7 Steps of a Cyber Attack, & What You Can do to Protect Your Windows Privileged Accounts

Derek A. Smith, CISSP

TABLE OF CONTENTS

INTRODUCTION

Today, more than 1.2 billion people use Microsoft Office in 140 countries and 107 languages around the world. According to Microsoft, 80% of Fortune 500 companies are now in the Microsoft Azure cloud, and more than 400 million devices are running Windows 10.

Regardless of what your opinions might be regarding how Windows stacks up versus some other product like Linux or Unix— when it comes to security, the point is that you probably use Microsoft products over the course of a workday, and therefore need to know how to protect your privileged Windows accounts.

Whether obtained maliciously or leveraged inappropriately by a valid user, exploited privileged user accounts are now the chief cause of most data breaches. As your environment become more complex, so increases the challenge of defending against ever more sophisticated, and damaging, cyber attacks.

After reading this white paper, you should come away with a better understanding of threats to Windows privileged accounts, the distinct steps (or phases) of an attack lifecycle, how to defend against an attack each step of the way, and how to improve your Windows privileged access management.

WHAT ARE PRIVILEGES?

Before I dive into the why's and how's of Windows privileged account protection, let's review what "privilege" means in a Windows computing environment.

A privilege, as far as computers and networks are concerned, is the right of an account, (such as a user or group account), to perform various system-related operations on your local computer. This includes processes such as shutting down your system, or loading

device drivers. Privileges differ from your normal "access rights" in two significant ways:

1. *While your regular access rights allow you access to your "securable objects" on your computer, the privileged accounts control access to your system resources and system-related tasks.*

2. *A system administrator assigns you user or group privileges while the system itself grants or denies access to a securable object based on your granted access rights.*

Information about your privileges is stored in an account database maintained by the previously mentioned user and group accounts. When you, as a user, log on, the system will issue you an "access token" containing your authorized privileges. When you attempt to perform a privileged operation, the system checks this access token to validate that you have the proper privileges and that they are enabled. If the access token doesn't include the proper privileges, the system will not perform the operation.

TYPES OF PRIVILEGED ACCOUNTS

Now that we've covered the basics of how privileges work and the difference between user and system privileges, let's examine some of the privileged accounts types that you may encounter on a daily basis. Privileged accounts exist in many forms across an enterprise environment, and usually include:

- ***Local Administrative Accounts,*** *which are non-personal accounts that provide administrative access to only the local host or instance used by the IT staff to perform maintenance.*

- ***Privileged User Accounts,*** *which are usually the most frequently used and are named credentials with administrative privileges on one or more systems allowing users administrative rights on the systems they manage.*

- ***Domain Administrative Accounts,*** *which have privileged administrative access across all workstations and servers within the domain.*

- ***Emergency Accounts**, which provide unprivileged users the administrative access that they may need in an emergency / break-glass scenario.*

- ***Service Accounts,** which can be privileged local or domain accounts used by an application or service to interact with the operating system.*

- ***Application Accounts,** which are used by the applications themselves to access databases, run batch jobs or scripts, or provide access to other applications.*

All of these types of accounts present substantial security risks if not properly protected, managed, and monitored. (Here's a blog that details the challenges associated with managing privileges, and common privileged account attacks.)

SHORTCOMINGS OF RELYING ON MANUAL PROCESSES & PEOPLE FOR SECURITY

In Windows, Server Administrators often need to use domain admin (DA) accounts to perform standard administrative tasks. Typically, but not always, organizations rely on Active Directory (AD). Consistent with the security principle of least privilege, AD domain admin accounts should only be used when privilege is required, and not for everyday tasks. Furthermore, in order to ensure accountability and auditability, different users should not share these accounts.

