PRIVILEGED ACCOUNTS DISCOVERY FOR WINDOWS

Executive Summary

Prepared for Acme Inc

Scan Date	01/08/2016 18:35:38. Scan completed in 50 minutes.
Directory Domain Scanned	test.acmeinc.com - Ou(s) Scanned: Entire Domain
Account Types Scanned	Windows Local Accounts, Active Directory Service Accounts

From insider threats to external attacks from nation states, the risks today are enormous including company reputation damage, dismissal of executives, punitive fines, costly remediation and expensive outages. IT infrastructure needs to be secured and that starts with privileged accounts which control the most critical access to your networks, systems and data. Privileged Account Management (PAM) is an area that needs to be addressed as part of any comprehensive security plan.

The analysis tested various configuration settings for accounts and passwords on your network and also included looking for areas where best practices are not being followed. Controlling the entire surface area of your network related to privileged account access is critical to maintaining your security posture. Many times these settings are left with default values or policies are often turned off for convenience of system administration rather than enforcing security best practice.

There are accounts on your network with local administrator rights on computers which is typically a sign of misconfiguration, abuse of privilege or even possible intrusion. The administrators group which conveys administrator rights must be tightly controlled to ensure no abuse of privilege is occurring.

There are service accounts on your network that have probably not been isolated correctly and are not being managed effectively. Service accounts represent enormous risk since they have privileged access and are often targeted in attacks. Best practices need to be followed for isolating the service accounts and the applications they run including inventory management and mandatory password rotation to reduce risk and prevent outages.

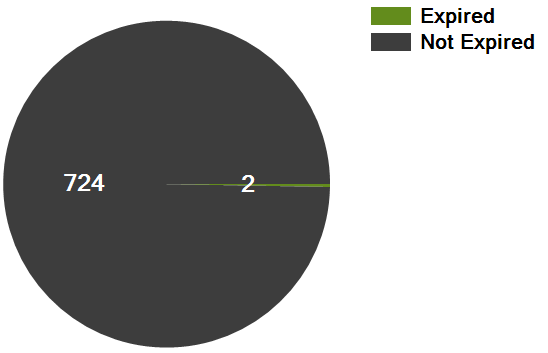
Executive Summary Continued

Non-expiring accounts on your network are a security risk and also indicate that your teams may be cutting some corners on procedures and best practices. All accounts should be set to expire to ensure that passwords are rotated which reduces their window of exposure for compromise.

There are accounts on your network which have not had their password changed within an acceptable period. This shows that accounts are being managed poorly and are vulnerable to compromise. There may also be password sharing, mismanaged accounts and probably some lack of accountability. Controls should be put in place to inventory password age and ensure that all account passwords are being changed on a regular basis.

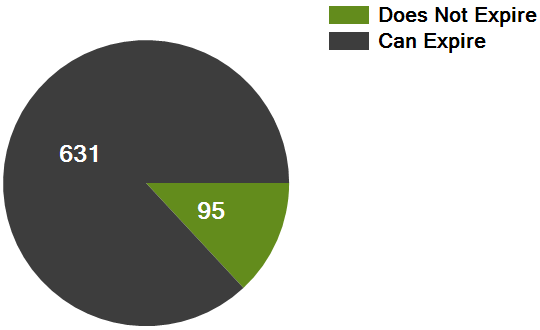
After reviewing the various controls, it is easy to see that improvements can be made to privileged account security which could greatly reduce your organization's risk to attack. Global brands such as Adobe are leveraging Thycotic's technology to ensure that their organization is secure. Can you really afford to hold off on your PAM initiative?

