Group Policy, Lateral Movement & Privileged Access Management

Understand how Windows Group Policy plays a key role in your Windows security posture

By Darren Mar-Elia

CTO & Founder

SDM Software, Inc.

October, 2016

Overview

Today's threat landscape is ever-changing: from ransomware to malware to botnets, there is no shortage of attack vectors to worry about. But as this landscape has evolved, there are steps that we've learned to take to slow down or mitigate the most common attacks. Many of these steps have their foundation in core principles such as "least privilege" administration and basic security "hardening" techniques. And many of these principles, in a Windows environment, can be implemented with the technology that has been the foundation of Windows configuration management for more than 15 years—Group Policy. In this whitepaper, I'll talk about some of these modern threats, how you can protect against them, and how Group Policy, and SDM Software, can help you reduce or eliminate some of the more challenging security risks in today's enterprise environment.

Understanding the Threats—Lateral Movement & Pass the Hash

Over the last two years, Microsoft has provided a couple of whitepapers (https://www.microsoft.com/en-us/download/details.aspx?id=36036) to help explain mitigations for attacks that compromise administrative credentials and access within your network. Indeed, one of the papers starts with the two-word premise, "Assume Compromise." That is, assume that an attacker has compromised an account and gotten onto your network. How do you detect them? How do you contain them? The Microsoft whitepapers describe the exploit known as "Pass the Hash" (PtH), which is based on the fact that user credentials, logged into a Windows server or desktop, can be "mined" using readily available tools like Mimikatz, for their LANManager (LM) hashes, or simply compromised using good old social engineering tactics. An attacker with an LM Hash for a compromised user account can then take that hash and use it to log into other systems where that user has access. If that compromised user account is an administrator, then the attacker has administrative access everywhere that the compromised user does. If that user has broad administrative access within an Active Directory domain, then the attacker can "move laterally" from machine to machine, finding more high-valued targets (think servers with customer account information, employee personal information, etc.).

The discovery of those higher-valued targets can take time. You might think that time is on your side in a sufficiently large and complex network, but that attitude assumes that: a) you will detect the attackers in time, and b) the attackers don't have tools to help them speed their discovery process. To this last point, I created a blog post that describes an open source tool called Bloodhound, that helps an attacker map a path to higher privilege using lateral movement and PtH. This tool essentially shortens the time it takes for the attacker on your network to find those high-valued targets. So hiding behind a large and complex network may not be enough to protect you anymore (and wasn't a good strategy anyway!).

Given these risks, what can you do about it and how can Group Policy help?

Group Policy's Role in Mitigating PtH and Lateral Movement

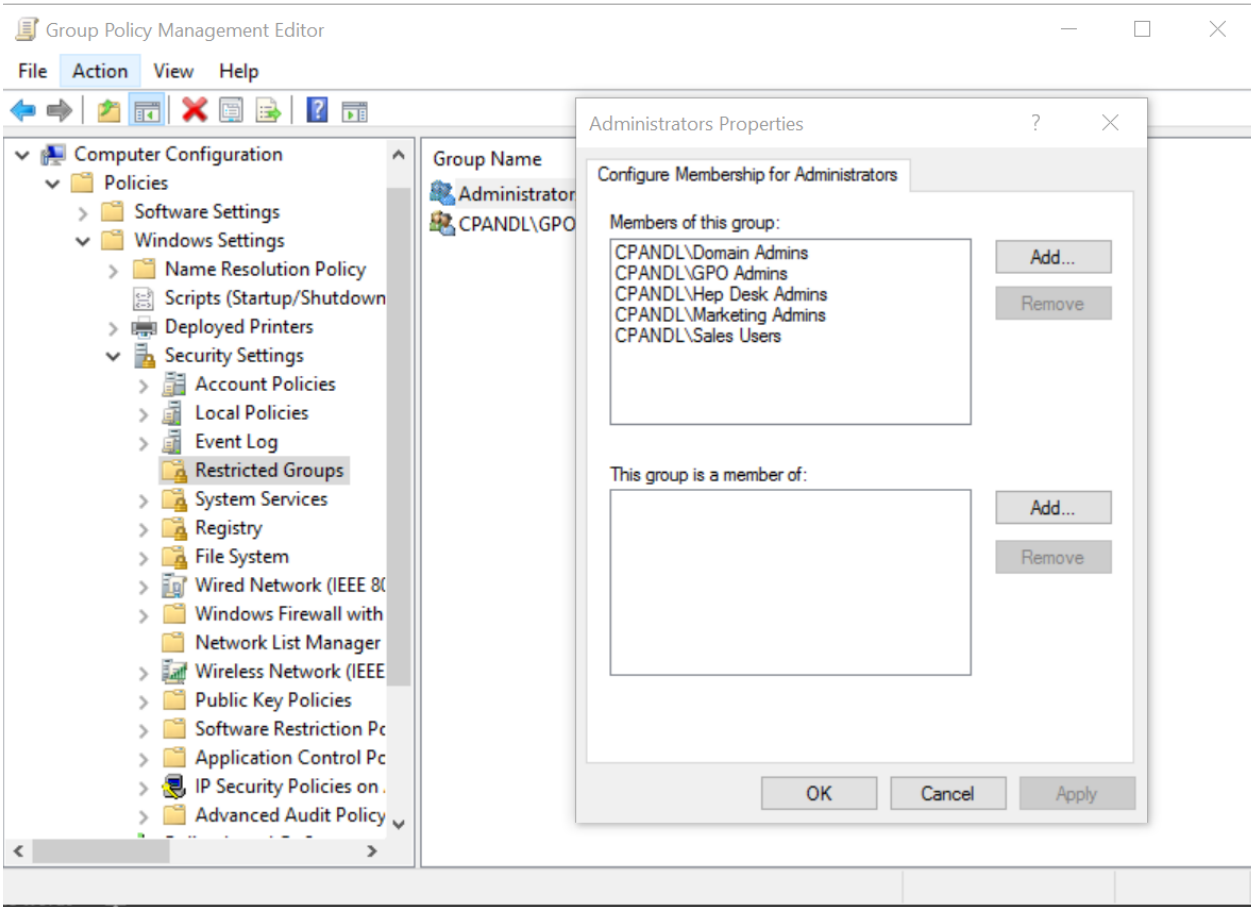
The Microsoft PtH whitepaper talks about a variety of mitigations that you can do to prevent lateral movement by attackers from getting to higher valued targets. These fall into a couple of broad categories, and one that I've added myself below:

1. Separate resources (desktops, servers, Domain Controllers) into **Tiers**, based on the criticality of the data that resides on them. Domain Controllers get a special tier because a compromise of a

domain controller essentially gives an attacker the "keys to the kingdom," because they can access the AD Directory Information Table (DIT).

2. Control which administrative accounts can access which **Tiers** to protect more privileged accounts (e.g. Domain Admins or Server Administrators) from being compromised by logging into less privileged systems (e.g. desktops).
3. Protect the information about how access is granted to prevent attackers from gaining knowledge about your security posture.

Group Policy is used in most organizations, to control both #1 and #2. Specifically, through policies like Restricted Groups (see figure 1), and GP Preferences Local Users and Groups, IT admins can manage the users and groups who have administrative access on your servers and desktops.



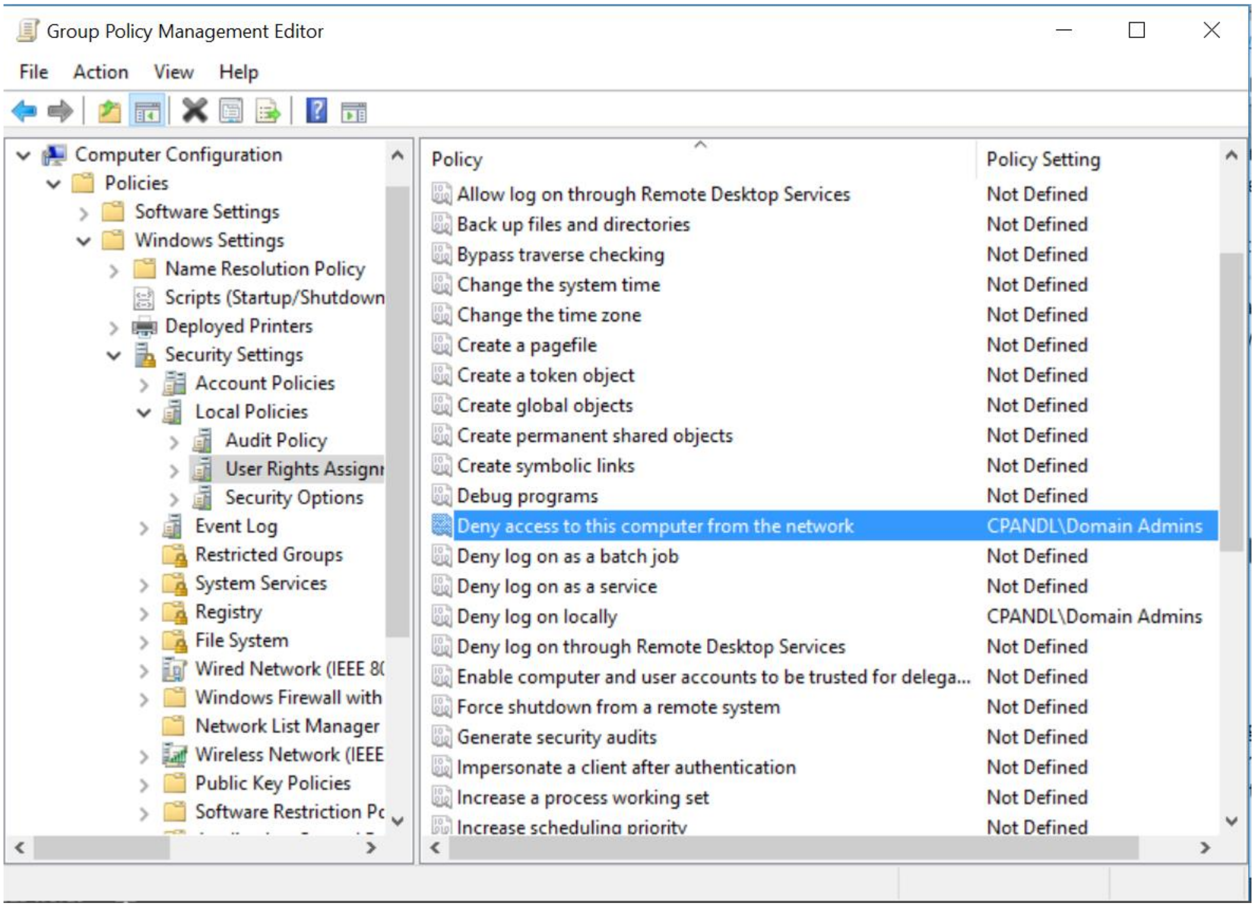
Members of this group:

CPANDL\Domain Admins
CPANDL\GPO Admins
CPANDL\Hep Desk Admins
CPANDL\Marketing Admins
CPANDL\Sales Users

This group is a member of:

Figure 1: Controlling local administrative access with Restricted Groups policy

Using these GP capabilities and Group Policy's inherent ability to target policy settings, you can effectively create the tiers that are discussed above to control which users have administrative access in which groups of servers. The goal, as laid out in the Microsoft paper, is that each tier requires a different administrative ID, and that IDs at higher tier levels are not used to log in to machines at lower tiers. For example, my DC_Darren_Admin account that is a member of the Domain Admins group, should not be allowed to log into a given workstation on the corporate network, let alone be an administrator on that workstation. This control of who can log on where, as specified in #2 above, can also be deployed via Group Policy, using User Rights Assignment policy, as shown in Figure 2. You can set "Deny log on locally” and “Deny access to this computer from the network” rights to higher tiered administrative groups, and then apply those policies to lower tiered workstations, to prevent the crossing of tiers that can leave you vulnerable.



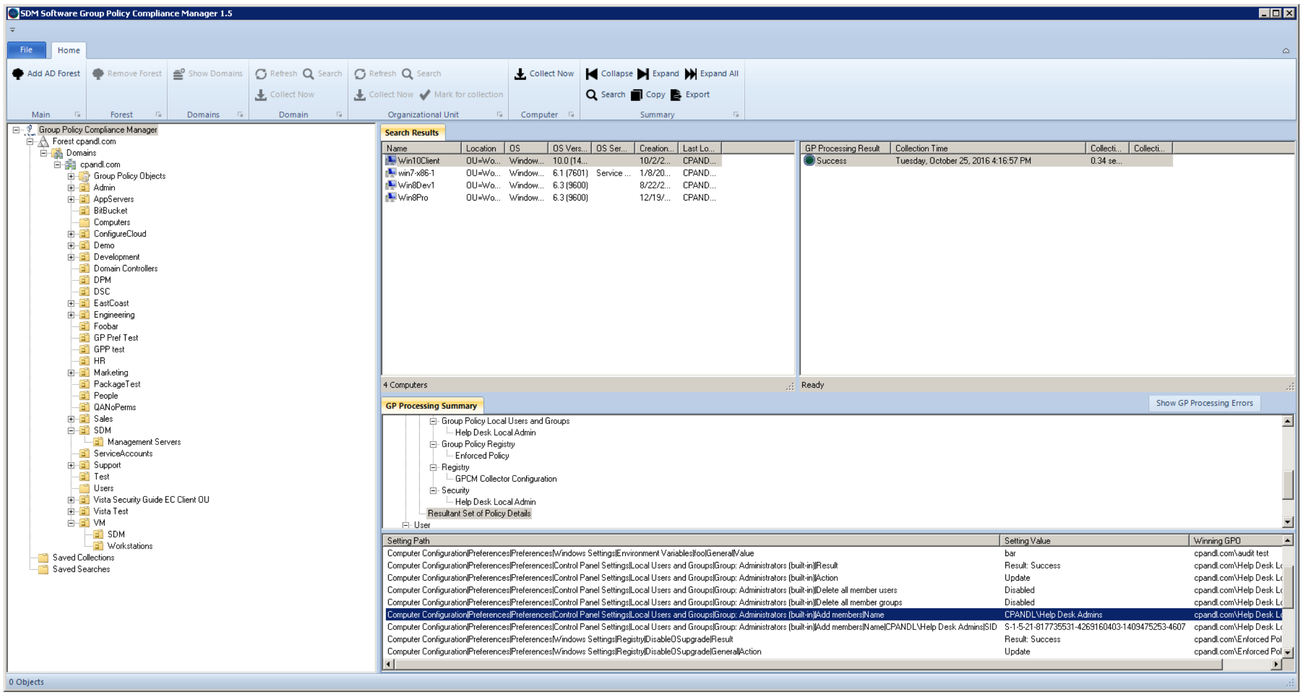
Policy	Policy Setting
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	CPANDL\Domain Admins
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	CPANDL\Domain Admins
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined