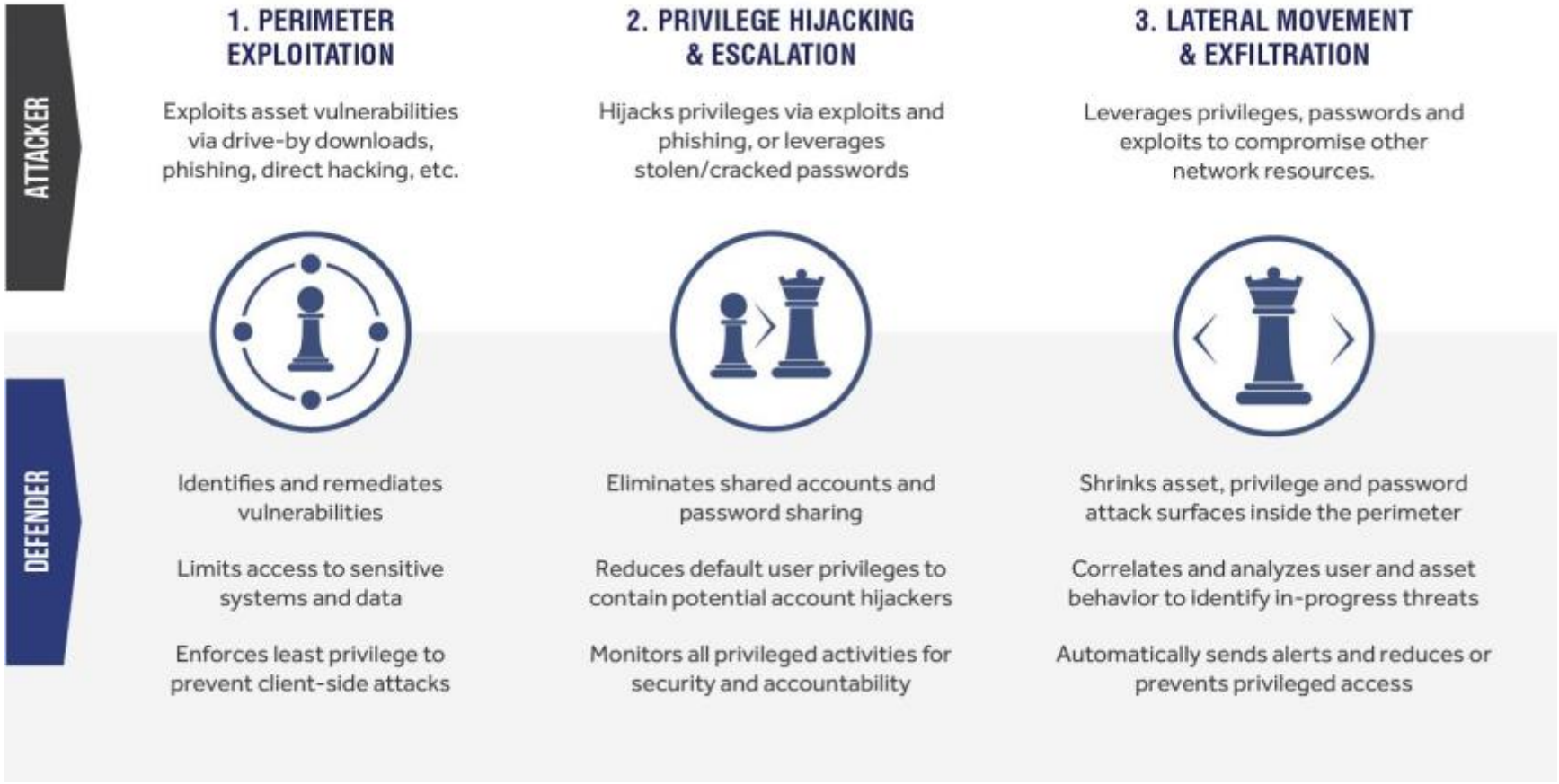
In practice, administrators are often negligent in changing the account passwords, leaving the accounts highly susceptible to "Pass-the-Hash" (PtH) attacks, which involve an attacker using the password hash from a previous domain admin logon to pretend to be that user on other systems. A successful PtH attack of this sort would give the attacker domain admin access across the network.

