400 Totten Pond Road ▸ Waltham, MA 02451 ▸ 781.810.4320 ▸ www.viewfinity.com

Viewfinity and Pass-the-Hash

By Alex Shoykhet

TABLE OF CONTENTS

Overview

Pass-the-hash (PtH) is an extremely common method hackers employ to use your own systems against you. Most pass-the-hash attacks are done via human speed attacks, not through automated malware, using a remote human controller (remote shell). Using PtH techniques, an entire domain can be compromised in 6 minutes to 24 hours. If all computers have the same local admin password, then one compromised PC will compromise all PCs. There are several preventive measures that can be used to thwart off a PtH attack – in this paper we'll focus on how removing admin rights from users significantly decreases the ability to use local admin credentials in a PtH attack.

From Wikipedia

"Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM hash of a user's password, instead of requiring the associated plain text password as is normally the case.

After an attacker obtains a valid user name and user password hashes values (somehow, using different methods and tools), he or she is then able to use that information to authenticate to a remote server/ service using LM or NTLM authentication without the need to brute-force the hashes to obtain the clear text password (as it was required before this technique was published). The attack exploits an implementation weakness in the authentication protocol in that the password hashes are not salted, and therefore remain static from session to session until the password is next changed.

This technique can be performed against any server/service accepting LM or NTLM authentication, whether it is running on a machine with Windows, Unix, or any other operating system"

Hash Harvesting

Before an attacker can carry out a pass-the-hash attack, he/she must obtain the password hashes of the target user accounts. To this end, penetration testers/attackers can harvest password hashes using a number of different methods:

- Hashes/credentials can be dumped from the SAM by anyone who has **Administrator-level privileges on a machine. The caching of hashes/credentials can however be disabled by administrators, so this technique does not always work.**
- Dumping the local users account database (SAM). This database only contains user accounts local to the particular machine that was compromised. For example, in a domain environment, the SAM database of a machine will not contain domain users, only users local to that machine that more likely will not be very useful to authenticate to other services on the domain.
- Sniffing LM and NTLM challenge-response dialogues between client and servers, and later brute-forcing captured encrypted hashes (since the hashes obtained in this way are encrypted, it is necessary to perform a brute-force attack to obtain the actual hashes).
- Dumping authenticated users' credentials stored by Windows in the memory of the lsass.exe process. The credentials dumped in this way may include those of domain users/administrators, such as those logged in via RDP. This technique may therefore be used to obtain credentials of user accounts that are not local to the compromised computer, but rather originate from the security domain that the machine is a member of.

Mitigations

The exploit is very difficult to defend against, because there are countless exploits in Windows and applications running on Windows that can be used by an attacker to **elevate their privileges** and then carry out the hash harvesting that facilitates the attack. Furthermore, **it may only require one machine in a Windows domain to not be configured correctly or be missing a security patch for an attacker to find a way in.**

A wide range of penetration testing tools are furthermore available to automate the process of discovering a weakness on a machine.

There is no single defense against the technique, so standard defense in depth practices apply[10] - for example use of firewalls, intrusion prevention systems, 802.1x authentication, IPsec, antivirus software, full disk encryption**, reducing the number of people with elevated privileges**, pro-active security patching etc. Preventing Windows from storing cached credentials may limit attackers to obtaining hashes from memory, which usually means that the target account must be logged into the machine when the attack is executed. Allowing domain administrators to log into systems that may be compromised or untrusted will create a scenario where the administrators' hashes become the targets of attackers; limiting domain administrator logons to trusted domain controllers can therefore limit the opportunities for an attacker. **The principle of least privilege suggests that a least user access (LUA) approach should be taken, in that users should not use accounts with more privileges than necessary to complete the task at hand**.

Viewfinity and pass-the-hash

Viewfinity provides the only solution which offers complete application control features and least user access (LUA) administrative privilege capabilities to protect against pass-the-hash, sophisticated zero-day attacks, malware, and advanced persistent threats. Our next generation application control provides everything needed for whitelisting - from trusted sources and updaters to a cloud-based system which can rank unknown applications, reinforced with managed administrative privileges. Applications not yet classified run in a "greylist mode" and are automatically verified by the industry leading threat detection platforms of PaloAlto, FireEye, Virus Total, and NSRL. Our patent-pending forensics automatically tracks file origins to enable rapid, more conclusive investigations into malware incidents. This fortified approach leads to more secure desktop and server environments, enables high operational IT efficiency via a lower TCO model, and maximizes end user productivity.