Windows Local Accounts



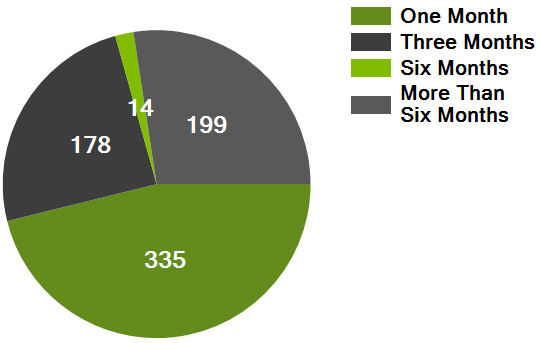
Password Expiration Health

The number of Windows local accounts that haven't had their password changed and are now expired. Expired passwords are an attack vector because they can be leveraged by both internal and external attackers. Frequent password changes help prevent abuse of privileged accounts.



Windows Accounts That Never Expire

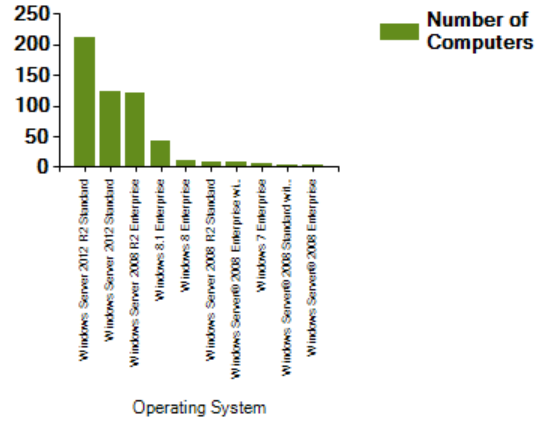
The number of Windows local accounts that have been marked on the operating system to never expire. Non-expiring passwords are security risks because if no automated solution is in place, privileged users are never prompted to change these passwords.



Password Age By Month

Windows local accounts with passwords that change infrequently are a security risk, because prior employees or attackers may use old passwords to gain access. Passwords should be changed on a regular basis, preferably on a schedule.

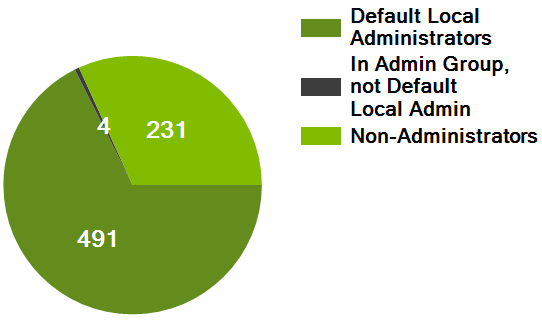
Windows Local Accounts



Operating System Breakdown

The distribution of operating systems found during Discovery. Older unsupported operating systems may present an attack vector for malware if updates are no longer issued.
The following operating systems are no longer supported by Microsoft:

- Windows XP
- Windows Server 2003
- Windows 2000



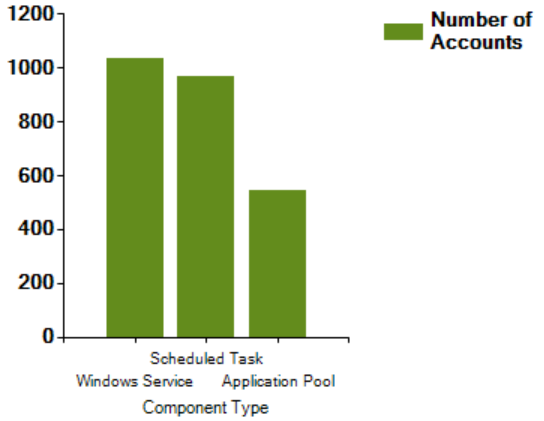
Unexpected Administrator Accounts

Windows local accounts that are not the default administrator account that are in the administrator's group. The presence of local accounts other than the built in administrator can signify misconfiguration or backdoor local accounts.

