CYBERARK®

Pass-the-Hash

Solution Brief

What is Pass-the-Hash?

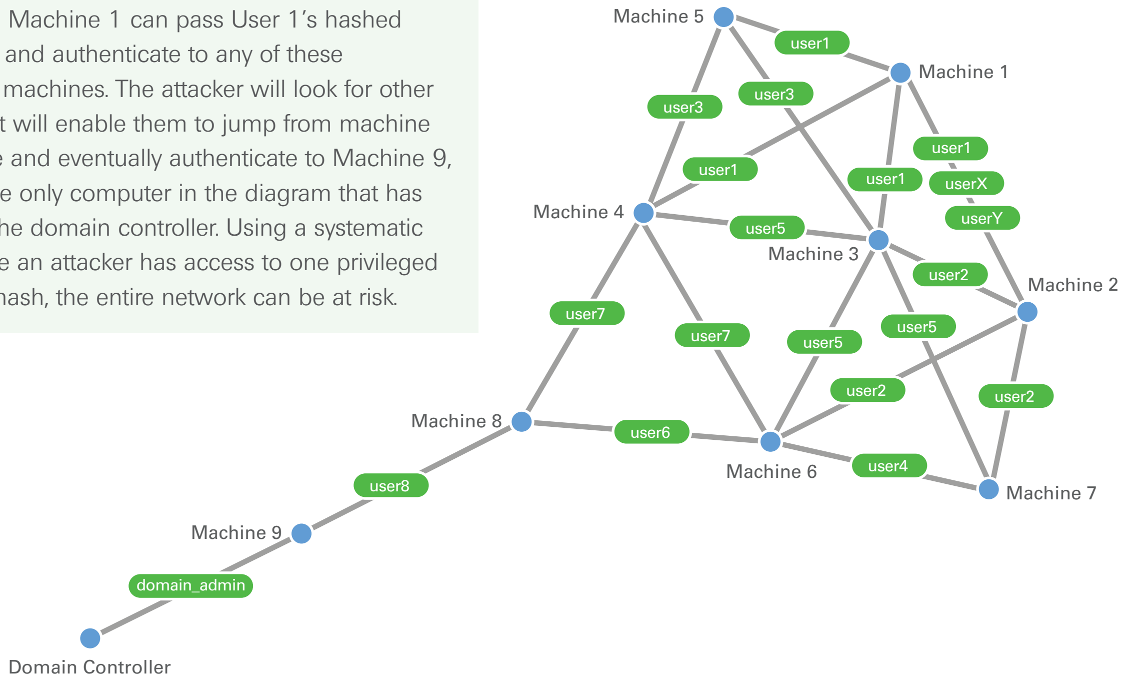
The tools and techniques that hackers use to infiltrate an organization are constantly evolving. Credential theft is a consistent concern as compromised credentials make it easier to gain access to an organization's most critical assets without being noticed.

Pass-the-Hash, an attack leveraging stolen credentials, is often used in advanced threats 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 with password hashes. A password hash is the value that is created when a password is stored. The original password goes through a one-way mathematical function to create the password hash and protect the plaintext credentials.

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 credentials and have access to all the resources, rights, and privileges of that account throughout the domain. This way, attackers can inch their way to the heart of the organization 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. These attacks are able to bypass perimeter security and 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 threat 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 uses patent-pending technology to scan the entire network and identify machines that are currently and potentially vulnerable to Pass-the-Hash attacks. The tool answers 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?