The following will outline, step-by-step, how the Viewfinity solution can help mitigate pass-the-hash in a least privileges environment.

1 - Viewfinity monitoring mode

Viewfinity silently monitors all low level activities on desktops and servers and passes this information to the Viewfinity console or to Security Events Management platforms (SIEM) such as Splunk and others for further security analysis and investigation.

In the example below we observe hash harvesting which dumps domain admin hashes from the SAM database and successfully impersonates an admin session through possession of excessive user privileges on a PC/ Server.

```
admin:DMN:13FE51336A20AC8EAAD3B435B51404EE:8895E989934E3B8F39A9F099FD71BFC4
Administrator:DMN:13FE51336A20AC8EAAD3B435B51404EE:8895E989934E3B8F39A9F099FD71BFC4
admin_mike:WIN7GR:13FE51336A20AC8EAAD3B435B51404EE:8895E989934E3B8F39A9F099FD71BFC4
alex:DMN:13FE51336A20AC8EAAD3B435B51404EE:8895E989934E3B8F39A9F099FD71BFC4
WIN7GR$:DMN:00000000000000000000000000000000:8E922CA0C0B96DEFEFFE6B4C368B4803

c:\temp\wce>wce -s Administrator:DMN:13FE51336A20AC8EAAD3B435B51404EE:8895E989934E3B8F39A9F099FD71BFC4
WCE v1.0 (Windows Credentials Editor) - (c) 2010 Amplia Security - by Hernan Ochoa (hernan@ampliasecur
Use -h for help.

Changing NTLM credentials of current logon session (0A216399h) to:
Username: Administrator
domain: DMN
LMHash: 13FE51336A20AC8EAAD3B435B51404EE
NTHash: 8895E989934E3B8F39A9F099FD71BFC4
NTLM credentials successfully changed!
```

Figure 1: Pass-the-hash executed

2 - Investigating the attack using Viewfinity

As a part of our forensics and file inheritance history, Viewfinity monitors the true point of origination of files/ applications. These points of origin can be traced back and identify:

by whom and when an application was introduced into the environment;
from which source an application originated, such as the Internet (including the URL), Network, USB, etc.;
the first user who downloaded and used the malicious software and which action the application performed.

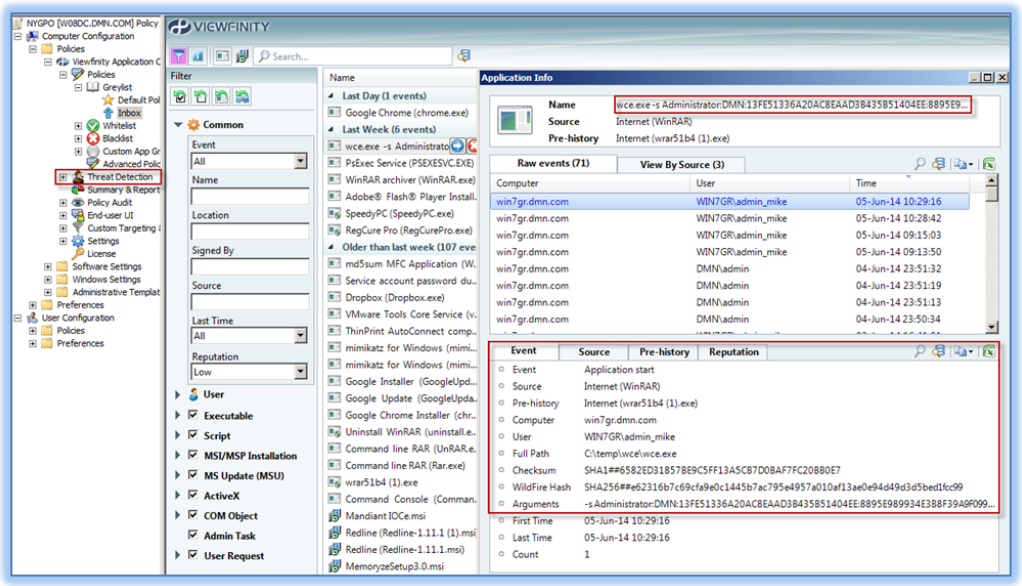


Figure 2: Viewfinity captured pass-the-hash including the origination of tool used for attack

3 - Viewfinity's verification with threat detection platforms

APT attacks like pass-the-hash are verified by Viewfinity by cross-referencing with external threat detection platforms, such as Palo Alto, FireEye, NSRL, and Google Virus Total.