Windows Computer Scan Summary

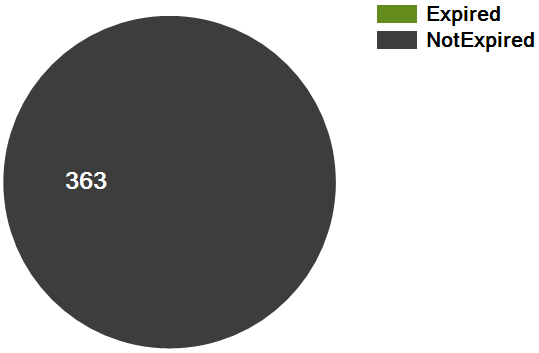
Windows Computers Scanned	552
Windows Accounts Found	726
Windows Accounts with Non-Expiring Passwords	95
Windows Accounts With Expired Passwords	2
Unexpected Privileged Windows Accounts	4

Active Directory Service Accounts



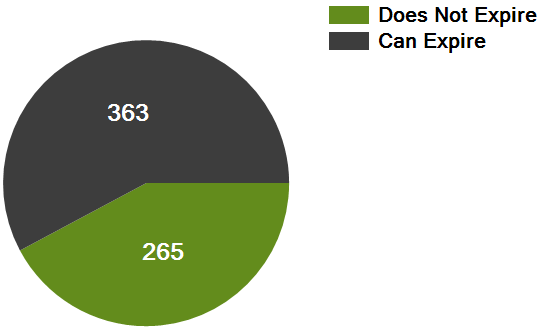
Windows Component Breakdown

The distribution of what service accounts are running among IIS Application Pools, Windows Services, and Scheduled Tasks.



Service Account Password Expiration Health

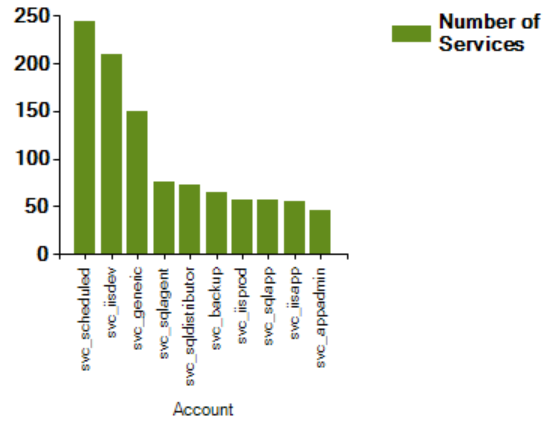
The number of domain service accounts that haven't had their password changed and are now expired. Due to the steps required to change service account passwords, these often do not get updated. Frequent password changes help prevent abuse of privileged accounts.



Service Accounts That Never Expire

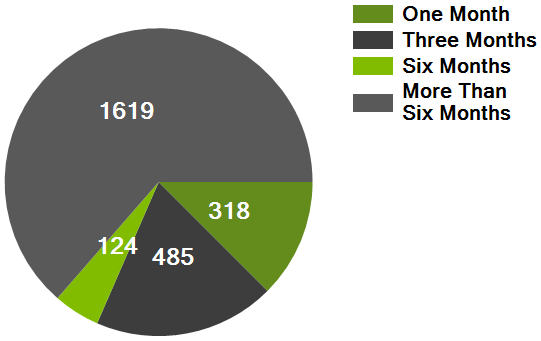
The number of domain service accounts that have been marked on the domain to never expire. Non-expiring passwords are security risks because over time the password proliferates and can be used by insider and outsider attacks.

Active Directory Service Accounts



Number of Applications Run By A Single Service Account

The more services, scheduled tasks, or application pools a single service account runs, the potential for greater risk during a breach. Running more applications means greater exposure if the password is ever compromised. More applications running under a single account also creates complexity and makes it difficult to change the password as dictated by compliance or security mandates.



Service Accounts Password Age By Month

Service accounts with passwords that change infrequently are a security risk, because prior employees or attackers may use old passwords to gain access. Passwords should be changed on a regular basis, preferably on a schedule.

Active Directory Service Accounts

Service Account Computer Scan Summary	
Windows Computers Scanned	552
Service Accounts in Use	363
Microsoft Scheduled Tasks	966
Windows Services	1037
IIS Application Pools	543
Service Accounts with Expired Passwords	0
Service Accounts with Non-Expiring Passwords	265
Number of Accounts Running More Than One Application	10