WHY WINDOWS PRIVILEGED ACCOUNTS ARE IN THE CROSSHAIRS

Today, Windows privileged accounts are routinely exploited, resulting in data breaches, damaged networks/systems, and frequently, leaving organizations susceptible to future exploits as the attackers remains undetected, or has installed rootkits or other malware allowing him/her to easily sneak back in.

Regardless of how an attacker gets into your network—a phishing attack, stolen credentials, malware, etc.—once inside your network, the *modus operandi* is almost invariably to seek out privileged accounts and escalate privileged access. Why is this pathway and behavior so predictable? Simply put, privileged accounts provide attackers with the ability to act as an insider. Since many organizations have inadequate control, auditing, and reporting capabilities over privileged accounts, once with "insider access", attackers can move undetected, even erasing any trail of their activity.

ANATOMY OF AN ATTACK



7 Steps of a Cyber Attack, & What You Can do to Protect Your Windows Privileged Accounts

Let's briefly examine how an attack typically occurs and what happens during the attack. While there are many flavors of attack types, there are several common elements and steps shared by successful cyber-attacks:

1. Reconnaissance

Before launching an attack, hackers first identify a vulnerable target and explore the best ways to exploit it. The attacker is looking for a single point of entry to get started.

2. Scanning

Once the target is identified, the attacker attempts to identify a weak point that allows him or her to gain access. Often, this step progresses slowly as the attacker searches for vulnerabilities.

3. Access and Escalation

Once a weak spot is discovered, the next step is to gain access and then escalate privileges to allow the attacker to move freely within the environment. Once the attacker has access and privileges are escalated, they have effectively taken over your system.

4. Exfiltration

Now that the attacker can freely move around the network, he / she can now access systems with an organization's most sensitive data and take his / her time extracting it.

5. Sustainment

With unrestricted access throughout your network, the attacker seeks to remain undetected for as long as possible by secretly installing

malicious programs, like root kits, that allow the attacker to return as frequently as desired.

6. Assault

This step, while not always part of an attack, is the stage when the hacker might change the functionality of your hardware, or disable it altogether. Once accomplished, the attacker has effectively taken control of your network, making it too late for you to defend yourself.

7. Obfuscation

Usually the attackers want to hide their tracks, but sometimes the bold hacker may want to leave a "calling card" behind to brag about his or her achievements. While doing so, the attacker tries to confuse, disorient, and divert your forensic examination process with log cleaners, spoofing, misinformation, backbone hopping, zombie accounts, Trojan commands, etc.

Today, comprehensive privileged account management is paramount. Access to privileged accounts should be controlled and audited, and passwords must be changed frequently to prevent these types of attacks.

DEFENDING AGAINST THE SEVEN STEPS OF A CYBER ATTACK

So, how do you defend against each of the seven steps of an attack? Well, first realize that hackers can break into almost any network. Mandiant reported that 97% of organizations have been victimized at least once by a breach. Against today's increasingly sophisticated threats, perimeter security tools, like IDS's and firewalls, simply aren't enough.

Controlling access to privileged accounts is the key to blocking the types of sophisticated, cyber-attacks that we often see organizations succumb to today. Recognize that steps four through seven each require privileged credentials to succeed. If you stymie privileged access, you have a good chance of derailing attacks.

There are many ways to secure Windows privileged account access, but we can divide it into two main categories:

1. **Manual Protection** – While better than doing nothing, manually protecting, managing, and monitoring privileged accounts can be a tedious, time-consuming, and resource-draining process. You won't be able to maintain proper security with manual processes, so I don't recommend this route.

2. **Privileged Account Management,** also called privileged access management, (PAM) solutions - Mid and large-size organizations will find it is more efficient, and ultimately more effective, to purchase and manage their own privileged account security solution, or contract with a partner who provides managed services for a solution. Partnering with a PAM expert and integrating with existing security investments, such as Security Information and Event Management (SIEM) solutions provide the best protection and value for most organizations.