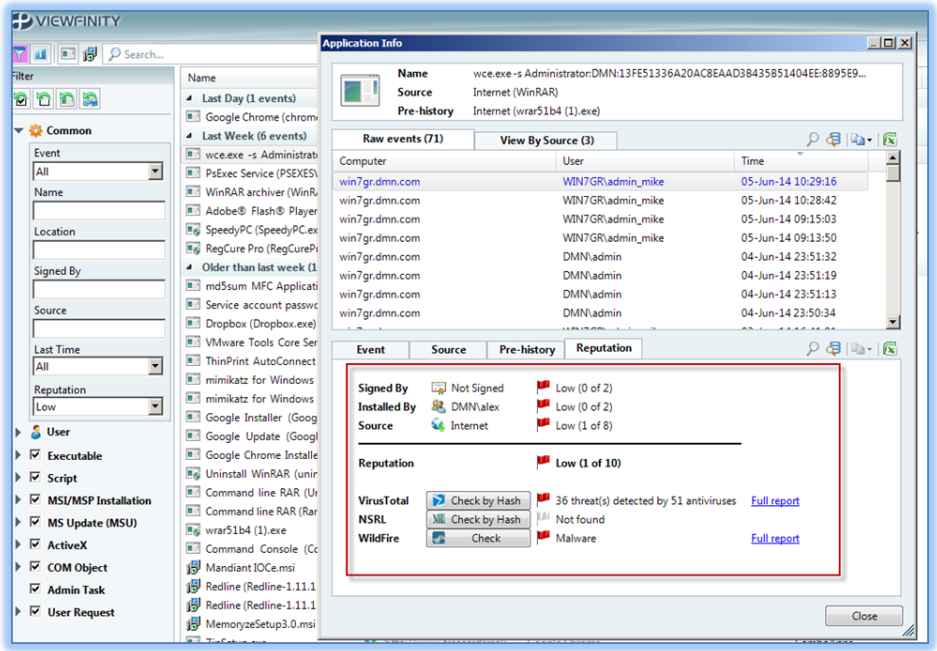
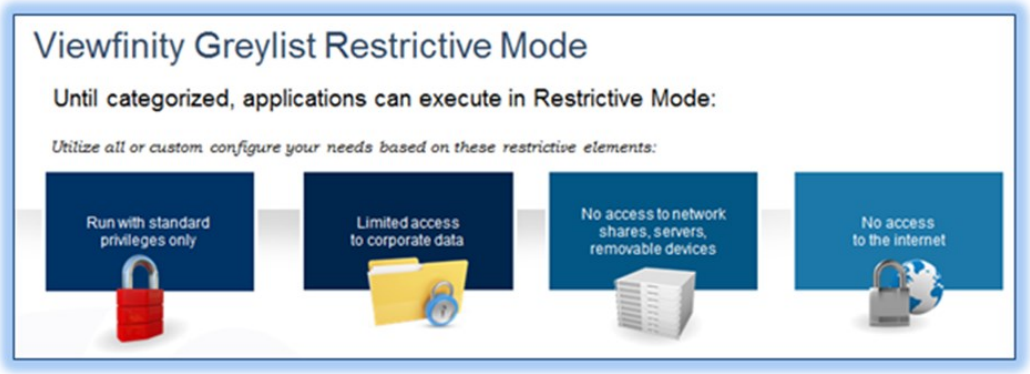


Figure 3: Viewfinity cross-references malicious software with threat detection platforms

4 - Block and restrict malicious and suspect applications

Upon detection and verification with threat detection platforms that an application (or file) is malicious, Viewfinity blocks dangerous events/applications or restricts its access to critical resources (network shares, files, registries).



Viewfinity's "Greylisted" Application Management offers a risk-based application control framework that doesn't necessarily block all unknown applications but instead establishes monitored discovery and restrictive usage behavior for managing the applications not yet classified. These are the applications that are not part of the white or black lists and are allowed to run on the computer but in monitoring, elevated, blocked or isolated mode. Restrictive rules may be set and enforced related to files originating from removable storage devices, local disks, network or Internet downloads.

