Managing and Securing Windows Service Accounts

Bob McCoy, MCSE, CISSP/ISSAP
Technical Account Manager
Microsoft Corporation
Agenda

The basics
Best practices
Accounts and privileges
Tools
Why This is Important

“... service accounts are one of the simplest ways to turn a compromise of one computer system into a compromise of an entire network.”

“Protect Your Windows Network”
Least Privilege

A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform, and no others.
Least Service

The principle of least service states that the operating system and the network protocols available on any networked device should run only the exact services and protocols required to support the business purpose.
Attack Surface Reduction

Uninstall unnecessary components
Disable unnecessary features
Block access to unnecessary interfaces

Necessary / Unnecessary
Your mileage may vary
Privileges for Services

How do you know what privilege level a service really needs?

- User
- Print operators
- Backup operators
- Administrators
- AD account for network access
- Domain administrator account
- Software documentation?
Warning

“A process running on clients as a domain administrator is hazardous to your network health. It degrades the security of the entire domain to that of the least secure machine in the domain.”

“Protect Your Windows Network”
Account Types

Domain or Local
Admin or User
Unique or Shared

If shared, do you share across security boundaries?
Windows Privileges

SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeTcbPrivilege

C:\> showpriv SeRestorePrivilege
My Privileges

C:\>whoami /priv

(X) SeChangeNotifyPrivilege= Bypass traverse checking

(O) SeShutdownPrivilege= Shut down the system

(X) SeUndockPrivilege= Remove computer from docking

(X) SeCreateGlobalPrivilege= Create global objects
Good Practices

Create new account, with leading underscore in name
Use a very strong password
Revoke all logon rights – local and network
Set “Password never expires”
Set “User cannot change password”
Good Practices

Remove the account from all default groups

Never use an existing user’s account
Built-In Accounts

System
Local Service
Network Service
Local System

- Full access to the computer
- Includes Dir Svcs on domain controllers
- Host computer account in the domain
  - `DOMAIN\<machine name>$`
  - `NT AUTHORITY\System`
- Resource authorization can be managed by security groups
Local Service

Reduced privileges – similar to a local user account

Network access via null session – anonymous credentials

NT AUTHORITY\LocalService
Network Service

Reduced privileges – similar to a local user account

Host computer account in the domain

DOMAIN\<machine name>$

NT AUTHORITY\NetworkService
Task List

demo
Account Security Spectrum

- Most Secure
  - One-time account per System
  - You may want to be here

- Least Secure
  - One account everywhere, forever
  - Or possibly here

You may want to be here or possibly here.
Mitigation

Segmentation
Very strong passwords
Desired configuration monitoring
Tools

Services.msc
GPEdit.msc
RSoP.msc
SC.exe
WMIC.exe
Task Manager
Tlist / Tasklist
Process Explorer
Passgen
Windows Power Shell
Tools

demo
Resources

“Protect Your Windows Network”
http://www.protectyourwindowsnetwork.com

Windows XP Security Guide
http://www.microsoft.com/technet/security/prodtech/windowsxp/


The Services and Service Accounts Security Planning Guide
Download
http://go.microsoft.com/fwlink/?LinkId=41312

Threats and Countermeasures (Chapter 7- System Services)
http://www.microsoft.com/technet/security/topics/serversecurity/