What is Pass-the-Hash?

The tools and techniques that hackers use to infiltrate an organization are constantly evolving. Yet, credential theft is a consistent concern as compromised credentials make it easier to gain access to an organization’s most critical assets without being noticed.

Pass-the-Hash, an attack technique leveraging stolen credentials, is often used in advanced attacks and represents a significant risk to organizations. This technique involves an attacker stealing account credentials from one computer, and using them to authenticate to other access points in a network. Instead of requiring plaintext passwords, Pass-the-Hash attacks allow the attacker to authenticate using password hashes. A password hash is the value that is created when the original password goes through a one-way mathematical function to create the password hash for secure storage.

Because a Pass-the-Hash attack leverages passwords in the protected hash form, it allows an attacker to impersonate an authenticated user without ever knowing the password in plaintext. Attackers can also reuse (pass) the stolen, hashed credentials to other systems and services to gain broader and deeper access. For example, if an attacker gains access to a machine that a domain administrator has logged into, the attacker can steal the domain account credential and access to all the resources, rights, and privileges of that account throughout the domain. This way, attackers can inch their way closer to the domain controller one step at a time.

Therefore, any machine with stored hashes could constitute the first step in the pathway for a Pass-the-Hash attack to reach an organization’s most critical and sensitive data. Stored hashes create vulnerabilities on multiple machines throughout a network. The diagram below shows how a Pass-the-Hash attack can initiate on one machine and easily gain access to the domain controller.

From Machine 1, User 1 has access to Machine 2, Machine 3, Machine 4, and Machine 5. Therefore, an attacker on Machine 1 can pass User 1’s hashed credentials and authenticate to any of these connected machines. The attacker will look for other hashes that will enable them to jump from machine to machine and eventually authenticate to Machine 9, which is the only computer in the diagram that has access to the domain controller. Using a systematic attack, once an attacker has access to one privileged password hash, the entire network can be at risk.

Pass-the-Hash represents a significant threat to organizations because it enables access to the heart of the organization if passwords and their hashes are not properly managed. These attacks enable attackers to navigate a network without being noticed, making them difficult to detect.
Determining Pass-the-Hash Vulnerabilities

The first step in mitigating the risk of Pass-the-Hash attacks is to identify accounts and machines that are vulnerable to these attacks. To gain an accurate picture, CyberArk's Discovery & Audit (CyberArk DNA™) is a standalone, easy to use tool that scans the network and identifies machines that are potentially vulnerable to Pass-the-Hash attacks. The tool addresses the following questions:

- Which machines are vulnerable to Pass-the-Hash?
- How can an attack be carried out in an organization?
- Which accounts can initiate a Pass-the-Hash attack and put the organization at risk?
- Which machines are most at risk and should be mitigated first?
- What is causing machines to be vulnerable and how can risk be reduced?

In addition to Pass-the-Hash vulnerabilities, CyberArk DNA also exposes the magnitude of the privileged account security risk, often the root-cause of audit failures and advanced targeted attacks.

Mitigating Pass-the-Hash Attacks

Pass-the-Hash attacks exploit the fact that password hashes are not salted in Microsoft Windows environments, and therefore remain static until the password is manually changed. Microsoft has recognized this weakness and issued a report that emphasizes the dangers of Pass-the-Hash and elaborates on “Why can’t Microsoft release an update to address this issue?”

In order to execute a Pass-the-Hash attack, an attacker must breach the perimeter and then harvest password hashes. Hash harvesting can be done using a number of different methods including hash/credential dumping from the Security Account Manager (SAM) by anyone who has administrator-level privileges, dumping credentials stored in the memory of the lsass.exe process, and sniffing LM and NTLM challenge-response dialogues between clients and servers.

To mitigate the risk of Pass-the-Hash attacks, organizations should implement a defense-in-depth strategy. In Microsoft's report, two of the primary recommendations for mitigating Pass-the-Hash attacks are to “restrict and protect high privileged domain accounts” and “restrict and protect local accounts with administrative privileges”. In direct alignment with these recommendations, CyberArk solutions deliver a comprehensive suite of privileged account security solutions to protect against Pass-the-Hash attacks.

Best practices for mitigating the risk of Pass-the-Hash

Control and manage the “keys to the kingdom”. CyberArk Enterprise Password Vault® can reduce risk by creating unique passwords for every privileged user and service account and limiting access to only authorized users. This reduces the chance of unauthorized users or attackers gaining access to privileged account hashes and user passwords. Even if an attacker does gain access to a hash, it’s less valuable because each privileged account hash is unique.

Change passwords frequently. Privileged passwords should be rotated as frequently as possible to shorten the window of opportunity in which hashes can be exploited. For example, by using the CyberArk Enterprise Password Vault, passwords can automatically change on a regular schedule, based on the enterprise policy. The CyberArk Privileged Account Security Solution can also enforce “one-time passwords” for mission-critical privileged accounts.

---

Pass-the-Hash

Remove local administrator privileges. CyberArk Endpoint Privilege Manager enables organizations to remove administrative rights from local accounts and enforce least privilege policies. By removing administrative rights from local accounts, even if an attacker compromises the local account, an organization can help prevent an attacker from acquiring the privileges required to harvest the hashes and execute a Pass-the-Hash attack.

Secure privileged sessions. CyberArk Privileged Session Manager® acts as a proxy between the administrator and target machines, which protects privileged account credentials and helps to assure that they will not be leaked to potential vulnerable endpoints. CyberArk Privileged Session Manager prevents privileged credentials from being exposed on endpoints, thus reducing the risk of them being used in a credential theft attack to initiate Pass-the-Hash.

Quickly detect threats. CyberArk Privileged Threat Analytics™ analyzes Kerberos traffic in order to detect in-progress attacks. With targeted threat detection on privileged account activity and critical attack vectors, organizations can be alerted to potential compromises such as credential theft attacks, and quickly respond to threats before they cause significant damage.

Identify and block suspected credential theft attempts. CyberArk Endpoint Privilege Manager controls privileges on the endpoint and contains threats. The solution identifies unknown applications and runs them in restricted mode to limit potential damage. In addition, the solution uses behavioral analytics to block credential theft attempts such as Pass-the-Hash. These critical protection technologies enable organizations to strengthen existing endpoint security.

Summary

Pass-the-Hash is a cyber attack technique that is becoming more common and thus a growing concern for organizations. Understanding and identifying the threat is the first step toward mitigating the risk of Pass-the-Hash attacks. CyberArk’s range of solutions can help organizations identify machines that are vulnerable to Pass-the-Hash attacks and can mitigate the risks of these attacks with Privileged Account Security.

CASE STUDY:
Detect and mitigate the risk of Pass-the-Hash with CyberArk Endpoint Privilege Manager

BEFORE
An organization lacks mature security practices. All employees have access to local administrator accounts on their workstations and for ease of use, they frequently use these accounts. In this situation, attackers could easily gain access to a workstation via phishing and from that one endpoint, harvest domain administrator hashes from the SAM database because they have excessive user privileges.

AFTER
The organization implements CyberArk Endpoint Privilege Manager and virtually eliminates the possibility of attackers successfully harvesting hashes from the organization’s endpoints because they are not able to gain the necessary privileges. By removing local administrator rights, the organization reduces the overall attack surface and mitigates the risk of Pass-the-Hash attacks. In addition to proactively protecting against attacks, Endpoint Privilege Manager also detects and blocks attempted credential theft, helping the organization to block attackers from conducting Pass-the-Hash attacks and gaining unauthorized access.