With this in mind, let's now look at three phases of action and protection you need to put in place. The third phase is the most complicated because it recommends the most changes to your established processes for administrative tasks and requires that an organization run more recent -- or current -- versions of Windows Server.

Here is a detailed outline of the actions you may take in each phase:

- *Phase one directives:*
    - *Mitigate the most frequent attack vectors.*
    - *Make a separate administrative account just for administrative tasks and set up dedicated privileged access workstations for Active Directory administrators.*

    - *Implement Privileged Password Management Solutions to generate unique local admin passwords for workstations and servers.*

- *Phase two directives:*
    - *Add visibility into administrative activity and build a wall against common follow-up attacks that target administrator accounts.*
    - *Expand the privileged access workstation concept from Active Directory administrators only to all enterprise admins.*
    - *Turn off additional features, such as Credential Guard and RDP Restricted Administrator groups, to harden these workstations.*
    - *Use time-bound privileges so there is no permanent administrator.*
    - *Turn on multifactor authentication to elevate ordinary accounts to privileged levels and enable Just Enough Administration (JEA) to manage domain controllers.*
    - *Reduce the attack surface on domain controllers and security boundaries overall, and develop methods to detect real-time attacks.*

- *Phase three directives:*
    - *Move into role-based administration and implement models to delegate privilege.*
    - *All administrators will use smartcard or Microsoft Passport authentication.*
    - *Create a separate forest for Active Directory administrators to provide a second security boundary that protects accounts with the highest privilege.*
    - *Using Windows Server 2016, enable code-integrity policies for another layer of malware protection on domain controllers.*
    - *Move virtualized workloads to shielded VMs on the Windows Server 2016 Hyper-V fabric. If a VM is copied, the encryption will prevent data loss.*

CONCLUSION

Securing privileged accounts should be an ongoing process, with continuous monitoring and improvement as your business and threat landscape change. You can try to avoid data breaches alone, but it is much better to automate this process and to rely on a vendor or partner who specializes in PAM to offer you a proven, comprehensive solution.

As you strive to proactively protect and monitor your privileged accounts, keep your business needs in mind while evaluating your available options to determine the best solution for your organization.

ADDITIONAL RESOURCES

2017 Gartner Market Guide for Privileged Access Management (analyst research)

What is Privilege Management and Where Do You Start?

Stop the Evil; Protect the Endpoint (on-demand webinar)

How to Use a Least Privilege Strategy to Balance User Empowerment and Security in a Windows Environment (webinar)

Privileged Password Management Explained (white paper)

Disrupting the Cyber Attack Chain (infographic)

Petya Ransomware Strikes Hard: Be the Master of the Universe (or at least be master of your boot record) (blog)

BeyondTrust Customer Case Study: Transaction Services Group Leverages BeyondTrust to Attack Complexity and Reduce Risk (video)

BeyondTrust PowerBroker Endpoint Least Privilege Solution (data sheet)

ABOUT DEREK A. SMITH

Derek A. Smith is an expert at cybersecurity, cyber forensics, healthcare IT, SCADA security, physical security, investigations, organizational leadership and training. He is currently an IT Program Manager for the Internal Revenue Service and is the former Director of Cybersecurity Initiatives for the National Cybersecurity Institute at Excelsior College. Formerly, he has worked for several IT companies including Computer Sciences Corporation and Booz Allen Hamilton. Derek spent 18 years as a special agent for various government agencies and the military. He has also taught business and IT courses at several universities for over 20 years. Derek has served in the US Navy, Air Force and Army for a total of 24 years. He completed an MBA, MS in IT Information Assurance, Masters in IT Project Management, and a BS in Education.

Website: http://derekallensmith.net/

Twitter: https://twitter.com/DerekASmith1

LinkedIn: https://www.linkedin.com/in/dsmith8952/