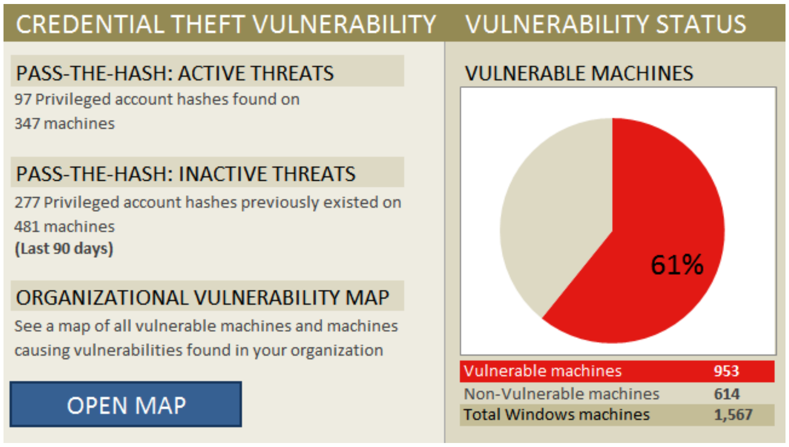
In addition to Pass-the-Hash vulnerabilities, CyberArk DNA also exposes the magnitude of the privileged account security risk, often the root-cause of audit failures and advanced targeted attacks. It is an innovative discovery and audit tool that automatically scans an organization's network for the following:

- Privileged account focused data
- Potential credential theft vulnerabilities

Once the scan is complete, auditors and security managers receive a detailed report into the status of privileged accounts, highlighting the relevant compliance and vulnerability information of each privileged account.

The DNA Report

The DNA report provides comprehensive and detailed machine and account information and the organization's vulnerability status to Pass-the-Hash attacks. For Pass-the-Hash, the report includes a simple Executive Summary Dashboard that provides a comprehensive view of current credential theft vulnerabilities.



CREDENTIAL THEFT VULNERABILITY

PASS-THE-HASH: ACTIVE THREATS
97 Privileged account hashes found on 347 machines

PASS-THE-HASH: INACTIVE THREATS
277 Privileged account hashes previously existed on 481 machines
(Last 90 days)

ORGANIZATIONAL VULNERABILITY MAP
See a map of all vulnerable machines and machines causing vulnerabilities found in your organization

VULNERABILITY STATUS

VULNERABLE MACHINES

Vulnerable machines	**953**
Non-Vulnerable machines	**614**
Total Windows machines	**1,567**

(Example Pass-the-Hash Vulnerability Report)

Mitigating Pass-the-Hash Attacks

Pass-the-Hash attacks exploit an inherent weakness in Microsoft Windows that password hashes are not salted, 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?"[1]

In the report, Microsoft's 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 delivers 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 include:

- **Control and manage the "keys to the kingdom".** CyberArk Enterprise Password Vault® can reduce risk by creating unique passwords for every privilege user and service account, limiting access to authorized users. This reduces the chance of unauthorized users or attackers gaining access to privileged account hashes and user passwords.
- **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 automatically change on a regular schedule, based on the enterprise policy. The CyberArk privileged account security solution can also use "one-time passwords" for mission-critical privileged accounts.
- **Implement and enforce a "least-privilege" security strategy.** CyberArk On-Demand Privileges Manager™ enforces the reduction of administrative rights from the end user by enabling on-demand rights elevation. This makes it difficult for an attacker to steal a hash because it prevents users from having excessive admin rights on their local systems.
- **Isolate privileged sessions.** CyberArk Privileged Session Manager® acts as a proxy between the administrator and target machines, which protects privileged account credentials and assures that they will never be leaked to potential vulnerable endpoints. Privileged Session Manager prevents privileged credentials from being exposed on endpoints, thus reducing the risk of them being used in a credential theft attack.

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 identify machines that are vulnerable to Pass-the-Hash attacks and can proactively secure against such threats before attacks can escalate and do irreparable damage.

[1] "Mitigating Pass-the-Hash (PtH) and Other Credential Theft Techniques", http://www.microsoft.com/en-us/download/details.aspx?id=36036

CYBERARK®

All rights reserved. This document contains information and ideas, which are proprietary to Cyber-Ark Software Ltd.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of Cyber-Ark Software Ltd.

© 2000-2014 by Cyber-Ark® Software Ltd. All rights reserved.