PxM PLATFORM

The trouble with Privileged Passwords: Five reasons why separation is essential

osirium.com

OSIRIUM

SECURE • SCALE • SIMPLIFY

v1.0

OSIRIUM

PxM PLATFORM

X = Account, Access, Analytics, User, Task & Session manaagement

The trouble with Privileged Passwords:
Five reasons why separation is essential

Written by **Andy Harris** & **Chris Heslop**
Osirium Chief Technology Officer & Marketing Director

Why Privileged Accounts are a favourite line of attack for hackers...

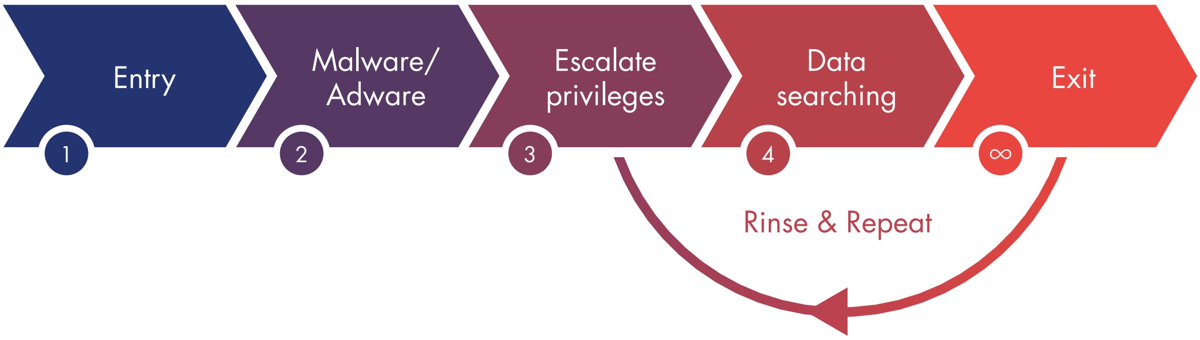
The threat from internal and external cyberattacks continues to evolve. Increasingly, rather than expending efforts breaking into the accounts of users running routine applications, it's the Privileged Accounts that they target.

So one would assume that System Administrators managing the critical infrastructure – the servers, databases, firewalls, routers and switches that the organisation relies on – are protected by a rigorously applied set of security systems, passwords and processes? Five of the common flaws in this premise are what we will explore in this White Paper.

Privileged Access Management: the Trouble with Passwords

Although many organisations have made great steps in devising and implementing rigorous password policies, much remains to be completed to ensure SysAdmin credentials are protected from abuse. According to a survey carried out by Identity Management Solutions, 20% of organisations have never changed their default passwords on Privileged Accounts, and 40% use the same password model for Privileged Accounts as for standard accounts.

For both insider and external attempted security breaches the attackers follow a variety of approaches and seek to exploit a range of vulnerabilities. What they have in common however is that they follow variations on the five key steps outlined below. They (1) effect entry, allowing them to (2) lay Malware that grabs privileged credentials as they pass. From this the attackers can (3) raise their privilege levels and (4) search for key data across the infrastructure, returning over time to repeat this process.



With passwords at the heart of an organisation's security strategy, we therefore look at five password-related issues posing challenges for the security of Privileged Accounts

The compromised workstation

In looking at attacks on Privileged Accounts we see the need for a clear assumption: that workstations are currently compromised, or will be compromised in the future. This situation is the result of a combination of factors.

- According to a study by Verizon, 86% of instances of loss of privileged credentials occur through compromised workstations
- It's also calculated that a new piece of malware for Windows operating systems is written every 0.6 of a second
- Malicious code created ten to twenty years ago tended to be generic in its targeting. Malware today has the functionality to be organisation or even individual-specific.

Time is also a factor. According to research by the Ponemon Institute, once a data breach occurs it takes an average of 98 days for financial services companies to detect intrusion on their networks and an average of 197 days in retail businesses.

For security and compliance reasons therefore, businesses frequently set out policies mandating the regular refresh of passwords. In practice however, complex processes involved in refreshing intricate passwords (such as considerations for shared passwords) means that these credentials may not automatically be refreshed after each use. For this period of time, hackers will therefore be able to monitor, record and abuse privileged passwords.

Phishing attacks: a vault doesn't protect you

The attacker's challenge: how to access a series of highly complex passwords securely lodged in a password vault. Increasingly, phishing is the line of attack used.

