Cheatography

Security Problem Over-Privileged Accounts Cheat Sheet

by [deleted] via cheatography.com/2754/cs/12811/

Introduction

During a persistent attack, intruders will gain access to various accounts. If they stumble upon a highly privileged account suddenly they can take a giant leap forward and bypass everything we've done to slow them down and detect them. The worst thing is when the account they get access to is one that should never have had that amount of authority in the first place – an over-privileged account. Such security assessments are far too common. It will bebe difficult to stop this security violation but we need to put controls in place to prevent or at least notice when accounts have become over privileged. Here are 8 ways over-privileged accounts commonly arise and corresponding techniques for preventing them and tips for detecting them with the Windows Security Log where possible

Credit: http://www.ultimatewindowssecurity.com

Causes of Over Privileged Accounts

1. Granting inappropriate logon session type rights
2. Re-use of accounts
3. Lack of designated ownership for non-human accounts
4. Unreviewed job changes
5. Direct entitlements: failure to use groups
6. Out of control nested groups
7. Temporary emergency entitlements that never get removed
8. Lack of data or application owner involvement