of main users and domain administrator. For example, the hash of the authenticated domain users isn't stored consistently, and therefore the local SAM also can be dumped.

The attack is often implemented instantaneously with no requirement for expensive research to carry out the brute force attack. This is used by Windows credential editors which extends the first tools' functionality and OS support. Some antivirus vendors classify them as a minor problem. Before an attacker carries out the attack, the hash of the target user account should first be obtained.

Pass the Hash attack is completed by capturing the password hash then simply pass it through for authentication and potentially gain access to the networked systems. Here, the advantage is that the actor doesn't need to decrypt the hash to get the plain text password. Password hash remains an equivalent until consecutive modification within the password is completed.

There are some tools employed by the attackers to capture he password Hash. One is Mimi Katz, during this one account is compromised and if that account has admin rights on computer or workstation, where the compromising the user account takes place which is where the opposite credentials are restored within the system. One sort of credential is that the NTLM password hash, If the attacker gets the access to the present Hash then they will replay against other machines or the systems within the user's environment to maneuver laterally and elevate their privileges. To mitigate the threat of Pass the Hash attack, the organization should ensure domain controllers can only be accessed from trusted system without internet access. Two factor authentication that used token should be enforced with the principle of least privilege.

Organizations should closely monitor hosts and traffic within their environment and network for suspect activity.

Mitigations

Password policies: This ensures that inbuilt and created local administrator account have complex and unique passwords.

Privileged Account Manager: This limits credential overlap across systems to stop the damage of credential compromise and reduce the adversary’s ability to perform lateral movement between systems.

Update Software: Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts within the local administrator group.

User Account Control: Enable Pass the Hash mitigations to use UAC restrictions to local accounts on network logon.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

Through GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons

User Account Management: Do not allow a domain user to be within the local administrator group on multiple systems.

References

- https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjbgtXntqTnAhXJHzQIHSgrDgQQjRx6BAgBEAQ&url=http%3A%2F%2Ftechgenix.com%2Fdissecting-pass-hash-attack%2F&psig=AOvVaw0duZVxqUmJx69CQrgNlJqk&ust=1580236758885166
- https://en.wikipedia.org/wiki/Pass_the_hash
- https://www.sans.org/reading-room/whitepapers/testing/paper/33283

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.