- An email or forged service ticket is sent
- Privileged users click on the ticket or link and are presented with a login screen
- The screen appears to be the login for the system the privileged users want to access but is in fact fake
- Users retrieve a password from the vault and inject it into the fake screen, which redirects them to the real system or, more commonly, gives an innocuous error message.

At this point, however, the password has been revealed. The attacker now has a window of opportunity to access the system until such as time as the password is changed.

Alternatively, a more sophisticated version of this line of attack is DNS poisoning, where the IP address of real systems is substituted in an attack system, and all users in the targeted organisation go to the attacker's address where their credentials are captured, before being forwarded to the real system.

The practice of password sharing

Password sharing covers the scenario where multiple privileged users, often including third parties and contractors, know and use a single password. Sharing often applies to apparently minor network elements like switches or routers that multiple SysAdmins need to access. Two factors underline the consequences of password sharing:

1. For systems with 'shared' passwords the issue is frequently a simple factor of conflicting priorities e.g. the effort needed to make the changes to passwords (contacting and informing all the Admins that need to access switches and routers) is outweighed by the need to keep the organisation running without disruption.
2. Shared systems may be considered minor in terms of the strategic data they hold, but are nonetheless important from a security perspective. For example, switches in port-mirroring mode can see and record traffic. Traffic may be encrypted but, should the organisation have instances of weak cryptography, or should an insider attacker have access to private keys, the potential for a serious breach is magnified. Moreover, because this would likely be an invisible attack, the hacker would have time to break the encryption and access the targeted information.

The limits of the human cognitive load

To deter brute forcing and other hacker attacks, organisations frequently deploy complex passwords. Yet herein lies the problem for users as well, leading to password policies creating the opposite effect of their intended outcome.

For example, a security policy may specify the need for passwords to exceed 12 characters, contain both uppercase and lowercase, as well as specific digits and punctuation signs. The policy may also require a change of passwords every 30 days. The inherent complexity of this approach rapidly puts mounting demands on a user's cognitive load. Reviews by Osirium with customers have uncovered a limit of 6 to 7 complex passwords that users can reliably remember over a 12 month period.

In practice what happens is that, in order to be compliant with the policy, users soon adopt recognisable patterns to their passwords. A long word such as 'Liverpool' uses up 9 characters. By extending this to 'LiverpoolFC2018' the requirements for uppercase characters and digits are included. By adding '01#' for January and changing this in February to 'LiverpoolFC201802#', and so on every 30 days, the user is ostensibly compliant with the policy. However, using names of towns, football clubs, names with predictable date patterns becomes easy for a hacker to compute, and the password becomes a liability rather than a strength.

Shoulder surfing

Shoulder surfing is a disconcertingly accurate description for the practice of reading sensitive information over a user's shoulder, with the information typically sought by the shoulder surfer including passwords and PIN numbers. For holders of elevated account privileges, such as SysAdmins, the consequences of this are acute: one well-executed glance (ID typed in, PIN keystrokes entered) and there they have keys to your network in seconds. And as the surfed SysAdmin probably has little awareness of this happening, the resulting breach may not be immediately apparent.