Figure 2: Using User Rights Assignment policy to control who can log on where.

For the 3rd item in the list above, controlling how discoverable your security posture is to a would-be attacker, if you are using Group Policy to control numbers 1 & 2, then you will want to ensure that Group Policy can’t be used against you, by delegating read access to those GPOs that grant these group memberships and user rights. I wrote about this topic in the blog post I referenced above, specifically in the section entitled **GPO Discoverability**. The gist of this is that you should remove Authenticated Users Read Access from all GPOs that perform Restricted Groups, GPP Local Users and Groups and User Rights Assignment policy and, ideally, only allow the machine accounts that need to process these policies, read access to the GPOs.

Assessing Your Current State

Of course, if you are using Group Policy to manage privileged access to your Windows systems, the first step in getting to a model like the one described here, is to assess what you have. Fortunately, SDM Software’s **Group Policy Compliance Manager** **(GPCM)** has the ability to ask questions of your existing servers and desktops, to find out where administrative group membership or User Rights Assignment has been deployed across your environment—making it easier to determine who has administrative access to what. In Figure 3, you can see how, using GPCM, you can search for particular administrative policy, and find all the machines that have implemented that across your AD infrastructure:



Name	Location	OS	OS Vers...	OS Ser...	Creation...	Last Lo...
Win10Client	OU=Wo...	Window...	10.0 (14...		10/2/2...	CPAND...
win7-x86-1	OU=Wo...	Window...	6.1 (7601)	Service ...	1/8/20...	CPAND...
Win8Dev1	OU=Wo...	Window...	6.3 (9600)		8/22/2...	CPAND...
Win8Pro	OU=Wo...	Window...	6.3 (9600)		12/19/...	CPAND...

GP Processing Result	Collection Time	Collecti...	Collecti...
Success	Tuesday, October 25, 2016 4:16:57 PM	0.34 se...	

Setting Path	Setting Value	Winning GPO
Computer Configuration|Preferences|Preferences|Windows Settings|Environment Variables|foo|General|Value	bar	cpandl.com\audit test
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Result	Result: Success	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Action	Update	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Delete all member users	Disabled	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Delete all member groups	Disabled	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Add members|Name	CPANDL\Help Desk Admins	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Control Panel Settings|Local Users and Groups|Group: Administrators (built-in)|Add members|Name|CPANDL\Help Desk Admins|SID	S-1-5-21-817735531-4269160403-1409475253-4607	cpandl.com\Help Desk Lo
Computer Configuration|Preferences|Preferences|Windows Settings|Registry|DisableOSupgrade|Result	Result: Success	cpandl.com\Enforced Pol
Computer Configuration|Preferences|Preferences|Windows Settings|Registry|DisableOSupgrade|General|Action	Update	cpandl.com\Enforced Pol

Figure 3: Using SDM Software's GPCM to find where administrative access has been granted.

You can likewise find out which groups have been granted User Rights Assignments on which machines within your environment. Armed with this information, it becomes easier to organize your administrative access into the tiers described above—and to get to a model of controlled privileged access that can keep any would-be attackers from moving laterally at-will within your network.

Summary

Group Policy plays a key role in both the protection against, and the enabling of, lateral movement and Pass-the-Hash style attacks. You can either use it to protect yourself, or cause more harm. At SDM Software, we believe Group Policy is a powerful protection mechanism against would-be attackers, when properly deployed and managed. Our Group Policy solutions like the Group Policy Compliance Manager, our GPO Reporting Pak and our GP Automation Engine, can help you get to a secure and protected network. For more information on how SDM Software can help with **your** security posture and protection against lateral movement, contact us at sales@sdmsoftware.com.