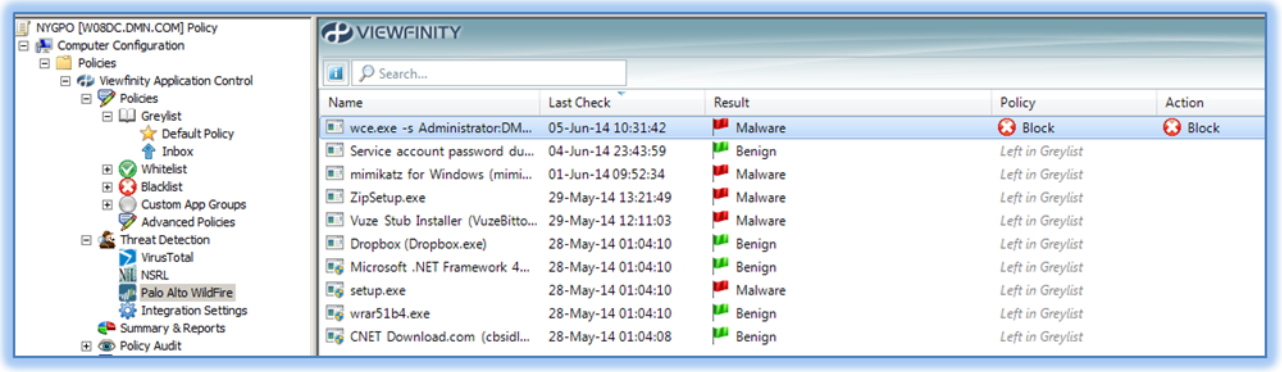


Figure 4: Viewfinity blocks or restricts the usage of unclassified and/or applications verified as malicious

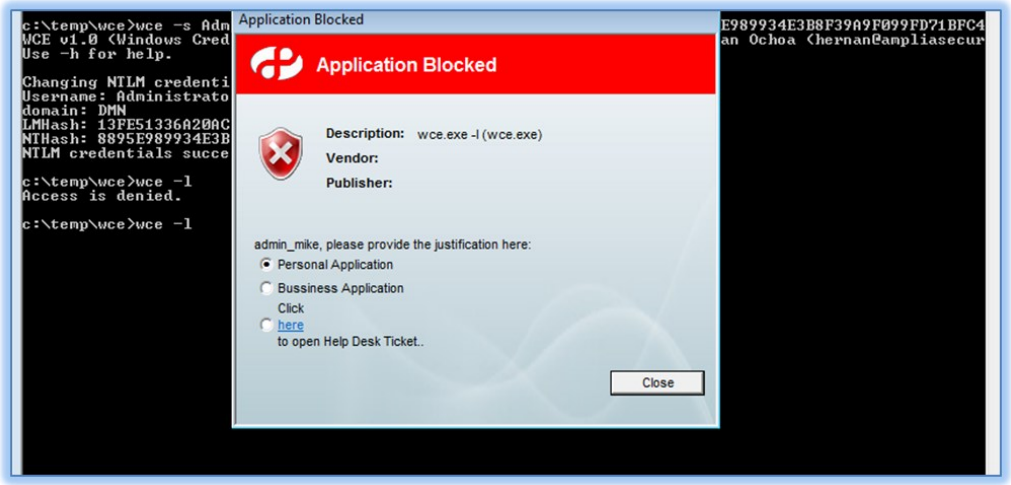


Figure 5: Attacker is blocked from executing the malicious tool

Summary

There are a number of scenarios in which the PtH technique can play itself out. However, one decisive method for deterring and preventing a hacker from using this approach on your systems is to remove administrative rights from your environment. In fact, running more of your Windows users without administrator rights is one of the most important steps a company can take to improve its endpoint security posture. However, the complete removal of administrative rights may trigger conflicts related to end user productivity, causing an increase in calls to IT support to help with privilege elevation needs. Viewfinity Privilege Management eases the burden on IT by managing applications and tasks that require elevated privileges through automated policies. It also addresses many corporate IT security and compliance mandates.

From a centralized management console, for both AD and non-AD computers, Viewfinity controls end user and privileged user rights for applications and systems which require elevated permissions. Viewfinity's granular-level control enables companies to establish and enforce consistent policies for least privilege Windows-based environments based on segregation of duties. For more information, please contact us at info@viewfinity.com.