Resolving the Password Challenge with Osirium: Separating People from Passwords

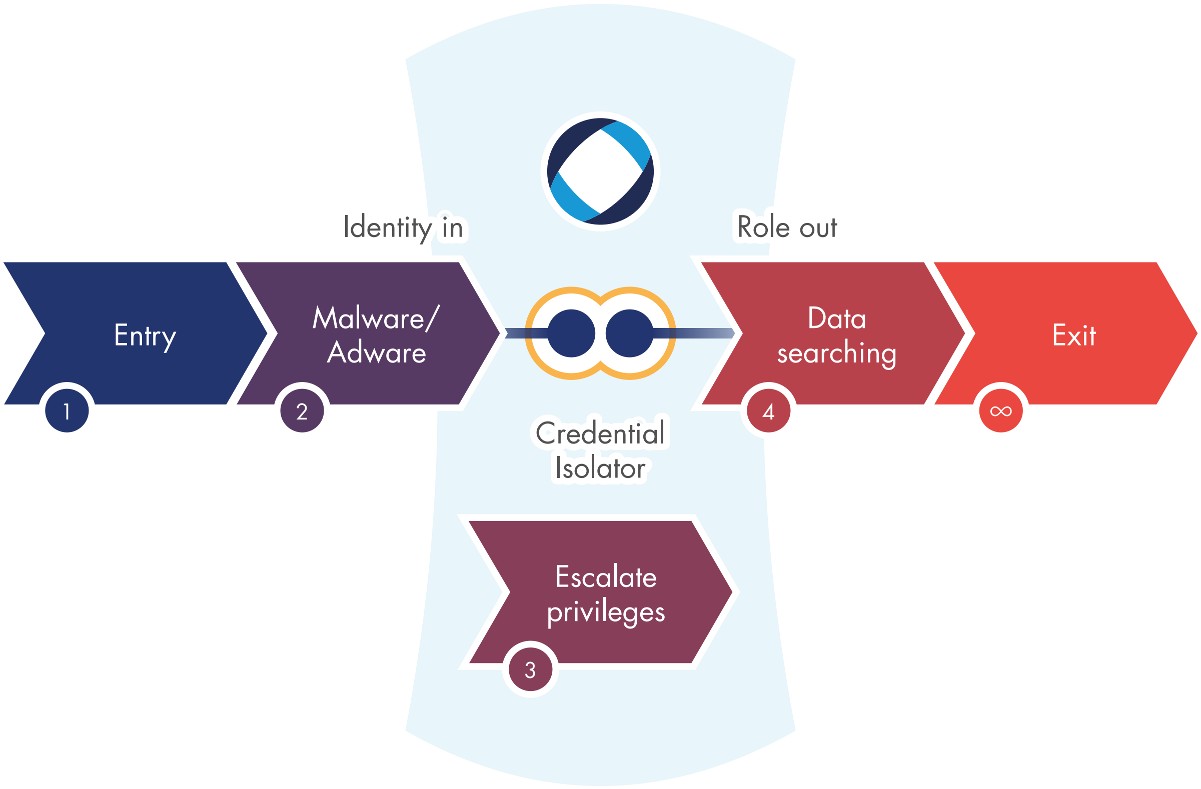
In this paper we have looked at several of the security breaches that can occur in creating and distributing passwords to privileged users.

In essence , it frequently comes down to two recurring issues:

- If privileged passwords have to pass through users' workstations they are vulnerable
- Human factors make giving passwords to privileged users a risk.

It was to avoid these breaches that Osirium invented its Privileged User Management solution, the PxM Platform, with its key tenets:

- Take the people out of the password problem using a model of 'Identity in, role out'
- Don't oblige people to remember or write down passwords
- Protect all systems and applications by 128 random character passwords that are automatically refreshed every week… but never enter user workstations
- Reduce the attack surface by automating routine tasks such as stop / start server, stop / start print queues, reset domain password.



In the diagram above we see how The Osirium PxM Platform separates privileged users from privileged credentials. The attacker may (1) have effected entry (if an insider attacker, he has an immediate advantage) and (2) installed Malware. At the crucial stage however of setting or raising privileges (3) Osirium acts as a proxy connection between the user and the devices they manage, effectively isolating credentials. All privileged users need to do is verify their identity, from which they are granted access to systems on the basis of the roles and times assigned to them. You could summarise the model succinctly as “Identity in, role out”.

In each instance the PxM Platform carries out the single sign-on or initiates the task. Privileges are restricted to the roles that users need on specific systems to carry out their job, and credentials are never revealed. Unlike VPN-connected users there is no opportunity for lateral movement. As privileged credentials never cross into the domain of the users’ system, they cannot be stolen, misused or phished.

Likewise, by allowing customers to automate a wide number of routine tasks, no privileged login is required.

In this way, Osirium emphatically addresses the five key password-related issues examined earlier. As passwords are never passed to or visible on the workstation, the risk from compromised workstations is avoided. The same applies for excessive demands on the human cognitive load and protecting against shoulder surfing. With regard to password sharing and phishing, in addition to never revealing the password to privileged users, Osirium only allows one instance of a password, and this negates the threat from these approaches. As an additional security measure, Osirium’s ability to carry out ‘certificate pinning’ means we would immediately detect if the wrong certificate were being used.

Separate people from passwords – or, to be exact, separate privileged users from privileged credentials. That’s one of the key design principles of the Osirium PxM platform, and one of the means by which Osirium continues to uniquely deliver value and cybersecurity protection for its customers.

NOTES

OSIRIUM

Osirium Ltd.
Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH

0118 324 2444 | info@osirium.com | osirium.com