Understanding Pass-the-Hash (PtH) Attacks…and Mitigating the Risk

Explore this Evolving Threat and the Dell Software Solutions that Can Help Protect Your Organization

Abstract

Even though the pass-the-hash (PtH) attack was originally published by Paul Ashton in 1997 and several white papers and tech briefs have been written on the topic[1], these types of attacks have recently come to the forefront again. Given this reality, organizations need advanced solutions that can help protect them. After providing a quick overview of what a hash is and how PtH attacks work, this paper discusses the mitigation strategies recommended by Microsoft and the National Security Agency (NSA), and explains how two solutions from Dell Software can help your organization implement those mitigations.

Introduction

What is a hash?

Before we can explore the pass-the-hash attack, it's essential to define a hash. For each user and administrator account on a system, the operating system stores the username and a password in order to perform authentication. However, instead of storing the password in clear text, the operating system uses cryptographic hash functions to create a hash value that it stores instead.

When a user tries to authenticate to the system, the system takes the password input by the user, computes its hash value and compares the computed hash against the stored hash. If the hashes match, then the user is allowed access to the system.

All of the hash values used to log on to a computer are stored in the Security Account Manager (SAM) file on that computer. This includes hash values for the user accounts, the administrator account, and any other account that has been used to log on to other systems from that computer.

[1]*For instance, one useful paper is "Pass-the-hash attacks: Tools and Mitigation" from the SANS Institute.*

Privileged Password Manager automates, controls and secures the entire process of granting privileged access.

What is a PtH attack?

In a PtH attack, an attacker gains access to a user's local administrative hash and then tries to use the hashes compromised from that system to authenticate to other systems on the network, potentially gaining access to additional hashes along the way. The attacker then continues this lateral movement of compromising different systems within the network, gaining more hashes on each compromised system. The ultimate goal is to gain access to a privileged domain account that can be used to access critical servers and data.

How a PtH attack works

Several requirements must be met in order for a PtH attack to be successful. Fundamentally, a PtH attack relies on three main factors: the ability to gain administrative rights on the system storing the needed hashes, use of the same password on multiple systems, and administrative passwords that are rarely changed.

- **The ability to gain local administrative access** — An external attacker can gain local administrative access to a computer by exploiting a vulnerability on the system, by enticing a user into executing malicious code or through other techniques.
- **Common administrative passwords** — Using the same password for multiple administrative accounts is a common practice for two reasons. First, when systems are deployed in an enterprise network, a base image is created for both a workstation and a server, and that image is then used for every workstation or server that is deployed. As a result, all of the standard administrative accounts within the image — and their passwords — are propagated to every workstation or server deployed on the network. Second, changing the password for each device would introduce management complexities, including the challenges of maintaining a record of each different password in a secure place and enabling IT staff to access those passwords when needed.
- **Static passwords** — Because most organizations have a large number of both local and server administrative accounts and many people need access to them regularly, they often keep the administrative passwords the same, changing them only if someone in IT leaves the organization. And even in that case, they might change only the passwords for the servers and not those for each individual workstation.

Mitigating a PtH attack

There is no single action an organization can take to prevent a PtH attack. Both Microsoft and the NSA recommend the "Defense-in-Depth" approach — they advise organizations to restrict and protect local and domain administrative accounts through such techniques as creating unique local administrative passwords and implementing least-privileged access. In addition, they both recommend restricting inbound traffic and lateral movement on the network with firewall rules.

Dell Software solutions for mitigating risk

Dell Software solutions can help you implement the mitigations recommended by Microsoft and the NSA. This is achieved by restricting and protecting administrative tasks based on a two-pronged approach: implement a privilege safe with Privileged Password Manager, and implement least-privileged access and monitor use of privileged credentials using Privileged Session Manager.

Privileged Password Manager

Privileged Password Manager automates, controls and secures the entire process of granting privileged access. This is done whether the process is for the local administrative password on a workstation, a domain or admin account on a server, or even the administrative password on network devices or within applications. Privileged Password Manager ensures that access to privileged credentials is granted according to established policy and with

appropriate approvals, that all actions are fully audited and tracked, and that the password is changed immediately upon its return.

Privileged Password Manager is also designed to deal with the passwords that are often hard-coded into applications. There may be dozens or hundreds of administrators who have, over time, learned those hard-coded passwords — an obvious security risk. Dell eliminates the need for hardcoded passwords; instead applications and databases are configured to make runtime calls to Privileged Password Manager. With this approach, nobody knows the application passwords, and the passwords can be changed, rather than being locked into scripts, mitigating security and compliance risks.

Privileged Session Manager

Privileged Session Manager enables you to issue access to privileged credentials for a specified time or session. In addition, you can limit access to only specific commands to ensure least-privileged access. Since Privileged Session Manager only provides proxy access to the target, no hashes are stored on the administrator's workstation.

In addition to logging keystrokes and specific commands, Privileged Session Manager enables managers to record and monitor all activity performed using privileged credentials. They can watch over things as they happen on the screen and play back recorded sessions after the fact, whether the session was on Unix, Windows, Active Directory, Web applications, databases, devices or mainframes. And they can even remotely kill a session or revoke access, if needed.

Privileged Session Manager provides an extra layer of accountability and visibility, Plus, its forensics-ready recording and playback of privileged access sessions helps organizations with both compliance and troubleshooting.

Conclusion

Pass-the-hash attacks continue to pose a serious risk for organizations. By gaining access to a user's local administrative hash and moving through other systems throughout the network, an attacker can gain access to a privileged domain account and use it to access critical servers and data.

Privileged Password Manager and Privileged Session Manager can help your organization mitigate these risks by:

- Securing the process of granting privileged access
- Eliminating the need for hard-coded passwords in applications
- Enabling least-privileged access
- Ensuring accountability through forensics-ready recording and playback of privileged access sessions

Although pass-the-hash attacks have been around a long time, they are on the rise again. These Dell Software solutions can help your organization take the right steps to mitigate your risk.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

In addition to logging keystrokes and specific commands, Privileged Session Manager enables managers to record and monitor all activity performed using privileged credentials.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.